Simetrični stožci v evklidskih prostorih

Znanstvene monografije
Fakultete za management Koper

ISSN 1855-0878

Simetrični stožci v evklidskih prostorih

Rok Strašek

Management

Simetrični stožci
v evklidskih prostorih
izr. prof. dr. Rok Strašek

Strokovni recenzenti · prof. dr. Borut Zalar,
izr. prof. dr. Maja Fošner in doc. dr. Ajda Fošner
Izdala in založila · Univerza na Primorskem,
Fakulteta za management Koper,
Cankarjeva 5, 6104 Koper
Oblikovanje in tehnična
ureditev · Alen Ježovnik
Oktober 2010

Monografija je izšla s finančno podporo
Javne agencije za knjigo Republike Slovenije

CIP – KatEložni zapis o publikaciji
Narodna in univerzitetna knjižnica, Ljubljana

514.17:512.646.33

STRAŠEK, Rok
Simetrični stožci v evklidskih prostorih [Elektronski vir] /
Rok Strašek. – El. knjiga. – Koper : Fakulteta za management, 2010. –
(Znanstvene monografije Fakultete za management, ISSN 1855-0878)

Način dostopa (URL): http://www.fm-kp.si/
zalozba/ISBN/978-961-266-074-1.pdf

ISBN 978-961-266-074-1
COBISS.SI-ID 252744704

Kazalo

1 Uvod

1.1 Pojem stožca

V obravnavi mnogih fizikalnih, inženirskih in matematičnih problemov se poleg gladkih struktur pojavljajo tudi strukture z robovi, vogali, klini in podobnimi negladkimi lastnostmi. Smiselen model za obravnavo takih mnogoterosti predstavljajo stožci v $\mathbb{R}^n$. *Stožec* $\mathcal{P}$, kot podmnožico prostora $\mathbb{R}^n$, definiramo kot množico, ki izpolnjuje pogoj: produkt elementa stožca s pozitivnim številom iz obsega realnih števil je element stožca. Simbolno pogoj zapišemo

$$\mathbb{R}^+\mathcal{P} \subset \mathcal{P}\,.$$

Stožcu $\mathcal{P}$, ki zadošča pogoju: vsota elementov iz stožca je element stožca, pravimo *konveksen stožec*. Očitno je omenjena definicija konveksnosti v skladu z običajno definicijo konveksnosti. Simbolno pogoj konveksnosti zapišemo

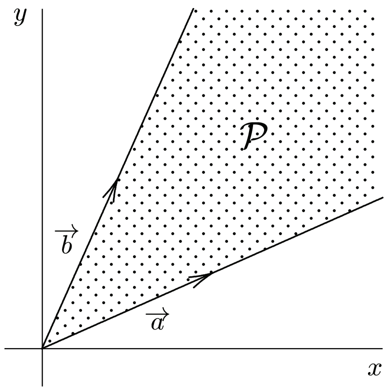
$$\mathcal{P} + \mathcal{P} \subseteq \mathcal{P}\,.$$

Stožcu, ki zadošča le pogoju $\mathbb{R}^+\mathcal{P} \subset \mathcal{P}$ pravimo *nekonveksen stožec*.

Zgled 1. V $\mathbb{R}$ sta množici $\mathcal{P} = (0, \infty)$ in $\mathcal{P} = [0, \infty)$ očitno konveksna stožca. Prvega imenujemo *odprti*, drugega pa *zaprti* konveksni stožec.

Zgled 2. V $\mathbb{R}^2$ sta množici $\mathcal{P} = \{\,(x, y); x, y > 0\,\}$ in $\mathcal{P} = \{\,(x, y); x, y \geq 0\,\}$ konveksna stožca. Omenjena stožca lahko zapišemo kot kartezični produkt stožcev prejšnjega zgleda oziroma v obliki $(0, \infty) \times (0, \infty)$ ter $[0, \infty) \times [0, \infty)$.

Stožec, ki ga lahko zapišemo kot produkt stožcev nižje dimenzije, imenujemo *reducibilni* stožec. Sicer stožcu pravimo, da je *ireducibilen*. V zgledu 2 smo se prepričali v obstoj reducibilnih konveksnih stožcev. V prostoru $\mathbb{R}^2$ pa obstajajo tudi ireducibilni konveksni stožci:



Stožec $\mathcal{P} = \{\, \alpha \overrightarrow{a} + \beta \overrightarrow{b}\,;\, \alpha,\, \beta \geq 0 \,\}$

Zgled 3. V prvem kvadrantu izberimo vektorja $\overrightarrow{a} = (x_1, y_1)$ in $\overrightarrow{b} = (x_2, y_2)$ ter pokažimo, da množica podana s predpisom $\mathcal{P} = \{\, \alpha \overrightarrow{a} + \beta \overrightarrow{b}\,;\, \alpha,\, \beta \geq 0 \,\}$ predstavlja stožec v $\mathbb{R}^2$. Pokazati zadošča zaprtost množice $\mathcal{P}$ za množenje z nenegativnim skalarjem. Naj bo $\overrightarrow{c} \in \mathcal{P}$ in $\gamma \geq 0$. Ker je

$$\overrightarrow{c} = \alpha \overrightarrow{a} + \beta \overrightarrow{b}\,, \alpha, \beta \geq 0\,,$$

sledi

$$\gamma \overrightarrow{c} = \gamma \,(\, \alpha \overrightarrow{a} + \beta \overrightarrow{b}\,) = \gamma\, \alpha \overrightarrow{a} + \gamma\, \beta \overrightarrow{b} \in \mathcal{P}\,.$$

Pokažimo še zaprtost množice $\mathcal{P}$ za seštevanje, oziroma konveksnost stožca $\mathcal{P}$. Naj bosta $\overrightarrow{c}$ in $\overrightarrow{d} \in \mathcal{P}$. Potem velja

$$\overrightarrow{c} = \alpha_1 \overrightarrow{a} + \beta_1 \overrightarrow{b} \quad \text{in} \quad \overrightarrow{d} = \alpha_2 \overrightarrow{a} + \beta \overrightarrow{b}\,, \quad \alpha_1, \alpha_2, \beta_1, \beta_2 \geq 0\,.$$

Od tod sledi

$$\begin{aligned} \overrightarrow{c} + \overrightarrow{d} &= \alpha_1 \overrightarrow{a} + \beta_1 \overrightarrow{b} + \alpha_2 \overrightarrow{a} + \beta_2 \overrightarrow{b} = \\ &= (\, \alpha_1 + \alpha_2\,) \overrightarrow{a} + (\, \beta_1 + \beta_2\,) \overrightarrow{b} \in \mathcal{P} + \mathcal{P} \subset \mathcal{P}\,. \end{aligned}$$

Zgoraj definirana množica $\mathcal{P}$ je torej ireducibilen konveksen stožec v $\mathbb{R}^2$.

Zgled 4. Naj bo množica $\mathcal{P}$ unija dveh disjunktnih množic, $\mathcal{P}_1 \cup \mathcal{P}_2$ iz zgleda 3. Dokazali smo, da sta $\mathcal{P}_1$ in $\mathcal{P}_2$ vsaka zase stožec. Očitno je tudi njuna unija stožec, ki pa ni konveksen. Če namreč vzamemo $a \in \mathcal{P}_1$ in $b \in \mathcal{P}_2$, njuna vsota $a + b$ ni nujno element $\mathcal{P}$.

Zgled 5. Primer ireducibilnega stožca v $\mathbb{R}^3$ predstavlja množica $\mathcal{P} = \{(x, y, z); \sqrt{x^2 + y^2} < z \text{ in } z > 0\}$. Prepričajmo se, da omenjena množica predstavlja konveksen stožec. Dokazati moramo, da $\mathcal{P}$ zadošča pogojema definicije. Dokažimo najprej zaprtost $\mathcal{P}$ za množenje s skalarjem $\alpha > 0$. Ker je $\sqrt{x^2 + y^2} < z$, za vsak $\alpha > 0$ velja

$$\sqrt{(\alpha x)^2 + (\alpha y)^2} = \alpha\sqrt{x^2 + y^2} < \alpha z\,,$$

kar pomeni, da množica $\mathcal{P}$ predstavlja stožec. Pokažimo še njegovo konveksnost. Naj bosta $a = (x_1, y_1, z_1)$ in $b = (x_2, y_2, z_2) \in \mathcal{P}$. Potem za a in b velja $\sqrt{x_1^2 + y_1^2} < z_1$ in $\sqrt{x_2^2 + y_2^2} < z_2$, oziroma

$$\sqrt{x_1^2 + y_1^2} + \sqrt{x_2^2 + y_2^2} < z_1 + z_2\,.$$

Po kvadriranju dobimo

$$x_1^2 + y_1^2 + x_2^2 + y_2^2 + 2\sqrt{x_1^2 + y_1^2}\sqrt{x_2^2 + y_2^2} < (z_1 + z_2)^2\,.$$

Od tod, z uporabo neenakosti

$$2\sqrt{x_1^2 + y_1^2}\sqrt{x_2^2 + y_2^2} \geq 2(x_1x_2 + y_1y_2)\,,$$

sledi

$$x_1^2+y_1^2+x_2^2+y_2^2+2(x_1x_2+y_1y_2) = (x_1+x_2)^2+(y_1+y_2)^2 < (z_1+z_2)^2\,.$$

Ker je $z_1 + z_2 > 0$, dobimo

$$\sqrt{(\,x_1 + x_2\,)^2 + (\,y_1 + y_2\,)^2} < z_1 + z_2\,.$$

Podobno bi pokazali, da je tudi množica $\mathcal{P} = \{\,(x_1, x_2, \ldots, x_n);$ $\sqrt{x_1^2 + x_2^2 + \ldots + x_{n-1}^2} < x_n$ in $x_n > 0\}$ ireducibilen konveksen stožec prostora $\mathbb{R}^n$. Stožec $\mathcal{P}$ imenujemo tudi *Lorentzov stožec*. Lorentzov stožec bo predmet posebne obravnave naslednjega poglavja.

Naj bo $\mathcal{P}$ stožec prostora $\mathcal{V}$. Podmnožico $\mathcal{Q}$ stožca $\mathcal{P}$ imenujemo *podstožec*, če velja

$$a + b \in \mathcal{Q} \quad \text{in} \quad \alpha a \in \mathcal{Q} \quad \forall\, a, b \in \mathcal{Q} \text{ in } \alpha \geq 0\,.$$

Stožci realnega vektorskega prostora zadoščajo lastnosti krajšanja

$$a + c = b + c \;\Rightarrow\; a = b, \qquad \forall\, a, b, c \in \mathcal{P}\,.$$

Drži pa tudi obrat trditve. Če elementi stožca $\mathcal{P}$ izpolnjujejo omenjeno lastnost, je $\mathcal{P}$ stožec realnega vektorskega prostora. Toda v splošnem ne velja, da je poljuben stožec tudi stožec vektorskega prostora.

Zgled 6. Z $Conv(\mathcal{P})$ označimo množico vseh nepraznih konveksnih podmnožic stožca $\mathcal{P}$. Očitno je $Conv(\mathcal{P})$, opremljena z običajnima operacijama seštevanja in množenja množic

$$A + B = \{\, a + b; a \in \mathcal{P} \text{ in } b \in \mathcal{P}\,\} \qquad A, B \in Conv(\mathcal{P})\,,$$

$$\alpha A = \{\, \alpha a; a \in \mathcal{P}\,\} \qquad A \in \mathcal{P} \text{ in } \alpha \geq 0\,,$$

stožec. Za konveksnost $Conv(\mathcal{P})$ zadošča pokazati, da je $(\alpha+\beta)A = \alpha A + \beta A$. Očitno je $(\alpha + \beta)A$ podmnožica $\alpha A + \beta A$. Pokažimo še obratno inkluzijo. Vzemimo poljuben element $c \in \alpha A + \beta A$. Element c potem lahko zapišemo kot $c = \alpha a + \beta b$, kjer $a, b \in A$. Ker je

$$c = (\alpha + \beta)\Big(\frac{\alpha}{\alpha + \beta}\, a + \frac{\beta}{\alpha + \beta}\, b \Big)\,,$$

zaradi konveksnosti A velja

$$\frac{\alpha}{\alpha + \beta}\, a + \frac{\beta}{\alpha + \beta}\, b \in A\,,$$

od koder sledi $c \in (\alpha + \beta)A$.

Opazimo, da množica nepraznih konveksnih podmnožic realnega vektorskega prostora tvori stožec, ki ne zadošča lastnosti krajšanja. Primer stožca, ki ne zadošča lastnosti krajšanja predstavlja tudi naslednji

Zgled 7. Naj bo $\mathcal{P}$ stožec in X poljubna množica. Z $\mathcal{F}(X, \mathcal{P})$ označimo množico vseh funkcij definiranih na X, katerih zaloga vrednosti je $\mathcal{P}$. Če v $\mathcal{F}(X, \mathcal{P})$ definiramo operaciji seštevanja in množenja s skalarjem po točkah, predstavlja $\mathcal{F}(X, \mathcal{P})$ stožec, v katerem ne velja pravilo krajšanja.

Zgled 8. Eden osnovnih načinov generiranja konveksnih stožcev izhaja iz teorije nelinearnega programiranja, kjer iščemo ekstreme danih funkcij na konveksnih, a včasih negladkih, množicah. Naj bo torej $\mathcal{K} \subseteq \mathbb{R}^n$ konveksna množica in $b \in \mathcal{K}$. Definirajmo

$$\mathcal{P} = \{\, \dot{\gamma}(0);\, \gamma\colon [0,T] \to \mathcal{K} \text{ gladka}\,,\, \gamma(0) = b \,\}\,,$$

kjer je

$$\dot{\gamma}(0) = \lim_{\substack{t\to 0\\ t>0}} \frac{\gamma(t) - b}{t}\,.$$

Pokažimo, zaprtost množice $\mathcal{P}$ za množenje z nenegativnim skalarjem in seštevanje.

Naj bo $v \in \mathcal{P}$ tak, da je $v = \dot{\gamma}(0)$ in $\gamma : [0,T] \to \mathcal{K}$. Za $\alpha > 0$, definirajmo $\delta\colon [0, \frac{T}{\alpha}] \to \mathcal{K}$ s predpisom

$$\delta(t) = \gamma(\alpha t)\,.$$

Ker je potem

$$\dot{\delta}(0) = \alpha\, \dot{\gamma}(0) = \alpha v\,,$$

in $\dot{\delta}(0) \in \mathcal{P}$, sledi $\mathbb{R}^+\mathcal{P} \subseteq \mathcal{P}$.

Vzemimo $v, w \in \mathcal{P}$ taka, da je $v = \dot{\gamma}(0)$, $w = \dot{\delta}(0)$ in $\gamma,\ \delta\colon [0,T] \to \mathcal{K}$. Definirajmo $\epsilon\colon [0,T] \to \mathcal{K}$ na naslednji način

$$\epsilon(t) = \tfrac{1}{2}\,\gamma(t) + \tfrac{1}{2}\,\delta(t)\,.$$

Hitro se lahko prepričamo, da je ϵ dobro definirana in velja

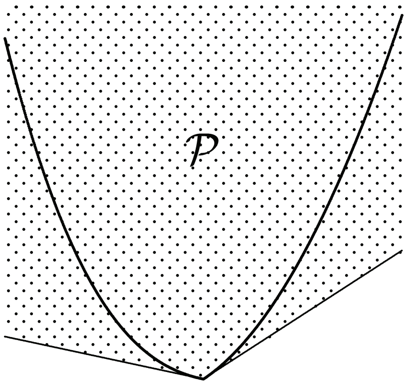
$$\dot{\epsilon}(0) = \tfrac{1}{2}\,v + \tfrac{1}{2}\,w \in \mathcal{P}\,.$$

Po prej dokazanem sledi, da je $2\,(\,\frac{1}{2}\,v + \frac{1}{2}\,w\,) = v + w \in \mathcal{P}$. Zgoraj definirana množica $\mathcal{P}$ je torej konveksen stožec.

Dokažimo, da za konveksno množico $\mathcal{K}$ in stožec $\mathcal{P}$ velja

$$\mathcal{K} \subseteq b + \mathcal{P}\,.$$

Vzemimo poljubno točko $b \in \mathcal{K}$ in zapišimo $\gamma(t) = b + t\,(k - b)$. Ker je $\dot{\gamma}(t) = -b + k$, sledi $\dot{\gamma}(0) = -b + k \in \mathcal{P}$. Od tod sledi, da je $k = b + (-b + k) \in b + \mathcal{P}$.



Stožec $\mathcal{P} = \{\, \dot\gamma(0)\,;\, \gamma\colon [0,T] \to \mathcal{K} \text{ gladka}\,,\ \gamma(0) = b\,\}$

1.2 Delno urejeni stožci

Naj bo dan končno razsežen realen vektorski prostor $\mathcal{V}$. Prostor $\mathcal{V}$ je *delno urejen vektorski prostor*, če je opremljen z relacijo delne urejenosti $\leq$, ki je usklajena z naslednjima pogojema

$$\begin{array}{ll} (i) & a \leq b \ \Rightarrow\ a + c \leq b + c \quad \forall\, a, b, c \in \mathcal{V} \\ (ii) & a \leq b \ \Rightarrow\ \alpha a \leq \alpha b \quad \forall\, a, b \in \mathcal{V} \text{ in } \alpha \geq 0\,. \end{array}$$

V prostoru $\mathcal{V}$ izberimo stožec $\mathcal{P}$, ki zadošča pogoju $\mathcal{P} \cap -\mathcal{P} = \{0\}$. Stožec $\mathcal{P}$ v prostoru $\mathcal{V}$ določa delno urejenost $\leq$ z naslednjim predpisom: če $a, b \in \mathcal{V}$, potem

$$a \leq b \quad\Longleftrightarrow\quad b - a \in \mathcal{P}\,.$$

Hitro se lahko prepričamo, da zgoraj definirana relacija $\leq$ res delno ureja vektorski prostor $\mathcal{V}$. Najprej preverimo refleksivnost, antisimetričnost in tranzitivnost:

$$\begin{array}{rl} \text{refleksivnost}: & \forall a \in \mathcal{P} \text{ velja } a - a = 0 \in \mathcal{P} \Rightarrow a \leq a\,. \\ \text{antisimetričnost}: & \text{če je } a - b \in \mathcal{P} \text{ in } b - a \in \mathcal{P} \\ & \Rightarrow a - b = b - a = 0 \text{ oziroma } a = b\,. \\ \text{tranzitivnost}: & \text{če je } b - a \in \mathcal{P} \text{ in } c - b \in \mathcal{P}, \text{ zaradi zaprtosti} \\ & \mathcal{P} \text{ za seštevanje velja } c - a = c - b + \\ & + b - a \in \mathcal{P} + \mathcal{P} \subseteq \mathcal{P} \Rightarrow a \leq c\,. \end{array}$$

Seveda je relacija $\leq$ usklajena tudi s pogojema (i) in (ii):

$$\begin{aligned} (\, a \leq b \iff b-a \in \mathcal{P}\,) \Rightarrow & \\ \Rightarrow \quad & (\,(b+c)-(a+c) \in \mathcal{P} \iff a+c \leq b+c\,)\,, \\ (\, a \leq b \iff b-a \in \mathcal{P}\,) \Rightarrow & \\ \Rightarrow \quad & (\,\alpha b - \alpha a \in \mathcal{P} \iff \alpha a \leq \alpha b\,) \quad \forall\, \alpha \geq 0\,. \end{aligned}$$

Stožec $\mathcal{P}$ torej v prostoru $\mathcal{V}$ določa neko delno urejenost. Velja pa tudi obrat trditve. Poljubna relacija delne urejenosti $\leq$ vektorskega prostora $\mathcal{V}$, usklajena s pogojema (i) in (ii), določa v $\mathcal{V}$ nek stožec.

Naj bo $\mathcal{V}_+ = \{\, a \in \mathcal{V};\, a \geq 0\,\}$ in $\geq$ relacija usklajena s pogojema (i) in (ii). Pokažimo najprej, da je $\mathcal{V}_+$ zaprta za seštevanje. Če sta $a, b \in \mathcal{V}_+$ velja $a \geq 0$ in $b \geq 0$. Ker $\geq$ ustreza pogoju (i), je $a + b \geq 0 + b$. Zaradi tranzitivnosti je potem $a + b \geq 0$, od koder sledi $a + b \in \mathcal{V}_+$.

Pokažimo še zaprtost $\mathcal{V}_+$ za množenje s pozitivnim skalarjem. Če $a \in \mathcal{V}_+$ in $\alpha > 0$, zaradi pogoja (ii) sledi $\alpha a \geq 0$, oziroma $\alpha a \in \mathcal{V}_+$.

Množica $\mathcal{V}_+$ je torej stožec, ki ga imenujemo *pozitivni stožec* delno urejenega prostora $\mathcal{V}$. Elemente v $\mathcal{V}_+$ imenujemo *pozitivni* elementi. Podobno definiramo *negativni stožec*, kot množico $\mathcal{V}_- = \{\, a \in \mathcal{V};\, a \leq 0\,\}$. Elemente v $\mathcal{V}_-$ imenujemo *negativni* elementi.

Zgled 1. Prostor $\mathbb{R}$ je s stožcema $\mathcal{P} = (0, \infty)$ in $\mathcal{P} = [\,0, \infty)$ delno urejen vektorski prostor.

Zgled 2. Vektorski prostor $\mathbb{R}^2$ je s stožcem $\mathcal{P} = \{\,(x, y); x, y \geq 0\,\}$ primer delno urejenega vektorskega prostora, ki ni *linearno urejen*. Vektorski prostor je namreč linearno urejen, če je delno urejen in za vsak par elementov a in b tega prostora velja bodisi $a \leq b$, bodisi $b \leq a$. Če vzamemo elementa $a = (1, 1)$ in $b = (0, 2)$, njuni razliki $a - b = (1, -1)$ in $b - a = (-1, 1)$, ne ležita v $\mathcal{P}$, tako da ne velja niti $a \leq b$ niti $b \leq a$.

Zgled 3. Naj bo X poljubna neprazna množica. Če v prostoru $\mathcal{F}(X, \mathbb{R})$ definiramo urejenost na naslednji način

$$f \leq g \iff f(x) \leq g(x)\,,\ \forall\, x \in X\,,$$

pripadajoči stožec predstavlja množica nenegativnih realnih funkcij. Hitro se lahko prepričamo, da prostor $\mathcal{F}(X, \mathbb{R})$ ni linearno urejen.

1.3 Dualni stožci in polare

Naj bo $\mathcal{W}$ n-dimenzionalen vektorski prostor nad obsegom realnih števil. V $\mathcal{W}$ naj bo skalarni produkt definiran na običajni način

$$\langle (x_1, x_2, \ldots, x_n), (y_1, y_2, \ldots, y_n) \rangle = x_1 y_1 + x_2 y_2 + \ldots + x_n y_n \,.$$

Na običajni način vpeljimo tudi pojem evklidske razdalje

$$|| \, x \, ||^2 = \langle \, x, x \, \rangle \,.$$

Danemu stožcu $\mathcal{P}$ prostora $\mathcal{W}$ priredimo množico

$$\mathcal{P}^\bullet = \{ \, y \in \mathcal{W}; \, \langle \, x, y \, \rangle \geq 0 \, , \, \forall \, x \in \mathcal{P} \, \} \, ,$$

in jo imenujmo *dualni stožec* stožca $\mathcal{P}$. Očitno je zaradi aditivnosti in homogenosti skalarnega produkta množica $\mathcal{P}^\bullet$ stožec prostora $\mathcal{W}$.

Naj bo $x \in \mathcal{P}$ in $\{y_n\}_{n \in \mathbb{N}}$ poljubno konvergentno zaporedje vektorjev iz $\mathcal{P}^\bullet$ z limito y. Očitno velja

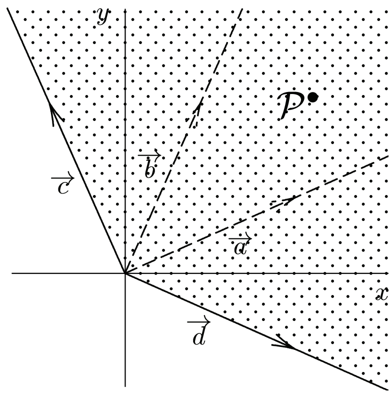
$$\lim_{n \to \infty} \langle \, x, y_n \, \rangle = \langle \, x, \lim_{n \to \infty} y_n \, \rangle = \langle \, x, y \, \rangle \, .$$

Ker je $\langle \, x, y_n \, \rangle \geq 0$, za vsak $n \in \mathbb{N}$, sledi tudi nenegativnost limitne vrednosti za vsak $x \in \mathcal{P}$. Po definiciji dualnega stožca je potem $y \in \mathcal{P}^\bullet$. Stožec $\mathcal{P}^\bullet$ je torej vedno zaprta množica.

Zgled 1. Naj bo $\mathcal{P}$ stožec iz zgleda 1.1.3, torej množica točk prvega kvadranta, ki ju določata vektorja $\overrightarrow{a}$ in $\overrightarrow{b}$.

Oglejmo si najprej geometrijsko mesto točk, ki zadoščajo pogoju $\langle \, x, a \, \rangle \geq 0$, za $a \in \mathbb{R}^2$. Po zgornji definiciji skalarnega produkta je to polprostor, ki vsebuje točko a in katerega rob poteka skozi koordinatno izhodišče O ter je pravokoten na zveznico skozi O in a. Množica točk $y \in \mathcal{P}^\bullet$, ki zadošča pogoju $\langle \, x, y \, \rangle \geq 0$, $x \in \mathcal{P}$, je torej presek takih polprostorov. Če je rob stožca $\mathcal{P}$ generiran z vektorjema $\overrightarrow{a} = (\, x_1, y_1 \,)$ in $\overrightarrow{b} = (\, x_2, y_2 \,)$, $x_1, x_2, y_1, y_2 \geq 0$, je rob njemu dualnega stožca $\mathcal{P}^\bullet$ generiran z vektorjema $\overrightarrow{c} = (\, -y_1, x_1 \,)$ in $\overrightarrow{d} = (\, y_2, -x_2 \,)$.

Če za stožec $\mathcal{P}$ izberemo 1.kvadrant, opazimo, da je njegov dualni stožec kar 1. kvadrant, oziroma $\mathcal{P} = \mathcal{P}^\bullet$.



Dual stožca $\mathcal{P} = \{\, \alpha \overrightarrow{a} + \beta \overrightarrow{b}\,;\ \alpha,\ \beta \geq 0 \,\}$

V nadaljevanju bo predmet posebne obravnave množica

$$\mathcal{S}^o = \{\, y \in \mathcal{W}\,;\ \langle\, x, y \,\rangle \leq 1\,,\ \forall\, x \in \mathcal{S} \,\}\,,$$

ki jo imenujemo *polarna množica* oziroma *polara* množice $\mathcal{S}$.

Zgled 2. Naj bo množica $\mathcal{S}$ stožec $\mathcal{P}$ iz zgleda 1.1.3. Geometrijsko mesto točk, ki zadoščajo pogoju $\langle\, x, a \,\rangle \leq 1$, za $a = (x_1, y_1) \in \mathbb{R}^2$, predstavlja polprostor, ki ne vsebuje točke a in katerega rob predstavlja premica $y = -\frac{x_1}{y_1} x + \frac{1}{y_1}$. Množica točk $y \in \mathcal{S}^o$, ki zadošča pogoju $\langle x, y \,\rangle \leq 1$, $x \in \mathcal{P}$, je potem presek takih polprostorov. Če je rob stožca $\mathcal{P}$ generiran z vektorjema $\overrightarrow{a} = (\, x_1, y_1 \,)$ in $\overrightarrow{b} = (\, x_2, y_2 \,)$, $x_1, x_2, y_1, y_2 \geq 0$, je rob njegove polare $\mathcal{S}^o$ generiran z vektorjema $\overrightarrow{e} = (\, -y_2, x_2 \,)$ in $\overrightarrow{f} = (\, y_1, -x_1 \,)$.

Trditev 3.1. *Naj bo $\mathcal{S}$ poljubna zaprta, konveksna množica, ki vsebuje element 0. Potem velja*

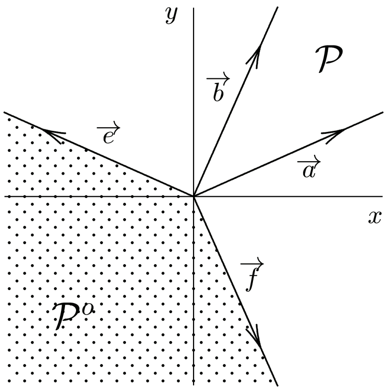
$$\mathcal{S}^{oo} = \mathcal{S}\,.$$

Dokaz: Inkluzija $\mathcal{S} \subseteq \mathcal{S}^{oo}$ je očitna. Kot dokaz inkluzije $\mathcal{S}^{oo} \subseteq \mathcal{S}$ zadošča pokazati: če $x_0 \notin \mathcal{S}$, potem obstaja tak y, da za vsak $x \in \mathcal{S}$ velja $\langle\, x, y \,\rangle \leq 1$ in $\langle\, x_0, y \,\rangle > 1$. Naj bo $x_1 \in \mathcal{S}$ tak, da je razdalja od x_1 do x_0 minimalna. Za vsak $x \in \mathcal{S}$, torej velja

$$||\, x - x_0 \,|| \geq ||\, x_1 - x_0 \,||\,.$$

Za $0 \leq \lambda \leq 1$ in $x \in \mathcal{S}$, zaradi konveksnosti $\mathcal{S}$, sledi $\lambda x + (1-\lambda)\, x_1 \in \mathcal{S}$. Od tod velja

$$||\, \lambda x + (1-\lambda)\, x_1 - x_0 \,||^2 \geq ||\, x_1 - x_0 \,||^2$$



Polara stožca $\mathcal{P} = \{\, \alpha\vec{a} + \beta\vec{b};\ \alpha,\ \beta \geq 0\,\}$

$$\text{oziroma } \lambda^2 \,||\, x - x_1 \,||^2 + 2\lambda \,\langle\, x - x_1, x_1 - x_0 \,\rangle \geq 0\,.$$

Ker neenakost velja za vsak $0 \leq \lambda \leq 1$, mora neničelen koren polinoma na levi, ki je enak $-2\frac{\langle\, x - x_1, x_1 - x_0 \,\rangle}{||\, x - x_1 \,||^2}$, biti negativno število. To pomeni, da je

$$\langle\, x - x_1, x_1 - x_0 \,\rangle \geq 0\,,$$

in od tod

$$\langle\, x, x_0 - x_1 \,\rangle \leq \langle\, x_1, x_0 - x_1 \,\rangle\,.$$

Če je $x = 0$, sledi

$$\langle\, x_1, x_0 - x_1 \,\rangle \geq 0\,.$$

Ker je $\langle\, x_0 - x_1, x_0 - x_1 \,\rangle > 0$, obstaja tak $\mu > 0$, da velja

$$\langle\, x_1, x_0 - x_1 \,\rangle < \mu < \langle\, x_0, x_0 - x_1 \,\rangle\,,$$

Za vsak $x \in \mathcal{S}$ torej velja

$$\langle\, x, x_0 - x_1 \,\rangle \leq \langle\, x_1, x_0 - x_1 \,\rangle < \mu < \langle\, x_0, x_0 - x_1 \,\rangle\,.$$

Od tod sledi, da $y = \frac{1}{\mu}(x_0 - x_1)$ zadošča pogoju trditve. □

Trditev 3.2. *Za poljuben neprazen in zaprt stožec $\mathcal{P}$ velja $\mathcal{P}^{\bullet\bullet} = \mathcal{P}$.*

Dokaz: Dokažimo najprej enakost $\mathcal{P}^o = -\mathcal{P}^\bullet$.

Naj bo $y \in \mathcal{P}^\bullet$. Po definiciji duala je potem $\langle\, \mathcal{P}, y \,\rangle \geq 0$, oziroma $\langle\, \mathcal{P}, -y \,\rangle \leq 0$. Ker je očitno $\langle\, \mathcal{P}, -y \,\rangle \leq 1$, sledi $-y \in \mathcal{P}^o$ in $-\mathcal{P}^\bullet \subseteq \mathcal{P}^o$.

Naj bo $y \in \mathcal{P}^o$. Za vsak $x \in \mathcal{P}$ torej velja $\langle\, x, y \,\rangle \leq 1$. Ker je $\mathcal{P}$ zaprt za množenje z nenegativnim skalarjem, je zaprt tudi za množenje z $n \in \mathbb{N}$ in velja $\langle\, nx, y \,\rangle \leq 1$. Od tod je $\langle\, x, y \,\rangle \leq \frac{1}{n}$, za vsak $n \in \mathbb{N}$, oziroma $\langle\, x, y \,\rangle \leq 0$. Ker je potem $\langle\, x, -y \,\rangle \geq 0$, za vsak $x \in \mathcal{P}$, sledi $-y \in \mathcal{P}^\bullet$ in $\mathcal{P}^o \subseteq -\mathcal{P}^\bullet$. Od tod torej dobimo $\mathcal{P}^o = -\mathcal{P}^\bullet$.

Po dokazanem velja

$$\mathcal{P}^{\bullet\bullet} = -(\mathcal{P}^\bullet)^o = -(-\mathcal{P}^o)^o\,.$$

Ker je $(-\mathcal{P})^o = -(\mathcal{P}^o)$, sledi

$$-(-\mathcal{P}^o)^o = -(-(\mathcal{P}^{oo}))\,.$$

Ker po trditvi 3.1 velja $-(-(\mathcal{P}^{oo})) = \mathcal{P}$, sledi $\mathcal{P}^{\bullet\bullet} = \mathcal{P}$. □

Trditev 3.3. *Naj bo $\mathcal{P}$ poljuben stožec. Potem je $\mathcal{P}^o$ konveksen stožec, za katerega velja*

$$\mathcal{P}^o = \{\, y\,;\, \langle\, y, \mathcal{P} \,\rangle \leq 0 \,\}\,.$$

Dokaz: Naj bo $\mathcal{P}$ stožec. Poglejmo njegovo polaro. Po definiciji je $y \in \mathcal{P}^o \;\Leftrightarrow \langle\, y, \mathcal{P} \,\rangle \leq 1$. Zaradi zaprtosti $\mathcal{P}$ za množenje z nenegativnim skalarjem velja

$$\langle\, y, \mathbb{R}^+\mathcal{P} \,\rangle \leq 1 \quad \Rightarrow \quad \mathbb{R}^+ \langle\, y, \mathcal{P} \,\rangle \leq 1 \quad \Rightarrow \quad \langle\, y, \mathcal{P} \,\rangle \leq 0\,.$$

Od tod sledi

$$\mathcal{P}^o = \{\, y\,;\, \langle\, y, \mathcal{P} \,\rangle \leq 0 \,\}\,.$$

Pokažimo, da je $\mathcal{P}^o$ stožec:

$$\begin{aligned}
&(i)\ \ y_1, y_2 \in \mathcal{P}^o\,,\ \langle\, y_1 + y_2, \mathcal{P} \,\rangle = \langle\, y_1, \mathcal{P} \,\rangle + \langle\, y_2, \mathcal{P} \,\rangle \leq 0\\
&\qquad \Rightarrow \mathcal{P}^o + \mathcal{P}^o \subseteq \mathcal{P}^o\\
&(ii)\ \langle\, \mathbb{R}^+ y, \mathcal{P} \,\rangle = \mathbb{R}^+ \langle\, y, \mathcal{P} \,\rangle \subset \mathbb{R}^+\,\mathbb{R}^- \subseteq \mathbb{R}^- \;\Rightarrow \mathbb{R}^+\, y \in \mathcal{P}^o\\
&\qquad \Rightarrow \mathbb{R}^+\,\mathcal{P}^o \subseteq \mathcal{P}^o\,.
\end{aligned}$$

Naj $\mathcal{S}^\perp$ pomeni običajno ortogonalno množico, definirano s predpisom

$$\mathcal{S}^\perp = \{\, y \in \mathcal{W}\,;\, \langle\, y, \mathcal{S} \,\rangle = 0 \,\}\,.$$

Očitno je $\mathcal{S}^\perp$ vedno podprostor v $\mathcal{W}$.

Trditev 3.4. *Za poljuben neprazen zaprt konveksen stožec $\mathcal{P}$ velja*

$$(\mathcal{P}^\bullet - \mathcal{P}^\bullet)^\perp = \mathcal{P} \cap -\mathcal{P}\,.$$

Dokaz: Naj bo $z \in (\mathcal{P}^\bullet - \mathcal{P}^\bullet)^\perp$. Ker je $\mathcal{P}^\bullet - \mathcal{P}^\bullet = \{\, y_1 - y_2 \in \mathcal{W};\, y_1, y_2 \in \mathcal{P}^\bullet \,\}$ in $0 \in \mathcal{P}^\bullet$, velja $\mathcal{P}^\bullet \subseteq \mathcal{P}^\bullet - \mathcal{P}^\bullet$. Od tod sledi $z \in (\mathcal{P}^\bullet)^\perp$, oziroma $\langle\, \mathcal{P}^\bullet, z \,\rangle = 0$. Seveda je $\langle\, \mathcal{P}^\bullet, z \,\rangle \geq 0$, od koder sledi $z \in \mathcal{P}^{\bullet\bullet}$. Po trditvi 3.2 je potem $z \in \mathcal{P}$.

Po drugi strani je tudi $-\mathcal{P}^\bullet \subseteq \mathcal{P}^\bullet - \mathcal{P}^\bullet$. Po analognem sklepu sledi $z \in -\mathcal{P}$. Torej je $z \in \mathcal{P} \cap -\mathcal{P}$.

Naj bo $z \in \mathcal{P} \cap -\mathcal{P}$. Ker sta potem $z \in \mathcal{P}$ in $-z \in \mathcal{P}$ za poljuben $\lambda \in \mathbb{R}$ velja:

$$\begin{aligned}
(i)&\ \ \lambda > 0 \Rightarrow \lambda z \in \mathcal{P}\,;\\
(ii)&\ \ \lambda = 0 \Rightarrow \lambda z = 0 \in \mathcal{P},\ \text{zaradi zaprtosti } \mathcal{P}\,;\\
(iii)&\ \ \lambda < 0 \Rightarrow \lambda = -\mu \Rightarrow \lambda z = \mu(-z) \in \mathcal{P}\,.
\end{aligned}$$

Sledi torej $\mathbb{R}z \subseteq \mathcal{P}$. Vzemimo $y \in \mathcal{P}^\bullet$. Ker je potem $\langle\, y, \mathcal{P} \,\rangle \geq 0$, sledi

$$\langle\, y, \mathbb{R}z \,\rangle \geq 0 \Rightarrow \mathbb{R}\,\langle\, y, z \,\rangle \geq 0 \Rightarrow \langle\, y, z \,\rangle = 0$$

in od tod $z \in (\mathcal{P}^\bullet)^\perp$. Očitno je potem zaradi

$$\langle\, z, \mathcal{P}^\bullet - \mathcal{P}^\bullet \,\rangle \subseteq \langle\, z, \mathcal{P}^\bullet \,\rangle - \langle\, z, \mathcal{P}^\bullet \,\rangle = 0\,,$$

$z \in (\mathcal{P}^\bullet - \mathcal{P}^\bullet)^\perp$. □

Trditev 3.5. *Naj bo $\mathcal{P}$ zaprt neprazen konveksen stožec. Potem je*

$$int(\mathcal{P}^\bullet) = \{\, y\,;\, \langle\, x, y \,\rangle > 0,\, \forall\, x \in \mathcal{P} \setminus \{0\} \,\}\,,$$

in velja ekvivalenca naslednjih trditev:

$$\begin{aligned}
(i)&\ \ \mathcal{P}\ \textit{je pravi, oziroma}\ \mathcal{P} \cap -\mathcal{P} = \{0\}\,.\\
(ii)&\ \ int\,(\mathcal{P}^\bullet) \neq 0\,.
\end{aligned}$$

Opomba: *$int(\mathcal{P}^\bullet)$ pomeni običajno notranjost množice v (evklidskem) topološkem prostoru.*

Dokaz: Dokažimo najprej $int(\mathcal{P}^\bullet) = \{\, y\,;\, \langle\, x, y \,\rangle > 0,\, \forall\, x \in \mathcal{P} \setminus \{0\} \,\}$. Označimo z $\mathcal{O} = \{\, y\,;\, \langle\, x, y \,\rangle > 0,\, \forall\, x \in \mathcal{P} \setminus \{0\} \,\}$. Očitno je $\mathcal{O} =$

$\{\, y\,;\, \langle\, x, y\,\rangle > 0, \forall\, x \in \mathcal{P}$ in $||\, x\,|| = 1\,\}$. Pokažimo, da je $\mathcal{O}$ odprta množica. Ker je množica $\{\, x \in \mathcal{P}\,;\, ||\, x\,|| = 1\,\} = \mathcal{P} \cap \mathcal{S}_1$, presek zaprte in kompaktne množice, je kompaktna. Naj bo $y \in \mathcal{O}$. Ker je funkcija $f : \mathcal{P} \cap \mathcal{S}_1 \longrightarrow \mathbb{R}^+$, definirana s predpisom $f(x) = \langle\, y, x\,\rangle$ zvezna, zavzame na $\mathcal{P} \cap \mathcal{S}_1$ minimum $\epsilon > 0$. Torej velja $\langle\, y, x\,\rangle \geq \epsilon > 0$, za vsak $x \in \mathcal{P} \cap \mathcal{S}_1$. Če je $||\, y - z\,|| < \frac{\epsilon}{2}$ velja

$$\langle\, z, x\,\rangle = \langle\, z - y + y, x\,\rangle = \langle\, y, x\,\rangle - \langle\, y - z, x\,\rangle \geq \epsilon - |\,\langle\, y - z, x\,\rangle\,| \geq$$

$$\geq \epsilon - ||\, y - z\,|| \cdot ||\, x\,|| = \epsilon - ||\, y - z\,|| \geq \epsilon - \frac{\epsilon}{2} = \frac{\epsilon}{2}\,.$$

Po definiciji je potem $z \in \mathcal{O}$, kar pomeni, da je krogla s polmerom $\frac{\epsilon}{2}$ in središčem v točki y vsebovana v $\mathcal{O}$. To pomeni, da je $\mathcal{O}$ odprta, od koder sledi $\mathcal{O} \subset int(\mathcal{P}^\bullet)$.

Naj bo $y \in int(\mathcal{P}^\bullet)$. Če je $x \in \mathcal{P}\backslash\{0\}$, za vsak $y + u \in \mathcal{P}^\bullet$, $||\, u\,|| < \epsilon$, velja $\langle\, y + u, x\,\rangle \geq 0$, oziroma $\langle\, y, x\,\rangle + \langle\, u, x\,\rangle \geq 0$. Denimo, da je $\langle\, y, x\,\rangle = 0$. Potem je $\langle\, u, x\,\rangle \geq 0, \forall\, u\; :\; ||\, u\,|| < \epsilon$. Če vzamemo $u = -\frac{\epsilon}{2}\, x \neq 0$, sledi $\langle\, u, x\,\rangle = -\frac{\epsilon}{2}\,\langle\, x, x\,\rangle \geq 0$. Ker je $\langle\, x, x\,\rangle \neq 0$, sledi $-\frac{\epsilon}{2} \geq 0$, kar je protislovje s predpostavko, da je $\epsilon > 0$. Sledi torej $\langle\, y, x\,\rangle > 0$, oziroma $int(\mathcal{P}^\bullet) \subset \mathcal{O}$.

Dokažimo ekvivalenco trditev (i) in (ii). $(i) \Rightarrow (ii)$ Naj bo $\mathcal{P} \cap -\mathcal{P} = 0$. Po trditvi 3.4 je $(\,\mathcal{P}^\bullet - \mathcal{P}^\bullet\,)^\perp = 0$. Ker je $\mathcal{P}^\bullet$ konveksen stožec, je $\mathcal{P}^\bullet - \mathcal{P}^\bullet$ podprostor. Ker je njegov ortogonalni komplement trivialen, je $\mathcal{P}^\bullet - \mathcal{P}^\bullet = \mathcal{W}$. To pa pomeni, da $\mathcal{P}^\bullet$ vsebuje neko bazo prostora $\mathcal{W}$ in ima zato neprazno notranjost.

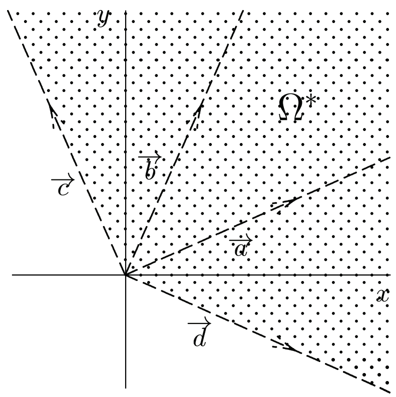
$(ii) \Rightarrow (i)$ Ker je $int(\mathcal{P}^\bullet) \neq 0$, obstaja tak y, da velja $\langle\, y, \mathcal{P}\backslash\{0\}\,\rangle > 0$. Naj bo $x \in \mathcal{P} \cap -\mathcal{P}$. Ker sta potem x in $-x \in \mathcal{P}$, velja $\langle\, x, y\,\rangle \geq 0$ in $\langle\, -x, y\,\rangle \geq 0$. Od tod sledi $\langle\, x, y\,\rangle = 0$, oziroma $x = 0$. Od tod torej dobimo $\mathcal{P} \cap -\mathcal{P} = \{0\}$. □

Trditev 3.6. *Naj bo $\mathcal{U} \subset int(\mathcal{P}^\bullet)$ kompaktna. Potem obstaja taka pozitivna realna konstanta ρ, da za vsak $x \in \mathcal{P}$ in $y \in \mathcal{U}$ velja*

$$\langle\, x, y\,\rangle \geq \rho\, ||\, x\,||\,.$$

Dokaz: Trditev je očitna za $x = 0$. Za $x \neq 0$ naj bo $u = \frac{x}{||x||}$. Zadošča dokazati obstoj takega $\rho > 0$, da je

$$\langle\, u, y\,\rangle \geq \rho\,, \quad \forall\, u \in S(\mathcal{V}) \cap \mathcal{P}\,,\, y \in \mathcal{U}\,.$$



Odprti dual stožca $\mathcal{P} = \{\, \alpha \overrightarrow{a} + \beta \overrightarrow{b}\,;\, \alpha,\, \beta \geq 0 \,\}$

To pa je očitno po prvem delu trditve 3.5, saj je $\langle\, u, y \,\rangle$ strogo pozitivna zvezna funkcija na kompaktni množici $(\, S(\mathcal{V}) \cap \mathcal{P}\,) \times \mathcal{U}$. $\square$

Trditev 3.7. *Naj bo $\mathcal{P}$ zaprt konveksen stožec. Potem je za vsak $y \in int(\mathcal{P}^\bullet)$ množica*

$$\{\, x \in \mathcal{P}\,;\, \langle\, x, y \,\rangle \leq 1 \,\}$$

kompaktna.

Dokaz: Ker je množica $\{\, x \in \mathcal{P}\,;\, \langle\, x, y \,\rangle \leq 1 \,\}$ zaprta in po trditvi 3.6 vsebovana v krogli z radijem $\frac{1}{\rho}$, je kompaktna. $\square$

Odprtemu konveksnemu stožcu Ω prostora $\mathcal{W}$ priredimo množico

$$\Omega^* = \{\, y \in \mathcal{W};\, \langle\, x, y \,\rangle > 0\,,\, \forall x \in \overline{\Omega} \setminus \{0\} \,\}\,,$$

in jo imenujmo *odprti dual* stožca Ω. Simbol $\overline{\Omega}$ pomeni zaprtje v evklidski topologiji.

Zgled 3. Naj bo Ω notranjost stožca $\mathcal{P}$ iz zgleda 1.1.3. Očitno je stožec Ω odprti stožec. Oglejmo si geometrijsko mesto točk, ki zadoščajo pogoju $\langle\, x, y \,\rangle > 0$, za vsak neničelen $x \in \overline{\Omega}$. Hitro se lahko prepričamo, da so to ravno vse tiste točke duala $\mathcal{P}^\bullet$, ki ne ležijo na njegovem robu.

Trditev 3.8. *Zaprtje poljubnega konveksnega stožca je konveksen stožec.*

Dokaz: Naj bosta $x, y \in \overline{\Omega}$. Potem obstajata taki zaporedji $\{x_n\}$ in $\{y_n\}$, da velja $x = \lim x_n$ in $y = \lim y_n$, $x_n, y_n \in \Omega$. Tedaj je

$$
\begin{array}{ll}
(i) & x + y = \lim x_n + \lim y_n = \lim(\, x_n + y_n\,) \in \overline{\Omega} \Rightarrow \overline{\Omega} + \overline{\Omega} \subseteq \overline{\Omega}\,; \\
(ii) & \alpha > 0 \,:\, \alpha x = \lim \alpha x_n \in \overline{\Omega} \Rightarrow \mathbb{R}^+\overline{\Omega} \subseteq \overline{\Omega}\,.
\end{array}
$$

$\overline{\Omega}$ je torej stožec. □

Trditev 3.9. *Odprt konveksen stožec je notranjost svojega zaprtja, oziroma*

$$int(\,\overline{\mathcal{P}}\,) = \mathcal{P}\,.$$

Dokaz: Dokažimo najprej inkluzijo $\mathcal{P} \subset int(\overline{\mathcal{P}})$. Naj bo $S \in \mathcal{P}$. Ker je $\mathcal{P}$ odprt, obstaja odprta krogla $\mathcal{K}$ s središčem v S, ki je vsebovana v $\mathcal{P}$. Ker je $\mathcal{P} \subset \overline{\mathcal{P}}$, leži $\mathcal{K}$ v $\overline{\mathcal{P}}$. Od tod sledi, da je S je notranja točka $\overline{\mathcal{P}}$ in $\mathcal{P} \subset int(\,\overline{\mathcal{P}}\,)$.

Naj bo $S \in int(\,\overline{\mathcal{P}}\,)$. Potem obstaja taka krogla $\mathcal{K}$ s središčem v S, da vse njene točke ležijo v $\overline{\mathcal{P}}$. Včrtajmo v $\mathcal{K}$ n - dimenzionalno hiperkocko $\mathcal{K}_n$, ki vsebuje S kot svojo notranjo točko. Ker ležijo oglišča $\mathcal{K}_n$ v $\overline{\mathcal{P}}$, ležijo torej v $\mathcal{P}$ ali na njegovem robu $\partial\mathcal{P}$. Če katero izmed oglišč $\mathcal{K}_n$ leži na $\partial\mathcal{P}$, izberemo točke, ki so jim poljubno blizu in ležijo v notranjosti $\mathcal{P}$. Te točke tvorijo n - dimenzionalno hiperkocko $\mathcal{K}'_n$, ki vsebuje S, vse njene točke pa ležijo v $\mathcal{P}$. Ker je $\mathcal{P}$ konveksen, S leži v $\mathcal{P}$. Odtod sledi $int(\,\overline{\mathcal{P}}\,) \subset \mathcal{P}$. □

Omenjena trditev ne velja za poljubni stožec $\mathcal{P}$. Če namreč za $\mathcal{P}$ vzamemo stožec iz zgleda 1.1.4, le ta očitno ni notranjost svojega zaprtja. Razlog zato leži v tem, da $\mathcal{P}$ ni konveksen stožec.

Trditev 3.10. Ω^* *je notranjost* $\overline{\Omega}^*$.

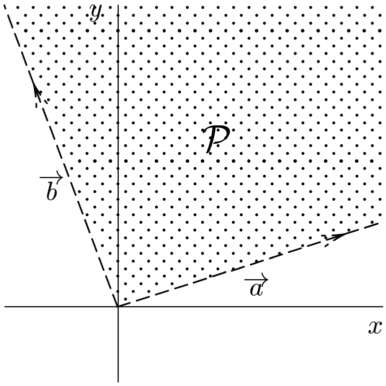
Dokaz: Trditev sledi neposredno iz prvega dela trditve 3.5, če vzamemo $\mathcal{P} = \overline{\Omega}$. □

Trditev 3.11. Ω^* *je neprazen natanko takrat, kadar je*

$$\overline{\Omega} \cap (-\overline{\Omega}) = \{0\}.$$

Dokaz: Trditev je direktna posledica trditev 3.5 in 3.10. □

Za konveksni stožec Ω pravimo, da je *sebi dualen*, če velja $\Omega = \Omega^*$. Po zgoraj navedenih ugotovitvah, je sebi dualen stožec očitno pravi.



Stožec $\mathcal{P} = \{\, \alpha \overrightarrow{a} + \beta \overrightarrow{b}\,;\ \alpha,\ \beta > 0\,,\ \overrightarrow{a} \perp \overrightarrow{b}\,\}$ je sebi dualen.

Zgled 3. Naj bo $\mathcal{P}$ stožec iz zgleda 1.1.3. Hitro se lahko prepričamo, da je stožec $\mathcal{P} = \{\, \alpha \overrightarrow{a} + \beta \overrightarrow{b}\,;\ \alpha,\ \beta > 0\,\}$ sebi dualen natanko tedaj, kadar sta vektorja $\overrightarrow{a}$ in $\overrightarrow{b}$ pravokotna drug na drugega.

1.4 Avtomorfizemska grupa

Naj bo Ω odprt konveksen stožec. *Grupa avtomorfizmov* stožca Ω je definirana kot množica

$$G(\Omega) = \{\, g \in GL(\mathcal{W})\,;\ g\,\Omega = \Omega\,\}\,.$$

Tukaj $GL(\mathcal{W})$ označuje grupo obrnljivih linearnih preslikav na prostoru $\mathcal{W}$.

Trditev 4.1 *Preslikava $g \in GL(\mathcal{W})$ je element $G(\Omega)$ natanko takrat, ko je $g\,\overline{\Omega} = \overline{\Omega}$.*

Dokaz: Ker je g zvezna preslikava za katero velja $g\,\Omega = \Omega$, sledi

$$g\,\overline{\Omega} \subset \overline{g\,\Omega} = \overline{\Omega}\,.$$

Ker je g bijekcija, je tudi $g^{-1}\Omega = \Omega$. Zaradi zveznosti g^{-1} sledi

$$g^{-1}\overline{\Omega} \subset \overline{g^{-1}\Omega} = \overline{\Omega}\,.$$

Seveda zaradi bijektivnosti g sledi

$$\overline{\Omega} = g\,g^{-1}\overline{\Omega} \subset g\,\overline{\Omega} \text{ oziroma } g\,\overline{\Omega} = \overline{\Omega}. \qquad \square$$

Grupa avtomorfizmov $G(\Omega)$ je torej zaprta podgrupa grupe $GL(\mathcal{W})$. Odprti stožec Ω imenujemo *homogeni stožec*, če grupa avtomorfizmov deluje nanj *tranzitivno*, tj. $\forall\, x, y \in \Omega$ obstaja tak $g \in G(\Omega)$, da velja $g(x) = y$. Kot bomo videli v nadaljevanju, g ni enolično določen.

Odprti stožec Ω imenujemo *simetričen stožec*, če je homogen in sebi dualen.

Zgled 1. Naj bo $\Omega = \{\, (x, y) \in \mathbb{R}^2\, ;\, x > 0,\, y > 0,\, \frac{b}{a} < \frac{y}{x} < \frac{d}{c}\,\}$, pri čemer sta (a, b), $(c, d) \in \mathbb{R}^2$ takšna, da je $d > b$ in $ad - bc \neq 0$. V zgledu 1.1.3 smo pokazali, da je Ω odprt stožec. Poiščimo njegovo grupo avtomorfizmov. Po definiciji je

$$G(\Omega) = \{\, A \in GL_2(\mathbb{R})\, ;\, A\,\Omega = \Omega\,\}\,.$$

Po trditvi 4.1 ležita $A\,[a, b]^T$ in $A\,[c, d]^T$ na robu stožca Ω. Ker sta $[a, b]^T$ in $[c, d]^T$ baza ravnine in je A obrnljiva, njuni sliki ne moreta ležati na isti premici. Ločimo torej primera:

$$(i)\quad A\begin{bmatrix} a \\ b \end{bmatrix} = k_1 \begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} k_1 a \\ k_1 b \end{bmatrix}, \quad A\begin{bmatrix} c \\ d \end{bmatrix} = k_2 \begin{bmatrix} c \\ d \end{bmatrix} = \begin{bmatrix} k_2 c \\ k_2 d \end{bmatrix},$$

$$k_1, k_2 > 0 \;\Rightarrow$$

$$A\begin{bmatrix} a & c \\ b & d \end{bmatrix} = \begin{bmatrix} k_1 a & k_2 c \\ k_1 b & k_2 d \end{bmatrix} \;\Rightarrow\; A = \begin{bmatrix} k_1 a & k_2 c \\ k_1 b & k_2 d \end{bmatrix}\begin{bmatrix} a & c \\ b & d \end{bmatrix}^{-1} \;\Rightarrow$$

$$A = \frac{1}{ad - bc}\begin{bmatrix} k_1 a & k_2 c \\ k_1 b & k_2 d \end{bmatrix}\begin{bmatrix} d & -c \\ -b & a \end{bmatrix} \;\Rightarrow$$

$$A = \frac{1}{ad - bc}\begin{bmatrix} k_1 ad - k_2 bc & (k_2 - k_1)ac \\ (k_1 - k_2)bd & k_2 ad - k_1 bc \end{bmatrix} =: A_i\,.$$

$$(ii)\quad A\begin{bmatrix} a \\ b \end{bmatrix} = k_1 \begin{bmatrix} c \\ d \end{bmatrix} = \begin{bmatrix} k_1 c \\ k_1 d \end{bmatrix}, \quad A\begin{bmatrix} c \\ d \end{bmatrix} = k_2 \begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} k_2 a \\ k_2 b \end{bmatrix},$$

$$k_1, k_2 > 0 \;\Rightarrow$$

$$A\begin{bmatrix} a & c \\ b & d \end{bmatrix} = \begin{bmatrix} k_1 c & k_2 a \\ k_1 d & k_2 b \end{bmatrix} \;\Rightarrow\; A = \begin{bmatrix} k_1 c & k_2 a \\ k_1 d & k_2 b \end{bmatrix}\begin{bmatrix} a & c \\ b & d \end{bmatrix}^{-1} \;\Rightarrow$$

$$A = \frac{1}{ad - bc}\begin{bmatrix} k_1 c & k_2 a \\ k_1 d & k_2 b \end{bmatrix}\begin{bmatrix} d & -c \\ -b & a \end{bmatrix} \;\Rightarrow$$

$$A = \frac{1}{ad-bc}\begin{bmatrix} k_1cd - k_2ab & k_2a^2 - k_1c^2 \\ k_2d^2 - k_1b^2 & k_2ab - k_1cd \end{bmatrix} =: A_j\,.$$

Množica $\{\, A_i,\ A_j;\ k_1, k_2 > 0 \,\}$ je torej grupa avtomorfizmov stožca Ω.

Zgled 2. Oglejmo si poseben primer stožca Ω iz prejšnjega zgleda. Naj bo $(a,b) = (1,0)$ in $(c,d) = (1,1)$. Grupa avtomorfizmov $G(\Omega)$ je potem generirana z matrikami oblike

$$A_i = \begin{bmatrix} k_1 & k_2 - k_1 \\ 0 & k_2 \end{bmatrix} \quad \text{in} \quad A_j = \begin{bmatrix} k_1 & k_2 - k_1 \\ k_2 & -k_1 \end{bmatrix}\,,\ k_1, k_2 > 0\,.$$

Ali grupa $G(\Omega)$ deluje na stožcu Ω tranzitivno? Preveriti zadošča, ali za poljubna $(x,y),(u,v) \in \Omega$ obstaja tak $A \in G(\Omega)$, da velja $A[x,y]^T = [u,v]^T$. Ker sta $(x,y),(u,v) \in \Omega$ velja $0 < y < x$ in $0 < v < u$. Ločimo primera:

$$(i)\quad \begin{bmatrix} k_1 & k_2 - k_1 \\ 0 & k_2 \end{bmatrix}\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} u \\ v \end{bmatrix} \quad \Rightarrow \begin{bmatrix} k_1(x-y) + k_2y \\ k_2y \end{bmatrix} = \begin{bmatrix} u \\ v \end{bmatrix}$$

$$\Rightarrow \quad k_2 := \frac{v}{y} \quad \text{in} \quad k_1 = \frac{u-v}{x-y}\,.$$

$$(ii)\quad \begin{bmatrix} k_1 & k_2 - k_1 \\ k_2 & -k_1 \end{bmatrix}\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} u \\ v \end{bmatrix} \quad \Rightarrow \begin{bmatrix} k_1(x-y) + k_2y \\ k_2x - k_1y \end{bmatrix} = \begin{bmatrix} u \\ v \end{bmatrix}$$

$$\Rightarrow \quad k_1 := \frac{xu - yv}{x^2 - xy + y^2} \quad \text{in} \quad k_2 = \frac{v + k_1y}{x}\,.$$

Ker grupa $G(\Omega)$ deluje tranzitivno, je stožec Ω po definiciji homogen. Ker Ω ni sebi dualen, očitno ni simetričen. Obstajajo torej homogeni nesimetrični stožci.

Zgled 3. Naj bo Ω stožec iz zgleda 1.4.1, pri čemer je $(a,b) = (1,0)$ in $(c,d) = (0,1)$. Pripadajoča grupa avtomorfizmov je generirana z matrikama oblike

$$A_i = \begin{bmatrix} k_1 & 0 \\ 0 & k_2 \end{bmatrix} \quad \text{in} \quad A_j = \begin{bmatrix} 0 & k_2 \\ k_2 & 0 \end{bmatrix}\,,\ k_1, k_2 > 0\,.$$

Podobno kot v prejšnjem zgledu se prepričamo, da $G(\Omega)$ deluje na Ω tranzitivno. Ker je Ω sebi dualen, po definiciji sledi, da je Ω simetričen stožec.

Trditev 4.2. *Za poljuben pravi odprt konveksen stožec* Ω *velja*

$$G(\Omega^*) = G(\Omega)^* .$$

Če je $\Omega = \Omega^*$, *potem za vsak* $g \in G(\Omega)$ *velja* $g^* \in G(\Omega)$.

