UNIVERZITA PALACKÉHO V OLOMOUCI
PŘÍRODOVĚDECKÁ FAKULTA
KATEDRA ALGEBRY A GEOMETRIE

Mediální kvazigrupy a geometrie

Diplomová práce

Vedoucí práce:
Doc. RNDr. Alena Vanžurová, CSc.

Vypracovala:
Bc. Zuzana Bartošková
Matematika – Geografie, 2. ročník

Rok odevzdání práce: 2011

Prohlášení

Prohlašuji, že jsem zpracovala tuto diplomovou práci samostatně pod vedením Doc. RNDr. Aleny Vanžurové, CSc. a že jsem v seznamu použité literatury uvedla všechny zdroje použité při zpracování práce.

V Olomouci dne 26. 7. 2011

Zuzana Bartošková

Poděkování

Na tomto místě bych ráda poděkovala své vedoucí diplomové práce, Doc. RNDr. Aleně Vanžurové, CSc., za obětavou spolupráci a čas, který mi věnovala při konzultacích.

Obsah

Úvod

Kvazigrupy nepatří mezi příliš známé algebraické struktury, při studiu na vysoké škole se s nimi většina studentů nesetká. Většina autorů o nich publikuje pouze v angličtině. Mým úkolem bylo navázat na bakalářskou práci a rozšířit ji o další vlastnosti kvazigrup.

Práce je rozdělena do pěti kapitol, v první z nich jsou uvedeny potřebné poznatky z univerzálních algeber, druhá kapitola se zabývá kvazigrupami, zvláště pak GS-kvazigrupami a hexagonálními kvazigrupami. Ve třetí kapitole jsou sestrojeny konkrétní příklady GS a hexagonálních kvazigrup z konečných těles. Čtvrtá část se zabývá izotopiemi kvazigrup. Poslední část se věnuje geometrii v GS-kvazigrupách.

1 Univerzální algebry

Tato úvodní kapitola se věnuje hlavně zavedení potřebných pojmů z teorie univerzálních algeber, čerpáno bylo z literatury [1], [4], [5] a [6] .

1.1 Operace, algebra

Definice 1.1.1: Nechť $A \neq \emptyset$ je neprázdná množina a f_i^A je n_i-ární operace na A pro $i = 1,...,k$. Pak dvojici $\mathbf{A} = \left(A, \left(f_i^A\right)_{i=1}^k\right)$ nazveme *algebrou typu* $\tau = (n_1,...,n_k)$. Množině A říkáme *nosič algebry*.

Pro $n = 2$ mluvíme o *binární operaci* na množině A. Zde budeme pro binární operace $f : A^2 \to A$ nejčastěji používat symboly $\cdot$, +, -, $\oplus$, $\otimes$ apod. Zpravidla místo $f(a,b)$ píšeme $a\, f\, b$.

Zobrazení $f : A^n \to A$ nazveme *n-ární operace* na A. Doplníme-li $A^0 = \{\emptyset\}$, pak nulární operaci lze brát jako zobrazení $f : \{\emptyset\} \to A$; jedná se vlastně o výběr jednoho prvku z A.

1.2 Grupoidy

Definice 1.2.1: Algebru $\mathbf{G} = (G,\cdot)$ typu (2), tedy s jednou binární operací, nazveme *grupoidem*. Řekneme, že grupoid $\mathbf{G}$ má vlastnost *krácení zleva*, platí-li kvaziidentita $z \cdot x = z \cdot y \Rightarrow x = y$, tedy pro libovolný výběr prvků a,b,c z nosiče G platí implikace $c \cdot a = c \cdot b \Rightarrow a = b$; *krácení zprava*, platí-li v $\mathbf{G}$, že $x \cdot z = y \cdot z \Rightarrow x = y$; *krácení*, má-li současně vlastnost krácení zleva i zprava.

Definice 1.2.3: Prvek $e \in G$ nazveme *levým neutrálním prvkem* grupoidu $\mathbf{G} = (G,\cdot)$, splňuje-li identitu $e \cdot x = x$, tj. $e \cdot a = a$ pro všechna $a \in G$. Podobně *pravý neutrální prvek* je charakterizován identitou $x \cdot e = x$. *Neutrální prvek* je současně levým i pravý neutrálním prvkem.

Snadno se ukáže, že grupoid nemůže mít dva různé neutrální prvky: $e' \neq e$ $(e' = e' \cdot e = e)$.

Definice 1.2.4: Grupoid, který splňuje asociativní zákon, tedy identitu $x \cdot (y \cdot z) = (x \cdot y) \cdot z$, nazveme *pologrupou*.

Definice 1.2.5: Prvek $a \in G$ grupoidu $(G,\cdot)$ nazveme *idempotentní*, jestliže splňuje $a^2 = a$. Grupoid je *idempotentní*, platí-li v něm identita $x^2 = x$.

Definice 1.2.6: Grupoid se nazývá *komutativní* nebo *abelovský*, platí-li v něm identita $x \cdot y = y \cdot x$.

Definice 1.2.7: Grupoid je *mediální*, jestliže v něm platí $(xy)(uv) = (xu)(yv)$.

Definice 1.2.8: Ke každému grupoidu $(G,\cdot)$ můžeme sestrojit tzv. *duální* grupoid $(G,\cdot^{op})$, kde $x \cdot^{op} y = y \cdot x$.

Definice 1.1.10: *Levá translace* L_a prvkem a v grupoidu $(G,\cdot)$ je zobrazení $L_a : G \to G$, $L_a(y) = a \cdot y$. *Pravá translace* R_b prvkem b v grupoidu $(G,\cdot)$ je zobrazení $R_b : G \to G$, $R_b = x \cdot b$.

1.3 Grupy a kvazigrupy

Definice 1.3.1: *Kvazigrupa* je grupoid $(G,\cdot)$, ve kterém mají rovnice tvaru $x \cdot a = b$, $a \cdot y = b$ jednoznačně určená řešení pro všechny prvky *a,b* z *G*.
Jinak řečeno, ve vztahu $x \cdot y = z$ je každý prvek určen zbývajícími dvěma.

Pozn. 1.3.1: Každá kvazigrupa má vlastnost krácení (zleva i zprava). Pro kvazigrupu vznikají z této jednoznačné řešitelnosti rovnic další dvě doprovodné operace:
pro $a,b \in G$, $a \setminus b$ je právě ten prvek *x*, pro který $a \cdot y = b$;
operaci \: $G \times G \to G, (a,b) \mapsto a \setminus b$ můžeme říkat *levé dělení*.
Operaci /: $G \times G \to G, (a,b) \mapsto b / a$, kde b / a je rovno právě tomu *y*, pro které $x \cdot a = b$, můžeme říkat *pravé dělení*.

Jestliže $(G,.)$ je kvazigrupa, pak také duální grupoid $(G,\cdot^{op})$ je kvazigrupou, pro kterou zřejmě platí $/^{op} = \backslash$ a $\backslash^{op} = /$, tedy operace pravého a levého dělení v duální kvazigrupě jsou rovny levému respektive pravému dělení v původní kvazigrupě.

Poznamenejme, že kvazigrupu lze definovat i v typu $(2,2,2)$ pomocí všech tří zmíněných operací $\cdot,\backslash,/$ a vhodných identit.

Definice 1.3.2: Kvazigrupě s neutrálním prvkem budeme říkat *lupa*. Značit ji budeme $\mathbf{L}=(G,e,\cdot)$.

Pozn. 1.3.2: *Latinským čtvercem* řádu *n* nad množinou *G* , kde $G=|n|$, nazveme matici $A(i, j)$, $1 \le i, j \le n$, prvků z *G*, pro kterou

(i) v každém řádku jsou všechny prvky různé,

(ii) v každém sloupci jsou všechny prvky různé.

Jinak řečeno, v řádcích a sloupcích jsou permutace (konečné) množiny *G*. Místo o matici se častěji hovoří o tabulce prvků.

Vynecháme-li operaci, „levé“ a „horní“ záhlaví v tabulce kvazigrupy, zůstane nám v podstatě latinský čtverec.

Vysvětlení názvu lze najít např. v literatuře [4], prvky takových schémat totiž bývaly značeny latinskými písmeny.

Definice 1.3.3: *Grupu* můžeme zavést jako kvazigrupu, která je současně pologrupou.

Lze pak ukázat, že grupa má oboustranný neutrální prvek *e* a ke každému prvku $a \in G$ existuje oboustranný inverzní prvek a^{-1}; $a \cdot a^{-1} = a^{-1} \cdot a = e$; [1].

Poznamenejme, že grupa se často zavádí jako pologrupa s neutrálním prvkem, v níž ke každému prvku existuje prvek inverzní.

Definice 1.3.4: (alternativní definice pro grupu)

Grupa je neprázdná podmnožina $G \neq \emptyset$ spolu s binární operací, označovanou jako skládání, která má následující vlastnosti:

(i) (asociativita) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ pro všechna $a, b, c \in G$.

(ii) (existence jednotky) Existuje prvek $e \in G$ takový, že $e \cdot a = a \cdot e = a$ pro každé $a \in G$.

(iii) (inverzní prvky) Pro každé $a \in G$ existuje prvek $a^{-1} \in G$ takový, že platí $a \cdot a^{-1} = a^{-1} \cdot a = e$.

Obvyklé značení: multiplikativní … $(G, e, \cdot)$, aditivní … $(G, 0, +)$.

Grupa je *konečná*, obsahuje-li konečný počet prvků.

Definice 1.3.5: *Podgrupa* je podmnožina grupy, která je sama grupa vzhledem k zúžené operaci.

Definice 1.3.6: Mohutnost nosiče *G* konečné grupy **G** se nazývá *řádem* grupy, ozn. $|G| = moh\ G$.

Definice 1.3.7: Grupa (podgrupa) se nazývá *cyklická*, je-li generována jedním prvkem, tj. je-li tvaru $\langle a \rangle = \{a^n | n \in Z\}$.

Definice 1.3.8: Zobrazení $\psi : G \to H$ nazveme *homomorfismem* grupy $\mathbf{G} = (G, \cdot)$ na grupu $\mathbf{H} = (H, \circ)$, jestliže platí $\psi(a \cdot b) = \psi(a) \circ \psi(b)$. Bijektivní homomorfismus se nazývá *izomorfismus*. *Automorfismus* grupy $\mathbf{G} = (G, \cdot)$ je izomorfismem **G** na **G**. Všechny automorfismy grupy **G** spolu s operací skládání opět tvoří grupu označovanou jako *Aut* **G**.

Definice 1.3.9: Nechť *M* je množina a $\mathbf{G} = (G, e, \cdot)$ je grupa. Zobrazení $\rho : G \times M \to M$, $(g, m) \mapsto g \cdot m$ nazveme operací nebo akcí grupy **G** na množině *M*, platí-li:

(i) $e \cdot m = m$ pro libovolné $m \in M$,

(ii) $(gh)(m) = g(hm)$ pro všechna $m \in M$ a libovolná $g, h \in G$.

Řekneme, že *G* operuje *tranzitivně* na *M*, jestliže pro libovolná $m, m' \in M$ existuje $g \in G$ tak, že $g \cdot m = m'$. *G* operuje *dvojně tranzitivně*, jestliže pro libovolné prvky $a, b, a', b' \in M$ existuje *g* z *G* takové, že $g(a) = a'$, $g(b) = b'$.

Pozn. 1.3.3: Každý prvek $g \in G$ operuje na M jako permutace množiny M, $\pi_g : m \mapsto g \cdot m$; zobrazení $g \mapsto \pi_g$ je pak grupový homomorfismus grupy $\mathbf{G}$ na podgrupu permutační grupy *Perm M*.

1.4 Okruhy, obory integrity, tělesa

Definice 1.4.1: *Okruh* je algebra $(R,0,+,\cdot)$ typu $(0,2,2)$ taková, že

(i) $(R,0,+)$ je komutativní grupa (inverzní operaci označíme –),

(ii) násobení je asociativní,

(iii) sčítání a násobení jsou vázány distributivními zákony.

Jako důsledek základních axiomů dostaneme

$a \cdot 0 = 0 \cdot a = 0$ pro všechna $a \in R$, $(-a) \cdot b = a \cdot (-b) = -a \cdot b$ pro všechna $a, b \in R$.

Definice 1.4.2: *Oborem integrity* rozumíme okruh $\mathbf{R}$ s jednotkou $1 \neq 0$ (tj. prvkem splňujícím $a \cdot 1 = 1 \cdot a = a$ pro $a \in R$), který je komutativní a nemá dělitele nuly, tedy splňuje $a \cdot b = 0 \Rightarrow a = 0$ nebo $b = 0$.

Definice 1.4.3: *Těleso* (nekomutativní) je algebra $\mathbf{F}=(F,0,1,+,\cdot)$ typu $(0,0,2,2)$ taková, že

(i) $(F,0,+)$ je komutativní grupa,

(ii) $0 \neq 1$,

(iii) $\mathbf{F}^* = (F \setminus \{0\},1,\cdot)$ je grupa,

(iv) násobení je asociativní, tedy platí identita $(x \cdot y) \cdot z = x \cdot (y \cdot z)$,

(v) platí identity („distributivita“ zprava a zleva)

$(x + y) \cdot z = x \cdot z + y \cdot z$, $z \cdot (x + y) = z \cdot x + z \cdot y$.

Tedy těleso je speciálním případem okruhu.

Je-li splněno $x \cdot y = y \cdot x$, nazýváme těleso *komutativním* (komutativní těleso je oborem integrity).

Jestliže $|F| = m$ pro nějaké přirozené číslo, mluvíme o *konečném tělese*; značíme $GF(m)$ („*G*“ podle E. Galoise).

Vlastnosti konečných těles byly podrobně prozkoumány a jejich struktura je známa. Mimo jiné, konečné těleso je vždy komutativní; [5].

1.5 Konečná tělesa

Konečná tělesa mají řadu důležitých aplikací např. v teorii kódování (hledání a opravování chyb), kryptografii a kombinatorice.
Je-li $\mathbf{F}$ konečné těleso a $\mathbf{F}^*$ jeho multiplikativní grupa, dá se dokázat následující.

Věta 1.5.1: Je-li $\mathbf{F} = (F, 0, 1, +, \cdot)$ konečné těleso, pak platí:

(i) $\mathbf{F}$ má prvočíselnou charakteristiku p (tedy nejmenší prvočíslo p, pro které $p \times 1 = 0$, kde $\times$ značí přirozený násobek , $p \times 1 = 1 + 1 + ... + 1$, kde 1 sčítáme p-krát),

(ii) multiplikativní grupa $\mathbf{F}^*$ tělesa $\mathbf{F}$ je cyklická.

Pozn. 1.5.1: Řád prvku α v grupě je nejmenší kladné číslo r, pro které $\alpha^r = 1$. Číslu k, pro které $\alpha^k = 1$, se říká *exponent*; řád je tedy nejmenší exponent daného prvku α.

Důkaz věty 1.5.1:

(i) Kdyby p bylo složené číslo, $p = k \cdot l$, pak by $p \times 1 = 1 \times 1 \times ... \times 1 = (k \times 1) \cdot (l \times 1) = 0$, tedy aspoň jeden z činitelů $k \times 1$, $l \times 1$ by musel být roven nule. Potom by však p nebylo nejmenším číslem takové vlastnosti.

(ii) Je-li $|F| = m$, pak $|F^*| = m - 1$. Mezi prvky z F^* vybereme ten prvek α, který má maximální řád $r \leq m - 1$. Protože F^* je komutativní grupa, dá se použít věty z teorie grup. Dostaneme $\alpha^r = 1$ pro všechna $\alpha \in F^*$.

Definice 1.5.1: *Podtěleso* tělesa $\mathbf{F}$ je každá podmnožina P tohoto tělesa, která je sama tělesem vzhledem k operacím definovaným na F.

Definice 1.5.2: Těleso, které nemá žádná vlastní podtělesa, nazveme *prvotělesem*. Značíme $\mathbf{F_0}$.

Věta 1.5.2: Každé těleso $\mathbf{F}$ obsahuje některé prvotěleso jako své podtěleso.

Důkaz: Lze najít např. v [6].

Věta 1.4.3: Buď $\mathbf{F}$ konečné těleso. Pak $\mathbf{F}$ obsahuje p^n prvků, kde p je prvočíslo a n nějaké přirozené číslo.

Důkaz: Protože je $\mathbf{F}$ konečné, má nutně prvočíselnou charakteristiku. Podle předchozí věty obsahuje $\mathbf{F}$ prvotěleso $\mathbf{F_0}$. Těleso $\mathbf{F}$ je tedy množina všech lineárních kombinací prvků z n-členné báze vektorového prostoru $\mathbf{F}$ nad tělesem $\mathbf{F_0}$, přičemž koeficienty těchto lineárních kombinací probíhají nezávisle na sobě p-prvkové těleso $\mathbf{F_0}$. Tedy $|F| = p^n$.

2 Vztah komutativních grup a některých typů kvazigrup

Tato kapitola čerpá hlavně z literatury [3], [8] a [9].

2.1 Toyodova věta

Věta 2.1.1: *T-kvazigrupa* $(G,\circ)$ („T“ podle japonského autora Toyody, převzato z [3]) je dána následující konstrukcí. Je-li $\mathbf{G}=(G,+)$ komutativní grupa, $c \in G$ a $\alpha, \beta \in Aut\ \mathbf{G}$ jsou automorfismy grupy, zavedeme binární operaci „$\circ$“ vztahem $x \circ y = \alpha(x) + \beta(y) + c$ pro všechna $x, y \in G$.

Konvence: Abychom ušetřili psaní závorek, budeme předpokládat, že vynecháme-li explicitní zápis operace, má provedení součinu přednost před vyznačeným násobením. Např. medialitu pak můžeme psát $ab \circ cd = ac \circ bd$.

Pozn. 2.1.1: Jak plyne z tzv. Toyodovy věty, každá mediální kvazigrupa je T-kvazigrupa, pro niž příslušné grupové automorfismy komutují, $\alpha\beta = \beta\alpha$.

Příklad 2.1.1: Uvažujme komutativní grupu $(Z_n,\oplus)$ zbytkových tříd modulo $n \in N$ s příslušnou operací sčítání tříd. Zvolme $\bar{a}, \bar{b} \in Z_n$ tak, aby příslušná čísla *a*, *b* reprezentující tyto třídy byla nesoudělná, tedy $NSD(a,n) = NSD(b,n) = 1$, $\bar{c} \in Z_n$.
Pak $x \circ y = a \cdot x + b \cdot y + c \pmod{n}$ definuje T-kvazigrupu $(Z_n,\circ)$, (stačí si uvědomit, že $\alpha : x \mapsto ax \pmod{n}$ a $\beta : y \mapsto by \pmod{n}$ jsou automorfismy, dokonce komutující, a $x \circ y = \alpha(x) + \beta(y) + c$).

Věta 2.1.3: Je-li $(G,0,+)$ grupa a $f : G \to G$ zobrazení, říkáme, že f je *lineární*, platí-li $f(x+y) = f(x) + f(y)$ pro všechna $x, y \in G$, a *afinní*, je-li splněno $f(x+y) = f(x) + f(y) - f(0)$.

V poněkud jiné terminologii, užité v [3], řekneme, že grupoid $(G,*)$ je *lineární nad komutativní grupou* $\mathbf{G}=(G,0,+)$ *se zobrazením* φ, existuje-li automorfismus $\varphi \in Aut\ \mathbf{G}$ $(\varphi \neq id_G)$ takový, že platí pro všechna $x, y \in G$

$$x * y = x + \varphi(y - x). \tag{2.1}$$

V dalším ukážeme, že ve speciálním případě se konstrukcí (2.1) získá jistá zajímavá třída kvazigrup, tzv. GS-kvazigrup.

2.2 GS-kvazigrupy

V této části nás budou zajímat idempotentní kvazigrupy, které splňují jisté speciální identity (viz následující lemma), kterým budeme říkat GS-identity.

Lemma 2.2.1: Je-li $(G,\cdot)$ grupoid s krácením (zleva i zprava), pak jsou v něm následující identity (GS-identity) ekvivalentní :

(i) $x(xy \cdot z) \cdot z = y$, tj. $[x \cdot ((x \cdot y) \cdot z] \cdot z = y$,

(ii) $x \cdot (x \cdot yz)z = y$.

Důkaz: Užijeme identitu (i) pro *x*, *z* a yz. Použijeme $[x \cdot ((x \cdot yz) \cdot z)] \cdot z = yz$, odtud po krácení zprava dostáváme (ii). Podobně naopak: $x \cdot [x \cdot (xy \cdot z) \cdot z] = xy$ (podle (i) pro *x*, *z* a *xy*), nyní krátíme zleva.

Lemma 2.2.2: Grupoid s krácením, který splňuje identitu (i), je kvazigrupa.

Důkaz: Máme zjistit, zda rovnice $a \cdot x = b$ a $y \cdot a = b$ mají jednoznačně určené řešení. Pro druhou rovnici stačí vzít $y = a(ab \cdot a)$, podle (i) je řešením. Pro první rovnici lze sestrojit prvek $x = (a \cdot ab)a$, který je řešením dle (ii) (díky implikaci (i)$\Rightarrow$(ii)). Jednoznačnost plyne z vlastnosti krácení.

2.2.1 Elementární vlastnosti GS-kvazigrup

Definice 2.2.1.1: *GS-kvazigrupou*, nebo *kvazigrupou zlatého řezu*, nazveme idempotentní kvazigrupu $(x^2 = x)$, která splňuje kteroukoli z identit z lemmatu 2.2.1 (a tedy též tu zbývající).

Lemma 2.2.1.1: Je-li $(G,\cdot)$ GS-kvazigrupa, pak i duální grupoid $(G,\cdot^{op})$ je GS-kvazigrupa.

Důkaz: Řešitelnost rovnic je zřejmá (jen se vymění pořadí rovnic oproti původní struktuře), idempotentnost je splněna, definující identita (i) pro $\cdot^{op}$ je ekvivalentní s vlastností (ii) pro původní operaci.

Věta 2.2.1.1: Nechť $\mathbf{G}=(G,e,+)$ je komutativní grupa. Nechť existuje automorfismus $\varphi \in Aut\ \mathbf{G}$ grupy takový, že

$$\varphi^2 = \varphi + id_G . \tag{2.2}$$

Zaveďme na nosiči G binární operaci „$*$“ vztahem $a * b = a + \varphi(b - a)$ pro libovolné $a,b \in G$. Pak $(G,*)$ je GS-kvazigrupa.

Důkaz: Ukažme nejprve, že rovnice $a * x = b$ a $y * a = b$ mají v G jednoznačně určené řešení: $a * x = b \Leftrightarrow a + \varphi(x - a) = b \Leftrightarrow \varphi(x - a) = b - a \Leftrightarrow x = a + \varphi^{-1}(b - a)$,

tedy $x = a + \varphi^{-1}(b - a)$ je řešením $a * x = b$. Pro případ druhé rovnice musíme použít podmínky (2.2): $y * a = b \Leftrightarrow y + \varphi(a - y) = b \Leftrightarrow y + \varphi(a) - \varphi(y) = b \Leftrightarrow \varphi(y) + \varphi \circ \varphi(a) -$

$- \varphi \circ \varphi(y) = \varphi(b) \Leftrightarrow$ (použijeme: $(\varphi \circ \varphi)(y) = \varphi(y) + y$)) $\Leftrightarrow (\varphi \circ \varphi)(a) - y = \varphi(b) \Leftrightarrow$

$\Leftrightarrow y = \varphi^2(a) - \varphi(b)$. Tedy $y = \varphi^2(a) - \varphi(b)$ je jediným řešením rovnice $y * a = b$.