Dokaz: Naj bosta $g \in G(\Omega)$ in $y \in \Omega^*$. Ker za vsak neničelen $x \in \overline{\Omega}$ velja

$$\langle\, g(x), y\,\rangle > 0\,,$$

zaradi $\langle\, g(x), y\,\rangle = \langle\, x, g^*(y)\,\rangle$, sledi $g^*\Omega^* \subset \Omega^*$. Analogno zaradi bijektivnosti g sledi tudi $(g^{-1})^*\Omega^* = (g^*)^{-1}\Omega^* \subset \Omega^*$. Od tod sledi $g^* \in G(\Omega^*)$, oziroma $G(\Omega)^* \subset G(\Omega^*)$. Če dokaz ponovimo za $g \in G(\Omega^*)$, analogno dobimo $G(\Omega^*)^* \subset G(\Omega^{**})$. Ker je Ω pravi, ima po trditvi 3.5 neprazno notranjost ter po trditvi 3.2 velja $\Omega^{**} = \Omega$. Od tod sledi $G(\Omega^*)^* \subset G(\Omega)$, oziroma $G(\Omega^*) = G(\Omega)^*$. □

Odprt stožec smo proglasili za simetričen, če je homogen in hkrati sebi dualen. Po kratkem premisleku, z upoštevanjem zgornje trditve ugotovimo, da homogen pravi in odprt stožec z lastnostjo $G(\Omega)^* = G(\Omega)$ prav tako karakterizira simetrični stožec.

Naj grupa avtomorfizmov $G(\Omega)$ deluje na odprtem konveksnem stožcu Ω. Za $x \in \Omega$ definirajmo množico

$$G_x = \{\, g(x)\,;\, g \in G(\Omega)\,\}\,,$$

in jo imenujmo *orbita elementa* x. Če na stožcu Ω definiramo relacijo s predpisom

$$x \sim y \iff y \in G_x\,,$$

je $\sim$ ekvivalenčna relacija, ki stožec Ω razdeli na ekvivalenčne razrede. Ekvivalenčne razrede imenujemo *orbite delovanja.* V zgornjem smislu je odprti stožec Ω homogen, tj. grupa avtomorfizmov deluje na stožcu Ω tranzitivno, če je orbita delovanja ena sama.

Poljubni točki $a \in \Omega$ priredimo množico

$$G(\Omega)_a = \{\, g \in G(\Omega)\,;\, g(a) = a\,\}$$

in jo imenujmo *stabilizator* točke a v $G(\Omega)$.

Trditev 4.3. *Če je* Ω *pravi odprt konveksen stožec, potem za vsak* $a \in \Omega$ *velja, da je stabilizator* $G(\Omega)_a$ *kompaktna množica znotraj* $GL(\mathcal{W})$.

Dokaz: Naj bo Ω pravi odprt konveksen stožec. Pokažimo najprej, da je množica $\Omega\cap(\,a-\Omega\,)$ omejena. Naj bo $y\in\Omega^*$ in $x\in\Omega\cap(\,a-\Omega\,)$. Potem lahko pišemo $x=v=a-w$, pri čemer sta $v,w\in\Omega$. Po definiciji duala, za v in w velja $\langle\,y,v\,\rangle>0$ in $\langle\,y,w\,\rangle>0$. Očitno je $\langle\,x,y\,\rangle=\langle\,v,y\,\rangle>0$. Ker velja $\langle\,x,y\,\rangle=\langle\,a,y\,\rangle-\langle\,w,y\,\rangle$, ob upoštevanju $\langle\,a,y\,\rangle=\alpha$, sledi $\langle\,x,y\,\rangle=\alpha-\langle\,w,y\,\rangle\leq\alpha$ in od tod

$$\Omega\cap(\,a-\Omega\,)\subseteq\{\,x\in\overline{\Omega}\,;\,\langle\,x,y\,\rangle\leq\alpha\,\}=\alpha\,\{\,x\in\overline{\Omega}\,;\,\langle\,x,y\,\rangle\leq 1\,\}\,.$$

Ker je po trditvi 3.7 množica $\{\,x\in\overline{\Omega}\,;\,\langle\,x,y\,\rangle\leq 1\}$ omejena, je takšna tudi $\alpha\,\{\,x\in\Omega\,;\,\langle\,x,y\,\rangle\leq 1\,\}$. Ker sta Ω in $a-\Omega$ odprti, je odprta tudi $\Omega\cap(\,a-\Omega\,)$. Ker je $\frac{1}{2}a\in\Omega\cap(\,a-\Omega\,)$, je očitno tudi neprazna. Po definiciji stabilizatorja elementa a, $G(\Omega)_a$ ohranja množico $\Omega\cap(\,a-\Omega\,)$. Ker $\Omega\cap(\,a-\Omega\,)$ vsebuje neko bazo prostora $\mathcal{W}$, sledi, da za vsak $g\in G(\Omega)_a$ in $x\in\mathcal{W}$, obstaja taka konstanta c, da velja

$$\tfrac{1}{c}\,||\,x\,||\leq||\,g(x)\,||\leq c\,||\,x\,||\,.$$

Torej je $\frac{1}{c}\leq||\,g\,||\leq c$, za vsak $g\in G(\Omega)_a$. To pomeni, da je $G(\Omega)_a$ omejena znotraj $GL(\mathcal{W})$. Ker je $G(\Omega)_a$ praslika ničle zvezne preslikave $\phi(g)=g(a)-a$, je očitno tudi zaprta znotraj $GL(\mathcal{W})$ in zato kompaktna. $\square$

Zgled 4. Množica $\Omega=\mathbb{R}^+$ je primer stožca v $\mathbb{R}^2$, ki ni pravi. Grupa matrik oblike

$$\begin{bmatrix}1 & 0\\ 0 & z\end{bmatrix},$$

kjer je $z\in\mathbb{R}$, očitno ohranja element $a=(\,1,0\,)$. Za vsak $g\in G$ namreč velja $g(a)=a$. To pomeni, da je grupa G vsebovana v stabilizatorju točke a. Ker je G neomejena in velja $G\subseteq G(\Omega)_a$, je očitno neomejena tudi $G(\Omega)_a$. To pomeni, da $G(\Omega)_a$ ni kompaktna.

Trditev 4.4. *Naj bo H kompaktna podgrupa $G(\Omega)$. Potem obstaja tak $a\in\Omega$, da je $H\subset G(\Omega)_a$.*

Dokaz: Ker je $H\subset G(\Omega)$ lokalno kompaktna grupa, po izreku 2.10 [Faraut, 1994, str. 37] na H obstaja Haarova mera μ, to je neničelna Radonova mera, za katero velja

$$\mu(uE)=\mu(E)\ \text{ in }\mu(H)=1\,,$$

kjer je $u \in H$ in E Borelova podmnožica H. Naj bo $x_0 \in \Omega$ in $y \in \Omega^*$. Definirajmo preslikavo

$$\phi \,:\, H \longrightarrow \mathbb{R}^+ \,,$$

s predpisom

$$\phi(h) = \langle\, h(x_0), y \,\rangle \,.$$

Ker je $h(x_0) \in \Omega$ in $y \in \Omega^*$ sledi, da je $\langle\, h(x_0), y \,\rangle > 0$. To pomeni, da je ϕ pozitivna in zvezna funkcija na H, oziroma velja $\phi(h) \geq \epsilon > 0$. Od tod sledi

$$\int_H \phi(h)dh \geq \epsilon \cdot \int_H dh = \epsilon\, \mu(H) = \epsilon > 0 \,,$$

kjer je dh Haarova mera na H. Za poljuben $x_0 \in \Omega$ definirajmo

$$a = \int_H h(x_0)dh \,.$$

Ker je integral na desni, po trditvi 2.9 [Faraut, 1994, str. 36], invarianten za poljuben $h \in H$, je a fiksen glede na H. Ker za vsak $y \in \Omega^*$ velja

$$\begin{aligned} \langle\, a, y \,\rangle &= \langle \int_H h(x_0)dh, y \,\rangle = \int_H \langle\, h(x_0)dh, y \,\rangle \\ &= \int_H \langle\, h(x_0), y \,\rangle\, dh = \int_H \phi(h)dh > 0 \,, \end{aligned}$$

sledi, da je $a \in \Omega$. □

Trditev 4.5. *Če je Ω homogen stožec, so vse podgrupe $G(\Omega)_x$, $x \in \Omega$, izomorfne.*

Dokaz: Naj bosta a in $b \in \Omega$. Pripadajoča stabilizatorja sta množici

$$G(\Omega)_a = \{\, g \in G(\Omega)\,;\, g(a) = a \,\}$$

in

$$G(\Omega)_b = \{\, g \in G(\Omega)\,;\, g(b) = b \,\} \,.$$

Zaradi homogenosti Ω, obstaja tak $g_0 \in G(\Omega)$, da je $g_0(a) = b$. Definirajmo preslikavo

$$\phi \,:\, G(\Omega)_a \longrightarrow G(\Omega)_b$$

podano s predpisom $\phi(g) = g_0 g g_0^{-1}$. Ker velja

$$\phi(g)(b) = g_0 g g_0^{-1}(b) = g_0 g(a) = g_0(a) = b\,,$$

je ϕ dobro definirana. Ker velja tudi

$$\phi(gh) = g_0(gh)g_0^{-1} = g_0 g g_0^{-1}\, g_0 h g_0^{-1} = \phi(g)\,\phi(h)\,,$$

je ϕ homomorfizem. Preslikava, podana s predpisom

$$\phi^{-1}(h) = g_0^{-1} h g_0$$

je očitno inverz preslikave ϕ, ki je tako izomorfizem med $G(\Omega)_a$ in $G(\Omega)_b$. $\square$

2 Lorentzovi stožci

2.1 Posebna teorija relativnosti

Z zakoni klasične fizike v svetu makroskopskih teles shajamo vse dokler se ne soočimo: z opisi pojavov pri katerih postane hitrost teles precej večja, kot je sicer običajno hitrost velikih teles, z opisovanjem elektronov, atomskih jeder, atomov, molekul in pojavov, pri katerih sodeluje le majhno število le-teh ter opisi pojavov, kjer je gravitacijsko polje takšno, da njegov vpliv ni zanemarljiv. Omenjene težave so fizikom dale pobudo za posplošitev zakonov Newtonove mehanike in Maxwellove elektrodinamike na področja, na katerih ti zakoni ne veljajo. Posplošitev Newtonove mehanike na hitre delce je tako privedla do posebne teorije relativnosti, posplošitev klasične fizike na majhne delce do kvantne fizike in posplošitev Newtonove mehanike in gravitacijskega zakona do splošne teorije relativnosti.

Razvoj klasične fizike je potekal predvsem na osnovi opazovanja in opisovanja pojavov. Po opravljenem poskusu je sledila analiza rezultatov in oblikovanje zakona. Z vplivanjem na okoliščine v katerih je poskus potekal je iz zakona sledilo oblikovanje izrekov in enačb, ki podajajo odvisnosti med opazovanimi količinami. V moderni fiziki je poskuse le težko izvajati in zato še težje vplivati na okoliščine v katerih potekajo. Razvoj v moderni fiziki zatorej poteka nekoliko drugače. Že ob samem začetku obravnave kakega problema postavimo trditve, imenovane tudi načela, ki niso v nasprotju z rezultati poskusov. Iz načel nato izpeljemo zakone, iz zakonov pa izreke in enačbe. Dobljeno teorijo naposled sprejmemo za veljavno, če se izreki in enačbe ujemajo z rezultati poskusov.

Temeljni načeli posebne teorije relativnosti je leta 1905 s člankom Zur Elektrodynamik bewegter Kőrper, oblikoval Albert Einstein. Galilejevo načelo relativnosti, ki je zajemalo le mehanične pojave, je razširil tudi na elektromagnetne pojave in s tem dobil načelo relativnosti. Na osnovi načela relativnosti so vsi nepospešeni opazovalni sistemi enakopravni in tako enako uporabni za opisovanje vseh fizikalnih pojavov, ki potekajo v njih. Načelu relativnosti je dodal še načelo o hitrosti svetlobe, ki pravi, da je hitrost svetlobe v praznem prostoru v vseh nepospešenih opazovalnih sistemih enaka. Čeprav ju Einstein ni navedel kot osnovni načeli, posebna teorija relativnosti privzame še načeli o homogenosti časa ter homogenosti in izotropnosti prostora. Prvo pravi, da ima čas enake lastnosti, kot jih je imel v preteklosti in jih bo imel tudi v prihodnosti. Drugo načelo isto lastnost priredi tudi prostoru ter doda, da ima prostor enake lastnosti v izbrani smeri, kot tudi v drugih smereh.

Nova načela so predstavljala pobudo za uvedbo nove transformacije, s katero podamo koordinate in čas v nepospešenem opazovalnem sistemu S', če poznamo koordinate in čas v nepospešenem koordinatnem sistemu S. Čeprav je izhodišče oblikovanja nove transformacije predstavljala Galilejeva transformacija, ki je uspešna pri opisovanju gibanj teles z majhnimi hitrostmi, se je Einstein uprl na ugotovitve Hendrika Antoona Lorentza. Njegovo transformacijo je Einstein izpopolnil, do danes znane *Lorentzove transformacije*

$$\begin{aligned}
t' &= \gamma_0 \left(t - \frac{v_0 x}{c_0} \right) \\
x' &= \gamma_0 \left(x - v_0 t \right) \\
y' &= y \\
z' &= z \,,
\end{aligned}$$

kjer je v_0 hitrost opazovalnega sistema S' glede na sistem S, koeficient γ_0 pa določa enačba

$$\gamma_0 = \sqrt{1 - \frac{v_0^2}{c_0^2}} \,.$$

Lorentzova transformacija s svojimi enačbami podaja novo pojmovanje prostora in časa. Ugotovitev, da se poleg transformiranja koordinat, transformira tudi čas, napeljuje na definiranje novega pojma. *Dogodek* je izbran trenutni pojav v neki točki, ki ga določajo štirje podatki: tri koordinate x, y in z ter čas t. Lorentzova transformacija torej dogodku x, y, z, t v nepospešenem opazovalnem sistemu S priredi dogodek x', y', z', t' v nepospešenem opazovalnem sistemu S'.

2.2 Prostor–čas Minkowskega

Ker v Lorentzovi transformaciji čas ne nastopa več kot zunanji parameter, ga je smiselno obravnavati kot novo, četrto koordinato. Za obravnavo posebne teorije relativnosti je torej pripraven štiridimenzionalen prostor, v katerem poleg običajnih koordinatnih osi x, y in z nastopa še četrta koordinata $c_0 t$. Čeprav je osnovne zamisli o štiridimenzionalnem prostoru podal že Albert Einstein, je njegovo današnjo podobo leta 1908 izoblikoval nemško - poljski matematik Hermann Minkowski.

Prostor–čas Minkowskega je torej definiran kot štiridimenzionalen realen vektorski prostor $\mathcal{M}$, pri čemer točkam tega prostora ustrezajo dogodki. Dogodku ct, x, y, z v prostoru $\mathcal{M}$ priredimo *štiridimenzionalni vektor* ali *četverec*:

$$x = (\, x_1, x_2, x_3, x_4 \,)\,,$$

pri čemer komponenta $(\, x_1 \,)$ ustreza časovni komponenti četverca, $(\, x_2, x_3, x_4 \,)$ pa krajevni komponenti četverca.

Medtem, ko za seštevanje in odštevanje četvercev, ter njihovo množenje s skalarjem, veljajo pravila, ki so posplošitev pravil za računanje s trirazsežnimi vektorji, zaradi načela o homogenosti in izotropnosti prostora $\mathcal{M}$, skalarnega produkta ne moremo vpeljati na običajen način.

Skalarni produkt v $\mathcal{M}$ definiramo s predpisom

$$g(v, w) = v_1 w_1 - v_2 w_2 - v_3 w_3 - v_4 w_4\,,$$

in ga imenujemo *Lorentov skalarni produkt.* Posebej bomo označevali $\mathcal{Q}(v) = g(v, v)$. Lorentzov skalarni produkt očitno ni pozitivno definiten. V prostoru $\mathcal{M}$ namreč obstajajo neničelni vektorji v, za katere velja $\mathcal{Q}(v) = g(v, v) = 0$. Vektor $v = e_1 + e_4$ je očitno takšen. Zanj namreč velja: $g(v, v) = \mathcal{Q}(e_1) - 2g(e_1, e_4) + \mathcal{Q}(e_4) = 1 - 0 - 1 = 0$. Neničelne vektorje v, prostora $\mathcal{M}$, za katere velja $g(v, v) = 0$ imenujemo *ničelni* ali *svetlobni vektorji.* Smisel takšnega poimenovanja bo razviden v nadaljevanju.

Vektor v prostora $\mathcal{M}$, za katerega je $\mathcal{Q}(v)$ enak 1 ali -1, imenujemo *enotski vektor* prostora $\mathcal{M}$. Bazo $\{\, e_1, e_2, e_3, e_4 \,\}$ prostora $\mathcal{M}$, med seboj ortogonalnih enotskih vektorjev imenujemo *ortonormirana baza* prostora $\mathcal{M}$.

Ob kratkem premisleku se nam zastavi vprašanje ali obstaja baza ničelnih vektorjev prostora $\mathcal{M}$. Naslednji zgled nas prepriča v obstoj takšne baze.

Zgled 1. Naj bodo $u = e_1 + e_2$, $v = e_1 + e_3$, $w = e_1 + e_4$ in $z = e_1 - e_2$. Ker velja $\mathcal{Q}(u) = \mathcal{Q}(v) = \mathcal{Q}(w) = \mathcal{Q}(z) = 0$, so u, v, w in z ničelni vektorji prostora $\mathcal{M}$. Hitro se lahko prepričamo, da so u, v, w in z tudi linearno neodvisni in zato predstavljajo ničelno bazo prostora $\mathcal{M}$.

Seveda pa ne obstaja ničelna baza prostora $\mathcal{M}$, katere bazni vektorji bi bili paroma ortogonalni. Velja namreč

Izrek 2.1 *Ničelna vektorja v in $w \in \mathcal{M}$ sta ortogonalna natanko takrat, kadar sta vzporedna, tj. ko obstaja tak $t \in \mathbb{R}$, da velja $v = tw$.*

Dokaz: Vektorja x in $y \in \mathcal{M}$ zapišimo v obliki $v = \alpha + x$ in $w = \beta + y$, kjer sta α in β časovni, x in y pa krajevni komponenti pripadajočih četvercev. Po definiciji Lorentzovega produkta sledi

$$g(v, v) = \alpha^2 - \langle x, x \rangle ,$$

$$g(w, w) = \beta^2 - \langle y, y \rangle ,$$

pri čemer je $\langle .,. \rangle$ običajni skalarni produkt. Ker sta v in w po predpostavki ničelna vektorja, sledi $\alpha = \pm|| x ||$ in $\beta = \pm|| y ||$. Zaradi ortogonalnosti v in w velja

$$0 = g(v, w) = g(\alpha + x, \beta + y) = \alpha\beta - \langle x, y \rangle = \pm|| x || \cdot || y || - \langle x, y \rangle .$$

Ker je $|| x || \cdot || y || = | \langle x, y \rangle |$, po Cauchy - Schwarzu sledi $y = tx$, za nek $t \in \mathbb{R}$. Ločimo primera

(i) $v = || x || + x \, , \; w = t \, || x || \pm tx \, .$
Ker je $g(v, w) = t \, || x ||^2 \mp t \, \langle x, x \rangle = (t \mp t) \, || x ||^2 = 0 \, ,$ sledi
$w = t \, || x || + tx = t \, (|| x || + x) = tv.$

(ii) $v = || x || - x \, , \; w = t \, || x || \pm tx \, .$
Ker je $g(v, w) = t \, || x ||^2 \pm t \, \langle x, x \rangle = (t \pm t) \, || x ||^2 = 0 \, ,$ sledi
$w = t \, || x || - tx = t \, (|| x || - x) = tv.$

Dokaz implikacije v nasprotni smeri je očiten. Če je namreč $v = tw$, sledi

$$g(v, w) = g(tw, w) = t\, g(w, w) = 0\,,$$

zaradi ničelnost vektorja w. $\square$

V nadaljevanju si nekoliko podrobneje oglejmo zvezo med poljubnima dogodkoma. Naj bosta x in x_0 takšna različna dogodka, da je vektor $v = x - x_0$, med dogodkoma x_0 in x, ničelen oziroma svetloben. Fiziki za taka dogodka pravijo, da sta v razmiku *svetlobnega tipa*. Ob upoštevanju načela vzročnosti (učinek sledi v času svojemu vzroku), bi zanju veljalo: če dogodek x ustreza izsevanju bliska v dani točki (vzrok), potem dogodek x_0 ustreza sprejetju bliska v neki drugi točki (učinek). Če dogodkoma x in x_0 v poljubni ortonormirani bazi prostora $\mathcal{M}$, priredimo pripadajoča četverca $x = (\, x_1, x_2, x_3, x_4\,)$ in $x_0 = (\, x_{10}, x_{20}, x_{30}, x_{40}\,)$, sledi

$$(\, x_1 - x_{10}\,)^2 - (\, x_2 - x_{20}\,)^2 - (\, x_3 - x_{30}\,)^2 - (\, x_4 - x_{40})^2 = 0\,.$$

Zaradi podobnosti zgornje enačbe z enačbo stožca v $\mathbb{R}^3$, imenujemo množico, definirano s predpisom

$$\mathcal{P}_S(x_0) = \{\, x \in \mathcal{M}\,;\ \mathcal{Q}(x - x_0) = 0\,\}$$

svetlobni ali *ničelni stožec* prostora $\mathcal{M}$ v točki x_0. Stožec $\mathcal{P}_S(x_0)$ torej vsebuje vse tiste dogodke prostora $\mathcal{M}$, ki so s svetlobo vzročno povezani z dogodkom x_0. Dogodku $x \in \mathcal{M}$, ki je s svetlobo vzročno povezan z dogodkom x_0, priredimo *svetlobni žarek*. Svetlobni žarek, prirejen dogodkoma x in x_0 je definiran s predpisom

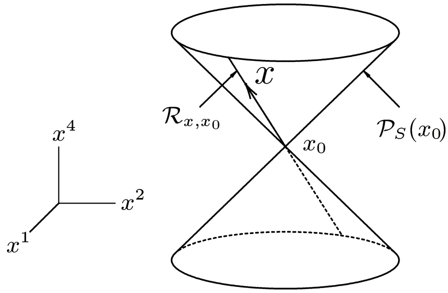
$$\mathcal{R}_{x,x_0} = \{\, x_0 + t\,(x - x_0)\,;\ t \in \mathbb{R}\,\}\,.$$

Opomba: Na sliki svetlobnega stožca $\mathcal{P}_S(x_0)$, je krajevni komponenti x^3 prirejena vrednost 0.

Trditev 2.2. *Če je $\mathcal{Q}(x - x_0) = 0$, potem velja*

$$\mathcal{R}_{x,x_0} = \mathcal{R}_{x_0,x}\,.$$

Dokaz: Naj bo $v \in \mathcal{R}_{x,x_0}$. Obstaja torej tak $t \in \mathbb{R}$, da velja $v = x + t\,(x_0 - x)$, oziroma $v - x = t\,(x_0 - x)$. Ker je $\mathcal{Q}(v - x) = \mathcal{Q}(t\,(x_0 - x)) = t^2\, \mathcal{Q}(x_0 - x) = 0$, obstaja tak $k \in \mathbb{R}$, da je $0 = k^2\, \mathcal{Q}(x - x_0) =$



Svetlobni stožec $\mathcal{P}_S(x_0)$

$\mathcal{Q}(k\,(x-x_0)) = \mathcal{Q}(v-x_0)$. Od tod sledi $v-x_0 = k\,(x-x_0)$, oziroma $v = x_0 + k\,(x-x_0) \in \mathcal{R}_{x_0,x}$.

Obratno inkluzijo dobimo z zamenjavo vloge elementov x in x_0. □

Svetlobni stožec je torej unija svetlobnih žarkov prirejenih dogodku x_0.

Izrek 2.3. *Naj bosta x in x_0 različna dogodka, za katera velja $\mathcal{Q}(x-x_0) = 0$. Potem velja*

$$\mathcal{R}_{x_0,x} = \mathcal{P}_S(x_0) \cap \mathcal{P}_S(x)\,.$$

Dokaz: Naj bo $z = x_0 + t\,(x-x_0) \in \mathcal{R}_{x_0,x}$. Ker je $z - x_0 = t\,(x-x_0)$ in $\mathcal{Q}(x-x_0) = 0$, sledi $z \in \mathcal{P}_S(x_0)$. Analogno je, po trditvi 2.2., $z \in \mathcal{P}_S(x)$. Sledi torej $z \in \mathcal{P}_S(x_0) \cap \mathcal{P}_S(x)$, oziroma $\mathcal{R}_{x_0,x} \subseteq \mathcal{P}_S(x_0) \cap \mathcal{P}_S(x)$.

Naj bo $z \in \mathcal{P}_S(x_0) \cap \mathcal{P}_S(x)$. Potem so vektorji $z-x$, $z-x_0$ in $x-x_0$ ničelni, tj. $\mathcal{Q}(z-x) = \mathcal{Q}(z-x_0) = \mathcal{Q}(x-x_0) = 0$. Ker je $z-x_0 = (z-x)-(x_0-x)$, velja $0 = \mathcal{Q}(z-x_0) = \mathcal{Q}(z-x) - 2g(z-x, x_0-x) + \mathcal{Q}(x_0-x) = -2g(z-x, x_0-x)$. Če je $z = x$, sledi $z \in \mathcal{R}_{x_0,x}$. Če pa $z \neq x$, zaradi ortogonalnosti $z-x$ in x_0-x, po izreku 2.1., obstaja tak $t \in \mathbb{R}$, da velja $z - x = t\,(x_0-x)$. Od tod sledi $z = x + t\,(x_0-x) \in \mathcal{R}_{x_0,x}$, oziroma $\mathcal{P}_S(x_0) \cap \mathcal{P}_S(x) \subseteq \mathcal{R}_{x_0,x}$. □

Oglejmo si sedaj še poljubna dogodka x in x_0, za katera velja $\mathcal{Q}(x-x_0) > 0$ ali $\mathcal{Q}(x-x_0) < 0$.

Če za dogodka x in x_0 velja $\mathcal{Q}(x-x_0) > 0$, pravimo, da sta v razmiku *časovnega tipa*. Taka dogodka sta lahko vzročno povezana s pojavom, ki potuje počasneje kot svetloba. Prvi dogodek ustreza na primer prehodu delca mimo dane točke (vzrok), drugi pa prehodu delca mimo druge točke (učinek).

Če za dogodka x in x_0 velja $\mathcal{Q}(x - x_0) < 0$, pravimo, da sta v razmiku *krajevnega tipa*. Taka dogodka ne moreta biti vzročno povezana, saj bi zanju veljalo, da se v danem trenutku zgodita v različnih točkah. Do danes pojava, ki bi bil hitrejši kot je svetloba še nismo spoznali.

Izrek 2.4. *Naj bo $v = \alpha + x$ vektor časovnega tipa in $w = \beta + y$ vektor svetlobnega ali časovnega tipa; α in β sta pri tem časovni, x in y pa krajevni komponenti četverca. Potem velja ena od možnosti*

$$(i)\ \ \alpha\,\beta > 0\,,\ \ \textit{od koder sledi } g(v,w) > 0 \ \ \text{ali}$$
$$(ii)\ \ \alpha\,\beta < 0\,,\ \ \textit{od koder sledi } g(v,w) < 0\,.$$

Dokaz: Po predpostavki je $g(v,v) = \alpha^2 - \langle\, x, x\,\rangle > 0$ in $g(w,w) = \beta^2 - \langle\, y, y\,\rangle \geq 0$. Ker je $\alpha^2 > \langle\, x, x\,\rangle$ in $\beta^2 \geq \langle\, y, y\,\rangle$ sledi $(\,\alpha\beta\,)^2 > \langle\, x, x\,\rangle\langle\, y, y\,\rangle \ \geq\ \langle\, x, y\,\rangle^2$. Od tod sledi $|\,\alpha\beta\,| > |\,\langle\, x, y\,\rangle\,|$, oziroma $\alpha\beta \neq 0$. Denimo, da je $\alpha\beta > 0$. Potem je $\alpha\beta = |\,\alpha\beta\,| > |\,\langle\, x, y\,\rangle\,| \geq \langle\, x, y\,\rangle$. Od tod sledi $g(v,w) = \alpha\beta - \langle\, x, y\,\rangle > 0$. Po drugi strani za $\alpha\beta < 0$ velja $-\alpha\beta = |\,\alpha\beta\,| > |\,\langle\, x, y\,\rangle\,| \geq -\langle\, x, y\,\rangle$. Ker je $g(v,w) = \alpha\beta - \langle\, x, y\,\rangle < 0$, sledi $g(v,w) < 0$. □

Posledica 2.5. *Naj bo $v = \alpha + x$ od nič različen vektor. Denimo, da je pravokoten na vektor $w = \beta + y$, ki je časovnega tipa. Potem je v krajevnega tipa.*

Dokaz: Vektor v je lahko časovnega, svetlobnega ali krajevnega tipa. Če je v časovnega ali svetlobnega tipa, po izreku 2.4 sledi, da je $g(v,w) \neq 0$. Ker je po predpostavki $g(v,w) = 0$, preostane le tretja možnost. Vektor v je krajevnega tipa. □

Označimo z τ množico vseh vektorjev časovnega tipa prostora $\mathcal{M}$. Na množici τ definirajmo relacijo $\sim$ s predpisom

$$u, v \in \tau \ :\ u \sim v \iff g(u,v) > 0\,.$$

Pokažimo, da je $\sim$ ekvivalenčna relacija, ki podprostor vseh vektorjev časovnega tipa razdeli na dva ekvivalenčna razreda.

- refleksivnost : sledi iz definicije časovnosti

- simetričnost: sledi iz simetričnosti Lorentzovega produkta
- tranzitivnost: Naj bo $v \sim w$ in $w \sim u$. Pišimo $v = x + \alpha$, $v = y + \beta$ in $u = z + \gamma$. Ker je $v \sim w$, po definiciji sledi $\langle x, y \rangle < \alpha\beta$ in $-\langle x, y \rangle < |\alpha\beta|$. Od tod sledi $0 < \alpha\beta + |\alpha\beta|$, oziroma $\alpha\beta > 0$. Po analognem sklepu dobimo $\beta\gamma > 0$. Ker imajo α in β ter β in γ paroma iste predznake sledi, da imata tudi α in γ isti predznak. Velja torej $\alpha\gamma > 0$. Ker je $\langle x, z \rangle \leq ||x|| \cdot ||y|| < |\alpha||\gamma| = |\alpha\gamma| = \alpha\gamma$, sledi $v \sim u$.

Vektorja $v = 1 + 0$ in $w = -1 + 0$ sta očitno časovnega tipa. Ker je $g(v, w) = -1 < 0$, velja $0 + 1 \not\sim 0 - 1$. To pa pomeni, da sta ekvivalenčna razreda, na katera $\sim$ razdeli prostor $\mathcal{M}$, vsaj dva.

Naj bodo u, v in w vektorji časovnega tipa. Denimo, da ležijo v različnih ekvivalenčnih razredih. Njihove časovne komponente so potem bodisi pozitivne bodisi negativne. Ker so vektorji trije, se vsaj dva (naprimer u in v) ujemata v predznaku časovne komponente. Po izreku 2.4 je tedaj $g(u, v) > 0$, kar je v protislovju s predpostavko, da u in v ležita v različnih razredih.

Ekvivalenčni razred časovnih vektorjev s pozitivno časovno komponento označimo s τ^+, razred z negativno časovno komponento pa s τ^-. Za vsak $x_0 \in \mathcal{M}$ definirajmo množice

$$\mathcal{P}_T(x_0) = \{ x \in \mathcal{M} \,;\, \mathcal{Q}(x - x_0) > 0 \},$$

$$\mathcal{P}_T^+(x_0) = \{ x \,;\, x - x_0 \in \tau^+ \} = \mathcal{P}_T(x_0) \cap \tau^+,$$

$$\mathcal{P}_T^-(x_0) = \{ x \,;\, x - x_0 \in \tau^- \} = \mathcal{P}_T(x_0) \cap \tau^-$$

in dokažimo naslednjo

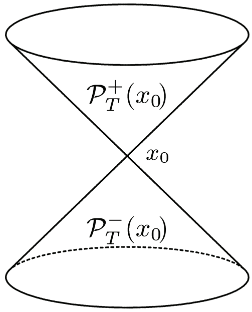
Trditev 2.6. *Množica $\mathcal{P}_T^+(x_0)$ je konveksni stožec glede na x_0, oziroma $\mathcal{P}_T^+(0)$ je konveksni stožec v običajnem smislu.*

Dokaz: Ker je $\mathcal{P}_T^+(0) = \{ \alpha + x \,;\, ||x|| < \alpha \}$, za poljuben pozitiven λ velja

$$||\lambda x|| = \lambda ||x|| < \lambda\alpha.$$

Torej je $\lambda\alpha + \lambda x \in \mathcal{P}_T^+(0)$. Če sta $\alpha + x$ in $\beta + y \in \mathcal{P}_T^+(0)$, velja $||x|| < \alpha$ in $||y|| < \beta$. To pomeni, da je

$$||x + y|| \leq ||x|| + ||y|| < \alpha + \beta,$$



Časovni stožec $\mathcal{P}_T(x_0)$

od koder sledi $(\alpha+\beta)+(x+y)=(\alpha+x)+(\beta+y)\in\mathcal{P}_T^+(0)$. $\square$

Analogno bi pokazali, da sta tudi $\mathcal{P}_T^-(x_0)$ in $\mathcal{P}_T(x_0)$ stožca. Stožec $\mathcal{P}_T(x_0)$ imenujemo *časovni stožec*, stožec $\mathcal{P}_T^+(x_0)$ *stožec prihodnosti* in stožec $\mathcal{P}_T^-(x_0)$ *stožec preteklosti.*

Časovni stožec $\mathcal{P}_T(x_0)$ je torej notranjost svetlobnega stožca $\mathcal{P}_S(x_0)$. Notranjost tega stožca po eni strani zajema tiste dogodke, ki so mogoča preteklost dogodka x_0, stožec $\mathcal{P}_T^-(x_0)$, po drugi strani pa dogodke, ki so mogoča prihodnost dogodka x_0, stožec $\mathcal{P}_T^+(x_0)$.

Če analogno, kot smo to storili za časovni stožec, tudi svetlobni stožec zapišemo kot unijo $\mathcal{P}_S^+(x_0)$ in $\mathcal{P}_S^-(x_0)$, stožec $\mathcal{P}_S^+(x_0)$ ustreza dogodkom, do katerih bi lahko prispel svetlobni blisk, ki bi bil izsevan v danem trenutku, stožec $\mathcal{P}_S^-(x_0)$ pa dogodkom, v katerih bi morali biti izsevani svetlobni bliski, da bi dospeli do danega dogodka.

Če smo dogodkoma svetlobnega stožca ali njegove notranjost lahko priredili pojav, za zunanjost tega ne moremo storiti. Zunanjosti svetlobnega stožca namreč pojavi, ki izhajajo iz danega dogodka, ne morejo doseči.

2.3 Lorentzova grupa

Naj bosta x in y poljubna dogodka prostora $\mathcal{M}$. Definirajmo množico *Lorentzovih transformacij* s predpisom

$$\mathcal{L}_G=\{\,A\in GL_4(\mathbb{R})\,;\,g(Ax,Ay)=g(x,y)\,\}\,.$$

Trditev 3.1. *Množica $\mathcal{L}_G$ je grupa.*

Dokaz: Matrika $A = I$ je očitno element $\mathcal{L}_G$.

Vzemimo A in $B \in \mathcal{L}_G$. Potem velja

$$g(ABx, ABy) = g(A\cdot Bx, A\cdot By) = g(Bx, By) = g(x, y)\,,$$

od koder sledi $AB \in \mathcal{L}_G$.

Naj bodo $A \in \mathcal{L}_G$ in $x, y \in \mathbb{R}^4$. Potem obstajata u in v taka, da velja $Au = x$ in $Av = y$. Ker je

$$g(A^{-1}x, A^{-1}y) = g(u, v) = g(Au, Av) = g(x, y)\,,$$

sledi $A^{-1} \in \mathcal{L}_G$. $\square$

Opomba : Lorentzov skalarni produkt lahko pišemo tudi v obliki

$$g(u, v) = \langle\, \mathcal{J}u, v\,\rangle\,,$$

kjer je

$$\mathcal{J} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}$$

in $\langle\, .\,, .\,\rangle$ običajni skalarni produkt v $\mathbb{R}^4$.

Trditev 3.2. *Denimo, da $A \in GL_4(\mathbb{R})$ ohranja Lorentzov skalarni produkt. Tedaj je*

$$A^*\mathcal{J}A = \mathcal{J}\,,$$

kjer je A^* običajno adjungiranje.

Dokaz: Če je $g(Au, Av) = g(u, v)$, je zaradi zgornje opombe

$$\langle\, \mathcal{J}Au, Av\,\rangle = \langle\, A^*\mathcal{J}Au, v\,\rangle = \langle\, \mathcal{J}u, v\,\rangle\,.$$

Od tod očitno sledi $A^*\mathcal{J}A = \mathcal{J}$. $\square$

Trditev 3.3. *Če je $A \in GL_4(\mathbb{R})$ Lorentzova, je Lorentzova tudi A^*.*

Dokaz: Vemo že, da je $A^*\mathcal{J}A = \mathcal{J}$. Ker je $\mathcal{J}^2 = I$, sledi

$$A^*\mathcal{J} = \mathcal{J}A^{-1} \Rightarrow \mathcal{J}A^*\mathcal{J} = \mathcal{J}^2A^{-1} = A^{-1}\,.$$

Od tod je

$$\mathcal{J}A^*\mathcal{J}^2 = A^{-1}\mathcal{J} \Rightarrow \mathcal{J}A^* = A^{-1}\mathcal{J}\,,$$

oziroma $A\mathcal{J}A^* = AA^{-1}\mathcal{J} = \mathcal{J}$. Od tod sledi A^* je Lorentzova. $\square$

Trditev 3.4. *Matriko $A \in \mathcal{L}_G$ pišimo v obliki*

$$\begin{bmatrix} \alpha & x \\ y & M \end{bmatrix},$$

kjer je $M \in GL_3(\mathbb{R})$, $x, y \in \mathbb{R}^3$ in $\alpha \in \mathbb{R}$. Potem velja

$$\begin{aligned} &(i) && M^*M = I + x \otimes x\,,\ MM^* = I + y \otimes y\,, \\ &(ii) && y = \frac{1}{\alpha}Mx\,,\ x = \frac{1}{\alpha}M^*y\,, \\ &(iii) && \alpha^2 = 1 + ||\,x\,||^2\,, \\ &(iv) && ||\,x\,|| = ||\,y\,|| < |\,\alpha\,|\,. \end{aligned}$$

Dokaz: Ker je $A \in \mathcal{L}_G$, velja $A^*\mathcal{J}A = \mathcal{J}$, oziroma

$$\begin{bmatrix} \alpha & y \\ x & M^* \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & -I \end{bmatrix} \begin{bmatrix} \alpha & x \\ y & M \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & -I \end{bmatrix},$$

$$\begin{bmatrix} \alpha & -y \\ x & -M^* \end{bmatrix} \begin{bmatrix} \alpha & x \\ y & M \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & -I \end{bmatrix},$$

$$\begin{bmatrix} \alpha^2 - ||\,y\,||^2 & \alpha x - M^*y \\ \alpha x - M^*y & x \otimes x - M^*M \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & -I \end{bmatrix},$$

kjer $x \otimes x$ pomeni tenzorski produkt vektorja x, oziroma izraz, za katerega velja $(\,x \otimes x\,)\,v = \langle\, v, x\,\rangle\, x$. Od tod direktno sledita enakosti

$$x = \frac{1}{\alpha}\,M^*y \ \text{ in } \ \alpha^2 = 1 + ||\,x\,||^2\,.$$

Ker je tudi $A\mathcal{J}A^* = \mathcal{J}$, podobno kot prej sledi

$$\begin{bmatrix} \alpha^2 - ||\,x\,||^2 & \alpha y - Mx \\ \alpha y - Mx & y \otimes y - MM^* \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & -I \end{bmatrix},$$

od koder je

$$y = \frac{1}{\alpha}\,Mx \ \text{ in } \ \alpha^2 = 1 + ||\,y\,||^2\,.$$

Od tod sledi

$$||\,x\,|| = ||\,y\,|| < |\,\alpha\,|$$

in

$$MM^* = I + y \otimes y\,,\ M^*M = I + x \otimes x\,.$$

Trditev 3.5. *Vedno velja $\alpha \geq 1$ ali $\alpha \leq -1$.*

Dokaz: Trditev je direktna posledica točke (iii) prejšnje trditve. □

Trditev 3.6. *Množica*

$$\mathcal{L}_{G+} = \{ \begin{bmatrix} \alpha & x \\ y & M \end{bmatrix} \in \mathcal{L}_G \, ; \, \alpha \geq 1 \}$$

je podgrupa, ki jo imenujemo grupa Lorentzovih transformacij, ki ohranjajo čas.

Dokaz: Matrika

$$I_4 = \begin{bmatrix} 1 & 0 \\ 0 & I_3 \end{bmatrix}$$

je očitno element $\mathcal{L}_{G+}$.

Naj bosta $A, B \in \mathcal{L}_{G+}$ in $\alpha, \beta \geq 1$. Če A in B zapišemo kot

$$A = \begin{bmatrix} \alpha & x \\ y & M \end{bmatrix} , \quad B = \begin{bmatrix} \beta & u \\ v & N \end{bmatrix}$$

velja

$$AB = \begin{bmatrix} \alpha & x \\ y & M \end{bmatrix} \begin{bmatrix} \beta & u \\ v & N \end{bmatrix} = \begin{bmatrix} \alpha\beta + \langle x, v \rangle & \alpha u + N^* x \\ \beta y + Mv & MN + y \otimes u \end{bmatrix} .$$

Ker je $|\langle x, v \rangle| \leq ||\, x \,|| \cdot ||\, v \,|| \leq |\, \alpha \,|\,|\, \beta \,| = \alpha\, \beta$, sledi $\langle x, v \rangle + \alpha\, \beta \geq 0$. Od tod po trditvi 3.5 sledi $AB \in \mathcal{L}_{G+}$. Inverz elementa

$$\begin{bmatrix} \alpha & x \\ y & M \end{bmatrix} \text{ je } \begin{bmatrix} \alpha & -y \\ -x & M^* \end{bmatrix} .$$

Od tod za vsak $A \in \mathcal{L}_{G+}$ sledi $A^{-1} \in \mathcal{L}_{G+}$. □

Opravičimo ime grupe $\mathcal{L}_{G+}$, grupe Lorentzovih transformacij, ki ohranjajo čas. Naj bo $v = t + u$ vektor časovnega tipa s pozitivno časovno komponento. Potem je vektor $v \in \mathcal{P}_T^+$, za katerega velja $t > ||\, u \,||$. Ker je

$$\begin{bmatrix} \alpha & x \\ y & M \end{bmatrix} \begin{bmatrix} t \\ u \end{bmatrix} = \begin{bmatrix} \alpha t + \langle x, u \rangle \\ ty + Mu \end{bmatrix} ,$$

sledi

$$\alpha t + \langle x, u \rangle \geq \alpha \,||\, u \,|| + \langle x, u \rangle \geq \alpha \,||\, u \,|| - |\, \langle x, u \rangle \,| \geq$$

$$\geq \alpha \,||\, u \,|| - ||\, x \,||\,||\, u \,|| = (\, \alpha - ||\, x \,||\,)||\, u \,|| > 0$$

in

$$||\, ty + Mu \,||^2 = t^2 ||\, y \,||^2 + 2t \,\langle\, M^* y, u \,\rangle + \langle\, M^* M u, u \,\rangle =$$

$$= t^2\,(\, \alpha^2 - 1\,) + 2t\alpha \,\langle\, x, u \,\rangle + \langle\, u + \langle\, u, x \,\rangle\, x, u \,\rangle =$$

$$= \alpha^2 t^2 - t^2 + 2t\alpha \,\langle\, u, x \,\rangle + ||\, u \,||^2 + \langle\, u, x \,\rangle^2 < \alpha^2 t^2 + \langle\, x, u \,\rangle^2 +$$

$$+ 2\alpha t \,\langle\, x, u \,\rangle = ||\, \alpha t + \langle\, x, u \,\rangle\, ||^2 \,,$$

oziroma

$$\alpha t + \langle\, x, u \,\rangle > ||\, ty + Mu \,|| \,.$$

Elementi grupe $\mathcal{L}_{G+}$ torej ohranjajo pozitivnost časovne komponente vektorjev časovnega tipa. Analogno pokažemo, da ohranjajo tudi negativnost časovne komponente. Vzemimo poljubna dogodka časovnega tipa v_1 in v_2 ter njuni časovni komponenti označimo z t_1 in t_2. Če za dogodka v_1 in v_2 velja, $t_1 > t_2$, potem tudi za dogodka v_1' in v_2', kjer je $v_1' = Av_1$ in $v_2' = Av_2$ ter $A \in \mathcal{L}_{G+}$, velja $t_1' > t_2'$.

Trditev 3.7. *Če je A Lorentzova transformacija, je*

$$det(A) \in \{\, \pm\, 1\} \,.$$

Dokaz: Ker je $A^* \mathcal{J} A = \mathcal{J}$ in $det(A) = det(A^*)$ sledi

$$det(A)^2\, det(\mathcal{J}) = det(\mathcal{J}) = -1 \,,$$

od koder dobimo $det(A)^2 = 1$, oziroma $det(A) = \pm 1$. □

Trditev 3.8. *Naj bo $\mathcal{L}_{G++} = \{\, A \in \mathcal{L}_{G+} \,;\, det(A) = 1\,\}$. Tedaj je $\mathcal{L}_{G++}$ grupa, ki jo imenujemo grupa pravih Lorentzovih transformacij.*

Dokaz: $\mathcal{L}_{G++} = \mathcal{L}_{G+} \cap \{\, A \in GL_4(\mathbb{R}) \,;\, det(A) = 1\,\}$. Ker je determinanta multiplikativna, je druga množica jedro homomorfizma $det : GL \longrightarrow \mathbb{R}$, torej je podgrupa. Ker je presek dveh podgrup tudi podgrupa, je $\mathcal{L}_{G++}$ podgrupa v GL. □

Trditev 3.9. *Matrika M v Lorentzovi transformaciji je unitarna natanko tedaj, ko je $x = y = 0$ in $\alpha = \pm 1$. Množica*

$$\mathcal{L}_R = \{\, \begin{bmatrix} 1 & 0 \\ 0 & M \end{bmatrix} \,;\, MM^* = I \;\; in\; det\, M = 1\,\}$$

je podgrupa grupe pravih transformacij $\mathcal{L}_{G++}$. Imenujemo jo grupa Lorentzovih rotacij.

Dokaz: Z enostavnim računom lahko preverimo, da je matrika

$$\begin{bmatrix} \pm 1 & 0 \\ 0 & M \end{bmatrix},$$

pri $M^*M = I$, Lorentzova.

Po drugi strani, po točki (i) trditve 3.4 sledi, da je $x = 0$. Po točki (iii) je potem $\alpha^2 = 1$, oziroma $\alpha = \pm 1$. Po (ii) je tudi $y = 0$.

Da je $\mathcal{L}_R$ grupa, je očitno. □

2.4 Splošni Lorentzovi stožci v $\mathbb{R}^n$

V nadaljevanju si nekoliko podrobneje oglejmo posplošitev ugotovitev prejšnjega razdelka na n-dimenzionalen prostor $\mathbb{R} \times \mathbb{R}^{n-1}$. Podobno kot smo v prostor-času Minkowskega definirali Lorentzov skalarni produkt, definirajmo v $\mathbb{R} \times \mathbb{R}^{n-1}$ bilinearno formo s predpisom

$$g(v, w) = v_1 w_1 - v_2 w_2 - \ldots - v_n w_n \,.$$

Zapišimo elementa v in w prostora $\mathbb{R} \times \mathbb{R}^{n-1}$ v obliki $v = \alpha + x$ in $w = \beta + y$, kjer sta $x = (\, x_2, x_3, \ldots, x_n \,)$ in $y = (\, y_2, y_3, \ldots, y_n \,)$. Komponenti x in y imenujemo *krajevni komponenti*, α in β pa *časovni komponenti* vektorjev v in w. Zgoraj definirano formo lahko zapišemo v obliki

$$g(v, w) = \alpha\beta - \langle\, x, y \,\rangle \,,$$

kjer je $\langle\, .,. \,\rangle$ običajni skalarni produkt v $\mathbb{R}^{n-1}$. Tako definirano bilinearno formo imenujemo tudi *splošni Lorentzov skalarni produkt.*

Naj bo

$$\mathcal{L}(n) = \{\, v \,;\, g(v, v) > 0 \text{ in } \alpha > 0 \,\} = \{\, x + \alpha \,;\, \alpha > ||\, x \,||\, \} \,.$$

V prejšnjem razdelku smo dokazali, da je $\mathcal{L}(n)$ za $n = 4$, odprt konveksen stožec. Podobno bi lahko pokazali, da je za vsak $n \geq 2$, množica $\mathcal{L}(n)$ odprt konveksen stožec, ki ga imenujemo *pozitivni Lorentzov časovni stožec* ali *stožec prihodnosti.*

Pokažimo najprej naslednjo

Trditev 4.1. *Vsak Lorentzov stožec $\mathcal{L}(n)$, $n \geq 2$, je sebi dualen.*

Dokaz: Stožec $\mathcal{L}(n) = \mathcal{L}$ je sebi dualen, če velja

$$\mathcal{L} = \mathcal{L}^* = \{\, v\,;\, \langle\, v, w \,\rangle > 0\,,\, \forall\, w \in \overline{\mathcal{L}} \backslash \{0\}\,\}.$$

Pokažimo najprej, da je $\mathcal{L} \subset \mathcal{L}^*$. Naj bo $\alpha + x \in \mathcal{L}$ in $\beta + y \in \overline{\mathcal{L}} \backslash 0$. Očitno je $\beta > 0$. Če bi namreč veljalo $0 = \beta = \lim_{n\to\infty} \beta_n$ in $y = \lim_{n\to\infty} y_n$, kjer $\beta_n + y_n \in \mathcal{L}$, bi zaradi $||\, y_n \,|| \leq \beta_n$ sledilo $y = 0$. To pa je protislovje s predpostavko, da je $\beta + y \neq 0$. Zaradi Cauchy- Schwartzove neenakosti sledi

$$|\, \langle\, x, y \,\rangle\, | = \lim_{n\to\infty} |\, \langle\, x, y_n \,\rangle\, | \leq \lim_{n\to\infty} ||\, x \,|| \cdot ||\, y_n \,|| \leq ||\, x \,||\, \beta\,.$$

Od tod je

$$\langle\, \alpha + x, \beta + y \,\rangle = \alpha\beta + \langle\, x, y \,\rangle \geq \alpha\beta - ||\, x \,|| \cdot ||\, y \,|| \geq \alpha\beta - ||\, x \,||\, \beta =$$

$$= (\, \alpha - ||\, x \,||\,)\, \beta > 0\,.$$

To pomeni, da je $\alpha + x \in \mathcal{L}^*$.

Pokažimo še, da je $\mathcal{L}^* \subset \mathcal{L}$. Naj bo $\beta + y \in \mathcal{L}^*$. Ker je $1 + 0 \in \mathcal{L}$, mora veljati $\langle\, \beta + y, 1 + 0 \,\rangle = \beta > 0$. Če je $y = 0$, je inkluzija očitna. Če je $y \neq 0$, poglejmo neničelni element $||\, y \,|| - y$, ki je limita elementov oblike $||\, y \,|| + \frac{1}{n} - y \in \mathcal{L}$. Očitno je torej $||\, y \,|| - y$ element zaprtja $\mathcal{L}$. Ker je $\beta + y \in \mathcal{L}^*$, mora veljati

$$0 < \langle\, \beta + y, ||\, y \,|| - y \,\rangle = ||\, y \,||\, (\, \beta - ||\, y \,||\,)\,,$$

od koder sledi $\beta - ||\, y \,|| > 0$, oziroma $\beta > ||\, y \,||$. To pa pomeni, da je $\beta + y \in \mathcal{L}$. □

Na povsem podoben način, kot smo to storili v $\mathbb{R}^4$, definirajmo množico Lorentzovih transformacij s predpisom

$$\mathcal{L}_G = \{\, A \in GL_n(\mathbb{R})\,;\, g(Ax, Ay) = g(x, y)\,\}\,.$$

V nadaljevanju bomo za Lorentzove transformacije ponovno uporabljali bločni zapis

$$\begin{bmatrix} \alpha & x \\ y & M \end{bmatrix},$$

kjer so $M \in GL_{n-1}(\mathbb{R})$, $\alpha \in \mathbb{R}$ ter $x, y \in \mathbb{R}^{n-1}$. Analogno kot v $\mathbb{R}^4$ definiramo tudi grupo Lorentzovih transformacij, ki ohranjajo čas, grupo pravih Lorentzovih transformacij in grupo Lorentzovih rotacij.

Trditev 4.2. *Naj bo $A \in \mathcal{L}_{G+}$ in $s > 0$. Potem sA ohranja Lorentzov stožec.*

Dokaz: Naj bo $v \in \mathcal{L}$. Pokazati zadošča, da $sA\,v \in \mathcal{L}$. Če v zapišemo v obliki $v = \beta + u$ sledi

$$s \begin{bmatrix} \alpha & x \\ y & M \end{bmatrix} \begin{bmatrix} \beta \\ u \end{bmatrix} = \begin{bmatrix} s\alpha\beta + s\,\langle\, x, u\,\rangle \\ s\beta y + s\,Mu \end{bmatrix}.$$

Od tod sledi

$$s\alpha\beta + s\,\langle\, x, u\,\rangle \geq s\alpha\,||\,u\,|| + s\,\langle\, x, u\,\rangle \geq s\alpha\,||\,u\,|| - s\,|\,\langle\, x, u\,\rangle\,| \geq$$

$$\geq s\,(\,\alpha\,||\,u\,|| - ||\,x\,|| \cdot ||\,u\,||\,) = s\,(\,\alpha - ||\,x\,||\,)||\,u\,|| > 0\,.$$

Ker je, upoštevajoč trditev 3.4

$$||\,s\beta y + sMu\,||^2 = s^2\beta^2||\,y\,||^2 + 2s\beta\,\langle\, M^*y, u\,\rangle + s\,\langle\, M^*Mu, u\,\rangle =$$

$$= s^2\beta^2\,(\,\alpha^2 - 1\,) + 2s\alpha\beta\,\langle\, x, u\,\rangle + s^2\langle\, u + \langle\, u, x\,\rangle\, x, u\,\rangle =$$
$$= s^2\alpha^2\beta^2 - s^2\beta^2 + 2s\alpha\beta\,\langle\, u, x\,\rangle + ||\,u\,||^2 + s^2\langle\, u, x\,\rangle^2\,,$$

ter velja $s\beta > s||\,u\,||$, sledi

$$s^2\alpha^2\beta^2 - s^2\beta^2 + 2s\alpha\beta\,\langle\, u, x\,\rangle + s^2||\,u\,||^2 + s^2\langle\, u, x\,\rangle^2 < s^2\alpha^2\beta^2 +$$

$$+ s^2\langle\, x, u\,\rangle^2 + 2s\alpha\beta\,\langle\, x, u\,\rangle = ||\,s\alpha\beta + s\,\langle\, x, u\,\rangle\,||^2\,.$$

Od tod torej sledi

$$s\alpha\beta + s\,\langle\, x, u\,\rangle > s\,||\,\beta y + Mu\,||\,,$$

oziroma sA ohranja Lorentzov stožec. □

Trditev 4.3. *Lorentzov stožec je homogen.* Dokaz: Ker je množica avtomorfizmov grupa, zadošča pokazati da lahko element $1 + 0 \in \mathcal{L}(n)$ s primernim avtomorfizmom premaknemo v vsak drug element $\beta + v \in \mathcal{L}(n)$. Na osnovi izreka 4.2 bomo avtomorfizem iskali v obliki

$$T = s \begin{bmatrix} \alpha & x \\ y & M \end{bmatrix},$$

kjer je $s > 0$ in matrika predstavlja Lorentzovo transformacijo s pozitivnim α. Ker je $\beta + v$ iz stožca, je $\beta > ||\,v\,||$. Če je $T(\,1 + 0\,) = \beta + v$, je očitno $s\alpha = \beta$ in $sy = v$. Ker mora veljati $||\,x\,|| = ||\,y\,||$ (glej trditev 3.4), je smiselno vzeti kar $x = y = \frac{1}{s}v$. S pomočjo trditve 3.4 lahko izračunamo tudi s. Ker velja $\alpha^2 = 1 + ||\,x\,||^2$, je $s^2\alpha^2 = s^2 + s^2||\,x\,||^2 = s^2 + s^2||\,y\,||^2$. Iz zgornjih zvez sledi $s^2\alpha^2 = \beta^2$ ter $s^2||\,y\,||^2 = ||\,v\,||^2$. Od tod sledi $s^2 = \beta^2 - ||\,v\,||^2$. Definirajmo torej $s = \sqrt{\beta^2 - ||\,v\,||^2}$, kar je smiselno zaradi $\beta > ||\,v\,||$. Videti moramo samo še, da lahko pravilno izberemo tudi M. Po trditvi 3.4 mora veljati $M^*M = MM^* = I + \frac{1}{s^2}\,v \otimes v$ ter $Mx = M\frac{v}{s} = \frac{1}{s}Mv = \alpha y = \frac{\alpha}{s}v$, oziroma $Mv = \alpha v$. Takih matrik je najbrž več, zato je smiselno poiskati M z nastavkom $M = I + \gamma\, v \otimes v$. Tedaj je $M = M^*$, in dobimo pogoja:

$$M^2 = I + \frac{1}{s^2}\, v \otimes v\,,$$

$$Mv = \alpha v\,.$$

Najprej dobimo

$$M^2 = (\,I + \gamma\, v \otimes v\,)^2 = I + 2\gamma\, v \otimes v + \gamma^2||\,v\,||^2\, v \otimes v =$$

$$= I + (\,2\gamma + \gamma^2||\,v\,||^2\,)\, v \otimes v\,.$$

Od tod sledi

$$\frac{1}{s^2} = 2\gamma + \gamma^2||\,v\,||^2\,,$$

kar je kvadratna enačba za γ. Njena rešitev je $\gamma = \frac{\beta - s}{s||\,v\,||^2}$. Če dobljeno vrednost vstavimo v izraz Mv, dobimo

$$Mv = Iv + \gamma||\,v\,||^2 v = (\,1 + \gamma||\,v\,||^2\,)v =$$

$$= (\,1 + \frac{\beta - s}{s}\,)v = \frac{\beta}{s}v = \alpha v\,,$$

kar pomeni, da izbrani M zadošča tudi drugi enačbi. Iskani avtomorfizem Lorentzovega stožca, ki element $1 + 0$ preslika v $\beta + v$ ima torej obliko

$$T = s\begin{bmatrix} \frac{\beta}{s} & \frac{v}{s} \\ \frac{v}{s} & I + \frac{\beta - s}{s||\,v\,||^2}\, v \otimes v \end{bmatrix} = \begin{bmatrix} \beta & v \\ v & sI + \frac{\beta - s}{||\,v\,||^2}\, v \otimes v \end{bmatrix},$$

kjer je $s = \sqrt{\beta^2 - ||\,v\,||^2}$. $\square$

Iz dokaza razberemo še eno zanimivo lastnost avtomorfizmov Lorentzovega stožca v primeru, ko je $\beta = 1$ in $v = 0$. To lastnost lahko zapišemo v obliki

Trditev 4.4. *Naj bo $T : \mathbb{R}^n \longrightarrow \mathbb{R}^n$ avtomorfizem stožca $\mathcal{L}(n)$, ki slika element $1+0$ vase. Tedaj je T unitarna (v običajnem smislu) preslikava.*

Dokaz: Pišimo T v obliki

$$T = \begin{bmatrix} \alpha & x \\ y & M \end{bmatrix}.$$

Iz pogoja $T(1+0) = (1+0)$ sledi $\alpha = 1$ in $y = 0$. Če preslikava

$$\begin{bmatrix} 1 & x \\ 0 & M \end{bmatrix}$$

ohranja Lorentzov stožec, mora elementa $||\,x\,|| + x$ ter $||\,x\,|| - x$, ki ležita na robu stožca, ponovno preslikati na rob stožca (glej trditev 1.4.1). To pomeni

$$\begin{bmatrix} ||\,x\,|| + ||\,x\,||^2 \\ Mx \end{bmatrix}, \begin{bmatrix} ||\,x\,|| - ||\,x\,||^2 \\ -Mx \end{bmatrix} \in \partial\mathcal{L}(n),$$

oziroma

$$||\,x\,|| + ||\,x\,||^2 = ||\,Mx\,||,$$
$$||\,x\,|| - ||\,x\,||^2 = ||\,-Mx\,|| = ||\,Mx\,||.$$

Od tod sledi $||\,x\,|| + ||\,x\,||^2 = ||\,x\,|| - ||\,x\,||^2$, oziroma $x = 0$. Če torej preslikava

$$\begin{bmatrix} 1 & 0 \\ 0 & M \end{bmatrix}$$

ohranja Lorentzov stožec, mora preslikati element $||\,z\,|| + z$ v element $||\,z\,|| + Mz$ na robu stožca. Od tod sledi $||\,z\,|| = ||\,Mz\,||$, kar pomeni, da je M unitarna matrika na $\mathbb{R}^{n-1}$. Od tod očitno sledi, da je

$$\begin{bmatrix} 1 & 0 \\ 0 & M \end{bmatrix}$$

unitarna na $\mathbb{R}^n$. □

Trditvi 4.2 in 4.3 pomenita, da je Lorentzov stožec simetričen.

V prostoru $\mathbb{R} \times \mathbb{R}^{n-1}$ definirajmo formo s predpisom

$$\phi(v,w) = vw = (\,\alpha + x\,)\,(\,\beta + y\,) = \alpha\beta + \langle\, x, y\,\rangle + \alpha y + \beta x\,.$$

Pokažimo, da je zgoraj definirana forma bilinearna z enoto $1+0$.

Naj bodo v_1, v_2, w_1 in w_2 poljubni elementi prostora $\mathbb{R} \times \mathbb{R}^{n-1}$ in a, b, c in d poljubna realna števila. Potem velja

$$\begin{aligned}
\phi(av_1 + bv_2, w_1) &= \phi(a(\alpha_1 + x_1) + b(\alpha_2 + v_2), \beta_1 + y_1) = \\
&= (a\alpha_1 + b\alpha_2)\beta_1 + \langle\, ax_1 + bx_2, y\,\rangle + \\
&\quad + (a\alpha_1 + b\alpha_2)y + \beta_1(ax_1 + bx_2) = \\
&= a\alpha_1\beta_1 + a\langle\, x_1, y_1\,\rangle + a\alpha_1 y_1 + \beta_1 a x_1 + \\
&\quad + b\alpha_2\beta_1 + b\langle\, x_2, y_1\,\rangle + b\alpha_2 y_1 + \beta_1 b x_2 = \\
&= a\,\phi(\alpha_1 + x_1) + b\,\phi(\alpha_2 + x_2) = \\
&= a\,\phi(v_1, w_1) + b\,\phi(v_2, w_2)
\end{aligned}$$

in

$$\begin{aligned}
\phi(v_1, cw_1 + dw_2) &= \phi(\alpha_1 + x_1, c(\beta_1 + y_1) + d(\beta_2 + y_2)) = \\
&= \alpha_1(c\beta_1 + d\beta_2) + \langle\, x_1, cy_1 + dy_2\,\rangle + \\
&\quad + \alpha_1(cy_1 + dy_2) + (c\beta_1 + d\beta_2)x_1 = \\
&= c\alpha_1\beta_1 + c\langle\, x_1, y_1\,\rangle + c\alpha_1 y_1 + c\beta_1 x_1 + d\alpha_1\beta_2 + \\
&\quad + d\langle\, x_1, y_2\,\rangle + d\alpha_1 y_2 + d\beta_2 x_1 = \\
&= c\,\phi(\alpha_1 + x_1, \beta_1 + y_1) + d\,\phi(\alpha_1 + x_1, \beta_2 + y_2) = \\
&= c\,\phi(v_1, w_1) + d\,\phi(v_1, w_2)\,.
\end{aligned}$$

Ker velja $(1+0)(\alpha+x) = \alpha + x$ je element $1+0$ enota. Na ta način smo $\mathbb{R}^n$ opremili v strukturo algebre z enoto. To algebro bomo označevali z $\mathcal{L}or(n)$ in jo imenovali *Lorentzovo algebra* dimenzije n. Njeno zvezo z Lorentzovim stožcem podaja naslednja

Trditev 4.5. *Množica* $\{\, v^2\,;\, v \in \mathbb{R} \times \mathbb{R}^{n-1}\,\}$ *je natanko zaprtje Lorentzovega stožca.*

Opomba: *Zaprtje Lorentzovega stožca je* $\overline{\mathcal{L}} = \{\,\alpha + x\,;\, \alpha \geq ||\,x\,||\,\}$.

Dokaz: Naj bo $v = \alpha + x$. Potem je

$$v^2 = (\,\alpha + x\,)^2 = \alpha^2 + ||\,x\,||^2 + 2\alpha x\,.$$

Ker je
$$\|\, 2\alpha x \,\| = 2\,|\,\alpha\,|\,\|\, x \,\| \leq \alpha^2 + \|\, x \,\|^2 \,,$$
sledi $(\,\alpha + x\,)^2 \in \overline{\mathcal{L}}$. Če je $\|\, 2\alpha x \,\| = \alpha^2 + \|\, x \,\|^2$, v leži na robu stožca $\overline{\mathcal{L}}$.

Naj bo $\beta + y \in \overline{\mathcal{L}}$. Tedaj je $\beta \geq \|\, y \,\|$, od koder sledi $\beta^2 - \|\, y \,\|^2 \geq 0$. Iščemo taka α in x, da bo $(\,\alpha + x\,)^2 = \beta + y$. Ker je $(\,\alpha + x\,)^2 = \alpha^2 + \|\, x \,\|^2 + 2\alpha x$, sledi $\alpha^2 + \|\, x \,\|^2 = \beta$ in $2\alpha x = y$. Od tod zaradi $2\alpha\|\, x \,\| = \|\, y \,\|$ sledi $4\alpha^4 - 4\beta\alpha^2 + \|\, y \,\|^2 = 0$, od koder je $\alpha^2 = \frac{1}{2}(\,\beta + \sqrt{\beta^2 - \|\, y \,\|^2}\,)$. Ker je $\beta \geq 0$ in $\beta^2 - \|\, y \,\|^2 \geq 0$ sledi $\alpha^2 \geq 0$, oziroma α je lahko realen. Od tod $x := \frac{1}{2\alpha}\, y$. Če je $\alpha = 0$, potem sledi $y = 0$ in x izberemo tako, da velja $\|\, x \,\|^2 = \beta$. $\square$

3 Sieglovi stožci

3.1 Kvaternioni in pozitivne matrike

V naslednjem poglavju bo predmet posebne obravnave stožec pozitivnih matrik na realnih, kompleksnih in kvaternionskih prostorih. Medtem, ko je vpeljava pojma Lorentzovega stožca povezana z obravnavo posebne teorije relativnosti, je pojem stožca pozitivnih matrik povezan s študijem problemov kvantne mehanike. Pobudo za študij stožcev pozitivnih matrik je podal nemški matematik C. L. Siegel s proučevanjem modularnih form v teoriji števil. Taki stožci so lahko zgrajeni iz realnih, kompleksnih ali kvaternionskih matrik. V nadaljevanju si nekoliko podrobneje oglejmo prostor kvaternionov.

Prostor *kvaternionov* $\mathbb{H}$ definiramo kot direktno vsoto prostorov $\mathbb{R}$ in $\mathbb{R}^3$, kar zapišemo

$$\mathbb{H} = \mathbb{R} \oplus \mathbb{R}^3 \,.$$

Vsak *kvaternion*, element prostora $\mathbb{H}$, torej lahko enolično zapišemo kot

$$h = \alpha + v \,,$$

kjer je $\alpha \in \mathbb{R}$ in $v \in \mathbb{R}^3$. Komponento α imenujemo *skalarni del*, komponento v pa *vektorski del* kvaterniona h.

Prostor $\mathbb{H}$ lahko interpretiramo kot vektorski prostor $\mathbb{R}^4$, opremljen z *produktom kvaternionov*, definiranim s predpisom

$$h_1 \, h_2 = (\, \alpha + v \,)\, (\, \beta + w \,) = \alpha\beta + \alpha w + \beta v + v \cdot w \,,$$

kjer je

$$v \cdot w = -\langle \, v, w \, \rangle + v \times w$$

in $\langle \, v, w \rangle$ pomeni običajni skalarni, $v \times w$ pa običajni vektorski produkt v $\mathbb{R}^3$.

Četverka $\{\, 1, i, j, k \,\}$ predstavlja bazo prostora kvaternionov. Trojica $\{\, i, j, k \,\}$ predstavlja standardno ortonormirano bazo prostora

$\mathbb{R}^3$. Oglejmo si kavaternionske produkte nekaterih baznih vektorjev.

$$\begin{aligned} i\,i &= -\langle\, i, i\,\rangle + i\times i = -1 + \overrightarrow{0}\,,\\ j\,j &= -\langle\, j, j\,\rangle + j\times j = -1 + \overrightarrow{0}\,,\\ k\,k &= -\langle\, k, k\,\rangle + k\times k = -1 + \overrightarrow{0}\,,\\ i\,j &= -\langle\, i, j\,\rangle + i\times j = 0 + k\,,\\ j\,i &= -\langle\, j, i\,\rangle + j\times i = 0 - k\,. \end{aligned}$$

Če izračunamo še preostale produkte, sledi tabela množenja:

$\cdot$	*1*	*i*	*j*	*k*
1	*1*	*i*	*j*	*k*
i	*i*	*-1*	*k*	*-j*
j	*j*	*-k*	*-1*	*i*
k	*k*	*j*	*-i*	*-1*

Očitno je produkt kvaternionov nekomutativen. Pokažimo, da je produkt kvaternionov asociativen. Naj bodo $p = \alpha + u$, $q = \beta + v$ in $h = \gamma + w \in \mathbb{H}$. Oglejmo si naprej produkt $p\,(\,qh\,)$.

$$\begin{aligned} p\,(\,qh\,) &= (\,\alpha + u\,)\,[\,(\,\beta + v\,)\,(\,\gamma + w\,)\,] =\\ &= (\,\alpha + u\,)\,[\,\beta\gamma + \beta w + \gamma v - \langle\, v, w\,\rangle + v\times w\,] =\\ &= \alpha\beta\gamma - \alpha\,\langle\, v, w\,\rangle + \alpha\beta w + \alpha\gamma v + \alpha\,(\,v\times w\,) +\\ &\quad + \beta\gamma u - \langle\, v, w\,\rangle\, u + u\cdot(\,\beta w + \gamma v + v\times w\,) =\\ &= \alpha\beta\gamma - \{\,\alpha\,\langle\, v, w\,\rangle + \beta\,\langle\, u, w\,\rangle + \gamma\,\langle\, u, v\,\rangle\,\} +\\ &\quad + \{\alpha\beta\, w + \alpha\gamma\, v + \beta\gamma\, u\,\} + \{\,\alpha\,(\,v\times w\,) + \beta\,(\,u\times w\,) +\\ &\quad + \gamma\,(\,u\times v\,)\,\} - \langle\, v, w\,\rangle\, u - \langle\, u, v\times w\,\rangle + u\times(\,v\times w\,)\,. \end{aligned}$$

Analogno izračunamo še produkt $(\,pq\,)\,h$.

$$\begin{aligned} (\,pq\,)\,h &= [\,(\,\alpha + u\,)\,(\,\beta + v\,)\,]\,(\,\gamma + w\,) =\\ &= [\,\alpha\beta + \alpha v + \beta u - \langle\, u, v\,\rangle + u\times v\,]\,(\,\gamma + w\,) =\\ &= \alpha\beta\gamma - \gamma\,\langle\, u, v\,\rangle + \alpha\beta w - \langle\, u, v\,\rangle\, w + \alpha\gamma v +\\ &\quad + \beta\gamma u + \gamma\,(\,u\times v\,) + (\,\alpha v + \beta u + u\times v\,)\cdot w =\\ &= \alpha\beta\gamma - \{\,\alpha\,\langle\, v, w\,\rangle + \beta\,\langle\, u, w\,\rangle + \gamma\,\langle\, u, v\,\rangle\,\} +\\ &\quad + \{\alpha\beta\, w + \alpha\gamma\, v + \beta\gamma\, u\,\} + \{\,\alpha\,(\,v\times w\,) + \beta\,(\,u\times w\,) +\\ &\quad + \gamma\,(\,u\times v\,)\,\} - \langle\, u, v\,\rangle\, w - \langle\, u\times v, w\,\rangle + (\,u\times v\,)\times w\,. \end{aligned}$$

Za dokaz asociativnosti torej zadošča pokazati enakost

$$\begin{aligned} -\langle\, v, w \,\rangle\, u - \langle\, u, v \times w \,\rangle + u \times (\, v \times w \,) = \\ = -\langle\, u, v \,\rangle\, w - \langle\, u \times v, w \,\rangle + (\, u \times v \,) \times w \,. \end{aligned}$$

Če upoštevamo, da je

$$u \times (\, v \times w \,) = (\, uw \,)\, v - (\, uv \,)\, w \,, \quad (\, u \times v \,) \times w = (\, uw \,)\, v - (\, uv \,)\, w$$

in

$$\langle\, u, v \times w \,\rangle = \langle\, u \times v, w \,\rangle \,,$$

zgornja enakost očitno drži. Produkt kvaternionov je torej asociativen. Definirajmo *konjugacijo* $*$ s predpisom

$$(\, \alpha + v \,)^* = \alpha - v$$

in pokažimo, da velja

$$\begin{aligned} (i)&\ \ (\, h_1 + h_2 \,)^* = h_1^* + h_2^* \,, \\ (ii)&\ \ (\, rh \,)^* = rh^* \,, \forall\, r \in \mathbb{R}, \\ (iii)&\ \ (\, h^* \,)^* = h \,, \\ (iv)&\ \ (\, h_1 h_2 \,)^* = h_2^* h_1^* \,. \end{aligned}$$

Naj bo $h_1 = \alpha + v$, $h_2 = \beta + w$ in $r \in \mathbb{R}$. Potem je

$$\begin{aligned} (i) \quad (\, h_1 + h_2 \,)^* &= (\, (\, \alpha + \beta \,) + (\, v + w \,)\,)^* = (\, \alpha + \beta \,) - (\, v + w \,) \\ &= (\, \alpha - v \,) + (\, \beta - w \,) = h_1^* + h_2^* \,. \\ (ii) \quad (\, rh_1 \,)^* &= (\, r(\, \alpha + v \,)\,)^* = (\, r\alpha + rv \,)^* = r\alpha - rv \\ &= r(\, \alpha - v \,) = rh_1^* \\ (iii) \quad (h_1^*)^* &= (\, (\, \alpha + v \,)^*)^* = (\, \alpha - v \,)^* = (\, \alpha - (-v)\,) \\ &= \alpha + v = h_1 \,. \\ (iv) \quad (\, h_1 h_2 \,)^* &= (\, \alpha\beta + \alpha w + \beta v - \langle\, v, w \,\rangle + v \times w \,)^* \\ &= (\, (\, \alpha\beta - \langle\, v, w \,\rangle\,) + (\, \alpha w + \beta v + v \times w \,)\,)^* \\ &= (\, (\, \alpha\beta - \langle\, v, w \,\rangle\,) - (\, \alpha w + \beta v + v \times w \,)\,) \\ &= \alpha\beta - \langle\, v, w \,\rangle - \alpha w - \beta v - v \times w \\ &= \beta\alpha - \beta v - \alpha w + (-w) \times (-v) - \langle\, -w, -v \,\rangle \\ &= (\, \beta - w \,)(\, \alpha - v \,) = h_2^* h_1^* \,. \end{aligned}$$

V prostoru kvaternionov definiramo *normo* kot

$$|| \alpha + v ||^2 = \alpha^2 + || v ||^2 .$$

Ta norma je inducirana s skalarnim produktom

$$\langle \alpha + v, \beta + w \rangle = \alpha\beta + \langle v, w \rangle .$$

Oglejmo si produkt hh^*, kjer je $h \in \mathbb{H}$. Ker je

$$(\alpha + v)(\alpha + v)^* = (\alpha + v)(\alpha - v) =$$
$$= \alpha^2 + \alpha v - \alpha v - v \cdot v = \alpha^2 + \langle v, v \rangle - v \times v =$$
$$= \alpha^2 + || v ||^2 = || \alpha + v ||^2$$

sledi

$$hh^* = h^*h = || h ||^2 .$$

Od tod sledi, da je $\frac{1}{|| h ||^2} h^*$ inverz elementa $h \neq 0$. Vsak neničelen kvaternion ima torej inverz. Ker kvaternioni niso komutativni, tvorijo nekomutativni obseg. Očitno je kvaternion $h \in \mathbb{R}$ natanko tedaj, ko velja $h = h^*$.

V nadaljevanju bomo množico $\mathbb{H}^n$ obravnavali kot desni vektorski prostor nad $\mathbb{H}$. Definirajmo *kvaternionski skalarni produkt*

$$\langle\ ,\ \rangle : \mathbb{H}^n \times \mathbb{H}^n \longrightarrow \mathbb{H}$$

s predpisom

$$\langle x, y \rangle = x_1 y_1^* + x_2 y_2^* + \ldots + x_n y_n^* .$$

Pokazali smo, da je $x_1 x_1^* = || x_1 ||^2 \in \mathbb{R}^+$. Analogno je potem tudi $\langle x, x \rangle$ nenegativno realno število za vsak $x \in \mathbb{H}^n$.

Množenje s skalarjem $h \in \mathbb{H}$ definirajmo kot

$$\cdot : \mathbb{H} \times \mathbb{H}^n \longrightarrow \mathbb{H}^n$$

s predpisom

$$h \cdot x = (hx_1, hx_2, \ldots, hx_n) .$$

Očitno velja

$$h \cdot (x + y) = h \cdot x + h \cdot y ,$$

$$(h+k)\cdot x = h\cdot x + k\cdot x\,,$$

$$1\cdot x = x\,,$$

$$k\cdot(h\cdot x) = kh\cdot x\,,$$

za vse $x, y \in \mathbb{H}^n$ ter vse $h, k \in \mathbb{H}$. Pri tako definiranem množenju s skalarji očitno velja

$$\langle\, h{\cdot}x, y\,\rangle = h{\cdot}\langle\, x, y\,\rangle$$

ter

$$\langle\, x, h{\cdot}y\,\rangle = \sum_i x_i(\,h{\cdot}y_i\,)^* = \sum_i x_i y_i^* h^* = \langle\, x, y\,\rangle\, h^*\,.$$

Poleg tega velja tudi

$$\langle\, x, y\,\rangle = \langle\, y, x\,\rangle^*\,.$$

Zdaj lahko definiramo tudi linearne preslikave na prostoru $\mathbb{H}^n$. Naj bo torej $\phi : \mathbb{H}^n \longrightarrow \mathbb{H}^n$ neka preslikava na prostoru $\mathbb{H}^n$. Za preslikavo ϕ bomo rekli, da je $\mathbb{H}$ - *linearna preslikava*, če velja

$$\phi(x+y) = \phi(x) + \phi(y)\,,$$

$$\phi(h{\cdot}x) = h{\cdot}\phi(x)\,,$$

za poljubna $x, y \in \mathbb{H}^n$ ter $h \in \mathbb{H}$.

Podobno kot preslikavam na $\mathbb{R}^n$ in $\mathbb{C}^n$, poskusimo tudi preslikavam na $\mathbb{H}^n$ prirediti ustrezne matrike. Če preslikavi $\phi : \mathbb{H}^2 \longrightarrow \mathbb{H}^2$ priredimo matriko

$$\begin{bmatrix} h_2 & h_1 \\ h_4 & h_3 \end{bmatrix}\,,$$

deluje ϕ na prostoru $\mathbb{H}^2$ z naslednjim predpisom

$$\begin{bmatrix} h \\ k \end{bmatrix} \circ \begin{bmatrix} h_2 & h_1 \\ h_4 & h_3 \end{bmatrix} = \begin{bmatrix} hh_1 + kh_2 \\ hh_3 + kh_4 \end{bmatrix}.$$

Trivialno je preveriti, da je tako definirana preslikava $\mathbb{H}$ - linearna. Naj bosta ϕ in ψ preslikavi prostora $\mathbb{H}^2$ vase, ki jima pripadata matriki H in K. Oglejmo si izraz $K(Hq)$, $q \in \mathbb{H}^2$. V smislu prejšnjega dobimo

$$\left(\begin{bmatrix} h \\ k \end{bmatrix} \circ \begin{bmatrix} h_2 & h_1 \\ h_4 & h_3 \end{bmatrix}\right) \circ \begin{bmatrix} k_2 & k_1 \\ k_4 & k_3 \end{bmatrix} =$$

$$\begin{bmatrix} hh_1 + kh_2 \\ hh_3 + kh_4 \end{bmatrix} \circ \begin{bmatrix} k_2 & k_1 \\ k_4 & k_3 \end{bmatrix} =$$

$$= \begin{bmatrix} hh_1k_1 + kh_2k_1 + hh_3k_2 + kh_4k_2 \\ hh_1k_3 + kh_2k_3 + hh_3k_4 + kh_4k_4 \end{bmatrix} =$$

$$= \begin{bmatrix} h(\, h_1k_1 + h_3k_2\,) + k(\, h_2k_1 + h_4k_2\,) \\ h(\, h_1k_3 + h_3k_4\,) + k(\, h_2k_3 + h_4k_4\,) \end{bmatrix} =$$

$$= \begin{bmatrix} h \\ k \end{bmatrix} \circ \begin{bmatrix} h_2k_1 + h_4k_2 & h_1k_1 + h_3k_2 \\ h_2k_3 + h_4k_4 & h_1k_3 + h_3k_4 \end{bmatrix}.$$

Če torej želimo usklajenost z linearnostjo, moramo produkt matrik po zgornjem računu definirati kot

$$\begin{bmatrix} h_2 & h_1 \\ h_4 & h_3 \end{bmatrix} \circ \begin{bmatrix} k_2 & k_1 \\ k_4 & k_3 \end{bmatrix} = \begin{bmatrix} h_2k_1 + h_4k_2 & h_1k_1 + h_3k_2 \\ h_2k_3 + h_4k_4 & h_1k_3 + h_3k_4 \end{bmatrix}.$$

Analogno postopamo v višjih dimenzijah. Naj bo torej $\mathbb{F} \in \{\, \mathbb{R}, \mathbb{C}, \mathbb{H} \,\}$ in P linearna preslikava na $\mathbb{F}^n$. Če za vsak neničelen $v \in \mathbb{F}^n$ velja

$$\langle\, P(v), v \,\rangle > 0\,,$$

pravimo, da je P *pozitivna*.

V nadaljevanju si oglejmo nekatere lastnosti kvaternionskih preslikav, oziroma njim prirejenih kvaternionskih matrik. Naj bo H pozitivna kvaternionska matrika prirejena neki preslikavi na $\mathbb{H}^2$. Pokažimo, da sta potem elementa glavne diagonale matrike H pozitivni realni števili. Če torej matriko H zapišemo v obliki

$$\begin{bmatrix} h_2 & h_1 \\ h_4 & h_3 \end{bmatrix},$$

zaradi desnega zapisa, to pomeni, da sta pozitivna in realna h_1 in h_4. Ker je H pozitivna, mora za vsak neničelen $v = (\, k_1, k_2\,) \in \mathbb{H}^2$ veljati

$$\langle\, H(v), v \,\rangle > 0\,,$$

oziroma

$$\left\langle \begin{bmatrix} k_1 \\ k_2 \end{bmatrix} \circ \begin{bmatrix} h_2 & h_1 \\ h_4 & h_3 \end{bmatrix}, \begin{bmatrix} k_1 \\ k_2 \end{bmatrix} \right\rangle > 0\,,$$

in od tod

$$k_1h_1k_1^* + k_2h_2k_1^* + k_1h_3k_2^* + k_2h_4k_2^* > 0\,.$$

V prostoru $\mathbb{H}^n$ neenakost $\langle\, H(v), v\,\rangle > 0$ pomeni, da je $\langle\, H(v), v\,\rangle$ realen in nenegativen. Če torej v zgornjo neenakost vstavimo $k_1 = 0$ in $k_2 = 1$ sledi $h_4 > 0$. Analogno za $k_2 = 0$ in $k_1 = 1$ dobimo $h_1 > 0$.

Trditev 1.1 *Pozitivne kvaternionske matrike dimenzije 2 so natanko tiste, ki so oblike*

$$\begin{bmatrix} h & \alpha \\ \beta & h^* \end{bmatrix},$$

kjer sta $\alpha, \beta > 0$ in velja

$$||\, h\,||^2 < \alpha\beta\,.$$

Dokaz: Pokažimo najprej, da so pozitivne kvaternionske matrike dimenzije 2 zgornje oblike. Po prej dokazanem sta h_1 in h_2 realni števili in ju zato lahko pišemo kot $h_1 = \alpha$ in $h_2 = \beta$. Ker za poljubna kvaterniona $k_1 = \alpha + u$ in $k_2 = \beta + v$ velja neenakost

$$\alpha\,||\, k_1\,||^2 + k_2 h_2 k_1^* + k_1 h_3 k_2^* + \beta\,||\, k_2\,||^2 > 0\,,$$

za $k_1 = 1$ in $k_2 = 1$ dobimo

$$\alpha + \beta + h_2 + h_3 > 0\,.$$

Če zapišemo $h_2 = \gamma + w$ in $h_3 = \delta + z$, sledi $w = z = 0$ ali $w = -z$, oziroma $h_2 = \gamma + w$ in $h_3 = \delta - w$. Pokažimo še, da je $\gamma = \delta$. Denimo, da je $w = 0$. Potem je

$$\begin{aligned} k_2 h_2 k_1^* &= \gamma\,(\,\beta + v\,)\,(\,\alpha - u\,) \\ &= \gamma\,(\,\alpha\beta + \alpha v - \beta u + \langle\, u, v\,\rangle + v \times (\,-u\,)\,) \\ &= \alpha\beta\gamma + \alpha\gamma v - \beta\gamma u + \gamma\,\langle\, u, v\,\rangle + \gamma\,(\,u \times v\,) \end{aligned}$$

in

$$\begin{aligned} k_1 h_3 k_2^* &= \delta\,(\,\alpha + v\,)\,(\,\beta - v\,) \\ &= \delta\,(\,\alpha\beta - \alpha v + \beta u + \langle\, u, v\,\rangle + u \times (\,-v\,)\,) \\ &= \alpha\beta\delta - \alpha\delta v - \beta\delta u + \delta\,\langle\, u, v\,\rangle - \delta\,(\,u \times v\,)\,. \end{aligned}$$

Ker je vsota

$$\begin{aligned} k_2 h_2 k_1^* + k_1 h_3 k_2^* = \alpha\beta(\,\gamma + \delta\,) + \alpha\,(\,\gamma - \delta\,)\,v - \beta\,(\,\gamma - \delta\,)\,u\, + \\ +\,(\,\gamma - \delta\,)\,(\,u \times v\,) > 0\,, \end{aligned}$$

za vsak $u, v \in \mathbb{R}^3$, sledi

$$\gamma = \delta\,.$$

Če torej pišemo $h_2 = h$, potem sledi $h_3 = h^*$. Dokažimo še zadnjo neenakost. Naj bo $k_1 = h$ in $k_2 = t$, kjer je t poljubno realno število. Ker potem za vsak t velja neenakost

$$\alpha\,||\,h\,||^2 + \beta\,t^2 + 2\,||\,h\,||^2\,t > 0\,,$$

od tod sledi

$$4\,||\,h\,||^4 - 4\alpha\beta\,||\,h\,||^2 < 0\,,$$

oziroma

$$\alpha\beta > ||\,h\,||^2\,.$$

Dokažimo trditev še v drugo smer. Naj bo dana matrika

$$P = \begin{bmatrix} h & \alpha \\ \beta & h^* \end{bmatrix},$$

za katero sta $\alpha, \beta > 0$ ter velja $\alpha\beta > ||\,h\,||^2$. Vzemimo poljuben $(\,a, b\,) \in \mathbb{H}^2$. Po definiciji je potem

$$\langle\, P\,(\,a, b\,), (\,a, b\,)\,\rangle = \alpha\,||\,a\,||^2 + bha^* + ah^*b^* + \beta\,||\,b\,||^2\,.$$

Ker je

$$|\,bha^* + ah^*b^*\,| \leq 2\,||\,ah^*b^*\,|| = 2\,||\,a\,||\cdot||\,b\,||\cdot||\,h\,||\,,$$

od tod sledi

$$\begin{aligned} \langle\, P(\,a, b\,), (\,a, b\,)\,\rangle &\geq \alpha\,||\,a\,||^2 - 2\,||\,a\,||\cdot||\,b\,||\cdot||\,h\,|| + \beta\,||\,b\,||^2 > \\ &> \alpha\,||\,a\,||^2 - 2\,||\,a\,||\cdot||\,b\,||\,\sqrt{\alpha\beta} + \beta\,||\,b\,||^2 = \\ &= (\,\sqrt{\alpha}\,||\,a\,|| - \sqrt{\beta}\,||\,b\,||\,)^2 \geq 0\,. \end{aligned}$$

Matrika P je torej pozitivna. □

Poleg pozitivnih matrik bodo v nadaljevanju predmet posebne obravnave tudi simetrične matrike. Te so karakterizirane z enačbo $A^* = A$. V prostoru kvaternionov je zaradi desnega zapisa transponiranje definirano nekoliko drugače. Če je namreč

$$A = \begin{bmatrix} h_2 & h_1 \\ h_4 & h_3 \end{bmatrix},$$

je potem

$$A^* = \begin{bmatrix} h_3^* & h_1^* \\ h_4^* & h_2^* \end{bmatrix}.$$

Trditev 1.2. *Pozitivna simetrična kvaternionska matrika dimenzije 2 je oblike*

$$\begin{bmatrix} h & \alpha \\ \beta & h^* \end{bmatrix},$$

kjer sta $\alpha, \beta > 0$ in $h \in \mathbb{H}$.

Dokaz: Naj bo S matrika zgornje oblike. Pokazati zadošča enakost

$$\langle\, Sv, w \,\rangle = \langle\, v, Sw \,\rangle\,,$$

kjer sta $v, w \in \mathbb{H}^2$. Če zapišemo $v = (\, v_1, v_2 \,)$ in $w = (\, w_1, w_2 \,)$ sledi

$$\left\langle \begin{bmatrix} v_1 \\ v_2 \end{bmatrix} \circ \begin{bmatrix} h & \alpha \\ \beta & h^* \end{bmatrix}, \begin{bmatrix} w_1 \\ w_2 \end{bmatrix} \right\rangle = \left\langle \begin{bmatrix} v_1\alpha + v_2 h \\ v_1 h^* + v_2\beta \end{bmatrix}, \begin{bmatrix} w_1 \\ w_2 \end{bmatrix} \right\rangle =$$

$$= v_1 \alpha w_1^* + v_2 h w_1^* + v_1 h^* w_2^* + v_2 \beta w_2^* =$$

$$= v_1 \alpha^* w_1^* + v_1 h^* w_2^* + v_2 h w_1^* + v_2 \beta^* w_2^* =$$

$$= v_1 (\, w_1 \alpha + w_2 h \,)^* + v_2 (\, w_1 h^* + w_2 \beta \,)^* =$$

$$= \left\langle \begin{bmatrix} v_1 \\ v_2 \end{bmatrix}, \begin{bmatrix} w_1\alpha + w_2 h \\ w_1 h^* + w_2\beta \end{bmatrix} \right\rangle = \left\langle \begin{bmatrix} v_1 \\ v_2 \end{bmatrix}, \begin{bmatrix} w_1 \\ w_2 \end{bmatrix} \circ \begin{bmatrix} h & \alpha \\ \beta & h^* \end{bmatrix} \right\rangle.$$

Trditev 1.3. *Simetrične matrike nad $\mathbb{F}^n$ tvorijo realen vektorski prostor.*

Dokaz: Ker vemo, da je množica matrik nad $\mathbb{F}^n$ z običajnim seštevanjem in množenjem s skalarjem vektorski prostor nad $\mathbb{R}$, zadošča pokazati, da je množica simetričnih matrik nad $\mathbb{F}^n$ njen podprostor. Naj bosta A in B simetrični matriki nad $\mathbb{F}^n$. Ker za poljubna v in $w \in \mathbb{F}^n$ velja

$$\langle\, (\, A + B \,)\, v, w \,\rangle = \langle\, Av, w \,\rangle + \langle\, Bv, w \,\rangle =$$

$$= \langle\, v, Aw \,\rangle + \langle\, v, Bw \,\rangle = \langle\, v, (\, A + B \,)\, w \,\rangle\,,$$

je množica simetričnih matrik nad $\mathbb{F}^n$ zaprta za seštevanje.

Pokažimo še zaprtost za množenje s skalarjem. Naj bo A simetrična nad $\mathbb{F}^n$ in $\alpha \in \mathbb{R}$. Potem je očitno

$$\langle\, (\, \alpha A \,)\, v, w \,\rangle = \langle\, v, (\, \alpha^* A \,)\, w \,\rangle = \langle\, v, (\, \alpha A \,)\, w \,\rangle\,.$$

Množica simetričnih matrik je torej realen vektorski prostor. $\square$

Trditev 1.4. *Pozitivne matrike nad $\mathbb{F}^n$ tvorijo znotraj prostora ustreznih simetričnih matrik odprt konveksen stožec.*

Dokaz: Naj bosta A in B pozitivni simetrični matriki nad $\mathbb{F}^n$. Ker je torej $A = A^*$, $B = B^*$ in za vsak neničelen x velja $\langle Ax, x \rangle > 0$ ter $\langle Bx, x \rangle > 0$, sledi

$$(A + B)^* = A^* + B^* = A + B$$

in

$$\langle (A + B)x, x \rangle = \langle Ax, x \rangle + \langle Bx, x \rangle > 0\,.$$

Ker za pozitivno simetrično matriko A in $\lambda > 0$ velja tudi

$$(\lambda A)^* = \lambda A^* = \lambda A$$

in

$$\langle \lambda Ax, x \rangle = \lambda \langle Ax, x \rangle > 0$$

sledi, da pozitivne matrike nad $\mathbb{F}^n$ tvorijo konveksen stožec $\mathcal{P}$.

Pokažimo še, da je dobljeni stožec $\mathcal{P}$ odprt. Glede na to ali je $\mathbb{F} = \mathbb{R}$, $\mathbb{F} = \mathbb{C}$ ali $\mathbb{F} = \mathbb{H}$, lahko prostor matrik nad $\mathbb{F}^n$ enačimo z evklidskim prostorom $\mathbb{R}^n$, $\mathbb{R}^{2n}$ ali $\mathbb{R}^{4n}$. Naj bo $P(n, \mathbb{F})$ realni podprostor pozitivnih simetričnih matrik. Preslikava $\phi_x : P(n, \mathbb{F}) \longrightarrow \mathbb{R}$, definirana s predpisom $\phi_x(A) = \langle Ax, x \rangle$, kjer je $||\, x \,|| = 1$, je polinomska in zato zvezna. To pomeni, da obstaja tak $\epsilon > 0$, da je $\langle Ax, x \rangle > \epsilon$. Denimo, da je B simetrična matrika za katero velja $||\, A - B \,|| < \frac{\epsilon}{2}$. Ker je

$$\langle Bx, x \rangle = \langle Ax, x \rangle + \langle (B - A)x, x \rangle\,,$$

sledi

$$\langle Bx, x \rangle \geq \epsilon + \langle (B - A)x, x \rangle \geq \epsilon - |\langle (B - A)x, x \rangle| \geq$$

$$\geq \epsilon - ||\, B - A \,|| \cdot ||\, x \,||^2 = \epsilon - ||\, B - A \,|| \geq \tfrac{\epsilon}{2}\,.$$

Ker za poljuben $x \neq 0$ velja

$$\langle Bx, x \rangle = ||\, x \,||^2 \langle B \tfrac{x}{||x||}, \tfrac{x}{||x||} \rangle \geq ||\, x \,||^2 \tfrac{\epsilon}{2} > 0\,,$$

sledi, da je B pozitivna matrika. $\square$

Zaprtje stožca pozitivnih matrik je stožec pozitivno semidefinitnih matrik. Matrika M je *pozitivno semidefinitna*, če za vsak $v \in \mathbb{F}^n$ velja

$$\langle\, Q(v), v \,\rangle \geq 0\,,$$

kjer je $\mathbb{F} \in \{\, \mathbb{R}, \mathbb{C}, \mathbb{H} \,\}$.

3.2 Dualnost matričnih stožcev

V nadaljevanju bo predmet posebne obravnave prostor simetričnih matrik nad $\mathbb{R}^n$. Prostor simetričnih matrik nad $\mathbb{R}^n$ bomo označevali s $\mathcal{S}(n)$, pripadajoči stožec pozitivnih matrik nad $\mathbb{R}^n$ pa s $\mathcal{P}(n)$. Glavni namen razdelka je dokazati, da je stožec $\mathcal{P}(n)$ sebi dualen znotraj prostora $\mathcal{S}(n)$.

Funkcijo $\mathcal{Q}\,(x, y)$, definirano na prostoru $\mathbb{R}^n$, ki vsakemu paru elementov x in $y \in \mathbb{R}^n$ priredi realno število in zadošča pogojema

$$\mathcal{Q}\,(\alpha x_1 + \beta x_2, y_1) = \alpha\, \mathcal{Q}\,(x_1, y_1) + \beta\, \mathcal{Q}\,(x_2, y_1)$$

$$\mathcal{Q}\,(x_1, \gamma y_1 + \delta y_2) = \gamma\, \mathcal{Q}\,(x_1, y_1) + \delta\, \mathcal{Q}\,(x_1, y_2)\,,$$

kjer so x_1, x_2, y_1 in $y_2 \in \mathbb{R}^n$ ter α, β, γ in $\delta \in \mathbb{R}$, imenujemo *bilinearna forma*. Če v $\mathbb{R}^n$ izberemo bazo $e_1, \ldots, e_n$, se vektorja x in y izražata kot $x = \xi_1 e_1 + \ldots + \xi_n e_n$ in $y = \eta_1 e_1 + \ldots + \eta_n e_n$. Po definiciji bilinearne forme je potem

$$\mathcal{Q}\,(x, y) = \mathcal{Q}\,(\,\xi_1 e_1 + \ldots + \xi_n e_n, \eta_1 e_1 + \ldots + \eta_n e_n\,) =$$

$$= \sum_{j=1}^{n} \sum_{i=1}^{n} \xi_i\, \eta_j\, \mathcal{Q}\,(e_i, e_j)\,.$$

Če upoštevamo, da so vrednosti $\mathcal{Q}\,(e_i, e_j) = a_{ij}$ realna števila, lahko pišemo

$$\mathcal{Q}\,(x, y) = \sum_{j=1}^{n} \sum_{i=1}^{n} a_{ij}\, \xi_i\, \eta_j\,.$$

Ob ustrezni izbiri baze prostora se torej da bilinearna forma zapisati v zgornji obliki. Pri tem koeficienti a_{ij} predstavljajo matriko $A = (a_{ij})$, prirejeno bilinearni formi $\mathcal{Q}\,(x, y)$ v bazi $e_1, \ldots, e_n$.

Bilinearna forma $\mathcal{Q}(x,y)$ je *simetrična*, če za vsak par elementov x in $y \in \mathbb{R}^n$ velja

$$\mathcal{Q}(x,y) = \mathcal{Q}(y,x)\,.$$

Ker v tem primeru za vsaka bazna vektorja e_i in e_j velja

$$a_{ij} = \mathcal{Q}(\,e_i, e_j\,) = \mathcal{Q}(\,e_j, e_i\,) = a_{ji}\,,$$

pripada simetrični bilinearni formi v vsaki bazi prostora $\mathbb{R}^n$ simetrična matrika.

Če v simetrični bilinearni formi postavimo $y = x$, dobimo *kvadratno formo* $\mathcal{Q}(x,x)$, oziroma v nadaljevanju $\mathcal{Q}(x)$. Če upoštevamo zgoraj navedeno, lahko po izbiri baze prostora $\mathbb{R}^n$ kvadratno formo zapišemo v obliki

$$\mathcal{Q}(x) = \sum_{j=1}^{n}\sum_{i=1}^{n} a_{ij}\,\xi_i\,\xi_j\,,$$

kjer so koeficienti a_{ij} elementi, kvadratni formi pripadajoče simetrične matrike.

Izrek 2.1. *Naj bo $\mathcal{Q}(x)$ kvadratna forma, definirana na prostoru $\mathbb{R}^n$. Obstaja takšna ortonormirana baza prostora $\mathbb{R}^n$, da ima v njej kvadratna forma obliko $\mathcal{Q}(\,x\,) = \lambda_1\,\xi_1^2 + \lambda_2\,\xi_2^2 + \ldots + \lambda_n\,\xi_n^2$, kjer so $\lambda_1, \ldots, \lambda_n \in \mathbb{R}$.*

Dokaz: Naj bo $e_1, \ldots, e_n$ ortonormirana baza prostora $\mathbb{R}^n$. Kvadratni formi $\mathcal{Q}(x)$ pripada tedaj v tej bazi simetrična matrika $A = (\,a_{ij}\,)$. Če vektor $x \in \mathbb{R}^n$ pišemo v obliki $x = \xi_1 e_1 + \ldots + \xi_n e_n$, je potem

$$Ax = \sum_{i=1}^{n} \xi_i\,Ae_i = \sum_{j=1}^{n}\sum_{i=1}^{n} a_{ij}\,\xi_j\,e_i\,.$$

Če izračunamo skalarni produkt $\langle\,Ax, x\,\rangle$, dobimo zaradi ortogonalnosti in normiranosti baze

$$\langle\,Ax, x\,\rangle = \left\langle\,\sum_{j=1}^{n}\sum_{i=1}^{n} a_{ij}\xi_j\,e_i, \sum_{i+1}^{n} \xi_i\,e_i\,\right\rangle = \sum_{j=1}^{n}\sum_{i=1}^{n} a_{ij}\,\xi_i\,\xi_j\,.$$

Ker je izraz na desni enak $\mathcal{Q}(x)$, velja enakost

$$\mathcal{Q}(x) = \langle\,Ax, x\,\rangle\,.$$

Ker je matrika A simetrična, premore z njo določen sebi adjungiran endomorfizem prostora $\mathbb{R}^n$ n lastnih vektorjev $f_1, f_2, \ldots, f_n$, ki so paroma ortogonalni. Zanje veljajo enačbe

$$Af_1 = \lambda_1 f_1\,,\ Af_2 = \lambda_2 f_2\,,\ \ldots\,,\ Af_n = \lambda_n f_n\,,$$

kjer so $\lambda_1, \lambda_2, \ldots, \lambda_n$ lastne vrednosti. Če torej v izraz $\mathcal{Q}(x) = \langle Ax, x \rangle$, vstavimo $x = \xi_1 f_1 + \xi_2 f_2 + \ldots + \xi_n f_n$, dobimo

$$\langle Ax, x \rangle = \langle \xi_1 Af_1 + \ldots + \xi_n Af_n, \xi_1 f_1 + \ldots + \xi_n f_n \rangle\,.$$

Od tod z upoštevanjem distributivnosti in homogenosti skalarnega produkta sledi

$$\langle Ax, x \rangle = \lambda_1 \xi_1^2 + \lambda_2 \xi_2^2 + \ldots + \lambda_n \xi_n^2\,,$$

oziroma

$$\mathcal{Q}(x) = \sum_{i=1}^{n} \lambda_i \xi_i^2\,.$$

V prostoru $\mathcal{S}(n)$ je skalarni produkt definiran s predpisom

$$\langle A, B \rangle = Sl\,(AB) = \sum_{i,j}^{n} a_{ij}\, b_{ij} = \sum_{i=j}^{n} a_{ii}\, b_{ii} + 2 \sum_{i<j}^{n} a_{ij}\, b_{ij}\,.$$

Tako definiran skalarni produkt je opredeljen s pozitivno definitno kvadratno formo oblike

$$\mathcal{Q}(x) = \sum_{i,j}^{n} a_{ij}\, \xi_i\, \xi_j\,,$$

pri čemer so a_{ij} koeficienti simetrične matrike A. Če vektor x zapišemo kot $n \times 1$ matriko, kvadratna forma dobi obliko

$$\mathcal{Q}(x) = \langle A, xx^T \rangle\,.$$

Ker po izreku 2.1 pozitivno kvadratno formo $\mathcal{Q}(x)$ lahko zapišemo kot vsoto kvadratov, sledi

$$\mathcal{Q}(x) = \sum_{j=1}^{n} \Big(\sum_{i=1}^{n} \alpha_{ij}\, \xi_i \Big)^2,$$

in od tod

$$A = \sum_{j=1}^{n} \alpha_j \alpha_j^T = \alpha\alpha^T \,,$$

kjer je $\alpha_j = (\,\alpha_{1j},\, \alpha_{2j},\, \ldots,\, \alpha_{nj}\,)$.

Izrek 2.2. *Stožec $\mathcal{P}(n)$ je sebi dualen znotraj prostora $\mathcal{S}(n)$.*

Dokaz: Naj bo $B \in \mathcal{P}^*(n) = \mathcal{P}^*$. Če je x poljuben neničelen vektor dimenzije n, matrika $A = xx^T$ pripada $\overline{\mathcal{P}}\backslash\{0\}$. Velja namreč

$$\langle\, xx^T\, y, y\,\rangle = \langle\, \langle\, x, y\,\rangle\, x, y\,\rangle = \langle\, x, y\,\rangle\, \langle\, x, y\,\rangle = |\, \langle\, x, y\,\rangle\, |^2 \geq 0\,.$$

Ker je $xx^T\, x = ||\, x\, ||^2 x \neq 0$ sledi, da je $xx^T \neq 0$. Ker za simetrično matriko B velja

$$(\, xx^T\,)\, By = \langle\, By, x\,\rangle\, x = \langle\, B^* y, x\,\rangle\, x = \langle\, y, Bx\,\rangle\, x = (\, x(Bx)^T)y\,,$$

sledi

$$0 < \langle\, A, B\,\rangle = \langle\, xx^T, B\,\rangle = Sl\,(\, xx^T B\,) = Sl\,(\, x(Bx)^T) = \langle\, Bx, x\,\rangle\,,$$

od koder sledi, da je $B \in \mathcal{P}$, oziroma $\mathcal{P}^* \subset \mathcal{P}$.

Pokažimo še obratno inkluzijo. Poljuben element $A \in \overline{\mathcal{P}}\backslash\{0\}$, ki je pozitivno semidefinitna matrika, lahko zapišemo v obliki

$$A = \sum_{j=1}^{n} \alpha_j \alpha_j^T \,,$$

kjer so α_j matrike dimenzije $n \times 1$. Seveda je vsaj eden izmed vektorjev α_j neničelen. Ker za poljuben $B \in \mathcal{P}$ velja

$$\langle\, B, A\,\rangle = \sum_{j=1}^{n} \langle\, B, \alpha_j \alpha_j^T\,\rangle = \sum_{j=1}^{n} \langle\, B\,\alpha_j, \alpha_j\,\rangle > 0\,,$$

sledi $\mathcal{P} \subset \mathcal{P}^*$. Stožec pozitivnih simetričnih matrik nad $\mathbb{R}^n$ je torej sebi dualen. □

Na podoben način bi omenjeni izrek dokazali tudi v primeru $\mathbb{F} = \mathbb{C}$ in $\mathbb{F} = \mathbb{H}$. Pripomniti je potrebno le, da v primeru $\mathbb{H}^n$ realni skalarni produkt definiramo s predpisom

$$\langle\, A, B\,\rangle = \tfrac{1}{2}\, Sl\,(\, AB + BA\,)\,.$$

3.3 Homogenost matričnih stožcev

Namen razdelka je dokazati, da avtomorfizemska grupa stožca $\mathcal{P}(n)$ znotraj prostora $\mathcal{S}(n)$ deluje na tem stožcu tranzitivno. Za dokaz bomo potrebovali nekatere trditve spektralne teorije.

Trditev 3.1. *Naj bo A pozitivno semidefinitna matrika prostora matrik nad $\mathbb{R}^n$. Potem veljajo naslednje trditve*

- (i) *Lastne vrednosti matrike A so nenegativna realna števila;*
- (ii) *Matriko A lahko zapišemo v obliki $A = UDU^*$, kjer je U unitarna, D pa diagonalna matrika oblike*

$$D = \begin{bmatrix} \lambda_1 & 0 & \dots & 0 \\ 0 & \lambda_2 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & \lambda_n \end{bmatrix},$$

  kjer so λ_i lastne vrednosti matrike A;
- (iii) Obstaja taka pozitivna semidefinitna simetrična matrika B, da velja $B^2 = A$. Lastne vrednosti matrike B so $\sqrt{\lambda_i}$.

Dokaz: Ker je trditev standardna trditev dodiplomskega študija, dokaz opuščamo. □

Trditev 3.2. *Naj bo A pozitivna matrika prostora matrik nad $\mathbb{R}^n$. Potem veljajo naslednje trditve*

- (i) *Lastne vrednosti matrike A so strogo pozitivna realna števila;*
- (ii) *Matriko A lahko zapišemo v obliki $A = UDU^*$, kjer je U unitarna, D pa diagonalna matrika oblike*

$$D = \begin{bmatrix} \lambda_1 & 0 & \dots & 0 \\ 0 & \lambda_2 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & \lambda_n \end{bmatrix},$$

  kjer so λ_i lastne vrednosti matrike A;
- (iii) *Obstaja taka pozitivna simetrična matrika B, da velja $B^2 = A$. Lastne vrednosti matrike B so $\sqrt{\lambda_i}$.*

Dokaz: Ker je tudi ta trditev dobro znana, dokaz opuščamo. □

Izrek 3.3. *Naj bodo A pozitivno semidefinitna, B pozitivna in S obrnljiva matrika prostora matrik nad $\mathbb{R}^n$. Potem je SAS^* pozitivno semidefinitna, SBS^* pa pozitivno definitna matrika, oziroma*

$$SAS^* \geq 0 \quad \text{in} \quad SBS^* > 0\,.$$

Dokaz: Pokažimo najprej pozitivno semidefinitnost SAS^*. Naj bo x poljuben vektor prostora $\mathbb{R}^n$. Ker velja

$$\langle\, SAS^*x, x\,\rangle = \langle\, AS^*x, S^*x\,\rangle = \langle\, Ay, y\,\rangle \geq 0\,,$$

je SAS^* očitno pozitivno semidefinitna.

Naj bo x poljuben neničelen vektor prostora $\mathbb{R}^n$. Potem očitno velja

$$\langle\, SBS^*x, x\,\rangle = \langle\, BS^*x, S^*x\,\rangle = \langle\, By, y\,\rangle\,.$$

Ker je S obrnljiva, je potem obrnljiva tudi S^*. Očitno je zaradi neničelnosti elementa x, neničelen tudi $y = S^*x$. Od tod, zaradi pozitivne definitnosti B sledi

$$\langle\, By, y\,\rangle > 0\,.$$

Posledica 3.4. *Če je S obrnljiva in X pozitivna simetrična matrika prostora matrik nad $\mathbb{R}^n$, je preslikava*

$$\phi_S(X) = SXS^*$$

avtomorfizem stožca pozitivnih simetričnih matrik $\mathcal{P}(n)$.

Dokaz: Pokažimo najprej, da je preslikava ϕ_S obrnljiva. Definirajmo preslikavo ϕ_S^{-1} s predpisom

$$\phi_S^{-1}(X) = S^{-1}X(S^{-1})^*\,.$$

Ker je

$$\phi_S\phi_S^{-1}(X) = S(S^{-1}X(S^{-1})^*)S^* = SS^{-1}X(SS^{-1})^* = X$$

in

$$\phi_S^{-1}\phi_S(X) = S^{-1}(SXS^*)(S^{-1})^* = S^{-1}SX(S^{-1}S)^* = X\,,$$

je preslikava ϕ_S^{-1} inverz preslikave ϕ_S.

Po izreku 3.3 preslikavi ϕ_S in ϕ_S^{-1} ohranjata stožec $\mathcal{P}(n) = \mathcal{P}$. Ker je torej $\phi_S(\mathcal{P}) \subset \mathcal{P}$ in $\phi_S^{-1}(\mathcal{P}) \subset \mathcal{P}$ ter velja

$$\phi_S \phi_S^{-1}(\mathcal{P}) \subset \phi_S(\mathcal{P}),$$

zaradi enakosti $\phi_S \phi_S^{-1}(\mathcal{P}) = \mathcal{P}$, sledi $\mathcal{P} \subset \phi_S(\mathcal{P})$. To pa pomeni $\phi_S(\mathcal{P}) = \mathcal{P}$, oziroma preslikava ϕ_S je avtomorfizem stožca $\mathcal{P}(n)$. □

Izrek 3.5. *Stožec $\mathcal{P}(n)$ je homogen znotraj prostora $\mathcal{S}(n)$.*

Dokaz: Dokazati zadošča, da lahko matriko $I \in \mathcal{P}(n)$ premaknemo v vsako pozitivno matriko $B \in \mathcal{P}(n)$. Naj bo B poljubna matrika stožca $\mathcal{P}(n)$. Po trditvi 3.2 obstaja koren $\sqrt{B}$, ki je element stožca $\mathcal{P}(n)$. Definirajmo preslikavo $\phi_{\sqrt{B}}$ s predpisom

$$\phi_{\sqrt{B}}(X) = \sqrt{B} X \sqrt{B}^* = \sqrt{B} X \sqrt{B}.$$

Ker je po posledici 3.4 preslikava $\phi_{\sqrt{B}}$ avtomorfizem stožca $\mathcal{P}(n)$, potem sledi

$$\phi_{\sqrt{B}}(I) = \sqrt{B}\sqrt{B} = B.$$

Trditev 3.6. *Stožec $\mathcal{P}(n)$ je simetričen znotraj prostora $\mathcal{S}(n)$.*

Dokaz: Trditev je direktna posledica izrekov 2.2 in 3.5. □

Trditev 3.7. *Stožec $\mathcal{P}(n)$ ni sebi dualen znotraj prostora vseh matrik $\mathcal{M}(n)$.*

Dokaz: Naj bo A matrika oblike

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}.$$

Pokažimo, da je matrika A element $\mathcal{P}^*(2) \subset \mathcal{M}(2)$. Naj bo

$$\begin{bmatrix} x & y \\ y & z \end{bmatrix} \in \overline{\mathcal{P}(2)} \backslash \{0\}.$$

Ker za pozitivno semidefinitno matriko velja, da so vsi njeni glavni minorji nenegativni, sledi, da je $y^2 \leq xz$ in vsaj eden od elementov x in z različen od nič. Po definiciji skalarnega produkta sledi

$$\left\langle \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} x & y \\ y & z \end{bmatrix} \right\rangle = Sl\left(\begin{bmatrix} x+y & y+z \\ y & z \end{bmatrix} \right) = x + y + z.$$

Če bi bila vsota $x+y+z \leq 0$, bi to pomenilo, da je $(x+z)^2 \leq y^2$, oziroma

$$x^2+z^2+2xz \leq y^2 \leq xz \leq 2xz\,.$$

Od tod bi sledilo $x=z=0$, kar pa je protislovje s predpostavko. Matrika A je torej element $\mathcal{P}^*(2)$. Ker A očitno ni element stožca $\mathcal{P}(2)$ je trditev dokazana. $\square$

3.4 Vložitev pozitivnih matrik v algebraično strukturo

Na prostoru simetričnih matrik $\mathcal{S}(n)$ definirajmo operacijo množenja z naslednjim predpisom

$$A \circ B = \tfrac{1}{2}(AB+BA)\,.$$

Ker je

$$\begin{gathered}(A \circ B)^* = \tfrac{1}{2}(AB+BA)^* = \\ = \tfrac{1}{2}(B^*A^*+A^*B^*) = \tfrac{1}{2}(BA+AB) = A \circ B\end{gathered}$$

je množenje $\circ$ dobro definirano. Množico simetričnih matrik $\mathcal{S}(n)$ torej lahko z zgoraj definiranim množenjem obravnavamo kot realno algebro $\mathcal{A}$. V nadaljevanju naj zapis A^2 pomeni $A \circ A$. Očitno se A^2 ujema z običajnim matričnim A^2.

Trditev 4.1. *Zaprtje stožca $\mathcal{P}(n)$ je stožec pozitivnih semidefinitnih matrik.*

Dokaz: Naj bo $B \in \overline{\mathcal{P}(n)}$. Potem obstaja tako zaporedje $A_n > 0$, da je $B = \lim A_n$. Ker je

$$\langle Bx, x \rangle = \lim \langle A_n x, x \rangle\,,$$

zaradi $\langle A_n x, x \rangle > 0$ sledi $\lim \langle A_n x, x \rangle \geq 0$, oziroma $B \geq 0$. Od tod torej sledi $\overline{\mathcal{P}(n)} \subset \{ B \geq 0 \}$.

Pokažimo še obratno inkluzijo. Naj bo $B \geq 0$. Potem po trditvi 3.1 (ii) matriko B lahko zapišemo v obliki $B = UDU^*$, kjer je U unitarna, D pa diagonalna matrika oblike

$$D = \begin{bmatrix} \lambda_1 & 0 & \dots & 0 & 0 & \dots & 0 \\ 0 & \lambda_2 & \dots & 0 & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & \lambda_k & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 0 & 0 & \dots & 0 \end{bmatrix}.$$

Če zapišemo matrike A_n v obliki $A_n = UD'U^*$, kjer je

$$D' = \begin{bmatrix} \lambda_1 & 0 & \dots & 0 & 0 & \dots & 0 \\ 0 & \lambda_2 & \dots & 0 & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & \lambda_k & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 & \frac{1}{n} & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 0 & 0 & \dots & \frac{1}{n} \end{bmatrix},$$

sledi $A_n > 0$. Ker je

$$\lim A_n = \begin{bmatrix} \lim \lambda_1 & 0 & \dots & 0 & 0 & \dots & 0 \\ 0 & \lim \lambda_2 & \dots & 0 & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & \lim \lambda_k & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 & \lim \frac{1}{n} & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 0 & 0 & \dots & \lim \frac{1}{n} \end{bmatrix} = B\,,$$

sledi $B \in \overline{\mathcal{P}(n)}$, oziroma $\{\, B \geq 0 \,\} \subset \overline{\mathcal{P}(n)}$. □

Trditev 4.2. *Množica kvadratov* $\{\, A^2\,;\, A \in \mathcal{A} \,\}$ *je zaprtje stožca* $\mathcal{P}(n)$. Dokaz: Ker je $A = A^*$ sledi

$$\langle\, A^2 x, x \,\rangle = \langle\, Ax, Ax \,\rangle = ||\, Ax \,||^2 \geq 0\,,$$

oziroma A^2 je pozitivno semidefinitna in zato $A^2 \in \overline{\mathcal{P}(n)}$.

Naj bo $B \in \overline{\mathcal{P}(n)}$. Ker je potem $B \geq 0$, po trditvi 3.1 (iii) obstaja taka $A \geq 0$, da je $A^2 = B$. Ker je A element $\mathcal{S}(n)$, je očitno tudi $B \in \{\, A^2\,;\, A \in \mathcal{A} \,\}$. □

4 Simetrični stožci

4.1 Liejeve algebre

Naj bo $\mathcal{O}$ odprta podmnožica prostora $\mathbb{R}^n$ in f preslikava

$$f : \mathcal{O} \longrightarrow \mathbb{R}^n .$$

Preslikavi f pravimo, da je na $\mathcal{O}$ *gladka preslikava* razreda $\mathcal{C}^r$, če je v vsaki točki $x \in \mathcal{O}$ odvedljiva natanko r krat, odvod $f^{(r)}$ pa je na $\mathcal{O}$ zvezna preslikava. Če je preslikava f v vsaki točki $x \in \mathcal{O}$ poljubno krat odvedljiva in so odvodi zvezni, pravimo, da je f gladka razreda $\mathcal{C}^\infty$. V nadaljevanju bomo z besedo gladka preslikava označevali preslikave, ki bodo na prostoru $\mathcal{O}$ vsaj enkrat zvezno odvedljive.

Naj $GL(n, \mathbb{R})$ označuje grupo vseh realnih obrnljivih matrik reda $n \times n$ z običajnim množenjem matrik, kot grupno operacijo. Podobno zapis $GL(n, \mathbb{C})$ označuje grupo obrnljivih kompleksnih matrik reda $n \times n$.

V nadaljevanju si najprej oglejmo primer, kako na naraven način konstruiramo Liejeve algebre. Naj bo G množica matrik definiranih s predpisom

$$SO(3) = \{\, X \in GL(3, \mathbb{R})\, ;\, XX^T = I\, ,\ det\, X = 1 \,\} .$$

Množica $SO(3)$, imenovana tudi množica ortogonalnih matrik z determinanto 1, je zaradi zaprtosti za množenje in invertiranje znotraj prostora $GL(3, \mathbb{R})$ grupa. Ker sta preslikavi $X \mapsto XX^T - I$ ter $X \mapsto det\, X$ zvezni in je $SO(3) \subset [\,-1, 1\,]^9$, je množica G kompaktna podmnožica prostora $\mathbb{R}^9$.

Preslikava $\gamma : (\,-T, T\,) \longrightarrow G$, podana s predpisom

$$\gamma(t) = \begin{bmatrix} \cos t & \sin t & 0 \\ -\sin t & \cos t & 0 \\ 0 & 0 & 1 \end{bmatrix} ,$$

kjer je T poljubna pozitivna konstanta, je očitno gladka preslikava na G, za katero velja, da je $\gamma(0) = I$. Seveda lahko za poljubno preslikavo zgornjega tipa, tj. gladko preslikavo za katero je $\gamma(0) = I$, izračunamo $\gamma'(t)$, ki je matrika reda 3×3. V našem primeru je

$$\gamma'(t) = \begin{bmatrix} -\sin t & \cos t & 0 \\ -\cos t & -\sin t & 0 \\ 0 & 0 & 0 \end{bmatrix}$$

in od tod

$$\gamma'(0) = \begin{bmatrix} 0 & 1 & 0 \\ -1 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}.$$

Ker je odvod funkcije γ v točki $\gamma(0) = I$ linearna transformacija iz $(-T, T)$ v G, predstavlja $\gamma'(0)$ tangentni vektor na γ v točki $\gamma(0) = I$.

Definirajmo množico $\mathcal{G}$ s predpisom

$$\mathcal{G} = \{\, \gamma'(0)\,;\, \gamma(t) \text{ gladka na } G \text{ in } \gamma(0) = I \,\}.$$

Očitno je $\mathcal{G}$ podmnožica $M(3, \mathbb{R})$, katere elementi pa niso nujno obrnljivi. Množico $\mathcal{G}$, vseh prvih odvodov gladkih funkcij skozi točko I, lahko interpretiramo kot *tangentni prostor* na G v točki I.

Oglejmo si nekatere lastnosti množice $\mathcal{G}$. Naj bosta $\gamma'(0)$ in $\delta'(0) \in \mathcal{G}$. Definirajmo preslikavo $\rho : (-T, T) \longrightarrow G$ s predpisom

$$\rho(t) = \gamma(t)\delta(t).$$

Ker velja

$$\rho'(t) = \gamma'(t)\delta(t) + \gamma(t)\delta'(t),$$

oziroma

$$\rho'(0) = \gamma'(0)\delta(0) + \gamma(0)\delta'(0) = \gamma'(0) + \delta'(0),$$

sledi, da je množica $\mathcal{G}$ zaprta za seštevanje.