Dokažme idempotentnost: $a * a = a + \varphi(a - a) = a + \varphi(e) = a + e = a$.

Ukažme platnost „identity zlatého řezu“. Dostáváme postupně: $(a * b) * c =$

$= a * b + \varphi(c - a * b) = a + \varphi(b - a) + \varphi(c - a - \varphi(b - a)) = a + \varphi(b + c - 2a) - \varphi^2(b - a) =$
$= a + \varphi(b) + \varphi(c) - 2\varphi(a) - \varphi(b) + \varphi(a) - b + a = \varphi(c - a) - b + 2a$, tedy $(a * b) * c =$

$= 2a - \varphi(a) - b + \varphi(c)$.

Tedy $[a * ((a * b) * c)] * c = 2a - \varphi(a) - [2a - \varphi(a) - b + \varphi(c)] + \varphi(c) = b$.

Lze dokázat, že také naopak každá GS-kvazigrupa vzniká z nějaké komutativní grupy právě popsaným způsobem, [3].

Věta 2.2.1.2. Je-li **F**=$(F,0,1,+,\cdot)$ těleso, v němž má rovnice

$$q^2 - q - 1 = 0 \tag{2.3}$$

řešení $q \in F$, a binární operace $*$ na F je daná vztahem

$$a * b = (1-q)\cdot a + q \cdot b, \tag{2.4}$$

pak $(F,*)$ je GS-kvazigrupa.

Prvku *q* budeme v dalším říkat *směrnice*.

Důkaz: Zobrazení φ dané vztahem $\varphi(a) = L_q(a) = q \cdot a$, tedy levá translace prvkem *q*, je jistě automorfismem (komutativní) aditivní grupy $(F,0,+)$ daného tělesa **F** a zobrazení $\varphi = L_q$ můžeme nazvat *dilatací* prvkem *q*. Ze vztahu (2.3) dostáváme (po násobení zprava prvkem *a*) $q\cdot(qa) - q\cdot a - a = 0$ pro libovolné $a \in F$ a dále $\varphi^2 - \varphi - id_F = 0$; $\varphi^2 = \varphi + id_F$. Zobrazení φ tedy splňuje předpoklad (2.2) předchozí věty . Vztah (2.4) můžeme přepsat takto: $a * b = a + q\cdot(b-a) = a + \varphi(b-a)$. Naše operace $*$ je tedy definována stejně jako ve větě 2.2.1.1, a proto je $(F,*)$ GS-kvazigrupa.

Lemma 2.2.1.2: Nechť $(G,*)$ je GS-kvazigrupa sestrojená pomocí vztahu (2.4) z konečného tělesa a řešení rovnice (2.3), pak i duální kvazigrupa $(G,*^{op})$ je kvazigrupou zlatého řezu. [8]

Důkaz: Násobení v kvazigrupě je pomocí směrnice *q* zavedeno takto:
$a * b = (1-q)\cdot a + q\cdot b$, pro $q = q_1$: $a * b = (1-q_1)\cdot x + q_1 \cdot y$, ale $1 - q_1 = q_2$ a $q_1 = 1 - q_2$,
duální operaci můžeme tedy vyjádřit takto:
$x *^{op} y = y * x = (1-q_1)\cdot y + q_1 \cdot x = (1-q_2)\cdot x + q_1 \cdot y$.

Lemma 2.2.1.3: Každá GS-kvazigrupa je mediální.

Důkaz: Máme dokázat, že platí $xy \cdot uv = xu \cdot yv$. Opakovaně použijeme GS-identity (i) a (ii), získáme $xu\cdot(xy\cdot uv)v = [xu]\cdot[(xy\cdot uv)v] = [x[xy\cdot(xy\cdot uv)v]]\cdot[(xy\cdot uv)v] = y =$
$= xu\cdot(xu\cdot yv)\cdot v$. Užitím krácení zleva prvkem *xu* a zprava prvkem *v* dostaneme $xy\cdot uv = xu\cdot yv$.

Příklad 2.2.1.1: Uvažujme těleso komplexních čísel $(C,+,\cdot)$ a jeho prvek $q=\frac{1}{2}\left(1+\sqrt{5}\right)$ nebo $q=\frac{1}{2}\left(1-\sqrt{5}\right)$. Snadno se ověří (díky levé distributivitě), že levý zdvih prvkem *q*, tj. zobrazení $L_q : z \mapsto zq$, $z \in C$, je automorfismem komutativní grupy $(C,+)$ (to platí samozřejmě pro levý zdvih libovolným prvkem z *C*). Na *C* zaveďme novou operaci „$\circ$“ vztahem (2.1) pro $\varphi = L_q$, tj. $z \circ w = z + q \cdot (w - z)$ pro $z, w \in C$. Ukážeme, že grupoid $(C,\circ)$ (lineární nad $(C,+)$ se zobrazením L_q) je idempotentní kvazigrupa splňující identitu (i).

Nejprve dokažme jednoznačnou řešitelnost rovnic. Vztah $a \circ x = b$ znamená $a + q \cdot (x - a) = b$, tedy má platit $a + q \cdot x - q \cdot a = b$, nebo ekvivalentně $q \cdot x = b + (q-1) \cdot a$. Tato rovnice má v *C* jediné řešení $x = a + L_{q^{-1}}(b-a) = = a + q^{-1}(b-a)$. Najít řešení druhé rovnice se nám podaří takto. Vztah $y \circ a = b$ je ekvivalentní s $y + q(y-a) = b$, neboli $y + q \cdot y - q \cdot a = b$, což lze psát jako $(1-q)y = b - qa$. Odtud $y = (1-q)^{-1}(b-qa)$. Řešení *y* lze zapsat ještě v jiném tvaru. Snadno ověříme, že náš prvek splňuje $q^2 - q - 1 = 0$. Odtud plyne, že pro automorfismus $\varphi = L_q$ platí $(\varphi \cdot \varphi)(a) - \varphi(a) - a = 0$, $a \in C$, neboli $\varphi^2 - \varphi - id_C = 0$, což je (2.2).

Ze vztahu $y + \varphi(a) - \varphi(y) = b$ (pro $\varphi = L_q$) dostaneme $\varphi(y) + (\varphi \cdot \varphi)(a) - (\varphi \cdot \varphi)(y) = = \varphi(b)$, a tedy díky předchozímu $y = (\varphi \cdot \varphi)(a) - \varphi(b)$, což můžeme přepsat jako $y = q \cdot (q \cdot a) - q \cdot b$.

Idempotentnost plyne přímo z definice operace: $a \circ a = a + q(a-a) = a$.

Ověřme (i). Postupně dostáváme $a \circ b = a + \varphi(b-a)$, $(a \circ b) \circ c = = a + \varphi(b-a) + \varphi(c - (a + \varphi(b-a))) = (\varphi \cdot \varphi)(a) - 2\varphi(a) + a - (\varphi \cdot \varphi)(b) + \varphi(b) + \varphi(c)$. Užitím (2.2) vztah zjednodušíme na $(a \circ b) \circ c = 2a - \varphi(a) - b + \varphi(c)$. Postupujeme dále, předchozí rovnosti použijeme pro $(a \circ b) \circ c$ místo *b*: $(a \circ ((a \circ b) \circ c)) \circ c = 2a - \varphi(a) - (2a - \varphi(a) - b + \varphi(c)) + \varphi(c) = b$.

Uvažujme $C \approx R \times R$ jako Gaussovu rovinu. Povšimneme si, že pro dva různé prvky $a, b \in C$ můžeme vztah „$\circ$“ přepsat jako $\frac{a \circ b - a}{b - a} = q$, nebo $a \circ b - a = q(b-a)$. Přitom $a, b, a \circ b$ jsou tři body na přímce, *q* je tedy dělící poměr bodu $a \circ b$ vzhledem k bodům *a*, *b* (v Gaussově rovině). Pro $q = \frac{1}{2}\left(1+\sqrt{5}\right)$(popř. pro $q = \frac{1}{2}\left(1-\sqrt{5}\right)$) dělí bod *b* (popř. bod *a*)

dvojici $a,\ a \circ b$ $(b,\ a \circ b)$ v poměru *zlatého řezu*, proto byl pro tuto třídu kvazigrup v [2] zvolen název GS-kvazigrupy (z anglického golden section, i když přesnější by bylo golden ratio).

Pozn. 2.2.1.1. Pro lepší představu si uveďme definici zlatého řezu na úsečce. Mějme úsečku AB, kterou rozdělíme bodem C na dvě části tak, aby úsečka AC byla delší než úsečka CB. Je-li poměr delší části k celé úsečce stejný jako poměr kratší části k delší části, pak je úsečka rozdělena v poměru zlatého řezu. Zajímá nás poloha bodu C, pokud si označíme $|AB| = a$, $|AC| = x$, $|CB| = x - a$, obdržíme rovnici $\frac{x}{a} = \frac{a-x}{x}$, jejím řešením jsou čísla $\frac{1}{2}\left(1+\sqrt{5}\right)$ a $\frac{1}{2}\left(1-\sqrt{5}\right)$, která jsme obdrželi jako směrnice v předchozím příkladu. Poměr zlatého řezu bývá užíván v malířství, architektuře nebo fotografii.

2.3 Hexagonální kvazigrupy

Definice 2.3.1: Kvazigrupa $(G,\cdot)$ se nazývá *hexagonální*, pokud je splněna identita hexagonality:

$$x(yz \cdot ww) = y(xz \cdot w). \tag{2.5}$$

Pozn. 2.3.1: Každá hexagonální kvazigrupa je idempotentní.

Důkaz: Dosaďme do vztahu (2.5) $x = y$, užitím krácení zleva dostaneme idempotentnost.

Věta 2.3.1: Je-li $\mathbf{F}=(F,0,1,+,\cdot)$ těleso, v němž má rovnice

$$q^2 - q + 1 = 0 \tag{2.6}$$

řešení $q \in F$, a binární operace $*$ na F je daná vztahem

$$a * b = (1-q) \cdot a + q \cdot b = a + q(b-a), \tag{2.4}$$

pak $(F,*)$ je hexagonální kvazigrupa.

Důkaz: Důkaz by se prováděl podobně jako v případě věty 2.2.1.2.

Věta 2.3.2: V kvazigrupě $(G,\cdot)$ jsou následující podmínky ekvivalentní:

(i) $(G,\cdot)$ je hexagonální,

(ii) $(G,\cdot)$ je idempotentní a splňuje podmínku levé hexagonální identity:

$$x(yz \cdot w) = y(xz \cdot w) \text{ (levá hexagonalita),} \tag{2.7}$$

(iii) $(G,\cdot)$ je idempotentní a splňuje podmínku pravé hexagonální identity:

$$(x \cdot yz)w = (x \cdot yw)z \quad \text{(pravá hexagonalita).} \tag{2.8}$$

Důkaz: Můžeme vidět, že (2.7) a (2.8) jsou ekvivalentní, za předpokladu, že platí idempotentnost; důkaz (2.7) a (2.8) je zrcadlový.

Lemma 2.3.1: Nechť $(G,\cdot)$ je idempotentní kvazigrupa, pak v ní pravá hexagonalita implikuje identitu

$$(xy)x = y, \tag{2.9}$$

a levá hexagonalita implikuje duální (zrcadlovou identitu)

$$x(yx) = y. \tag{2.10}$$

Důkaz: Dosadíme-li do vztahu (2.8) $x = y = w$, obdržíme $(x \cdot xz)x = (x \cdot xx)z$, což je ekvivalentní s

$$(x \cdot xz)x = xz, \tag{2.11}$$

za předpokladu, že platí idempotentnost.

Z druhé strany: nechť $a, b \in Q$ jsou libovolné pevné prvky a g je jediné řešení rovnice $ay = b$ v Q, pak $(ab)a = (a \cdot ag)a = ag = b$, což je (2.9). Druhá část by se dokazovala zrcadlově.

Pozn. 2.3.2: Každá hexagonální kvazigrupa je elastická:

$$(xy)x = x(yx) \quad \text{(elasticita).} \tag{2.12}$$

Věta 2.3.3: Pro každou hexagonální kvazigrupu $(G,\cdot)$ existuje komutativní grupa $\mathbf{G} = (G, e, +)$ a automorfismus $\varphi \in Aut\ \mathbf{G}$ tak, že $(G,\cdot)$ je lineární nad $\mathbf{G}$ s netriviálním automorfismem φ, zároveň je splněno:

$$\varphi^2 - \varphi + id_G = \varepsilon, \tag{2.13}$$

kde $\varepsilon : G \to G$ je konstantní zobrazení $\varepsilon(x) = e$ pro každé $x \in G$ a e je jednotkový prvek grupy G.

Důkaz: Dokažme, že $(G,\cdot)$ mediální kvazigrupa. Rovnici $y \cdot a = b$, kde $a,b \in G$, můžeme přepsat do tvaru $y + \varphi(a - y) = b$. Aplikujeme automorfismus φ:

$\varphi(y) + \varphi \circ \varphi(a) - \varphi \circ \varphi(b) = \varphi(b)$, použitím věty 2.2.1.1 dostáváme:

$\varphi(y) + (\varphi(a) - a) + (-\varphi(y) + y) = \varphi(b)$, dále $y - a = \varphi(b) - \varphi(a) = \varphi(b - a)$. Z toho máme $y = a + \varphi(b - a)$.

3 Konstrukce hexagonálních kvazigrup a GS-kvazigrup z komutativních těles

V následujících příkladech budeme sestrojovat kvazigrupy zlatého řezu a hexagonální kvazigrupy z některých komutativních těles. Jako komutativní tělesa nám převážně budou sloužit zbytkové třídy po prvočíslech, tedy tělesa $GF(p)$, kde p je prvočíslo.

Existence GS-kvazigrupy (resp. hexagonální kvazigrupy) nad daným tělesem závisí na tom, zda polynom $x^2 - x - 1 = 0$ (resp. $x^2 - x + 1$) má v příslušném tělese kořeny, viz. věta 2.2.1.1. Kořeny těchto polynomů můžeme počítat tak, jak jsme zvyklí ze střední školy (s výjimkou těles charakteristiky 2), tedy pomocí vzorce s diskriminantem $x_{1,2} = \frac{-b \pm \sqrt{D}}{2a}$, $D = b^2 - 4ac$, kde $a \in R/\{0\}, b, c \in R$, musíme však brát v úvahu, nad jakým tělesem rovnici řešíme. Dále je třeba si určit kvadratické zbytky, tj. čísla, která vzniknou umocněním jednotlivých prvků tělesa, jen z těchto čísel lze určit druhou odmocninu. Pak nad daným tělesem mohou existovat až dva kořeny q_1, q_2, pro které platí $q_2 = 1 - q_1$.

Může však nastat i situace, kdy daný polynom bude nad tělesem nerozložitelný, tj. nebude existovat odmocnina z diskriminantu. V tomto případě nemůžeme konstrukci z věty 2.2.1.1 použít. Tato skutečnost však nevylučuje možnost, že nad daným tělesem nelze nějakou GS-kvazigrupu sestrojit nějak jinak.

Poznamenejme také, že všechny výpočty byly prováděny bez použití výpočetní techniky.

Příklad 3.1: Jako těleso si vezmeme zbytkové třídy mod 2, v těchto nejsou jiné prvky než 0 a 1, tudíž žádnou GS-kvazigrupu podle návodu uvedeného výše sestrojit nejde.

Příklad 3.2: $(Z_3, \oplus, \otimes)$

$\oplus$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\otimes$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

Proto, abychom našli směrnice GS-kvazigrupy budeme řešit rovnici $x^2 - x - 1 = 0$, tu si můžeme přepsat do tvaru $x^2 \oplus 2x \oplus 2 = 0$, pro diskriminant platí

$D = 2^2 - 4 \cdot 2 = 1 - 2 = 1 \oplus 1 = 2$, 2 není kvadratický zbytek, tedy směrnice pro GS-kvazigrupu neexistuje.

Hledejme nyní směrnici pro hexagonální kvazigrupu, řešme rovnici $x^2 - x + 1 = 0$, tu lze přepsat $x^2 \oplus 2x \oplus 1 = 0$, $D = 2^2 - 4 \otimes 1 = 1 - 1 \otimes 1 = 1 \oplus 2 = 0$, nula je kvadratický zbytek, tedy $x = (-2) \otimes (2^{-1}) = 1 \otimes 2 = 2$, hexagonální kvazigrupa existuje, její směrnice je $q = 2$.

Pro prvky naší kvazigrupy platí $a * b = a \oplus q \otimes (b - a)$.

Tedy $0 * 0 = 0 \oplus 2 \otimes (0 - 0) = 0$, $0 * 1 = 0 \oplus 2 \otimes (1 - 0) = 2$, $0 * 2 = 0 \oplus 2 \otimes (2 - 0) = 1$,

$1 * 0 = 1 \oplus 2 \otimes (0 - 1) = 2$, $1 * 1 = 1 \oplus 2 \otimes (1 - 1) = 1$, $1 * 2 = 1 \oplus 2 \otimes (2 - 1) = 0$,

$2 * 0 = 2 \oplus 2 \otimes (0 - 2) = 1$, $2 * 1 = 2 \oplus 2 \otimes (1 - 2) = 0$, $2 * 2 = 2 \oplus 2 \otimes (2 - 2) = 2$.

Obdržíme následující tabulku pro násobení v hexagonální kvazigrupě:

$*$	0	1	2
0	0	2	1
1	2	1	0
2	1	0	2

Příklad 3.3: $(Z_5, \oplus, \otimes)$:

$\oplus$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$\otimes$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Výpočet směrnice pro GS-kvazigrupu: $x^2 - x - 1 = 0$, rovnici přepíšeme do tvaru $x^2 - 4x \oplus 4 = 0$, upravíme $(x - 2)^2$, rovnice má tedy dvojnásobný kořen, který je roven prvku inverznímu ke 2, a to je trojka. Jedinou směrnicí *q* je tedy 3. Sestrojme nyní tabulku pro operaci $*$ v kvazigrupě.

Tedy:

$0 * 0 = 0 \oplus 3 \otimes (0 - 0) = 0$, $0 * 1 = 0 \oplus 3 \otimes (1 - 0) = 3$, $0 * 2 = 0 \oplus 3 \otimes (2 - 0) = 1$,

$0 * 3 = 0 \oplus 3 \otimes (3 - 0) = 4$, $0 * 4 = 0 \oplus 3 \otimes (4 - 0) = 2$,

$1*0=1\oplus 3\otimes(0-1)=3$, $1*1=1\oplus 3\otimes(1-1)=1$, $1*2=1\oplus 3\otimes(2-1)=4$,

$1*3=1\oplus 3\otimes(3-1)=2$, $1*4=1\oplus 3\otimes(4-1)=0$

$2*0=2\oplus 3\otimes(0-2)=1$, $2*1=2\oplus 3\otimes(1-2)=1$, $2*2=2\oplus 3\otimes(2-2)=2$,

$2*3=2\oplus 3\otimes(3-2)=0$, $2*4=2\oplus 3\otimes(4-2)=3$

$3*0=3\oplus 3\otimes(0-3)=4$, $3*1=3\oplus 3\otimes(0-3)=2$, $3*2=3\oplus 3\otimes(2-3)=0$,

$3*3=3+3\otimes(3-3)=3$, $3*4=3+3\otimes(4-3)=1$,

$4*0=4\oplus 3\otimes(0-4)=2$, $4*1=4\oplus 3\otimes(1-4)=0$, $4*2=4\oplus 3\otimes(2-4)=3$,

$4*3=4\oplus 3\otimes(3-4)=1$, $4*4=4\oplus 3\otimes(4-4)=4$.

Obdržíme následující tabulku pro násobení v GS-kvazigrupě:

$*$	0	1	2	3	4
0	0	3	1	4	2
1	3	1	4	2	0
2	1	4	2	0	3
3	4	2	0	3	1
4	2	0	3	1	4

Můžeme si všimnout, že tabulka násobení v kvazigrupě je symetrická, $a*b=b*a$, tedy $(Z_5,*)$ je komutativní GS-kvazigrupa. Tato skutečnost se dá vyjádřit i takto: operace $*$ v Z_5 je autoduální, $*^{op}=*$.

Výpočet směrnice pro hexagonální kvazigrupu: řešíme rovnici x^2-x+1, tu jde přepsat $x^2\oplus 4x\oplus 1=0$, $D=4^2-4=1\oplus 1=2$, dvojka není kvadratickým zbytkem, tudíž rovnice nemá kořen nad tělesem $(Z_5,\oplus,\otimes)$.

Příklad 3.4: $(Z_7, \oplus, \otimes)$

$\oplus$	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	2
3	3	4	5	6	0	2	3
4	4	5	6	0	2	3	4
5	5	6	0	2	3	4	5
6	6	0	2	3	4	5	1

$\otimes$	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

Rovnici pro hledání směrnice pro GS-kvazigrupu lze přepsat takto: $x^2 + 6x + 6 = 0$, kvadratické zbytky v tělese jsou $1^2 = 6^2 = 1$, $2^2 = 5^2 = 4$, $3^2 = 4^2 = 2$, diskriminant je roven $6^2 - 4 \otimes 6 = 1 \oplus 4 = 5$, 5 není kvadratický zbytek, rovnice nemá nad zadaným tělesem řešení.

Pro směrnici hexagonální kvazigrupy řešíme rovnici $x^2 \oplus 6x \oplus 1 = 0$, $D = 6^2 - 4 = 1 \oplus 3 = 4$, čtyřka je kvadratický zbytek, její odmocněním získáme 2 a 5, nám stačí uvažovat jen jedno z těchto čísel, protože 2 a 5 jsou vzhledem ke sčítání vzájemně opačné. Budou existovat dvě směrnice q_1 a q_2, $q_1 = (-6-2) \otimes 2^{-1} = 6 \otimes 4 = 3$, $q_2 = (-6 \oplus 2) \otimes 2^{-1} = 3 \otimes 4 = 5$.

Sestrojme nyní tabulky pro hexagonální kvazigrupy.