Naj bo preslikava $\sigma : (-T, T) \longrightarrow G$ podana s predpisom

$$\sigma(t) = \gamma(\alpha t),$$

kjer je $\gamma'(0) \in \mathcal{G}$ in $\alpha \in \mathbb{R}$.

Ker velja

$$\sigma(0) = \gamma(0) = I$$

in

$$\sigma'(0) = \alpha\gamma'(0)\,,$$

je $\mathcal{G}$ zaprta tudi za množenje s skalarjem. Očitno je torej množica $\mathcal{G}$ vektorski prostor.

Hitro se lahko prepričamo, da sta tudi preslikavi

$$\alpha(t) = \begin{bmatrix} \cos t & 0 & \sin t \\ 0 & 1 & 0 \\ -\sin t & 0 & \cos t \end{bmatrix}$$

in

$$\beta(t) = \begin{bmatrix} 1 & 0 & 0 \\ 0 & \cos t & \sin t \\ 0 & -\sin t & \cos t \end{bmatrix}$$

gladki preslikavi za kateri velja $\alpha(0) = \beta(0) = I$. Ker so

$$\alpha'(0) = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ -1 & 0 & 0 \end{bmatrix}\,,\ \beta'(0) = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & -1 & 0 \end{bmatrix}\,,$$

$$\gamma'(0) = \begin{bmatrix} 0 & 1 & 0 \\ -1 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$$

elementi vektorskega prostora $\mathcal{G}$, sledi naslednja inkluzija

$$\mathcal{G} \supseteq \left\{ \begin{bmatrix} 0 & c & a \\ -c & 0 & b \\ -a & b & 0 \end{bmatrix} \right\} = \{\, A \in GL(3,\mathbb{R})\,;\ A = -A^T \,\}\,.$$

Pokažimo, da lahko v zgornjem izrazu inkluzijo nadomestimo z enačajem. Če je namreč $c(t)^T \cdot c(t) = I$, potem velja

$$c'(t)^T \cdot c(t) + c(t)^T \cdot c'(T) = 0\,,$$

$$c'(0)^T \cdot I + c'(0)^T \cdot I = 0\,,$$

$$c'(0)^T + c'(0) = 0\,,$$

oziroma
$$\mathcal{G} = \{\, A \in GL(3,\mathbb{R})\,;\; A = -A^T \,\}\,.$$
Naj bo $\gamma(t)$ gladka preslikava na G, ki gre skozi točko $\gamma(0) = I$. Zaradi zaprtosti G za invertiranje, je tudi preslikava $g\gamma(t)g^{-1}$, kjer je $g \in G$, gladka na G in gre skozi točko $\gamma(0) = I$. Če izračunamo odvod izraza $g\gamma(t)g^{-1}$ v točki $\gamma(0) = I$, dobimo $g\gamma'(0)g^{-1}$, kar je očitno element $\mathcal{G}$. To pa pomeni, da je $\mathcal{G}$ zaprta znotraj prostora linearnih preslikav
$$\mathcal{L}_g : \mathcal{G} \longrightarrow \mathcal{G}$$
podanih s predpisom
$$\mathcal{L}_g(X) = gXg^{-1}\,,$$
kjer je $g \in G$. Naj bo $X \in \mathcal{G}$ in $\gamma(t)$ gladka na G, ki gre skozi $\gamma(0) = I$. Pokažimo, da je preslikava $\mathcal{L}_{\gamma(t)} : \mathcal{G} \longrightarrow \mathcal{G}$ podana s predpisom
$$\mathcal{L}_{\gamma(t)}(X) = \gamma(t)X\gamma^{-1}(t)\,,$$
gladka na $\mathcal{G}$. Če v izrazu
$$\mathcal{L}_g(X) = gXg^{-1}\,,$$
naredimo substitucijo $g = \gamma(t)$, dobimo
$$\mathcal{L}_{\gamma(t)}(X) = \gamma(t)X\gamma(t)^{-1}\,.$$
Po definiciji odvoda je
$$\tfrac{d}{dt}\mathcal{L}_{\gamma(t)}(X)|_{t=0} = \lim_{t\to 0} \tfrac{1}{t}\,[\,\mathcal{L}_{\gamma(t)}(X) - \mathcal{L}_{\gamma(0)}(X)\,]\,,$$
oziroma
$$\tfrac{d}{dt}\mathcal{L}_{\gamma(t)}(X)|_{t=0} = \lim_{t\to 0} \tfrac{1}{t}\,[\,\mathcal{L}_{\gamma(t)}(X) - X\,]\,.$$
Ker sta $\mathcal{L}_{\gamma(t)}(X)$ in $X \in \mathcal{G}$, zaradi zaprtosti $\mathcal{G}$, kot podprostora $\mathbb{R}^n$, sledi, da je limita element $\mathcal{G}$. Izračunajmo to limito. Ker je $\gamma(t)\cdot\gamma(t)^{-1} = I$, po odvajanju sledi
$$\gamma'(t)\cdot\gamma(t)^{-1} + \gamma(t)\cdot(\,\tfrac{d}{dt}\gamma(t)^{-1}\,) = 0$$
in od tod
$$\tfrac{d}{dt}\gamma(t)^{-1} = -\,\gamma(t)^{-1}\gamma'(t)\gamma(t)^{-1}\,.$$

Z uporabo dobljene zveze sledi

$$\tfrac{d}{dt}\mathcal{L}_{\gamma(t)}(X) = \tfrac{d}{dt}[\,\gamma(t)X\gamma(t)^{-1}\,] =$$
$$= \gamma'(t)X\gamma(t)^{-1} + \gamma(t)X'\gamma(t)^{-1} + \gamma(t)X[\,\tfrac{d}{dt}\gamma(t)^{-1}\,] =$$
$$= \gamma'(t)X\gamma(t)^{-1} - \gamma(t)X\gamma(t)^{-1}\gamma'(t)\gamma(t)^{-1}\,.$$

Če v izraz vstavimo za $t = 0$, sledi

$$\gamma'(0)X - X\gamma'(0) \in \mathcal{G}\,.$$

Od tod sledi, da je množica $\mathcal{G}$ zaprta za operacijo

$$[\,X, Y\,] = XY - YX\,,$$

ki jo imenujemo *Liejev komutator*. Množico $\mathcal{G}$, ki je realen vektorski prostor in je zaprta za Liejev komutator, imenujemo *Liejeva algebra* množice $\mathcal{G}$.

Hitro se lahko prepričamo, da sta množici $GL(n,\mathbb{R})$ in $GL(n,\mathbb{C})$, opremljeni z operacijo Liejevega komutatorja, Liejevi algebri. Označimo ju z $\mathcal{GL}(n,\mathbb{R})$ in $\mathcal{GL}(n,\mathbb{C})$. Če torej zgornji primer matrik reda 3×3 posplošimo na grupo

$$SO(n) = \{\,X \in GL(n,\mathbb{R})\,;\; XX^T = I\,,\; det\,X = 1\,\}\,,$$

je njej pripadajoča Liejeva algebra, množica

$$\mathcal{SO}(n) = \{\,X \in \mathcal{GL}(n,\mathbb{R})\,;\; X + X^T = 0\,\}\,,$$

Podobno, kot smo to storili na primeru grupe $SO(n,\mathbb{R})$, lahko tudi naslednjim linearnim grupam

$$U(n) = \{\,X \in GL(n,\mathbb{C})\,;\; XX^* = I\,\}\,,$$
$$SU(n) = \{\,X \in GL(n,\mathbb{C})\,;\; XX^* = I\,,\; det\,X = 1\,\}\,,$$
$$SL(n,\mathbb{R}) = \{\,X \in GL(n,\mathbb{R})\,;\; det\,X = 1\,\}\,,$$
$$SL(n,\mathbb{C}) = \{\,X \in GL(n,\mathbb{C})\,;\; det\,X = 1\,\}\,,$$

priredimo ustrezne Liejeve algebre

$$\mathcal{U}(n) = \{\,X \in \mathcal{GL}(n,\mathbb{C})\,;\; X + X^* = 0\,\}\,,$$

$$\mathcal{SU}(n) = \{ X \in \mathcal{GL}(n,\mathbb{C})\,;\; X + X^* = 0\,,\; Sl\,X = 0 \}\,,$$
$$\mathcal{SL}(n,\mathbb{R}) = \{ X \in \mathcal{GL}(n,\mathbb{R})\,;\; Sl\,X = 0 \}\,,$$
$$\mathcal{SL}(n,\mathbb{C}) = \{ X \in \mathcal{GL}(n,\mathbb{C})\,;\; Sl\,X = 0 \}\,.$$

Posplošimo definicijo Liejeve algebre na poljuben vektorski prostor. Vektorski prostor $\mathcal{L}$ nad obsegom $\mathbb{F}$, opremljen z operacijo komutatorja

$$[\,x,y\,] = xy - yx\,,$$

kjer sta $x, y \in \mathcal{L}$, imenujemo *Liejeva algebra* nad $\mathbb{F}$, če velja

($L1$) komutator je bilinearna operacija;

($L2$) $[\,x,x\,] = 0$, za vsak $x \in \mathcal{L}$;

($L3$) $[\,x,[\,y,z\,]\,] + [\,y,[\,z,x\,]\,] + [\,z,[\,x,y\,]\,] = 0\,, \forall\, x,y,z \in \mathcal{L}$.

Aksiom ($L3$) imenujemo *Jacobijeva identiteta.*

Ker je Liejev komutatator antikomutativna operacija,

$$[\,x,y\,] = xy - yx = -(\,yx - xy\,) = -\,[\,y,x\,]$$

velja

$$[\,x,y\,] + [\,y,x\,] = 0\,.$$

Če v dobljeni izraz vstavimo $x = y$, dobimo

$$2\,[\,x,x\,] = 0\,.$$

V algebrah, katerih karakteristika je različna od 2, torej lahko aksiom ($L2$) nadomestimo z enakostjo

$$[\,x,y\,] = -\,[\,y,x\,]\,,$$

kjer sta $x, y \in \mathcal{L}$.

V nadaljevanju bodo predmet naše obravnave predvsem Liejeve algebre, ki so prirejene grupi avtomorfizmov danega stožca. Pripadajoče Liejeve algebre so vedno predstavljene z množico matrik.

V uvodu razdelka smo grupi G, vseh ortogonalnih matrik z determinanto 1, priredili Liejevo algebro $\mathcal{G}$. Podobno lahko tudi grupi S, ki je zaprta za adjungiranje, priredimo ustrezno Liejevo algebro $\mathcal{S}$. Če je torej

$$S = S^*\,,$$

je njej pripadajoča Liejeva algebra, množica

$$\mathcal{S} = \{ \gamma'(0)\,;\, \gamma : (-T,T) \to S \text{ gladka in } \gamma(0) = I \}\,.$$

Naj bo $s \in \mathcal{S}$. Potem obstaja taka gladka preslikava $\sigma : (-T,T) \to S$, da je $\sigma(0) = 1$ in $\sigma'(0) = s$. Definirajmo preslikavo $\delta : (-T,T) \to S$, s predpisom $\delta(t) = \sigma(t)^*$. Ker je $\sigma(t)^* \in S^*$ ter velja $S^* = S$, sledi $\delta(t) \in S$. Očitno je $\delta'(t) = \sigma'(t)^*$ in od tod $\delta'(0) = \sigma'(0)^* = s^*$. Ker je torej tudi $s^* \in \mathcal{S}$ sledi

$$\mathcal{S} = \mathcal{S}^*\,.$$

Definirajmo množici

$$\mathcal{S}_+ = \{ X \in \mathcal{S}\,;\, X = X^* \}$$

in

$$\mathcal{S}_- = \{ X \in \mathcal{S}\,;\, X = -X^* \}\,,$$

ter si oglejmo njun presek. Naj bo $X \in \mathcal{S}_+ \cap \mathcal{S}_-$. Ker je potem $X = X^* = -X$, sledi $X = 0$, oziroma

$$\mathcal{S}_+ \cap \mathcal{S}_- = \{0\}\,.$$

Ker sta $\mathcal{S}_+$ in $\mathcal{S}_- \subseteq \mathcal{S}$, očitno sledi inkluzija

$$\mathcal{S}_+ + \mathcal{S}_- \subseteq \mathcal{S}\,.$$

Naj bo $X \in \mathcal{S}$. Ker je $X^* \in \mathcal{S}^*$ in velja $\mathcal{S}^* = \mathcal{S}$, sledi $\frac{1}{2}(X + X^*) \in \mathcal{S}$. Ker je $\frac{1}{2}(X + X^*)$ simetrična matrika, sledi $\frac{1}{2}(X + X^*) \in \mathcal{S}_+$. Podobno je $\frac{1}{2}(X - X^*) \in \mathcal{S}$. Ker je $\frac{1}{2}(X - X^*)$ antisimetrična matrika, sledi $\frac{1}{2}(X - X^*) \in \mathcal{S}_-$. Če torej X zapišemo kot $X = \frac{1}{2}(X + X^*) + \frac{1}{2}(X - X^*)$, sledi $X \in \mathcal{S}_+ + \mathcal{S}_-$, oziroma

$$\mathcal{S} \subseteq \mathcal{S}_+ + \mathcal{S}_-\,.$$

Če torej združimo zgornji inkluziji in upoštevamo, da je $\mathcal{S}_+ \cap \mathcal{S}_- = \{0\}$, sledi

$$\mathcal{S} = \mathcal{S}_+ \oplus \mathcal{S}_-\,.$$

Oglejmo si množico

$$[\mathcal{S}_+, \mathcal{S}_+] = \{ XY - YX,:\ X, Y \in \mathcal{S}_+ \}\,.$$

Naj bosta $X, Y \in \mathcal{S}_+$. Ker velja $X = X^*$ in $Y = Y^*$, sledi

$$[X, Y]^* = (XY - YX)^* = Y^*X^* - X^*Y^* = YX - XY = -[X, Y],$$

oziroma

$$[\mathcal{S}_+, \mathcal{S}_+] \subseteq \mathcal{S}_- .$$

Podobno za

$$[\mathcal{S}_-, \mathcal{S}_-] = \{ XY - YX, : X, Y \in \mathcal{S}_- \},$$

velja

$$[\mathcal{S}_-, \mathcal{S}_-] \subseteq \mathcal{S}_- .$$

Če sta namreč $X, Y \in \mathcal{S}_-$, velja $X = -X^*$ in $Y = -Y^*$. Od tod sledi

$$[X, Y]^* = (XY - YX)^* = Y^*X^* - X^*Y^* = YX - XY = -[X, Y].$$

Končno naj bosta $X \in \mathcal{S}_+$ in $Y \in \mathcal{S}_-$. Ker velja $X = X^*$ in $Y = -Y^*$, sledi

$$[X, Y]^* = (XY - YX)^* = Y^*X^* - X^*Y^* = -YX + XY = [X, Y],$$

oziroma

$$[\mathcal{S}_+, \mathcal{S}_-] \subseteq \mathcal{S}_+ .$$

Analogno je

$$[\mathcal{S}_-, \mathcal{S}_+] \subseteq \mathcal{S}_+ .$$

Če torej obravnavamo $\mathcal{S}_-$ kot podprostor prostora $\mathcal{S}$, je $\mathcal{S}_-$ zaprta znotraj $\mathcal{S}$ za operacijo Liejevega komutatorja

Zgornji primer nas je prepričal v smiselnost definicije pojma *Liejeve podalgebre*. Posplošimo torej definicijo na poljubno Liejevo algebro $\mathcal{L}$. Podprostor $\mathcal{K}$ imenujemo *Liejeva podalgebra* prostora $\mathcal{L}$, če za poljubna x in $y \in \mathcal{K}$ velja $[x, y] \in \mathcal{K}$.

4.2 Simetrični stožci in Liejeve algebre

Ponovimo definicijo simetričnega stožca iz uvodnega poglavja.

Odprt konveksen stožec $\Omega \subset \mathbb{R}^n$ imenujemo *simetričen*, če je *homogen* glede na njegovo grupo avtomorfizmov

$$G(\Omega) = \{ g \in GL(n, \mathbb{R}) \,;\, g\,\Omega = \Omega \}$$

in *sebi dualen* v smislu, da je njegovo zaprtje $\overline{\Omega}$, enako

$$\overline{\Omega} = \{\, y \in \mathbb{R}^n\,;\, \langle\, x, y\,\rangle \geq 0\,,\, \forall\, x \in \overline{\Omega}\,\}\,.$$

V uvodnem poglavju smo dokazali, da je avtomorfizemska grupa sebi dualnega stožca Ω zaprta za transponiranje.

Definirajmo *ortogonalno grupo stožca* Ω s predpisom

$$O(\Omega) = G(\Omega) \cap O(n)\,,$$

kjer je $O(n)$ ortogonalna grupa prostora $\mathbb{R}^n$, podana kot

$$O(n) = \{\, A \in \mathbb{R}^{n\times n}\,;\, AA^* = I\,\}\,.$$

Oglejmo si ortogonalne grupe doslej znanih simetričnih stožcev, stožcev pozitivnih matrik nad $\mathbb{R}, \mathbb{C}$ in $\mathbb{H}$ ter Lorentzovega stožca.

Zgled 1. Naj bo $\mathcal{P}(n, \mathbb{R})$ stožec pozitivnih realnih matrik znotraj prostora pripadajočih simetričnih matrik $\mathcal{S}(n, \mathbb{R})$. Če torej označimo

$$\mathcal{S}(n, \mathbb{R}) = \{\, X \in \mathbb{R}^{n\times n}\,;\, X^T = X\,\}\,,$$

je pripadajoči stožec

$$\mathcal{P}(n, \mathbb{R}) = \{\, Y \in \mathcal{S}(n, \mathbb{R})\,;\, Y > 0\,\}\,.$$

Grupo avtomorfizmov stožca $\mathcal{P}(n, \mathbb{R})$ tvorijo preslikave

$$P_A \,:\, \mathbb{R}^{n\times n} \longrightarrow \mathbb{R}^{n\times n}\,,$$

podane s predpisom

$$P_A(Y) = A\,Y A^T\,,$$

kjer je $A \in GL(n, \mathbb{R})$. Ker je na prostoru $\mathbb{R}^{n\times n}$ skalarni produkt definiran s predpisom $\langle\, X, Y\,\rangle = Sl\,(XY)$ in zanj veljata identiteti $Sl\,(X) = Sl\,(X^T)$ ter $Sl\,(XY) = Sl\,(YX)$, sledi

$$\langle\, P_A X, Y\,\rangle = \langle\, AXA^T, Y\,\rangle = Sl\,(\,AXA^T Y\,) = Sl\,(\,A^T Y AX\,) =$$

$$= Sl\,(XA^T Y A\,) = \langle\, X, A^T Y A\,\rangle = \langle\, X, P_{A^T} Y\,\rangle\,,$$

oziroma

$$P_A^T = P_{A^T}\,.$$

Če je $P_A(I) = I$, je $AA^T = I$, kar v prostorih s končno dimenzijo pomeni, da je A ortogonalna matrika. Ker potem velja

$$P_A P_A^T Y = P_A P_{A^T} Y = A(A^T Y A)A^T = AA^T Y AA^T = Y\,,$$

sledi, da je $P_A P_A^T = I$, kar pomeni, da je tudi P_A ortogonalna. Od tod sledi, da je

$$O(\mathcal{P}(n,\mathbb{R})) = \{\, P_A\,;\, A \in O(n)\,\}\,,$$

oziroma

$$O(\mathcal{P}(n,\mathbb{R})) = \{\, \phi \in G(\mathcal{P}(n,\mathbb{R}))\,;\, \phi(I) = I\,\}\,.$$

Zgled 2. Naj bo $\mathcal{P}(n,\mathbb{F})$, $\mathbb{F} \in \{\,\mathbb{C},\mathbb{H}\,\}$, stožec pozitivnih kompleksnih oziroma kvaternionskih matrik znotraj prostora pripadajočih simetričnih matrik $\mathcal{S}(n,\mathbb{F})$. Če torej označimo

$$\mathcal{S}(n,\mathbb{F}) = \{\, X \in \mathbb{F}^{n\times n}\,;\, X^* = X\,\}\,,$$

kjer * pomeni adjungiranje znotraj $\mathbb{C}^{n\times n}$ in transponiranje znotraj $\mathbb{H}^{n\times n}$, je pripadajoči stožec

$$\mathcal{P}(n,\mathbb{F}) = \{\, Y \in \mathcal{S}(n,\mathbb{F})\,;\, Y > 0\,\}\,.$$

Grupo avtomorfizmov stožca $\mathcal{P}(n,\mathbb{F})$ tvorijo preslikave

$$P_A \,:\, \mathbb{F}^{n\times n} \longrightarrow \mathbb{F}^{n\times n}\,,$$

podane s predpisom

$$P_A(Y) = A\,Y A^*\,,$$

kjer je $A \in GL(n,\mathbb{F})$. Ker je na prostoru $\mathbb{C}^{n\times n}$ realni skalarni produkt definiran s predpisom $\langle\, X, Y\,\rangle = Re\,Sl\,(XY)$ in veljata identiteti $Re\,Sl\,(X) = Re\,Sl\,(X^*)$ ter $Re\,Sl\,(XY) = Re\,Sl\,(YX)$, sledi

$$P_A^* = P_{A^*}\,.$$

Če je $P_A(I) = I$, je $AA^* = I$, kar v prostorih s končno dimenzijo pomeni, da je A unitarna matrika. Podobno kot v prejšnjem zgledu, je tudi P_A unitarna matrika, od koder sledi

$$O(\Omega_{\mathbb{R}}) = \{\, P_A\,;\, A \in O(n)\,\}\,,$$

oziroma

$$O(\Omega_{\mathbb{R}}) = \{\, \phi \in G(\Omega_{\mathbb{R}})\,;\, \phi(I) = I\,\}\,.$$

Zgled 3. Naj bo $\mathcal{L}_n$ Lorentzov časovni stožec oziroma stožec prihodnosti. V drugem poglavju smo $\mathcal{L}_n$ definirali kot

$$\mathcal{L}_n = \{\, (\alpha, x)\, ;\, \alpha > ||\, x\, ||\, \} \subset \mathbb{R} \times \mathbb{R}^{n-1} \, .$$

V trditvi 2.4.4 smo dokazali, da avtomorfizmu stožca $\mathcal{L}_n$, ki ohranja element $1 + 0 = I$, ustreza unitarna matrika. To pa pomeni, da je pripadajoča ortogonalna grupa Lorentzovega stožca

$$O(\mathcal{L}_n) = \{\, \phi \in G(\mathcal{L}_n)\, ;\, \phi(I) = I\, \} \, .$$

Omenjeni zgledi nas napeljujejo na misel, da za vsak simetričen stožec Ω obstaja tak element $e \in \Omega$, da velja

$$O(\Omega) = \{\, \phi \in G(\Omega)\, ;\, \phi(e) = e\, \} \, .$$

V nadaljevanju bomo z G označevali komponento enote grupe avtomorfizmov $G(\Omega)$. Definirajmo preslikavo

$$\psi : G(\Omega) \to G(\Omega)$$

s predpisom

$$\psi(g) = g^* \, .$$

Zaradi zveznosti tako definirane preslikave, je $\psi(G)$ očitno vsebovana v neki komponenti $G(\Omega)$. Ker je $\psi(e) = e$ sledi, da je $\psi(e) \in G$ in od tod $\psi(G) \subset G$. Grupa G je torej zaprta za transponiranje.

Definirajmo množico K s predpisom

$$K = G \cap O(\Omega) \, .$$

Ker sta G in K Liejevi grupi, jima pripadata ustrezni Liejevi algebri. Označimo z $\mathcal{G}$ Liejevo algebro, ki pripada grupi G in z $\mathcal{G}_-$ Liejevo algebro, ki pripada grupi K. Pokažimo, da je

$$\mathcal{G}_- = \{\, X \in \mathcal{G}\, ;\, X^* = -X\, \} \, .$$

Ker sta Liejevim grupam G in K pripadajoči algebri oblik $\mathcal{K} = \{\, \gamma'(0)\, ;\, \gamma$ gladka na K in $\gamma(0) = I\, \}$ in $\mathcal{G} = \{\, \gamma'(0)\, ;\, \gamma$ gladka na G in $\gamma(0) = I\, \}$, je očitno $\mathcal{K} \subseteq \mathcal{G}$. Če z $\mathcal{O}(\mathbb{R}^n)$ označimo Liejevo algebro, ki pripada grupi ortogonalnih matrik in upoštevamo, da je $K \subseteq O(\Omega) \subseteq O(\mathbb{R}^n)$, sledi

$$\mathcal{K} \subseteq \mathcal{O}(\mathbb{R}^n) = \{\, X \in \mathcal{G}\,;\, X^T = -X \,\},$$

kar pomeni, da je $\mathcal{K} \subseteq \mathcal{G}_-$. Naj bo $X \in \mathcal{G}_-$. Potem je $\gamma(t) = \exp(\,tX)$ gladka preslikava na Liejevi grupi G, za katero velja $\gamma(0) = I$ [Knapp, 1988, str. 10]. Ker je

$$\exp(\,tX)\exp(\,tX)^* = \exp(\,tX)\exp(\,(tX)^*) = \exp(\,tX)\exp(\,tX^*) =$$

$$= \exp(\,tX)\exp(\,-tX) = \exp(\,tX - tX) = \exp(0) = I\,,$$

sledi, da je $\gamma(t) \in G \cap O(\Omega) = K$ in $\gamma'(0) \in \mathcal{K}$. Ker je $\gamma'(t) = X\exp(\,tX)$ in od tod $\gamma'(0) = X\,I = X$, sledi, da je $X \in \mathcal{K}$. To pomeni, da je $\mathcal{G}_- \subset \mathcal{K}$, oziroma $\mathcal{G}_- = \mathcal{K}$.

Če definiramo Liejevo algebro $\mathcal{G}_+$ s predpisom

$$\mathcal{G}_+ = \{\, X \in \mathcal{G} \,:\, X^* = X \,\},$$

zaradi zaprtosti $\mathcal{G}$ za transponiranje, sledi

$$\mathcal{G} = \mathcal{G}_+ \oplus \mathcal{G}_-\,.$$

V prejšnjem razdelku smo za podalgebri $\mathcal{G}_+$ in $\mathcal{G}_-$ dokazali inkluziji

$$[\,\mathcal{G}_+, \mathcal{G}_+\,] \subset \mathcal{G}_-\,,$$

$$[\,\mathcal{G}_-, \mathcal{G}_+\,] \subset \mathcal{G}_+\,.$$

V nadaljevanju naj G_e pomeni podgrupo $G_e = \{\, g \in G\,,\, g(e) = e\,\}$, torej stabilizator elementa e glede na grupo G.

Izrek 2.1. *Naj bo Ω simetričen stožec. Potem obstajajo taki elementi $e \in \Omega$, da velja*

$$G(\Omega) \cap O(\mathbb{R}^n) \subset G(\Omega)_e\,.$$

Za vsak tak element e je

$$G_e = K$$

povezana podgrupa v G.

Dokaz: Ker je grupa $O(\mathbb{R}^n)$ kompaktna, je očitno tudi $H = G(\Omega) \cap O(\mathbb{R}^n)$ kompaktna znotraj $G(\Omega)$. Po trditvi 1.4.4 potem obstaja tak e, da je $G(\Omega) \cap O(\mathbb{R}^n) \subset G(\Omega)_e$. Ker je $G_e = \{\, g \in G\,;\, g(e) = e\,\}$, očitno velja $G_e = G(\Omega)_e \cap G$. Od tod zaradi $K = G \cap O(\mathbb{R}^n) \subseteq G(\Omega) \cap O(\mathbb{R}^n)$ sledi, da je $K \subset G(\Omega)_e$. Ker je $K \subseteq G$, sledi $K \subset G_e$.

Naj bo $\mathcal{G}_e$ Liejeva algebra grupe G_e in $X \in \mathcal{G}_e$. Ker je $G_e \subset G$, je očitno $\mathcal{G}_e \subset \mathcal{G}$. Zapišimo torej X kot $X_+ + X_-$, kjer sta $X_+ \in \mathcal{G}_+$ in $X_- \in \mathcal{G}_-$. Ker je $K \subset G_e$, je $\mathcal{K} \subset \mathcal{G}_e$. Če upoštevamo, da je $\mathcal{K} = \mathcal{G}_-$, sledi $\mathcal{G}_- \subset \mathcal{G}_e$, oziroma $X_- \in \mathcal{G}_e$. To pomeni, da je tudi $X - X_- = X_+ \in \mathcal{G}_e$. Od tod sledi, da je $\exp(\,tX_+)$ v Liejevi grupi algebre $\mathcal{G}_e$, oziroma $\exp(\,tX_+) \in G_e$. Ker je po trditvi 1.4.3 grupa G_e kompaktna množica, zaradi omejenosti sledi, da je $X_+ = 0$. To pomeni, da je $\mathcal{G}_e \subset \mathcal{G}_- = \mathcal{K}$, oziroma $G_e \subset K$. □

Trditev 2.2. *Naj bo $X \in \mathcal{G}$. Potem $X \in \mathcal{G}_-$ natanko tedaj, ko je*

$$X(e) = 0\,.$$

Dokaz: Naj bo $X \in \mathcal{G}_-$. V prejšnjem izreku smo pokazali, da je $\mathcal{G}_-$ Liejeva algebra tako za K, kot za G_e. Za vsak $t \in \mathbb{R}$ je torej $\exp(\,tX) \in G_e$. To pomeni, da je

$$\exp(\,tX)\,e = e\,.$$

Če identiteto odvajamo, dobimo

$$X(\,\exp(\,tX)\,e\,) = 0\,.$$

Od tod za $t = 0$ sledi $X(\,Ie) = 0$, oziroma $X(e) = 0$.

Naj bo $X(e) = 0$. Če X zapišemo v obliki $X = X_+ + X_-$, kjer sta $X_+ \in \mathcal{G}_+$ in $X_- \in \mathcal{G}_-$, ter upoštevamo, da je tedaj $X_+(e) = 0$, sledi $\exp(\,tX_+)\,e = e$. To pomeni, da je $\exp(\,tX_+) \in G_e$. Ker je G_e kompaktna, je očitno $X_+ = 0$. Od tod sledi, da je $X \in \mathcal{G}_-$. □

4.3 Simetrični stožci in Jordanske algebre

Naj bo Ω simetričen stožec evklidskega prostora $\mathcal{V}$ in $e \in \Omega$ tak fiksen element izreka 2.1, da je njegov stabilizator ravno grupa K. Definirajmo preslikavo

$$T\,:\mathcal{G}_+ \longrightarrow \mathcal{V}$$

s predpisom $T(X) = X(e)\,.$

Ker je T po prejšnjem izreku injektivna, je $dim(\mathcal{G}_+) \leq dim(\mathcal{V})$. Če je $dim(\mathcal{G}_+) = dim(\mathcal{V})$, je T očitno bijektivna. Pokažimo, da je bijektivna tudi v primeru, ko je $dim(\mathcal{G}_+) < dim(\mathcal{V})$. Definirajmo preslikavo

$$\rho : \mathcal{G}_+ \longrightarrow \mathcal{V}$$

s predpisom $\rho(X) = \exp(X)\, e$.

Množica $\{\exp(X), X \in \mathcal{G}\}$ je komponenta enote grupe G. Ker po trditvi 2.2 velja $\mathcal{G}_-(e) = 0$, sledi

$$\rho(\mathcal{G}_+) = \{\exp(X)\, e\,;\, X \in \mathcal{G}\} = \{\exp(X)\, e\,;\, X \in \mathcal{G}_+\}.$$

Če upoštevamo, da komponenta enote tranzitivno delujoče grupe tudi sama deluje tranzitivno [Faraut, 1994, str. 5], je zaloga vrednosti preslikave ρ enaka $G(\Omega)\, e = \Omega$. Ker je Ω odprta množica v $\mathbb{R}^n$, je njena mera neničelna.

Po drugi strani preslikava ρ slika iz $\mathbb{R}^k$ v $\mathbb{R}^n$, kjer je $k < n$ (k je dimenzija prostora $\mathcal{G}_+$, n pa dimenzija prostora $\mathcal{V}$). To pomeni, da je $rang(d\rho_X) \leq k < n$, v vseh točkah definicijskega območja. Na tem mestu lahko uporabimo klasičen Sardov izrek, ki ga povzemamo po [Milnor, 1969, str. 10] in se glasi:

Izrek 3.1. *(Sardov) Naj bosta $f : U \longrightarrow \mathbb{R}^n$ gladka preslikava in U odprta množica v $\mathbb{R}^m$. Naj bo*

$$C = \{x \in U, rang(df_X) < n\}.$$

Potem ima $f(C)$ mero 0 v prostoru $\mathbb{R}^n$.

Ker je preslikava ρ gladka, lahko Sardov izrek uporabimo na množici $C = \mathcal{G}_+$. Po njem ima množica $\rho(C) = \Omega$ mero 0, kar je protislovje s trditvijo, da je mera Ω neničelna. Ker torej možnost $dim(\mathcal{G}_+) < dim(\mathcal{V})$ odpade, je T surjektivna, oziroma bijektivna.

Ker je T bijekcija obstaja njen inverz. Označimo ga z L. Za vsak element $x \in \mathcal{V}$ je potem $L(x)$ tak enolično določen element algebre $\mathcal{G}_+$, da velja

$$L(x)\, e = x.$$

Naj bosta $L(x)\, e = x$ in $L(y)\, e = y$. Po definiciji je

$$(L(x) + L(y))\, e = x + y = L(x + y)\, e.$$

Zaradi bijektivnosti preslikave $X \mapsto X(e)$ sledi

$$L(x+y) = L(x) + L(y)\,,$$

oziroma, preslikava $x \mapsto L(x)$ je linearna.

Če na prostoru $\mathcal{V}$ definiramo množenje s predpisom

$$x \circ y = L(x)\, y\,,$$

je $\circ$ bilinearna operacija. Za poljubne $x_1, x_2, y_1, y_2 \in \mathcal{V}$ in $\alpha, \beta \in \mathbb{R}$ namreč velja

$$(\, x_1 + x_2\,) \circ y_1 = L(x_1 + x_2)\, y_1 = (\, L(x_1) + L(x_2)\,)\, y_1 =$$

$$= L(x_1)\, y_1 + L(x_2)\, y_1 = x_1 \circ y_1 + x_2 \circ y_1\,,$$

$$x_1 \circ (\, y_1 + y_2\,) = L(x_1)\,(\, y_1 + y_2\,) = L(x_1)\, y_1 + L(x_1)\, y_2 =$$

$$= x_1 \circ y_1 + x_1 \circ y_2\,,$$

$$(\, \alpha x_1\,) \circ y_1 = L(\alpha x_1)\, y_1 = \alpha\, L(x_1)\, y_1 = \alpha\,(\, x_1 \circ y_1\,)\,,$$

$$x_1 \circ (\, \beta y_1\,) = L(x_1)\,(\, \beta y_1\,) = \beta\, L(x_1)\, y_1 = \beta\,(\, x_1 \circ y_1\,)\,.$$

Pokažimo, da je zgoraj definirano množenje tudi komutativno. Naj bosta x in y poljubna elementa prostora $\mathcal{V}$. Po zgoraj dokazanem sta potem $L(x)$ in $L(y)$ enolično določena elementa $\mathcal{G}_+$. Ker po trditvi 2.2 velja enakost $\mathcal{G}_-(e) = 0$, za poljubna elementa $\mathcal{G}_+$ pa velja $[\,\mathcal{G}_+, \mathcal{G}_+\,] \subset \mathcal{G}_-$, sledi

$$0 = [\, L(x), L(y)\,]\, e = L(x)L(y)\, e - L(y)L(x)\, e = x \circ y - y \circ x\,,$$

oziroma

$$x \circ y = y \circ x\,.$$

Ker je za poljuben $x \in \mathcal{G}_+$ preslikava $L(x)$ simetrična (po definiciji prostora $\mathcal{G}_+$), za poljubne elemente u, v in $x \in \mathcal{V}$ velja

$$\langle\, L(x)u, v\,\rangle = \langle\, u, L(x)v\,\rangle\,,$$

kjer je $\langle\, .,.\,\rangle$ skalarni produkt na prostoru $\mathcal{V}$. Omenjeno lastnost imenujemo *asociativnost skalarnega produkta.*

Definirajmo *asociator* elementov x, y in $z \in \mathcal{V}$ s predpisom

$$[\, x, z, y\,] = x \circ (\, z \circ y\,) - (\, x \circ z\,) \circ y = [\, L(x), L(y)\,]\, z\,.$$

Izračunajmo vrednost izraza

$$[\,[\,L(x), L(y)\,]\,, L(z)\,]\,e\,.$$

Ker je $[\,L(x), L(y)\,] \in \mathcal{G}_-$ sledi

$$[\,[\,L(x), L(y)\,]\,, L(z)\,]\,e = [\,L(x), L(y)\,]\,L(z)\,e - L(z)\,[\,L(x), L(y)\,]\,e =$$

$$= [\,L(x), L(y)\,]\,z = [\,x, y, z\,] = L(\,[\,x, z, y\,]\,)\,e\,.$$

Zaradi bijektivnosti velja

$$[\,[\,L(x), L(y)\,]\,, L(z)\,] = L(\,[\,x, z, y\,]\,)\,.$$

Če uporabimo levo stran dobljene identitete na elementu $z \in \mathcal{V}$, dobimo

$$[\,[\,L(x), L(y)\,]\,, L(z)\,]\,z = [\,L(x), L(y)\,]\,L(z)\,z - L(z)\,[\,L(x), L(y)\,]\,z =$$

$$= [\,L(x), L(y)\,]\,(\,z \circ z\,) - L(z)\,(\,L(x)L(y)\,z - L(y)L(x)\,z\,) =$$

$$= L(x)L(y)\,z^2 - L(y)L(x)\,z^2 - L(z)\,(\,L(x)\,(\,y \circ z\,) - L(y)\,(\,x \circ z\,)\,) =$$

$$= x \circ (\,y \circ z^2\,) - y \circ (\,x \circ z^2\,) - z \circ (\,x \circ (\,y \circ z\,) - y \circ (\,x \circ z\,)\,) =$$

$$= [\,x, z^2, y\,] - z \circ [\,x, z, y\,]\,.$$

Ker je

$$L(\,[\,x, z, y\,]\,)\,z = z \circ [\,x, z, y\,]\,,$$

po združitvi dobljenih enakosti sledi

$$[\,x, z^2, y\,] = 2\,[\,x, z, y\,] \circ z\,. \qquad (1)$$

Za poljubne elemente x, y in $z \in \mathcal{V}$ izračunajmo vrednost skalarnega produkta $\langle\,[\,x^2, y, x\,]\,,\, z\,\rangle$. Z upoštevanjem asociativnosti skalarnega produkta sledi

$$\langle\,[\,x^2, y, x\,]\,,\, z\,\rangle = \langle\,x^2 \circ (\,y \circ x\,) - (x^2 \circ y\,) \circ x\,,\, z\,\rangle =$$

$$= \langle\,x^2 \circ (\,y \circ x\,)\,,\, z\,\rangle - \langle\,(\,x^2 \circ y\,) \circ x\,,\, z\,\rangle =$$

$$= \langle\,x^2\,,\, (\,y \circ x\,) \circ z\,\rangle - \langle\,x^2\,,\, (\,x \circ z\,) \circ y\,\rangle =$$

$$= \langle\,x^2\,,\, (\,y \circ x\,) \circ z - (\,x \circ z\,) \circ y\,\rangle = \langle\,x^2\,,\, [\,z, x, y\,]\,\rangle\,. \qquad (2)$$

Podobno velja tudi

$$\begin{aligned}\langle\,[\,x^2,y,x\,]\,,\,z\,\rangle &= \langle\,x^2\circ(\,y\circ x\,)-(\,x^2\circ y\,)\circ x\,,\,z\,\rangle = \\ &= \langle\,x^2\circ(\,y\circ x\,)\,,\,z\,\rangle-\langle\,(\,x^2\circ y\,)\circ x\,,\,z\,\rangle = \\ &= \langle\,x\,,\,(\,z\circ x^2\,)\circ y\,\rangle-\langle\,x\,,\,z\circ(\,x^2\circ y\,)\,\rangle = \\ &= \langle\,x\,,\,(\,z\circ x^2\,)\circ y-z\circ(\,x^2\circ y\,)\,\rangle=\langle\,x\,,\,[\,y,x^2,z\,]\,\rangle\,. \end{aligned} \tag{3}$$

Če v identiteti (1) naredimo substitucijo $x = y$, $z = x$ in $y = z$, dobimo

$$[\,y,x^2,z\,]=2\,[\,y,x,z\,]\circ x\,.$$

Po identiteti (3) potem sledi

$$\begin{aligned}\langle\,[\,x^2,y,x\,]\,,\,z\,\rangle &= \langle\,x\,,\,2\,[\,y,x,z\,]\circ x\,\rangle = \\ &= 2\,\langle\,x\,,\,[\,y,x,z\,]\circ x\,\rangle = 2\,\langle\,x^2\,,\,[\,y,x,z\,]\,\rangle\,.\end{aligned}$$

Ker je

$$[\,y,x,z\,]=-\,[\,z,x,y\,]\,,$$

sledi

$$\langle\,[\,x^2,y,x\,]\,,\,z\,\rangle=-2\,\langle\,x^2\,,\,[\,z,x,y\,]\,\rangle\,. \tag{4}$$

Po združitvi (2) in (4), za vsak $z \in \mathcal{V}$ velja

$$\langle\,[\,x^2,y,x\,]\,,\,z\,\rangle=0\,.$$

Od tod sledi

$$[\,x^2,y,x\,]=0\,,$$

oziroma

$$x^2\circ(\,x\circ y\,)=x\circ(\,x^2\circ y\,)\,. \tag{5}$$

Algebrsko strukturo, opremljeno z operacijo množenja $\circ$, ki zadošča dobljeni enakosti in je hkrati še komutativna, imenujemo *jordanska algebra.* Dokazali smo torej

Izrek 3.2. *Naj bo Ω simetričen stožec evklidskega prostora $\mathcal{V}$. Tedaj je $\mathcal{V}$ mogoče opremiti s strukturo jordanske algebre.*

Identiteta (5) je v matematični literaturi znana že iz časov pred pojavom teorije simetričnih stožcev in z njo povezanih jordanskih algeber. Jordanske algebre so se prvič pojavile v literaturi leta 1934. Njihovi utemeljitelji, Jordan, von Neumann in Wigner, so pojem jordanske algebre vpeljali ob iskanju ustreznega formalizma za obravnavo kvantne mehanike.

5 Algebraična analiza evklidskih algeber

5.1 Jordanske algebre

Posplošimo definicijo jordanske algebre na poljuben vektorski prostor $\mathcal{J}$ nad obsegom $\mathbb{F}$.

Vektorski prostor $\mathcal{J}$, opremljen z bilinearno operacijo

$$\circ \,:\, \mathcal{J} \times \mathcal{J} \longrightarrow \mathcal{J}\,,$$

imenujemo *jordanska algebra* nad $\mathbb{F}$, če za vsak $a, b \in \mathcal{J}$ velja

$(J1)$ $a \circ b = b \circ a\,,$

$(J2)$ $a^2 \circ (\,a \circ b\,) = a \circ (\,a^2 \circ b\,)\,,$

pri čemer je $a^2 = a \circ a$.

Zgled 1. Naj bo $\mathcal{S}$ množica vseh simetričnih matrik in $A, B \in \mathcal{S}$. Ker velja

$$(\,A + B\,)^* = A^* + B^* = A + B\,,$$

je $\mathcal{S}$ zaprta za seštevanje. Zaradi nekomutativnosti množenja matrik, $\mathcal{S}$ očitno ni zaprta za množenje. Velja namreč

$$(\,AB\,)^* = B^* A^* = BA\,.$$

Definirajmo na množici $\mathcal{S}$ množenje s predpisom

$$A \circ B = \tfrac{1}{2}\,(\,AB + BA\,)\,.$$

Ker velja

$$A \circ B = \tfrac{1}{2}\,(\,AB + BA\,) = \tfrac{1}{2}\,(\,BA + AB\,) = B \circ A\,,$$

je $\mathcal{S}$ zaprta za zgoraj definirano množenje. Preverimo še asociativnost množenja. Ker je

$$A \circ (\,B \circ C\,) = \tfrac{1}{4}\,(\,ABC + ACB + BCA + CAB\,)$$

in

$$(\,A \circ B\,) \circ C = \tfrac{1}{4}\,(\,ABC + BAC + CBA + CAB\,)$$

v splošnem velja

$$A \circ (B \circ C) \neq (A \circ B) \circ C\,.$$

Množica $\mathcal{S}$ torej za zgornji produkt, razen v primeru $n = 1$, ko množenje lahko interpretiramo kot običajno množenje števil, ni asociativna. Če pa v zgornjih izrazih nadomestimo C z izrazom $A \circ A = A^2$, dobimo

$$\begin{aligned}
A \circ (B \circ C) &= A \circ (B \circ (A \circ A)) = A \circ (B \circ A^2) = \\
&= \tfrac{1}{2}(A(B \circ A^2) + (B \circ A^2)A) = \\
&= \tfrac{1}{4}(A(BA^2 + A^2B) + (BA^2 + A^2B)A) = \\
&= \tfrac{1}{4}(ABA^2 + A^3B + BA^3 + A^2BA) = \\
&= \tfrac{1}{4}(ABA^2 + BA^3 + A^3B + A^2BA) = \\
&= \tfrac{1}{4}((AB + BA)A^2 + A^2(AB + BA)) = \\
&= \tfrac{1}{2}((A \circ B)A^2 + A^2(A \circ B)) = \\
&= (A \circ B) \circ A^2 = (A \circ B) \circ (A \circ A) = (A \circ B) \circ C\,,
\end{aligned}$$

oziroma

$$A \circ (B \circ A^2) = (A \circ B) \circ A^2\,.$$

Če dobljeni izraz zapišemo v obliki

$$A^2 \circ (A \circ B) = A \circ (A^2 \circ B)$$

je $\mathcal{S}$, opremljena z množenjem $\circ$, jordanska algebra.

Zgled 2. Naj bo $\mathcal{W}$ vektorski prostor nad obsegom $\mathbb{F}$ in $B : \mathcal{W} \times \mathcal{W} \longrightarrow \mathbb{F}$ simetrična bilinearna forma. Na vektorskem prostoru $\mathcal{V} = \mathbb{F} \times \mathcal{W}$ definirajmo produkt s predpisom

$$(\lambda, u) \circ (\mu, v) = (\lambda\mu + B(u, v), \lambda v + \mu u)\,.$$

Ker tako definiran produkt očitno izpolnjuje pogoja definicije, je prostor $\mathcal{V}$ jordanska algebra.

Zgled 3. Prostor $\mathcal{V}$, vseh antisimetričnih matrik dimenzije $2m \times 2m$, opremljen s produktom

$$x \circ y = \tfrac{1}{2}(xJy + yJx)\,,$$

kjer je

$$J = \begin{bmatrix} 0 & I_m \\ -I_m & 0 \end{bmatrix},\ \text{je jordanska algebra.}$$

Na jordanski algebri $\mathcal{J}$ definirajmo operator množenja

$$L(a) : \mathcal{J} \longrightarrow \mathcal{J}$$

s predpisom

$$L(a)\, b = a \circ b\,,$$

kjer sta $a, b \in \mathcal{J}$.

Če za poljubna operatorja množenja A in B jordanske algebre $\mathcal{J}$, uporabimo zapis

$$[\, A, B\,] = AB - BA\,,$$

lahko aksiom $(J2)$ nadomestimo z

$$[\, L(a), L(a^2)\,] = 0\,.$$

Velja namreč

$$[\, L(a), L(a^2)\,]\, b = L(a)L(a^2)\, b - L(a^2)L(a)\, b =$$

$$= L(a)(\, a^2 \circ b\,) - L(a^2)(\, a \circ b\,) = a \circ (\, a^2 \circ b\,) - a^2 \circ (\, a \circ b\,)\,.$$

Ob upoštevanju aksioma $(J1)$ od tod sledi

$$[\, L(a), L(a^2)\,] = 0\,.$$

Trditev 4.1. *Naj bo $\mathcal{J}$ jordanska algebra. Potem veljajo naslednje identitete:*

(i) $[\, L(a), L(b^2)\,] + 2\,[\, L(b), L(a \circ b)\,] = 0\,;$

(ii) $[\, L(a), L(b \circ c)\,] + [\, L(b), L(a \circ c)\,] + [\, L(c), L(a \circ b)\,] = 0\,;$

(iii) $L(a^2 \circ b) - L(a^2)L(b) = 2\,(\, L(a \circ b) - L(a)L(b)\,)\, L(a)\,.$

Dokaz:

(i) Poljubno identiteto, zapisano v operatorski obliki, uporabimo na enoti e jordanske algebre $\mathcal{J}$. Ker za poljuben $a \in \mathcal{J}$ velja $L(a)\, e = a \circ e = a$, je dobljeni izraz polinom oblike $p(a, b) = 0$. Definirajmo njegov odvod s predpisom

$$p'_b(a, b) = \frac{p(a + tb, b) - p(a, b)}{t}\, \Big|_{t=0}\,.$$

Če torej aksiom $(J2)$, zapisan v obliki $[L(a), L(a^2)] = 0$, uporabimo na enoti e, dobimo

$$p(a,b) = a \circ a^2 - a^2 \circ a = 0\,.$$

Izračunajmo njegov odvod.

$$\begin{aligned}
p'_b(a,b) &= \frac{1}{t}\,[\,(a+tb)\circ(a+tb)^2 - (a+tb)^2\circ(a+tb) \\
&\quad - a\circ a^2 + a^2\circ a\,]\Big|_{t=0} = \\
&= \frac{1}{t}\,[\,(a\circ tb)\circ(a^2 + tb\circ a + ta\circ b + t^2b^2) \\
&\quad - (a^2 + tb\circ a + ta\circ b + t^2b^2)\circ(a+tb) - a\circ a^2 + \\
&\quad + a^2\circ a\,]\Big|_{t=0} = \\
&= \frac{1}{t}\,[\,a\circ a^2 + ta\circ(b\circ a) + ta\circ(a\circ b) + t^2a\circ b^2 + \\
&\quad + tb\circ a^2 + t^2b\circ(b\circ a) + t^2b\circ(a\circ b) + t^3b\circ b^2 \\
&\quad - a^2\circ a - ta^2\circ b - t(b\circ a)\circ a - t^2(b\circ a)\circ b \\
&\quad - t(a\circ b)\circ a - t^2(a\circ b)\circ b - t^2b^2\circ a + \\
&\quad + t^3b^2\circ b - a\circ a^2 + a^2\circ a\,]\Big|_{t=0} = \\
&= b\circ a^2 - a^2\circ b + a\circ(b\circ a) - (b\circ a)\circ a + \\
&\quad + a\circ(a\circ b) - (a\circ b)\circ a = \\
&= b\circ a^2 - a^2\circ b + 2\,[\,a\circ(b\circ a) - (b\circ a)\circ a\,] = 0\,.
\end{aligned}$$

Če dobljeni izraz zapišemo v operatorski obliki, dobimo

$$[\,L(b), L(a^2)\,] + 2\,[\,L(a), L(b\circ a)\,] = 0\,,$$

od koder z zamenjavo spremenljivk a in b sledi

$$[\,L(a), L(b^2)\,] + 2\,[\,L(b), L(a\circ b)\,] = 0\,.$$

(ii) V dokazu prejšnje identitete smo pokazali, da operatorju

$$[\,L(a), L(b^2)\,] + 2\,[\,L(b), L(a\circ b)\,] = 0\,,$$

ustreza polinom

$$p(a,b) = a\circ b^2 - b^2\circ a + 2\,b\circ(b\circ a) - 2\,(b\circ a)\circ a = 0\,.$$

Izračunajmo njegov odvod, $p'_c(a,b)$. Po definiciji je

$$\begin{aligned} p'_c(a,b) = \frac{1}{t}\,[\,2\,(\,a+tc\,)\circ(\,b\circ(\,a+tc\,)\,) \\ -2\,(\,b\circ(\,a\circ tc\,)\,)\circ(\,a+tc\,)+ \\ +b\circ(\,a+tc\,)^2-(\,a+tc\,)^2\circ b-2\,a\circ(\,b\circ a\,)+ \\ +2\,(\,b\circ a\,)\circ a-b\circ a^2+a^2\circ b\,]\,\Big|_{t=0}\,. \end{aligned}$$

Od tod sledi

$$\begin{aligned} \frac{1}{t}[2\,(\,a+tc\,)\circ(\,b\circ a+tb\circ c\,) \\ -2\,(\,b\circ a+tb\circ c\,)\circ(a+tc\,)+ \\ +b\circ(\,a^2+ta\circ c+tc\circ a+t^2c^2\,) \\ -(\,a^2+ta\circ c+tc\circ a+t^2c^2\,)\circ b-\;2\,a\circ(\,b\circ a\,)+ \\ +2\,(\,b\circ a\,)\circ a-b\circ a^2+a^2\circ b\,]\,\Big|_{t=0}=0\,, \end{aligned}$$

oziroma

$$a\circ(\,b\circ c\,)-(\,b\circ c\,)\circ a+b\circ(\,a\circ c\,)-(\,a\circ c\,)\circ b+c\circ(\,b\circ a\,)-(\,b\circ a\,)\circ c=0\,.$$

Če dobljeno identiteto zapišemo v operatorski obliki, dobimo

$$[\,L(a),L(b\circ c)\,]+[\,L(b),L(a\circ c)\,]+[\,L(c),L(a\circ b)\,]=0\,.$$

(iii) Če uporabimo identiteto (i) na elementu c, dobimo

$$L(a)L(b^2)c-L(b^2)L(a)c+2L(b)L(a\circ b)c-2L(a\circ b)L(b)c=0\,,$$

oziroma

$$L(a)(b^2\circ c)-L(b^2)(a\circ c)+2L(b)((a\circ b)\circ c)-2L(a\circ b)(b\circ c)=0\,.$$

Od tod z uporabo enakosti $L(b^2)(a\circ c)=L(b^2\circ c)a$ in upoštevanjem komutativnosti, sledi

$$L(b^2\circ c)a-L(b^2)L(c)a+2L(b)L(c)L(b)a-2L(b\circ c)L(b)a=0\,,$$

in od tod

$$L(b^2\circ c)-L(b^2)L(c)+2L(b)L(c)L(b)-2L(b\circ c)L(b)=0\,.$$

Z zamenjavo b in a ter c in b, sledi

$$L(a^2 \circ b) - L(a^2)L(b) = 2L(a \circ b)L(a) - L(a)L(b)L(a)\,,$$

oziroma

$$L(a^2 \circ b) - L(a^2)L(b) = 2\,(\,L(a \circ b) - L(a)L(b)\,)\,L(a)\,.$$

$\square$

Trditev 4.2.

(i) *Naj bo $\mathcal{J}$ jordanska algebra. Potem za vsak $a \in \mathcal{J}$ in pozitivni števili p in q velja*

$$[\,L(a^p), L(a^q)\,] = 0\,.$$

(ii) *Jordanska algebra je potenčno asociativna.*

Dokaz:

(i) Najprej z indukcijo po p pokažimo, da je $a^p \circ a^2 = a^{p+2}$. Denimo, da je $a^{p+1} = a^2 \circ a^{p-1}$. Ker je

$$a^{p+2} = a \circ a^{p+1} = a \circ (\,a^2 \circ a^{p-1}\,)$$

z upoštevanjem $(J2)$ sledi

$$a^{p+2} = a^2 \circ (\,a \circ a^{p-1}\,) = a^2 \circ a^p = a^p \circ a^2\,.$$

V nadaljevanju pokažimo, da je $[\,L(a^p), L(a^q)\,] = 0$. Če v identiteti (iii) trditve 3.1 pišemo $b = a^{n-1}$ dobimo

$$L(a^{n+1}) = L(a^2)L(a^{n-1}) + 2L(a^n)L(a) - 2L(a)L(a^{n-1})L(a)\,.$$

Za vsako naravno število n je torej $L(a^n)$ element podalgebre endomorfizmov jordanske algebre $\mathcal{J}$, ki je po $(J2)$ komutativna in generirana z $L(a)$ in $L(a^2)$. Od tod torej sledi

$$[\,L(a^p), L(a^q)\,] = 0.$$

(ii) Pokažimo še potenčno asociativnost. Dokazati zadošča, da velja $a^p \circ a^q = a^{p+q}$. Enakost dokažimo z indukcijo po q. Denimo, da je $a^p \circ a^q = a^{p+q}$. Ker velja

$$a^{p+q+1} = a^{p+q} \circ a = (\,a^p \circ a^q\,) \circ a = a \circ (\,a^p \circ a^q\,) = L(a)L(a^p)a^q\,,$$

z upoštevanjem (i) sledi $a^{p+q+1} = L(a^p)L(a)a^q = a^p \circ a^{q+1}$. $\square$

Opomba: Potenčna asociativnost pomeni, da je podalgebra generirana z enim samim elementom a enaka

$$Gen(a) = \{\, p(a)\,;\, p \;-\; \text{polinom}\,\}$$

in je torej asociativna in komutativna.

5.2 Minimalni polinomi

Naj bo $\mathcal{V}$ končno dimenzionalna potenčno asociativna algebra nad obsegom $\mathbb{F}$ z enoto e. Z $\mathbb{F}[X]$ označimo algebro polinomov ene spremenljivke s koeficienti iz $\mathbb{F}$. Elementu $u \in \mathcal{V}$ priredimo množico $\mathbb{F}[x]$ s predpisom

$$\mathbb{F}[x] = \{\, p(x)\,;\, p \in \mathbb{F}[x]\,\}\,.$$

Množica $\mathbb{F}[x]$ je očitno podalgebra $\mathcal{V}$ in je generirana z elementoma x in e. ker je $\mathcal{V}$ algebra konňe dimenzije, elementi

$$x,\, x^2,\, x^3,\, \ldots, x^n, \ldots$$

podalgebre $\mathbb{F}[x]$ očitno ne morejo biti linearno neodvisni. Za nek $k \in \mathbb{N}$ torej velja

$$\alpha_k x^k + \alpha_{k-1}x^{k-1} + \ldots + \alpha_2 x^2 + \alpha_1 x = 0\,,$$

pri čemer je vsaj eden od α_i različen od nič. Zaradi potenčne asociativnosti algebre $\mathcal{V}$, za poljuben $x \in \mathcal{V}$ potem obstaja tak polinom $p \in \mathbb{F}[x]$, da velja $p(x) = 0$. Očitno je torej množica $\mathcal{J}(x)$, definirana s predpisom

$$\mathcal{J}(x) = \{\, p \in \mathbb{F}[X]\,;\, p(x) = 0\,\}\,,$$

neprazna znotraj $\mathbb{F}[X]$. ker je $\mathcal{J}(x)$ neprazna, v njej obstaja polinom najmanjše stopnje. Označimo ga s p_0. Ker je za poljuben polinom $p \in \mathcal{J}(x), st(p_0) \leq st(p)$, po evklidovem algoritmu obstajata taka q in $r \in \mathbb{F}[X]$, da velja

$$p = qp_0 + r\,,$$

in je $st(r) < st(p_0)$. Ker je

$$p(x) = q(x)p_0(x) + r(x) = 0\,,$$

zaradi potenčne asociativnosti sledi, da je $r(x) = 0$ in od tod, zaradi minimalnosti p_0 tudi $r = 0$. Polinom p_0 določen do konstante natančno, torej deli vse polinome iz $\mathcal{J}(x)$. Če se dogovorimo, da bomo s p_0 označevali tistega, ki ima vodilni koeficient enak 1, dobimo enolično določen polinom. Imenujemo ga *minimalni polinom* elementa x. Stopnjo minimalnega polinoma p_0 elementa x označimo z $m(x)$. Očitno je stopnja $m(x)$ omejena z dimenzijo prostora $\mathcal{V}$. Definirajmo *rang* algebre $\mathcal{V}$ kot

$$r = \max\{\, m(x)\, ;\, x \in \mathcal{V}\}\,.$$

V nadaljevanju bomo element $x \in \mathcal{V}$ imenovali *regularen*, če bo veljalo

$$m(x) = r\,.$$

5.3 Evklidske algebre in projektorji

Naj bo $\mathcal{E}$ vektorski prostor y enoto e nad obsegom $\mathbb{R}$, opremljen z bilinearno operacijo

$$\circ \,:\, \mathcal{J} \times \mathcal{J} \longrightarrow \mathcal{J}\,,$$

in skalarnim produktom

$$\langle\, .,.\,\rangle \,:\, \mathcal{J} \times \mathcal{J} \longrightarrow \mathbb{R}\,.$$

Če za poljubne x, y in $z \in \mathcal{E}$ velja

(*E*1) $x \circ y = y \circ x\,,$
(*E*2) $x^2 \circ (\,x \circ y\,) = x \circ (\,x^2 \circ y\,)\,,$
(*E*3) $\langle\, x \circ y\,,\, z\,\rangle \;=\; \langle\, x, y \circ z\,\rangle\,,$

$\mathcal{E}$ imenujemo *evklidska jordanska algebra* ali krajše *evklidska algebra.*

Zgled 1. Naj bo $\mathcal{L}$ Lorentzov stožec. V drugem poglavju smo mu priredili evklidsko algebro na naslednji način. Naj bo $\mathcal{H}$ $n-1$ dimenzionalen Hilbertov prostor, katerega ortonormirano bazo tvorijo vektorji $x_1, x_2, \ldots, x_n$ in $\mathcal{E}$ algebrska struktura oblike $\mathcal{E} = \mathbb{R} \oplus \mathcal{H}$. Elemente $\mathcal{E}$ torej pišemo v obliki $\alpha + x$. Če v $\mathcal{E}$ definiramo skalarni produkt s predpisom

$$\langle\, \alpha + x, \beta + y\,\rangle \;= \alpha\beta + \langle\, x, y\,\rangle\,,$$

kjer je skalarni produkt na desni originalni skalarni produkt prostora $\mathcal{H}$, in množenje s predpisom

$$(\alpha + x, \beta + y) = \alpha\beta + \langle x, y \rangle + \alpha y + \beta x\,,$$

je $\mathcal{E}$ evklidska algebra. Imenovali smo jo Lorentzova algebra dimenzije n in jo označili s simbolom $\mathcal{L}or(n)$.

Zgled 2. Naj bo $\mathcal{P}$ stožec pozitivnih matrik na realnem, kompleksnem ali kvaternionskem prostoru $\mathcal{H}$ dimenzije n. Naj bo $\mathcal{E}$ podana s predpisom $\mathcal{E} = \{ A : \mathcal{H} \longrightarrow \mathcal{H}\,;\, A^* = A \}$. Če na $\mathcal{E}$ definiramo skalarni produkt s predpisom

$$\langle A, B \rangle = ReSl\,(AB)\,,$$

ter algebraični produkt s predpisom

$$A \circ B = \tfrac{1}{2}\,(AB + BA)\,,$$

kjer je AB običajni produkt matrik, je $\mathcal{E}$ evklidska algebra. Imenujemo jo algebra simetričnih matrik dimenzije $n \times n$ in označimo z $Sim(n, \mathbb{R})$, oziroma $\mathcal{H}er(n, \mathbb{F})$, kjer je $\mathbb{F} = \{ \mathbb{C}, \mathbb{H} \}$.

Element $p \neq 0$ evklidkse algebre $\mathcal{E}$ z lastnostjo

$$p^2 = p\,,$$

imenujemo projektor algebre $\mathcal{E}$. Če za neka projektorja p in q algebre $\mathcal{E}$ velja

$$p \circ q = 0\,,$$

pravimo, da sta p in q *algebraično pravokotna* projektorja. Naj bosta p in q algebraično pravokotna projektorja algebre $\mathcal{E}$. Ker velja $p \circ q = 0$, sledi

$$\langle p, q \rangle = \langle p \circ p, q \rangle = \langle p, p \circ q \rangle = 0\,,$$

oziroma, p in q sta tudi evklidsko pravokotna glede na inducirani skalarni produkt.

Če za projektorje $p_1, p_2, \ldots, p_k$ algebre $\mathcal{E}$ velja

$$p_i^2 = p_i\,,$$

$$p_i \circ p_j = 0\,,\ \text{če} i \neq j\,,$$

$$p_1 + p_2 + \ldots + p_k = e\,,$$

kjer je e enota v $\mathcal{E}$, pravimo, da $p_1, p_2, \ldots, p_k$ tvorijo *kompleten sistem* pravokotnih projektorjev.

Zgled 3. V Lorentzovi algebri $\mathcal{L}or(n)$, kjer je množenje podano s predpisom $(\,\alpha + x, \beta + y\,) = \alpha\beta + \langle\, x, y\,\rangle + \alpha y + \beta x$, so projektorji elementi $1 + 0$ in $\frac{1}{2} + \frac{1}{2}\frac{x}{||x||}$. Če je namreč $p = \alpha + x$ neničelen projektor, zaradi $p^2 = (\,\alpha + x\,)^2 = \alpha^2 + ||x||^2 + 2\alpha x$, velja $\alpha^2 + ||x||^2 = \alpha$ in $2\alpha x = x$. Rešitev dobljenega sistema so projektorji oblike $x = 0$ in $\alpha = 1$, ter $\alpha = \frac{1}{2}$ in $||x||^2 = \frac{1}{4}$, oziroma $||x|| = \frac{1}{2}$.

Zgled 4. Znotraj algebre simetričnih matrik $\mathcal{H}er(n, \mathbb{F})$, so projektorji matrike, ki zadoščajo identiteti $A^2 = A$. Ker je kvadriranje znotraj algebre $\mathcal{H}er(n, \mathbb{F})$ po definiciji ekvivalentno običajnemu kvadriranju matrik, so projektorji v $\mathcal{H}er(n, \mathbb{F})$ kar običajni matrični projektorji.

Izrek 3.1. *(Prvi spektralni izrek) Vsak neničelen element x evklidske algebre $\mathcal{E}$ lahko enolično zapišemo kot končno vsoto,*

$$x = \lambda_1 p_1 + \lambda_2 p_2 + \ldots + \lambda_k p_k\,,$$

kjer so λ_i različna realna števila in $p_1, p_2, \ldots, p_k$ kompleten sistem pravokotnih projektorjev. Za vsak $j = 1, \ldots, k$, je $p_j \in \mathbb{R}[x]$.

Opomba: *Koeficiente λ_j imenujemo lastne vrednosti, vsoto $\lambda_1 p_1 + \lambda_2 p_2 + \ldots + \lambda_k p_k$ pa spektralna dekompozicija elementa x.*

Dokaz: Naj bo $y \in \mathbb{R}[x]$. Z $L_0(y)$ označimo zožitev $L(y)$ na $\mathbb{R}[x]$. Ker je $\mathbb{R}[x]$ podalgebra $\mathcal{E}$, v kateri velja

$$\langle\, L(y)x, z\,\rangle = \langle\, y \circ x, z\,\rangle = \langle\, x, y \circ z\,\rangle = \langle\, x, L(y)z\,\rangle\,,$$

je $L_0(y)$ simetričen endomorfizem evklidskega prostora $\mathbb{R}[x]$. To pomeni, da obstajajo take projekcije $P_1, P_2, \ldots, P_k$ prostora $\mathbb{R}[x]$, da velja $P_1 + P_2 + \ldots + P_n = I$, in taka realna števila $\lambda_1, \lambda_2, \ldots, \lambda_k$, da je $L_0(x) = \lambda_1 P_1 + \lambda_2 P_2 + \ldots + \lambda_k P_k$. Od tod sledi, da obstajajo polinomi q_j, za katere velja $P_j = q_j(L_0(x))$. Če definiramo $p_j = q_j(x)$ in upoštevamo asociativnost algebre $\mathbb{R}[x]$, dobimo

$$L_0(p_j) = L_0(q_j(x)) = q(L_0(x)) = P_j\,.$$

Podobno sledi

$$\begin{aligned}
L_0(p_i \circ p_j) &= L_0(q_i(x) \circ q_j(x)) = L_0(q_i(x))L_0(q_j(x)) = P_i P_j\,,\\
L_0(\sum p_j) &= L_0(\sum q_j(x)) = \sum L_0(q_j(x)) =\\
&= \sum q_j(L_0(x)) = \sum P_j = I\,,\\
L_0(\sum \lambda_j p_j) &= L_0(\sum \lambda_j q_j(x)) = \sum L_0(\lambda_j q_j(x))\\
&= \sum \lambda_j L_0(q_j(x)) = \sum \lambda_j q_j(L_0(x))\\
&= \sum \lambda_j P_j = L_0(x)\,.
\end{aligned}$$

Zaradi bijektivnosti L, sledi injektivnost L_0 in od tod

$$p_i^2 = p_i\,,\; p_i \circ p_j = 0\,,\; \text{če } i \neq j\,,$$

$$\sum p_j = e\,,\; \sum \lambda_j p_j = x\,.$$

Dokažimo še enoličnost. Denimo, da je $x = \sum \lambda_j p_j$. Potem je $x^n = \sum \lambda_j^n p_j$. Naj bo q poljuben polinom $\mathbb{R}[x]$. Če zapišemo $q(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$, sledi

$$\begin{aligned}
q(x) &= a_n(\sum \lambda_j^n p_j) + a_{n-1}(\sum \lambda_j^{n-1} p_j) +\\
&\quad \ldots + a_1(\sum \lambda_j p_j) + a_0 e0\\
&= a_n(\sum \lambda_j^n p_j) + a_{n-1}(\sum \lambda_j^{n-1} p_j) +\\
&\quad \ldots + a_1(\sum \lambda_j p_j) + a_0(\sum p_j) =\\
&= (\sum a_n\lambda_j^n + a_{n-1}\lambda_j^{n-1} + \ldots + a_1\lambda_j + a_0)p_j =\\
&= \sum q(\lambda_j)p_j\,.
\end{aligned}$$

Če za fiksen j definiramo

$$q^{(j)}(X) = \prod_{i\neq j}(\, X - \lambda_i\,)\,,$$

dobimo

$$q^{(j)}(x) = \prod_{i\neq j}(\, \lambda_1 p_1 + \lambda_2 p_2 + \ldots + \lambda_k p_k - \lambda_i e\,)$$

$$= \prod_{i\neq j}(\,\lambda_1 p_1 + \lambda_2 p_2 + \ldots + \lambda_k p_k - \lambda_i(\,p_1 + p_2 + \ldots + p_k)\,)$$
$$= \prod_{i\neq j}(\,(\lambda_1 - \lambda_i)p_1 + (\lambda_2 - \lambda_i)p_2 + \ldots + (\lambda_j - \lambda_i)p_j$$
$$+ \ldots + (\lambda_k - \lambda_i)p_k)\,)\,.$$

Ker v vsakem členu produkta nastopa le $(\lambda_j - \lambda_i)p_j$, dobimo

$$q^{(j)}(x) = \prod_{i\neq j}(\,(\lambda_j - \lambda_i)p_j\,,$$

od koder zaradi različnosti λ_j sledi, da je $p_j \in \mathbb{R}[x]$. To pomeni, da so $L_0(p_j)$ paroma pravokotne projekcije in λ_j lastne vrednosti operatorja $L_0(x)$. Vsak p_j je torej pravokotna projekcija enote e na tisti lastni podprostor prostora $L_0(x)$, ki pripada lastni vrednosti λ_j. To pa pomeni natanko enoličnost zapisa $x = \sum \lambda_j p_j$. $\square$

Po prejšnjem izreku lahko vsak element evklidske algebre $\mathcal{E}$ enolično zapišemo kot linearno kombinacijo pravokotnih projektorjev. Podoben sklep velja tudi za poljuben projektor algebre $\mathcal{E}$. Če pa projektor $p \in \mathcal{E}$ ni ničelen in ga ni mogoče zapisati kot linearno kombinacijo dveh neničelnih pravokotnih projektorjev, p imenujemo *primitivni projektor*. Kompleten sistem pravokotnih projektorjev $p_1, p_2, \ldots, p_m$, imenujemo *jordanski sistem*, če je poljuben projektor p_j primitiven in velja

$$p_j \circ p_k = 0\,, \text{ če } j \neq k$$

ter

$$p_1 + p_2 + \ldots + p_m = e\,.$$

Izrek 3.2. *(Drugi spektralni izrek) Naj ima evklidska algebra $\mathcal{E}$ rang r. Potem lahko vsak neničelen element x evklidkse algebre $\mathcal{E}$ zapišemo kot končno vsoto,*

$$x = \lambda_1 p_1 + \lambda_2 p_2 + \ldots + \lambda_r p_r\,,$$

kjer so λ_i realna števila in $p_1, p_2, \ldots, p_r$ jordanski sistem pravokotnih projektorjev. Množica spektralnih vrednosti $\{\,\lambda_1, \lambda_2, \ldots, \lambda_r\,\} = \sigma(x)$ je enolično določena.

Dokaz: Če je $x = \lambda_1 p_1 + \lambda_2 p_2 + \ldots + \lambda_r p_r$ spektralna dekompozicija elementa $x \in \mathcal{E}$, je očitno $q(x) = \sum q(\lambda_i) p_i$, za poljuben polinom $q \in \mathbb{R}[x]$. Od tod sledi, da je minimalni polinom elementa x oblike

$$f(X, x) = \prod_{i=1}^{k} (\, X - \lambda_i \,) \,.$$

Od tod sledi, da je $k \leq r$, oziroma $k = r$ natanko tedaj, ko je x regularen element. V tem primeru je vsak p_j primitiven, saj bi sicer obstajal jordanski sistem z več kot r elementi. To pomeni, da bi obstajali elementi algebre $\mathcal{E}$, katerih minimalni polinomi bi imeli stopnjo večjo od r, kar je v protislovju z definicijo ranga. Enoličnost zapisa je direktna posledica prvega spektralnega izreka. □

Zgled 5. Naj bo $\mathcal{E}$ algebra realnih simetričnih matrik dimenzije 2×2. V tem primeru se lastne vrednosti λ_i spektralne dekompozicije poljubnega elementa algebre $\mathcal{E}$, ujemajo z običajnimi matričnimi lastnimi vrednostmi. Spektralna dekompozicija poljubnega elementa algebre $\mathcal{E}$ je potem oblike

$$\begin{aligned} \begin{bmatrix} a & b \\ b & c \end{bmatrix} = \lambda_1 & \begin{bmatrix} u & -\sqrt{u-u^2} \\ -\sqrt{u-u^2} & 1-u \end{bmatrix} \\ & + \lambda_2 \begin{bmatrix} 1-u & \sqrt{u-u^2} \\ \sqrt{u-u^2} & u \end{bmatrix}, \end{aligned}$$

kjer sta λ_1 in λ_2 običajni matrični lastni vrednosti, u pa ustrezno realno število. V primeru, da sta elementa algebre $\mathcal{E}$ oblike

$$\begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix} \quad \text{in} \quad \begin{bmatrix} a & b \\ b & a \end{bmatrix},$$

sta njuni spektralni dekompoziciji

$$\begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix} = a \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

$$\begin{bmatrix} a & b \\ b & a \end{bmatrix} = (a+b) \begin{bmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{bmatrix} + (a-b) \begin{bmatrix} \frac{1}{2} & -\frac{1}{2} \\ -\frac{1}{2} & \frac{1}{2} \end{bmatrix}.$$

V asociativnih algebrah velja

$$L(p)L(p)x = p \circ (p \circ x) = (p \circ p) \circ x = p^2 \circ x = L(p)x \,,$$

za vsak projektor p. To pa pomeni, da ima lahko operator $L(p)$ lastni vrednosti le 0 in 1. Pri jordanskih algebrah je situacija nekoliko bolj zapletena. Velja namreč

Trditev 3.3. *Naj bo p projektor Jordanske algebre $\mathcal{J}$. Edine možne lastne vrednosti operatorja $L(p)$ so 0, $\frac{1}{2}$ in 1.*

Dokaz: Če na identiteti (iii), trditve 1.1 uporabimo $a = b = p$, dobimo

$$\begin{aligned} L(p^3) - L(p^2)L(p) &= 2(\,L(p^2) - L(p)L(p)\,)L(p) \\ &= 2L(p^2)L(p) - 2L(p)^3\,, \end{aligned}$$

oziroma

$$L(p^3) = 3L(p^2)L(p) - 2L(p)^3\,.$$

Ker je $p^3 = p^2 \circ p = p \circ p = p$, od tod sledi

$$L(p) = 3L(p)L(p) - 2L(p)^3\,,$$

oziroma

$$2L(p)^3 - 3L(p)^2 + L(p) = 0\,.$$

Lastne vrednosti operatorja $L(p)$ so torej ničle karakterističnega polinoma

$$2\lambda^3 - 3\lambda^2 + \lambda = 0\,.$$

Pripadajoče ničle so $\lambda_1 = 0$, $\lambda_2 = \frac{1}{2}$ in $\lambda_3 = 1$. $\square$

Trditev 3.4. *Če sta p in q pravokotna projektorja jordanske algebre $\mathcal{J}$, potem $L(p)$ in $L(q)$ komutirata.*

Dokaz: Trditev je neposredna posledica identitete (ii) trditve 1.1. Če namreč v omenjeni identiteti pišemo $a = p$ in $b = c = q$, dobimo

$$[\,L(p), L(q \circ q)\,] + [\,L(q), L(p \circ q)\,] + [\,L(q), L(p \circ q)\,] = 0\,.$$

Od tod, z upoštevanjem $p \circ q = 0$, sledi

$$[\,L(p), L(q)\,] = 0\,.$$

5.4 Mc Crimmonov operator in obrnljivost

Naj bo $\mathcal{J}$ jordanska algebra nad obsegom $\mathbb{F}$ z enoto e. Definirajmo preslikavo

$$P : \mathcal{J} \longrightarrow End(\mathcal{J}),$$

s predpisom

$$P(a) = 2L(a)^2 - L(a^2).$$

Tako definirano preslikavo P imenujemo *Mc Crimmonov operator.*

Ker nas v tem delu zanima zgolj uporaba realnih algeber, se bomo v nadaljevanju razdelka omejili zgolj na primer $\mathbb{F} = \mathbb{R}$. ta omejitev nam bo omogočila precejšnjo poenostavitev nekaterih dokazov. Preden začnemo s proučevanjem lastnosti Mc Crimmonovega operatorja P, dokažimo naslednjo

Lema 4.1. *Če je p neničelni realni polinom n spremenljivk, je množica $\mathcal{M} = \{ x \in \mathbb{R}^n ; p(x) \neq 0 \}$ gosta v običajni topologiji $\mathbb{R}^n$.*

Dokaz: Naj bo $p(a) = 0$ za nek $a \in \mathbb{R}^n$. Če a ni v zaprtju množice $\mathcal{M}$, potem obstaja taka $\epsilon-$ okolica točke a, da so vse njene točke ničle polinoma p. Brez škode za splošnost lahko predpostavimo, da je $a = 0$. Polinom p torej lahko zapišemo kot

$$p(x_1, \ldots, x_n) = q_0(x_1, \ldots, x_n) + q_1(x_1, \ldots, x_n)x_n +$$
$$+ q_2(x_1, \ldots, x_n)x_n^2 + \ldots + q_k(x_1, \ldots, x_n)x_n^k.$$

Fiksirajmo neko točko $b \in \mathbb{R}^{n-1}$ znotraj krogle s polmerom ϵ. V tem primeru dobimo polinom ene spremenljivke

$$p(b, x_n) = q(x_n),$$

ki ima po zgornji predpostavki neskončno ničel, saj mednje sodi cel interval $(-\epsilon, \epsilon)$. To pa pomeni, da je q ničelen polinom, oziroma $p(b, x_n) = 0$, za vsak $x_n \in \mathbb{R}$. Če bi fiksirali x_n, bi dobili polinom $n - 1$ spremenljivk

$$p(x_1, \ldots, x_n) = r(x_1, \ldots, x_{n-1}),$$

ki bi imel ničle vse $(n-1)-$ terice z lastnostjo $|\, x_i \,| < \epsilon$. Ker je le teh neskončno sledi, da je r ničelen polinom, oziroma $p(x_1, \ldots, x_n) = 0$, za fiksen $x_n \in \mathbb{R}$. Ker trditev leme očitno velja za $n = 1$, lahko z manjšanjem dimenzije in indukcijo zaključimo dokaz. $\square$

Če je na algebri $\mathcal{J}$ definiran produkt s predpisom

$$a \circ b = \tfrac{1}{2}(\, ab + ba\,)\,,$$

velja

$$\begin{aligned} P(a)b &= (2L(a)^2(a^2))b = 2L(a)^2b - L(a^2)b = \\ &= 2L(a)L(a)b - L(a^2)b = \\ &= a \circ (a \circ b) - a^2 \circ b = \\ &= a \circ (ab + ba) - a^2 \circ b = \\ &= \tfrac{1}{2}(a^2b + aba + aba + ba^2) - \tfrac{1}{2}(a^2b + ba^2)\,, \end{aligned}$$

oziroma

$$P(a)b = aba\,.$$

Če, podobno kot v dokazu trditve 1.1, definiramo odvod preslikave P s predpisom

$$P'_b(a) = \frac{P(a+tb) - P(a)}{t}\Big|_{t=0}\,,$$

sledi

$$\begin{aligned} P'_b(a) &= \tfrac{1}{t}[\,2L(a+tb)^2 - L((a+tb)^2) - 2L(a)^2 + L(a)^2]\Big|_{t=0} = \\ &= \tfrac{1}{t}[\,2L(a+tb)L(a+tb) - L(a^2 + a \circ tb + tb \circ a + t^2b^2) \\ &\quad - 2L(a)^2 + L(a)^2]\Big|_{t=0}\,. \end{aligned}$$

Od tod, z upoštevanjem linearnosti preslikave L, sledi

$$\begin{aligned} P'_b(a) &= \tfrac{1}{t}[\,2[L(a) + tL(b)][L(a) + tL(b)] - L(a^2) + tL(a \circ b) + \\ &\quad +\; tL(b \circ a) + t^2L(b^2) - 2L(a)^2 + L(a)^2]\Big|_{t=0} = \\ &= \tfrac{1}{t}[\,2L(a)^2 + 2tL(a)L(b) + 2tL(b)L(a) + 2t^2L(b)^2 \\ &\quad -\; L(a^2) - tL(a \circ b) - tL(b \circ a) - t^2L(b^2) \\ &\quad - 2L(a)^2 + L(a^2)]\Big|_{t=0} = \\ &= 2L(a)L(b) + 2L(b)L(a) - L(a \circ b) - L(b \circ a)\,. \end{aligned}$$

Ker je $a \circ b = b \circ a$, sledi

$$P'_b(a) = 2L(a)L(b) + 2L(b)L(a) - 2L(a \circ b)\,.$$

Če definiramo

$$P(a,b) = \tfrac{1}{2}P_b'(a)\,,$$

sledi identiteta

$$P(a,b) = L(a)L(b) + L(b)L(a) - L(a \circ b)\,.$$

Zapišimo $P(a,b)$ v obliki

$$\begin{aligned} P(a,b) = {} & L(a)L(b) + L(b)L(a) - L(a \circ b) + L(a)^2 \\ & - L(a)^2 + L(b)^2 - L(b)^2 \\ & + \tfrac{1}{2}L(a^2) - \tfrac{1}{2}L(a^2) + \tfrac{1}{2}L(b^2) - \tfrac{1}{2}L(b^2)\,. \end{aligned}$$

Z upoštevanjem linearnosti preslikave L sledi

$$\begin{aligned} P(a,b) &= (L(a) + L(b))(L(a) + L(b)) - \tfrac{1}{2}L(a^2) - \tfrac{1}{2}L(a \circ b) \\ &\quad - \tfrac{1}{2}L(b \circ a) + \tfrac{1}{2}L(b^2) - L(a)^2 + \tfrac{1}{2}L(a^2) - L(b^2) - \tfrac{1}{2}L(b^2) \\ &= (L(a) + L(b))(L(a) + L(b)) - \tfrac{1}{2}L(a^2 + a \circ b + b \circ a + b^2) \\ &\quad - L(a)^2 + \tfrac{1}{2}L(a^2) - L(b)^2 + \tfrac{1}{2}L(b)^2 \\ &= L(a+b)^2 - \tfrac{1}{2}L((a+b)^2) - L(a)^2 \\ &\quad + \tfrac{1}{2}L(a^2) - L(b)^2 + \tfrac{1}{2}L(b^2) \\ &= \tfrac{1}{2}[(2L(a+b)^2 - L((a+b)^2)) - (2L(a)^2 - L(a^2)) \\ &\quad - (2L(b)^2 - L(b^2))]\,, \end{aligned}$$

oziroma

$$P(a,b) = \tfrac{1}{2}(P(a+b) - P(a) - P(b))\,.$$

Če uporabimo $P(a,b)$ na elementu c, dobimo

$$P(a,b)c = L(a)L(b)c + L(b)L(a)c - L(a \circ b)c \ =$$

$$= \ a \circ (b \circ c) + b \circ (a \circ c) - (a \circ b) \circ c \ =$$

$$= \tfrac{1}{2}(a \circ (bc \circ cb) + b \circ (ac + ca) - (ab + ba) \circ c) \ =$$

$$= \tfrac{1}{2}(abc + bca + acb + cba + bac + acb$$

$$+bca + cab - abc - cab - bac - cba)\,.$$

Od tod sledi, da v asociativni algebri velja

$$P(a,b)c = \tfrac{1}{2}(acb + bca)\,.$$

Naj bo a element jordanske algebre $\mathcal{J}$ z enoto e in $\mathbb{F}[a]$ njena podalgebra, generirana z elemntoma e in a. Če v $\mathbb{F}[a]$ obstaja enolično določen element b, za katerega velja

$$a \circ b = b \circ a = e\,,$$

pravimo, da je element a *obrnljiv*. Element b označujemo z običajnim simbolom a^{-1} in imenujemo *inverz* elementa a.

Opomba: Enakost $a \circ b = b \circ a = e$ sama po sebi ne pomeni, da je b inverz elementa a. če je namreč $\mathcal{J} = Sim(2, \mathbb{R})$ in

$$a = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}\,, \quad b = \begin{bmatrix} 1 & x \\ x & -1 \end{bmatrix}\,,\ x \in \mathbb{R}\,,$$

je a obrnljiv in velja $a^{-1} = a$. Očitno je $a \circ b = b \circ a = e$, toda $b \notin \mathbb{R}[a]$, za $x \neq 0$.

Trditev 4.2. *Če je $L(a)$ obrnljiv operator in velja $a \circ b = e$, je b inverz elementa a.*

Dokaz: ker je $\mathbb{F}[a]$ generirana z e in a, in je $L(a)$ bijekcija, je njena skrčitev na $\mathbb{F}[a]$ injektivna. Zaradi končne dimenzije je ta skrčitev tudi bijektivna. Obstaja torej tak $c \in \mathbb{F}[a]$, da je $L(a)c = a \circ c = e$. Ker je $L(a)$ bijekcija na vsej jordanski algebri $\mathcal{J}$, je $c = b$ in b je inverz elemnta a. □

Izrek 4.3. *Element a je obrnljiv natanko tedaj, ko je obrnljiv $P(a)$. Potem velja*

$$P(a)a^{-1} = a\,,$$
$$P(a)^{-1} = P(a^{-1})\,.$$

Dokaz: Naj bo $P(a)$ obrnljiv. Potem je skrčitev $P(a)$ na $\mathbb{F}[a]$ bijekcija za katero velja $b = P(a)^{-1}a \in \mathbb{F}[a]$. Ker velja

$$P(a)e = 2L(a)^2 e - L(a^2)e = 2a \circ (a \circ e) - a^2 \circ e = a^2\,,$$

in po trditvi 1.2

$$P(a)L(a) = 2L(a)^2 L(a) - L(a^2)L(a) = 2L(a)L(a^2) - L(a)L(a^2) =$$
$$= L(a)(2L(a)^2 - L(a^2)) = L(a)P(a)$$

sledi

$$b \circ a = (P(a)^{-1}a)a = L(a)P(a)^{-1}a =$$

$$= \ P(a)^{-1}L(a)a = P(a)^{-1}a^2 = e\,,$$

od koder je po zgornji definiciji $b = a^{-1}$ inverz elementa a. Poleg tega sledi

$$P(a)a^{-1} = P(a)b = P(a)P(a)^{-1}a = a\,.$$

Dokažimo še obratno implikacijo. Naj bo a obrnljiv. Če v identiteti (iii) trditve 1.2 nadomestimo b z a^{-1}, dobimo

$$L(a^2 \circ a^{-1}) - L(a^2)L(a^{-1}) = 2(L(a \circ a^{-1}) - L(a)L(a^{-1}))L(a)\,,$$

$$L(a) - L(a^2)L(a^{-1}) = 2(L(a \circ a^{-1}))L(a) - L(a)L(a^{-1})L(a))\,.$$

Z upoštevanjem komutativnosti $L(a)$ in $L(a^{-1})$, od tod sledi

$$L(a) - L(a^2)L(a^{-1}) = 2L(a) - 2L(a)^2L(a^{-1})\,,$$

$$L(a)^2L(a^{-1})L(a^2)L(a^{-1}) = L(A0\,,$$

oziroma

$$P(a)L(a^{-1}) = L(a)\,.$$

Z zamenjavo a in a^{-1}, dobimo

$$P(a^{-1})L(a) = L(a^{-1})$$

in od tod

$$P(a)P(a^{-1})L(a) = P(a)L(a^{-1}) = L(a)\,.$$

Če je $det\,L(a) \neq 0$ sledi, da je $P(a)P(a^{-1}) = I/$ Če si izberemo v $\mathcal{J}$ neko bazo, je preslikava $a \longmapsto det\,L(a)$ polinom. Ker je $det\,L(e) = detI = 1$, je ta polinom neničelen. Po lemi 4.1 je množica $\{\, a\,;\, det\,L(a) \neq 0 \,\}$ gosta v $\mathcal{J}$. Seveda je ta množica gosta tudi v manjši množici vseh obrnljivih elementov. Ker je tudi preslikava $a \longmapsto P(a)P(a^{-1}) - I$ polinomska in zvezna, sledi identiteta

$$P(a)^{-1} = P(a^{-1})\,.$$

Posledica 4.4. Množica obrnljivih elementov $\mathcal{I}$ je podana z

$$\mathcal{I} = \{\, a\,;\, det\,P(a) \neq 0 \,\}$$

in je gosta v algebri $\mathcal{J}$.

Izrek 4.5. *Odvod preslikave $a \longmapsto a^{-1}$ je $-P(a)^{-1}$, oziroma*

$$(a^{-1})'_b = -P(a)^{-1}b\,.$$

Če sta a in b obrnljiva, je obrnljiv tudi $P(a)b$ in velja

$$(P(a)b)^{-1} = P(a^{-1})b^{-1}\,.$$

Za poljubna elementa a in b velja

$$P(P(a)b) = P(a)P(b)P(a)$$

oziroma

$$P(aba) = P(a)P(b)P(a)\,.$$

Opomba: *Omenjeno lastnost Mc Crimmonovega operatorja imenujemo kvadratna reprezentacija.*

Dokaz: (i) Če uporabimo Mc Crimmonov operator na elementu a^{-1}, dobimo

$$P(a)a^{-1} = 2L(a)^2a^{-1} - L(a^2)a^{-1} = 2 \circ (a \circ a^{-1}) - a^2 \circ a^{-1} = a\,,$$

oziroma

$$P(a)a^{-1} = a\,.$$

Odvajajmo dobljeno identiteto. Po definiciji odvoda velja

$$(P(a)a^{-1})'_b = \tfrac{1}{t}[\,P(a+tb)(a+tb)^{-1} - P(a)a^{-1}\,]\Big|_{t=0}$$

in

$$(a)'_b = \tfrac{1}{t}[\,(a+tb) - a\,]\Big|_{t=0} = \tfrac{1}{t}tb\Big|_{t=0} = b\,.$$

Ker velja

$$\begin{aligned}
P(a+tb) &= 2L(a+tb)^2 - L((a+tb)^2) = \\
&= 2L(a+tb)L(a+tb) - L(a^2 + a \circ tb + tb \circ a + t^2b^2) = \\
&= \ 2[\,L(a) + L(tb)\,][\,L(a) + L(tb)\,] - L(a^2) \\
&\quad + 2tL(a \circ b) + L(t^2b^2) = \\
&= \ 2L(a)^2 + 2L(a)L(tb) + 2L(tb)L(a) + 2L(tb)^2 \\
&\quad - L(a^2) + L(2t \circ b) + L(t^2b^2) = \\
&= P(a) + P(tb) + 2P(a,tb)
\end{aligned}$$

in

$$\begin{aligned} P(tb) &= 2L(tb)^2 - L((tb)^2) = 2L(tb)L(tb) - L(t^2b^2) \ = \\ &= \ 2t^2L(b)L(b) - t^2L(b^2) = t^2[\,2L(b)L(b) - L(b^2)\,] = t^2P(b)\,, \end{aligned}$$

sledi

$$\begin{aligned} (P(a)a^{-1})'_b &= \tfrac{1}{t}[\,(2P(a,tb) + P(a) + P(tb))(a+tb)^{-1} - P(a)a^{-1}]\Big|_{t=0} = \\ &= \ \tfrac{1}{t}[\,(2P(a,tb)(a+tb)^{-1} + P(tb)(a+tb)^{-1}]\Big|_{t=0} + \\ &\quad + \tfrac{1}{t}[\,(P(a)(a+tb)^{-1} - P(a)a^{-1}]\Big|_{t=0} = \\ &= \tfrac{1}{t}[\,2tP(a,b)(a+tb)^{-1} + t^2P(b)(a+tb)^{-1}]\Big|_{t=0} + \\ &\quad + P(a)(a^{-1})'_b = \\ &= \ 2P(a,b)(a+tb)^{-1}\Big|_{t=0} + tP(b)(a+tb)^{-1}\Big|_{t=0} + \\ &\quad + P(a)(a^{-1})'_b\,, \end{aligned}$$

oziroma

$$(P(a)a^{-1})'_b = 2P(a,b)a^{-1} + P(a)(a^{-1})'_b\,.$$

Po odvajanju dobimo torej naslednjo identiteto

$$2P(a,b)a^{-1} + P(a)(a^{-1})'_b = b\,.$$

Če upoštevamo, da je

$$\begin{aligned} P(a,b)a^{-1} &= [\,L(a)L(b) + L(b)L(a) - L(a\circ b)\,]a^{-1} \\ &= L(a)L(b)a^{-1} + L(b)L(a)a^{-1} - L(a\circ b)a^{-1} \\ &= \ a\circ(b\circ a^{-1}) + b\circ(a\circ a^{-1}) - (a\circ b)\circ a^{-1} = b\,, \end{aligned}$$

sledi

$$P(a)(a^{-1})'_b = -b\,,$$

oziroma

$$(a^{-1})'_b = -P(a)^{-1}b\,.$$

(ii) Če uporabimo identiteto

$$P(a)L(a^{-1}) = L(a)$$

na elementu b in upoštevamo komutativnost operatorjev $P(a)$ in $L(a^{-1})$, dobimo

$$a^{-1}\circ P(a)b = a\circ b\,.$$

Odvajajmo dobljeno identiteto po c. Ker je

$$(a \circ P(a)b)'_c = \tfrac{1}{t}[\,(a+tc)^{-1} \circ P(a+tc)b - a^{-1} \circ P(a)b\,]\Big|_{t=0} =$$

$$= \tfrac{1}{t}[\,(a+tc)^{-1} \circ (P(a)b + t^2 P(c)b + 2P(a,tc)b) - a^{-1} \circ P(a)b\,]\Big|_{t=0} =$$

$$= \tfrac{1}{t}[\,(a+tc)^{-1} \circ P(a)b - a^{-1} \circ P(a)b\,]\Big|_{t=0} + t(a+tc)^{-1} \circ P(c)b\Big|_{t=0} +$$

$$+ (a+tc)^{-1} \circ 2P(a,c)b\Big|_{t=0} = (a)'_c \circ P(a)b + 2a^{-1} \circ P(a,c)b =$$

$$= -P(a^{-1})c \circ P(a)b + 2a^{-1} \circ P(a,c)b$$

in

$$(a \circ b)'_c = \tfrac{1}{t}[\,(a+tc) \circ b - a \circ b\,]\Big|_{t=0} = \tfrac{1}{t} tc \circ b\Big|_{t=0} = c \circ b\,,$$

sledi

$$-P(a^{-1}) \circ P(a)b + 2a^{-1} \circ P(a,c)b = c \circ b\,.$$

Če v dobljeni identiteti c zamenjamo z b^{-1}, dobimo

$$-P(a^{-1})b^{-1} \circ P(a)b + 2a^{-1} \circ P(a,b^{-1})b = b^{-1} \circ b\,.$$

Od tod, z upoštevanjem $P(a,b^{-1})b = a$, sledi

$$-P(a^{-1})b^{-1} \circ P(a)b + 2a^{-1} \circ a = e\,.$$

oziroma

$$P(a^{-1})b^{-1} \circ P(a)b = e\,.$$

če označimo $y = P(a^{-1})b^{-1}$ in $x = P(a)b$, dobljena enakost predstavlja izraz $x \circ y = e$, ki pa ne zadošča za zaključek, da je y inverz x. Dokazati je namrečše potrebno, da je $y \in \mathbb{F}[x]$. Za dokaz enakosti $(P(a)b)^{-1} = P(a^{-1})b^{-1}$, po trditvi 4.2 zadošča pokazati, da je $det\, L(P(a)b) \neq 0$. Izraz $det\, L(P(a)b)$ je polinom na prostoru $\mathcal{J} \times \mathcal{J}$. Ker je $det\, L(P(e)) = det\, I = 1$, je ta polinom neničelen. Ker po lemi 4.1 pogoj $det\, L(P(a)b) \neq 0$ predstavlja gosto množico, identiteta

$$(P(a)b)^{-1} = P(a^{-1})b^{-1}$$

velja za vse obrnljive a in $b \in \mathcal{J}$.

(*iii*) Identiteto
$$(P(b)a)^{-1} = P(b^{-1})a^{-1}\,,$$
odvajamo po c. Če izraz na levi odvajamo kot kompozitum, dobimo

$$\begin{aligned}
(\,(P(b)a)^{-1})'_c &= -P(P(b)a)^{-1}(P(b)a)'_c = \\
&= -P(P(b)a)^{-1}\tfrac{1}{t}\,[\,(P(b)(a+tc) - P(b)a\,]\,\Big|_{t=0} = \\
&= -P(P(b)a)^{-1}P(b)\tfrac{1}{t}[(a+tc) - a]\,\Big|_{t=0} = \\
&= -P(P(b)a)^{-1}P(b)c\,.
\end{aligned}$$

Ker je odvod izraza na desni

$$\begin{aligned}
(P(b^{-1})a^{-1})'_c &= \tfrac{1}{t}[(P(b^{-1})(a+tc)^{-1} - P(b^{-1})a^{-1}]\,\Big|_{t=0} = \\
&= -(P(b^{-1})\tfrac{1}{t}[(a+tc)^{-1} - a^{-1}]\,\Big|_{t=0} = \\
&= P(b^{-1})(a^{-1})'_c = \\
&= -P(b^{-1})P(a)^{-1}c\,,
\end{aligned}$$

sledi identiteta

$$-P(P(b)a)^{-1}P(b)c = -P(b^{-1})P(a)^{-1}c\,.$$

Če upoštevamo, da je $P(b^{-1}) = P(b)^{-1}$ in c nadomestimo s $P(b)$, dobimo

$$-P(P(b)a)^{-1}P(b)P(b) = -P(b)^{-1}P(a)^{-1}P(b)\,,$$

od koder sledi

$$P(P(b)a)^{-1} = P(b)^{-1}P(a)^{-1}P(b)^{-1}\,,$$

oziroma
$$P(P(b)a) = P(b)P(a)P(b)\,.$$
Po substituciji a z b in b z a sledi

$$P(P(a)b) = P(a)P(b)P(a)\,.$$

Omenjena identiteta velja le v primeru, ko sta a in b obrnljiva elementa. Ker so obrnljivi elementi gosti, ta identiteta velja tudi za poljubna elementa a in $b \in \mathcal{J}$. $\square$

5.5 Pierceova dekompozicija

V tem razdelku si bomo ogledali Pierceovo dekompocijo jordanske algebre $\mathcal{J}$, glede na projektor $p \in \mathcal{J}$. V razdelku o projektorjih smo dokazali, da so edine lastne vrednosti operatorja $L(p)$ števila 0, $\frac{1}{2}$ in 1. Jordansko algebro $\mathcal{J}$ torej lahko zapišemo kot direktno vsoto lastnih podprostorov

$$\mathcal{J} = \mathcal{J}_0 \oplus \mathcal{J}_{\frac{1}{2}} \oplus \mathcal{J}_1\,,$$

pri čemer je

$$\mathcal{J}_i = \{\, x \in \mathcal{J}\,;\, L(p)\,x = i \circ x\,\}\,.$$

Dekompozicijo jordanske algebre $\mathcal{J}$ na direktno vsoto lastnih podprostorov imenujemo *Pierceova dekompozicija*. Elementi podprostora $\mathcal{J}_i$ so lastni vektorji, ki pripadajo lastni vrednosti i. V zgornjem primeru jordanska algebra $\mathcal{J}$ razpade na direktno vsoto naslednjih lastnih podprostorov

$$\begin{aligned}
\mathcal{J}_0 &= \{\, x \in \mathcal{J}\,;\, L(p)\,x = 0\,\} = \{\, x \in \mathcal{J}\,;\, p \circ x = 0\,\}\,,\\
\mathcal{J}_{\frac{1}{2}} &= \{\, x \in \mathcal{J}\,;\, L(p)\,x = \tfrac{1}{2}\,x\,\} = \{\, x \in \mathcal{J}\,;\, p \circ x = \tfrac{1}{2}\,x\,\}\,,\\
\mathcal{J}_1 &= \{\, x \in \mathcal{J}\,;\, L(p)\,x = x\,\} = \{\, x \in \mathcal{J}\,;\, p \circ x = x\,\}\,.
\end{aligned}$$

V nadaljevanju razdelka bodo predmet obravnave predvsem multiplikativne lastnosti Pierceove dekompozije, ki nikakor niso očitne. V kasnejših razdelkih bomo namreč dekompozicijo, zaradi številnih uporabnih lastnosti uporabljali kot orodje pri dokazovanju nekaterih trditev.

Zgled 1. Naj bo $\mathcal{J}$ množica realnih simetričnih matrik dimenzije $m \times m$, opremljena z jordanskim produktom. V prvem razdelku tega poglavja smo dokazali, da je $\mathcal{J}$ jordanska algebra. Naj bo $m = r + q$. Pokažimo, da je matrika oblike

$$p = \begin{bmatrix} I_r & 0 \\ 0 & 0 \end{bmatrix},$$

projektor prostora $\mathcal{J}$. Ker je

$$p^2 = \begin{bmatrix} I_r & 0 \\ 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} I_r & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} I_r & 0 \\ 0 & 0 \end{bmatrix} = p\,,$$

očitno sledi, da je matrika p projektor prostora $\mathcal{J}$. V nadaljevanju izračunajmo Pierceovo dekompozicijo prostora $\mathcal{J}$ glede na projektor p zgornje oblike. Najprej si oglejmo dekompozicijo v primeru, ko je $m = 2$. Po definiciji lastnih podprostorov, je podprostor $\mathcal{J}_0$ določen s predpisom

$$\mathcal{J}_0 = \left\{ \begin{bmatrix} a & b \\ b & c \end{bmatrix} ; \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \circ \begin{bmatrix} a & b \\ b & c \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \right\}.$$

Ker za poljubna A in $B \in \mathcal{J}$ velja

$$\tfrac{1}{2} \, (AB + BA) = A \circ B \,,$$

sledi

$$\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} a & b \\ b & c \end{bmatrix} + \begin{bmatrix} a & b \\ b & c \end{bmatrix} \cdot \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} = 2 \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} ,$$

oziroma

$$\begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix} + \begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} .$$

Od tod dobimo sistem

$$\begin{bmatrix} 2a & b \\ b & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} ,$$

katerega rešitev je $a = b = 0$ in $c \in \mathbb{R}$. Dobimo torej

$$\mathcal{J}_0 = \left\{ \begin{bmatrix} 0 & 0 \\ 0 & c \end{bmatrix} ; c \in \mathbb{R} \right\}.$$

Za podprostor

$$\mathcal{J}_{\frac{1}{2}} = \left\{ \begin{bmatrix} a & b \\ b & c \end{bmatrix} ; \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \circ \begin{bmatrix} a & b \\ b & c \end{bmatrix} = \tfrac{1}{2} \begin{bmatrix} a & b \\ b & c \end{bmatrix} \right\},$$

dobimo sistem

$$\begin{bmatrix} 2a & b \\ b & 0 \end{bmatrix} = 2 \cdot \tfrac{1}{2} \begin{bmatrix} a & b \\ b & c \end{bmatrix} ,$$

katerega rešitev je $a = c = 0$ in $b \in \mathbb{R}$.

Sledi torej

$$\mathcal{J}_{\frac{1}{2}} = \left\{ \begin{bmatrix} 0 & b \\ b & 0 \end{bmatrix} ; b \in \mathbb{R} \right\}.$$

Podobno tudi za podprostor

$$\mathcal{J}_1 = \left\{ \begin{bmatrix} a & b \\ b & c \end{bmatrix} ; \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \circ \begin{bmatrix} a & b \\ b & c \end{bmatrix} = \begin{bmatrix} a & b \\ b & c \end{bmatrix} \right\},$$

dobimo sistem

$$\begin{bmatrix} 2a & b \\ b & 0 \end{bmatrix} = 2 \begin{bmatrix} a & b \\ b & c \end{bmatrix},$$

katerega rešitev je $b = c = 0$ in $a \in \mathbb{R}$. Od tod torej sledi

$$\mathcal{J}_1 = \left\{ \begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix} ; a \in \mathbb{R} \right\}.$$

S kratkim premislekom lahko dobljeni rezultat posplošimo tudi na jordansko matično algebro dimenzije $m \times m$. V tem primeru so projektorju p pripadajoči lastni podprostori oblike

$$\mathcal{J}_1 = \left\{ \begin{bmatrix} A & 0 \\ 0 & 0 \end{bmatrix} ; A \text{ je } r \times r \text{ simetrična matrika} \right\},$$

$$\mathcal{J}_0 = \left\{ \begin{bmatrix} 0 & 0 \\ 0 & B \end{bmatrix} ; B \text{ je } q \times q \text{ simetrična matrika} \right\},$$

$$\mathcal{J}_{\frac{1}{2}} = \left\{ \begin{bmatrix} 0 & C \\ C^T & 0 \end{bmatrix} ; C \text{ je } r \times q \text{ matrika} \right\}.$$

Zgled 2. Naj bo $\mathcal{W}$ vektorski prostor nad obsegom $\mathbb{F}$ in $B : \mathcal{W} \times \mathcal{W} \longrightarrow \mathbb{F}$ simetrična bilinearna forma. Vektorski prostor $\mathcal{V} = \mathbb{F} \times \mathcal{W}$, opremljen s produktom

$$(\lambda, u) \circ (\mu, v) = (\lambda\mu + B(u, v), \lambda v + \mu u),$$

je jordanska algebra. Poiščimo najprej njegove projektorje. Ker je

$$\begin{aligned} (\lambda, u)^2 &= (\lambda, u) \circ (\lambda, u) = (\lambda^2 + B(u, u), \lambda u + \lambda u) \\ &= (\lambda^2 + B(u, u), 2\lambda u), \end{aligned}$$

so projektorji rešitve sistema enačb

$$\lambda = \lambda^2 + B(u, u),$$

$$u = 2\lambda u.$$

Neničelni rešitvi zgornjega sistema sta

$$e = (1, 0) \quad \text{in} \quad p = (\tfrac{1}{2}, w),$$

pri čemer je $B(w, w) = \frac{1}{4}$. V nadaljevanju izračunajmo prostoru $\mathcal{V}$ pripadajoče lastne podprostore. V primeru, ko je $p = e$, je očitno $\mathcal{V}_1 = \mathcal{V}$ in $\mathcal{V}_0 = \mathcal{V}_{\frac{1}{2}} = 0$. V primeru netrivialnih projektorjev postopamo na naslednji način. Po definiciji je podprostor $\mathcal{V}_1$, ki pripada lastni vrednosti 1, oblike

$$\mathcal{V}_1 = \{ (\lambda, u) ; (\lambda, u) \circ (\tfrac{1}{2}, w) = (\lambda, u) \}.$$

Ker je

$$(\lambda, u) \circ (\tfrac{1}{2}, w) = (\tfrac{1}{2}\lambda + B(u, w), \lambda w + \tfrac{1}{2}u),$$

dobimo sistem enačb

$$\tfrac{1}{2}\lambda + B(u, w) = \lambda,$$

$$\lambda w + \tfrac{1}{2}u = u,$$

katerega rešitev je

$$\lambda = 2B(u, w),$$

$$u = 2\lambda w.$$

Od tod sledi

$$(\lambda, u) = (2B(u, w), 2\lambda w) = 4B(u, w)(\tfrac{1}{2}, w) \in \mathbb{F}\cdot(\tfrac{1}{2}, w),$$

oziroma

$$\mathcal{V}_1 = \{ k (\tfrac{1}{2}, w) ; k \in \mathbb{F} \} = \mathbb{F}\cdot p.$$

Za podprostor

$$\mathcal{V}_0 = \{ (\lambda, u) ; (\lambda, u) \circ (\tfrac{1}{2}, w) = (0, 0) \},$$

dobimo sistem enačb

$$\tfrac{1}{2}\lambda + B(u, w) = 0,$$

$$\lambda w + \tfrac{1}{2}u = 0,$$

katerega rešitve so oblike

$$\lambda = -2B(u, w),$$

$$u = -2\lambda w.$$

Če torej zapišemo

$$\begin{aligned}(\lambda, u) &= (-2B(u,w), -2\lambda w)\\ &= -4B(u,w)\,(\tfrac{1}{2}, -w) \in \mathbb{F}\cdot(\tfrac{1}{2}, -w)\,,\end{aligned}$$

sledi, da je

$$\mathcal{V}_0 = \{\, k\,(\tfrac{1}{2}, -w)\,;\, k \in \mathbb{F}\,\} = \mathbb{F}\cdot(e-p)\,.$$

Podobno za podprostor

$$\mathcal{V}_{\frac{1}{2}} = \{\,(\lambda, u)\,;\, (\lambda, u)\circ(\tfrac{1}{2}, w) = \tfrac{1}{2}(\lambda, u)\,\}\,,$$

dobimo sistem enačb

$$\tfrac{1}{2}\lambda + B(u,w) = \tfrac{1}{2}\lambda\,,$$

$$\lambda w + \tfrac{1}{2}u = \tfrac{1}{2}u\,,$$

katerega rešitev zadošča pogojema

$$B(u,w) = 0\,,$$

$$\lambda = 0\,.$$

Podprostor $\mathcal{V}_{\frac{1}{2}}$ je torej oblike

$$\mathcal{V}_{\frac{1}{2}} = \{\,(0, u)\,;\, B(u,w) = 0\,\}\,.$$

Če jordanska algebra $\mathcal{J}$ zadošča pogoju $(E3)$ definicije evklidske algebre,

$$\langle\, a\circ b\,,\, c\,\rangle = \langle\, a\,,\, b\circ c\,\rangle \quad \text{za vse } a, b, c \in \mathcal{J}\,,$$

ima razcep $\mathcal{J} = \mathcal{J}_0 + \mathcal{J}_{\frac{1}{2}} + \mathcal{J}_1$ naslednjo lastnost

Trditev 5.1. *Prostori $\mathcal{J}_i$ so paroma ortogonalni.*

Dokaz: Naj bosta $a \in \mathcal{J}_\alpha$ in $b \in \mathcal{J}_\beta$, pri čemer je $\alpha \neq \beta$. Tedaj velja

$$(\alpha-\beta)\,\langle\, a, b\,\rangle = \langle\, \alpha a, b\,\rangle - \langle\, a, \beta b\,\rangle = \langle\, p\circ a, b\,\rangle - \langle\, a, p\circ b\,\rangle = 0\,.$$

Ker je $\alpha - \beta \neq 0$, sledi $\langle\, a, b\,\rangle = 0$. □

Trditev 5.2. *Če je $\mathcal{J}$ jordanska algebra in p njen projektor, sta $\mathcal{J}_0$ in $\mathcal{J}_1$ ortogonalni podalgebri algebre $\mathcal{J}$,*

$$\mathcal{J}_0 \circ \mathcal{J}_1 = \{\, 0\,\}\,,$$

za kateri velja

$$(\mathcal{J}_0 + \mathcal{J}_1) \circ \mathcal{J}_{\frac{1}{2}} \subset \mathcal{J}_{\frac{1}{2}} \,,$$
$$\mathcal{J}_{\frac{1}{2}} \circ \mathcal{J}_{\frac{1}{2}} \subset \mathcal{J}_0 + \mathcal{J}_1 \,.$$

Dokaz: Če v identiteti (iii) trditve 1.1, nadomestimo a z p in b z a dobimo

$$L(p^2 \circ a) - L(p^2)L(a) = 2\,(\, L(p \circ a) - L(p)L(a) \,) \, L(p) \,,$$

oziroma

$$L(p \circ a) - L(p)L(a) = 2\,(\, L(p \circ a) - L(p)L(a) \,) \, L(p) \,.$$

Naj bosta $a \in \mathcal{J}_\lambda$ in $b \in \mathcal{J}_\mu$. Če dobljeno identiteto uporabimo na elementu b, dobimo

$$L(\lambda a)\, b - L(p)L(a)\, b = 2\,(\, L(\lambda a)L(p)\, b - L(p)L(a)L(p)\, b \,) \,,$$
$$(\, \lambda - L(p) \,)L(a)\, b - 2\,\lambda L(a)\, \mu b + 2\, L(p)L(a)\, \mu b = 0 \,,$$
$$(\, \lambda - L(p) \,)L(a)\, b - 2\,\mu\lambda L(a)\, b + 2\,\mu L(p)L(a)\, b = 0 \,,$$
$$(\, \lambda - L(p) \,)L(a)\, b - 2\mu\,(\, \lambda - L(p) \,)L(a)\, b = 0 \,,$$
$$(\, \lambda - L(p) \,)(\, 1 - 2\mu \,)\, (a \circ b) = 0 \,.$$

V primeru, da je $\mu = 0$ ali 1, sledi

$$L(p)\,(a \circ b) = \lambda(a \circ b) \,,$$

kar pomeni, da je $a \circ b \in \mathcal{J}_\lambda$. Vzemimo, da je $\lambda = 0$. Ker za poljubna $a \in \mathcal{J}_0$ in $b \in \mathcal{J}_0$ ali $\mathcal{J}_1$ velja $a \circ b \in \mathcal{J}_0$ sledi, da je $\mathcal{J}_0$ podalgebra algebre $\mathcal{J}$. Podobno za $\lambda = 1$ dobimo, da je tudi $\mathcal{J}_1$ podalgebra algebre $\mathcal{J}$. Ker je $\mathcal{J}$ direktna vsota podprostorov $\mathcal{J}_0$, $\mathcal{J}_1$ in $\mathcal{J}_{\frac{1}{2}}$, sledi

$$\mathcal{J}_0 \circ \mathcal{J}_1 = \{ \, 0 \, \} \,.$$

Če vzamemo, da je $\lambda = \frac{1}{2}$, dobimo

$$L(p)\,(a \circ b) = \tfrac{1}{2}(a \circ b) \,,$$

kar pomeni, da je za poljubna $a \in \mathcal{J}_{\frac{1}{2}}$ in $b \in \mathcal{J}_0 + \mathcal{J}_1$ produkt $a \circ b \in \mathcal{J}_{\frac{1}{2}}$. Od tod sledi

$$(\mathcal{J}_0 + \mathcal{J}_1) \circ \mathcal{J}_{\frac{1}{2}} \subset \mathcal{J}_{\frac{1}{2}} \,.$$

Kot dokaz zadnje inkluzije zadošča pokazati, da za $a \in \mathcal{J}_{\frac{1}{2}}$ velja $a^2 \in \mathcal{J}_0 + \mathcal{J}_1$, oziroma

$$a^2 = a_0 + a_1 \,,$$

pri čemer je $a_0 \in \mathcal{J}_0$ in $a_1 \in \mathcal{J}_1$. Če definiramo

$$a_0 = a^2 - a^2 \circ p \quad \text{in} \quad a_1 = a^2 \circ p \,,$$

sledi

$$\begin{aligned} L(p)\, a_0 &= (\, I - L(p)\,)\, a_1 = a^2 \circ p - (\, a^2 \circ p\,) \circ p = \\ &= a^2 \circ p^2 - (\, a^2 \circ p\,) \circ p = (\, L(a^2)L(p) - L(a^2 \circ p)\,)\, p \,, \end{aligned}$$

in od tod, z uporabo identitete (iii), trditve 1.1,

$$\begin{aligned} L(p)\, a_0 &= 2\, (\, L(a)L(p) - L(a \circ p)\,)\, L(a)\, p = \\ &= (\, L(a)L(p) - \tfrac{1}{2}\, L(a)\,)\, a = L(a)\, (\, L(p) - \tfrac{1}{2}\,)\, x = 0 \,. \end{aligned}$$

Zgoraj definiran a_0 je torej element $\mathcal{J}_0$. Ker velja

$$(\, I - L(p)\,)\, a_1 = 0 \,,$$

oziroma

$$L(p)\, a_1 = p \circ a_1 = a_1 \,,$$

je očitno tudi $a_1 \in \mathcal{J}_1$. □

Zgornjo trditev lahko predstavimo z naslednjo tabelo

$\circ$	$\mathcal{J}_0$	$\mathcal{J}_{\frac{1}{2}}$	$\mathcal{J}_1$
$\mathcal{J}_0$	$\mathcal{J}_0$	$\mathcal{J}_{\frac{1}{2}}$	0
$\mathcal{J}_{\frac{1}{2}}$	$\mathcal{J}_{\frac{1}{2}}$	$\mathcal{J}_0 + \mathcal{J}_1$	$\mathcal{J}_{\frac{1}{2}}$
$\mathcal{J}_1$	0	$\mathcal{J}_{\frac{1}{2}}$	$\mathcal{J}_1$

Iz tabele lahko razberemo, da sta v primeru $\mathcal{J}_{\frac{1}{2}} = 0$ podalgebri $\mathcal{J}_0$ in $\mathcal{J}_1$ celo ideala algebre $\mathcal{J}$.

V tretjem razdelku tega poglavja smo pokazali, da sta algebraično pravokotna projektorja tudi evklidsko pravokotna. Pokažimo, da velja tudi nasprotna implikacija oziroma naslednja

Trditev 5.3. *Naj bosta* p *in* q *projektorja evklidske jordanske algebre* $\mathcal{J}$*. Algebraična pravokotnost* $p \circ q = 0$ *in evklidska pravokotnost* $\langle p, q \rangle = 0$ *sta ekvivalentni.*

Dokaz: Pokazati torej zadošča, da iz $\langle p, q \rangle = 0$ sledi $p \circ q = 0$. Naj bo $\langle p, q \rangle = 0$. Očitno je tudi $\langle p \circ q, q \rangle = 0$. Zapišimo projektor q v obliki $q = q_0 + q_{\frac{1}{2}} + q_1$. Od tod sledi

$$p \circ q = p \circ (q_0 + q_{\frac{1}{2}} + q_1) = p \circ q_0 + p \circ q_{\frac{1}{2}} + p \circ q_1 = \tfrac{1}{2}\, q_{\frac{1}{2}} + q_1 \,.$$

Zaradi pravokotnosti Pierceovih podprostorov velja

$$0 = \langle p \circ q, q \rangle = \langle \tfrac{1}{2}\, q_{\frac{1}{2}} + q_1, q_0 + q_{\frac{1}{2}} + q_1 \rangle = \tfrac{1}{2}\, || \, q_{\frac{1}{2}} ||^2 + || \, q_1 ||^2 \,,$$

od koder sledi $q_{\frac{1}{2}} = q_1 = 0$, oziroma $p \circ q = 0$. □

Trditev 5.4. *Projektor* $p \in \mathcal{J}$ *je primitiven natanko tedaj, ko je* $\mathcal{J}_1 = \mathbb{R} \cdot p$*.*

Dokaz: Naj bo $\mathcal{J}_1 = \mathbb{R} \cdot p$. Če p ni primitiven, je $p = q + r$, pri čemer je $q \circ r = 0$. Ker velja

$$p \circ q = (q + r) \circ q = q \circ q + r \circ q = q + 0 = q \,,$$

sledi, da je $q \in \mathcal{J}_1$ in $q \notin \mathbb{R} \cdot p$, kar je protislovje.