Výpočet prvků v hexagonální kvazigrupě pro $q_1 = 3$:

$0 * 0 = 0 \oplus 3 \otimes (0-0) = 0$, $0 * 1 = 0 \oplus 3 \otimes (1-0) = 3$, $0 * 2 = 0 \oplus 3 \otimes (2-0) = 6$,

$0 * 3 = 0 \oplus 3 \otimes (3-0) = 2$, $0 * 4 = 0 \oplus 3 \otimes (4-0) = 5$, $0 * 5 = 0 \oplus 3 \otimes (5-0) = 1$,

$0 * 6 = 0 \oplus 3 \otimes (6-0) = 4$,

$1 * 0 = 1 \oplus 3 \otimes (0-1) = 5$, $1 * 1 = 1 \oplus 3 \otimes (1-1) = 1$, $1 * 2 = 1 \oplus 3 \otimes (2-1) = 4$,

$1 * 3 = 1 \oplus 3 \otimes (3-1) = 0$, $1 * 4 = 1 \oplus 3 \otimes (4-1) = 3$, $1 * 5 = 1 \oplus 3 \otimes (5-1) = 6$,

$1 * 6 = 1 \oplus 3 \otimes (6-1) = 2$,

$2 * 0 = 2 \oplus 3 \otimes (0-2) = 3$, $2 * 1 = 2 \oplus 3 \otimes (1-2) = 6$, $2 * 2 = 2 \oplus 3 \otimes (2-2) = 2$,

$2 * 3 = 2 \oplus 3 \otimes (3-2) = 5$, $2 * 4 = 2 \oplus 3 \otimes (4-2) = 1$, $2 * 5 = 2 \oplus 3 \otimes (5-2) = 4$,

$2 * 6 = 2 \oplus 3 \otimes (6-2) = 0$,

$3*0=3\oplus 3\otimes(0-3)=1,$ $3*1=3\oplus 3\otimes(1-3)=4,$ $3*2=3\oplus 3\otimes(2-3)=0,$

$3*3=3\oplus 3\otimes(3-3)=3,$ $3*4=3\oplus 3\otimes(4-3)=6,$ $3*5=3\oplus 3\otimes(5-3)=2,$

$3*6=3\oplus 3\otimes(6-3)=5,$

$4*0=4\oplus 3\otimes(0-4)=6,$ $4*1=4\oplus 3\otimes(1-4)=2,$ $4*2=4\oplus 3\otimes(2-4)=5,$

$4*3=4\oplus 3\otimes(3-4)=1,$ $4*4=4\oplus 3\otimes(4-4)=4,$ $4*5=4\oplus 3\otimes(5-4)=0,$

$4*6=4\oplus 3\otimes(6-4)=3,$

$5*0=5\oplus 3\otimes(0-5)=4,$ $5*1=5\oplus 3\otimes(1-5)=0,$ $5*2=5\oplus 3\otimes(2-5)=3,$

$5*3=5\oplus 3\otimes(3-5)=6,$ $5*4=5\oplus 3\otimes(4-5)=2,$ $5*5=5\oplus 3\otimes(5-5)=5,$

$5*6=5\oplus 3\otimes(6-5)=1,$

$6*0=6\oplus 3\otimes(0-6)=2,$ $6*1=6\oplus 3\otimes(1-6)=5,$ $6*2=6\oplus 3\otimes(2-6)=1,$

$6*3=6\oplus 3\otimes(3-6)=4,$ $6*4=6\oplus 3\otimes(4-6)=0,$ $6*5=6\oplus 3\otimes(5-6)=3,$

$6*6=6\oplus 3\otimes(6-6)=6.$

Tabulka hexagonální kvazigrupy pro $q_1=3$:

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

Výpočet prvků v hexagonální kvazigrupě pro $q_2=5$:

$0*0=0\oplus 5\otimes(0-0)=0,$ $0*1=0\oplus 5\otimes(1-0)=5,$ $0*2=0\oplus 5\otimes(2-0)=3,$

$0*3=0\oplus 5\otimes(3-0)=1,$ $0*4=0\oplus 5\otimes(4-0)=6,$ $0*5=0\oplus 5\otimes(5-0)=4,$

$0*6=0\oplus 5\otimes(6-0)=2,$

$1*0=1\oplus 5\otimes(0-1)=3,$ $1*1=1\oplus 5\otimes(1-1)=1,$ $1*2=1\oplus 5\otimes(2-1)=6,$

$1*3=1\oplus 5\otimes(3-1)=4,$ $1*4=1\oplus 4\otimes(4-1)=2,$ $1*5=1\oplus 5\otimes(5-1)=0,$

$1*6=1\oplus 5\otimes(6-1)=5,$

$2*0=2\oplus 5\otimes(0-2)=6,$ $2*1=2\oplus 5\otimes(1-2)=4,$ $2*2=2\oplus 5\otimes(2-2)=2,$

$2*3=2\oplus 5\otimes(3-2)=0,$ $2*4=2\oplus 5\otimes(4-2)=5,$ $2*5=2\oplus 5\otimes(5-2)=3,$

$2*6=2\oplus 5\otimes(6-2)=1,$

$3*0=3\oplus 5\otimes(0-3)=2,$ $3*1=3\oplus 5\otimes(1-3)=0,$ $3*2=3\oplus 5\otimes(2-3)=5,$

$3*3=3\oplus 5\otimes(3-3)=3,$ $3*4=3\oplus 5\otimes(4-3)=1,$ $3*5=3\oplus 5\otimes(5-3)=6,$

$3*6=3\oplus 5\otimes(6-3)=4,$

$4*0=4\oplus 5\otimes(0-4)=5,$ $4*1=4\oplus 5\otimes(1-4)=3,$ $4*2=4\oplus 5\otimes(2-4)=1,$

$4*3=4\oplus 5\otimes(3-4)=6,$ $4*4=4\oplus 5\otimes(4-4)=4,$ $4*5=4\oplus 5\otimes(5-4)=2,$

$4*6=4\oplus 5\otimes(6-4)=0,$

$5*0=5\oplus 5\otimes(0-5)=1,$ $5*1=5\oplus 5\otimes(1-5)=6,$ $5*2=5\oplus 5\otimes(2-5)=4,$

$5*3=5\oplus 5\otimes(3-5)=2,$ $5*4=5\oplus 5\otimes(4-5)=0,$ $5*5=5\oplus 5\otimes(5-5)=5,$

$5*6=5\oplus 5\otimes(6-5)=3,$

$6*0=6\oplus 5\otimes(0-6)=4,$ $6*1=6\oplus 5\otimes(1-6)=2,$ $6*2=6\oplus 5\otimes(2-6)=0,$

$6*3=6\oplus 5\otimes(3-6)=5,$ $6*4=6\oplus 5\otimes(4-6)=3,$ $6*5=6\oplus 5\otimes(5-6)=1,$

$6*6=6\oplus 5\otimes(6-6)=6.$

Přeznačme operaci v hexagonální kvazigrupě z $*$ na $\circ$ (z technických důvodů).

Tabulka hexagonální kvazigrupy pro $q_2=5$:

$\circ$	0	1	2	3	4	5	6
0	0	5	3	1	6	4	2
1	3	1	6	4	2	0	5
2	6	4	2	0	5	3	1
3	2	0	5	3	1	6	4
4	5	3	1	6	4	2	0
5	1	6	4	2	0	5	3
6	4	2	0	5	3	1	6

Příklad 3.5: $(Z_{11},\oplus,\otimes)$

$\oplus$	0	1	2	3	4	5	6	7	8	9	10
0	0	1	2	3	4	5	6	7	8	9	10
1	1	2	3	4	5	6	7	8	9	10	0
2	2	3	4	5	6	7	8	9	10	0	1
3	3	4	5	6	7	8	9	10	0	1	2
4	4	5	6	7	8	9	10	0	1	2	3
5	5	6	7	8	9	10	0	1	2	3	4
6	6	7	8	9	10	0	1	2	3	4	5
7	7	8	9	10	0	1	2	3	4	5	6
8	8	9	10	0	1	2	3	4	5	6	7
9	9	10	0	1	2	3	4	5	6	7	8
10	10	0	1	2	3	4	5	6	7	8	9

$\otimes$	0	1	2	3	4	5	6	7	8	9	10
0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9	10
2	0	2	4	6	8	10	1	3	5	7	9
3	0	3	6	9	1	4	7	10	2	5	8
4	0	4	8	1	5	9	2	6	10	3	7
5	0	5	10	4	9	3	8	2	7	1	6
6	0	6	1	7	2	8	3	9	4	10	5
7	0	7	3	10	6	2	9	5	1	8	4
8	0	8	5	2	10	7	4	1	9	6	3
9	0	9	7	5	3	1	10	8	6	4	2
10	0	10	9	8	7	6	5	4	3	2	1

Kvadratické zbytky: $1^2 = 10^2 = 1$, $2^2 = 9^2 = 4$, $3^2 = 8^2 = 9$, $4^2 = 7^2 = 5$, $5^2 = 6^2 = 3$.

Výpočet rovnice pro GS-kvazigrupu: $x^2 \oplus 10x \oplus 10 = 0$, $D = 10^2 - 4 \otimes 10 = 1 \oplus 4 = 5$, odmocnina z diskriminantu je rovna 4 a 7, stejně jako v předchozím příkladu stačí počítat jen s jedním z těchto prvků, tedy $q_1 = (-10-4) \otimes 2^{-1} = 8 \otimes 6 = 4$, $q_2 = (-10 \oplus 4) \otimes 2^{-1} = 5 \otimes 6 = 8$.

Směrnicemi jsou prvky 4 a 8. Nyní sestrojíme tabulky pro kvazigrupy.

Výpočet prvků v GS-kvazigrupě pro $q_1 = 4$:

$0 * 0 = 0 \oplus 4 \otimes (0-0) = 0$, $0 * 1 = 0 \oplus 4 \otimes (1-0) = 4$, $0 * 2 = 0 \oplus 4 \otimes (2-0) = 8$,

$0 * 3 = 0 \oplus 4 \otimes (3-0) = 1$, $0 * 4 = 0 \oplus 4 \otimes (4-0) = 5$, $0 * 5 = 0 \oplus 4 \otimes (5-0) = 9$,

$0 * 6 = 0 \oplus 4 \otimes (6-0) = 2$, $0 * 7 = 0 \oplus 4 \otimes (7-0) = 6$, $0 * 8 = 0 \oplus 4 \otimes (8-0) = 10$,

$0 * 9 = 0 \oplus 4 \otimes (9-0) = 3$, $0 * 10 = 0 \oplus 4 \otimes (10-0) = 7$,

$1 * 0 = 1 \oplus 4 \otimes (0-1) = 8$, $1 * 1 = 1 \oplus 4 \otimes (1-1) = 1$, $1 * 2 = 1 \oplus 4 \otimes (2-1) = 5$,

$1 * 3 = 1 \oplus 4 \otimes (3-1) = 9$, $1 * 4 = 1 \oplus 4 \otimes (4-1) = 2$, $1 * 5 = 1 \oplus 4 \otimes (5-1) = 6$,

$1 * 6 = 1 \oplus 4 \otimes (6-1) = 10$, $1 * 7 = 1 \oplus 4 \otimes (7-1) = 3$, $1 * 8 = 1 \oplus 4 \otimes (8-1) = 7$,

$1 * 9 = 1 \oplus 4 \otimes (9-1) = 0$, $1 * 10 = 1 \oplus 4 \otimes (10-1) = 4$,

$2 * 0 = 2 \oplus 4 \otimes (0-2) = 5$, $2 * 1 = 2 \oplus 4 \otimes (1-2) = 9$, $2 * 2 = 2 \oplus 4 \otimes (2-2) = 2$,

$2 * 3 = 2 \oplus 4 \otimes (3-2) = 6$, $2 * 4 = 2 \oplus 4 \otimes (4-2) = 10$, $2 * 5 = 2 \oplus 4 \otimes (5-2) = 3$,

$2*6=2\oplus 4\otimes(6-2)=7,$ $2*7=2\oplus 4\otimes(7-2)=0,$ $2*8=2\oplus 4\otimes(8-2)=4,$

$2*9=2\oplus 4\otimes(9-2)=8,$ $2*10=2\oplus 4\otimes(10-2)=1,$

$3*0=3\oplus 4\otimes(0-3)=2,$ $3*1=3\oplus 4\otimes(1-3)=6,$ $3*2=3\oplus 4\otimes(2-3)=10,$

$3*3=3\oplus 4\otimes(3-3)=3,$ $3*4=3\oplus 4\otimes(4-3)=7,$ $3*5=3\oplus 4\otimes(5-3)=0,$

$3*6=3\oplus 4\otimes(6-3)=4,$ $3*7=3\oplus 4\otimes(7-3)=8,$ $3*8=3\oplus 4\otimes(8-3)=1,$

$3*9=3\oplus 4\otimes(9-3)=5,$ $3*10=3\oplus 4\otimes(10-3)=9,$

$4*0=4\oplus 4\otimes(0-4)=10,$ $4*1=4\oplus 4\otimes(1-4)=3,$ $4*2=4\oplus 4\otimes(2-4)=7,$

$4*3=4\oplus 4\otimes(3-4)=0,$ $4*4=4\oplus 4\otimes(4-4)=4,$ $4*5=4\oplus 4\otimes(5-4)=8,$

$4*6=4\oplus 4\otimes(6-4)=1,$ $4*7=4\oplus 4\otimes(7-4)=5,$ $4*8=4\oplus 4\otimes(8-4)=9,$

$4*9=4\oplus 4\otimes(9-4)=2,$ $4*10=4\oplus 4\otimes(10-4)=6,$

$5*0=5\oplus 4\otimes(0-5)=7,$ $5*1=5\oplus 4\otimes(1-5)=0,$ $5*2=5\oplus 4\otimes(2-5)=4,$

$5*3=5\oplus 4\otimes(3-5)=8,$ $5*4=5\oplus 4\otimes(4-5)=1,$ $5*5=5\oplus 4\otimes(5-5)=5,$

$5*6=5\oplus 4\otimes(6-5)=9,$ $5*7=5\oplus 4\otimes(7-5)=2,$ $5*8=5\oplus 4\otimes(8-5)=6,$

$5*9=5\oplus 4\otimes(9-5)=10,$ $5*10=5\oplus 4\otimes(10-5)=3,$

$6*0=6\oplus 4\otimes(0-6)=4,$ $6*1=6\oplus 4\otimes(1-6)=8,$ $6*2=6\oplus 4\otimes(2-6)=1,$

$6*3=6\oplus 4\otimes(3-6)=5,$ $6*4=6\oplus 4\otimes(4-6)=9,$ $6*5=6\oplus 4\otimes(5-6)=2,$

$6*6=6\oplus 4\otimes(6-6)=6,$ $6*7=6\oplus 4\otimes(7-6)=10,$ $6*8=6\oplus 4\otimes(8-6)=3,$

$6*9=6\oplus 4\otimes(9-6)=7,$ $6*10=6\oplus 4\otimes(10-6)=0,$

$7*0=7\oplus 4\otimes(0-7)=1,$ $7*1=7\oplus 4\otimes(1-7)=5,$ $7*2=7\oplus 4\otimes(2-7)=9,$

$7*3=7\oplus 4\otimes(3-7)=2,$ $7*4=7\oplus 4\otimes(4-7)=6,$ $7*5=7\oplus 4\otimes(5-7)=10,$

$7*6=7\oplus 4\otimes(6-7)=3,$ $7*7=7\oplus 4\otimes(7-7)=7,$ $7*8=7\oplus 4\otimes(8-7)=0,$

$7*9=7\oplus 4\otimes(9-7)=4,$ $7*10=7\oplus 4\otimes(10-7)=8,$

$8*0=8\oplus 4\otimes(0-8)=9,$ $8*1=8\oplus 4\otimes(1-8)=2,$ $8*2=8\oplus 4\otimes(2-8)=6,$

$8*3=8\oplus 4\otimes(3-8)=10,$ $8*4=8\oplus 4\otimes(4-8)=3,$ $8*5=8\oplus 4\otimes(5-8)=7,$

$8*6=8\oplus 4\otimes(6-8)=0,$ $8*7=8\oplus 4\otimes(7-8)=4,$ $8*8=8\oplus 4\otimes(8-8)=8,$

$8*9=8\oplus 4\otimes(9-8)=1,$ $8*10=8\oplus 4\otimes(10-8)=5,$

$9*0=9\oplus 4\otimes(0-9)=6,$ $9*1=9\oplus 4\otimes(1-9)=10,$ $9*2=9\oplus 4\otimes(2-9)=3,$

$9*3=9\oplus 4\otimes(3-9)=7,$ $9*4=9\oplus 4\otimes(4-9)=0,$ $9*5=9\oplus 4\otimes(5-9)=4,$

$9*6=9\oplus 4\otimes(6-9)=8,$ $9*7=9\oplus 4\otimes(7-9)=1,$ $9*8=9\oplus 4\otimes(8-9)=5,$

$9*9=9\oplus 4\otimes(9-9)=9,$ $9*10=9\oplus 4\otimes(10-9)=2,$

$10*0=10\oplus 4\otimes(0-10)=3$, $10*1=10\oplus 4\otimes(1-10)=7$, $10*2=10\oplus 4\otimes(2-10)=0$,

$10*3=10\oplus 4\otimes(3-10)=4$, $10*4=10\oplus 4\otimes(4-10)=8$, $10*5=10\oplus 4\otimes(5-10)=1$,

$10*6=10\oplus 4\otimes(6-10)=5$, $10*7=10\oplus 4\otimes(7-10)=9$, $10*8=10\oplus 4\otimes(8-10)=2$,

$10*9=10\oplus 4\otimes(9-10)=6$, $10*10=10\oplus 4\otimes(10-10)=10$.

Tabulka GS-kvazigrupy pro $q_1=4$:

$*$	0	1	2	3	4	5	6	7	8	9	10
0	0	4	8	1	5	9	2	6	10	3	7
1	8	1	5	9	2	6	10	3	7	0	4
2	5	9	2	6	10	3	7	0	4	8	1
3	2	6	10	3	7	0	4	8	1	5	9
4	10	3	7	0	4	8	1	5	9	2	6
5	7	0	4	8	1	5	9	2	6	10	3
6	4	8	1	5	9	2	6	10	3	7	0
7	1	5	9	2	6	10	3	7	0	4	8
8	9	2	6	10	3	7	0	4	8	1	5
9	6	10	3	7	0	4	8	1	5	9	2
10	3	7	0	4	8	1	5	9	2	6	10

Výpočet prvků v GS-kvazigrupě pro $q_2=8$:

$0*0=0\oplus 8\otimes(0-0)=0$, $0*1=0\oplus 8\otimes(1-0)=8$, $0*2=0\oplus 8\otimes(2-0)=5$,

$0*3=0\oplus 8\otimes(3-0)=2$, $0*4=0\oplus 8\otimes(4-0)=10$, $0*5=0\oplus 8\otimes(5-0)=7$,

$0*6=0\oplus 8\otimes(6-0)=4$, $0*7=0\oplus 8\otimes(7-0)=1$, $0*8=0\oplus 8\otimes(8-0)=9$,

$0*9=0\oplus 8\otimes(9-0)=6$, $0*10=0\oplus 8\otimes(10-0)=3$,

$1*0=1\oplus 8\otimes(0-1)=4$, $1*1=1\oplus 8\otimes(1-1)=1$, $1*2=1\oplus 8\otimes(2-1)=9$,

$1*3=1\oplus 8\otimes(3-1)=6$, $1*4=1\oplus 8\otimes(4-1)=3$, $1*5=1\oplus 8\otimes(5-1)=0$,

$1*6=1\oplus 8\otimes(6-1)=8$, $1*7=1\oplus 8\otimes(7-1)=5$, $1*8=1\oplus 8\otimes(8-1)=2$,

$1*9=1\oplus 8\otimes(9-1)=10$, $1*10=1\oplus 8\otimes(10-1)=7$,

$2*0=2\oplus 8\otimes(0-2)=8$, $2*1=2\oplus 8\otimes(1-2)=5$, $2*2=2\oplus 8\otimes(2-2)=2$,

$2*3=2\oplus 8\otimes(3-2)=10$, $2*4=2\oplus 8\otimes(4-2)=7$, $2*5=2\oplus 8\otimes(5-2)=4$,

$2*6=2\oplus 8\otimes(6-2)=1,$ $2*7=2\oplus 8\otimes(7-2)=9,$ $2*8=2\oplus 8\otimes(8-2)=6,$

$2*9=2\oplus 8\otimes(9-2)=3,$ $2*10=2\oplus 8\otimes(10-2)=0,$

$3*0=3\oplus 8\otimes(0-3)=1,$ $3*1=3\oplus 8\otimes(1-3)=9,$ $3*2=3\oplus 9\otimes(2-3)=6,$

$3*3=3\oplus 8\otimes(3-3)=3,$ $3*4=3\oplus 8\otimes(4-3)=0,$ $3*5=3\oplus 8\otimes(5-3)=8,$

$3*6=3\oplus 8\otimes(6-3)=5,$ $3*7=3\oplus 8\otimes(7-3)=2,$ $3*8=3\oplus 8\otimes(8-3)=10,$

$3*9=3\oplus 8\otimes(9-3)=7,$ $3*10=3\oplus 8\otimes(10-3)=4,$

$4*0=4\oplus 8\otimes(0-4)=5,$ $4*1=4\oplus 8\otimes(1-4)=2,$ $4*2=4\oplus 8\otimes(2-4)=10,$

$4*3=4\oplus 8\otimes(3-4)=7,$ $4*4=4\oplus 8\otimes(4-4)=4,$ $4*5=8\oplus 4\otimes(5-4)=1,$

$4*6=4\oplus 8\otimes(6-4)=9,$ $4*7=4\oplus 8\otimes(7-4)=6,$ $4*8=4\oplus 8\otimes(8-4)=3,$

$4*9=4\oplus 8\otimes(9-4)=0,$ $4*10=4\oplus 8\otimes(10-4)=8,$

$5*0=5\oplus 8\otimes(0-5)=9,$ $5*1=5\oplus 8\otimes(1-5)=6,$ $5*2=5\oplus 8\otimes(2-5)=3,$

$5*3=5\oplus 8\otimes(3-5)=0,$ $5*4=5\oplus 8\otimes(4-5)=8,$ $5*5=5\oplus 8\otimes(5-5)=5,$

$5*6=5\oplus 8\otimes(6-5)=2,$ $5*7=5\oplus 8\otimes(7-5)=10,$ $5*8=5\oplus 8\otimes(8-5)=7,$

$5*9=5\oplus 8\otimes(9-5)=4,$ $5*10=5\oplus 8\otimes(10-5)=1,$

$6*0=6\oplus 8\otimes(0-6)=2,$ $6*1=6\oplus 8\otimes(1-6)=10,$ $6*2=6\oplus 8\otimes(2-6)=7,$

$6*3=6\oplus 8\otimes(3-6)=4,$ $6*4=6\oplus 8\otimes(4-6)=1,$ $6*5=6\oplus 8\otimes(5-6)=9,$

$6*6=6\oplus 8\otimes(6-6)=6,$ $6*7=6\oplus 8\otimes(7-6)=3,$ $6*8=6\oplus 8\otimes(8-6)=0,$

$6*9=6\oplus 8\otimes(9-6)=8,$ $6*10=6\oplus 8\otimes(10-6)=5,$

$7*0=7\oplus 8\otimes(0-7)=6,$ $7*1=7\oplus 8\otimes(1-7)=3,$ $7*2=7\oplus 8\otimes(2-7)=0,$

$7*3=7\oplus 8\otimes(3-7)=8,$ $7*4=7\oplus 8\otimes(4-7)=5,$ $7*5=7\oplus 8\otimes(5-7)=2,$

$7*6=7\oplus 8\otimes(6-7)=10,$ $7*7=7\oplus 8\otimes(7-7)=7,$ $7*8=7\oplus 8\otimes(8-7)=4,$

$7*9=7\oplus 8\otimes(9-7)=1,$ $7*10=7\oplus 8\otimes(10-7)=9,$

$8*0=8\oplus 8\otimes(0-8)=10,$ $8*1=8\oplus 8\otimes(1-8)=7,$ $8*2=8\oplus 8\otimes(2-8)=4,$

$8*3=8\oplus 8\otimes(3-8)=1,$ $8*4=8\oplus 8\otimes(4-8)=9,$ $8*5=8\oplus 8\otimes(5-8)=6,$

$8*6=8\oplus 8\otimes(6-8)=3,$ $8*7=8\oplus 8\otimes(7-8)=0,$ $8*8=8\oplus 8\otimes(8-8)=8,$

$8*9=8\oplus 8\otimes(9-8)=5,$ $8*10=8\oplus 8\otimes(10-8)=2,$

$9*0=9\oplus 8\otimes(0-9)=3,$ $9*1=9\oplus 8\otimes(1-9)=0,$ $9*2=9\oplus 8\otimes(2-9)=8,$

$9*3=9\oplus 8\otimes(3-9)=5,$ $9*4=9\oplus 8\otimes(4-9)=2,$ $9*5=9\oplus 8\otimes(5-9)=10,$

$9*6=9\oplus 8\otimes(6-9)=7,$ $9*7=9\oplus 8\otimes(7-9)=4,$ $9*8=9\oplus 8\otimes(8-9)=1,$

$9*9=9\oplus 8\otimes(9-9)=9,$ $9*10=9\oplus 8\otimes(10-9)=6,$

$10 * 0 = 10 \oplus 8 \otimes (0-10) = 7$, $10 * 1 = 10 \oplus 8 \otimes (1-10) = 4$, $10 * 2 = 10 \oplus 8 \otimes (2-10) = 1$,
$10 * 3 = 10 \oplus 8 \otimes (3-10) = 9$, $10 * 4 = 10 \oplus 8 \otimes (4-10) = 6$, $10 * 5 = 10 \oplus 8 \otimes (5-10) = 3$,
$10 * 6 = 10 \oplus 8 \otimes (6-10) = 0$, $10 * 7 = 10 \oplus 8 \otimes (7-10) = 8$, $10 * 8 = 10 \oplus 4 \otimes (8-10) = 5$,
$10 * 9 = 10 \oplus 8 \otimes (9-10) = 2$, $10 * 10 = 10 \oplus 8 \otimes (10-10) = 10$.