Naj bo $p \in \mathcal{J}_1$ primitiven projektor. Če je $x \in \mathcal{J}_1(p)$, je po spektralnem izreku $x = \sum \lambda_i \, p_i$, kjer so p_i projektorji algebre generirane z x. Ker je $\mathcal{J}_1(p)$ podalgebra, so očitno $p_i \in \mathcal{J}_1(p)$. To med drugim pomeni, da je $p \circ p_1 = p_1$, od koder sledi

$$p_1 + (p - p_1) = p \,,$$

$$(p - p_1)^2 = p \circ p - 2\, p \circ p_1 + p_1 \circ p_1 = p - 2\, p_1 + p_1 = p - p_1 \,,$$

ter

$$p_1 \circ (p - p_1) = p_1 \circ p - p_1 \circ p_1 = p_1 - p_1 = 0 \,.$$

Ker je p primitiven, je $p_1 = p$, preostalih p_i pa sploh ni. Torej je $x = \lambda_1 \, p \in \mathbb{R} \cdot p$. □

Trditev 5.5. *Naj bosta* p *in* q *pravokotna primitivna projektorja evklidske jordanske algebre* $\mathcal{J}$*,* $\mathcal{J}_{\frac{1}{2}}(p)$ *in* $\mathcal{J}_{\frac{1}{2}}(q)$ *pa njima pripadajoča Pierceova podprostora. Če* $a \in \mathcal{J}_{\frac{1}{2}}(p) \cap \mathcal{J}_{\frac{1}{2}}(q)$*, potem velja* $|| \, p \, || = || \, q \, ||$ *in*

$$a^2 = \tfrac{1}{2} \, \tfrac{|| \, a \, ||^2}{|| \, p \, ||^2} \, (p + q) \,.$$

Opomba: *Ker imajo torej vsi pravokotni primitivni projektorji enako normo, lahko v nadaljevanju brez škode za splošnost predpostavimo, da je ta norma enaka 1. Identiteto trditve torej lahko zapišemo v obliki*

$$a^2 = \tfrac{1}{2}\,||\,a\,||^2\,(\,p+q\,)\,.$$

Dokaz: Če sta p in q pravokotna projektorja, je projektor tudi $p+q$. Velja namreč

$$(\,p+q\,)^2 = p\circ p + p\circ q + q\circ p + q\circ q = p^2+q^2 = p+q\,.$$

Denimo, da je $a\in\mathcal{J}_1(\,p\,)$, oziroma velja $p\circ a = a$. Ker po trditvi 3.4 $L(p)$ in $L(q)$ komutirata, velja

$$p\circ(\,q\circ a\,) = q\circ a\,.$$

To pa pomeni, da je $q\circ a\in\mathcal{J}_1(\,p\,)$. Podobno za $a\in\mathcal{J}_1(\,q\,)$ sledi, da je $p\circ a\in\mathcal{J}_1(\,q\,)$. Po definiciji je

$$\begin{aligned}
\mathcal{J}_1(\,p+q\,) &= \{\,a\in\mathcal{J}\,;\,(\,p+q\,)\circ a = a\,\}\\
&= \{\,a\in\mathcal{J}\,;\,p\circ a + q\circ a = a\,\}\\
&= \{\,a\in\mathcal{J}\,;\,p\circ a = a \text{ in } q\circ a = 0\,\}+\\
&\quad +\{\,a\in\mathcal{J}\,;\,p\circ a = 0 \text{ in } q\circ a = a\,\}+\\
&\quad +\{\,a\in\mathcal{J}\,;\,p\circ a = \tfrac{1}{2}\,a \text{ in } q\circ a = \tfrac{1}{2}\,a\,\}\,.
\end{aligned}$$

Če upoštevamo prejšnji ugotovitvi, dobimo

$$\mathcal{J}_1(\,p+q\,) = \mathcal{J}_1(\,p\,)+\mathcal{J}_1(\,q\,)+\mathcal{J}_{\frac{1}{2}}(\,p\,)\cap\mathcal{J}_{\frac{1}{2}}(\,q\,)\,.$$

Če je $a\in\mathcal{J}_{\frac{1}{2}}(\,p\,)\cap\mathcal{J}_{\frac{1}{2}}(\,q\,)$, po trditvi 5.2 sledi, da je $a^2\in\mathcal{J}_1(\,p\,)+\mathcal{J}_1(\,q\,)$. Ker sta p in q primitivna, je $\mathcal{J}_1(\,p\,)=\mathbb{R}\cdot p$ in $\mathcal{J}_1(\,q\,)=\mathbb{R}\cdot q$. Zapišimo a^2 v obliki

$$a^2 = \lambda\,p + \mu\,q\,,$$

in pokažimo, da je $||\,p\,|| = ||\,q\,||$. Če upoštevamo, da je

$$\lambda\,||\,p\,||^2 = \langle\,p, a^2\rangle = \langle\,p\circ a, a\,\rangle = \tfrac{1}{2}\,||\,a\,||^2\,,$$

in

$$\mu\,||\,q\,||^2 = \langle\,q, a^2\rangle = \langle\,q\circ a, a\,\rangle = \tfrac{1}{2}\,||\,a\,||^2\,,$$

dobimo identiteti

$$\lambda \,||\, p \,||^2 = \tfrac{1}{2} \,||\, a \,||^2 \quad \text{in} \quad \mu \,||\, q \,||^2 = \tfrac{1}{2} \,||\, a \,||^2 \,.$$

Ker v jordanski algebri $\mathcal{J}$ velja

$$[\, a^2, p, a \,] = 0 \,,$$

dobimo

$$\begin{aligned}
[\, \lambda\, p + \mu\, q, p, a \,] &= \lambda\, [\, p, p, a \,] + \mu\, [\, q, p, a \,] = \\
&= \lambda\, (\, p \circ (\, p \circ a \,) - (\, p \circ p \,) \circ a \,) + \\
&\quad + \mu\, (\, q \circ (\, p \circ a \,) - (\, q \circ p \,) \circ a \,)\,) = \\
&= \lambda\, (\, \tfrac{1}{4}\, a - \tfrac{1}{2}\, a \,) + \mu\, (\, \tfrac{1}{4}\, a \,) = \\
&= - \tfrac{1}{4}\, (\, \lambda - \mu \,)\, a = 0 \,,
\end{aligned}$$

od koder sledi, da je $\lambda = \mu$ oziroma

$$||\, p \,|| = ||\, q \,|| \,.$$

Če torej predpostavimo, da sta dobljeni normi projektorjev p in q enaki 1, sledi

$$a^2 = \tfrac{1}{2} \,||\, a \,||^2 \,(\, p + q \,) \,.$$

Posledica 5.6. *Naj bosta p in q pravokotna primitivna projektorja evklidske jordanske algebre $\mathcal{J}$. Če je $\mathcal{J}_{\frac{1}{2}}(\, p \,) \cap \mathcal{J}_{\frac{1}{2}}(\, q \,) \neq 0$, potem obstaja tak element $w \in \mathcal{J}$, da je $w^2 = e$ in velja*

$$P(\, w \,)\, p = q \,.$$

Dokaz: Naj bo w_0 tak element $\mathcal{J}_{\frac{1}{2}}(\, p \,) \cap \mathcal{J}_{\frac{1}{2}}(\, q \,)$, da je $||\, w_0 \,||^2 = 2$. Potem po prejšnji trditvi velja $w_0^2 = p + q$. Naj bo $w = w_0 + (\, e - p - q \,)$. Potem velja

$$\begin{aligned}
w^2 &= w_0^2 + 2\, w_0 \circ (\, e - p - q \,) + (\, e - p - q \,)^2 = \\
&= \; w_0^2 + 2\, w_0 \circ e - 2\, w_0 \circ p - 2\, w_0 \circ q + \\
&\quad + e^2 + p^2 + q^2 - 2\, e \circ q - 2\, e \circ q + 2\, p \circ q = \\
&= \; p + q + 2w_0 - w_0 - w_0 + e + p + q - 2p - 2q = e \,.
\end{aligned}$$

Od tod sledi

$$\begin{aligned} P(\,w\,)\,p &= P(\,w_0 + (\,e - p - q\,)\,)\,p = \\ &= 2\,L(\,w_0 + e - p - q\,)^2 p - L(\,(\,w_0 + e - p - q\,)^2\,)\,p = \\ &= \;2\,L(\,w_0 + e - p - q\,)\,(w_0 \circ a + e \circ p - p \circ p - q \circ p) \\ &\quad\; - e \circ p = \\ &= \;2\,L(\,w_0 + e - p - q\,)\,(\,\tfrac{1}{2}\,w_0 + p - p\,) - p = \\ &= L(\,w_0 + e - p - q\,)\,w_0 - p = \\ &= \;w_0^2 + e \circ w_0 - p \circ w_0 - q \circ w_0 - p = \\ &= p + q + w_0 - \tfrac{1}{2}\,w_0 - \tfrac{1}{2}\,w_0 - p = q\,. \end{aligned}$$

V nadaljevanju si nekoliko podrobneje oglejmo Pierceove podprostore $\mathcal{J}_i$, ki pripadajo različnim paroma pravokotnim projektorjem, za katere velja $p_1 + \ldots + p_n = e$. Najprej si oglejmo naslednji

Zgled 3. Naj bo $\mathcal{J}$ jordanska algebra realnih simetričnih matrik dimenzije $3{\times}3$. Če upoštevamo, da je na $\mathcal{J}$ skalarni produkt definiran s predpisom $\langle\, A, B\,\rangle = Sl\,(AB)$, so paroma pravokotni projektorji z lastnostjo, da je njihova vsota identiteta, naslednje matrike

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}, \quad \begin{bmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix}, \quad \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

Če jih povrsti označimo s p, q in r, so njim pripadajoči Pierceovi podprostori naslednjih oblik

$$\begin{aligned} p: \quad & \mathcal{J}_1 = \left\{ \begin{bmatrix} a & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} \right\}, \quad \mathcal{J}_0 = \left\{ \begin{bmatrix} 0 & 0 & 0 \\ 0 & b & f \\ 0 & f & c \end{bmatrix} \right\}, \\ & \mathcal{J}_{\frac{1}{2}} = \left\{ \begin{bmatrix} 0 & d & e \\ d & 0 & 0 \\ e & 0 & 0 \end{bmatrix} \right\}, \\ q: \quad & \mathcal{J}_1 = \left\{ \begin{bmatrix} 0 & 0 & 0 \\ 0 & b & 0 \\ 0 & 0 & 0 \end{bmatrix} \right\}, \quad \mathcal{J}_0 = \left\{ \begin{bmatrix} a & 0 & e \\ 0 & 0 & 0 \\ e & 0 & c \end{bmatrix} \right\}, \\ & \mathcal{J}_{\frac{1}{2}} = \left\{ \begin{bmatrix} 0 & d & 0 \\ d & 0 & f \\ 0 & f & 0 \end{bmatrix} \right\}, \end{aligned}$$

$$r: \quad \mathcal{J}_1 = \left\{ \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & c \end{bmatrix} \right\}, \quad \mathcal{J}_0 = \left\{ \begin{bmatrix} a & d & 0 \\ d & b & 0 \\ 0 & 0 & 0 \end{bmatrix} \right\},$$

$$\mathcal{J}_{\frac{1}{2}} = \left\{ \begin{bmatrix} 0 & 0 & e \\ 0 & 0 & f \\ e & f & 0 \end{bmatrix} \right\},$$

kjer so $a, b, c, d, e, f \in \mathbb{R}$. Z $\mathbb{R}{\cdot}p$, $\mathbb{R}{\cdot}q$ in $\mathbb{R}{\cdot}r$ označimo tisti Pierceove podprostore $\mathcal{J}_1$, ki pripadajo algebri $\mathcal{J}$ glede na projektorje p, q in r. Ker očitno $\mathcal{J}$ ne moremo zapisati v obliki $\mathcal{J} = \mathbb{R}{\cdot}p \oplus \mathbb{R}{\cdot}q \oplus \mathbb{R}{\cdot}r$, je smiselno definirati podprostore oblike

$$\mathcal{J}_{pq} = \left\{ \begin{bmatrix} 0 & d & 0 \\ d & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} \right\}, \quad \mathcal{J}_{pr} = \left\{ \begin{bmatrix} 0 & 0 & e \\ 0 & 0 & 0 \\ e & 0 & 0 \end{bmatrix} \right\},$$

$$\mathcal{J}_{qr} = \left\{ \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & f \\ 0 & f & 0 \end{bmatrix} \right\},$$

saj potem velja

$$\mathcal{J} = \mathbb{R}{\cdot}p \oplus \mathbb{R}{\cdot}q \oplus \mathbb{R}{\cdot}r \oplus \mathcal{J}_{pq} \oplus \mathcal{J}_{pr} \oplus \mathcal{J}_{qr}\,.$$

Hitro se lahko prepričamo, da so zgoraj definirani podprostori podani z naslednjimi predpisi

$$\mathcal{J}_{pq} = \{\, A \in \mathcal{J} \;:\; p \circ A = \tfrac{1}{2}\, A \;\text{ in }\; q \circ A = \tfrac{1}{2}\, A \,\},$$

$$\mathcal{J}_{pr} = \{\, A \in \mathcal{J} \;:\; p \circ A = \tfrac{1}{2}\, A \;\text{ in }\; r \circ A = \tfrac{1}{2}\, A \,\},$$

$$\mathcal{J}_{qr} = \{\, A \in \mathcal{J} \;:\; q \circ A = \tfrac{1}{2}\, A \;\text{ in }\; r \circ A = \tfrac{1}{2}\, A \,\}.$$

Zgornja dekompozicija predstavlja zgolj podrobnejšo delitev že obstoječe Pierceove dekompozicije glede na projektor p. Podalgebra $\mathcal{J}_1 = \mathbb{R}\cdot p$ je namreč ostala nespremenjena, podprostor $\mathcal{J}_{\frac{1}{2}}$ smo razdelili na $\mathcal{J}_{pq} \oplus \mathcal{J}_{pr}$, podprostor $\mathcal{J}_0$ pa na $\mathbb{R}\cdot q \oplus \mathbb{R}\cdot r \oplus \mathcal{J}_{qr}$.

Naj bo $\{\, p_1, \ldots, p_n \,\}$ sistem pravokotnih primitivnih projektorjev z lastnostjo $p_1 + \ldots + p_n = e$. Po prejšnjem zgledu je smiselno definirati naslednje podprostore jordanske algebre $\mathcal{J}$

$$\mathcal{J}_{ii} = \mathcal{J}_1(p_i) = \mathbb{R}{\cdot}p_i\,,$$

$$\mathcal{J}_{ij} = \mathcal{J}_{\frac{1}{2}}(p_i) \cap \mathcal{J}_{\frac{1}{2}}(p_j)\,.$$

Simbola $\mathcal{J}_1(p_i)$ in $\mathcal{J}_{\frac{1}{2}}(p_i)$ pri tem označujeta Pierceova podprostora $\mathcal{J}_1$ in $\mathcal{J}_{\frac{1}{2}}$, ki pripadata projektorju p_i.

Izrek 5.7. (i) Poljubno evklidsko jordansko algebro $\mathcal{J}$ lahko zapišemo kot direktno vsoto oblike

$$\mathcal{J} = \bigoplus_{i \leq j} \mathcal{J}_{ij}\,.$$

(ii) Veljajo naslednje identitete

$$\mathcal{J}_{ij} \circ \mathcal{J}_{ij} \subset \mathcal{J}_{ii} + \mathcal{J}_{jj}\,,$$

$$\mathcal{J}_{ij} \circ \mathcal{J}_{jk} \subset \mathcal{J}_{ik}\,, \ \text{če } i \neq k\,,$$

$$\mathcal{J}_{ij} \circ \mathcal{J}_{kl} = \{\,0\,\}\,, \ \text{če } \{\,i,j\,\} \cap \{\,k,l\,\} = 0\,.$$

Opomba : *Dekompozicijo* $\mathcal{J} = \oplus_{i\leq j}\,\mathcal{J}_{ij}$ *imenujemo tudi Pierceova dekompozicija algebre* $\mathcal{J}$*, glede na sistem pravokotnih projektorjev.*

Dokaz: (i) Ker so linearne transformacije $L(p_i)$ evklidske jordanske algebre $\mathcal{J}$ simetrične in po trditvi 3.4 tudi komutativne, obstaja taka baza algebre $\mathcal{J}$, da so transformacijam $L(p_i)$ pripadajoče matrike diagonalne. Ker so 0, $\frac{1}{2}$ in 1 edine lastne vrednosti transformacij $L(p_i)$ in velja $\sum L(p_i) = L(\sum p_i) = L(\,e\,) = I$, so edini možni skupni lastni prostori

$$\mathcal{L}_{ii} = \{\,a \in \mathcal{J}\,,\ L(\,p_k\,)\,a = \delta_{ik}\,a\,\}\,,$$

$$\mathcal{L}_{ij} = \{\,a \in \mathcal{J}\,,\ L(\,p_k\,)\,a = \tfrac{1}{2}\,(\,\delta_{ik} + \delta_{jk}\,)\,a\,\}\,,$$

pri čemer je δ_{ik} Kroneckerjev simbol. Če upoštevamo definicijo prostorov $\mathcal{J}_1(p)$ in $\mathcal{J}_{\frac{1}{2}}(p)$, sledi

$$\mathcal{L}_{ii} = \mathcal{J}_{ii} = \mathcal{J}_1(p_i)\,,$$

$$\mathcal{L}_{ij} = \mathcal{J}_{ij} = \mathcal{J}_{\frac{1}{2}}(p_i) \cap \mathcal{J}_{\frac{1}{2}}(p_j)\,.$$

(ii) Naj bo $e = p_i + p_j$. Potem je $\mathcal{B} = \mathcal{J}_{ii} + \mathcal{J}_{jj} + \mathcal{J}_{ij}$, Pierceova dekompozicija $\mathcal{B}$ glede na p_i in p_j. Če zapišemo, da je $\mathcal{J}_{ii} = \mathcal{B}_1(p_i)$,

$\mathcal{J}_{jj} = \mathcal{B}_0(p_i)$ in $\mathcal{J}_{ij}(p_i) = \mathcal{B}_{\frac{1}{2}}(p_i)$, z upoštevanjem trditve 5.2, dobimo naslednje inkluzije in identitete

$$\mathcal{J}_{ii}^2 \subset \mathcal{J}_{ii}\,,\;\; \mathcal{J}_{ij} \circ \mathcal{J}_{ii} \subset \mathcal{J}_{ij}\,,\;\; \mathcal{J}_{ij}^2 \subset \mathcal{J}_{ii} + \mathcal{J}_{jj}\,,\;\; \mathcal{J}_{ii} \circ \mathcal{J}_{jj} = \{\,0\,\}\,,$$

$$\text{če } i \neq j\ .$$

Naj bo $f = p_i + p_j + p_k$. Podobno kot prej, je $\mathcal{C} = \mathcal{J}_{ii} + \mathcal{J}_{jj} + \mathcal{J}_{kk} + \mathcal{J}_{ij} + \mathcal{J}_{ik} + \mathcal{J}_{jk}$, Pierceova dekompozicija $\mathcal{C}$ glede na p_i, p_j in p_k. Če označimo $e = p_i + p_j$, je očitno e idempotent prostora $\mathcal{C}$, za katerega velja $\mathcal{C}_1(e) = \mathcal{J}_{ii} + \mathcal{J}_{ij} + \mathcal{J}_{jj}$, $\mathcal{C}_0(e) = \mathcal{J}_{kk}$ in $\mathcal{J}_{\frac{1}{2}}(e) = \mathcal{J}_{ik} + \mathcal{J}_{jk}$. Ker po trditvi 5.2 velja $\mathcal{C}_0(e) \circ \mathcal{C}_1(e) = \{0\}$, sledi $\mathcal{J}_{ij} \circ \mathcal{J}_{kk} = \{0\}$. Če upoštevamo, da je $\mathcal{C}_{\frac{1}{2}}(e) \circ \mathcal{C}_1(e) \subset \mathcal{C}_{\frac{1}{2}}(e)$, dobimo

$$\mathcal{J}_{ij} \circ \mathcal{J}_{jk} \subset \mathcal{J}_{ik} + \mathcal{J}_{jk}\,.$$

Ker velja $\mathcal{J}_{ij} = \mathcal{J}_{ji}$ in $\mathcal{J}_{jk} = \mathcal{J}_{kj}$, sledi tudi

$$\mathcal{J}_{ij} \circ \mathcal{J}_{jk} = \mathcal{J}_{kj} \circ \mathcal{J}_{ji} \subset \mathcal{J}_{ki} + \mathcal{J}_{ji}\,.$$

Od tod sledi

$$\mathcal{J}_{ij} \circ \mathcal{J}_{jk} \subset (\,\mathcal{J}_{ik} + \mathcal{J}_{jk}\,) \cap (\,\mathcal{J}_{ki} + \mathcal{J}_{ji}\,) = \mathcal{J}_{ik}\,.$$

Pokažimo še zadnjo identiteto. Naj bo $g = p_i + p_j + p_k + p_l$. Potem je $\mathcal{D} = \mathcal{J}_{ii} + \mathcal{J}_{jj} + \mathcal{J}_{kk} + \mathcal{J}_{ll} + \mathcal{J}_{ij} + \mathcal{J}_{ik} + \mathcal{J}_{il} + \mathcal{J}_{jk} + \mathcal{J}_{jl} + \mathcal{J}_{kl}$, Pierceova dekompozicija prostora $\mathcal{D}$ glede na p_i, p_j, p_k in p_l. Če označimo $e = p_i + p_j$, je očitno e idempotent prostora $\mathcal{D}$, za katerega velja $\mathcal{J}_{ij} \subset \mathcal{D}_1(e)$ in $\mathcal{J}_{kl} \subset \mathcal{D}_0(e)$. Po trditvi 5.2 potem sledi, da je $\mathcal{D}_0(e) \circ \mathcal{D}_1(e) = \{0\}$, oziroma $\mathcal{J}_{ij} \circ \mathcal{J}_{kl} = \{0\}$. □

Trditev 5.8. *Za $a \in \mathcal{J}_{ij}$ in $b \in \mathcal{J}_{jk}$, $i \neq j \neq k$ veljata naslednji identiteti*

$$L(a)\,(\,a \circ b\,) = \tfrac{1}{8}\,||\,a\,||^2\,b\,,$$

$$||\,a \circ b\,||^2 = \tfrac{1}{8}\,||\,a\,||^2\,||\,b\,||^2\,.$$

Dokaz: Če v identiteti $(\,iii\,)$ trditve 1.1 najprej b nadomestimo s p_j, nato pa dobljen izraz uporabimo na elementu b, dobimo

$$[\,L(a^2 \circ p_j) - L(a^2)L(p_j)\,]\,b = 2\,[\,L(a \circ p_j) - L(a)L(p_j)\,]\,L(a)\,b\,,$$

oziroma

$$(\,a^2 \circ p_j\,) \circ b - a^2 \circ (\,p_j \circ b\,) = 2\,(\,a \circ p_j\,) \circ (\,a \circ b\,) - 2\,a \circ (\,p_j \circ (\,a \circ b\,)\,)\,.$$

Ker po trditvi 5.5 velja

$$a^2 = \tfrac{1}{2} ||\,a\,||^2\,(\,p_i + p_j\,)\,,$$

od tod sledi

$$\tfrac{1}{2}\,||\,a\,||^2\,(\,(\,p_i + p_j\,) \circ p_j\,) \circ b - \tfrac{1}{2}\,||\,a\,||^2\,(\,p_i + p_j\,) \circ (\,c_j \circ b\,) =$$

$$= 2\,(\,a \circ p_j\,) \circ (\,a \circ b\,) - 2\,a \circ (\,p_j \circ (\,a \circ b\,)\,)\,,$$

oziroma

$$\tfrac{1}{2}\,||\,a\,||^2\,(\,p_j \circ b - p_i \circ (\,p_j \circ b\,) - p_j \circ (\,p_j \circ b\,)\,) =$$

$$= 2\,(\,a \circ p_j\,) \circ (\,a \circ b\,) - 2\,a \circ (\,p_j \circ (\,a \circ b\,)\,)\,.$$

Ker je $b \in \mathcal{J}_{jk} \subset \mathcal{J}_1(\,p_j + p_k\,) \subset \mathcal{J}_0(\,p_i\,)$, sledi, da je $p_j \circ b = \frac{1}{2}\,b$ in $p_i \circ b = 0$. Od tod sledi

$$\tfrac{1}{2}\,||\,a\,||^2\,(\,\tfrac{1}{2}\,b - \tfrac{1}{4}\,b\,) = 2\,(\,a \circ p_j\,) \circ (\,a \circ b\,) - 2\,a \circ (\,p_j \circ (\,a \circ b\,)\,)\,.$$

Ker je $a \circ b \in \mathcal{J}_{ik} \subset \mathcal{J}_0(\,p_j\,)$ sledi, da je $p_j \circ (\,a \circ b\,) = 0$. Če upoštevamo, da je $a \in \mathcal{J}_{ij}$, oziroma velja $p_j \circ a = \frac{1}{2}\,a$, dobimo

$$\tfrac{1}{8}\,||\,a\,||^2\,b = a \circ (\,a \circ b\,)\,,$$

oziroma

$$\tfrac{1}{8}\,||\,a\,||^2\,b = L(a)\,(\,a \circ b\,)\,.$$

Če dobljeno identiteto skalarno pomnožimo z b, dobimo

$$\langle\,\tfrac{1}{8}\,||\,a\,||^2\,b, b\,\rangle = \langle\,L(a)\,(\,a \circ b\,), b\,\rangle\,,$$

$$\tfrac{1}{8}\,||\,a\,||^2\,\langle\,b, b\,\rangle = \langle\,a \circ b, a \circ b\,\rangle\,,$$

$$\tfrac{1}{8}\,||\,a\,||^2\,||\,b\,||^2 = ||\,a \circ b\,||^2\,.$$

Če zgoraj dobljeno identiteto renormiramo z

$$||\,x\,|| = \alpha\,|||\,x\,|||\,,$$

dobimo

$$\alpha^2\,|||\,a \circ b\,|||^2 = \tfrac{1}{8}\,\alpha^2\,|||\,a\,|||^2 \cdot \alpha^2\,|||\,b\,|||\,,$$

oziroma
$$|||\, a \circ b \,||| = \tfrac{1}{8}\,\alpha^2\, |||\, a \,|||^2 \cdot \; |||\, b \,|||^2 .$$
Če v dobljenem izrazu vzamemo, da je $\alpha = 2\sqrt{2}$, dobimo
$$|||\, a \circ b \,||| = |||\, a \,||| \cdot |||\, b \,||| .$$

Algebrske strukture, opremljene z normo takšne oblike, bodo predmet natančnejše obravnane naslednjega razdelka.

V nadaljevanju si oglejmo še nekatere lastnosti primitivnih projektorjev, ki jih bomo potrebovali v poglavju o klasifikaciji evklidskih algeber.

Trditev 5.9. *Naj bosta p in q različna nepravokotna primitivna projektorja jordanske algebre $\mathcal{J}$. Potem je algebra $\mathcal{J}(\, p, q\,)$, generirana s p in q, izomorfna $Sim(\, 2, \mathbb{R})$.*

Dokaz: Naj bo $\langle\, p, q\,\rangle = \lambda$. Po definiciji Pierceove projekcije velja
$$P(\, p\,)\, q = \lambda\, p\,, \;\; P(\, q\,)\, p = \lambda\, q\,.$$
Če definiramo $p \circ q = u$, dobimo
$$\lambda\, p = 2\, L(\, p\,)\, L(\, q\,)\, q - L(\, p^2)\, q \; =$$
$$= 2\, p \circ (\, p \circ q\,) - p^2 \circ q = 2\, p \circ u - p \circ q = 2\, p \circ u - u\,,$$
oziroma
$$p \circ u = \tfrac{1}{2}\, (\, \lambda\, p + u\,)\,.$$
Podobno dobimo, da je
$$q \circ u = \tfrac{1}{2}\, (\, \lambda\, q + u\,)\,.$$
Če uporabimo identiteto $(\, i\,)$ trditve 5.1.1 na elementih p in q ter upoštevamo zgornji zvezi, dobimo
$$\begin{aligned}
0 &= L(\, p\,)\, L(\, q\,)\, p - L(\, q\,)\, L(\, p\,)\, p + 2\, L(\, q\,)\, L(\, p \circ q\,)\, p \\
&\quad -2\, L(\, p \circ q\,)\, L(q\,)\, p = \\
&= \, p \circ (\, q \circ p\,) - q \circ p^2 + 2\, q \circ (\, (\, p \circ q\,) \circ p\,) - 2\, (\, p \circ q\,) \circ (\, q \circ p\,) = \\
&= p \circ u - u + 2\, q \circ (\, p \circ u\,) - 2\, u^2 = \\
&= \, \tfrac{1}{2}\, (\, \lambda\, p + u\,) - u + q \circ (\, \lambda\, p + u\,) - 2\, u^2 = \\
&= \tfrac{1}{2}\, \lambda\, a + \tfrac{1}{2}\, u - u + \lambda\, (\, q \circ p\,) + q \circ u - 2\, u^2 = \\
&= \, \tfrac{1}{2}\, \lambda\, p - \tfrac{1}{2}\, u + \lambda\, u + \tfrac{1}{2}\, \lambda\, q + \tfrac{1}{2}\, u - 2\, u^2 = \\
&= \tfrac{1}{2}\, \lambda\, p + \tfrac{1}{2}\, \lambda\, q + \lambda\, u - 2\, u^2\,,
\end{aligned}$$

oziroma

$$u^2 = \tfrac{\lambda}{4}\,(\,p + q + 2\,u\,)\,.$$

Ker veljata oceni

$$\lambda = \langle\, p, q\,\rangle = \langle\, p, q^2\,\rangle = \langle\, p \circ q, q\,\rangle = \langle\, L(\,p\,)\,q, q\,\rangle \geq 0$$

in

$$\lambda = \langle\, p, q\,\rangle = \langle\, p^2, q^2\,\rangle = \langle\, p\circ q, p\circ q\,\rangle = ||\,p\circ q\,||^2 \leq ||\,p\,||^2 \cdot ||\,q\,||^2 = 1\,,$$

lahko λ pišemo kot $\lambda = \cos^2\theta$. Naj bosta p_0 in q_0 matriki dimenzije 2×2, definirani s predpisom

$$p_0 = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \quad , \quad q_0 = \begin{bmatrix} \cos^2\theta & \cos\theta\,\sin\theta \\ \cos\theta\,\sin\theta & 0 \end{bmatrix}.$$

Če definiramo $u_0 = p_0 \circ q_0$, kjer $\circ$ predstavlja običajni jordanski produkt matrik, očitno velja

$$u_0 = \begin{bmatrix} \cos^2\theta & \frac{1}{2}\cos\theta\,\sin\theta \\ \frac{1}{2}\cos\theta\,\sin\theta & 0 \end{bmatrix}$$

in

$$u_0^2 = \tfrac{1}{2}\,(\,p_0 + q_0 + 2\,u_0\,)\,.$$

Ker je $\lambda \neq 0$, je očitno tudi $u_0 \neq 0$. Naj bo $\mathcal{J}' = \mathcal{S}im(\,2, \mathbb{R}\,)$. Definirajmo preslikavo $\rho : \mathcal{J}' \longrightarrow \mathcal{J}$ s predpisom

$$\rho(\,\alpha\,a_0 + \beta\,q_0 + \gamma\,u_0\,) = \alpha\,p + \beta\,q + \gamma\,u\,.$$

Očitno je ρ homomorfizem jordanskih algeber. Ker je $\mathcal{J}$ enostavna, je ρ tudi bijektiven. $\square$

Trditev 5.10. *Naj bosta p in q nepravokotna primitivna projektorja jordanske algebre $\mathcal{J}$. Potem obstaja tak element $w \in \mathcal{J}$, da je $w^2 = e$ in velja*

$$P(\,w\,)\,p = q\,.$$

Dokaz: Naj bo $w_0 \in \mathcal{J}'$ podan s predpisom

$$\begin{bmatrix} \cos\theta & \sin\theta \\ \sin\theta & -\cos\theta \end{bmatrix}.$$

Če sta p_0 in q_0 iz prejšnjega dokaza in je $\circ$ običajni jordanski produkt matrik, potem velja $P(w_0)\,p_0 = q_0$. Naj bo $c = \rho(e_0)$, pri čemer je

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

Če je $w_1 = \rho(w_0)$, potem velja $w_1^2 = c$. Če izberemo, da je $w = w_1 + e - c$, sledi

$$w^2 = e \text{ in } P(w)\,p = q\,.$$

Trditev 5.11. *Naj bo J enostavna jordanska algebra in $\{p_1, \dots, p_r\}$ množica takih pravokotnih primitivnih projektorjev, da je $p_1 + \dots + p_r = e$. Potem za vsak $1 \leq j \leq k \leq r$ velja $\mathcal{J}_{jk} \neq \{0\}$.*

Dokaz: Denimo, da je $\mathcal{J}_{ij} = \{0\}$, za neka i in j. Z ustrezno zamenjavo indeksov lahko dosežemo, da obstaja tak l, $1 \leq l < r$, da velja

$$\mathcal{J}_{1j} \neq \{0\}\,, \quad j = 1, \dots, l\,,$$
$$\mathcal{J}_{1j} = \{0\}\,, \quad j = l+1, \dots, r\,.$$

Naj bo $a = p_1 + \dots + p_l$. Potem velja

$$\mathcal{J}_{\frac{1}{2}}(a) = \sum_{i \leq l,\, j \geq l+1} \mathcal{J}_{ij}\,.$$

Ker je $\mathcal{J}$ enostavna jordanska algebra, očitno $\mathcal{J}_{\frac{1}{2}}(a)$ ni trivialna, oziroma velja $\mathcal{J}_{\frac{1}{2}}(a) \neq \{0\}$. Od tod sledi, da obstajata taka i in j, da je $i \leq l$, $j \geq l+1$ in velja $\mathcal{J}_{ij} \neq \{0\}$. Če privzamemo, da je $\mathcal{J}_{1i} \neq \{0\}$, potem sledi, da je tudi $\mathcal{J}_{1j} \neq \{0\}$, kar je protislovje s predpostavko. To pomeni, da je $\mathcal{J}_{jk} \neq \{0\}$, za vsak $1 \leq j \leq k \leq r$. $\square$

Posledica 5.12. *Naj bo $\mathcal{J}$ enostavna jordanska algebra.*

(i) Če sta p in q pravokotna primitivna projektorja, potem velja

$$\mathcal{J}_{\frac{1}{2}}(p) \cap \mathcal{J}_{\frac{1}{2}}(q) \neq \{0\}\,.$$

(ii) Če sta p in q primitivna projektorja, obstaja tak element $w \in \mathcal{J}$, da je $w^2 = e$ in velja

$$P(w)\,p = q\,.$$

To pomeni, da grupa avtomorfizmov $Aut(\mathcal{J})$ deluje na množici projektorjev tranzitivno.

Dokaz: (i) Ker sta po predpostavki p in q pravokotna in primitivna projektorja lahko množico $\{p, q\}$ dopolnimo do sistema paroma pravokotnih primitivnih projektorjev $\{p, q, p_1, \ldots, p_{r-2}\}$. Po prejšnji trditvi je potem očitno $\mathcal{J}_{\frac{1}{2}}(p) \cap \mathcal{J}_{\frac{1}{2}}(q) \neq \{0\}$.

(ii) Trditev je neposredna posledica trditve 5.10 in posledice 5.6.

□

Izrek 5.13. *Naj bodo $\mathcal{J}$ enostavna jordanska algebra, $\{p_1, \ldots, p_k\}$ in $\{q_1, \ldots, q_k\}$ pa taki množici pravokotnih primitivnih projektorjev, da je $p_1 + \ldots + p_k = q_1 + \ldots + q_k = e$. Potem obstaja tak avtomorfizem A, da velja*

$$A\, p_i = q_i\,.$$

Dokaz: Naj bodo $p_1, \ldots, p_l$ paroma pravokotni primitivni projektorji, p in q pa taka primitivna projektorja, da sta pravokotna na $p_1, \ldots, p_l$. Kot dokaz izreka zadošča pokazati obstoj takega avtomorfizma A, da velja

$$A\, p_j = p_j \;\text{ in }\; A\, p = q\,.$$

Naj bo $f = p_1 + \ldots + p_l$. Ker sta p in q pravokotna na $p_1, \ldots, p_l$, očitno velja p in $q \in \mathcal{J}_0(f)$. Po posledici 5.12 tedaj obstaja tak element $w_0 \in \mathcal{J}_0(f)$, da je $w_0^2 = e - f$ in velja $P(w_0)\,p = q$. Če zapišemo w v obliki $w = w_0 + f$, velja

$$\begin{aligned} w^2 &= (w_0 + f)^2 = w_0^2 + w_0 \circ f + f^2 = \\ &= e - f + (p_1 + \ldots + p_l) \circ (p_1 + \ldots + p_l) = \\ &= e - f + p_1 \circ p_1 + \ldots + p_l \circ p_l = \\ &= e - f + p_1 + \ldots + p_l = e - f + f = e\,. \end{aligned}$$

Ker velja

$$\begin{aligned} P(w)\,p &= P(w_0 + f)\,p = \\ &= 2\,L(w_0 + f)\,(w_0 \circ p + f \circ p) - L(w_0^2 + 2\,w_0 \circ f + f^2)\,p = \\ &= 2\,L(w_0 + f)\,(w_0 \circ p) - L(w_0^2 + f^2)\,p = \\ &= 2\,L(w_0)\,(w_0 \circ p) + 2\,L(f)\,(w_0 \circ p) - L(w_0^2)\,p - f \circ p = \\ &= 2\,L(w_0)\,(w_0 \circ p) - L(w_0^2) = P(w_0)\,p = q\,, \end{aligned}$$

je iskani avtomorfizem $A = P(w)$. □

Posledica 5.14. *Naj bosta* (p_1, q_1) *in* (p_2, q_2) *para različnih pravokotnih primitivnih projektorjev enostavne jordanske algebre* $\mathcal{J}$*. Potem velja*

$$dim\, \mathcal{J}_{\frac{1}{2}}(p_1) \cap \mathcal{J}_{\frac{1}{2}}(q_1) = dim\, \mathcal{J}_{\frac{1}{2}}(p_2) \cap \mathcal{J}_{\frac{1}{2}}(q_2).$$

5.6 Hurwitzove algebre

Algebro $\mathcal{A}$ nad obsegom $\mathbb{F} = \{\mathbb{R}, \mathbb{C}\}$, z enoto 1 in nedegenerirano multiplikativno kvadratno formo N,

$$N(a \circ b) = N(a) \cdot N(b),$$

imenujemo *Hurwitzova algebra.*

Opomba: Kvadratna forma N je nedegenerirana, če za njej pripadajočo simetrično bilinearno formo, podano s predpisom

$$f(a, b) = N(a+b) - N(a) - N(b),$$

velja

$$f(a,b) = 0, \quad \forall\, b \in \mathcal{A} \Longrightarrow a = 0.$$

Če je $\mathcal{A}$ Hurwitzova algebra nad obsegom $\mathbb{R}$ in je N pozitivno definitna kvadratna forma, potem algebro $\mathcal{A}$ imenujemo *evklidska Hurwitzova algebra.* Ime evklidska Hurwitzova algebra opravičimo z dejstvom, da je omenjena algebra opremljena z evklidsko strukturo. Če je namreč $\mathcal{A}$ Hurwitzova algebra in N pozitivno definitna kvadratna forma, lahko definiramo normo

$$||\ || : \mathcal{A} \longrightarrow \mathbb{R},$$

s predpisom

$$||\, a\, || = \sqrt{N(a)}.$$

Za tako definirano normo velja

$$||\, a \circ b\, || = \sqrt{N(a \circ b)} = \sqrt{N(a) \cdot N(b)} = ||\, a\, || \cdot ||\, b\, ||,$$

oziroma

$$||\, a \circ b\, || = ||\, a\, || \cdot ||\, b\, ||.$$

V nadaljevanju razdelka bodo predmet natančnejše obravnave predvsem evklidske Hurwitzove algebre. Naj bo torej $\mathcal{A}$ evklidska Hurwitzova algebra in N tista pozitivna kvadratna forma, ki opredeljuje običajni skalarni produkt. Namesto oznake $f(a,b)$ bomo tako v nadaljevanju uporabljali bolj običajno $\langle a,b\rangle$. Najprej definirajmo operacijo konjugiranja. Elementu a *konjugiran element* $\overline{a}$ je podan s predpisom

$$\overline{a} = 2\langle a,1\rangle 1 - a\,.$$

Ker je konjugiranje pravokotna simetrija glede na realno os $\mathbb{R}\cdot 1$, očitno veljajo naslednje identitete

$$||\,\overline{a}\,|| = ||\,a\,||\,,$$

$$\langle \overline{a},\overline{b}\rangle = \langle a,b\rangle\,,$$

$$\overline{\overline{a}} = a\,.$$

Ker je izraz

$$\langle a,1\rangle = \tfrac{1}{2}(a+\overline{a})$$

realno število, ga bomo v nadaljevanju imenovali *realni del* elementa a in označili z $\mathcal{R}e(a)$.

Podobno kot smo v prvem razdelku tega poglavja na jordanski algebri $\mathcal{J}$ definirali operator levega množenja, tudi na evklidski Hurwitzovi algebri $\mathcal{A}$ definirajmo operatorja levega in desnega množenja

$$L(a),\ R(a)\ :\ \mathcal{A}\longrightarrow\mathcal{A}\,,$$

s predpisom

$$L(a)\,b = a\circ b\,,\qquad R(a)\,b = b\circ a\,,$$

kjer sta $a,b\in\mathcal{A}$.

Trditev 6.1. *Za poljubne elemente a,b,u in v evklidske Hurwitzove algebre $\mathcal{A}$, velja naslednja identiteta*

$$\langle a\circ u, b\circ v\rangle + \langle a\circ v, b\circ u\rangle = 2\langle a,b\rangle\cdot\langle u,v\rangle\,.$$

Dokaz: Če v izrazu

$$||\,a\circ b\,|| = ||\,a\,||\cdot||\,b\,||\,,$$

element a nadomestimo z $a+u$, dobimo

$$\langle (a+u)\circ b, (a+u)\circ b\rangle = \langle a+u, a+u\rangle\cdot\langle b,b\rangle\,,$$

$$\langle a \circ b, a \circ b \rangle + \langle a \circ b, u \circ b \rangle + \langle u \circ b, a \circ b \rangle + \langle u \circ b, u \circ b \rangle =$$
$$= [\langle a, a \rangle + \langle a, u \rangle + \langle u, a \rangle + \langle u, u \rangle] \cdot \langle b, b \rangle$$
$$\text{in} \quad || a \circ b ||^2 + 2 \langle a \circ b, u \circ b \rangle + || u \circ b ||^2 =$$
$$= || a ||^2 || b ||^2 + 2 \langle a, u \rangle || b ||^2 + || u ||^2 || b ||^2 ,$$

oziroma

$$\langle a \circ b, u \circ b \rangle = \langle a, u \rangle \cdot || b ||^2 .$$

Če v dobljenem izrazu nadomestimo še element b z elementom $b+v$, dobimo

$$\langle a \circ b + a \circ v, u \circ b + u \circ v \rangle = \langle a, u \rangle \cdot \langle b + v, b + v \rangle ,$$

$$\langle a \circ b, u \circ b \rangle + \langle a \circ b, u \circ v \rangle + \langle a \circ v, u \circ b \rangle + \langle a \circ v, u \circ v \rangle =$$
$$= \langle a, u \rangle \cdot [\langle b, b \rangle + 2 \langle b, v \rangle + \langle v, v \rangle] .$$

Če upoštevamo, da za poljubna $x, y \in \mathcal{A}$ velja

$$\langle x, y \rangle = \tfrac{1}{2} (|| x + y ||^2 - || x ||^2 - || y ||^2) ,$$

dobimo naslednjo identiteto

$$\langle a \circ b, u \circ b \rangle = \tfrac{1}{2} (|| (a + u) \circ b ||^2 - || a \circ b ||^2 - || u \circ b ||^2) =$$
$$= \tfrac{1}{2} (|| a + u ||^2 - || a ||^2 - || u ||^2) \cdot || b ||^2 = \langle a, u \rangle \cdot \langle b, b \rangle .$$

Podobno dobimo, da je

$$\langle a \circ v, u \circ v \rangle = \langle a, u \rangle \cdot \langle v, v \rangle ,$$

od koder sledi

$$\langle a \circ b, u \circ v \rangle + \langle a \circ v, u \circ b \rangle = 2 \langle a, u \rangle \cdot \langle b, v \rangle .$$

Z zamenjavo elementov b in u sledi iskana identiteta

$$\langle a \circ u, b \circ v \rangle + \langle a \circ v, b \circ u \rangle = 2 \langle a, b \rangle \cdot \langle u, v \rangle .$$

Posledica 6.2. *Za poljubne elemente a, b in u evklidske Hurwitzove algebre $\mathcal{A}$, velja naslednja identiteta*

$$2 \mathcal{R}e(u) \cdot \langle a, b \rangle = \langle a \circ u, b \rangle + \langle a \circ \overline{u}, b \rangle .$$

Dokaz: Če v izrazu trditve 6.1 nadomestimo element v z elementom $\overline{u}$, dobimo identiteto

$$2\,\langle\, a, b\,\rangle \cdot \langle\, u, \overline{u}\,\rangle = \langle\, a \circ u, b \circ \overline{u}\,\rangle + \langle\, a \circ \overline{u}, b \circ u\,\rangle\,.$$

Če v prvem izrazu na desni nadomestimo $\overline{u}$ z $2\,\langle\, u, 1\,\rangle \cdot 1 - u$, v drugem pa u z $2\,\langle\, u, 1\,\rangle \cdot 1 - \overline{u}$, dobimo

$$\begin{aligned} 2\,\langle\, a, b\,\rangle \cdot \langle\, u, \overline{u}\,\rangle = {} & 2\,\langle\, u, 1\,\rangle\,[\,\langle\, a \circ u, b\,\rangle + \langle\, a \circ \overline{u}, b\,\rangle\,] \\ & + \langle\, a \circ u, b \circ -u\,\rangle + \langle\, a \circ \overline{u}, b \circ -\overline{u}\,\rangle\,. \end{aligned}$$

Ker velja

$$\langle\, u, \overline{u}\,\rangle = \langle\, u, 2\,\langle\, u, 1\rangle \cdot 1 - u\,\rangle = 2\,\langle\, u, 1\,\rangle \cdot \langle\, u, 1\,\rangle - \langle\, u, u\,\rangle\,,$$

lahko v zgornji identiteti izraz na levi zapišemo v obliki

$$2\,\langle\, a, b\,\rangle \cdot \langle\, u, \overline{u}\,\rangle = 4\,\langle\, a, b\,\rangle \cdot \langle\, u, 1\,\rangle^2 - 2\,\langle\, a, b\,\rangle \cdot \langle\, u, u\,\rangle\,.$$

Izračunajmo vrednost izraza

$$\begin{aligned} -2\,\langle\, a, b\,\rangle \cdot \langle\, u, u\,\rangle &= 2\,\langle\, a, -b\,\rangle \cdot \langle\, u, u\,\rangle \\ &= [\,||\, a - b\,||^2 - ||\, a\,||^2 - ||\, b\,||^2\,] \cdot ||\, u\,||^2\,. \end{aligned}$$

Ker tudi vsoto izrazov

$$\begin{aligned} \langle\, a \circ u, b \circ -u\,\rangle &= \tfrac{1}{2}\,[\,||\, a \circ u + b \circ -u\,||^2 - ||\, a \circ u\,||^2 - ||\, b \circ -u\,||^2\,] \\ &= \tfrac{1}{2}\,[\,||\, a \circ u - b \circ u\,||^2 - ||\, a \circ u\,||^2 - ||\, b \circ -u\,||^2\,] \\ &= \tfrac{1}{2}\,[\,||\, a - b\,||^2 - ||\, a||^2 - ||\, b\,||^2\,] \cdot ||\, u\,||^2 \end{aligned}$$

in

$$\begin{aligned} \langle\, a \circ \overline{u}, b \circ -\overline{u}\,\rangle &= \tfrac{1}{2}\,[\,||\, a \circ \overline{u} + b \circ -\overline{u}\,||^2 - ||\, a \circ \overline{u}\,||^2 - ||\, b \circ -\overline{u}\,||^2\,] \\ &= \tfrac{1}{2}\,[\,||\, a \circ \overline{u} - b \circ \overline{u}\,||^2 - ||\, a \circ \overline{u}\,||^2 - ||\, b \circ -\overline{u}\,||^2\,] \\ &= \tfrac{1}{2}\,[\,||\, a - b\,||^2 - ||\, a||^2 - ||\, b\,||^2\,] \cdot ||\, u\,||^2\,, \end{aligned}$$

lahko zapišemo v obliki

$$\langle\, a \circ u, b \circ -u\,\rangle + \langle\, a \circ \overline{u}, b \circ -\overline{u}\,\rangle = [\,||\, a - b\,||^2 - ||\, a||^2 - ||\, b\,||^2\,] \cdot ||\, u\,||^2\,,$$

sledi

$$-2\,\langle\, a, b\,\rangle\,\langle\, u, u\,\rangle = \langle\, a \circ u, b \circ -u\,\rangle + \langle\, a \circ \overline{u}, b \circ -\overline{u}\,\rangle\,.$$

Od tod sledi

$$2\langle a,b\rangle\cdot\langle u,1\rangle=\langle a\circ u,b\rangle+\langle a\circ\overline{u},b\rangle\,,$$

oziroma

$$2\,\mathcal{R}e(u)\cdot\langle a,b\rangle=\langle a\circ u,b\rangle+\langle a\circ\overline{u},b\rangle\,.$$

Trditev 6.3. *Naj bo $\mathcal{A}$ evklidska Hurwitzova algebra. Potem veljajo naslednje identitete*

$$\begin{aligned}
(i)\;\; & L(u)^*=L(\overline{u}),\;\; R(u)^*=R(\overline{u}),\\
(ii)\;\; & \mathcal{R}e(a\circ b)=\mathcal{R}e(b\circ a),\\
(iii)\;\; & \overline{a\circ b}=\overline{b}\circ\overline{a},\\
(iv)\;\; & a\circ\overline{a}=||\,a\,||^2,\\
(v)\;\; & L(u)^2=L(u^2),\;\; R(u)^2=R(u^2)\,.
\end{aligned}$$

Dokaz: (i) Če v identiteto trditve 6.1 vstavimo $v=1$, dobimo

$$2\,\mathcal{R}e(u)\cdot\langle a,b\rangle=\langle a\circ u,b\rangle+\langle a,b\circ u\rangle\,.$$

Ker hkrati, po posledici 6.2, velja

$$2\,\mathcal{R}e(u)\cdot\langle a,b\rangle=\langle a\circ u,b\rangle+\langle a\circ\overline{u},b\rangle\,,$$

od tod sledi

$$\langle a\circ\overline{u},b\rangle=\langle a,b\circ u\rangle\,.$$

Če dobljeno identiteto zapišemo v operatorski obliki, dobimo

$$\langle R(\overline{u})\,a,b\rangle=\langle a,R(u)\,b\rangle\,.$$

Ker je $R(u)$ endomorfizem algebre $\mathcal{A}$, očitno velja

$$R(\overline{u})=R(u)^*\,.$$

Podobno dokažemo, da velja tudi $\langle\overline{u}\circ a,b\rangle=\langle a,u\circ b\rangle$, oziroma

$$\langle L(\overline{u})\,a,b\rangle=\langle a,L(u)\,b\rangle\,.$$

Od tod sledi

$$L(\overline{u})=L(u)^*\,.$$

(ii) Po dokazu trditve (i) velja

$$\langle a, b \rangle = \langle \overline{b} \circ a, 1 \rangle = \mathcal{R}e(\overline{b} \circ a),$$

od koder sledi

$$\mathcal{R}e(b \circ a) = \langle a, \overline{b} \rangle = \langle a \circ b, 1 \rangle = \mathcal{R}e(a \circ b).$$

(iii) Če uporabimo trditev (i) in upoštevamo, da je $\langle \overline{u}, \overline{v} \rangle = \langle u, v \rangle$, sledi

$$\langle \overline{a \circ b}, c \rangle = \langle \overline{c}, a \circ b \rangle = \langle \overline{c} \circ \overline{b}, a \rangle = \langle \overline{b}, c \circ a \rangle = \langle \overline{b} \circ \overline{a}, c \rangle,$$

oziroma

$$\overline{a \circ b} = \overline{b} \circ \overline{a}.$$

(iv) Če v identiteti trditve 6.2 element v nadomestimo z u, dobimo

$$\langle ||u||^2 \cdot a, b \rangle = \langle a \circ u, b \circ u \rangle = \langle (a \circ u) \circ \overline{u}, b \rangle,$$

od koder sledi

$$||u||^2 \cdot a = (a \circ u) \circ \overline{u}.$$

Če v dobljeno identiteto vstavimo za $a = 1$, dobimo

$$||u||^2 = u \circ \overline{u}.$$

V splošnem to pomeni, da je

$$L(u) L(\overline{u}) = ||u||^2 \cdot I.$$

Če izraz $\overline{u} = 2\langle u, 1 \rangle \cdot 1 - u$, pomnožimo z u, po trditvi (iv) sledi

$$||u||^2 = \overline{u} \circ u = 2\langle u, 1 \rangle \cdot 1 \circ u - u \circ u.$$

Po prejšnjem torej sledi

$$L(u)\, L(2\langle u, 1 \rangle \cdot 1 - u) = 2\langle u, 1 \rangle \cdot u - u \circ u,$$

$$2\langle u, 1 \rangle\, L(u) - L(u)\, L(u) = 2\langle u, 1 \rangle\, L(u) - L(u \circ u),$$

oziroma

$$L(u)^2 = L(u^2).$$

Analogno dokažemo tudi trditev $R(u)^2 = R(u^2)$. $\square$

Definirajmo element a^{-1} s predpisom

$$a^{-1} = \frac{\overline{a}}{||\,a\,||^2}\,.$$

V nadaljevanju dokažimo upravičenost zgornje oznake. Z upoštevanjem identitet $(\,iv\,)$ in $(\,v\,)$ trditve 6.3, dobimo

$$L(\,a\,)\,L(\,a^{-1}) = \tfrac{1}{||\,a\,||^2}\,L(\,a\,)\,L(\,\overline{a}\,) = \tfrac{1}{||\,a\,||^2}\,L(\,a\,)\,L(\,2\,\langle\,1,a\,\rangle\cdot 1 - a\,) =$$

$$= \tfrac{1}{||\,a\,||^2}\,L(\,a\,)\,[\,2\,\langle\,1,a\,\rangle\cdot I - L(\,a\,)\,] = \tfrac{1}{||\,a\,||^2}\,[\,2\,\langle\,1,a\,\rangle\cdot L(\,a\,) - L(\,a\,)^2] =$$

$$= \tfrac{1}{||\,a\,||^2}\,[\,2\,\langle\,1,a\,\rangle\cdot L(\,a\,) - L(\,a^2)\,] = \tfrac{1}{||\,a\,||^2}\,[\,L(\,2\,\langle\,1,a\,\rangle\cdot a - a^2\,)\,] =$$

$$= \tfrac{1}{||\,a\,||^2}\,L(\,a\circ(\,2\,\langle\,1,a\,\rangle\cdot 1 - a\,)\,) = \tfrac{1}{||\,a\,||^2}\,L(\,a\circ\overline{a}\,) = I\,.$$

Podobno dokažemo, da je tudi

$$L(a^{-1})\,L(a) = I\,.$$

To pomeni, da je operator $L(a)$ obrnljiv. Podobno lahko dokažemo, da je obrnljiv tudi operator $R(a)$. Algebro $\mathcal{A}$ z lastnostjo, da sta pri vsakem neničelnem elementu $a \in \mathcal{A}$ operatorja $L(a)$ in $R(a)$ obrnljiva imenujemo *algebra z deljenjem.*

Če za poljubna elementa a in b algebre $\mathcal{A}$ velja

$$a\circ(\,a\circ b\,) = a^2\circ b\,,\ \ (\,b\circ a\,)\circ a = b\circ a^2\,,$$

oziroma

$$L(\,a\,)^2 = L(\,a^2\,)\,,\ \ R(\,a\,)^2 = R(\,a^2\,)\,,$$

algebro $\mathcal{A}$ imenujemo *alternativna algebra.* Dokazali smo, da je vsaka evklidska Hurwitzova algebra alternativna.

Analogno, kot smo to storili v tretjem razdelku četrtega poglavja, tudi na evklidski Hurwitzovi algebri $\mathcal{A}$ definirajmo *asociator* elementov a, b in $c \in \mathcal{A}$, z naslednjim predpisom

$$[\,a,b,c\,] = a\circ(\,b\circ c\,) - (\,a\circ b\,)\circ c\,.$$

Očitno je v primeru, da je algebra $\mathcal{A}$ asociativna, asociator ničelna funkcija. Po prejšnjem je algebra $\mathcal{A}$ alternativna, če za poljubna elementa a in $b \in \mathcal{A}$ velja

$$[\,a,a,b\,] = 0\ ,\ \ [\,b,a,a\,] = 0\,.$$

Od tod takoj sledi, da je asociator alternirajoča funkcija. Veljajo namreč naslednje identitete

$$[a,b,c] = [b,c,a] = [c,a,b] = -[c,b,a] = -[b,a,c] = -[a,c,b]\,.$$

Zgornje identitete dobimo , če v identiteti $[a,a,b] = 0$, elementa a in b zaporedoma nadomestimo z $a+b$ in c, $a+c$ in b ter $b+c$ in a.

Naj bo $(\mathcal{A}, \circ)$ algebra nad obsegom $\mathbb{R}$, z enoto 1 in konjugacijo, ki elementu a priredi element $\overline{a}$. Če na prostoru $\mathcal{A} \times \mathcal{A} = \mathcal{A}^2$, definiramo operacijo množenja s predpisom

$$(a,b)\cdot(u,v) = (a \circ u - \overline{v} \circ b, b \circ \overline{u} + v \circ a)\,,$$

$\mathcal{A}^2$ imenujemo *Cayley - Dicksonova razširitev* algebre $\mathcal{A}$. Če poljubnemu paru elementov a in $b \in \mathcal{A}$ priredimo elementa $(a,0)$ in $(b,0) \in \mathcal{A}^2$, sledi

$$(a,0)\cdot(b,0) = (a \circ b, 0)\,.$$

V zgornjem smislu torej lahko algebro $\mathcal{A}$ obravnavamo, kot podalgebro $(\mathcal{A}^2, \cdot)$. Očitno je element $(1,0)$ enota v $\mathcal{A}^2$. Če zapišemo $i = (0,1)$, v smislu zgoraj definiranega množenja sledi

$$i^2 = (-1,0)\,.$$

Vsak element $(a,b) \in \mathcal{A}^2$ torej lahko zapišemo v obliki $a + b \circ i$. Konjugiranje znotraj $\mathcal{A}^2$ definiramo s predpisom

$$\overline{a + b \circ i} = \overline{a} - b \circ i\,.$$

Očitno je torej $\mathcal{A}^2$ algebra z enoto in konjugacijo.

Zgled 1. Naj bo $\mathcal{A} = \mathbb{R}$, operacija $\circ$ pa običajno množenje realnih števil. Po zgornji definiciji je Cayley - Dicksonova razširitev algebre $\mathcal{A}$ ravno algebra kompleksnih števil, oziroma $\mathcal{A}^2 = \mathbb{C}$.

Zgled 2. Naj bo $\mathcal{A} = \mathbb{C}$. Najprej zgoraj definiran produkt Cayley - Dickensonove razširitve priredimo algebri $\mathbb{C}^2$. Če elemente algebre $\mathbb{C}$ pišemo v obliki (a,b), $a,b \in \mathbb{R}$ in upoštevamo, da je operacija $\circ$ običajno množenje realnih števil, sledi

$$[(a,b),(c,d)]\cdot[(x,y),(z,w)] =$$

$$= [\,(a,b)\cdot(x,y) - \overline{(z,w)}\cdot(c,d),(c,d)\cdot\overline{(x,y)} + (z,w)\cdot(a,b)\,] =$$

$$= [\,(a,b)\cdot(x,y) - (z,-w)\cdot(c,d),(c,d)\cdot(x,-y) + (z,w)\cdot(a,b)\,] =$$

$$= [\,(ax - yb, bx + ya) - (zc + dw, -wc + dz),$$

$$(cx + yd, dx - yc) + (za - bw, wa + bz)\,] =$$

$$= [\,(ax - \overline{y}b, b\overline{x} + ya) - (\overline{z}c + \overline{d}w, -w\overline{c} + d\overline{z}),$$

$$(c\overline{x} + \overline{y}d, dx - yc) + (za - \overline{b}w, w\overline{a} + bz)\,] =$$

$$= [\,(ax - \overline{y}b - \overline{z}c - \overline{d}w, b\overline{x} + ya + w\overline{c} - d\overline{z}),$$

$$(c\overline{x} + \overline{y}d + za - \overline{b}w, dx - yc + w\overline{c} + bz)\,].$$

Ker so $a,b,c,d,x,y,z,w \in \mathbb{R}$, lahko dobljeni izraz zapišemo v obliki

$$[\,(ax - by - cz - dw, ay + xb + cw - zd),$$

$$(az + xc + yd - bw, aw + xd + bz - yc)\,].$$

Če algebro $\mathbb{C}^2$ obravnavamo kot $\mathbb{R}^4$, lahko dobljeni izraz zapišemo v obliki

$$(ax - by - cz - dw, ay + xb + cw - zd,$$

$$az + xc + yd - bw, aw + xd + bz - yc),$$

od koder sledi

$$(a,b,c,d)\cdot(x,y,z,w) = (ax,0,0,0) + (0,ay,az,aw) +$$

$$+ (0, cw - zd, yd - bw, bz - yc) + (-by - cz - dw, 0,0,0).$$

Elemente prostora $\mathbb{R}^4$ zapišimo kot elemente prostora $\mathbb{R}+\mathbb{R}^3$. Zgornji produkt ima potem obliko

$$(a+u)\cdot(x+v) = ax - \langle u,v\rangle + av + xu + u \times v\,,$$

kjer $\langle u,v\rangle$ pomeni običajni skalarni, $u \times v$ pa običajni vektorski produkt v $\mathbb{R}^3$. Če za bazo izberemo četverko $\{1, e_1, e_2, e_3\}$, kjer je $\{e_1, e_2, e_3\}$ standardna ortonormirana baza prostora $\mathbb{R}^3$, dobimo, za zgornji produkt naslednjo tabelo množenja

$\cdot$	1	e_1	e_2	e_3
1	1	e_1	e_2	e_3
e_1	e_1	-1	e_3	$-e_2$
e_2	e_2	$-e_3$	-1	e_1
e_3	e_3	e_2	$-e_1$	-1

Cayley - Dicksonova razširitev algebre $\mathcal{A} = \mathbb{C}$ je torej izomorfna strukturi, ki smo jo v tretjem poglavju poimenovali algebra kvaternionov $\mathbb{H}$. V razdelku o kvaternionih smo dokazali, da je $\mathbb{H}$ asociativna in nekomutativna algebra.

Zgled 3. Naj bo $\mathcal{A} = \mathbb{H}$. Če podobno kot v prejšnjem zgledu, elemente razširitve $\mathbb{H}^2$ pišemo v obliki $a + u$, kjer je $a \in \mathbb{R}$ in $u \in \mathbb{R}^7$, lahko produkt iz definicije pišemo v obliki

$$(a+u)\cdot(x+v) = ax - \langle u, v \rangle + av + xu + u \times v\,.$$

Izraz $\langle u, v \rangle$ pri tem pomeni običajni skalarni, $u \times v$ pa vektorski produkt v $\mathbb{R}^7$.

Če za bazo izberemo osmerico $\{1, e_1, e_2, e_3, e_4, e_5, e_6, e_7\}$, kjer je $\{e_1, e_2, e_3, e_4, e_5, e_6, e_7\}$ ortonormirana baza prostora $\mathbb{R}^7$, dobimo, za zgornji produkt naslednjo tabelo množenja

$\cdot$	1	e_1	e_2	e_3	e_4	e_5	e_6	e_7
1	1	e_1	e_2	e_3	e_4	e_5	e_6	e_7
e_1	e_1	-1	e_3	$-e_2$	e_5	$-e_4$	$-e_7$	e_6
e_2	e_2	$-e_3$	-1	e_1	e_6	e_7	$-e_4$	$-e_5$
e_3	e_3	e_2	$-e_1$	-1	e_7	$-e_6$	e_5	$-e_4$
e_4	e_4	$-e_5$	$-e_6$	$-e_7$	-1	e_1	e_2	e_3
e_5	e_5	e_4	$-e_7$	e_6	$-e_1$	-1	$-e_3$	e_2
e_6	e_6	e_7	e_4	$-e_5$	$-e_2$	e_3	-1	$-e_1$
e_7	e_7	$-e_6$	e_5	e_4	$-e_3$	$-e_2$	e_1	-1

Dobljeno strukturo imenujemo algebra *oktonionov* $\mathbb{O}$. Očitno je algebra $\mathbb{H}$ podalgebra algebre $\mathbb{O}$. Zaradi nekomutativnosti $\mathbb{H}$ je očitno nekomutativna tudi $\mathbb{O}$. Ker je $e_1\cdot(e_2\cdot e_4) = e_1\cdot e_6 = -e_7$ in $(e_1\cdot e_2)\cdot e_4 = e_3\cdot e_4 = e_7$, algebra $\mathbb{O}$ ni asociativna.

Trditev 6.4. *Naj bo $\mathcal{A}$ evklidska Hurwitzova algebra. Potem je njena Cayley - Dicksonova razširitev $\mathcal{A}^2$, opremljena z normo, podano s predpisom*

$$||\, a+b\circ i\,||^2 = ||\, a\,||^2 + ||\, b\,||^2\,,$$

evklidska Hurwitzova algebra natanko tedaj, ko je algebra $\mathcal{A}$ asociativna. Dokaz: Izračunajmo vrednost izraza

$$||\,(\,a+b\circ i\,)\cdot(\,u+v\circ i\,)\,||^2\,.$$

Če upoštevamo, da je $a+b\circ i$ zapis elementa $(\,a,b\,)$, sledi

$$||\,(\,a+b\circ i\,)\cdot(\,u+v\circ i\,)\,||^2 = ||\,(\,a\circ u-\overline{v}\circ b, b\circ\overline{u}+v\circ a\,)\,||^2 =$$

$$= ||\, a\circ u-\overline{v}\circ b\,||^2 + ||\, b\circ\overline{u}+v\circ a\,||^2 =$$

$$= ||\,a\,||^2\cdot||\,u\,||^2 - 2\,\langle\, a\circ u,\overline{v}\circ b\,\rangle + ||\,v\,||^2\cdot||\,b\,||^2 + ||\,b\,||^2\cdot||\,u\,||^2 +$$

$$+2\,\langle\, b\circ\overline{u}, v\circ a\,\rangle + ||\,v\,||^2\cdot||\,a\,||^2\,.$$

Od tod sledi, da velja identiteta

$$||\,(\,a+b\circ i\,)\cdot(\,u+v\circ i\,)\,||^2 = ||\,a+b\circ i\,||^2 + ||\,u+v\circ i\,||^2\,,$$

natanko tedaj, ko velja

$$\langle\, a\circ u,\overline{v}\circ b\,\rangle = \langle\, b\circ\overline{u}, v\circ a\,\rangle\,,$$

oziroma

$$\langle\, v\circ(\,a\circ u\,), b\,\rangle = \langle\, b, (\,v\circ a\,)\circ u\,\rangle\,.$$

Od tod sledi, da omenjena identiteta velja natanko tedaj, ko je

$$v\circ(\,a\circ u\,) = (\,v\circ a\,)\circ u\,,$$

oziroma je algebra $\mathcal{A}$ asociativna. □

Trditev 6.5. *Naj bosta $\mathcal{A}$ evklidska Hurwitzova algebra z enoto 1 in $\mathcal{B}$ taka njena podalgebra, da je 1 element algebre $\mathcal{B}$ in $\mathcal{B}\neq\mathcal{A}$. Naj bo i enotski vektor algebre $\mathcal{A}$, ki je pravokoten na $\mathcal{B}$. Potem je podprostor $\mathcal{B}\circ i$ pravokoten na $\mathcal{B}$, vsota $\mathcal{B}+\mathcal{B}\circ i$ pa je podalgebra, ki je izomorfna Cayley - Dicksonovi razširitvi algebre $\mathcal{B}$. To pomeni, da za poljubna a in $b\in\mathcal{B}$ velja*

$$(\,a+b\circ i\,)\cdot(\,u+v\circ i\,) = (\,a\circ u-\overline{v}\circ b\,) + (\,b\circ\overline{u}+v\circ a\,)\circ i\,.$$

Dokaz: Dokažimo najprej, da se konjugiranje na $\mathcal{B}+\mathcal{B}\circ i$ ujema s tistim iz definicije konjugiranja na $\mathcal{A}^2$. Ker je $1\in\mathcal{B}$, i pa enotski vektor pravokoten na $\mathcal{B}$, sledi, da je $\langle\, i,1\,\rangle=0$. Ker je $\overline{i}=2\,\langle\, i,1\,\rangle\cdot 1-i=-i$, od tod sledi

$$i^2=-i\circ i=-||\, i\,||^2=-1\,.$$

Za vsak $a\in\mathcal{B}$ torej velja

$$\begin{aligned}0&=\langle\, a,i\,\rangle=\langle\, 1,i\circ\overline{a}\,\rangle=\tfrac{1}{2}\,(\, i\circ\overline{a}+\overline{\overline{a}\circ i}\,)\\&=\tfrac{1}{2}\,(\,\overline{a}\circ i+\overline{i}\circ a\,)=\tfrac{1}{2}\,(\,\overline{a}\circ i-i\circ a\,)\,,\end{aligned}$$

od koder sledi

$$i\circ a=\overline{a}\circ i\,.$$

Z upoštevanjem dobljene identitete sledi, da je

$$\overline{a\circ i}=\overline{i}\circ\overline{a}=-i\circ\overline{a}=-a\circ i\,.$$

Za a in $b\in\mathcal{B}$ je torej

$$\overline{a+b\circ i}=\overline{a}+\overline{b\circ i}=\overline{a}-b\circ i\,.$$

Ker za poljubna a in $b\in\mathcal{B}$ velja

$$\langle\, a,b\circ i\,\rangle=\langle\,\overline{b}\circ a,i\rangle=0\,,$$

sledi, da je $\mathcal{B}\circ i$ pravokoten na $\mathcal{B}$.

Ker velja

$$(\, a+b\circ i\,)\cdot(\, u+v\circ i\,)=a\circ u+a\circ(\, v\circ i\,)+(\, b\circ i\,)\circ u+(\, b\circ i\,)\circ(\, v\circ i\,)\,,$$

za dokaz izomorfnosti zadošča dokazati naslednje identitete

$$(\, a\circ i\,)\circ b=(\, a\circ\overline{b}\,)\circ i\,,$$

$$a\circ(\, b\circ i\,)=(\, b\circ a\,)\circ i\,,$$

$$(\, a\circ i\,)\circ(\, b\circ i\,)=-\overline{b}\circ a\,.$$

Ker je $\langle\,\overline{b},i\,\rangle=\langle\,\overline{i},b\,\rangle=-\,\langle\, i,b\,\rangle=0$, za vsak $c\in\mathcal{A}$, po trditvi 6.1 velja

$$0=2\,\langle\, i,\overline{b}\,\rangle\cdot\langle\, c,a\,\rangle=\langle\, c\circ\overline{b},a\circ i\,\rangle+\langle\, c\circ i,a\circ\overline{b}\,\rangle\,.$$

Od tod sledi

$$\langle c, (a \circ i) \circ b \rangle = \langle c, (a \circ \overline{b}) \circ i \rangle,$$

oziroma

$$(a \circ i) \circ b = (a \circ \overline{b}) \circ i.$$

Po konjugiranju obeh strani zgornje identitete, dobimo

$$\overline{b} \circ \overline{(a \circ i)} = -(a \circ \overline{b}) \circ i,$$

oziroma

$$\overline{b} \circ (a \circ i) = (a \circ \overline{b}) \circ i.$$

Če upoštevamo, da za poljubna a in $b \in \mathcal{B}$ velja

$$0 = \langle \overline{a} \circ b, i \rangle = \langle (\overline{a} \circ b) \circ i, 1 \rangle = \langle (\overline{a} \circ i) \circ \overline{b}, 1 \rangle = \langle \overline{a} \circ i, b \rangle = \langle \overline{a}, b \circ i \rangle,$$

po trditvi 6.1 sledi

$$0 = 2 \langle \overline{a}, b \circ i \rangle \cdot \langle c, i \rangle = \langle c \circ \overline{a}, i \circ (b \circ i) \rangle + \langle i \circ \overline{a}, c \circ (b \circ i) \rangle.$$

Ker je

$$i \circ (b \circ i) = i \circ (i \circ \overline{b}) = R(i)^2 \overline{b} = R(i^2)\, \overline{b} = -\overline{b},$$

sledi

$$0 = \langle c \circ \overline{a}, -\overline{b} \rangle + \langle i \circ \overline{a}, c \circ (b \circ i) \rangle,$$
$$\langle c, \overline{b} \circ a \rangle = \langle (i \circ \overline{a}) \circ \overline{(b \circ i)}, c \rangle,$$
$$\langle c, \overline{b} \circ a \rangle = -\langle (a \circ i) \circ (b \circ i), c \rangle,$$

in od tod

$$\overline{b} \circ a = -(a \circ i) \circ (b \circ i).$$

Hurwitzov izrek 6.6. *Edine evklidske Hurwitzove algebre so $\mathbb{R}$, $\mathbb{C}$, $\mathbb{H}$ in $\mathbb{O}$.*

Dokaz: Naj bo $\mathcal{A}$ evklidska Hurwitzova algebra. Označimo z $\mathcal{A}_1 = \mathbb{R} \cdot 1$. Če $\mathcal{A} \neq \mathcal{A}_1$, izberimo v algebri $\mathcal{A}$ tak enotski vektor i_1, da bo pravokoten na $\mathcal{A}_1$. Po trditvi 6.5 je potem podalgebra $\mathcal{A}_2 = \mathcal{A}_1 + \mathcal{A}_1 \circ i_1$ algebre $\mathcal{A}$, izomorfna $\mathbb{C}$. Če $\mathcal{A} \neq \mathcal{A}_2$, podobno konstruiramo podalgebro $\mathcal{A}_3$, ki je izomorfna $\mathbb{H}$. Če je tudi $\mathcal{A} \neq \mathcal{A}_3$, konstruiramo podalgebro $\mathcal{A}_4$, ki je izomorfna $\mathbb{O}$. Pokažimo, da je tedaj $\mathcal{A} = \mathcal{A}_4$. Denimo, da $\mathcal{A} \neq \mathcal{A}_4$. Potem lahko v algebri $\mathcal{A}$ izberemo tak enotski vektor i_4, da bo pravokoten na $\mathcal{A}_4$ in bo podalgebra $\mathcal{A}_5 = \mathcal{A}_4 + \mathcal{A}_4 \circ i_4$ evklidska Hurwitzova algebra. To pa po trditvi 6.4 pomeni, da je $\mathcal{A}_4$ asociativna algebra. Ker $\mathbb{O}$ ni asociativna, od tod sledi, da je $\mathcal{A} = \mathcal{A}_4$. □

6 Strukturna analiza evklidskih algeber

6.1 Ideali

Ker je pojem ideala dobro znan že iz dodiplomske algebre, osvežimo le nekatere elementarne lastnosti idealov, ki jih bomo potrebovali ob obravnavi strukturne teorije evklidskih algeber.

Naj bo $\mathcal{E}$ algebra, lahko tudi nekomutatvna, neasociativna in brez enote. Podprostor $\mathcal{J}$ algebre $\mathcal{E}$ imenujemo *levi ideal*, če izpolnjuje naslednji pogoj: produkt elementa množice $\mathcal{J}$ s poljubnim elementom algebre $\mathcal{E}$, z leve, je element $\mathcal{J}$. Simbolno pogoj zapišemo

$$\mathcal{E} \circ \mathcal{J} \subset \mathcal{J} .$$

Povsem analogno definiramo tudi *desni ideal*. V nadaljevanju bomo z besedo *ideal* označevali dvostranski ideal, torej strukturo za katero velja

$$\mathcal{J} \circ \mathcal{E}, \mathcal{E} \circ \mathcal{J} \subset \mathcal{J} .$$

Elementarno je dejstvo, da je presek poljubne družine levih ali desnih idealov spet ideal iste vrste. Zato vsaka množica $\mathcal{S} \subset \mathcal{E}$ generira najmanjši levi ideal, najmanjši desni ideal in najmanjši ideal, v katerem je vsebovana. Na povsem naraven način lahko torej definiramo *vsoto levih idealov* $\mathcal{L}_1 + \mathcal{L}_2 = \{ a + b \, : \, a \in \mathcal{L}_1 \text{ in } b \in \mathcal{L}_2 \}$, ki je prav tako levi ideal. Podobno definiramo tudi vsoto desnih in dvostranskih idealov. Očitno je presek $\mathcal{J}_1 \cap \mathcal{J}_2$ največji ideal, ki je vsebovan v idealih $\mathcal{J}_1$ in $\mathcal{J}_2$, vsota $\mathcal{J}_1 + \mathcal{J}_2$ pa najmanjši ideal, ki vsebuje $\mathcal{J}_1$ in $\mathcal{J}_2$.

V primeru, da je presek dveh idealov $\mathcal{J}_1$ in $\mathcal{J}_2$ trivialen, njuno vsoto pišemo kot $\mathcal{J}_1 \oplus \mathcal{J}_2$. Imenujemo jo *direktna vsota idealov* $\mathcal{J}_1$ in $\mathcal{J}_2$. Ker je $\mathcal{J}_1 \circ \mathcal{J}_2 \subset \mathcal{J}_1 \cap \mathcal{J}_2$, je v primeru direktne vsote produkt obeh idealov trivialen. Množenje v $\mathcal{J}_1 \oplus \mathcal{J}_2$ tako naravno razpade na množenje znotraj $\mathcal{J}_1$ in znotraj $\mathcal{J}_2$. Od tod ideja strukturne teorije, da algebre poskušamo razcepiti na direktne vsote idealov.

Ideali, ki jih ni mogoče razcepiti na manjše ideale, bodo tvorili osnovne gradnike iz katerih bomo tvorili kompleksnejše strukture. Če je $\mathcal{J}$ tak ideal algebre $\mathcal{E}$, da obstaja ideal $\mathcal{J}_1$ za katerega velja $\mathcal{J} \oplus \mathcal{J}_1 = \mathcal{E}$, $\mathcal{J}$ imenujemo *komplementiran ideal.* V primeru, da tak ideal ne obstaja pravimo, da $\mathcal{J}$ nima komplementa.

Množica, ki vsebuje samo element 0, je ideal v vsaki algebri. Prav tako je tudi množica, ki vsebuje vse elemente algebre $\mathcal{E}$ ideal. Taka ideala imenujemo *trivialna ideala. Pravi* oziroma *netrivialen* imenujemo torej tak ideal, ki ne vsebuje samo elementa 0 in ne vsebuje vseh elementov algebre $\mathcal{E}$. Denimo, da ima algebra $\mathcal{E}$ element 1 in da je 1 v nekem desnem idealu $\mathcal{J}$. Če je k poljuben element iz $\mathcal{E}$, pripada produkt $1 \circ k = k$ idealu $\mathcal{J}$. Torej vsebuje $\mathcal{J}$ vse elemente algebre $\mathcal{E}$ in zato ni pravi ideal. Naj bo a poljuben obrnljiv element ideala $\mathcal{J}$. Ker je potem v idealu tudi produkt $a \circ a^{-1} = 1$, če je $\mathcal{J}$ desni ideal oziroma $a^{-1} \circ a = 1$, če je $\mathcal{J}$ levi ideal, sledi $\mathcal{J} = \mathcal{E}$. Pravi ideal torej ne vsebuje identitete algebre in nobenega obrnljivega elementa.

Levi in desni ideal imenujemo *minimalen*, če je neničelen in ne vsebuje nobenega drugega neničelnega ideala iste vrste. Podobno je definiran maksimalni ideal, ki je po definiciji različen od cele algebre. Algebro, ki nima netrivialnih idealov imenujemo *enostavna.* Seveda ni nujno res, da enostavna algebra ne vsebuje netrivialnih levih ali desnih idealov. Če za ideala $\mathcal{J}_1$ in $\mathcal{J}_2$ algebre $\mathcal{E}$ velja, da iz $\mathcal{J}_1 \circ \mathcal{J}_2 = 0$ sledi $\mathcal{J}_1 = 0$ ali $\mathcal{J}_2 = 0$, algebro $\mathcal{E}$ imenujemo *praalgebra.* Ideal $\mathcal{J}$ algebre $\mathcal{E}$ imenujemo *praideal*, če iz $\mathcal{J}_1 \circ \mathcal{J}_2 \subset \mathcal{J}$ sledi $\mathcal{J}_1 \subset \mathcal{J}$ ali $\mathcal{J}_2 \subset \mathcal{J}$. To pa pomeni, da je $\mathcal{E}$ praalgebra natanko tedaj, ko je ideal 0 njegov praideal.

V nadaljevanju si oglejmo tiste lastnost idealov, ki jih bomo potrebovali pri opisu strukturne teorije evklidskih algeber. Naj bo $\mathcal{E}$ evklidska algebra. Pokažimo najprej naslednjo

Trditev 1.1. *Če je $\mathcal{I}$ ideal algebre $\mathcal{E}$, je ideal tudi njegov ortogonalni komplement $\mathcal{I}^{\perp}$, podan s predpisom*

$$\mathcal{I}^{\perp} = \{\, a \in \mathcal{E} \,:\, \forall\, b \in \mathcal{I},\ \langle\, a, b\,\rangle = 0\,\}\,.$$

Dokaz: Naj bosta $a \in \mathcal{E}$ in $b \in \mathcal{I}^{\perp}$. Ker za poljuben element $c \in \mathcal{I}$ velja

$$\langle\, a \circ b,\ c\,\rangle = \langle\, b, a \circ c\,\rangle = 0\,,$$

sledi $a \circ b \in \mathcal{I}^\perp$, oziroma zgoraj definirana množica $\mathcal{I}^\perp$ je ideal. $\square$

Ker je torej $\mathcal{E} = \mathcal{I} \oplus \mathcal{I}^\perp$, je vsak ideal evklidske algebre komplementiran. Denimo, da sta $\mathcal{I}$ in $\mathcal{J}$ različna minimalna ideala algebre $\mathcal{E}$. Očitno je, zaradi minimalnosti, $\mathcal{I} \cap \mathcal{J} = 0$, od koder sledi $\mathcal{I} \circ \mathcal{J} \subset \mathcal{I} \cap \mathcal{J} = 0$. Od tod sledi $\langle \mathcal{I}, \mathcal{J} \rangle = \langle 1, \mathcal{I} \circ \mathcal{J} \rangle = 0$. Dokazali smo torej

Trditev 1.2. *Različna minimalna ideala evklidske algebre $\mathcal{E}$ sta pravokotna.*

Tvorimo družino vseh minimalnih idealov $\mathcal{I}_n$ evklidske algebre $\mathcal{E}$. Po prejšnji trditvi obstaja direktna vsota

$$\mathcal{J}_1 \oplus \mathcal{J}_2 \oplus \ldots \oplus \mathcal{J}_n \subset \mathcal{E}\,.$$

Ker je ortogonalni komplement te vsote ideal v $\mathcal{E}$, ki ne vsebuje nobenega minimalnega ideala, je nujno trivialen. Ker ima algebra $\mathcal{E}$ končno dimenzijo, velja

$$\mathcal{J}_1 \oplus \mathcal{J}_2 \oplus \ldots \oplus \mathcal{J}_n = \mathcal{E}\,.$$

Izrek 1.3. *Vsako evklidsko algebro $\mathcal{E}$ lahko enolično zapišemo kot ortogonalno direktno vsoto svojih minimalnih idealov.*

Dokaz: Ker ima evklidska algebra $\mathcal{E}$ končno dimenzijo, ima tudi minimalne ideala. Ker je eksistenca razcepa algebre $\mathcal{E}$ na ortogonalne minimalne ideale posledica trditev 1.1 in 1.2, zadošča dokazati le enoličnost razcepa. Naj bosta

$$\mathcal{E} = \mathcal{I}_1 \oplus \mathcal{I}_2 \oplus \ldots \oplus \mathcal{I}_n = \mathcal{J}_1 \oplus \mathcal{J}_2 \oplus \ldots \oplus \mathcal{J}_m\,,$$

različna razcepa algebre $\mathcal{E}$ na minimalne ideale. Očitno je presek $\mathcal{I}_i \cap \mathcal{J}_1$ ideal. Zaradi minimalnosti idealov $\mathcal{I}_i$ in $\mathcal{J}_1$, je presek lahko 0 ali $\mathcal{I}_i = \mathcal{J}_1$. Denimo, da je za vsak i presek enak 0. Ker je potem

$$\mathcal{I}_i \circ \mathcal{J}_1 \subset \mathcal{I}_i \cap \mathcal{J} = 0$$

od tod sledi $\mathcal{E} \circ \mathcal{J}_1 = 0$ oziroma $\mathcal{J}_1 = e \circ \mathcal{J}_1 = 0$. Za nek i je torej presek idealov $\mathcal{I}_i$ in $\mathcal{J}_1$ enak $\mathcal{I}_i = \mathcal{J}_1$. Induktivno lahko s podobnim razmislekom pokažemo trditev izreka. $\square$

Trditev 1.4. *Vsak minimalni ideal evklidske algebre $\mathcal{E}$ je enostavna algebra.*

Dokaz: Denimo, da je $\mathcal{J}_1 \oplus \mathcal{J}_2 \oplus \ldots \oplus \mathcal{J}_n$ razcep evklidske algebre $\mathcal{E}$ na minimalne ideale. Definirajmo $\mathcal{J} = \mathcal{J}_2 \oplus \ldots \oplus \mathcal{J}_n$. Naj bo $\mathcal{I}$ ideal algebre $\mathcal{J}_1$. Ker je $\mathcal{J}_1 \circ \mathcal{J} \subset \mathcal{J}_1 \cap \mathcal{J} = 0$ in $\mathcal{J} \circ \mathcal{J}_1 \subset \mathcal{J} \cap \mathcal{J}_1 = 0$, je $\mathcal{I} \circ \mathcal{J} = \mathcal{J} \circ \mathcal{I} = 0$. Od tod sledi

$$\mathcal{E} \circ \mathcal{I} = (\,\mathcal{J}_1 + \mathcal{J}\,) \circ \mathcal{I} = \mathcal{J}_1 \circ \mathcal{I} + \mathcal{J} \circ \mathcal{I} \subset \mathcal{I} + 0 = \mathcal{I}\,,$$

$$\mathcal{I} \circ \mathcal{E} = \mathcal{I} \circ (\,\mathcal{J}_1 + \mathcal{J}\,) = \mathcal{I} \circ \mathcal{J}_1 + \mathcal{I} \circ \mathcal{J} \subset \mathcal{I} + 0 = \mathcal{I}\,,$$

oziroma $\mathcal{I}$ je ideal v $\mathcal{E}$. Ker je $\mathcal{J}_1$ minimalen, sledi $\mathcal{I} \in \{\,0, \mathcal{J}_1\,\}$. To pa pomeni, da $\mathcal{J}_1$ nima netrivialnih idealov oziroma je enostavna algebra. $\square$

6.2 Enoličnost skalarnega produkta

V prejšnjem razdelku smo dokazali, da vsaka evklidska algebra razpade na minimalne ideale, ki so med seboj pravokotni. To pomeni, da se lahko pri študiju enoličnosti skalarnega produkta omejimo na primer, ko je $\mathcal{E}$ enostavna algebra. Pri tem študiju bomo potrebovali pomožno sredstvo, ki se imenuje centralizator.

Linearna preslikava $C\,:\,\mathcal{E} \longrightarrow \mathcal{E}$, se imenuje *centralizator* algebre $\mathcal{E}$, če je

$$C(\,a \circ b\,) = C(\,a\,) \circ b = a \circ C(\,b\,)\,.$$

Očitno je vsak skalarni večkratnik identitete centralizator. Poleg tega lahko s povsem elementarnim računom pokažemo, da je vsota centralizatorjev ponovno centralizator, ter da isti sklep velja tudi za kompozitum centralizatorjev. To pomeni, da lahko vsaki (neasociativni) algebri $\mathcal{E}$ priredimo (asociativni) kolobar centralizatorjev $C(\,\mathcal{E}\,)$ z enoto. V primeru, da je $\mathcal{E}$ enostavna algebra, velja še nekoliko močnejša

Trditev 2.1. *Če je $\mathcal{E}$ enostavna algebra, je $C(\,\mathcal{E}\,)$ obseg.*

Dokaz: Naj bo $C \neq 0$ centralizator in $\mathcal{K} = \{\,a \in \mathcal{E}\,;\, C(\,a\,) = 0\,\}$ jedro preslikave C. Ker velja

$$C(\,x \circ a\,) = x \circ C(\,a\,) = x \circ 0 = 0\,,$$

$$C(\,a \circ x\,) = C(\,a\,) \circ x = 0 \circ x = 0\,,$$

je $\mathcal{K}$ ideal algebre $\mathcal{E}$. Ker je $C \neq 0$, očitno možnost $\mathcal{K} = \mathcal{E}$ odpade. Ker je $\mathcal{E}$ enostavna algebra, sledi $\mathcal{K} = 0$, oziroma C je injektivna preslikava.

Naj bo $\mathcal{L} = \{ C(a); a \in \mathcal{E} \}$ množica slik preslikave C. Naj bo $x \in \mathcal{E}$ in $b \in \mathcal{L}$. Element b torej lahko zapišemo kot $b = C(a)$. Tedaj velja

$$x \circ b = x \circ C(a) = C(x \circ a) \in \mathcal{L},$$
$$b \circ x = C(a) \circ x = C(a \circ x) \in \mathcal{L},$$

od koder sledi, da je $\mathcal{L}$ ideal. Ker je $C \neq 0$, možnost $\mathcal{L} = 0$ odpade. To pa pomeni, da je C tudi surjektivna preslikava. Dokazati torej zadošča, da je tudi C^{-1} centralizator. Naj bosta $x, y \in \mathcal{E}$. Tedaj obstajata taka a in $b \in \mathcal{E}$, da velja $x = C(a)$ in $y = C(b)$. Ker velja

$$\begin{aligned} x \circ C^{-1}(y) &= C(a) \circ C^{-1}C(b) = C(a) \circ b = C(a \circ b) = \\ &= a \circ C(b) = C^{-1}(x) \circ y, \end{aligned}$$

ter

$$\begin{aligned} C^{-1}(x \circ y) &= C^{-1}(C(a) \circ y) = C^{-1}C(a \circ y) = a \circ y = \\ &= C^{-1}(x) \circ y = x \circ C^{-1}(y), \end{aligned}$$

je trditev dokazana. □

Ker ima enostavna evklidska algebra $\mathcal{E}$ končno dimenzijo, je $C(\mathcal{E})$ realen obseg končne dimenzije. Iz klasične Wedderburnove strukturne teorije asociativnih algeber s končno dimenzijo, je znano, da je tak obseg izomorfen bodisi $\mathbb{R}$ bodisi $\mathbb{C}$. Dejansko lahko drugo možnost izključimo in dobimo

Trditev 2.2 *Če je $\mathcal{E}$ enostavna evklidska algebra, je $C(\mathcal{E}) = \mathbb{R}$.*

Dokaz: Če bi veljalo, da je $C(\mathcal{E}) = \mathbb{C}$, bi obstajal centralizator T, ki bi zadoščal enačbi $T^2 = -I$. Ker ima $\mathcal{E}$ enoto, bi potem veljalo

$$\begin{aligned} \| T(1) \|^2 &= \langle T(1), T(1) \rangle = \langle 1, T(1) \circ T(1) \rangle = \langle 1, T(1 \circ T(1)) \rangle = \\ &= \langle 1, TT(1) \rangle = -\langle 1, 1 \rangle = -\| 1 \|^2, \end{aligned}$$

kar je nemogoče. □

V nadaljevanju je naš namen določiti zvezo med centralizatorji in avtomorfizmi. Omenjena zveza nam bo namreč v veliko pomoč pri dokazu trditve, da je skalarni produkt v evklidski algebri enolično določen. Zvezo podaja naslednja

Trditev 2.3. *Naj bosta $\mathcal{E}_1$ in $\mathcal{E}_2$ enostavni evklidski algebri in $\Phi : \mathcal{E}_1 \longrightarrow \mathcal{E}_2$ algebraični izomorfizem. Tedaj je $\Phi^*\Phi$ centralizator algebre $\mathcal{E}_1$.*

Opomba : *Simbol Φ^* označuje adjungirano preslikavo v smislu klasične teorije Hilbertovih prostorov.*

Dokaz: Naj bo $C = \Phi^*\Phi$. Tedaj velja

$$\begin{aligned}\langle C(a \circ b), c\rangle &= \langle \Phi(a \circ b), \Phi(c)\rangle = \langle \Phi(a) \circ \Phi(b), \Phi(c)\rangle = \\ &= \langle \Phi(a), \Phi(b) \circ \Phi(c)\rangle = \langle \Phi(a), \Phi(b \circ c)\rangle = \\ &= \langle C(a), b \circ c\rangle = \langle C(a) \circ b, c\rangle .\end{aligned}$$

Ker so a, b in c poljubni, je $C(a \circ b) = C(a) \circ b$ za vsaka a in $b \in \mathcal{E}$. Podobno dokažemo, da je $C(a \circ b) = a \circ C(b)$. □

Posledica 2.4. *Algebraični izomorfizem med enostavnima evklidskima algebrama je večkratnik izometrije.*

Dokaz: Ker je $\Phi^*\Phi = \lambda \cdot I$ za nek realen in očitno pozitiven λ, velja

$$||\,\Phi(a)\,||^2 = \langle \Phi(a), \Phi(a)\rangle = \langle \Phi^*\Phi(a), a\rangle =$$

$$= \langle \lambda\, a, a\rangle = \lambda\,||\,a\,||^2 ,$$

oziroma

$$||\,\Phi(a)\,|| = \sqrt{\lambda}\,||\,a\,|| .$$

Na koncu dokažimo še trditev, ki predstavlja bistvo tega razdelka.

Trditev 2.5. *Skalarni produkt evklidske algebre je na vsakem minimalnem idealu določen do skalarnega večkratnika natančno.*

Dokaz: Naj bosta na enostavni jordanski algebri $\mathcal{J}$ podana taka skalarna produkta $\langle\, .,.\,\rangle_1$ in $\langle\, .,.\,\rangle_2$, da je $\mathcal{J}$ evklidska algebra. Če je $\mathcal{J}_i = (\mathcal{J}, \langle\, .,.\,\rangle_i)$, je $id : \mathcal{J}_1 \longrightarrow \mathcal{J}_2$ algebraični izomorfizem. Po prejšnji trditvi je potem

$$\langle a, b\rangle_2 = \langle id(a), id(b)\rangle = \lambda\,\langle a, b\rangle_1 .$$

6.3 Klasifikacija evklidskih algeber z rangom ≤ 2

Namen razdelka je klasificirati enostavne evklidske algebre. Osnovna ideja klasifikacije temelji na *rangu evklidske algebre.* Definiramo ga kot moč največje družine neničelnih projektorjev, ki so paroma pravokotni. To pomeni, da zadoščajo pogoju

$$p_i \circ p_j = 0 \quad \text{če } i \neq j\,.$$

Tako definiran rang se v primeru matričnih algeber ujema s klasično definiranim rangom.

Očitno je vsota projektorjev največje družine $\{\, p_1, \ldots, p_n \,\}$ vedno enaka 1. V nasprotnem primeru bi namreč družina $\{\, p_1, \ldots, p_n, 1 - p_1 - \ldots - p_n \,\}$ bila še večja množica paroma pravokotnih projektorjev.

Izrek 3.1. *Enostavna evklidska algebra ranga 1 je izomorfna* $\mathbb{R}$.
Dokaz: Naj bo x neničelen element enostavne evklidske algebre $\mathcal{E}$. Po prvem spektralnem izreku 5.3.1 lahko x enolično zapišemo kot

$$x = \lambda_1 p_1 + \lambda_2 p_2 + \ldots + \lambda_n p_n\,,$$

kjer so $\lambda_1, \ldots, \lambda_n$ realna števila, $p_1, \ldots, p_n$ pa pravokotni projektorji. Ker ima pravokotna družina projektorjev moč kvečjemu enako rangu algebre $\mathcal{E}$, je $n = 1$. To pa pomeni, da je vsak element algebre $\mathcal{E}$ večkratnik projektorja. Naj bo $\{\, x_1, x_2, \ldots, x_m \,\}$ ortogonalna baza vektorskega prostora $\mathcal{E}$. Ker so vsi njeni elementi večkratniki projektorjev, obstaja ortogonalna baza prostora $\mathcal{E}$, ki je sestavljena iz projektorjev. Ker je po predpostavki moč družine projektorjev enaka 1, sledi $m = 1$, oziroma $\mathcal{E} = \mathbb{R}$. □

V drugem poglavju so bili predmet obravnave Lorentzovi stožci. Poglavje smo strnili z vložitvijo Lorentzovega stožca v algebro $\mathcal{L}or(n)$. V naslednjem izreku bomo dokazali, da so Lorentzove algebre natanko tiste enostavne evklidske algebre, ki imajo rang 2.

Izrek 3.2. *Enostavna evklidska algebra ranga 2 je izomorfna* $\mathcal{L}or(n)$.

Dokaz: Naj bo $\mathcal{E}$ enostavna evklidska algebra ranga 2. Potem je $1 = p + q$, pri čemer sta p in q neničelna ortogonalna primitivna projektorja. Razcepimo $\mathcal{E}$ glede na projektor p. Po trditvi 5.5.2 sta $\mathcal{E}_0$ in $\mathcal{E}_1$ ortogonalni podalgebri. Obe imata enoto, prva $1 - p = q$, druga pa p. Ker aksiomi $(E1)$, $(E2)$ in $(E3)$ držijo tudi za podalgebre, sta $\mathcal{E}_0$ in $\mathcal{E}_1$ evklidski algebri. Ker je rang algebre $\mathcal{E}$ enak 2, imata $\mathcal{E}_0$ in $\mathcal{E}_1$ rang 1. Po izreku 3.1 sledi, da je $\mathcal{E}_0 = \mathbb{R}\, q$

in $\mathcal{E}_1 = \mathbb{R}\,p$. Ker je $\mathcal{E}$ enostavna, je očitno $\mathcal{E} \neq \mathbb{R}\,q \oplus \mathbb{R}\,p$, od koder sledi, da je $\mathcal{E}_{\frac{1}{2}} \neq 0$.

Vzemimo enotski vektor $x \in \mathcal{E}_{\frac{1}{2}}$. Ker po trditvi 5.5.2 velja $x^2 \in \mathcal{E}_{\frac{1}{2}} \circ \mathcal{E}_{\frac{1}{2}} \subset \mathcal{E}_0 + \mathcal{E}_1$, obstajata taka skalarja α in β, da je $x^2 = \alpha p + \beta q$. Ker je

$$x = (\,p + q\,) \circ x = p \circ x + q \circ x = \tfrac{1}{2}\,x + q \circ x\,,$$

sledi, da je $q \circ x = \frac{1}{2}\,x$, oziroma $p \circ x = q \circ x = \frac{1}{2}\,x$. Ker v evklidski algebri $\mathcal{E}$ velja identiteta

$$x^2 \circ (\,p \circ x\,) = (\,x^2 \circ p\,) \circ x\,,$$

sledi

$$x^2 \circ (\,p \circ x\,) = (\,\alpha p + \beta q\,) \circ (\,p \circ x\,) = (\,\alpha p \circ p + \beta q \circ p\,) \circ x \;=$$

$$=\; (\,\alpha p + 0\,) \circ x = \alpha p \circ x = \tfrac{\alpha}{2}\,x\,.$$

Ker po drugi strani velja

$$(\,\alpha p + \beta q\,) \circ (\,p \circ x\,) = (\,\alpha p + \beta q\,) \circ \tfrac{1}{2}\,x = \tfrac{\alpha}{2}\,p \circ x + \tfrac{\beta}{2}\,p \circ x = \tfrac{\alpha}{2} + \tfrac{\beta}{2}\,,$$

sledi identiteta

$$\tfrac{\alpha}{4}\,x + \tfrac{\beta}{4}\,x = \tfrac{\alpha}{2}\,x\,,$$

od koder sledi $\alpha = \beta$. Ker je $x^2 = \alpha p + \beta q = \alpha\,(\,p + q\,) = \alpha$, velja

$$\alpha\,||\,p\,||^2 = \alpha\,\langle\,p,p\,\rangle = \langle\,\alpha p,p\,\rangle = \langle\,x^2,p^2\,\rangle = \langle\,x^2,p\,\rangle =$$

$$= \langle\,x,p\circ x\,\rangle = \langle\,x,q\circ x\,\rangle = \langle\,x^2,q\,\rangle = \langle\,x^2,q^2\,\rangle = \alpha\,\langle\,q,q\,\rangle = \alpha\,||\,q\,||^2\,,$$

oziroma $||\,p\,|| = ||\,q\,||$. Če algebro $\mathcal{E}$ renormiramo tako, da je $||\,p\,|| = ||\,q\,|| = \frac{1}{\sqrt{2}}$, sta enotska vektorja 1 in $p - q$. Velja namreč

$$\langle\,1,p - q\,\rangle = \langle\,p + q,p - q\,\rangle = ||\,p\,||^2 - \langle\,p,q\,\rangle + \langle\,p,q\,\rangle - ||\,q\,||^2 = 0\,,$$

$$\langle\,p - q,p - q\,\rangle = ||\,p\,||^2 - \langle\,p,q\,\rangle - \langle\,q,p\,\rangle + ||\,q\,||^2 = \tfrac{1}{2} + \tfrac{1}{2} = 1\,.$$

Vzemimo poljuben $x \in \mathcal{E}_{\frac{1}{2}}$ in $y = \alpha\,(\,p - q\,) \in \mathbb{R}\,(\,p - q\,)$. Ker veljajo identitete

$$\langle\,1,p - q\,\rangle = \langle\,p + q,p - q\,\rangle = |\,p\,|^2 - p \circ q + q \circ p - |\,q\,|^2 = 0\,,$$

$$\begin{aligned}\langle 1, x\rangle &= \langle p+q, x\rangle = \langle p, x\rangle + \langle q, x\rangle = \langle p^2, x\rangle + \langle q^2, x\rangle = \\ &= \langle p, p\circ x\rangle + \langle q, q\circ x\rangle = \tfrac{1}{2}\langle p, x\rangle + \tfrac{1}{2}\langle q, x\rangle = \\ &= \tfrac{1}{2}\langle 1, p\circ x\rangle + \tfrac{1}{2}\langle 1, q\circ x\rangle = \tfrac{1}{4}\langle 1, x\rangle + \tfrac{1}{4}\langle 1, x\rangle = \\ &= \tfrac{1}{2}\langle 1, x\rangle \Longrightarrow \langle 1, x\rangle = 0\end{aligned}$$

in

$$\langle x, \alpha(p-q)\rangle = \langle x, \alpha p - \alpha q\rangle = \langle x, \alpha p\rangle - \langle x, \alpha q\rangle =$$

$$= \langle p\circ x, \alpha\rangle - \langle q\circ x, \alpha\rangle = \langle p\circ x, \alpha\rangle - \langle p\circ x, \alpha\rangle = 0\,,$$

sta podprostora $\mathcal{E}_{\frac{1}{2}}$ in $\mathbb{R}(p-q)$ pravokotna na enoto in pravokotna tudi med seboj. Če označimo z $\mathcal{F} = \{1\}^{\perp}$, sledi, da je $\mathcal{F} = \mathcal{E}_{\frac{1}{2}} \oplus \mathbb{R}(p-q)$. Zapišimo elemente algebre $\mathcal{E}$ v obliki $\alpha + a$, kjer je α večkratnik enote in $a \in \mathcal{F}$ ter izračunajmo vrednost produkta $(\alpha + a)\circ(\beta + b)$. V smislu zgornjega razcepa lahko a in b zapišemo v obliki $a = c + \gamma(p-q)$ in $b = d + \delta(p-q)$, pri čemer sta $c, d \in \mathcal{E}_{\frac{1}{2}}$, $\gamma, \delta \in \mathbb{R}$. Ker veljajo identitete

$$\langle c, c\rangle = \langle 1, c\circ c\rangle = \langle 1, c^2\rangle = \langle 1, \rho\rangle = \rho = c^2$$

in podobno $d^2 = \langle d, d\rangle$ in $(c+d)^2 = \langle c+d, c+d\rangle$, sledi $c\circ d = \langle c, d\rangle$. Veljata namreč identiteti

$$(c+d)\circ(c+d) = c\circ c + c\circ d + d\circ c + d\circ d = \langle c, c\rangle + 2\,c\circ d + \langle d, d\rangle$$

in

$$(c+d)\circ(c+d) = \langle c+d, c+d\rangle = \langle c, c\rangle + 2\langle c, d\rangle + \langle d, d\rangle\,.$$

Ker sta $c, d \in \mathcal{E}_{\frac{1}{2}}(p) \cap \mathcal{E}_{\frac{1}{2}}(q)$, velja $p\circ c = q\circ c = \frac{1}{2}c$ in $p\circ d = q\circ d = \frac{1}{2}d$. Od tod sledi

$$a\circ b = c\circ d + \delta\, c\circ(p-q) + \gamma\, d\circ(p-q) + \gamma\delta(p-q)^2 =$$

$$= \langle c, d\rangle + \gamma\delta(p-q)^2 = \langle c, d\rangle + \gamma\delta(p^2 - p\circ q - q\circ p + q^2) =$$

$$= \langle c, d\rangle + \gamma\delta(p+q) = \langle c, d\rangle + \gamma\delta = \langle a, b\rangle\,.$$

Množenje v algebri $\mathcal{E}$ je torej podano s predpisom

$$(\alpha + a)\circ(\beta + b) = \alpha\beta + \alpha b + \beta a + a\circ b = \alpha\beta + \langle a, b\rangle + \alpha b + \beta a\,,$$

kar je identično predpisu, s katerim je podano množenje v Lorentzovi algebri. □

Nadaljna klasifikacija enostavnih evklidskih algeber ranga ≥ 3 temelji na evklidskih Hurwitzovih algebrah in njim prirejenih algebrah simetričnih matrik. Pred končno klasifikacijo evklidskih algeber si torej oglejmo nekatere lastnosti algeber simetričnih matrik.

6.4 Algebre $\mathcal{H}er(m, A)$

Naj bo $\mathcal{A}$ evklidska Hurwitzova algebra. V petem razdelku prejšnjega poglavja smo dokazali, da je $\mathcal{A}$ izomorfna eni izmed algeber: $\mathbb{R}$, $\mathbb{C}$, $\mathbb{H}$ ali $\mathbb{O}$. V nadaljevanju bomo z $\mathcal{M}(m, \mathcal{A})$ označevali algebro matrik dimenzije $m \times m$ s členi iz $\mathcal{A}$. Očitno je zaradi asociativnosti algeber $\mathbb{R}$, $\mathbb{C}$ in $\mathbb{H}$, asociativna tudi pripadajoča algebra $\mathcal{M}(m, \mathcal{A})$.

Trditev 4.1. *Za poljubne a, b in $c \in \mathcal{M}(m, \mathcal{A})$ veljata identiteti*

$$(i)\ \ Re\,Sl\,(a \cdot b) = Re\,Sl\,(b \cdot a)\,,$$
$$(ii)\ \ Re\,Sl\,((a \cdot b) \cdot c) = Re\,Sl\,(a \cdot (b \cdot c))\,,$$

kjer $Re\,Sl\,(a)$ pomeni realni del sledi matrike a.

Dokaz: Če v trditvi 5.6.3 operacijo $\circ$ obravnavamo kot običajno množenje matrik, je identiteta (i) direktna posledica identitete (iii) omenjene trditve. Za poljubna a in $b \in \mathcal{A}$ namreč velja

$$Re\,(a \cdot b) = Re\,(b \cdot a)\,.$$

Za poljubne a, b in $c \in \mathcal{A}$, z upoštevanjem definicije realnega dela elementa, velja

$$Re\,((a \cdot b) \cdot c) = \langle (a \cdot b) \cdot c, 1 \rangle = \langle a \cdot b, \overline{c} \rangle = \langle b, \overline{a} \cdot \overline{c} \rangle =$$

$$= \langle b \cdot c, \overline{a} \rangle = \langle a \cdot (b \cdot c), 1 \rangle = Re\,(a \cdot (b \cdot c))\,,$$

od koder sledi identiteta (ii). □

V nadaljevanju označimo z $\mathcal{H}er(m, \mathcal{A})$ realni vektorski prostor hermitskih matrik dimenzije $m \times m$ s členi iz $\mathcal{A}$. Za element a prostora $\mathcal{H}er(m, \mathcal{A})$ potem velja $a^T = \overline{a}$, oziroma

$$a_{ij} = \overline{a_{ji}}\,.$$

Ker je kvadratna forma

$$Sl\,(a^2) = \sum_{i,j} a_{ij}\cdot a_{ji} = \sum_{i,j} |\, a_{ij}\,|^2\,,$$

pozitivno definitna, lahko na prostoru $\mathcal{H}er(m, \mathcal{A})$ definiramo skalarni produkt z naslednjim predpisom

$$\langle\, a, b\,\rangle = Re\,Sl\,(\, a\cdot b\,)\,.$$

Prostor $\mathcal{H}er(m, \mathcal{A})$, opremljen z zgornjim skalarnim produktom tako postane evklidski vektorski prostor.

Če na prostoru $\mathcal{H}er(m, \mathcal{A})$ definiramo jordanski produkt s predpisom

$$a \circ b = \tfrac{1}{2}\,(\, a\cdot b + b\cdot a\,)\,,$$

lahko zgoraj definiran skalarni produkt zapišemo v obliki

$$\langle\, a, b\,\rangle = Re\,Sl\,(\, a \circ b\,)\,.$$

Če upoštevamo, da je v primeru $\mathcal{A} = \mathbb{R}, \mathbb{C}$ ali $\mathbb{H}$, algebra $\mathcal{M}(m, \mathcal{A})$ asociativna, potem veljata naslednji identiteti

$$a \circ b = \tfrac{1}{2}\,(\, a\cdot b + b\cdot a\,) = \tfrac{1}{2}\,(\, b\cdot a + a\cdot b\,) = b \circ a$$

in

$$\begin{aligned} a \circ (\, a^2 \circ b\,) &= \tfrac{1}{2}\, a^2 \circ (\, a^2\cdot b + b\cdot a^2\,) = \\ &= \tfrac{1}{4}\,(\, a\cdot(\, a^2\cdot b\,) + (\, a^2\cdot b\,)\cdot a + a\cdot(\, b\cdot a^2\,) + (\, b\cdot a^2\,)\cdot a\,) = \\ &= \tfrac{1}{4}\,(\, a^2\cdot(\, a\cdot b\,) + (\, a\cdot b\,)\cdot a^2 + a^2\cdot(\, b\cdot a\,) + (\, b\cdot a\,)\cdot a^2\,) = \\ &= \tfrac{1}{2}\, a^2 \circ (\, a\cdot b + b\cdot a\,) = a^2 \circ (\, a \circ b\,)\,. \end{aligned}$$

Algebra $\mathcal{H}er(m, \mathcal{A})$, $\mathcal{A} = \{\, \mathbb{R}, \mathbb{C}, \mathbb{H}\,\}$, opremljena z jordanskim produktom $\circ$ je torej jordanska algebra.

Pokažimo, da je $\mathcal{H}er(m, \mathcal{A})$ celo evklidska jordanska algebra. Dokazati zadošča asociativnost skalarnega produkta oziroma veljavnost naslednje identitete

$$\langle\, a \circ b, c\,\rangle = \langle\, a, b \circ c\,\rangle\,.$$

Po definiciji skalarnega produkta velja

$$\langle\, a\circ b, c\,\rangle = Re\,Sl\,(\,(a\circ b\,)\cdot c\,) = \tfrac{1}{2}\,Re\,Sl\,(\,(\, a\cdot b\,)\cdot c\,) + \tfrac{1}{2}\,Re\,Sl\,(\,(\, b\cdot a\,)\cdot c\,)\,.$$

Od tod, z upoštevanjem trditve 3.1 sledi

$$\begin{aligned}\langle\, a\circ b, c\,\rangle &= \tfrac{1}{2}\, Re\, Sl\,(\, a\cdot(\, b\cdot c\,)\,) + \tfrac{1}{2}\, Re\, Sl\,(\, a\cdot(\, c\cdot b\,)\,) \\ &= Re\, Sl\,(\, a\cdot(\, b\circ c\,)\,) = \langle\, a, b\circ c\,\rangle\,,\end{aligned}$$

oziroma

$$\langle\, a\circ b, c\,\rangle = \langle\, a, b\circ c\,\rangle\,.$$

V nadaljevanju si nekoliko podrobneje oglejmo algebro $\mathcal{H}er(\,3,\mathbb{O}\,)$, dimenzije 27, ki jo imenujemo *Albertova algebra.*

Trditev 4.2. *Za vsak element $a\in\mathcal{H}er(\,m,\mathbb{O}\,)$ velja*

$$a\cdot(a^2)-(a^2)\cdot a=\lambda I\,,$$

kjer je $\lambda\in\mathbb{O}$.

Dokaz: Naj bo $b=a\cdot(\,a^2\,)-(\,a^2\,)\cdot a$. Potem za b_{ij} velja

$$b_{ij}=\sum_k a_{ik}(\,\sum_l a_{kl}a_{lj}\,)-\sum_l\,(\,\sum_k a_{ik}a_{kl}\,)a_{lj}=\sum_{k,l}\,[\,a_{ik},a_{kl},a_{lj}\,]\,.$$

Asociator $[\,\alpha,\beta,\gamma\,]$, elementov algebre $\mathbb{O}$ je enak nič, če je eden izmed elementov realen ali pa sta dva med seboj enaka. To pomeni, da je asociator različen od nič le v primeru, ko so indeksi elementov asociatorja, upoštevajoč tudi njihove permutacije, različni. Od tod torej sledi, da je za $i\neq j$ element $b_{ij}=0$, oziroma velja

$$\begin{aligned}b_{11}&=[\,a_{12},a_{23},a_{31}\,]+[\,a_{13},a_{32},a_{21}\,]\,,\\ b_{22}&=[\,a_{21},a_{13},a_{32}\,]+[\,a_{23},a_{31},a_{12}\,]\,,\\ b_{33}&=[\,a_{31},a_{12},a_{23}\,]+[\,a_{32},a_{21},a_{13}\,]\,.\end{aligned}$$

Ker je asociator alternirajoča funkcija, sledi

$$b_{11}=b_{22}=b_{33}\,.$$

Trditev 4.3. *Naj bo a taka antihermitska matrika s členi iz $\mathbb{O}$, da velja $Sl\,(a)=0$. Potem je linearna preslikava*

$$D\,:\,\mathcal{M}(\,m,\mathcal{A}\,)\longrightarrow\mathcal{M}(\,m,\mathcal{A}\,)\,,$$

podana s predpisom

$$Dx=a\cdot x-x\cdot a\,,$$

odvajanje algebre $\mathcal{H}er(\,m,\mathcal{A}\,)$.

Dokaz: Ker po trditvi 4.2 za vsak $x\in\mathcal{H}er(\,m,\mathbb{O}\,)$ velja

$$x\cdot(x^2) - (x^2)\cdot x = \lambda I\,,$$

sledi

$$\begin{aligned} Sl\,(\,a\cdot(\,x\cdot(\,x^2)\,)\,) - Sl\,(\,a\cdot(\,(\,x^2)\cdot x\,)\,) &= Sl\,(\,a\,\lambda\, I\,) = Sl\,(\,a\,\lambda\,) \\ &= \lambda^{dim\,\mathcal{H}er(m,\mathbb{O})}\,Sl\,(a) = 0\,. \end{aligned}$$

Od tod, z upoštevanjem trditve 4.1, dobimo

$$Re\,Sl\,(\,(\,a\cdot x\,)\cdot x^2\,) = Re\,Sl\,(\,(\,x\cdot a\,)\cdot x^2\,)\,.$$

Od tod sledi

$$\begin{aligned} 0 &= \tfrac{1}{2}\,Re\,Sl\,(\,(\,a\cdot x\,)\cdot x^2) - \tfrac{1}{2}\,Re\,Sl\,(\,(\,x\cdot a\,)\cdot x^2) = \\ &= Re\,Sl\,(\,\tfrac{1}{2}\,(\,a\cdot x\,)\cdot x^2 + \tfrac{1}{2}\,x^2\cdot(\,a\cdot x\,) - \tfrac{1}{2}\,x^2\cdot(\,a\cdot x\,) - \tfrac{1}{2}\,(\,a\cdot x\,)\cdot x^2\,) = \\ &= Re\,Sl\,(\,(a\cdot x\circ x^2\,) - (\,x\cdot a\circ x^2\,)\,) = \\ &= Re\,Sl\,(\,(\,a\cdot x - x\cdot a\,)\circ x^2\,)\,, \end{aligned}$$

oziroma

$$\langle\, Dx, x^2\rangle = 0\,.$$

Če v dobljeni identiteti najprej element x nadomestimo z $x+y$, nato pa še z $x-y$, dobimo identiteti

$$2\,\langle\, Dx, x\circ y\,\rangle + 2\,\langle\, Dy, x\circ y\,\rangle + \langle\, Dx, y^2\rangle + \langle\, Dy, x^2\rangle = 0\,,$$

$$-2\,\langle\, Dx, x\circ y\,\rangle + 2\,\langle\, Dy, x\circ y\,\rangle + \langle\, Dx, y^2\rangle - \langle\, Dy, x^2\rangle = 0\,.$$

Če dobljeni identiteti odštejemo, dobimo

$$2\,\langle\, Dy, x\circ y\,\rangle = -\,\langle\, Dx, y^2\rangle\,.$$

Podobno z zamenjavo elementa x z elementom $x+z$, dobimo identiteto

$$2\,\langle\, Dz, x\circ z\,\rangle = -\,\langle\, Dx, z^2\rangle\,.$$

Če v identiteti

$$2\,\langle\, Dy, x\circ y\,\rangle + \,\langle\, Dx, y^2\rangle = 0\,,$$

nadomestimo element y z $y+z$, dobimo

$$2\,\langle\, Dy, x\circ y\,\rangle + 2\,\langle\, Dy, x\circ z\,\rangle + 2\,\langle\, Dz, x\circ y\,\rangle + 2\,\langle\, Dz, x\circ z\,\rangle +$$

$$+\,\langle\, Dx, y^2\rangle + 2\,\langle\, Dx, y\circ z\,\rangle + \langle\, Dx, z^2\rangle = 0\,,$$

od koder z upoštevanjem zgornjih identiteti, sledi

$$\langle\, Dx, y \circ z \,\rangle + \langle\, Dy, z \circ x \,\rangle + \langle\, Dz, x \circ y \,\rangle = 0\,.$$

Z uporabo zgornje identitete na elementu $z = 1$, dobimo izraz

$$\langle\, Dx, y \,\rangle + \langle\, Dy, x \,\rangle = 0\,,$$

ki dokazuje antisimetričnost operatorja D. Ob upoštevanju asociativnosti skalarnega produkta sledi

$$\langle\, Dx \circ y, z \,\rangle + \langle\, Dy \circ x, z \,\rangle - \langle\, z, D(\, x \circ y \,) \,\rangle = 0\,,$$

oziroma

$$D(\, x \circ y \,) = Dx \circ y + x \circ Dy\,.$$

To pa pomeni, da je D odvajanje na algebri $\mathcal{H}er(\, m, \mathbb{O})$. □

Izrek 4.4. *(Freudenthalov) Naj bo H grupa avtomorfizmov algebre $\mathcal{H}er(\,3, \mathbb{O}\,)$, ki ohranja sled. Za poljuben $a \in \mathcal{H}er(\,3, \mathbb{O}\,)$ obstaja tak $h \in H$, da je $h \cdot a$ diagonalna matrika.*

Dokaz: Naj bo a antihermitska matrika s členi iz $\mathbb{O}$, za katero velja $Sl\,(a) = 0$. Po trditvi 4.3 je preslikava D, podana s predpisom $Dx = a{\cdot}x - x{\cdot}a$, odvajanje algebre $\mathcal{H}er(\,3, \mathbb{O}\,)$. Ker je H kompaktna grupa, za vsak $x \in \mathcal{H}er(\,3, \mathbb{O}\,)$ velja, da je orbita $H{\cdot}x$ kompaktna [Faraut, 1994, str. 90]. Denimo, da je maksimum funkcije φ, definirane na orbiti $H \cdot x$ in podane s predpisom

$$\varphi(z) = \sum_{i=1}^{3} z_{ii}^2\,,$$

dosežen v točki $y \in \mathcal{H}er(\,3, \mathbb{O}\,)$. Pokažimo, da je potem y diagonalna matrika. Če je torej D odvajanje algebre $\mathcal{H}er(\,3, \mathbb{O}\,)$, je $\exp(\,tD\,)$, $t \in \mathbb{R}$, enoparametrična podgrupa grupe H. Ker je $Sl\,(\,Dx\,) = 0$, za vsak x, namreč velja $Sl\,(\,\exp(\,tD\,)\,x\,) = Sl\,(x) + t\,Sl\,(Dx) + \frac{t^2}{2}\,Sl(D(Dx)) + \ldots = Sl(x)$. Če definiramo

$$f(t) = \varphi(\,\exp(\,tD\,)\,y\,)\,,$$

je $f(0) = \varphi(\,exp(0)\,y\,) = \varphi(\,y\,)$. Ker je y maksimum funkcije φ, sledi $f(t) \leq f(0)$, za vsak $t \in \mathbb{R}$. Če torej zapišemo

$$f(t) = \sum_{i=1}^{3} (\,\exp(\,tD\,)\,y_{ii}\,)^2\,,$$

po odvajanju dobimo

$$f'(t) = 2\sum_{i=1}^{3} (\exp(tD)\, y_{ii})\, D\, (\exp(tD)\, y_{ii})\,.$$

Od tod sledi

$$f'(0) = 2\sum_{i=1}^{3} y_{ii}\, D\, y_{ii} = 2\sum_{i=1}^{3} y_{ii}\, (D\, y)_{ii}\,.$$

Če upoštevamo, da je

$$\begin{aligned}(D\, y)_{ii} &= \sum_{j=1}^{3} a_{ij}y_{ji} - \sum_{j=1}^{3} y_{ij}a_{ji} = \sum_{j=1}^{3} a_{ij}y_{ji} + \sum_{j=1}^{3} y_{ij}(-a_{ji}) \\ &= \sum_{j=1}^{3} a_{ij}y_{ji} + \sum_{j=1}^{3} y_{ij}a_{ij}^{*} = \sum_{j=1}^{3} a_{ij}y_{ij}^{*} + \sum_{j=1}^{3} y_{ij}a_{ij}^{*} \\ &= 2\sum_{j=1}^{3} \langle a_{ij}, y_{ij} \rangle\end{aligned}$$

in velja $f'(0) = 0$, dobimo

$$\begin{aligned}0 &= 2\sum_{i=1}^{3} y_{ii}\, (D\, y)_{ii} = 4\sum_{i=1}^{3} y_{ii} \sum_{j=1}^{3} \langle a_{ij}, y_{ij} \rangle = \\ &= 4\sum_{i<j} \langle a_{ij}, y_{ij} \rangle\, (y_{ii} - y_{jj})\,.\end{aligned}$$

Ker identiteta velja za poljubno antihermitsko matriko a, sledi, da je $y_{ij} = 0$ ali $y_{ii} = y_{jj}$, za poljuben par indeksov i in j. Pokažimo, da za $i \neq j$ velja $y_{ij} = 0$. Denimo, da obstaja tak par indeksov i in j, da je $y_{ij} \neq 0$. Potem po zgornji identiteti velja $y_{ii} = y_{jj}$ in obstaja tak $\beta \in \mathbb{O}$, da velja $\langle \beta, y_{ij} \rangle \neq 0$. Predpostavimo, da je $i < j$. Naj bo a taka antihermitska matrika, da je $a_{ij} = \beta$ in $a_{kl} = 0$, za $\{k, l\} \neq \{i, j\}$. Če odvodu D priredimo funkcijo

$$y(t) = \exp(tD)\, y\,,$$

za $k \neq i, j$, dobimo

$$\tfrac{d}{dt}\, y_{kk}(t) = 0\,.$$

Od tod sledi, da je $y_{kk}(t) = y_{kk}(0) = y_{kk}$. Ker $\exp(\,tD\,)$ ohranja sled, sledi

$$y_{ii}(t) + y_{jj}(t) = y_{ii} + y_{jj} = 2y_{ii}$$

in od tod

$$f(t) = y_{ii}(t)^2 + y_{jj}(t)^2 + y_{kk}^2\,.$$

Če upoštevamo, da je $y_{kk}^2 = f(0) - y_{ii}^2 - y_{jj}^2 = f(0) - 2y_{ii}^2$ in velja $y_{jj}(t)^2 = 4y_{ii}^2 - 4y_{ii}\,y_{ii}(t) + y_{ii}(t)^2$, sledi

$$f(t) = f(0)+y_{ii}(t)^2+(\,2y_{ii}-y_{ii}(t)\,)^2-2y_{ii}^2 = f(0)+2\,(\,y_{ii}(t)-y_{ii}\,)^2\,.$$

Ker je $f(t) \leq f(0)$, sledi $y_{ii}(t) = y_{ii}$, oziroma

$$0 = \tfrac{d}{dt}\,y_{ii}(0) = 2\,\langle\, a_{ij}, y_{ij}\,\rangle = 2\,\langle\, \beta, y_{ij}\,\rangle\,,$$

kar je protislovje s predpostavko, da je $\langle\, \beta, y_{ij}\,\rangle \neq 0$. To pa pomeni, da je $y_{ij} = 0$ oziroma, da je y diagonalna matrika. □

Posledica 4.5. *Algebra $\mathcal{H}er(\,3,\mathbb{O}\,)$ je evklidska jordanska algebra ranga 3.*

Dokaz: Da je $\mathcal{H}er(\,3,\mathbb{O}\,)$ jordanska algebra zadošča pokazati, da za poljuben $a \in \mathcal{H}er(\,3,\mathbb{O}\,)$, operatorja $L(a)$ in $L(a^2)$ komutirata. Po trditvi 4.4 lahko matriko a obravnavamo kot diagonalno. Ker je kvadrat diagonalne matrike diagonalna matrika, diagonalne matrike pa komutirajo, sledi, da je algebra $\mathcal{H}er(\,3,\mathbb{O}\,)$, opremljena z jordanskim produktom $a \circ b = \frac{1}{2}\,(\,a{\cdot}b + b{\cdot}a\,)$, jordanska. Če upoštevamo, da je $\langle\, a, b\,\rangle = \mathcal{R}e\,Sl\,(\,a \circ b\,)$ in velja $\langle\, a \circ b, c\,\rangle = \langle\, a, b \circ c\,\rangle$, je $\mathcal{H}er(\,3,\mathbb{O}\,)$ tudi evklidska. Ker matrike

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}, \quad \begin{bmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix}, \quad \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix},$$

tvorijo jordanski sistem, je očitno $\mathcal{H}er(\,3,\mathbb{O}\,)$ ranga 3. □

6.5 Klasifikacija evklidskih algeber z rangom ≥ 3

V drugem razdelku smo dokazali, da so enostavne evklidske algebre ranga 1 izomorfne $\mathbb{R}$, enostavne evklidske algebre ranga 2 pa pripadojočim Lorentzovim algebram. V nadaljevanju bomo klasificirali še enostavne evklidske algebre ranga ≥ 3.