Přeznačme operaci v GS-kvazigrupě z $*$ na $\circ$ (z technických důvodů).
Tabulka GS- kvazigrupy pro $q_2 = 8$:

$\circ$	0	1	2	3	4	5	6	7	8	9	10
0	0	8	5	2	10	7	4	1	9	6	3
1	4	1	9	6	3	0	8	5	2	10	7
2	8	5	2	10	7	4	1	9	6	3	0
3	1	9	6	3	0	8	5	2	10	7	4
4	5	2	10	7	4	1	9	6	3	0	8
5	9	6	3	0	8	5	2	10	7	4	1
6	2	10	7	4	1	9	6	3	0	8	5
7	6	3	0	8	5	2	10	7	4	1	9
8	10	7	4	1	9	6	3	0	8	5	2
9	3	0	8	5	2	10	7	4	1	9	6
10	7	4	1	9	6	3	0	8	5	2	10

Srovnáme-li tabulky GS-kvazigrup $(Z_{11}, *)$ (pro $q_1 = 4$) a $(Z_{11}, \circ)$ (pro $q_2 = 8$) vidíme, že platí lemma 2.2.1.2.

Výpočet směrnic pro hexagonální kvazigrupu: $x^2 \oplus 10x \oplus 1 = 9$, $D = 10^2 - 4 \otimes 1 = 1 \oplus 7 = 8$, 8 není kvadratický zbytek, hexagonální kvazigrupu tedy sestrojit nelze.

Příklad 3.6:

Pokud bychom chtěli sestrojovat tabulky i pro další prvočísla, budeme postupovat stejně jako v předchozích příkladech. Nyní bude uveden jen výpočet směrnic a tabulky GS-kvazigrup a hexagonálních kvazigrup.

$(Z_{13}, \oplus, \otimes)$

Kvadratické zbytky: $1^2 = 12^2 = 1$, $2^2 = 11^2 = 4$, $3^2 = 10^2 = 9$, $4^2 = 9^2 = 3$, $5^2 = 8^2 = 12$, $6^2 = 7^2 = 10$.

Výpočet směrnic pro GS-kvazigrupu: $x^2 \oplus 12x \oplus 12 = 0$, $D = 12^2 - 4 \otimes 12 = 1 \oplus 4 = 5$, 5 není kvadratický zbytek, GS-kvazigrupu nemůžeme sestrojit.

Výpočet směrnic v hexagonální kvazigrupě: $x^2 \oplus 12x \oplus 1 = 0$, pro diskriminant platí: $D = 12^2 - 4 \otimes 1 = 1 \oplus 9 = 10$, 10 je kvadratickým zbytkem, tedy $q_1 = (-12 - 4) \otimes 2^{-1} = 10 \otimes 7 = 5$, $q_2 = (-12 + 4) \otimes 2^{-1} = 5 \otimes 7 = 9$.

Tabulka hexagonální kvazigrupy pro $q_1 = 5$:

*	0	1	2	3	4	5	6	7	8	9	10	11	12
0	0	5	10	2	7	12	4	9	1	6	11	3	8
1	9	1	6	11	3	8	0	5	10	2	7	12	4
2	5	10	2	7	12	4	9	1	6	11	3	8	0
3	1	6	11	3	8	0	5	10	2	7	12	4	9
4	10	2	7	12	4	9	1	6	11	3	8	0	5
5	6	11	3	8	0	5	10	2	7	12	4	9	1
6	2	7	12	4	9	1	6	11	3	8	0	5	10
7	11	3	8	0	5	10	2	7	12	4	9	1	6
8	7	12	4	9	1	6	11	3	8	0	5	10	2
9	3	8	0	5	10	2	7	12	4	9	1	6	11
10	12	4	9	1	6	11	3	8	0	5	10	2	7
11	8	0	5	10	2	7	12	4	9	1	6	11	3
12	4	9	1	6	11	3	8	0	5	10	2	7	12

Tabulka hexagonální kvazigrupy pro $q_2 = 9$:

∘	0	1	2	3	4	5	6	7	8	9	10	11	12
0	0	9	5	1	10	6	2	11	7	3	12	8	4
1	5	1	10	6	2	11	7	3	12	8	4	0	9
2	10	6	2	11	7	3	12	8	4	0	9	5	2
3	2	11	7	3	12	8	4	0	9	5	2	10	6
4	7	3	12	8	4	0	9	5	2	10	6	2	11
5	12	8	4	0	9	5	2	10	6	2	11	7	3
6	4	0	9	5	1	10	6	2	11	7	3	12	8
7	9	5	1	10	6	2	11	7	3	12	8	4	0
8	1	10	6	2	11	7	3	12	8	4	0	9	5
9	6	2	11	7	3	12	8	4	0	9	5	1	10
10	11	7	3	12	8	4	0	9	5	1	10	6	2
11	3	12	8	4	0	9	5	1	10	6	2	11	7
12	8	4	0	9	5	1	10	6	2	11	7	3	12

$(Z_{17}, \oplus, \otimes)$

Kvadratické zbytky: $1^2 = 16^2 = 1$, $2^2 = 15^2 = 4$, $3^2 = 14^2 = 9$, $4^2 = 13^2 = 16$, $5^2 = 12^2 = 8$, $6^2 = 11^2 = 2$, $7^2 = 10^2 = 15$, $8^2 = 9^2 = 13$.

Výpočet směrnic pro GS-kvazigrupu: $x^2 \oplus 16x \oplus 16 = 0$, $D = 16^2 - 4 \cdot 16 = 1 \oplus 4 = 5$, 5 není kvadratický zbytek, GS-kvazigrupu nemůžeme sestrojit.

Výpočet směrnic pro hexagonální kvazigrupu: $x^2 \oplus 16x \oplus 1 = 0$

$D = 16^2 - 4 \otimes 1 = 1 \oplus 13 = 14$, 14 není kvadratický zbytek, daná rovnice nemá nad tímto tělesem žádné řešení a hexagonální kvazigrupu nelze sestrojit.

$(Z_{19}, \oplus, \otimes)$

Kvadratické zbytky: $1^2 = 18^2 = 1$, $2^2 = 17^2 = 4$, $3^2 = 16^2 = 9$, $4^2 = 15^2 = 16$, $5^2 = 14^2 = 6$, $6^2 = 13^2 = 17$, $7^2 = 12^2 = 11$, $8^2 = 11^2 = 7$, $9^2 = 10^2 = 5$.

Výpočet směrnic pro GS-kvazigrupu: $x^2 \oplus 18x \oplus 18 = 0$, $D = 18^2 - 4 \otimes 18 = 1 \oplus 4 = 5$, 5 je kvadratickým zbytkem, spočtěme tedy směrnice $q_1 = (-18 \oplus 9) \otimes 2^{-1} = 10 \otimes 10 = 5$, $q_2 = (-18 - 9) \otimes 2^{-1} = 11 \otimes 10 = 15$.

Vidíme, že směrnicemi jsou prvky 5 a 15.

Tabulka GS-kvazigrupy pro $q_1 = 5$:

$*$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
0	0	5	10	15	1	6	11	16	2	7	12	17	3	8	13	18	4	9	14
1	15	1	6	11	16	2	7	12	17	3	8	13	18	4	9	14	0	5	10
2	11	16	2	7	12	17	3	8	13	18	4	9	14	0	5	10	15	1	6
3	7	12	17	3	8	13	18	4	9	14	0	5	10	15	1	6	11	16	2
4	3	8	13	18	4	9	14	0	5	10	15	1	6	11	16	2	7	12	17
5	18	4	9	14	0	5	10	15	1	6	11	16	2	7	12	17	3	8	13
6	14	0	5	10	15	1	6	11	16	2	7	12	17	3	8	13	18	4	9
7	10	15	1	6	11	16	2	7	12	17	3	8	13	18	4	9	14	0	5
8	6	11	16	2	7	12	17	3	8	13	18	4	9	14	0	5	10	15	1
9	2	7	12	17	3	8	13	18	4	9	14	0	5	10	15	1	6	11	16
10	17	3	8	13	18	4	9	14	0	5	10	15	1	6	11	16	2	7	12
11	13	18	4	9	14	0	5	10	15	1	6	11	16	2	7	12	17	3	8
12	9	14	0	5	10	15	1	6	11	16	2	7	12	17	3	8	13	18	4
13	5	10	15	1	6	11	16	2	7	12	17	3	8	13	18	4	9	14	0
14	1	6	11	16	2	7	12	17	3	8	13	18	4	9	14	0	5	10	15
15	16	2	7	12	17	3	8	13	18	4	9	14	0	5	10	15	1	6	11
16	12	17	3	8	13	18	4	9	14	0	5	10	15	1	6	11	16	2	7
17	8	13	18	4	9	14	0	5	10	15	1	6	11	16	2	7	12	17	3
18	4	9	14	0	5	10	15	1	6	11	16	2	7	12	17	3	8	13	18

Tabulka GS-kvazigrupy pro $q_2 = 15$:

∘	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
0	0	15	11	7	3	18	14	10	6	2	17	13	9	5	1	16	12	8	4
1	5	1	16	12	8	4	0	15	11	7	3	18	14	10	6	2	17	13	9
2	10	6	2	17	13	9	5	1	16	12	8	4	0	15	11	7	3	18	14
3	15	11	7	3	18	14	10	6	2	17	13	9	5	1	16	12	8	4	0
4	1	16	12	8	4	0	15	11	7	3	18	14	10	6	2	17	13	9	5
5	6	2	17	13	9	5	1	16	12	8	4	0	15	11	7	3	18	14	10
6	11	7	3	18	14	10	6	2	17	13	9	5	1	16	12	8	4	0	15
7	16	12	8	4	0	15	11	7	3	18	14	10	6	2	17	13	9	5	1
8	2	17	13	9	5	1	16	12	8	4	0	15	11	7	3	18	14	10	6
9	7	3	18	14	10	6	2	17	13	9	5	1	16	12	8	4	0	15	11
10	12	8	4	0	15	11	7	3	18	14	10	6	2	17	13	9	5	1	16
11	17	13	9	5	1	16	12	8	4	0	15	11	7	3	18	14	10	6	2
12	3	18	14	10	6	2	17	13	9	5	1	16	12	8	4	0	15	11	7
13	8	4	0	15	11	7	3	18	14	10	6	2	17	13	9	5	1	16	12
14	13	9	5	1	16	12	8	4	0	15	11	7	3	18	14	10	6	2	17
15	18	14	10	6	2	17	13	9	5	1	16	12	8	4	0	15	11	7	3
16	4	0	15	11	7	3	18	14	10	6	2	17	13	9	5	1	16	12	8
17	9	5	1	16	12	8	4	0	15	11	7	3	18	14	10	6	2	17	13
18	14	10	6	2	17	13	9	5	1	16	12	8	4	0	15	11	7	3	18

Výpočet směrnic pro hexagonální kvazigrupu: $x^2 \oplus 18x \oplus 1 = 0$, $D = 18^2 - 4 \otimes 1 = 1 \oplus 15 = 16$, 16 je kvadratickým zbytkem, spočtěme tedy směrnice $q_1 = (-18 - 4) \otimes 2^{-1} = 16 \otimes 10 = 8$, $q_2 = (-18 \oplus 4) \otimes 2^{-1} = 5 \otimes 10 = 12$.

Tabulka hexagonální kvazigrupy pro $q_1 = 8$:

$*$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
0	0	8	16	5	13	2	10	18	7	15	4	12	1	9	17	6	14	3	11
1	12	1	9	17	6	14	3	11	0	8	16	5	13	2	10	18	7	15	4
2	5	13	2	10	18	7	15	4	12	1	9	17	6	14	3	11	0	8	16
3	17	6	14	3	11	0	8	16	5	13	2	10	18	7	15	4	12	1	9
4	10	18	7	15	4	12	1	9	17	6	14	3	11	0	8	16	5	13	2
5	3	11	0	8	16	5	13	2	10	18	7	15	4	12	1	9	17	6	14
6	15	4	12	1	9	17	6	14	3	11	0	8	16	5	13	2	10	18	7
7	8	16	5	13	2	10	18	7	15	4	12	1	9	17	6	14	3	11	0
8	1	9	17	6	14	3	11	0	8	16	5	13	2	10	18	7	15	4	12
9	13	2	10	18	7	15	4	12	1	9	17	6	14	3	11	0	8	16	5
10	6	14	3	11	0	8	16	5	13	2	10	18	7	15	4	12	1	9	17
11	18	7	15	4	12	1	9	17	6	14	3	11	0	8	16	5	13	2	10
12	11	0	8	16	5	13	2	10	18	7	15	4	12	1	9	17	6	14	3
13	4	12	1	9	17	6	14	3	11	0	8	16	5	13	2	10	18	7	15
14	16	5	13	2	10	18	7	15	4	12	1	9	17	6	14	3	11	0	8
15	9	17	6	14	3	11	0	8	16	5	13	2	10	18	7	15	4	12	1
16	2	10	18	7	15	4	12	1	9	17	6	14	3	11	0	8	16	5	13
17	14	3	11	0	8	16	5	13	2	10	18	7	15	4	12	1	9	17	6
18	7	15	4	12	1	9	17	6	14	3	11	0	8	16	5	13	2	10	18

Tabulka hexagonální kvazigrupy pro $q_2 = 12$:

∘	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
0	0	12	5	17	10	3	15	8	1	13	6	18	11	4	16	9	2	14	7
1	8	1	13	6	18	11	4	16	9	2	14	7	0	12	5	17	10	3	15
2	16	9	2	14	7	0	12	5	17	10	3	15	8	1	13	6	18	11	4
3	5	17	10	3	15	8	1	13	6	18	11	4	16	9	2	14	7	0	12
4	13	6	18	11	4	16	9	2	14	7	0	12	5	17	10	3	15	8	1
5	2	14	7	0	12	5	17	10	3	15	8	1	13	6	18	11	4	16	0
6	10	3	15	8	1	13	6	18	11	4	16	9	2	14	7	0	12	5	17
7	18	11	4	16	9	2	14	7	0	12	5	17	10	3	15	8	1	13	6
8	7	0	12	5	17	10	3	15	8	1	13	6	18	11	4	16	0	2	14
9	15	8	1	13	6	18	11	4	16	9	2	14	7	0	12	5	17	10	3
10	4	16	9	2	14	7	0	12	5	17	10	3	15	8	1	13	6	18	11
11	12	5	17	10	3	15	8	1	13	6	18	11	4	16	0	2	14	7	0
12	1	13	6	18	11	4	16	9	2	14	7	0	12	5	17	10	3	15	8
13	9	2	14	7	0	12	5	17	10	3	15	8	1	13	6	18	11	4	16
14	17	10	3	15	8	1	13	6	18	11	4	16	9	2	14	7	0	12	5
15	6	18	11	4	16	9	2	14	7	0	12	5	17	10	3	15	8	1	13
16	14	7	0	12	5	17	10	3	15	8	1	13	6	18	11	4	16	9	2
17	3	15	8	1	13	6	18	11	4	16	9	2	14	7	0	12	5	17	10
18	11	4	16	9	2	14	7	0	12	5	17	10	3	15	8	1	13	6	18

$(Z_{23}, \oplus, \otimes)$

Kvadratické zbytky: $1^2 = 22^2 = 1,\ 2^2 = 21^2 = 4,\ 3^2 = 20^2 = 9,\ 4^2 = 19^2 = 16,\ 5^2 = 18^2 = 2,$ $6^2 = 17^2 = 13,\ 7^2 = 16^2 = 3,\ 8^2 = 15^2 = 18,\ 9^2 = 14^2 = 12,\ 10^2 = 13^2 = 8,\ 11^2 = 12^2 = 6.$

Výpočet směrnic pro GS-kvazigrupu: $x^2 \oplus 22x \oplus 22 = 0,$ $D = 22^2 - 4 \otimes 22 = 1 \oplus 4 = 5,$ 5 není kvadratický zbytek, GS-kvazigrupu nemůžeme sestrojit.

Výpočet směrnic pro hexagonální kvazigrupu: $x^2 \oplus 22x \oplus 1 = 0,$ $D = 22^2 - 4 \otimes 1 = 1 \oplus 19 = 20$, 20 není kvadratický zbytek, hexagonální kvazigrupu nelze sestrojit.

$(Z_{29}, \oplus, \otimes)$

Kvadratické zbytky: $1^2 = 28^2 = 1$, $2^2 = 27^2 = 4$, $3^2 = 26^2 = 9$, $4^2 = 25^2 = 16$, $5^2 = 24^2 = 25$, $6^2 = 23^2 = 7$, $7^2 = 22^2 = 20$, $8^2 = 21^2 = 6$, $9^2 = 20^2 = 23$, $10^2 = 19^2 = 13$, $11^2 = 18^2 = 5$, $12^2 = 17^2 = 28$, $13^2 = 16^2 = 24$, $14^2 = 15^2 = 22$.

Výpočet směrnic pro GS-kvazigrupu: $x^2 \oplus 28x \oplus 28 = 0$, $D = 28^2 - 4 \otimes 28 = 1 \oplus 4 = 5$, 5 je kvadratický zbytek, spočtěme tedy směrnice $q_1 = (-28 \oplus 11) \otimes 2^{-1} = 12 \otimes 15 = 6$, $q_2 = (-28 - 11) \otimes 2^{-1} = 19 \otimes 15 = 24$.

Směrnicemi jsou prvky 6 a 24.

Tabulka GS-kvazigrupy pro $q_1 = 6$:

*	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
0	0	6	12	18	24	1	7	13	19	25	2	8	14	20	26	3	9	15	21	27	4	10	16	22	28	5	11	17	23
1	24	1	7	13	19	25	2	8	14	20	26	3	9	15	21	27	4	10	16	22	28	5	11	17	23	0	6	12	18
2	19	25	2	8	14	20	26	3	9	15	21	27	4	10	16	22	28	5	11	17	23	0	6	12	18	24	1	7	13
3	14	20	26	3	9	15	21	27	4	10	16	22	28	5	11	17	23	0	6	12	18	24	1	7	13	19	25	2	8
4	9	15	21	27	4	10	16	22	28	5	11	17	23	0	6	12	18	24	1	7	13	19	25	2	8	14	20	26	3
5	4	10	16	22	28	5	11	17	23	0	6	12	18	24	1	7	13	19	25	2	8	14	20	26	3	9	15	21	27
6	28	5	11	17	23	0	6	12	18	24	1	7	13	19	25	2	8	14	20	26	3	9	15	21	27	4	10	16	22
7	23	0	6	12	18	24	1	7	13	19	25	2	8	14	20	26	3	9	15	21	27	4	10	16	22	28	5	11	17
8	18	24	1	7	13	19	25	2	8	14	20	26	3	9	15	21	27	4	10	16	22	28	5	11	17	23	0	6	12
9	13	19	25	2	8	14	20	26	3	9	15	21	27	4	10	16	22	28	5	11	17	23	0	6	12	18	24	1	7
10	8	14	20	26	3	9	15	21	27	4	10	16	22	28	5	11	17	23	0	6	12	18	24	1	7	13	19	25	2
11	3	9	15	21	27	4	10	16	22	28	5	11	17	23	0	6	12	18	24	1	7	13	19	25	2	8	14	20	26
12	27	4	10	16	22	28	5	11	17	23	0	6	12	18	24	1	7	13	19	25	2	8	14	20	26	3	9	15	21
13	22	28	5	11	17	23	0	6	12	18	24	1	7	13	19	25	2	8	14	20	26	3	9	15	21	27	4	10	16
14	17	23	0	6	12	18	24	1	7	13	19	25	2	8	14	20	26	3	9	15	21	27	4	10	16	22	28	5	11
15	12	18	24	1	7	13	19	25	2	8	14	20	26	3	9	15	21	27	4	10	16	22	28	5	11	17	23	0	6
16	7	13	19	25	2	8	14	20	26	3	9	15	21	27	4	10	16	22	28	5	11	17	23	0	6	12	18	24	1
17	2	8	14	20	26	3	9	15	21	27	4	10	16	22	28	5	11	17	23	0	6	12	18	24	1	7	13	19	25
18	26	3	9	15	21	27	4	10	16	22	28	5	11	17	23	0	6	12	18	24	1	7	13	19	25	2	8	14	20
19	21	27	4	10	16	22	28	5	11	17	23	0	6	12	18	24	1	7	13	19	25	2	8	14	20	26	3	9	15
20	16	22	28	5	11	17	23	0	6	12	18	24	1	7	13	19	25	2	8	14	20	26	3	9	15	21	27	4	10
21	11	17	23	0	6	12	18	24	1	7	13	19	25	2	8	14	20	26	3	9	15	21	27	4	10	16	22	28	5
22	6	12	18	24	1	7	13	19	25	2	8	14	20	26	3	9	15	21	27	4	10	16	22	28	5	11	17	23	0
23	1	7	13	19	25	2	8	14	20	26	3	9	15	21	27	4	10	16	22	28	5	11	17	23	0	6	12	18	24
24	25	2	8	14	20	26	3	9	15	21	27	4	10	16	22	28	5	11	17	23	0	6	12	18	24	1	7	13	19
25	20	26	3	9	15	21	27	4	10	16	22	28	5	11	17	23	0	6	12	18	24	1	7	13	19	25	2	8	14
26	15	21	27	4	10	16	22	28	5	11	17	23	0	6	12	18	24	1	7	13	19	25	2	8	14	20	26	3	9
27	10	16	22	28	5	11	17	23	0	6	12	18	24	1	7	13	19	25	2	8	14	20	26	3	9	15	21	27	4
28	5	11	17	23	0	6	12	18	24	1	7	13	19	25	2	8	14	20	26	3	9	15	21	27	4	10	16	22	28

Tabulka GS-kvazigrupy pro $q_2 = 24$:

∘	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
0	0	24	19	14	9	4	28	23	18	13	8	3	27	22	17	12	7	2	26	21	16	11	6	1	25	20	15	10	5
1	6	1	25	20	15	10	5	0	24	19	14	9	4	28	23	18	13	8	3	27	22	17	12	7	2	26	21	16	11
2	12	7	2	26	21	16	11	6	1	25	20	15	10	5	0	24	19	14	9	4	28	23	18	13	8	3	27	22	17
3	18	13	8	3	27	22	17	12	7	2	26	21	16	11	6	1	25	20	15	10	5	0	24	19	14	9	4	28	23
4	24	19	14	9	4	28	23	18	13	8	3	27	22	17	12	7	2	26	21	16	11	6	1	25	20	15	10	5	0
5	1	25	20	15	10	5	0	24	19	14	9	4	28	23	18	13	8	3	27	22	17	12	7	2	26	21	16	11	6
6	7	2	26	21	16	11	6	1	25	20	15	10	5	0	24	19	14	9	4	28	23	18	13	8	3	27	22	17	12
7	13	8	3	27	22	17	12	7	2	26	21	16	11	6	1	25	20	15	10	5	0	24	19	14	9	4	28	23	18
8	19	14	9	4	28	23	18	13	8	3	27	22	17	12	7	2	26	21	16	11	6	1	25	20	15	10	5	0	24
9	25	20	15	10	5	0	24	19	14	9	4	28	23	18	13	8	3	27	22	17	12	7	2	26	21	16	11	6	1
10	2	26	21	16	11	6	1	25	20	15	10	5	0	24	19	14	9	4	28	23	18	13	8	3	27	22	17	12	7
11	8	3	27	22	17	12	7	2	26	21	16	11	6	1	25	20	15	10	5	0	24	19	14	9	4	28	23	18	13
12	14	9	4	28	23	18	13	8	3	27	22	17	12	7	2	26	21	16	11	6	1	25	20	15	10	5	0	24	19
13	20	15	10	5	0	24	19	14	9	4	28	23	18	13	8	3	27	22	17	12	7	2	26	21	16	11	6	1	25
14	26	21	16	11	6	1	25	20	15	10	5	0	24	19	14	9	4	28	23	18	13	8	3	27	22	17	12	7	2
15	3	27	22	17	12	7	2	26	21	16	11	6	1	25	20	15	10	5	0	24	19	14	9	4	28	23	18	13	8
16	9	4	28	23	18	13	8	3	27	22	17	12	7	2	26	21	16	11	6	1	25	20	15	10	5	0	24	19	14
17	15	10	5	0	24	19	14	9	4	28	23	18	13	8	3	27	22	17	12	7	2	26	21	16	11	6	1	25	20
18	21	16	11	6	1	25	20	15	10	5	0	24	19	14	9	4	28	23	18	13	8	3	27	22	17	12	7	2	26
19	27	22	17	12	7	2	26	21	16	11	6	1	25	20	15	10	5	0	24	19	14	9	4	28	23	18	13	8	3
20	4	28	23	18	13	8	3	27	22	17	12	7	2	26	21	16	11	6	1	25	20	15	10	5	0	24	19	14	9
21	10	5	0	24	19	14	9	4	28	23	18	13	8	3	27	22	17	12	7	2	26	21	16	11	6	1	25	20	15
22	16	11	6	1	25	20	15	10	5	0	24	19	14	9	4	28	23	18	13	8	3	27	22	17	12	7	2	26	21
23	22	17	12	7	2	26	21	16	11	6	1	25	20	15	10	5	0	24	19	14	9	4	28	23	18	13	8	3	27
24	28	23	18	13	8	3	27	22	17	12	7	2	26	21	16	11	6	1	25	20	15	10	5	0	24	19	14	9	4
25	5	0	24	19	14	9	4	28	23	18	13	8	3	27	22	17	12	7	2	26	21	16	11	6	1	25	20	15	10
26	11	6	1	25	20	15	10	5	0	24	19	14	9	4	28	23	18	13	8	3	27	22	17	12	7	2	26	21	16
27	17	12	7	2	26	21	16	11	6	1	25	20	15	10	5	0	24	19	14	9	4	28	23	18	13	8	3	27	22
28	23	18	13	8	3	27	22	17	12	7	2	26	21	16	11	6	1	25	20	15	10	5	0	24	19	14	9	4	28

Výpočet směrnic pro hexagonální kvazigrupu: $x^2 \oplus 28x \oplus 1 = 0$,

$D = 28^2 - 4 \otimes 1 = 1 \oplus 25 = 26$, 26 není kvadratický zbytek, hexagonální kvazigrupu nelze sestrojit.

Pokud se na výše uvedené tabulky podíváme pozorněji, uvidíme několik zajímavých skutečností. Na úhlopříčce leží prvky 0, 1, 2, … tak, že na prvek *i* leží na průsečíku *i*-tého sloupce s *i*-tým řádkem. Důvodem je skutečnost, že každá GS-kvazigrupa i hexagonální kvazigrupa je idempotentní, tj. splňuje identitu $x^2 = x$.

Jak jsme již zmínili, v Z_5 je splněno $*^{op} = *$, operace je autoduální, tedy operace v GS-kvazigrupě je komutativní.

Nad Z_{11}, Z_{19}, Z_{29} se nám podařilo sestrojit vždy dvě navzájem duální GS-kvazigrupy, nad tělesy Z_3 , Z_7 , Z_{13}, Z_{19} byly sestrojeny navzájem duální hexagonální kvazigrupy.

Všimněme si, že nad tělesy Z_p, kde p prvočíslo, tabulka násobení v kvazigrupě vznikající podle vztahu (2.4) pomocí směrnice q je uspořádána poměrně pravidelným způsobem, protože každý řádek (sloupec) se liší od toho předchozího posunem. Vysvětlení je následující:
platí vztah $L_{a\oplus 1}(y) = L_a(y) \oplus (1-q) \pmod p$. (2.13)
Dokažme jej:
$L_{a\oplus 1} = (a \oplus 1) * y = (a \oplus 1) \otimes q \otimes (y - a - 1) = a \oplus 1 \oplus q \otimes y - q \otimes a - q = (1-q) \oplus$
$\oplus (a \oplus q \otimes (y - a)) = a * y \oplus (1-q) = L_a(y) \oplus (1-q)$ (vše mod p).

Lemma 3.1: Jestliže q je kořen rovnice $x^2 - x \oplus 1 = 0$ nebo $x^2 - x - 1 = 0$ nad Z_p, potom také $(1-q)$ je kořenem této rovnice.

Důkaz: Předpokládejme, že q je kořen rovnice $x^2 - x \oplus 1 = 0$, tedy $q^2 - q \oplus 1 = 0$, $(q-1)^2 - (q-1) \oplus 1 = 0$, po umocnění $1 - 2 \otimes q \oplus q^2 - 1 + q + 1 = q^2 - q \oplus 1 = 0$, tedy $(1-q)$ je kořen.
Nyní předpokládejme, že q je řešením $x^2 - x - 1 = 0$, platí $q^2 - q - 1 = 0$, po dosazení $(1-q)$ dostaneme $(q-1)^2 - (q-1) - 1 = 1 - 2 \otimes q \oplus q^2 - 1 \oplus q - 1 = q^2 - q - 1 = 0$. Kořenem je také $(1-q)$.

Pokusme se nyní sestrojit hexagonální a GS-kvazigrupy, nad tělesy $GF(q)$, kde $q = p^k$, $k \geq 2$. Tabulky těchto těles vkládáme, protože nejdou sestrojit tak lehce, jako tabulky těles v předchozích příkladech, pro těleso $GF(4)$ je převzata z [3], pro $GF(8)$ z [6] a pro $GF(9)$ z [7]. V tělesech charakteristiky 2 nemůžeme podle [11] užít vzorce s diskriminantem, použijeme však Viétových vztahů, $x^2 + rx + s = 0$, $x_1 \cdot x_2 = s$, $-r = x_1 + x_2$.

Příklad 3.7:

$GF(4)$

+	0	1	a	b
0	0	1	a	b
1	1	0	b	a
a	a	b	0	1
b	b	a	1	0

·	0	1	a	b
0	0	0	0	0
1	0	1	a	b
a	0	a	b	1
b	0	b	1	a

Výpočet směrnic pro GS-kvazigrupu: $x^2 + x + 1 = 0$, v našem případě je -*r* rovno 1 a *s* se též rovná jedna, v tělese platí $a \cdot b = 1$, $a + b = 1$, kořeny rovnice jsou tedy prvky *a* a *b* , tyto prvky jsou tedy směrnicemi GS-kvazigrupy.

Při výpočtu směrnic pro hexagonální kvazigrupu řešíme tutéž rovnici, jako pro GS-kvazigrupu. Tabulky GS-kvazigrupy a hexagonální kvazigrupy se tedy budou shodovat.

Tabulka GS-kvazigrupy (i hexagonální kvazigrupy) pro $q_1 = a$:

*	0	1	a	b
0	0	a	b	1
1	b	1	0	a
a	1	b	a	0
b	a	0	1	b

Tabulka GS-kvazigrupy (i hexagonální kvazigrupy) pro $q_2 = b$:

○	0	1	a	b
0	0	b	1	a
1	a	1	b	0
a	b	0	a	1
b	1	a	0	b

Pozorujeme, že tabulka není tak pravidelná, jako to bylo u kvazigrup nad Z_p.

$GF(8)$

+	0	1	a	b	c	d	e	f
0	0	1	a	b	c	d	e	f
1	1	0	b	a	d	c	f	e
a	a	b	0	1	e	f	c	d
b	b	a	1	0	f	e	d	c
c	c	d	e	f	0	1	a	b
d	d	c	f	e	1	0	b	a
e	e	f	c	d	a	b	0	1
f	f	e	d	c	b	a	1	0

·	0	1	a	b	c	d	e	f
0	0	0	0	0	0	0	0	0
1	0	1	a	b	c	d	e	f
a	0	a	c	e	b	1	f	d
b	0	b	e	d	f	c	1	a
c	0	c	b	f	e	a	d	1
d	0	d	1	c	a	f	b	e
e	0	e	f	1	d	b	a	c
f	0	f	d	a	1	e	c	b

Výpočet směrnic pro GS-kvazigrupu: $x^2 - x - 1 = 0, r = -1, s = -1$, -*r* je rovno 1, v tělese platí: $0 + 1 = 1$, $a + b = 1$, $c + d = 1$, $e + f = 1$, dále $1 \cdot 1 = 1$, $a \cdot d = 1$, $b \cdot e = 1$, $c \cdot f = 1$, z toho je patrné, že daná rovnice nemá nad tělesem řešení. Totéž platí i pro hexagonální kvazigrupu.

$GF(9)$

+	0	1	2	a	b	c	d	e	f
0	0	1	2	a	b	c	d	e	f
1	1	2	0	b	c	a	e	f	d
2	2	0	1	c	a	b	f	d	e
a	a	b	c	d	e	f	0	1	2
b	b	c	a	e	f	d	1	2	0
c	c	a	b	f	d	e	2	0	1
d	d	e	f	0	1	2	a	b	c
e	e	f	d	1	2	0	b	c	a
f	f	d	e	2	0	1	c	a	b

·	0	1	2	a	b	c	d	e	f
0	0	0	0	0	0	0	0	0	0
1	0	1	2	a	b	c	d	e	f
2	0	2	1	d	f	e	a	c	b
a	0	a	d	e	1	b	c	f	2
b	0	b	f	1	c	d	2	a	e
c	0	c	e	b	d	2	f	1	a
d	0	d	a	c	2	f	e	b	1
e	0	e	c	f	a	1	b	2	d
f	0	f	b	2	e	a	1	d	c

V tomto případě můžeme využít vzorce s diskriminantem. Kvadratické zbytky jsou následující: $1^2 = 2^2 = 1$, $a^2 = d^2 = e$, $b^2 = f^2 = c$, $c^2 = e^2 = 2$.

Řešme rovnici $x^2 - x - 1 = 0$, abychom získali směrnice pro GS-kvazigrupu. Diskriminant spočítáme následovně: $D = (-1)^2 - 4 \cdot 1 \cdot (-1) = (2)^2 - (1+1+1+1) \cdot 2 = 1 - 2 = 2$, 2 je kvadratický zbytek. Prvky *c* a *e* jsou vzájemně inverzní vzhledem ke sčítání, místo odčítání jednoho z prvků při výpočtu směrnic jednoduše přičteme ten druhý. Budou existovat směrnice

q_1 a q_2, $q_1 = (-(-1)+c)\cdot(2\cdot 1)^{-1} = a\cdot 2 = d$, $q_2 = (-(-1)+e)\cdot(2\cdot 1)^{-1} = f\cdot 2 = b$. kořeny rovnice jsou prvky *b* a *d*.

Tabulka GS-kvazigrupy pro $q_1 = b$:

*	0	1	2	a	b	c	d	e	f
0	0	b	f	1	c	d	2	a	e
1	d	1	c	e	2	a	f	d	b
2	a	e	2	b	f	0	c	d	1
a	c	d	1	a	e	2	b	f	0
b	2	a	e	0	b	f	1	c	d
c	f	0	b	d	1	c	e	2	a
d	e	2	a	f	0	b	d	1	c
e	b	f	0	c	d	1	a	e	2
f	1	c	d	2	a	e	0	b	f

Tabulka GS-kvazigrupy pro $q_2 = d$:

○	0	1	2	a	b	c	d	e	f
0	0	d	a	c	2	f	e	b	1
1	b	1	e	d	a	0	2	f	c
2	f	c	2	1	e	b	a	0	d
a	1	e	b	a	0	d	f	c	2
b	c	2	f	e	b	1	0	d	a
c	d	a	0	2	f	c	b	1	e
d	2	f	c	b	1	e	d	a	0
e	a	0	d	f	c	2	1	e	b
f	e	b	1	0	d	a	c	2	f

Výpočet směrnic pro hexagonální kvazigrupu: $x^2 + 2x + 1 = 0$, $-r = 1$, $s = 1$; v tělese platí: $0+1=1$, $2+2=1$, $a+e=1$, $b+d=1$, $c+f=1$, dále $1\cdot 1=1$, $2\cdot 2=1$, $a\cdot b=2$, $c\cdot e=1$, $d\cdot f=1$, vidíme, že rovnice má jeden dvojnásobný kořen 2.

Tabulka hexagonální kvazigrupy pro $q = 2$:

$*$	0	1	2	a	b	c	d	e	f
0	0	2	1	d	f	e	a	c	b
1	2	1	0	f	e	d	c	b	a
2	1	0	2	e	d	f	b	a	c
a	d	f	e	a	c	b	0	2	1
b	f	e	d	c	b	a	2	1	0
c	e	d	f	b	a	c	1	0	2
d	a	c	b	0	2	1	d	f	e
e	c	b	a	2	1	0	f	e	d
f	b	a	c	1	0	2	e	d	f

Pokud se pozorněji podíváme na rovnice řešené v tomto příkladě, můžeme si povšimnout, že součet kořenů je vždy roven 1. Podle definující rovnice operace pro kvazigrupu $(x, y) \to x * y$ dostaneme při výměně kořenů právě $(x, y) \to y * x$, čili duální operaci.

Tabulky vytvořených kvazigrup jsou pravidelné jiným způsobem než tomu bylo u Z_p, Uspořádání souvisí s tím, že aditivní grupa $GF(p^k)$ je rozložitelná, kdežto $Z_p = GF(p)$ rozložitelná není. U $GF(4)$ je aditivní grupa izomorfní s direktním součinem $Z_2 \times Z_2$, prvky jsou původně dvojice, ve kterých se počítá mod *2*, pak dojde k přeznačení, vyhovuje: $0 = (0,0)$, $1 = (0,1)$, $a = (1,0)$, $b = (1,1)$, tato skutečnost se projeví i v tabulce kvazigrupy.

Aditivní grupa tělesa $GF(9)$ je izomorfní s direktním součinem $Z_3 \times Z_3$, počítá se stejně jako ve výše uvedeném, prvky a odpovídající dvojice jsou následující: $0 = (0,0)$, $1 = (0,1)$, $2 = (0,2)$, $a = (1,0)$, $b = (1,1)$, $c = (1,2)$, $d = (2,0)$, $e = (2,1)$, $f = (2,2)$.

4 Izotopie kvazigrup

Definice 4.1: Jsou-li $(G,\cdot)$ a $(G',\cdot')$ grupoidy (nebo kvazigrupy), izotopií $(G,\cdot)$ na $(G',\cdot')$ nazveme uspořádanou trojici (α,β,γ) bijekcí G na G' takovou, že pro všechna $x,y\in G$ platí: $\alpha(x)\cdot'\beta(y)=\gamma(x\cdot y)$, nebo ekvivalentně $x\cdot y=\gamma^{-1}(\alpha(x)\cdot'\beta(y))$. Užijeme-li prvků $x',y'\in G'$, můžeme ekvivalentně psát $x'\cdot'y'=\gamma(\alpha^{-1}(x')\cdot'\beta^{-1}(y'))$. $(G',\cdot')$ je pak izotopem $(G,\cdot)$.
Inverzní izotopie má tvar $(\alpha^{-1},\beta^{-1},\gamma^{-1})$.

Lemma 4.1: Každý izotop kvazigrupy je kvazigrupa.

Důkaz: Nechť $(\alpha,\beta,\gamma):(G,\cdot)\to(G',\cdot')$ je izotopie kvazigrupy $(G,\cdot)$ na grupoid $(G',\cdot')$, kde $x'\cdot'y'=\gamma(\alpha^{-1}(x')\cdot'\beta^{-1}(y'))$ pro všechna $x',y'\in G'$. Ukažme jednoznačnou řešitelnost rovnic: Řešme pro $a',b'\in G'$, rovnice $a'\cdot'y=b'$ má zřejmě tvar $y=\beta(\alpha^{-1}(a')\setminus\gamma^{-1}(b'))$.
Stručně: Aplikujeme-li inverzní zobrazení β^{-1} , je předchozí vztah ekvivalentní s $\alpha^{-1}(a')\cdot\beta^{-1}(y)=\gamma^{-1}(b')$. Ekvivalentně můžeme psát $b'=\gamma(\alpha^{-1}(a')\cdot\beta'^{-1}(b'))=a'\cdot'y$. Jednoznačnost platí díky ekvivalenci předchozích rovností. Pro druhou rovnici podobně: $x\cdot a'=b'\Leftrightarrow\gamma(\alpha^{-1}(x)\cdot\beta^{-1}(a'))=b'\Leftrightarrow\alpha^{-1}(x)\cdot\beta^{-1}(a')=\gamma^{-1}(b')\Leftrightarrow x=\alpha(\gamma^{-1}(b')/\beta^{-1}(a'))$.
V případě, že $\gamma=id_Q$, mluvíme o hlavní izotopii a hlavním izotopu.
Jestliže hlavní izotopie $(\alpha,\beta,id_G):(G,\cdot)\to(G',\cdot')$ kvazigrupy $(G,\cdot)$ dává lupu $(G',\cdot')$, budeme užívat termínů LP-izotopie a LP-izotop (z anglického „loop principal“).
V případě, že $\alpha=\beta=\gamma$, příslušné izotopii (α,α,α) říkáme izomorfismus (grupoidů, kvazigrup,..) a značí se krátce α.
Izomorfním obrazem grupy (lupy) s jednotkou *e* je grupa (lupa) s jednotkou $\alpha(e)$.

Věta 4.1: Izotopické grupy jsou izomorfní.

Zatímco pro grupy je důležitějším pojmem izomorfismus, pro kvazigrupy hraje hlavní roli izotopie. Poznamenejme, že složení dvou izotopií je opět izotopie.

Lemma 4.2: Nechť $(G,\cdot)$ je mediální kvazigrupa s idempotentním prvkem $q \in G$. Zaveďme operaci $+_q$ vztahem: $x +_q y = R_q^{-1}(x) \cdot L_q^{-1}(y)$ pro všechna $x, y \in G$. Pak pro libovolné $x, y, z, w \in G$ platí: $x \cdot y +_q z \cdot w = (x +_q z) \cdot (y +_q w)$.
Řekneme, že operace $+_q$ a „$\cdot$“ vzájemně komutují.

Důkaz: Pišme $x = a \cdot q = q \cdot a'$ (tedy $a = x/q$), podobně $y = b \cdot q = q \cdot b'$, $z = c \cdot q = q \cdot c'$, $w = d \cdot q = q \cdot d'$. Pak díky medialitě a idempotentnosti prvku q, $x \cdot y = aq \cdot bq = ab \cdot (q \cdot q) = ab \cdot q$, podobně $zw = cq \cdot dq = (q \cdot q) \cdot (c' \cdot d') = q \cdot c'd'$. Nyní počítejme $xy +_q zw = ab \cdot c'd' = ac' \cdot bd' = (aq +_q qc') \cdot (bq +_q qd') = (x +_q z) \cdot (y +_q w)$.

Lemma 4.3: Je-li $\mathbf{G} = (G, +_q)$ komutativní grupa, která vznikla z mediální kvazigrupy a jejího idempotentního prvku q konstrukcí $x +_q y = R_q^{-1}(x) \cdot L_q^{-1}(y)$, pak jsou translace R_q a L_q komutující automorfismy grupy $\mathbf{G}$.

Důkaz: Abychom ukázali, že $R_q, L_q \in$ Aut($\mathbf{G}$) jsou automorfismy, užijeme lemmatu 4.2 a vztahu $q +_q q = q$:
$R_q(x) +_q R_q(y) = x \cdot q +_q y \cdot q = (x +_q y) \cdot (q +_q q) = (x +_q y) \cdot q = R_q(x +_q y)$, podobně pro L_q.
Dále pro každé $x \in G$, $R_q L_q(x) = (qx) \cdot q = (qx) \cdot (qq) = (qq) \cdot (xq) = q \cdot (xq) = L_q R_q(x)$, tedy $R_q L_q = L_q R_q$.

Věta 4.2: Nechť $(G,\cdot)$ je mediální kvazigrupa, $q \in G$ její idempotentní prvek, $q = q \cdot q$. Pak existuje komutativní grupa $\mathbf{G} = (G,*)$ a její komutující automorfismy $\alpha, \beta \in$ Aut ($\mathbf{G}$) takové, že platí $x \cdot y = \alpha(x) * \beta(y)$ pro všechna $x, y \in G$.

Důkaz: Podle předchozího stačí vzít: $\alpha = R_q$, $\beta = L_q$, $* = +_q$.

Věta 4.3: Nechť $(G, e, +)$ je komutativní grupa a nechť $\alpha, \beta \in$ Aut $(G,+)$ jsou její komutující automorfismy, $\alpha\beta = \beta\alpha$. Utvořme novou operaci „$\cdot$“ na nosiči G takto: $x \cdot y = \alpha(x) + \beta(y)$. Potom grupoid $(G,\cdot)$ je mediální kvazigrupa, jednotka e grupy je pro tento grupoid idempo-

tentním prvkem a zobrazení α, β se dají interpretovat jako pravý (respektive levý) zdvih prvkem *e* vzhledem k operaci „·“: $\alpha = R_e$, $\beta = L_e$.

Důkaz: Nechť $(Q, e, +)$ je komutativní grupa a α, β její komutující automorfismy. Zaveďme na *G* operaci „·“ vztahem $x \cdot y = \alpha(x) + \beta(y)$.

Vzniklý grupoid $(G, \cdot)$ je kvazigrupa, protože je izotopický s grupou $(G, +)$; (α, β, id) je hlavní isotopie $(G, \cdot)$ na lupu $(G, +)$ s jednotkou *e*. Zvolme prvky *u*, *v* z *G* takové, že $\alpha(u) = e = \beta(v)$. Z toho, že *e* je levá jednotka, odvodíme:

$L_u(y) = u \cdot y = \alpha(u) + \beta(y) = e + \beta(y) = \beta(y)$ pro všechna $y \in G$. Tedy $\beta = L_u$.