Naj bo $\mathcal{E}$ enostavna evklidska algebra ranga $r \geq 3$. Njeno Pierceovo dekompozicijo, glede na sistem pravokotnih projektorjev $\{ p_1, \ldots, p_r \}$, zapišimo v obliki

$$\mathcal{E} = \bigoplus_{i \leq j} \mathcal{E}_{ij} \, .$$

Trditev 5.1. *Za poljubne $a, c \in \mathcal{E}_{ij}$ in $b \in \mathcal{E}_{jk}$, pri čemer so i, j in k različni, velja naslednja identiteta*

$$L(c) \, (\, a \circ b \,) + L(a) \, (\, c \circ b \,) = \tfrac{1}{4} \, \langle \, a, c \, \rangle \, b \, .$$

Dokaz: Če v trditvi 5.5.8 nadomestimo element $a \in \mathcal{E}_{ij}$ z elementom $a + c \in \mathcal{E}_{ij}$, dobimo

$$L(a+c) \, (\, (\, a + c \,) \circ b \,) = \tfrac{1}{8} \, || \, a + c \, ||^2 b \, .$$

oziroma

$$L(a+c) \, (\, a \circ b \,) + L(a+c) \, (\, c \circ b \,) =$$
$$= \tfrac{1}{8} \, (\, || \, a \, ||^2 b + \langle \, a, c \, \rangle \, b + \langle \, c, a \, \rangle \, b + || \, c \, ||^2 b \,) \, .$$

Ker je $\langle \, a, c \, \rangle = \langle \, c, a \, \rangle$, sledi

$$L(a) \, (\, a \circ b \,) + L(c) \, (\, a \circ b \,) + L(a) \, (\, c \circ b \,) + L(c) \, (\, c \circ b \,) =$$
$$= \tfrac{1}{8} \, (\, || \, a \, ||^2 b + 2 \, \langle \, a, c \, \rangle \, b + || \, c \, ||^2 b \,) \, ,$$

in ob upoštevanju identitet $L(a) \, (\, a \circ b \,) = \frac{1}{8} \, || \, a \, ||^2 b$ ter $L(c) \, (\, c \circ b \,) = \frac{1}{8} \, || \, c \, ||^2 b$

$$L(c) \, (\, a \circ b \,) + L(a) \, (\, c \circ b \,) = \tfrac{1}{4} \, \langle \, a, c \, \rangle \, b \, .$$

Trditev 5.2. *Naj bodo $r \geq 4$ in i, j, k ter l paroma različni. Za $a \in \mathcal{E}_{ij}$, $b \in \mathcal{E}_{jk}$ in $c \in \mathcal{E}_{kl}$ velja naslednja identiteta*

$$a \circ (\, b \circ c \,) = (\, a \circ b \,) \circ c \, .$$

Dokaz: Naj bo $p = p_i + p_j + p_k$. Potem veljajo naslednje identitete

$$P(\, p \,) \, a = a \, , \;\; P(\, p \,) \, b = b \, , \;\; P(\, p \,) \, c = 0 \, .$$

Če namreč upoštevamo, da je

$$P(\, p \,) \, a = 2 \, L(\, p \,)^2 a - L(\, p^2) \, a \, ,$$

in velja

$$L(\,p_i+p_j+p_k\,)\,a = p_i\circ a + p_j\circ a + p_k\circ a = \tfrac{1}{2}\,a + \tfrac{1}{2}\,a = a\,,$$

sledi

$$P(\,p\,)\,a = 2\,L(\,p_i+p_j+p_k\,)^2 a - L(\,p_i+p_j+p_k\,)\,a =$$

$$= 2\,L(\,p_i+p_j+p_k\,)\,a - a = 2\,a - a = a\,.$$

S podobnim sklepom dokažemo tudi preostali identiteti. Če upoštevamo, v razdelku o Mc Crimmonovem operatorju dokazano identiteto

$$P(\,a,b\,)\,c = L(\,a\,)\,L(\,b\,)\,c + L(\,b\,)\,L(\,a\,)\,c - L(\,a\circ b\,)\,c$$

in trditev 5.5.7.(ii) , po kateri za $a\in\mathcal{E}_{ij}$ in $c\in\mathcal{E}_{kl}$ velja $L(\,a\,)\,c = 0$, sledi

$$L(\,a\,)\,L(\,b\,)\,c = L(\,a\circ b\,)\,c\,,$$

oziroma

$$a\circ(\,b\circ c\,) = (\,a\circ b\,)\circ c\,.$$

Trditev 5.3. *Obstajajo taki elementi $e_{ij}\in\mathcal{E}_{ij}$, $i\neq j$, da velja*

$$(\,i\,)\;\; e_{ij}^2 = 4\,(\,p_i+p_j\,)\,,$$
$$(\,ii\,)\; e_{ij}\circ e_{jk} = e_{ik}\,,$$

pri čemer so i, j in k različni.

Dokaz: Če upoštevamo, da je po trditvi 5.5.5

$$e_{ij}^2 = \tfrac{1}{2}\,||\,e_{ij}\,||^2\,(\,p_i+p_j\,)\,,$$

lahko identiteto $e_{ij}^2 = 4\,(\,p_i+p_j\,)$ zapišemo v obliki

$$||\,e_{ij}\,||^2 = 8\,.$$

Naj bo e_{1i}, $i=1,\ldots,r$, tak element $\mathcal{E}_{1i}$, da velja $||\,e_{1i}\,||^2 = 8$. Če za $i,j\geq 2$ in $i\neq j$ definiramo

$$e_{ij} = e_{1i}\circ e_{1j}\,,$$

je očitno $e_{ij} = e_{ji}$. Velja namreč

$$e_{ij} = e_{1i}\circ e_{1j} = e_{1j}\circ e_{1i} = e_{ji}\,.$$

Po trditvi 5.5.8 je potem

$$\| e_{ij} \|^2 = \| e_{1i} \circ e_{1j} \|^2 = \tfrac{1}{8} \| e_{1i} \|^2 \cdot \| e_{1j} \|^2 ,$$

od koder sledi (i).

Za dokaz identitete (ii) privzemimo najprej, da je $i = 1$. Potem po zgornji definiciji velja

$$e_{1j} \circ e_{jk} = e_{1j} \circ (e_{ij} \circ e_{1k}) ,$$

od koder, po trditvi 5.5.8, sledi

$$e_{1j} \circ e_{jk} = \tfrac{1}{8} \| e_{1j} \|^2 \cdot e_{1k} = e_{1k} .$$

Privzemimo sedaj, da je $r \geq 4$ in so i, j in k vsi različni ter večji od 1. Če upoštevamo zgornjo definicijo, dobimo

$$e_{ij} \circ e_{jk} = (e_{1i} \circ e_{1j}) \circ e_{jk} ,$$

od koder, z uporabo trditve 5.2, sledi

$$(e_{1i} \circ e_{1j}) \circ e_{jk} = e_{1i} \circ (e_{1j} \circ e_{jk}) .$$

Ker je po zgoraj dokazanem $e_{1j} \circ e_{jk} = e_{1k}$, sledi

$$e_{ij} \circ e_{jk} = e_{ik} .$$

Ker v primeru $i \neq j$, Pierceov podprostor $\mathcal{E}_{ij}$ ni podalgebra evklidske algebre $\mathcal{E}$, je na $\mathcal{E}_{ij}$ potrebno definirati produkt, za katerega bo $\mathcal{E}_{ij}$ algebra. Na prostoru $\mathcal{E}_{ij}$ torej definirajmo produkt z naslednjim predpisom

$$a * b = (e_{ik} \circ a) \circ (e_{kj} \circ b) .$$

Ker je po trditvi 5.5.7, produkt $e_{ik} \circ a \in \mathcal{E}_{ik} \circ \mathcal{E}_{ij} \subset \mathcal{E}_{jk}$ in $e_{kj} \circ b \in \mathcal{E}_{kj} \circ \mathcal{E}_{ij} \subset \mathcal{E}_{ik}$, je produkt $a * b \in \mathcal{E}_{jk} \circ \mathcal{E}_{ik} \subset \mathcal{E}_{ij}$. To pomeni, da je zgornji produkt dobro definiran.

Prostor $\mathcal{E}_{ij}$, opremljen z operacijo $*$ je torej algebra. Ker za $a \in \mathcal{E}_{ij}$, po trditvah 5.1 in 5.3 velja

$$e_{ij} * a = (e_{ik} \circ e_{ij}) \circ (e_{kj} \circ a) = e_{jk} \circ (e_{kj} \circ a) = \tfrac{1}{8} \| e_{jk} \|^2 a = a ,$$

in

$$a * e_{ij} = (e_{ik} \circ a) \circ (e_{kj} \circ e_{ij}) = (e_{ik} \circ a) \circ e_{ik} = \tfrac{1}{8} \| e_{ik} \|^2 a = a ,$$

je element e_{ij} enota algebre. Dobljeno algebro z enoto označimo z $\mathcal{A}_{ij}$.

Za $a, b \in \mathcal{E}_{ij}$, je norma produkta $a * b$ podana s predpisom

$$||\, a * b \,||^2 = \tfrac{1}{8}\, ||\, a \,||^2 \cdot ||\, b \,||^2 \,.$$

Če jo renormiramo z izrazom

$$N(\, a \,)^2 = \tfrac{1}{8}\, ||\, a \,||^2 \,,$$

dobi obliko

$$N(\, a * b \,)^2 = N(\, a \,)^2 \cdot N(\, b \,)^2 \,,$$

oziroma

$$N(\, a * b \,) = N(\, a \,) \cdot N(\, b \,) \,,$$

od koder sledi, da je $\mathcal{A}_{ij}$ evklidska Hurwitzova algebra.

Trditev 5.4. *Identiteta $\mathcal{A}_{ij} \longrightarrow \mathcal{A}_{ji}$ je anti-izomorfizem.*

Opomba: *Anti-izomorfizem $\phi : \mathcal{C} \longrightarrow \mathcal{D}$ je preslikava, ki zadošča identiteti*

$$\phi(\, a \underset{\mathcal{C}}{\cdot} b \,) = \phi(\, b \,) \underset{\mathcal{D}}{\cdot} \phi(\, a \,) \,.$$

Dokaz: Ker je evklidska algebra $\mathcal{E}$ komutativna, velja

$$a \underset{i,j}{*} b = (\, e_{ik} \circ a \,) \circ (\, e_{jk} \circ b \,) = (\, e_{jk} \circ b \,) \circ (\, e_{ik} \circ a \,) = b \underset{j,i}{*} a \,,$$

od koder sledi, da je identiteta $\mathcal{A}_{ij} \longrightarrow \mathcal{A}_{ji}$ antiizomorfizem. $\square$

Trditev 5.5. *Če je $r \geq 4$, je produkt $*$ asociativen in neodvisen od izbire k.*

Dokaz: Dokažimo najprej neodvisnost produkta $*$ od izbire k. Naj bo $l \neq i, j, k$. Potem z upoštevanjem trditve 5.2 in komutativnosti evklidske algebre $\mathcal{E}$, za poljubna a in $b \in \mathcal{E}_{ij}$ velja

$$\begin{aligned}
(\, e_{ik} \circ a \,) \circ (\, e_{jk} \circ b \,) &= (\, e_{ik} \circ a \,) \circ (\, (\, e_{kl} \circ e_{jl} \,) \circ b \,) \\
&= (\, (\, e_{ik} \circ a \,) \circ (\, e_{kl} \circ (\, e_{jl} \circ b \,) \,) \\
&= (\, (\, e_{ik} \circ a \,) \circ e_{kl} \,) \circ (\, e_{jl} \circ b \,) \\
&= (\, e_{kl} \circ (\, e_{ik} \circ a \,) \,) \circ (\, e_{jl} \circ b \,) \\
&= (\, (\, e_{kl} \circ e_{ik} \,) \circ a \,) \circ (\, e_{jl} \circ b \,) \\
&= (\, (\, e_{ik} \circ e_{kl} \,) \circ a \,) \circ (\, e_{jl} \circ b \,) \\
&= (\, e_{il} \circ a \,) \circ (\, e_{jl} \circ b \,) \,.
\end{aligned}$$

Z upoštevanjem dobljene lastnosti dokažemo še asociativnost produkta $*$.

$$\begin{aligned} a*(b*c) &= (e_{ik}\circ a)\circ(e_{jk}\circ(b*c)) \\ &= (e_{ik}\circ a)\circ[e_{jk}\circ((e_{il}\circ b)\circ(e_{jl}\circ c))] \\ &= (e_{ik}\circ a)\circ[((e_{il}\circ e_{jk})\circ b)\circ(e_{jl}\circ c)] \\ &= (e_{ik}\circ a)\circ[(e_{il}\circ(e_{jk}\circ b))\circ(e_{jl}\circ c)] \\ &= [(e_{il}\circ(e_{jk}\circ b))\circ(e_{ik}\circ a)]\circ(e_{jl}\circ c) \\ &= [e_{il}\circ((e_{jk}\circ b)\circ(e_{ik}\circ a))]\circ(e_{jl}\circ c) \\ &= [e_{il}\circ((e_{ik}\circ a)\circ(e_{jk}\circ b))]\circ(e_{jl}\circ c) \\ &= ((e_{ik}\circ a)\circ(e_{jk}\circ b))*c \\ &= (a*b)*c\,. \end{aligned}$$

Podobno kot v poglavju o Hurwitzovih algebrah, tudi v algebri $\mathcal{A}_{ij}$ definirajmo operacijo konjugiranja. Operacijo konjugacije, ki elementu $a\in\mathcal{A}_{ij}$ priredi $\overline{a}\in\mathcal{A}_{ij}$, definiramo s predpisom

$$\overline{a}=\tfrac{1}{4}\langle a,e_{ij}\rangle\cdot e_{ij}-a\,.$$

Tako definirana operacija konjugacije je pravokotna simetrija glede na os $\mathbb{R}\cdot e_{ij}$.

V nadaljevanju bomo operator levega množenja z elementom e_{ij} simbolno označevali z L_{ij}.

Trditev 5.6 *Če so i, j, k in l različni, veljata naslednji identiteti*

$$\begin{aligned} (i)\ & L_{ij}\,L_{jk}\,a=L_{ik}\,a\,,\ \text{če } a\in\mathcal{E}_{kl} \\ (ii)\ & L_{ij}\,L_{jk}\,a=\overline{L_{ik}\,a}\,,\ \text{če } a\in\mathcal{E}_{ij} \end{aligned}$$

Dokaz: (i) Ker po trditvi 5.2 za vsak $a\in\mathcal{E}_{kl}$ velja

$$e_{ij}\circ(e_{jk}\circ a)=(e_{ij}\circ e_{jk})\circ a=e_{ik}\circ a\,,$$

očitno sledi

$$L_{ij}\,L_{jk}\,a=L_{ik}\,a\,.$$

(ii) Z upoštevanjem trditve 5.1 in komutativnosti evklidske algebre $\mathcal{E}$, velja

$$\begin{aligned} e_{ij}\circ(e_{jk}\circ a) &= e_{ij}\circ(a\circ e_{jk}) = \\ = \tfrac{1}{4}\langle a,e_{ij}\rangle\cdot e_{jk}-a\circ(e_{ij}\circ e_{jk}) &= \tfrac{1}{4}\langle a,e_{ij}\rangle\cdot e_{jk}-a\circ e_{ik}\,. \end{aligned}$$

Ker velja

$$\langle L_{ik}\,a,e_{jk}\rangle=\langle e_{ik}\circ a,e_{jk}\rangle=\langle a,e_{ik}\circ e_{jk}\rangle=\langle a,e_{ij}\rangle\,,$$

je preslikava $L_{ik}:\mathcal{E}_{ij}\longrightarrow\mathcal{E}_{jk}$ izometrija. Od tod sledi

$$e_{ij} \circ (e_{jk} \circ a) = \tfrac{1}{4} \langle L_{ik}\, a, e_{jk} \rangle \cdot e_{jk} - L_{ik}\, a = \overline{L_{ik}\, a}\,.$$

Trditev 5.7. *Za različne i, j in k, je preslikava*

$$L_{ij} \,:\, \mathcal{A}_{ik} \longrightarrow \mathcal{A}_{kj}\,,$$

izomorfizem.

Dokaz: Po definiciji produkta $*$, za a in $b \in \mathcal{A}_{ik}$ velja

$$(L_{ij}\, a) \underset{k,j}{*} (L_{ij}\, b) = (e_{ik} \circ (e_{ij}\, a)) \circ (e_{ij} \circ (e_{ij} \circ b))\,.$$

Če v trditvi 5.1 nadomestimo element x z a, y z e_{ij} ter z z e_{ik}, dobimo

$$e_{ik} \circ (e_{ij} \circ a) = \tfrac{1}{4} \langle e_{ik}, a \rangle \cdot e_{ij} - a \circ (e_{ik} \circ e_{ij}) = \tfrac{1}{4} \langle e_{ik}, a \rangle \cdot e_{ij} - a \circ e_{jk}$$

in

$$e_{ij} \circ (e_{ij} \circ b) = \tfrac{1}{8}\, ||\, e_{ij}\, ||^2\, b = b\,,$$

od koder sledi

$$(L_{ij}\, a) \underset{k,j}{*} (L_{ij}\, b) = (\tfrac{1}{4} \langle e_{ik}, a \rangle \cdot e_{ij} - a \circ e_{jk}) \circ b\,,$$

oziroma

$$(L_{ij}\, a) \underset{k,j}{*} (L_{ij}\, b) = \tfrac{1}{4} \langle e_{ik}, a \rangle \cdot (e_{ij} \circ b) - (a \circ e_{jk}) \circ b\,.$$

Po drugi strani, velja identiteta

$$a \underset{i,k}{*} b = (e_{jk} \circ a) \circ (e_{ij} \circ b)\,.$$

Če uporabimo identiteto trditve 5.1 na elementih $e_{jk} \circ a$, e_{ij} in b, dobimo

$$\begin{aligned} a \underset{i,k}{*} b &= \tfrac{1}{4} \langle e_{ij}, e_{jk} \circ a \rangle \cdot b - e_{ij} \circ ((e_{jk} \circ a) \circ b) = \\ &= \tfrac{1}{4} \langle e_{ij} \circ e_{jk}, a \rangle \cdot b - e_{ij} \circ ((e_{jk} \circ a) \circ b) = \\ &= \tfrac{1}{4} \langle e_{ik}, a \rangle \cdot b - e_{ij} \circ ((e_{jk} \circ a) \circ b)\,. \end{aligned}$$

Od tod sledi

$$\begin{aligned} L_{ij} (a \underset{i,k}{*} b) &= \tfrac{1}{4} \langle e_{ik}, a \rangle \cdot (e_{ij} \circ b) - e_{ij} \circ [e_{ij} \circ ((e_{jk} \circ a) \circ b)] = \\ &= \tfrac{1}{4} \langle e_{ik}, a \rangle \cdot (e_{ij} \circ b) - (e_{jk} \circ a) \circ b)\,, \end{aligned}$$

oziroma

$$L_{ij}\,(\,a \underset{i,k}{*} b\,) = (\,L_{ij}\,a\,) \underset{k,j}{*} (\,L_{ij}\,b\,)\,.$$

Naj $\mathcal{A}_d$ označuje evklidsko Hurwitzovo algebro dimenzije d. Ker so po Hurwitzovem izreku 5.6.6 edine evklidske Hurwitzove algebre $\mathbb{R}$, $\mathbb{C}$, $\mathbb{H}$ in $\mathbb{O}$ sledi, da je $d \in \{\,1,2,4,8\,\}$.

Izrek 5.8. *Naj bo $\mathcal{E}$ enostavna evklidska algebra ranga ≥ 3 in d dimenzija $\mathcal{E}_{ij}$. Potem je $\mathcal{E}$ izomorfna $\mathcal{H}er(\,r,\mathcal{A}_d\,)$. V primeru, da je $r = 3$, je $d \in \{\,1,2,4,8\,\}$, v primeru, da je $r \geq 4$ pa je $d \in \{\,1,2,4\,\}$.*

Dokaz: Dokazali smo, da je algebra $\mathcal{A}_{ij}$, opremljena s produktom $*$, evklidska Hurwitzova algebra. Po Hurwitzovem izreku je izomorfna $\mathcal{A}_d$, kjer je $d \in \{\,1,2,4,8\,\}$. Če je $r \geq 4$, je po trditvi 5.5 algebra $\mathcal{A}_{ij}$ asociativna. Ker je $\mathcal{A}_8 = \mathbb{O}$ neasociativna, je torej v primeru $r \geq 4$ lahko $d \in \{\,1,2,4\,\}$.

Naj bo φ fiksen izomorfizem iz $\mathcal{A}_d$ na $\mathcal{A}_{ij}$. Definirajmo družino izomorfizmov $\{\,\varphi_{ij}\,\}$, $i \neq j$,

$$\varphi_{ij}\;:\;\mathcal{A}_d \longrightarrow \mathcal{A}_{ij}\,,$$

z naslednjim predpisom

$$\varphi_{12}(\,\alpha\,) = \varphi(\,\alpha\,)\,,\;\; \varphi_{21}(\,\alpha\,) = \varphi(\,\overline{\alpha}\,)\,,$$

$$\varphi_{1j}(\,\alpha\,) = L_{2j} \circ \varphi(\,\overline{\alpha}\,)\,,\;\; \varphi_{j1}(\,\alpha\,) = \varphi_{1j}(\,\overline{\alpha}\,)\,,\;\; \text{če je } j \geq 3$$

in

$$\varphi_{ji}(\,\alpha\,) = L_{1i} \circ \varphi_{1j}(\,\overline{\alpha}\,)\,,\;\; \varphi_{ij}(\,\alpha\,) = \varphi_{ji}(\,\overline{\alpha}\,)\,,\;\; \text{če je } i \geq 2 \text{ in } j > i\,.$$

Če so i, j in k različni, velja

$$\varphi_{ik}(\,\alpha\,) = \varphi_{ki}(\,\overline{\alpha}\,) = L_{1i} \circ \varphi_{1k}(\,\overline{\alpha}\,)\,,$$

od koder sledi

$$\begin{aligned}
L_{ij} \circ \varphi_{jk}(\,\alpha\,) &= L_{ij} \circ \varphi_{kj}(\,\overline{\alpha}\,) = L_{ij} \circ (\,L_{1j} \circ \varphi 1k(\,\overline{\alpha}\,) \\
&= L_{ij} \circ (\,(\,L_{ji} \circ L_{1i}\,) \circ \varphi_{1k}(\,\overline{\alpha}\,)\,) \\
&= L_{ij} \circ (\,L_{ji} \circ (\,L_{1i} \circ \varphi_{1k}(\,\overline{\alpha}\,)\,)\,) \\
&= L_{ij} \circ (\,L_{ji} \circ \varphi_{ik}(\,\alpha\,)\,) = \tfrac{1}{8}\,||\,e_{ij}\,||^2 \varphi_{ik}(\,\alpha\,) \\
&= \varphi_{ik}(\,\alpha\,)\,,
\end{aligned}$$

oziroma

$$L_{ij} \circ \varphi_{jk} = \varphi_{ik}\,.$$

Podobno je

$$\begin{aligned} L_{ij}\circ\varphi_{ki}(\,\alpha\,) &= L_{ij}\circ(\,L_{1i}\circ\varphi_{1k}(\,\alpha\,)\,)\\ &= L_{ij}\circ(\,(\,L_{ij}\circ L_{1j}\,)\circ\varphi_{1k}(\,\alpha\,)\\ &= L_{ij}\circ(\,L_{ij}\circ(\,L_{1j}\circ\varphi_{1k}(\,\alpha\,)\,)\,)\\ &= L_{ij}\circ(\,L_{ij}\circ\varphi_{kj}(\,\alpha\,)\,)\\ &= \varphi_{kj}(\,\alpha\,)\,, \end{aligned}$$

oziroma

$$L_{ij}\circ\varphi_{ki} = \varphi_{kj}\,.$$

V nadaljevanju bomo s $\sim$ označevali elemente $\tilde{\mathcal{E}} = \mathcal{H}er(\,r,\mathcal{A}_d\,)$. Naj bo

$$\tilde{p}_i = E_{ii}\,,$$

$$\tilde{e}_{ij} = 2\,(\,E_{ij}+E_{ji}\,)\,,$$

kjer E_{ij} označuje matriko, ki ima na $i,j-$tem mestu 1, drugod pa 0. Definirajmo preslikavo

$$\Phi\;:\;\tilde{\mathcal{E}}\longrightarrow\mathcal{E}\,,$$

s predpisom

$$\Phi(\,\{\,\alpha_{ij}\}_{i,j}^{r}\,) = \sum_{i=1}^{r}\alpha_{ii}\cdot p_i + \sum_{i<j}\varphi_{ij}(\,\alpha_{ij}\,)\,.$$

Ker velja

$$\Phi(\,\tilde{p}_i\,) = p_i\,,$$

$$\Phi(\,\tilde{\mathcal{E}}_{ij}\,) = \mathcal{E}_{ij}\,,$$

zožitev Φ_{ij} preslikave Φ na prostoru $\tilde{\mathcal{E}}_{ij}$ definira izomorfizem algeber $\tilde{\mathcal{A}}_{ij}$ in $\mathcal{A}_{ij}$. Če upoštevamo, da je $L_{ij}\circ\varphi_{jk} = \varphi_{ik}$ in $L_{ij}\circ\varphi_{ki} = \varphi_{kj}$, sledi identiteta

$$\Phi\circ\tilde{L_{ij}} = L_{ij}\circ\Phi\,.$$

Dokažimo, da je preslikava Φ, ki zadošča zgornji identiteti, ravno iskani izomorfizem evklidske algebre $\mathcal{E}$. Zadošča pokazati, da za elementa $a\in\tilde{\mathcal{E}}_{ij}$ in $b\in\tilde{\mathcal{E}}_{jk}$, kjer so i, j in k različni, velja identiteta $\Phi(\,a\cdot b\,) = \Phi(\,a\,)\cdot\Phi(\,b\,)$. Ker je

$$a\cdot b = (\,\tilde{L}_{jk}\,a\,)\underset{i,k}{*}(\,\tilde{L}_{ij}\,b\,)\,,$$

sledi

$$\Phi(\, a \cdot b\,) = \Phi_{ik}\,(\,(\,\tilde{L}_{jk}\, a\,) \underset{i,k}{*} (\,\tilde{L}_{ij}\, b\,)\,)\,.$$

Če upoštevamo, da je $\Phi_{ik} : \tilde{\mathcal{A}}_{ik} \longrightarrow \mathcal{A}_{ik}$ izomorfizem, dobimo

$$\begin{aligned}\Phi(\, a \cdot b\,) &= \Phi_{ik}\,(\,\tilde{L}_{jk}\, a\,) \underset{i,k}{*} \Phi_{ik}\,(\,\tilde{L}_{ij}\, b\,) \\ &= L_{jk}\,\Phi_{ij}(\, a\,) \underset{i,k}{*} L_{ij}\,\Phi_{jk}(\, b\,) \\ &= \Phi(\, a\,) \cdot \Phi(\, b\,)\,.\end{aligned}$$

Ugotovitve poglavja lahko strnemo v naslednji tabeli.

Ω	$\mathcal{E}$	$dim\,\mathcal{E}$	$rang\,\mathcal{E}$	d
$\mathcal{P}(m,\mathbb{R})$	$\mathcal{S}im(m,\mathbb{R})$	$\frac{1}{2}\,m(m+1)$	m	1
$\mathcal{P}(m,\mathbb{C})$	$\mathcal{H}er(m,\mathbb{C})$	m^2	m	2
$\mathcal{P}(m,\mathbb{H})$	$\mathcal{H}er(m,\mathbb{H})$	$m(2m-1)$	m	4
$\mathcal{L}_n$	$\mathcal{L}or(n) = \mathbb{R} \times \mathbb{R}^{n-1}$	n	2	$n-2$
$\mathcal{P}(3,\mathbb{O})$	$\mathcal{H}er(3,\mathbb{O})$	27	3	8

Iz tabele je mogoče razbrati naslednje izomorfizme

$$\begin{aligned}\mathcal{S}im(\,2,\mathbb{R}\,) &\simeq \mathbb{R} \times \mathbb{R}^2\,, \\ \mathcal{H}er(\,2,\mathbb{C}\,) &\simeq \mathbb{R} \times \mathbb{R}^3\,, \\ \mathcal{H}er(\,2,\mathbb{H}\,) &\simeq \mathbb{R} \times \mathbb{R}^5\,.\end{aligned}$$

7 Klasifikacija simetričnih stožcev

7.1 Stožec kvadratov evklidske algebre

Poglavji o Lorentzovih in Sieglovih stožcih smo sklenili s trditvijo, da množica kvadratov Lorentzove algebre oziroma algebre simetričnih matrik predstavlja zaprtje pripadajočih simetričnih Lorentzovih oziroma stožcev pozitivnih simetričnih matrik. Namen tega razdelka je dokazati, da množica kvadratov poljubne evklidske algebre predstavlja stožec, katerega notranjost je simetričen stožec.

Naj bo $\mathcal{E}$ evklidska algebra. Če je $x \in \mathcal{E}$, lahko definiramo njegovo determinanto s pomočjo spektralnega zapisa $x = \lambda_1 p_1 + \ldots + \lambda_n p_n$, kjer so p_i primitivni pravokotni projektorji, katerih vsota je 1. Nekateri skalarji λ_i so seveda lahko enaki 0. Determinanto definiramo s predpisom

$$det(x) = \lambda_1 \cdot \lambda_2 \cdot \ldots \cdot \lambda_n \,.$$

Čeprav spektralni zapis ni povsem enoličen (v primeru večkratnih spektralnih vrednosti), je funkcija $det(x)$ dobro definirana.

Naj bo $\overline{\mathcal{C}}$ množica kvadratov evklidske algebre $\mathcal{E}$, podana s predpisom

$$\overline{\mathcal{C}} = \{\, x^2 \,;\, x \in \mathcal{E} \} \,.$$

V nadaljevanju si oglejmo nekatere lastnosti množice kvadratov $\overline{\mathcal{C}}$. Še prej pa dokažimo naslednjo

Lema 1.1. *Če je p projektor evklidske algebre $\mathcal{E}$, za poljuben $x \in \mathcal{E}$ velja*

$$\langle\, p \circ x, x \,\rangle \geq 0 \,.$$

Dokaz: Če je $\mathcal{E}_0 + \mathcal{E}_{\frac{1}{2}} + \mathcal{E}_1$ dekompozicija algebre $\mathcal{E}$, lahko vsak element $x \in \mathcal{E}$ zapišemo v obliki

$$x = x_0 + x_{\frac{1}{2}} + x_1 \,.$$

Ker velja

$$p \circ x = p \circ x_0 + p \circ x_{\frac{1}{2}} + p \circ x_1 = 0x_0 + \tfrac{1}{2}x_{\frac{1}{2}} + x_1 = \tfrac{1}{2}x_{\frac{1}{2}} + x_1\,,$$

od tod sledi

$$\langle\, p \circ x, x\,\rangle = \langle\, \tfrac{1}{2}x_{\frac{1}{2}} + x_1, x_0 + \tfrac{1}{2}x_{\frac{1}{2}} + x_1\,\rangle = \tfrac{1}{2}||\, x_{\frac{1}{2}}||^2 + ||\, x_1\,||^2 \geq 0\,.$$

Trditev 1.2.

$$\begin{aligned}\overline{\mathcal{C}} = \{\, x^2\,;\, x \in \mathcal{E}\,\} = \{\, y \in \mathcal{E}\,;\, y \\ = \lambda_1 p_1 + \ldots + \lambda_n p_n,\ , \lambda_i \geq 0 \text{ in } p_1 + \ldots + p_n = 1\,\}\,.\end{aligned}$$

Dokaz: Naj bo $\mathcal{Q} = \{\, x \in \mathcal{E}\,;\, x = \lambda_1 p_1 + \ldots + \lambda_n p_n, \lambda_i \geq 0$ in $p_1 + \ldots + p_n = 1\,\}$ in $y \in \mathcal{Q}$. Ker lahko y zapišemo v obliki

$$y = (\,\sqrt{\lambda_1}p_1 + \ldots + \sqrt{\lambda_n}p_n\,)^2\,,$$

sledi, da je $\mathcal{Q} \subset \overline{\mathcal{C}}$.

Naj bo zdaj $y \in \overline{\mathcal{C}}$. Denimo, da je $y = x^2$. Tedaj je $y = \lambda_1 p_1 + \ldots + \lambda_n p_n,\ , \lambda_i = x^2$. Če x^2 skalarno pomnožimo s p_i, dobimo

$$\langle\, p_i, x^2\,\rangle = \langle\, p_i \circ x, x\,\rangle = \lambda_i\,\langle\, x, x\,\rangle = \lambda_i\,||\, x\,||^2\,.$$

Ker je po prejšnji lemi $\langle\, p_i \circ x, x\,\rangle \geq 0$, so vsi $\lambda_i \geq 0$. To pa pomeni, da je $y \in \mathcal{Q}$, oziroma $\overline{\mathcal{C}} \subset \mathcal{Q}$. □

Očitno je množica $\overline{\mathcal{C}}$ stožec. Njegova notranjost je stožec podan s predpisom

$$\begin{aligned}\mathcal{C} &= \{\, x \in \overline{\mathcal{C}}\,;\, det(x) \neq 0\,\} \\ &= \{\, x \in \mathcal{E}\,;\, x = \lambda_1 p_1 + \ldots + \lambda_n p_n, \lambda_i \geq 0 \quad \text{in} \\ &\qquad p_1 + \ldots + p_n = 1\,\}\,.\end{aligned}$$

Dokažimo najprej, da je stožec $\overline{\mathcal{C}}$ konveksen. Naj bosta x^2 in $y^2 \in \overline{\mathcal{C}}$. Element $x^2 = y^2$ torej lahko zapišemo kot

$$x^2 + y^2 = \lambda_1 p_1 + \ldots + \lambda_n p_n\,.$$

Ker za projektor p in poljuben $x \in \mathcal{E}$ velja $\langle\, p \circ x, x\,\rangle \geq 0$, sledi

$$\begin{aligned}\lambda_i|\, p_i|^2 = \lambda_i\langle\, p_i, p_i\,\rangle = \langle\, p_i, \lambda_i\,\rangle = \langle\, p_i, x^2 + y^2\,\rangle = \\ = \langle\, p_i, x^2\,\rangle + \langle\, p_i, y^2\,\rangle = \langle\, p_i \circ x, x\,\rangle + \langle\, p_i \circ y, y\,\rangle \geq 0\,,\end{aligned}$$

kar pomeni, da so vsi skalarji λ_i nenegativni. Od tod sledi

$$x^2 + y^2 = (\sqrt{\lambda_1} p_1 + \ldots + \sqrt{\lambda_n} p_n)^2 \in \overline{\mathcal{C}}\,.$$

Podobno dokažemo tudi konveksnost stožca $\mathcal{C}$. Naj bosta x^2 in $y^2 \in \mathcal{C}$. Denimo, da je $x^2 + y^2 \in \overline{\mathcal{C}} \setminus \mathcal{C}$. Potem obstaja neničelen projektor q, ki je pravokoten na $x^2 + y^2$, oziroma velja $\langle\, q, x^2 + y^2 \,\rangle = 0$. Ker sta $\langle\, q, x^2 \,\rangle$ in $\langle\, q, y^2 \,\rangle \geq 0$ sledi $\langle\, q, x^2 \,\rangle = \langle\, q, x^2 \,\rangle = 0$. Ker je $x^2 \in \mathcal{C}$, je $x^2 = \lambda_1 p_1 + \ldots + \lambda_n p_n$, kjer je vsota projektorjev p_i enaka 1 in so vsi λ_i pozitivni. Ker je

$$0 = \langle\, q, \lambda_1 p_1 \,\rangle + \ldots + \langle\, q, \lambda_n p_n \,\rangle = \lambda_1 \langle\, q, p_1^2 \,\rangle + \ldots + \lambda_n \langle\, q, p_n^2 \,\rangle\,,$$

oziroma

$$\lambda_1 \langle\, q \circ p_1, p_1 \,\rangle + \ldots + \lambda_n \langle\, q \circ p_n, p_n \,\rangle\,,$$

zaradi $\langle\, q \circ p_i, p_i \,\rangle \geq 0$ in pozitivnosti skalarjev λ_i sledi, da je $\langle\, q, p_i \,\rangle = 0$. To pa je protislovje, saj bi sicer veljalo

$$\langle\, q, q \,\rangle = \langle\, 1, q^2 \,\rangle = \langle\, 1, q \,\rangle = \langle\, p_1, q \,\rangle + \ldots + \langle\, p_n, q \,\rangle = 0\,.$$

Po definiciji je množica

$$\mathcal{C}^* = \{\, y \in \mathcal{E}\,;\, \langle\, y, x^2 \,\rangle > 0\,,\, \forall x \in \overline{\mathcal{C}} \setminus 0 \,\}\,,$$

odprt dual stožca $\mathcal{C}$. Ker velja

$$\langle\, y, x^2 \,\rangle = \langle\, y \circ x, x \,\rangle = \langle\, L(y)x, x \,\rangle\,,$$

lahko $\mathcal{C}^*$ zapišemo kot

$$\mathcal{C}^* = \{\, y \in \mathcal{E}\,;\, L(y) \quad \text{pozitivno definiten} \,\}\,.$$

Zaradi zaprtosti $\mathcal{C}^*$ za seštevanje in množenje s pozitivnim realnim skalarjem, je $\mathcal{C}^*$ odprt konveksen stožec.

Izrek 1.3. *Stožec $\mathcal{C}$ je sebi dualen.*

Dokaz: Naj bo $y \in \mathcal{C}$. Po spektralnem izreku je potem

$$y = \lambda_1 p_1 + \ldots + \lambda_n p_n\,,$$

kjer so vsi skalarji λ_i pozitivni. Ker za projektor p in poljuben element $x \in \mathcal{E}$ velja $\langle\, p \circ x, x \,\rangle \geq 0$, sledi

$$\begin{aligned}\langle\, y, x^2 \,\rangle &= \langle\, \lambda_1 p_1, x^2 \,\rangle + \ldots + \langle\, \lambda_n p_n, x^2 \,\rangle = \\ &= \lambda_1 \langle\, p_1 \circ x, x \,\rangle + \ldots + \lambda_n \langle\, p_n \circ x, x \,\rangle \geq 0\,.\end{aligned}$$

Če bi veljalo $\langle\, y, x^2 \,\rangle = 0$, bi to pomenilo, da so $\langle\, p_i \circ x, x \,\rangle = 0$ in od tod

$$\langle\, x, x \,\rangle = \langle\, 1, x^2 \,\rangle = \langle\, p_1 + \ldots + p_n, x^2 \,\rangle = \langle\, p_1, x^2 \,\rangle + \ldots + \langle\, p_n, x^2 \,\rangle = 0\,,$$

oziroma $x = 0$. Od tod torej sledi $y \in \mathcal{C}^*$, oziroma $\mathcal{C} \subset \mathcal{C}^*$.

Naj bo $x \in \mathcal{C}^*$. Če so p_i paroma pravokotni projektorji, velja

$$\begin{aligned} \lambda_i &= \frac{1}{||p_i||^2}\langle\, x, p_i \,\rangle = \frac{1}{||p_i||^2}\langle\, x, p_i^2 \,\rangle = \frac{1}{||p_i||^2}\langle\, x \circ p_i, p_i \,\rangle = \\ &= \frac{1}{||p_i||^2}\langle\, L(x)p_i, p_i \,\rangle > 0\,. \end{aligned}$$

Če torej zapišemo

$$y = \sqrt{\lambda_1}p_1 + \ldots + \sqrt{\lambda_n}p_n\,,$$

sledi, da je $x = y^2$, oziroma $\mathcal{C}^* \subset \mathcal{C}$. Od tod sledi, da je $\mathcal{C}$ sebi dualen stožec. □

7.2 Simetričnost stožca kvadratov

Namen razdelka je dokazati simetričnost notranjosti stožca kvadratov evklidske algebre. V prejšnjem razdelku smo dokazali, da je njegova notranjost sebi dualen stožec. Za dokaz simetričnosti torej zadošča pokazati še homogenost. Preden dokažemo homogenost dokažimo, da lahko notranjost stožca kvadratov definiramo kot množico oblike

$$\mathcal{C} = \{\, \exp x\,;\, x \in \mathcal{E} \,\}\,,$$

kjer je $\exp x$ definiran s predpisom

$$\exp x = \sum_{n=0}^{\infty} \tfrac{1}{n!}\, x^n\,.$$

Definicija je smiselna zaradi potenčne asociativnosti evklidske algebre $\mathcal{E}$ in konvergence eksponentne vrste na realni osi.

Naj bo $x^2 \in \mathcal{C}$. Tedaj x^2 lahko zapišemo v obliki $x^2 = \lambda_1 p_1 + \ldots + \lambda_n p_n$, kjer so $\lambda_i > 0$. Če uporabimo zapis $\lambda_i = e^{\alpha_i}$, lahko pišemo

$x^2 = e^{\alpha_1} p_1 + \ldots + e^{\alpha_n} p_n$. Če upoštevamo, da za poljuben projektor p_i velja $p_i^m = p_i$, sledi

$$\begin{aligned} x^2 &= \sum_{i=1}^{n} e^{\alpha_i} p_i = \sum_{i=1}^{n} \Big(\sum_{m=0}^{\infty} \tfrac{\alpha_i^m}{m!} \Big) p_i = \sum_{i=1}^{n} \sum_{m=0}^{\infty} \tfrac{\alpha_i^m p_i^m}{m!} = \\ &= \sum_{i=1}^{n} \sum_{m=0}^{\infty} \tfrac{(\alpha_i p_i)^m}{m!} = \sum_{m=0}^{\infty} \sum_{i=1}^{n} \tfrac{(\alpha_i p_i)^m}{m!} = \\ &= \sum_{m=0}^{\infty} \tfrac{1}{m!} \Big(\sum_{i=1}^{n} \alpha_i p_i \Big)^m = \sum_{m=0}^{\infty} \tfrac{u^m}{m!} = \exp u\,. \end{aligned}$$

To pomeni, da lahko $x^2 \in \mathcal{C}$, zapišemo kot $\exp u$, za nek $u \in \mathcal{E}$, oziroma velja $\mathcal{C} \subset \{ \exp u\,;\, u \in \mathcal{E} \}$.

Ker za poljuben $y \in \{ \exp u\,;\, u \in \mathcal{E} \}$ velja

$$y = \exp x = e^x = e^{\frac{x}{2}} \circ e^{\frac{x}{2}} = v \circ v = v^2\,,$$

sledi, da je $y \in \overline{\mathcal{C}}$. Ker je $\exp(x) \circ \exp(-x) = \exp(0) = e$, je $\{ \exp u\,;\, u \in \mathcal{E} \}$ vsebovana v množici obrnljivih elementov, ki ležijo v notranjosti $\overline{\mathcal{C}}$. To pomeni, da je $\{ \exp u\,;\, u \in \mathcal{E} \} \subset \mathcal{C}$, oziroma velja $\mathcal{C} = \{ \exp u\,;\, u \in \mathcal{E} \}$. Dokazali smo torej naslednjo

Trditev 2.1. *Notranjost stožca kvadratov $\mathcal{C}$ lahko zapišemo kot*

$$\mathcal{C} = \{ \exp x\,;\, x \in \mathcal{E} \}\,.$$

Trditev 2.2. *Stožec $\mathcal{C}$ je povezana komponenta enote množice obrnljivih elementov $\mathcal{I}(\mathcal{E})$.*

Dokaz: Dokažimo najprej, da je $\mathcal{C} = \exp(\mathcal{E})$ povezana množica. Ker je $e = \exp(0)$, je $e \in \exp(\mathcal{E})$. Naj bo $y \in \exp(\mathcal{E})$. Tedaj obstaja tak $a \in \mathcal{E}$, da je $y = \exp a$. Definirajmo preslikavo $\gamma : [0,1] \longrightarrow \exp(\mathcal{E})$ s predpisom $\gamma(t) = \exp(at)$. Ker velja $\gamma(0) = e$ in $\gamma(1) = y$, zaradi zveznosti γ sledi, da je γ pot med e in y. To pomeni, da sta e in y povezana. Če definiramo preslikavo $\delta : [0,1] \longrightarrow \exp(\mathcal{E})$ s predpisom $\delta(t) = \gamma(1-t)$, velja $\delta(0) = y$ ter $\delta(1) = e$. Zaradi zveznosti je δ pot med y in e. Naj bodo $x, y \in \exp(\mathcal{E})$, γ pot od e do y in δ pot od x do e. Potem preslikava $\gamma * \delta : [0,1] \longrightarrow \exp(\mathcal{E})$ podana s predpisom

$$(\gamma * \delta)(s) = \begin{cases} \delta(2s)\,, \ 0 \le s \le \frac{1}{2} \\ \gamma(2s-1)\,, \ \frac{1}{2} \le s \le 1 \end{cases}\,,$$

$$\begin{tikzcd} \Omega \arrow[r] \arrow[dr, dashed, leftrightarrow] & \mathcal{E} \arrow[d] \\ & \mathcal{C} \end{tikzcd}$$

Korenspodenca $\Omega \longleftrightarrow \mathcal{C}$

predstavlja pot od x do y. To pomeni, da sta elementa x in y povezana, oziroma, da je povezana $\mathcal{C}$.

Kot dokaz, da je $\mathcal{C}$ povezana komponenta enote v $\mathcal{I}(\mathcal{E})$, zadošča pokazati, da je $\mathcal{C}$ zaprta in odprta v $\mathcal{I}(\mathcal{E})$. Ker je $\mathcal{C} = \overline{\mathcal{C}} \cap \mathcal{I}(\mathcal{E})$, zaradi zaprtosti $\overline{\mathcal{C}}$ v $\mathcal{E}$, sledi, da je $\mathcal{C}$ zaprta v $\mathcal{I}(\mathcal{E})$. Po drugi strani je $\mathcal{C}$ odprta v $\mathcal{E}$. Ker je $\mathcal{C} \subset \mathcal{I}(\mathcal{E})$ in velja $\mathcal{C} = \mathcal{C} \cap \mathcal{I}(\mathcal{E})$, sledi, da je $\mathcal{C}$ tudi odprta v $\mathcal{I}(\mathcal{E})$. □

Trditev 2.3. *Stožec $\mathcal{C}$ je homogen.* Potem po izreku 5.4.5 zaradi obrnljivosti operatorja $P(x)P(y)P(x)$ sledi, da je obrnljiv tudi $P(x)y$. Ker je po trditvi 2.2 stožec $\mathcal{C}$ povezana komponenta enote množice obrnljivih elementov $\mathcal{I}(\mathcal{E})$ in velja $P(x)e = x^2 \in \mathcal{C}$, sledi, da je $P(x)\mathcal{C} \subset \mathcal{C}$. Ker po izreku 5.4.3 velja $P(x)^{-1}\mathcal{C} = P(x^{-1})\mathcal{C}$, je tudi $P(x^{-1})\mathcal{C} \subset \mathcal{C}$. Od tod sledi, da je $P(x)\mathcal{C} = \mathcal{C}$. To pomeni, da so operatorji $P(x)$ elementi grupe avtomorfizmov stožca $\mathcal{C}$. Naj bosta x^2 in $y^2 \in \mathcal{C}$. Ker sta potem $P(x)$ in $P(y)$ elementa grupe avtomorfizmov stožca $\mathcal{C}$, je avtomorfizem stožca $\mathcal{C}$ tudi preslikava definirana s predpisom $R = P(y)P(x^{-1})$. Ker je $P(x)e = x^2$, je potem $P(x)^{-1}x^2 = e$. Od tod sledi, da je $R(x^2) = P(y)P(x^{-1})x^2 = P(y)P(x)^{-1}x^2 = P(y)e = y^2$. Ker torej že podgrupa operatorjev $P(x)$, deluje na stožcu $\mathcal{C}$ tranzitivno, očitno tranzitivno deluje tudi grupa avtomorfizmov. □

Dokazali smo torej, da je stožec $\mathcal{C}$, notranjost množice kvadratov evklidske algebre $\mathcal{E}$, simetričen stožec.

7.3 Simetričen stožec in stožec kvadratov

V prejšnjem razdelku smo torej dokazali, da množica kvadratov poljubne evklidske algebre predstavlja stožec, katerega notranjost je simetrični stožec. Poglavje o simetričnih stožcih smo strnili z ugotovitvijo, ki predstavlja obrat omenjene trditve. Če je namreč dan simetričen stožec znotraj evklidskega prostora, lahko prostor opremimo s strukturo evklidske algebre.

Namen tega razdelka je dokazati, da obstaja bijektivna korespondenca med simetričnim stožcem Ω znotraj evklidske algebre $\mathcal{E}$ in stožcem $\mathcal{C}$, ki predstavlja notranjost množice kvadratov evklidske algebre $\mathcal{E}$.

Trditev 3.1. *Naj bo Ω simetričen stožec in $\mathcal{E}$ njemu prirejena evklidska algebra. Potem velja*

$$\overline{\Omega} = \{\, x^2\,;\, x \in \mathcal{E}\,\} = \mathcal{C}\,.$$

Dokaz: Pokazali smo, da je $\mathcal{C} = \{\, \exp x\,,\ x \in \mathcal{E}\,\}$. Po definiciji produkta evklidske algebre $\mathcal{E}$ vemo, da so operatorji levega množenja $L(x)$ elementi Liejeve algebre $\mathcal{L}_+$, ki je prirejena grupi avtomorfizmov stožca Ω. Ker je $\exp(\mathcal{L}_+)$ vsebovana v Liejevi grupi iz katere izhaja Liejeva algebra, je $\exp(L(x))$ avtomorfizem stožca Ω. Od tod sledi, da je $\exp(L(x))\, e \in \Omega$. Če izračunamo vrednost izraza $\exp(L(x))\, e$, ob upoštevanju potenčne asociativnosti in identitete $L(x)^n e = x^n$, dobimo

$$\exp(L(x))\, e = \Big(\sum_{n=0}^{\infty} \tfrac{1}{n!}\, L(x)^n\,\Big)\, e = \sum_{n=0}^{\infty} \tfrac{1}{n!}\,\big(\, L(x)^n\,\big)\, e \ =$$

$$= \sum_{n=0}^{\infty} \tfrac{1}{n!}\, L(x)^n e = \sum_{n=0}^{\infty} \tfrac{1}{n!}\, x^n = \exp x\,.$$

To pomeni, da je $\exp(\,\mathcal{E}\,) \subset \Omega$, oziroma $\mathcal{C} \subset \Omega$.

Od tod sledi, da je $\Omega^* \subset \mathcal{C}^*$, kjer $*$ pomeni dual stožca. Ker sta Ω in $\mathcal{C}$ simetrična stožca, velja $\Omega^* = \Omega$ in $\mathcal{C}^* = \mathcal{C}$. Od tod sledi, da je $\Omega \subset \mathcal{C}$, oziroma $\Omega = \mathcal{C}$. $\square$

7.4 Klasifikacija simetričnih stožcev

Naj bosta $\Omega_1 \subset \mathcal{E}_1$ in $\Omega_2 \subset \mathcal{E}_2$ simetrična stožca evklidskih prostorov $\mathcal{E}_1$ in $\mathcal{E}_2$. Stožca Ω_1 in Ω_2 imenujemo izomorfna, če obstaja taka bijektivna linearna preslikava $\Phi\, :\, \mathcal{E}_1 \longrightarrow \mathcal{E}_2$, da velja $\Phi(\Omega_1) = \Omega_2$ in $\Phi^{-1}(\Omega_2) = \Omega_1$.

Trditev 4.1. *Naj bosta Ω_1 in Ω_2 simetrična stožca, $\mathcal{E}_1$ in $\mathcal{E}_2$ pa njima prirejeni evklidski algebri. Če sta algebri $\mathcal{E}_1$ in $\mathcal{E}_2$ izomorfni, sta izomorfna tudi stožca Ω_1 in Ω_2.*

Dokaz: Naj bo preslikava $\Phi : \mathcal{E}_1 \longrightarrow \mathcal{E}_2$ izomorfizem evklidskih algeber $\mathcal{E}_1$ in $\mathcal{E}_2$. To pomeni, da je $\Phi(x \circ y) = \Phi(x) \circ \Phi(y)$ in $\Phi(e) = e$. Dokazali smo, da sta Ω_1 in Ω_2 podana s predpisoma $\Omega_1 = \{ u^2 , u \in \mathcal{E}_1, u \text{ obrnljiv} \}$ in $\Omega_2 = \{ v^2 , v \in \mathcal{E}_2, v \text{ obrnljiv} \}$.

Naj bo $u^2 \in \Omega_1$. Tedaj je $u \circ u^{-1} = e$. Ker velja $\Phi(u^2) = \Phi(u)^2$ in $\Phi(u) \circ \Phi(u^{-1}) = \Phi(u \circ u^{-1}) = \Phi(e) = e$, sledi, da je $\Phi(u) \in \Omega_2$, oziroma $\Phi(\Omega_1) \subset \Omega_2$.

Naj bo $v^2 \in \Omega_2$. Ker je $v = \Phi(x)$, za nek $x \in \Omega_1$ velja $v^2 = \Phi(x)^2 = \Phi(x^2)$. Ker je v obrnljiv, obstaja njegov inverz $v^{-1} \in \Omega_2$. Ker je Φ izomorfizem, je $v^{-1} = \Phi(y)$, za nek $y \in \Omega_1$. Ker velja

$$\Phi(x \circ y) = \Phi(x) \circ \Phi(y) = v \circ v^{-1} = e = \Phi(e)$$

in je Φ injektivna, je $x \circ y = e$, oziroma $y = x^{-1}$. Torej je $x^2 \in \Omega_1$ in $v^2 = \Phi(x^2) \in \Phi(\Omega_1)$. To pomeni, da je $\Omega_2 \subset \Phi(\Omega_1)$, oziroma $\Phi(\Omega_1) = \Omega_2$. $\square$

Trditev 4.2. *Naj bo Ω simetričen stožec in $\mathcal{E}$ njemu prirejena evklidska algebra. Denimo, da je $\mathcal{E} = \mathcal{I} \oplus \mathcal{J}$, kjer sta $\mathcal{I}$ in $\mathcal{J}$ neničelna ideala. Naj bosta $\Omega_{\mathcal{I}}$ in $\Omega_{\mathcal{J}}$ simetrična stožca, ki ustrezata evklidskima algebrama $\mathcal{I}$ in $\mathcal{J}$. Tedaj je stožec Ω izomorfen stožcu $\Omega_{\mathcal{I}} \times \Omega_{\mathcal{J}}$.*

Dokaz: Definirajmo preslikavo $\Phi : \mathcal{I} \times \mathcal{J} \longrightarrow \mathcal{E}$ s predpisom $\Phi(i, j) = i + j$. Ker je Φ bijektivna, zadošča dokazati identiteto

$$\Phi(\Omega_{\mathcal{I}} \times \Omega_{\mathcal{J}}) = \Omega .$$

Naj bo $x \in \Omega_{\mathcal{I}} \times \Omega_{\mathcal{J}}$. Tedaj lahko x pišemo v obliki $x = (a, b)$, kjer je $a \in \mathcal{I}^2 \cap Inv(\mathcal{I})$ in $b \in \mathcal{J}^2 \cap Inv(\mathcal{J})$.

Pišimo $a = i^2$ in $b = j^2$. Tedaj je $\Phi(a, b) = i^2 + j^2$. Ker je $\mathcal{I} \circ \mathcal{J} \subset \mathcal{I} \cap \mathcal{J} = 0$, je očitno $i \circ j = 0$. Torej je $(i + j)^2 = i^2 + j^2 + 2\, i \circ j = i^2 + j^2$, kar pomeni, da je $\Phi(a, b) = (i + j)^2$, oziroma $\Phi(a, b) \in \mathcal{E}^2$.

Po drugi strani zaradi obrnljivosti elementov i in j, $i^{-1} \in \mathcal{I}$ in $j^{-1} \in \mathcal{J}$, sledi $i^{-1} \circ j = i \circ j^{-1} = i^{-1} \circ j^{-1} = 0$. Ker velja

$$(i + j) \circ (i^{-1} + j^{-1}) = i \circ i^{-1} + i \circ j^{-1} + j \circ i^{-1} + j \circ j^{-1} =$$

$$= i \circ i^{-1} + j \circ j^{-1} = e_{\mathcal{I}} + e_{\mathcal{J}} = e_{\mathcal{E}}\,,$$

sledi, da je $(\,i + j\,)^2 \in \Omega$, oziroma $\Phi(\,\Omega_{\mathcal{I}} \times \Omega_{\mathcal{J}}\,) \subset \Omega$.

Naj bo $y \in \Omega$. Tedaj je $y = x^2$, $x \in \mathcal{E}$ obrnljiv element. Ker je $\mathcal{E} = \mathcal{I} \oplus \mathcal{J}$, lahko pišemo $x = i + j$, kjer sta $i \in \mathcal{I}$ in $j \in \mathcal{J}$. Podobno lahko x^{-1} zapišemo kot $x^{-1} = i_1 + j_1$, kjer sta $i_1 \in \mathcal{I}$ in $j_1 \in \mathcal{J}$. Ker je $e = x \circ x^{-1} = i \circ i_1 + j \circ j_1 \in \mathcal{I} \oplus \mathcal{J}$, $e = e_{\mathcal{I}} + e_{\mathcal{J}}$, ter velja enoličnost razcepa, sledi, da je $i \circ i_1 = e_{\mathcal{I}}$ in $j \circ j_1 = e_{\mathcal{J}}$. To pomeni, da sta i in j obrnljiva, oziroma $i^2 \in \Omega_{\mathcal{I}}$ in $j^2 \in \Omega_2$. Ker je $\Phi(i^2, j^2) = i^2 + j^2 = (\,i + j\,)^2 = x^2$, je $x^2 \in \Phi(\,\Omega_{\mathcal{I}} \times \Omega_{\mathcal{J}}\,)$, oziroma velja $\Omega \subset \Phi(\,\Omega_{\mathcal{I}} \times \Omega_{\mathcal{J}}\,)$. To pomeni, da je $\Phi(\,\Omega_{\mathcal{I}} \times \Omega_{\mathcal{J}}\,) = \Omega$. $\square$

Izrek 4.3. *Vsak simetričen stožec je izomorfen kartezičnemu produktu naslednjih stožcev:*

(*i*) $\mathbb{R}^+$

(*ii*) *Lorentzovih svetlobnih stožcev* $\mathcal{L}(n)$

(*iii*) *stožcev pozitivnih matrik* $\mathcal{P}(\,n, \mathbb{F}\,)$, *kjer je* $\mathbb{F} \in \{\,\mathbb{R}, \mathbb{C}, \mathbb{H}\,\}$ *in* $n \geq 3$.

(*iv*) *stožcev pozitivnih matrik* $\mathcal{P}(\,3, \mathbb{O}\,)$.

Dokaz: Izrek je posledica trditve 3.3, uporabljene induktivno na simetričnemu stožcu prirejeni evklidski algebri in klasifikacije enostavnih evklidskih algeber. $\square$

Literatura

1. Braun H., Koecher M., *Jordan Algebren*. Springer, Berlin, 1966.
2. Faraut J., Koranyi A., *Analysis on Symmetric Cones*. Clarendon Press, Oxford, 1994.
3. Folland G.B., *A Course in Abstract Harmonic Analysis*. CRC Press, Boca Raton, FL, 1995.
4. Hilgert J., Olafsson G., *Causal Symmetric Spaces*. Academic Press, New York, 1997.
5. Humphreys J.E., *Introduction to Lie Algebras and Representation Theory*. Springer, New York, 1972.
6. Jacobson N., *Lie Algebras*. Dover, New York, 1961.
7. Keimel K., Roth W., *Ordered Cones and Approximation*. Springer, Berlin, 1992.
8. Knapp A.W., *Lie Groups, Lie Algebras and Cohomology*. Princeton University Press, Princeton, NJ, 1988.
9. Lohmus J., Paal E., Sorgsepp L., *Nonassociative Algebras in Physics*. Hadronic Press, Palm Harbor, FL, 1994.
10. Milnor J.W., *Topology from the Differentiable Viewpoint*. University Press of Virginia, Charlottesville, VA, 1969.
11. Naber G.L., *The Geometry of Minkowski Spacetime*. Springer, New York, 1992.
12. Sattinger D.H., Weaver O.L., *Lie Groups and Algebras with Applications to Physics, Geometry and Mechanics*. Springer, New York, 1985.
13. Schafer R.D., *An Introduction to Nonassociative Algebras*. Academic Press, New York, 1966.
14. Siegel C.L., *Lectures on the Geometry of Numbers*. Springer, New York, 1989.
14. Unterberger A., Upmeier H., *Pseudodifferential Analysis on Symmetric Cones*. CRC Press, Boca Raton, FL, 1996.

15. Zhevlakov K.A., Slin'ko A.M., Shestakov I.P., Shirshov A.I., *Ringsa That Are Nearly Associative.* Academic Press, New York, 1982
16. Zalar B., Theory of Hilbert triple Systems. *Yokohama Mathematical Journal,* Vol. 41, 1994.
17. Zalar B., Povabilo v jordanski svet. *Obzornik mat. fiz.,* 43, 1996.
18. Ward J.P., *Quaternions and Cayley Numbers.* Kluwer Academic Publishers, Dordrecht, 1997.