Podobně *e* je pravá jednotka, tedy pro všechna $x \in G$ platí : $R_v(x) = x \cdot v = \alpha(x) + \beta(v) = \alpha(x) + e = \alpha(x)$. Tedy $\alpha = R_v$. Přitom zřejmě $e = uv$: $e = \alpha(u) = R_v(u) = uv = L_u(v) = \beta(v)$. Dále, vlastnosti $\alpha(e) = e = \beta(e)$ můžeme přepsat jako $e \cdot v = e = u \cdot e$. Nyní dokážeme, že *e* je idempotentní prvek v $(G, \cdot)$, tj. $e \cdot e = e$, $e \cdot e = \alpha(e) + \beta(e) = e \cdot v + u \cdot e = e + e = e$. Díky krácení zleva (zprava) získáme $v = e = u$. Máme tedy $x \cdot y = xe + ye$. Dokažme medialitu kvazigrupy $(G, \cdot)$. Počítejme $ab \cdot cd = (a \cdot e + e \cdot b) \cdot (c \cdot e + d \cdot e) = ((ae + eb) \cdot e) + (e \cdot (ce + ed)) = (ae \cdot e + eb \cdot e) + (e \cdot ce + e \cdot ed)$ (opakovaně jsme používali definici operace automorfismů $\alpha = R_e$, $\beta = L_e$).

Nyní podobně vyjádříme $ac \cdot bd = (ae \cdot e) + (ec \cdot e) + (e \cdot be) + (e \cdot ed)$. Pravou stranu ještě upravme použitím vztahů $e \cdot xe = L_e(R_e x) = R_e(L_e x) = ex \cdot e$, pro $x = c$ a $x = b$. Tím dostaneme stejný výraz jako ve výpočtech výše, a tedy medialitu $ab \cdot cd = ac \cdot bd$.

Důsledek 4.1:

Grupoid $(G, \cdot)$ je mediální kvazigrupa s idempotentní prvkem *e*, právě když existuje komutativní grupa $(G, e, +)$ s jednotkou *e* a dvojice jejích automorfismů $\alpha, \beta \in \mathrm{Aut}(\mathbf{G})$ splňujících $\alpha\beta = \beta\alpha$ a $x \cdot y = \alpha(x) + \beta(y)$. V tom případě je $\alpha = R_e$ a $\beta = L_e$.

Pozn. 4.1: Připomeňme, že automorfismus α aditivní grupy $(G, e, +)$ má vlastnosti $\alpha(e) = e$, $\alpha(x + y) = \alpha(x) + \alpha(y)$, $\alpha(-x) = -\alpha(x)$.

Speciálně automorfismus je bijekcí *G* na *G*, tedy permutací množiny *G*.

5 Rovnoběžníkové prostory

Poslední část diplomové práce byla zpracována podle [3].

5.1 Rovnoběžníkové prostory obecně

Definice 5.1.1: *Rovnoběžníkovým prostorem* budeme rozumět trojici $(P,V,*)$, kde P je neprázdná množina, V je množina, $*: P\times V \to P, (p,v) \mapsto p*v$ je zobrazení a platí:

(i) Pro libovolné prvky $A,B \in P$ existuje právě jedno $v \in V$ tak, že $A*v = B$ (pravidlo tranzivity),

(ii) $(A*v)*w = (A*w)*v$ pro všechna $A \in P$ a $v,w \in V$ (pravidlo rovnoběžníků).

Prvky množiny P nazýváme body a prvky V vektory, * se nazývá bodově-vektorové zobrazení.

Podle (i) můžeme zavést zobrazení $\vec{}: P\times P \to V$, takzvanou *translac*i na P tak, že

(iii) pro každé $A,B \in P$, $A*\vec{AB} = B$.

Podívejme se, jak lze zavést rovnoběžníkový prostor jinak:

Definice 5.1.2: Rovnoběžníkový prostor je čtveřice $(P,V,*,\vec{})$, kde P, V jsou neprázdné množiny, $*: P\times V \to P$, $\vec{}: P\times P \to V$ zobrazení a jsou splněny podmínky (ii) a (iii).

Rovnoběžníkový prostor lze definovat i následovně:

Definice 5.1.3: Rovnoběžníkový prostor je trojice $(P,V,\vec{})$, kde $P,V \neq \emptyset$ a zobrazení $\vec{}: P\times P \to V$ splňuje podmínky:

(i´) pro každé $A \in P$, $v \in V$ existuje právě jedno $B \in P$ takové, že $\vec{AB} = v$,

(ii´) pro všechna $A,B,C,D \in P$, $\vec{AB} = \vec{CD} \Leftrightarrow \vec{AC} = \vec{BD}$.

Ekvivalentnost definicí můžeme jednoduše zkontrolovat. Podle (i´) můžeme zavést zobrazení $*: P \times V \to P, (\mathrm{A}, v) \mapsto \mathrm{B}$, které splňuje (i), (iii). Nyní pomocí (ii´) dostaneme (ii) $\vec{\mathrm{AB}} = v, \vec{\mathrm{AC}} = w$. Naopak z (ii) dostáváme (ii´) pod označením $\mathrm{A} * v = \mathrm{B}, \mathrm{A} * w = \mathrm{C}$.

5.2 Strukturové vlastnosti rovnoběžníkových prostorů

Věta 5.2.1: (a) (*sčítání vyjádřené pomocí bodově-vektorového zobrazení*)
Nechť $(P, V, *)$ je rovnoběžníkový prostor, pak existuje právě jedno zobrazení $+: V \times V \to V$ takové, že pro všechna $\mathrm{A} \in P$ a $v, w \in V$ platí:

$$\mathrm{A} * (v + w) = (\mathrm{A} * v) * w. \tag{5.1}$$

(b) Rovnoběžníkový prostor $(P, V, *)$ lze získat z grupoidu $(V, +)$ právě tehdy, když $(V, +)$ je komutativní grupa. Operace „*“ a „+“spolu souvisejí podle (5.1).

Důkaz:
(a) Nechť $\mathrm{A}, \mathrm{B} \in P$ a $v, w \in V$. Dále nechť $\overline{v}, \overline{w} \in V$ jsou takové,že $(\mathrm{A} * v) * w = \mathrm{A} * \overline{v}$, $\mathrm{A} * \overline{w} = \mathrm{B}$. Použitím (ii) obdržíme $(\mathrm{B} * v) * w = ((\mathrm{A} * \overline{w}) * v) * w = ((\mathrm{A} * v) * w) * \overline{w} = (\mathrm{A} * \overline{v}) * \overline{w} = (\mathrm{A} * \overline{w}) * \overline{v} = \mathrm{B} * \overline{v}$, což ukazuje, že vzhledem k v, w je vektor $\overline{v}$ splňující $(\mathrm{A} * v) * w = \mathrm{A} * \overline{v}$ nezávislý na volbě bodu A. Tedy binární operace + na V, $(v, w) \to \overline{v}$ je podle (5.1) dobře definována. Použitím (i´), (ii´), (5.1) dostáváme

$$\vec{\mathrm{AB}} + \vec{\mathrm{BD}} = \vec{\mathrm{AD}}. \tag{5.1´}$$

(b) Nechť $(P, V, *)$ je rovnoběžníkový prostor a + je sčítání z (5.1). Použijme (i) k odvození komutativity + z (5.1) a (ii), asociativitu + dokážeme několikerým použitím (5.1).

Nyní nechť $\mathrm{A} \in P$. Označme e_{A} vektor určený pomocí $\mathrm{A} * e_{\mathrm{A}} = \mathrm{A}$ podle (i). Dle (5.1) obdržíme $\mathrm{A} * v = (\mathrm{A} * e_{\mathrm{A}}) * v = \mathrm{A} * (\mathrm{e}_A + v)$ pro všechna $v \in V$. Užitím (i) dostáváme $v = e_{\mathrm{A}} + v$, tedy e_{A} je neutrální prvek vzhledem k +, nezávisle na A. Místo e_{A} budeme psát jednodušeji e.

Podle (i) každé $v \in V$ jednoznačně určuje $\overline{v} \in V$, které splňuje $(\mathrm{A} * v) * \overline{v} = \mathrm{A}$. Ale podle (5.1) $\mathrm{A} * (v + \overline{v}) = \mathrm{A} = \mathrm{A} * e$, tedy opět podle (i) $(v + \overline{v}) = e$. Proto $\overline{v}$ je inverzní (opačný vektor) k v vzhledem k +, a $(V, +)$ je komutativní grupa.

Opačně, začněme s komutativní grupou $(V,+)$, trojice $(V,V,+)$ splňuje podmínky rovnoběžníkového prostoru. Opravdu, (i) plyne z rovnic ve tvaru $v+x=w$ pro $v,w\in V$, které jsou jednoznačně řešitelné pro $x\in V$. Vzhledem k asociativitě a komutativitě + platí (ii) a (5.1) je určena asociativitou.

Podle důkazu části (b) je splněno následující:

Poznámka 5.2.1: Pro každé $\mathrm{A}\in P$, $\mathrm{A}*e=\mathrm{A}$ a platí $\vec{\mathrm{AA}}=e$.

Dále uvažujme rovnoběžníkový prostor s význačným bodem $\mathrm{O}\in P$, kterému říkáme počáteční nebo referenční bod.

Definice 5.2.1: *Homomorfismus* vektorového prostoru $(P,V,*)$ do vektorového prostoru $(P',V',*')$ je definován jako dvojice zobrazení $\alpha:P\to P'$, $\beta:V\to V'$ takových, že

(iv) $\alpha(\mathrm{A})*'\beta(v)=\alpha(\mathrm{A}*v)$ pro všechna $\mathrm{A}\in P$, $v\in V$.

Homomorfismus se nazývá *izomorfismem*, když jsou zobrazení α a β bijektivní.

Věta 5.2.2: Nechť je dán rovnoběžníkový prostor $(P,V,*)$ s počátečním bodem O, pak dvojice zobrazení $P\to V$, $\mathrm{A}\mapsto\vec{\mathrm{OA}}$; $id_v:V\to V$, $v\mapsto v$ je izomorfismus $(P,V,*)$ do $(V,V,+)$. Operace + je definována podle (5.1).

Vztah mezi homomorfismy rovnoběžníkových prostorů a homomorfismy komutativních grup je popsán v následující větě.

Věta 5.2.3: (a) Nechť (α,β) jsou homomorfismy rovnoběžníkového prostoru $(P,V,*)$ do rovnoběžníkového prostoru $(P',V',*')$ a nechť + a $+'$ jsou odpovídající binární operace na V a V' zavedené podle (5.1) . Pak β je homomorfismus $(V,+)$ do $(V',+')$ takový, že

$$\alpha(\mathrm{A})=\alpha(\mathrm{O})*'\beta(\vec{\mathrm{AO}}) \text{ pro všechna } \mathrm{O},\mathrm{A}\in P. \qquad (5.2)$$

(b) Naopak, každý homomorfismus β z $(V,+)$ do $(V',+')$ společně s výběrem bodů $O \in P$, $O' \in P'$ určuje zobrazení $\alpha : P \to P', A \mapsto O *' \beta(\vec{OA})$ takové, že $O' = \alpha(O)$. Pak dvojice (α, β) je homomorfismus $(P,V,*)$ do $(P',V',*')$.

Důkaz: Ukažme, že zobrazení β je podle (iv) jednoznačně určeno zobrazením α. Jestliže je dán bod $B \in P$, pak existuje jediné $v' \in V'$ takové, že $\alpha(B) *' v' = \alpha(B * v)$ (kde jsme použili (i) pro $(P',V',*')$). Užitím (iv) a (5.1) obdržíme $\alpha(B) *' \alpha(v+w) = (\alpha(B) *' \beta(v)) *' \beta(w) =$ $= \alpha(B) *' (\beta(v) +' \beta(w))$. Použitím (i) dostáváme $\beta(v+w) = \beta(v) +' \beta(w)$ pro všechna $v, w \in V$. Tedy β je grupový homomorfismus grupy $(V,+)$ do grupy $(V',+')$. Nyní ověříme $\alpha(O) *' \beta(\vec{OB}) = \alpha(B)$ pro všechna $B \in P$.

Naopak, mějme dán homomorfismus β z $(V,+)$ do $(V',+')$ a body $A, B \in P$, použitím (5.1), (5.1′) a (5.2) obdržíme $\alpha(A) *' \beta(\vec{AB}) = (\alpha(O) *' \beta(\vec{OA})) *' \beta(\vec{AB}) = (\alpha(O) *'$ $(\beta(\vec{OA}) +' \beta(\vec{AB}) = \alpha(B) = \alpha(A * \vec{AB})$. Tedy (iv) platí pro $v = \vec{AB}$. Protože $\vec{OO}$ je neutrální prvek vzhledem k +, je i $\beta(\vec{OO})$ neutrálním prvkem vzhledem k +′, podle poznámky 5.2.1.

Když P, P' jsou afinní prostory a V, V' jsou vektorové prostory nad základním tělesem $\mathbf{T}$, pak podmínka (5.2) musí být doplněna požadavkem $\beta(a \cdot v) = a \cdot \beta(v)$ pro všechna $(a,v) \in \mathbf{T} \times V$. Zobrazení α je pak afinním zobrazením afinního prostoru a určuje podkladové lineární zobrazení β odpovídajících lineárních prostorů. Obráceně, nechť je dán obraz jediného bodu $A \in P$, pak je afinní zobrazení α jednoznačně určeno pomocí lineárního zobrazení β.

Nechť $(P,V,*) = (P',V',*')$, pak podmínka (iv) je ekvivalentní s podmínkou

$$\vec{O\alpha(A)} = \vec{O\alpha(O)} +' \beta(\vec{OA}). \qquad \text{(iv′)}$$

To můžeme ověřit pomocí následující rovnosti

$$O * (\vec{O\alpha(O)} +' \beta(\vec{OA})) = \alpha(O) * \beta(\vec{OA}),$$

která plyne z výše uvedeného a dohody, že $\vec{AB} = v$ právě tehdy, když $A * v = A * (a+b) = (A * a) * b$.

Obdržíme tak obvyklejší popis afinního zobrazení pomocí podkladového lineárního zobrazení β, polohových vektorů, bodů („radiusvektorů“) a jejich bodových obrazů vzhledem k počátku O.

Důkaz věty 5.2.3 vyžaduje pouze podmínky (i´), (ii´) a existenci pravého neutrálního prvku vzhledem k +. Důkaz věty 5.2.1 části (b) ukazuje, že $(V,+)$ je grupa. Skutečně, čtveřice $(P,V,*,+)$ splňující podmínky (i´) a (5.1) a s pravým neutrálním prvkem je grupa, která operuje jednoduše tranzitivně na *P*. Podmínka (ii´) zaručuje komutativitu +, která ve větě 5.2.3 nebyla třeba. Tedy pro každou grupu $(V,+)$ poskytuje věta 5.2.3 popis homomorfismu (α, β) z $(V,V,+)$ do $(V,V,+)$ pomocí akce grupy na sobě. Formule (iv), $\alpha(\mathrm{A})*' \beta(v) = \alpha(\mathrm{A}*v)$, kde $\mathrm{A} \in P, v \in V$, má tvar $\alpha(v) + \beta(w') = \alpha(v+w)$ pro všechna $v, w \in V$. Zde je β endomorfismus grupy $(V,+)$ a existuje právě jeden vektor $v_0 \in V$ takový, že $\alpha(v) = v_0 + \beta(v)$ pro každé $v \in V$. Zobrazení α je levou translací, právě když $\alpha = id_V$, α je vnitřní automorfismus $(V,+)$ v témž případě.

Vezměme nyní v úvahu rovnoběžníkový prostor $(V,V,+)$ vytvořený z komutativní grupy $(V,+)$ (poznamenejme, že podle věty 5.2.1 musí být uvažovaná grupa komutativní v případě, že se operace * a + v (5.1) shodují).

Věta 5.2.4: $(V,V,*)$ je rovnoběžníkový prostor právě tehdy, když existuje komutativní grupa $(V,+')$ a permutace $f: V \to V$ taková, že pro všechna $v, w \in V$ platí $v * w = v +' f(w)$.

Důkaz: Trojice $(V,V,*)$, $V \neq \emptyset$, $*: V \times V \to V$ určuje rovnoběžníkový prostor právě tehdy, když platí následující podmínky

(i°) pro všechna $u, v \in V$ existuje právě jedno $w \in V$ tak, že $v * w = u$,

(ii°) $(w*u)*v = (w*v)*u$ pro všechna $u, v, w \in V$.

Mějme dány vektory $a, b \in V$, nechť vektory $e, c \in V$ jsou určené pomocí (i°) tak, že $a * e = a, \quad a * c = b$, použitím (ii°) vypočítáme $b * e = (a*c)*e = (a*e)*c = a*c = e$, proto je vektor *e* pravým neutrálním prvkem vzhledem k *. Podle věty 5.2.1 (a) existuje binární operace $+: V \times V \to V$ splňující

$$v*(a+b) = (v*a)*b \text{ pro každé } a, b, v \in V. \qquad (5.3)$$

Podle věty 5.2.1 (b) je $(V,+)$ komutativní grupa s neutrálním prvkem *e*. Z (i°) vyplývá, že zobrazení $f:V\to V, v\mapsto e*v$ je permutací na *V*. Ve vztahu (5.3) položme $e=v$, dostaneme $f(a+b)=f(a)*b$. Zavedením binární operace $+'$ pomocí $f(a)+'f(b)=f(a+b)$ pro všechna $a,b\in V$ získáme izomorfismus $(V,+)$ na $(V',+')$. Tedy také $(V',+')$ je komutativní grupa a $f(a)*b=f(a)+'f(b)$ pro všechna $a,b\in V$. Obdrželi jsme izotopii $(V,*)$ na komutativní grupu.

Opačně, mějme komutativní grupu a permutaci $f:V\to V$. Izotopie zavedená výše zaručuje splnění podmínek (i°) a (ii°), což je vidět z následujícího: $(c*a)*b=(c+'f(a))+'f(b)=(c+'f(b))+'f(a)=(c*b)*a$, tedy $a*c=b$ právě tehdy, když $a+'f(c)=b$.

Nakonec popíšeme ještě jiné zavedení rovnoběžníkových prostorů: geometrické:

Definice 5.2.2: Rovnoběžníkový prostor nyní definujeme jako dvojici $(P,\mathbf{P})$ takovou, že *P* je neprázdná množina a $\mathbf{P}\neq\emptyset$ je kvaternární relace na *P*, musí platit následující axiomy:

1˘ Pro každé $a,b,c\in P$ existuje právě jedno $d\in P$ takové, že platí $\mathbf{P}(a,b,c,d)$.

2˘ Jestliže (e,f,g,h) je cyklická permutace prvků (a,b,c,d) nebo (d,c,b,a), kde $a,b,c,d\in G$, pak $\mathbf{P}(a,b,c,d)$ implikuje $\mathbf{P}(e,f,g,h)$.

3˘ Pro všechna $a,b,c,d,e,f\in G$, jestliže $\mathbf{P}(a,b,c,d)$ a $\mathbf{P}(c,d,e,f)$, pak $\mathbf{P}(a,b,f,e)$.

Prvky z *P* nazýváme body rovnoběžníkového prostoru. Každá čtveřice $(a,b,c,d)\in\mathbf{P}$ se nazývá rovnoběžník, zápis $(a,b,c,d)\in\mathbf{P}$ můžeme psát také jako $\mathbf{P}(a,b,c,d)$.

Mějme rovnoběžníkový prostor $(P,\mathbf{P})$ a binární operaci $\cong$ na $P\times P$ definovanou

$$(a,b)\cong(c,d)\Leftrightarrow\mathbf{P}(a,b,c,d). \qquad (5.4)$$

Jednoduše můžeme zkontrolovat, že $\cong$ je relace ekvivalence. Prvky (třídy) rozladu faktorové množiny $P\times P/\cong$ se nazývají vektory. Vektor se skládá z dvojice $(a,b)\in P\times P$, kterou označujeme $\overrightarrow{(a,b)}$.

Jestliže označíme $V = P \times P / \cong$, $\vec{\ } : P \times P \to V$, $(a,b) \mapsto (\overrightarrow{a,b})$, pak $(P,V,\vec{\ })$ je rovnoběžníkový prostor ve smyslu třetí definice. opravdu, podmínka (i´) vyplývá z definice $\vec{\ }$ a z 1˘, zatímco podmínka (ii´) vyplývá z 2˘ a 3˘ a z definice $\vec{\ }$.

Opačně, mějme dán rovnoběžníkový prostor $(P,V,\vec{\ })$ podle třetí definice, definujme na něm rovnoběžník (v novém smyslu) jako čtveřici (a,b,c,d), $a,b,c,d \in P$ takovou, že platí $(\overrightarrow{a,b}) = (\overrightarrow{c,d})$. Podmínky (i´) a (ii´) umožňují ověření 1˘, 2˘, 3˘. Tedy P společně s množinou všech „nových“ rovnoběžníků je rovnoběžníkový prostor v posledním smyslu.

Poznamenejme, že ve výše uvedeném přístupu k zavedení rovnoběžníkového prostoru může být podmínka 1˘ nahrazena podmínkou

4˘ Pro všechna $a,b,c \in P$ existuje právě jedno $d \in P$ takové, že platí $\mathbf{P}(a,b,c,d)$.

To můžeme ověřit, jestliže přejdeme od $\mathbf{P}(a,b,c,d)$ k $\mathbf{P}(b,a,d,c)$ a vhodně užijeme cyklickou permutaci a 2˘: $\mathbf{P}(a,b,c,d) \Leftrightarrow \mathbf{P}(c,d,a,b) \Leftrightarrow \mathbf{P}(b,a,d,c)$.

Čtveřice (a,b,c,d) je rovnoběžníkový prostor v „geometrickém“ smyslu právě tehdy, když čtveřice (a,b,c,d) je rovnoběžníkem ve výše uvedeném smyslu.

5.3 Grupy transferů mediální kvazigrupy

Definice 5.3.1: Nechť $\mathbf{G}=(G,\cdot)$ je mediální kvazigrupa. Pro každé $a,b \in G$ zavedeme *levý transfer* $L_{a,b}$ jako složení (zprava doleva) $L_b^{-1}L_a$ a *pravý transfer* jako $R_{a,b} =: R_b^{-1}R_a$. To je

$$L_{a,b}(c) = d \Leftrightarrow ac = bd \text{ pro všechna } a,b,c,d \in G \tag{5.5}$$

a podobně

$$R_{a,b}(c) = d \Leftrightarrow ca = db. \tag{5.6}$$

Proto v mediálních kvazigrupách platí následující „polární“ vlastnost:

$$L_{a,b}(c) = d \Leftrightarrow R_{c,d}(a) = b. \tag{5.7}$$

Protože $\mathbf{G}$ je kvazigrupa, vezmeme-li tři z prvků $a,b,c,d \in G$, rovnost $ac = bd$ (respektive $ca = db$) určuje v $\mathbf{G}$ jednoznačně čtvrtý prvek (což lze nazvat *„vlastnost čtvrtého prvku“*). Jako důsledek pomocí pravého (resp. levého) krácení obdržíme následující vlastnosti pro mediální kvazigrupy

$L_{a,b} = L_{a,b'} \Rightarrow b = b'$, $\quad L_{a,b} = L_{a',b} \Rightarrow a = a'$,

$R_{a,b} = R_{a,b'} \Rightarrow b = b'$, $\quad R_{a,b} = R_{a',b} \Rightarrow a = a'$.

Lemma 5.3.1: Nechť a,b,c,d,x_0 jsou prvky mediální kvazigrupy $\mathbf{G}=(G,\cdot)$ splňující $L_{a,b}(x_0) = R_{c,d}(x_0)$. Pak $L_{a,b} = R_{c,d}$.

Důkaz: Nechť $x \in G$ je libovolný prvek a $x' =: L_{a,b}(x)$ (tj. $ax = bx'$). Náš předpoklad lze zapsat jako $ax_0 = bx_0'$ a $x_0 c = x_0' d$. Z mediality G lze vyvodit $(ax_0)(xc) = (ax)(x_0 c) = (bx')(x_0' d) = (bx_0')(x' d) = (ax_0)(x' d)$. Použitím levého krácení dostáváme $xc = x' d$, což znamená $R_{c,d}(x) = x'$. Podle toho $L_{a,b} = R_{c,d}$ (protože *x* bylo libovolné).

Lemma 5.3.2: Nechť $\mathbf{G}=(G,\cdot)$ je mediální kvazigrupa, pak každá rovnice ve tvaru $L_{a,b} = R_{c,d}$, kde jsou dány tři z prvků $a,b,c,d \in G$ a čtvrtý je neznámý, je jednoznačně řešitelná v *G*.

Důkaz: Nechť $a,b,c \in G$, vyberme pomocné prvky $q,q' \in G$ takové, že $L_{a,b}(q) = q'$. Pak existuje jediné $d \in G$ tak, že $cq = dq'$ (podle vlastnosti čtvrtého prvku), tj. $R_{c,d}(q) = q'$. Proto $L_{a,b}(q) = R_{c,d}(q)$, tedy $L_{a,b} = R_{c,d}$ podle lemmatu 5.3.1. Jestliže $L_{a,b} = R_{c,d'}$, pak $R_{c,d} = R_{c,d'}$, následně $d = d'$. Podobně v ostatních případech.

Lemma 5.3.3: Nechť $\mathbf{G}=(G,\cdot)$ je mediální kvazigrupa a $a,b,c,d \in G$. Jestliže existuje $q \in G$ takové, že $L_{a,b}(q) = L_{c,d}(q)$, pak $L_{a,b} = L_{c,d}$. Jestliže existuje $q \in G$ tak, že $R_{a,b}(q) = R_{c,d}(q)$, pak $R_{a,b} = R_{c,d}$.

Důkaz: Předpokládejme $L_{a,b}(q) = L_{c,d}(q) = q'$ a zvolme pomocný prvek $r \in G$. Podle vlastnosti čtvrtého prvku existuje právě jeden prvek $s \in G$ tak, že $R_{r,s}(q) = q'$. Z rovnosti $L_{a,b}(q) = R_{r,s}(q) = L_{c,d}(q)$ podle lemmatu 5.3.1 vyplývá, že $L_{a,b} = R_{r,s} = L_{c,d}$. Analogicky pro pravý transfer.

Jako důsledek máme: Jestliže platí $L_{a,b} = L_{c,d}$ (respektive $R_{a,b} = R_{c,d}$), pak každé tři z prvků $a,b,c,d \in G$ jednoznačně určují třetí.

Nakonec uveďme, že v každé mediální kvazigrupě $\mathbf{G}=(G,\cdot)$ jsou splněny následující ekvivalence :

$$L_{a,b} = L_{c,d} \quad \Leftrightarrow \quad L_{a,c} = L_{b,d} \quad \Leftrightarrow \quad R_{a,b} = R_{c,d} \quad \Leftrightarrow \quad R_{a,c} = R_{b,d}\,. \tag{5.8}$$

Podle lemmatu 5.3.2 je každý levý transfer zároveň pravým transferem a opačně. Množinu všech levých transferů společně s množinou všech pravých transferů označíme $\mathbf{T_G}$. Její prvky nazýváme transfery na $\mathbf{G}$.

Věta 5.3.1: Nechť $\mathbf{G}=(G,\cdot)$ je mediální kvazigrupa. Pak $(\mathbf{T_G}, id_{\mathbf{G}}, \circ)$ je komutativní grupa, která působí jednoduše tranzitivně na $\mathbf{G}$.

Důkaz: Pro jednoduchost budeme psát skládání zobrazení vedle sebe místo zápisu binární operace $\circ$. Nechť $\tau_1, \tau_2 \in \mathbf{T_G}$ a $a \in G$. Podle lemmat 5.3.2 a 5.3.3 můžeme vybrat prvky $b,c,d \in G$ tak, že $\tau_1 = L_{a,b}, \tau_2 = L_{a,c}, \tau_1 = L_{c,d}$. Z toho vyplývá, že $L_{a,b} = L_{c,d}$ a následně $L_{a,c} = L_{b,d} = \tau_2$. Tedy dostáváme $\tau_1\tau_2 = L_{c,d}L_{a,c} = L_d^{-1}L_cL_c^{-1}L_a = L_{a,d} \in \mathbf{T_G}$.
Nyní $\tau_2\tau_1 = L_{b,d}L_{a,b} = L_d^{-1}L_bL_b^{-1}L_a = L_{a,d} = \tau_1\tau_2$. Proto platí komutativita. Pro pevné $a \in G$, libovolné, je zobrazení $L_{a,a} = id_{\mathbf{G}}$ neutrálním prvkem grupoidu $(\mathbf{T_G}, \circ)$. Jestliže $a,b \in G$, pak $L_{b,a}L_{b,a} = L_{a,a}$, tedy $L_{b,a}$ a $L_{a,b}$ jsou navzájem inverzní. Jestliže $c,d \in G$, pak existuje právě jeden transfer takový, že $\tau(c) = d$; podle vlastnosti čtvrtého prvku, pro každé $a \in G$ existuje právě jeden prvek $b \in G$ tak, že $L_{a,b}(c) = d$. Z rovnosti $\tau(c) = L_{a,b}(c) = d$ dostáváme podle lemmat 5.3.1 a 5.3.2 $\tau = L_{a,b}$.

Nyní uvedeme přehled některých další vlastností transferů mediální kvazigrupy $(G,\cdot)$.

(i) Následující rovnosti jsou platné pro všechna $a,b,c \in G$:

$$L_{a,b}L_{b,c} = L_{b,c}L_{a,b} = L_{a,c}\,, \tag{5.9}$$

$$R_{a,b}R_{b,c} = R_{b,c}R_{a,b} = R_{a,c}\,. \tag{5.10}$$

(ii) Ze dvou následujících rovností vyplývá třetí:

$$L_{a,c}(u) = u', \tag{5.11}$$

$$L_{b,d}(v) = v', \tag{5.12}$$

$$L_{ab,cd}(uv) = u'v'. \tag{5.13}$$

(iii) Ze dvou následujících rovností vyplývá třetí:

$$L_{a,c} = L_{á',c'}, \tag{5.14}$$

$$L_{b,d} = L_{b',d'}, \tag{5.15}$$

$$L_{ab,cd} = L_{a'b',c'd'}; \tag{5.16}$$

podobně pro trojici podmínek:

$$R_{a,c} = R_{á',c'}, \tag{5.17}$$

$$R_{b,d} = R_{b',d'}, \tag{5.18}$$

$$R_{ab,cd} = R_{a'b',c'd'}. \tag{5.19}$$

(iv) Z jakýchkoli čtyř z následujících pěti rovností vyplývá zbývající:

$$L_{a,b}(x) = x', \tag{5.20}$$

$$L_{c,d}(y) = y', \tag{5.21}$$

$$L_{ac,bd}(z) = z', \tag{5.22}$$

$$xy = z, \tag{5.23}$$

$$x'y' = z'; \tag{5.24}$$

podobně pro

$$R_{a,b}(x) = x', \tag{5.25}$$

$$R_{c,d}(y) = y', \tag{5.26}$$

$$R_{ac,bd}(z) = z', \tag{5.27}$$

$$xy = z, \tag{5.28}$$

$$x'y' = z'. \tag{5.29}$$

5.4 Rovnoběžníkové prostory mediálních kvazigrup

Nechť $\mathbf{G}=(G,\cdot)$ je mediální kvazigrupa. Ukažme nyní způsob jak přejít od grupy $(\mathbf{T}_\mathbf{G},\circ)$, která působí jednoduše tranzitivně na G, k rovnoběžníkovému prostoru v „geometrickém“ smyslu definice 5.2.1.

Uspořádané čtveřici $(a,b,c,d)\in G\times G\times G\times G$ budeme říkat rovnoběžník na $\mathbf{G}$ v případě, že $L_{a,b}=L_{d,c}$, nebo jinak řečeno, jestliže existuje transfer τ takový, že $\tau(a)=b,\ \tau(d)=c$. Množinu tvořenou všemi rovnoběžníky značíme $\mathbf{T}_\mathbf{G}$. Podle definice 5.2.1 binární relace $\cong$ na $\mathbf{G}$, určená pomocí $(a,b)\cong(c,d)\Leftrightarrow \mathbf{P}(a,b,c,d)$, definuje vektory jako třídy ekvivalence relace $\cong$. Vektor obsahující $(a,b)\in G\times G$ označíme $\overrightarrow{ab}$.

5.5 Vlastnosti vektorového sčítání

Nyní zavedeme sčítaní vektorů (podle Volence, [13]) vzhledem k prvku $o\in G$ (zvanému počátek) pomocí $\overrightarrow{oa}+_o\overrightarrow{ob}:=\overrightarrow{oc}\Leftrightarrow \mathbf{P}(o,a,b,c)$. Volba počátku není podstatná, protože pro každý výběr dostáváme komutativní grupu $(G,0,+_o)$ izomorfní s $(\mathbf{T}_\mathbf{G},id_\mathrm{G},\circ)$, odpovídající izomorfismus je $G\to\mathbf{T}_\mathbf{G},\ q\mapsto\overrightarrow{oq}$. Následující vlastnosti se dají ověřit:

$$\overrightarrow{ab}+\overrightarrow{bc}=\overrightarrow{ac}\ \text{pro všechna}\ a,b,c\in G. \tag{5.30}$$

$$\mathbf{P}_\mathbf{G}(a,a,b,c)\Leftrightarrow b=c\ \text{pro}\ a,b,c\in G, \tag{5.31}$$

Pro všechna $a,b,c,d,e,f\in G$,

$$\mathbf{P}_\mathbf{G}(a,b,d,e),\ \mathbf{P}_\mathbf{G}(b,c,e,f)\Rightarrow\mathbf{P}_\mathbf{G}(c,d,f,a). \tag{5.32}$$

Pro všechna $a_1,b_1,c_1,d_1,a_2,b_2,c_2,d_2\in G$,

$$\mathbf{P}_\mathbf{G}(a_1,b_1,c_1,d_1),\ \mathbf{P}_\mathbf{G}(a_2,b_2,c_2,d_2)\Rightarrow\mathbf{P}_\mathbf{G}(a_1a_2,b_1b_2,c_1c_2,d_1d_2). \tag{5.33}$$

Pro všechna $a,b,c,d,q\in G$,

$$\mathbf{P}_\mathbf{G}(a,b,c,d)\Leftrightarrow\mathbf{P}_\mathbf{G}(qa,qb,qc,qd)\Leftrightarrow\mathbf{P}_\mathbf{G}(aq,bq,cq,dq). \tag{5.34}$$

Pro všechna $a,b,c,d\in G$, jestliže $\mathbf{P}_\mathbf{G}(a,b,c,d)$, pak $\mathbf{P}_\mathbf{G}(ab,bc,ca,db)$,

$$\mathbf{P}_\mathbf{G}(ac,bd,ca,db),\quad \mathbf{P}_\mathbf{G}(ad,ba,cb,dc),\mathbf{P}_\mathbf{G}(ad,bc,cb,da). \tag{5.35}$$

Pro všechna $a,b,c,d\in G$ platí $\mathbf{P}_\mathbf{G}(ab,ad,cd,cb)$. (5.36)

$\mathbf{P}_{\mathbf{G}}(q,(q/q)a,ba,bq)$ a $\mathbf{P}_{\mathbf{G}}(q,a(q\setminus q),ab,qb)$ platí pro všechna $a,b,q\in G$. (5.37)

Vektory můžeme brát jako polohové vektory bodů z G vzhledem k počátku $o\in G$ a přejdeme od polohového vektoru k jeho koncovému bodu. Pro každé $a,b\in G$ definujeme $a+_o b$ jako prvek z G jednoznačně určený pomocí $\mathbf{P}_{\mathbf{G}}(o,a,a+_o b,b)$. Dostáváme komutativní grupu, která je izomorfní s $(\mathbf{T}_{\mathbf{G}},id_{\mathrm{G}},\circ)$.

Lemma 5.5.1: Nechť $\mathbf{G}=(G,\cdot)$ je mediální kvazigrupa a prvky $o,a,b,c,d\in G$. Pak

$$\mathbf{P}_{\mathbf{G}}(a,b,c,d)\Leftrightarrow a+_o c=b+_o d\,.$$

Důkaz: Jestliže $\mathbf{P}_{\mathbf{G}}(a,b,c,d)$, $\mathbf{P}_{\mathbf{G}}(o,a,a+_o c,c)$, pak $\mathbf{P}_{\mathbf{G}}(b,a+_o c,d,o)$ (vlastnost 5.32), následně $\mathbf{P}_{\mathbf{G}}(b,o,d,a+_o c)$. Podobně z $\mathbf{P}_{\mathbf{G}}(o,b,b+_o d,d)$ dostáváme $\mathbf{P}_{\mathbf{G}}(b,o,d,b+_o d)$, tedy $a+_o c=b+_o d$. Naopak $a+_o c=b+_o d$ znamená, že $\mathbf{P}_{\mathbf{G}}(a,o,c,a+_o c)$ a zároveň $\mathbf{P}_{\mathbf{G}}(o,b,b+_o d,d)$. Odkud podle (5.32) $\mathbf{P}_{\mathbf{G}}(b,c,d,a)$ nebo ekvivalentně $\mathbf{P}_{\mathbf{G}}(a,b,c,d)$.

Lemma 5.5.2: Nechť ($\mathbf{G}$,o) je mediální kvazigrupa s pevným bodem *o*, $\mathbf{G}=(G,\cdot)$. Pak zobrazení $L_{o/o}$ a $R_{o\setminus o}$ jsou automorfismy grupy $(G,+_o)$, které komutují, $L_{o/o}\circ R_{o\setminus o}=R_{o\setminus o}\circ L_{o/o}$.

Důkaz: Nechť $q\in G$. Položme $l_o=o/o$ a $r_o=o\setminus o$. Nyní postupně dostáváme $(l_o\cdot(qr_o)\cdot(o\cdot o)=(l_o o)((qr_o)\cdot o)=o((qr_o)\cdot o)=(or_o)\cdot((qr_o)\cdot o)=(o\cdot(qr_o))\cdot(r_o\cdot o)=((l_o o)(qr_o))\cdot(r_o o)=((l_o q)(or_o))\cdot(r_o o)=((l_o q)\cdot r_o)\cdot(o\cdot o)$. Pomocí pravého krácení: $l_o\cdot(q\cdot r_o)=(l_o q)\cdot r_o$, což znamená $L_{l_o}\circ R_{r_o}=R_{r_o}\circ L_{l_o}$. K tomu, abychom dokázali, že zobrazení jsou izomorfní, použijeme vlastnost (5.34): $\mathbf{P}_{\mathbf{G}}(o,a,a+_o b,b)$ je ekvivalentní (použitím $l_o o=o$) s $\mathbf{P}_{\mathbf{G}}(o,l_o a,l_o(a+_o b),l_o b)$, to můžeme zapsat jako $l_o(a+_o b)=l_o a+_o l_o b$. Tedy $L_{l_o}(a+_o b)=L_{l_o}(a)+_o L_{l_o}(b)$ pro všechna $a,b\in G$. Podobně pro všechna $a,b\in G$ platí $R_{r_o}(a+_o b)=R_{r_o}(a)+_o R_{r_o}(b)$.

Nyní jsme připraveni specializovat obecnou verzi Toyodovy věty:
Nechť $\mathbf{G}=(G,\cdot)$ je mediální kvazigrupa a $o\in G$. Pak pro všechna $a,b\in G$ platí rovnosti

$a \cdot b = a(o \setminus o) +_o b(o / o) +_o (o \cdot o)$.

Důkaz: Binární operace $+_o$ byla zavedena před lemmatem 5.5.1. Podle vlastnosti (5.37) máme $\mathbf{P_G}(o, ar_o, ab, ob)$ a $\mathbf{P_G}(o, l_o b, ob, o \cdot o)$ (kde jsme opět označili $l_o = o / o$ a $r_o = o \setminus o$), a tedy (podle definice sčítání $+_o$ na G) $a \cdot b = a \cdot r_o +_o o \cdot b$, $o \cdot b = l_o \cdot b +_o o \cdot o$, následně $a \cdot b = a \cdot r_o +_o l_o \cdot b +_o o \cdot o$. Platí $a \cdot b = R_{o\setminus o}(a) +_o L_{o/o}(b) +_o o \cdot o$ („Toyodova věta“).

5.6 Rovnoběžníky a lichoběžníky v GS-kvazigrupách

Začněme s přehledem těch vlastností GS-kvazigrup, které budou užitečné v následujících úvahách.

Mějme GS-kvazigrupu $(G, \cdot)$, následující identity platí pro všechna $a, b, c, d \in G$:

$(a((ab)c))c = b$,	první GS identita,	(5.38)
$a((a(bc))c) = b$,	druhá GS identita,	(5.39)
$aa = a$,	idempotentnost,	(5.40)
$(ab)(cd) = (ac)(bd)$,	medialita,	(5.41)
$a(ba) = (ab)a$,	elasticita,	(5.42)
$a(bc) = (ab)(ac)$,	levá distributivita,	(5.43)
$(ab)c = (ac)(bc)$,	pravá distributivita,	(5.44)
$a((ab)b) = b$,		(5.45)
$(b(ba))a = b$,	GS-identity dvou proměnných,	(5.46)
$a((ab)c) = b \cdot bc$		(5.47)
$(c(ba))a = cb \cdot b$,	zkrácené GS-identity,	(5.48)

další alternativní rovnosti pro násobení:

$$ab = c \Leftrightarrow a = c(cb), \tag{5.49}$$

$$ab = c \Leftrightarrow b = (ac)c, \tag{5.50}$$

dvě z následujících rovností implikují zbývající

$$ab = c,\ dc = b,\ ab = c,\ db = a, \tag{5.51}$$

a rovnosti pro duální operaci „$\circ^{op}$“ (danou na G vztahem $a \circ^{op} b := ba$ pro $a, b \in G$):

$$(42) \Leftrightarrow (42_{\circ^{op}}),\ (43) \Leftrightarrow (43_{\circ^{op}}),\ (44) \Leftrightarrow (44_{\circ^{op}}). \tag{5.52}$$

5.6.1 Rovnoběžníky v GS-kvazigrupách

Z podkapitoly 5.4 víme, že rovnoběžník v mediální kvazigrupě $(G,\cdot)$ můžeme definovat jako čtveřici $(a,b,c,d)\in G\times G\times G\times G$ takovou, že existuje transfer na G, který zobrazí a do b a d do c.

Prvky $a,b,c,d\in G$, které tvoří rovnoběžník, nazýváme *vrcholy* rovnoběžníku $(a,b,c,d)\in \mathbf{P}$.

Alternativně, jestliže platí $\mathbf{P}(a,b,c,d)$, pak existují $p,q\in G$ tak, že $ap=bq$ a $dp=cq$. Tedy v GS-kvazigrupě můžeme definovat rovnoběžník následovně:

Definice 5.6.1.1: Nechť $(G,\cdot)$ je GS-kvazigrupa a $a,b,c\in G$. Prvky *a, b, c* tvoří rovnoběžník právě tehdy, když platí $\mathbf{P}(a,b,c,a\cdot(b(ca\cdot b)))$.

Podle 1ˇ z definice 5.2.2 můžeme konstatovat:

Pro všechna $a,b,c,d\in G$, $\mathbf{P}(a,b,c,d)\Leftrightarrow d=a\cdot b(ca\cdot a)$.

Dokážeme, že pro $p=ab\cdot b$ a $q=b$ platí obě následující rovnosti: $ap=bq$ a $a(b(ca\cdot a))\cdot p=cp$. Pokračujme takto: $a(ab\cdot b)=b=bb$ (pomocí (5.45) a idempotentnosti),

$$a(b(ca\cdot a)))(ab\cdot b)\overset{5.39}{=}(a\cdot ab)((b(ca\cdot a))b)\overset{5.42}{=}(a\cdot ab)(b((ca\cdot c)b))\overset{5.39}{=}$$

$$(ab)\cdot(ab)((ca\cdot a)b)=(a((a(ca\cdot a))))b\overset{5.42}{=}(a((a\cdot ca)a))b\overset{5.35}{=}cb.$$

Nyní dokážeme přímo, že v GS-kvazigrupě čtveřice relací **P** na *G* definovaná jako: $\mathbf{P}(a,b,c,d)\Leftrightarrow d=a\cdot(b(ca\cdot a)$ splňuje vlastnosti 1ˇ, 2ˇ, 3ˇ. Opravdu, 1ˇ je splněna přímo z definice **P**. Pro 2ˇ stačí dokázat $\mathbf{P}(b,c,d,a)$ a $\mathbf{P}(c,b,a,d)$ z $\mathbf{P}(a,b,c,d)$, tj. $b(c(db\cdot b))=a$ a $c(b(ac\cdot c))=d$ z $d=a(b(ca\cdot a))$.

Tedy:

$$b(b(c(db\cdot b)))\overset{5.43}{=}b\cdot(bc)(b(db\cdot b))\overset{5.42}{=}b\cdot(bc)((b\cdot bd)b)\overset{5.48}{=}b((bc)(bd\cdot d))\overset{5.44}{=}$$

$$(b\cdot bc)(b(bd\cdot d))\overset{5.45}{=}(b\cdot bc)d=(b\cdot bc)(a(b(ca\cdot a)))\overset{5.41}{=}ba\cdot((bc)((b(ca\cdot a))))\overset{5.43}{=}$$

$$b(a(c(ca\cdot a)))\overset{5.43}{=}b\cdot aa=ba.$$

Z toho dostáváme $b(c(db\cdot b))=a$. Tudíž

$$c(b(ac\cdot c))\overset{5.43}{=}cb\cdot(c(ac\cdot c))\overset{5.42}{=}cb\cdot((c\cdot ac)c)\overset{5.44}{=}c((c\cdot ac)c)\cdot b((c\cdot ac)c)\overset{5.39}{=}$$

$$a\cdot b((c\cdot ac)c)\overset{5.48}{=}a(b(ca\cdot a))=d.$$

Zbývá potvrdit platnost 3ˇ. Budeme předpokládat, že pro $a,b,c,d,e,f \in G$ platí $\mathbf{P}(a,b,c,d)$ a $\mathbf{P}(c,d,e,f)$, to lze vyjádřit jako $a(b(ca\cdot a))=d$ a $c(d(ec\cdot c))=f$.

Takže:

$$f=c\cdot d(ec\cdot c)\overset{5.43}{=}cd\cdot c(ec\cdot c)\overset{5.42}{=}cd\cdot(c\cdot ce)c\overset{5.48}{=}cd\cdot(ce\cdot e)\overset{5.41}{=}(c\cdot ce)\cdot de\overset{5.47}{=}$$

$$e(ec\cdot ed)\cdot ec\overset{5.42}{=}(e\cdot ec)\cdot de\overset{5.44}{=}((e\cdot ec)d)e=(e\cdot ec)\cdot(a(b(ca\cdot a)))e\overset{5.41}{=}$$

$$(ea\cdot(ec)(b(ca\cdot a)))e\overset{5.41}{=}(ea\cdot(eb)(c(ca\cdot a)))e\overset{5.45}{=}(ea\cdot(eb)a)e\overset{5.44}{=}((e\cdot eb)a)e\overset{5.44}{=}$$

$$((e\cdot eb)e)\cdot ae\overset{5.42}{=}(e(eb\cdot e))\cdot ae\overset{5.47}{=}(b\cdot be)\cdot ae\overset{5.41}{=}ba\cdot(be\cdot e)\overset{5.44}{=}$$

$$(b(be\cdot e))(a(be\cdot e))\overset{5.45}{=}e(a(be\cdot e)).$$

Ale $f=e(a(be\cdot e))$ můžeme zapsat také takto $\mathbf{P}(e,a,b,f)$, následně dostáváme $\mathbf{P}(a,b,f,e)$ z 2ˇ.

Vlastnosti mediálních kvazigrup (5.30) až (5.37) uvedené v podkapitole 5.5 jsou samozřejmě platné i pro GS-kvazigrupy. Důkazy vlastností odvozených přímo pro GS-kvazigrupy jsou často jednodušší než v obecném případě. Jako příklad uveďme $\mathbf{P}(ab,cb,cd,ab)$ pro všechna $a,b,c,d\in G$. Následující tvrzení dokážeme užitím příslušných vlastností GS-kvazigrup.

Lemma 5.6.1.1: Nechť $\mathbf{G}=(G,\cdot)$ je GS-kvazigrupa. Jestliže $a,b,c\in G$ a $d=ac$, $e=ab$, $f=ec$, $g=df$, pak platí tvrzení $\mathbf{P}(a,b,d,f)$, $\mathbf{P}(b,e,f,g)$ a $\mathbf{P}(a,e,d,g)$.

Důkaz: Díky tomu, že $f=ec=(ab)c$ a $g=df=(ac)(ab\cdot c)\overset{5.44}{=}(a\cdot ab)c$ máme ověřenu platnost $\mathbf{P}(a,b,ac,(ab)c)$, $\mathbf{P}(b,ab,(ab)c,(a(ab))c)$ a $\mathbf{P}(a,ab,ac,(a(ab))c)$. Postupně dostáváme $a(b((a\cdot ca)a))\overset{5.43}{=}ab\cdot a((a\cdot ca)a)\overset{5.38}{=}ab\cdot c$,

$$b(ab\cdot((ab\cdot c)b)b\overset{5.43}{=}b((ab\cdot((ab)c)b)(ab\cdot b))\overset{5.47,5.43}{=}(b(c\cdot cb))(b(ab\cdot b))\overset{5.42}{=}(b(c\cdot cb))\cdot((b\cdot ab)b)\overset{5.42}{=}$$

$$(b(c\cdot bc))((b\cdot ab)b)\overset{5.41}{=}(b(b\cdot ab))((c\cdot cb)b)\overset{5.46}{=}(b(b\cdot ab))c\overset{5.42}{=}(b(ba\cdot b)c\overset{5.47}{=}(a\cdot ab)c,$$

$$a(ab\cdot((ac)a)a)\overset{5.42}{=}a(ab\cdot(a\cdot ca)a)\overset{5.48}{=}a(ab\cdot(ac\cdot c))\overset{5.43}{=}(a\cdot ab)(a(ac\cdot c))\overset{5.45}{=}(a\cdot ab)c.$$

Pro speciální volbu bodů $c = e = ab$ jsou splněny dvě z rovností (5.51), jmenovitě $ab = c$ a $ac = d$. Navíc díky idempotentnosti $f = ec = cc = c$ tak, že z $\mathbf{P}(a,b,d,f)$ dostáváme $\mathbf{P}(a,b,c,d)$.

Jako důsledek dostáváme:

Poznámka 5.6.1.1: Pro všechna $a,b \in G$ platí $\mathbf{P}(a,b,a(ab),ab)$.

5.6.2 GS-lichoběžníky

Definice 5.6.2.1: Čtveřici $a,b,c,d \in G$ nazveme GS-lichoběžníkem v $\mathbf{G}$, jestliže platí rovnost $a \cdot ab = d \cdot dc$. Budeme používat značení $GST(a,b,c,d)$ a odpovídající kvaternární relaci označíme *GST*. Prvky a,b,c,d budeme opět nazývat *vrcholy* GS-lichoběžníku.

Lemma 5.6.2.1: V GS-kvazigrupě $(G,\cdot)$ pro všechna $a,b,c,d \in G$, $GST(a,b,c,d)$ implikuje $GST(d,c,b,a)$.

Důkaz: Provedeme přímo z definice GS-lichoběžníku.

V GS-kvazigrupě mohou být kromě lichoběžníků zlatého řezu zavedeny také doprovodné GS-lichoběžníky druhého druhu.

Definice 5.6.2.1: *GS-lichoběžníkem druhého druhu* rozumíme čtveřici c,a,d,b splňující $GST(a,b,c,d)$. Zapisujeme $\overline{GST}(c,a,d,b)$.

To je: $\overline{GST}(c,a,d,b)$ platí právě tehdy, když $GST(a,b,c,d)$.

Podle lemmatu 5.6.2.1, $\overline{GST}(a,b,c,d)$ platí, právě když platí $GST(c,a,d,b)$.

Tedy permutace

$$\Pi = \begin{pmatrix} a & b & c & d \\ c & a & d & b \end{pmatrix} \tag{5.53}$$

vzájemně převádí relace *GST* a $\overline{GST}$.

Lemma 5.6.2.2: Nechť $(G,\cdot)$ je GS-kvazigrupa a nechť a,b,c,d jsou prvky *G*. Pak platí: $\overline{GST}(a,b,c,d)$ právě tehdy , když $ba\cdot a = cd\cdot d$.

Důkaz: Postupujeme následovně:

$d \overset{5.38}{=} c\cdot((c\cdot da)a) \overset{5.46}{=} c(((c\cdot ca)a)\cdot(da)a) \overset{5.44}{=} c((((c\cdot ca)d)a)a)$, z čehož plyne ekvivalence mezi $b=(c\cdot ca)d$ a $d=c(ba\cdot a)$. Dále z (5.49):

$b=(c\cdot ca)d \Leftrightarrow c\cdot ca = b\cdot bd \Leftrightarrow GST(c,a,d,b) \Leftrightarrow GST(b,d,a,c) \Leftrightarrow \overline{GST}(a,b,c,d)$. Podobně z (5.50), $d=c(ba\cdot a)$ právě tehdy, když $ba\cdot a = cd\cdot d$.

Přechodem ke kvazigrupě duální k $(G,\cdot)$ obdržíme výsledek týkající se duality lichoběžníků:

Ke každé větě o GS-lichoběžnících v GS-kvazigrupách existuje odpovídající duální věta o GS-lichoběžnících druhého druhu, (a naopak) pokud se ve všech uvedených binárních součinech ve větách zamění úlohy činitelů odpovídajícím způsobem.

Poznámka 5.6.2.1: Z každé věty o GS-lichoběžnících dostáváme opět větu o GS-lichoběžnících, jestliže každý výrok ve tvaru $GST(a,b,c,d)$ vyměníme za odpovídající výrok $GST(c,a,d,b)$. Role činitelů se vymění ve všech součinech. Poznamenejme, že relace $\mathbf{P}(a,b,c,d)$ platí v průběhu popisovaných změn, což je důsledkem ekvivalence

$d=a(b((ca)a)) \Leftrightarrow d=((a(ac))b)a$.

Opravdu:

$a(b(ca\cdot a)) \overset{5.43}{=} ab\cdot(a(ca\cdot a)) \overset{5.42}{=} ab\cdot((a\cdot ca)a) \overset{5.48}{=} ba(ac\cdot c) \overset{5.41}{=} (a\cdot ac)\cdot bc \overset{5.43}{=} (a\cdot ac)b\cdot(a\cdot ac)c \overset{5.46}{=} ((a\cdot ac)b)a$.

Lemma 5.6.2.3: V GS-kvazigrupě $(G,\cdot)$ platí $GST(a,b,c,d)$, právě když je rovnost $ac\cdot c = db\cdot b$ splněna pro všechna $a,b,c,d\in G$.

Důkaz: Stačí aplikovat výše uvedenou permutaci, (5.53), na ekvivalence:

$GST(b,d,a,c) \Leftrightarrow \overline{GST}(a,b,c,d) \quad \Leftrightarrow (ba)a=(cd)d$.

Lemma 5.6.2.4: V GS-kvazigrupě platí pro všechna $a,b,c,d\in G$ ekvivalence:

$$GST(a,b,c,d) \Leftrightarrow a = (d \cdot dc)b \Leftrightarrow b = (ac \cdot c) \Leftrightarrow c = a(db \cdot b) \Leftrightarrow d = (a \cdot ab)c .$$

Důkaz: Podle (5.53), $a \cdot ab = d \cdot dc$ je ekvivalentní s $(a \cdot ab)c = d$ a také s $(d \cdot dc)b = a$. Podobně z (5.50): rovnost $ac \cdot c = db \cdot b$ je ekvivalentní s rovnostmi $c = a(db \cdot b)$ a $b = d(ac \cdot c)$. V důsledku toho dostáváme výše vyslovené ekvivalence.

Poznámka 5.6.2.2: GS-lichoběžník je v $\mathbf{G}$ jednoznačně určen třemi svými vrcholy.

Lemma 5.6.2.5: Nechť $(G,\cdot)$ je GS-kvazigrupa. Pak pro všechna $a,b,c,d \in G$ jsou následující tři podmínky ekvivalentní:

$GST(a,b,c,d)$,

existuje prvek $e \in G$, který splňuje $eb = a, ec = d$,

existuje bod $f \in G$, který splňuje $af = c = df = b$.

Důkaz: Podle (5.49), $eb = a \Leftrightarrow e = a(ab)$ a také $ec = d \Leftrightarrow e = d(dc)$. Odtud: $GST(a,b,c,d) \Leftrightarrow a(ab) = d(dc)$, odtud vyplývá první část. Druhá část vyplývá z první pomocí duální záměny $\begin{pmatrix} a & b & c & d & e \\ b & d & a & c & f \end{pmatrix}$.

Lemma 5.6.2.6: Nechť $(G,\cdot)$ je GS-kvazigrupa. Pro všechna $a,b,c,d \in G$ jsou následující tři podmínky ekvivalentní:

$GST(a,b,c,d)$,

$(xa)b = (xd)c$ je splněno pro každé $x \in G$,

$a(cx) = d(bx)$ je splněno pro každé $x \in G$.

Důkaz: Mějme $a,b,x \in G$, vypočtěme

$$(xa)b \overset{5.45}{=} xa \cdot (a(ab \cdot b)) \overset{5.43}{=} xa \cdot ((a \cdot ab) \cdot ab) \overset{5.41}{=} (x(a \cdot ab)) \cdot (a \cdot ab) \overset{5.48}{=} (x((a \cdot ab)c))c)$$

takže $xa \cdot b = xd \cdot c$ právě tehdy, když $d = (a \cdot ab)c$, to je podle lemmatu 5.6.2.4 ekvivalentní s $GST(a,b,c,d)$.

Speciálně: Kvaternární relace *GST* na *G* má následující jednoduché vlastnosti:

Lemma 5.6.2.7: V GS-kvazigrupě pro všechna $a,b,c \in G$ platí $GST(ab,b,c,ac)$ a $GST(b,ca,ba,c)$.

Důkaz: Označme $d := ab$, $e := ac$. Z (5.49) vyplývá, že $a = d(db) = e(ec)$. Dostáváme tvrzení $GST(d,b,c,e)$. tj. $GST(ab,b,c,ac)$.

Důsledek 5.6.2.3: Pro všechna $a,b \in G$ platí následující:

$GST(a,b,b,a)$, $GST(a,a,b,ab)$, $GST(a,ba,a,b)$.

Důkaz: Je dáno $a,b \in G$, označme $c := a/b$. Pak $GST(a,b,b,a)$ je důsledkem $GST(cb,b,b,cb)$. Pro zbytek využijeme skutečnosti, že podle lemmatu 5.6.2.7 platí $GST(ac,c,b,ab)$ a $GST(c,ba,ca,b)$. Nyní stačí položit $a = c$ a aplikovat idempotentnost.

Lemma 5.6.2.8: V GS-kvazigrupě $(G,\cdot)$ jsou pro všechna $a,b,c \in G$ splněna následující tvrzení $GST(b,(ab)b,(ac)c,c)$ a $GST(b(ba),c,b,c(ca))$.

Důkaz: Mějme $a,b,c \in G$, počítejme

$b(b(ab\cdot b)) \overset{5.42}{=} b((b\cdot ab)b) \overset{5.39}{=} a \overset{5.39}{=} c((c\cdot ac)c) \overset{5.42}{=} c(c(ac\cdot c))$, tím jsme ověřili první tvrzení. Druhé vyplývá z duální záměny.

Lemma 5.6.2.9: Jestliže $(G,\cdot)$ je GS-kvazigrupa a $a,b,c \in G$, pak platí

$GST(a(ab),c(ca),b(ba),a(ac))$ a $GST((ab)b,(ba)a,(ca)a,(ac)c)$.

Důkaz: Dokážeme pouze první tvrzení (druhé by se dokazovalo pomocí duální výměny):
pro všechna $a,b,c \in G$,

$((a\cdot ab)\cdot((a\cdot ab)(c\cdot ca)))\cdot(b\cdot ba) \overset{5.41}{=} ((a\cdot ab)b)\cdot(((a\cdot ab)(c\cdot ca))\cdot ba) \overset{5.41}{=}$

$((a\cdot ab)b)\cdot(((a\cdot ab)b)((c\cdot ca)a)) \overset{5.47}{=} a\cdot ac$.

Lemma 5.6.2.10: Jestliže $(G,\cdot)$ je GS-kvazigrupa a $a,b,c,d \in G$, pak

$GST(a,b,c,d) \Rightarrow GST(c,d,ad,b(bc))$.

Důkaz: Za předpokladu $d = (a(ab))c$ (což je ekvivalentní s $GST(a,b,c,d)$), dostáváme: $(c \cdot cd) \cdot ad \overset{5.41}{=} ca \cdot (cd \cdot d) = ca \cdot (c \cdot ((a \cdot ab)c) \cdot (a \cdot ab)c) \overset{5.42}{=} ca \cdot (c(a \cdot ab) \cdot c) \cdot ((a \cdot ab)c) \overset{5.44}{=} ca \cdot (c(a \cdot ab) \cdot (a \cdot ab))c \overset{5.41}{=} c(c(a \cdot ab) \cdot (a \cdot ab)) \cdot ac \overset{5.45}{=} (a \cdot ab) \cdot ac \overset{5.43}{=} a(ab \cdot c) \overset{5.47}{=} b(bc)$, tedy platí $GST(c,d,ad,b(bc))$.

Lemma 5.6.2.11: Nechť $(G,\cdot)$ je GS-kvazigrupa, $n > 1$ je celé číslo a nechť $a_1, b_1 \ldots a_n, b_n$ jsou prvky *G*. Jestliže $GST(a_i, b_i, b_{i+1}, a_{i+1})$ platí pro všechna $i \in \{1, \cdots, n-1\}$, pak také platí $GST(a_n, b_n, b_1, a_1)$.

„Duálně“, jestliže $GST(b_{i+1}, a_i, a_{i+1}, b_i)$ je splněno pro všechna $i \in \{1, \cdots, n-1\}$, pak platí i $GST(b_1, a_n, a_1 b_n)$.

Důkaz: První část vyplývá z $a_1(a_1 b_1) = a_2(a_2 b_2) = \ldots = a_n(a_n b_n)$. Druhá část se dokazuje užitím duality.

V GS-kvazigrupě $(G,\cdot)$ platí následující implikace pro všechna $a,b,c,d,a',b',c',d' \in G$:
jestliže platí $GST(a,b,c,d)$ a $GST(a,b,c',d')$, pak platí $GST(d,c,c',d')$,
jestliže platí $GST(a,b,c,d)$ a $GST(a,b',c,d')$, pak platí $GST(d,b',b,d')$.
Dvojice připomíná něco jako „perspektivní Desargueskou pozici dvojice „trojúhelníků“ s vlastním středem a nevlastní osou.

Lemma 5.6.2.12: Pro libovolný výběr bodů $a,b,c,d,e \in G$ v GS-kvazigrupě $(G,\cdot)$, implikují dvě z následujících tvrzení $GST(a,b,c,d)$, $GST(b,c,d,e)$, $GST(c,d,e,a)$ to třetí.
Poznamenejme, že tvrzení $GST(c,d,e,a)$ můžeme nahradit tvrzením $GST(d,e,a,b)$, tedy závěr lemmatu 5.6.2.12 platí.

Důkaz: Ověřme, že tvrzení $GST(b,c,d,e)$ a $GST(c,d,e,a)$ jsou ekvivalentní za předpokladu $GST(a,b,c,d)$. Pro zbytek můžeme využít duality vztahů za výměny $(b,e) \to (e,b)$,

$(c,d) \to (d,c)$. Předpokládejme, že $d = (a(ab))c$ a ověřme platnost ekvivalence $e = (b(bc))d \Leftrightarrow (c(cd))e = a$. Doopravdy:

$$(c \cdot cd)((b \cdot bc)d) = (c[c \cdot (a \cdot ab)c]) \cdot [(b \cdot bc) \cdot (a \cdot ab)c)] \overset{5.42}{=} (c((c(a \cdot ab))c))((b \cdot bc)((a \cdot ab)c)) \overset{5.47}{=}$$

$$(((a \cdot ab)((a \cdot ab)c)) \cdot ((b \cdot bc)((a \cdot ab)c)) \overset{5.44}{=} ((a \cdot ab)(b \cdot bc))((a \cdot ab)c) \overset{5.43}{=} (a \cdot ab)((b \cdot bc)c) \overset{5.46}{=}$$

$$(a \cdot ab)b \overset{5.46}{=} a.$$

Lemma 5.6.2.13: V GS-kvazigrupě $(G,\cdot)$, pro všechna $a,b,c,d,e,b',c',d' \in G$, tři ze čtyř následujících tvrzení $GST(a,b,c,d)$, $GST(a,b',c',d)$, $GST(b,a,b',e)$, $GST(c,d,c',e)$ implikují to zbývající. „Duálně“, ze tří z následujících tvrzení $GST(a,b,c,d)$, $GST(a',b,c,d')$, $GST(a',a,e,c)$, $GST(d,d',e,b)$ vyplývá to čtvrté.

Důkaz: Stačí dokázat polovinu případů. Opravdu, použitím permutace $(a,d) \to (d,a)$, $(b,c) \to (c,b)$, $(b',c') \to (c',d')$ můžeme zkontrolovat, že tvrzení $GST(b,a,b',e)$ a $GST(c,d,c',e)$ jsou zaměnitelná, zatímco zbývající tvrzení jsou převedena do ekvivalentního tvrzení (Lemma 5.6.2.1). Předpokládejme, že platí $GST(b,a,b',e)$, tj. $e = (b \cdot ba)b'$. Z tohoto předpokladu máme dokázat, že dvě z tvrzení $GST(a,b,c,d)$, $GST(a,b',c',d)$, $GST(c,d,c',e)$ implikují to zbývající. Můžeme dokázat, že dvě z rovností

$$d(ac \cdot c) = b, \tag{5.54}$$

$$d(ac' \cdot c') = b', \tag{5.55}$$

$$(c \cdot cd)c' = e, \tag{5.56}$$

implikují tu zbývající. Argumenty jsou následující:

$$((d(ac \cdot c)((d(ac \cdot c))a)) \cdot (d((ac' \cdot c'))) \overset{5.41}{=} (d \cdot d(ac \cdot c))((ac \cdot c)a) \cdot d(ac' \cdot c') \overset{5.41}{=}$$

$$(d \cdot d(ac \cdot c))d \cdot ((ac \cdot c)a \cdot (ac' \cdot c') \overset{5.41}{=} (d \cdot d(ac \cdot c))d \cdot ((ac \cdot c)(ac') \cdot ac') \overset{5.41}{=}$$

$$(d \cdot d(ac \cdot c))d \cdot ((ac \cdot a)(cc') \cdot ac') \overset{5.41}{=} (d \cdot d(ac \cdot c))d \cdot ((ac \cdot a)a \cdot (cc' \cdot c') \overset{5.42}{=}$$

$$d(d((ac)c) \cdot d) \cdot ((a(ca))a \cdot (cc' \cdot c')) \overset{5.47,5.48}{=} ((ac \cdot c) \cdot ((ac \cdot c))d) \cdot ((ac \cdot c)(cc' \cdot c') \overset{5.43}{=}$$

$$(ac \cdot c)((ac \cdot c)d \cdot (cc' \cdot c')) \overset{5.47}{=} d \cdot d(cc' \cdot c') \overset{5.44}{=} d \cdot (d \cdot cc')(dc') \overset{5.48}{=} cc' \cdot (cc' \cdot dc') \overset{5.44}{=} (c \cdot cd)c'.$$

Implikace (5.54), (5.55) $\Rightarrow$ (5.56) a (5.54), (5.56) $\Rightarrow$ (5.55) jsou zřejmé. Jestliže jsou splněny (5.54) a (5.55), pak platí $e = (b \cdot ba)b' = (c \cdot cd)c'$, a (5.56) platí; podobně ostatní implikace.

Nyní začněme s dvojicí rovností (5.55), (5.56). Výše uvedené výpočty poskytují $(d((ac \cdot c))((d(ac \cdot c) \cdot a) \cdot b' = e = (b \cdot ba)b'$. Po zkrácení zprava prvkem b' dostaneme: $(d((ac \cdot c))((d(ac \cdot c) \cdot a) = (b \cdot ba)$. Vynásobením rovnice prvkem *a* zprava a použitím (5.51) dostaneme vztah (5.56).

Literatura

[1] A. G. KUROŠ: Kapitoly z obecné algebry. Praha: Academia, 1968.

[2] V. VOLENEC: GS-quasigroups. Časopis pro pěstování matematiky. 115(1990), No. 3, 307–308.

[3] V. J. HAVEL, A. VANŽUROVÁ: Medial Quasigroups and Geometry. Olomouc: Univerzita Palackého, 2006.

[4] J. BOSÁK: Latinské štvorce. Praha: Mladá Fronta, 1976.

[5] AIGNER, M., ZIEGLER, G. M. Proofs from the book. Berlin, Heidelberg, New York: Springer–Verlag, 2004.

[6] L. BERAN, L. BICAN: Vademekum z obecné algebry. Praha: SPN, 1982.

[7] R. LIDL, H. NIEDERREITER: Introduction to finite fields and their application. Cambridge University Press, 1986.

[8] VANŽUROVÁ, A.: Algebraic systems in cryptography and the security information. Proc. International conference on military technologies 2011, str. 525-532.

[9] VANŽUROVÁ, A., DOLEŽALOVÁ, J.: Hexagonal quasigroups. Proc. 7th Conference on Mathematics and Physics on Technical Universities Brno, 2011.

[10] VANŽUROVÁ, A.: Golden section quasigroups. Aplimat 2011.
Proc. 10th International Conference, February 1-4, 2011, Fac. of Mechanical Engineering, Slovak University of Technology in Bratislava (2011), str.183-190.

[11] KOŘÍNEK,V., Základy algebry, NČAV Praha, 1956, 430-434.

[12] BARTOŠKOVÁ, Z. Komutativní grupy a mediální kvazigrupy. Olomouc, 2009. 29 s. Vedoucí bakalářské práce Doc. RNDr. Alena Vanžurová, CSc.

[13] V. VOLENEC: Geometry of medial quasigroups. Rad. Jugosl. Akad. Umjet 421 (1986), 70–91.