Reella vektorprodukter

Erik Darpö

Matematiska institutionen
Uppsala universitet
Box 480
SE-75106 Uppsala
erik.darpo@math.uu.se

Den vanliga vektorprodukten i det reella tredimensionella rummet har bland annat följande viktiga egenskaper:

- Den är bilinjär,
- produkten av två vektorer är vinkelrät mot dem båda, samt
- längden av en produkt är lika med arean av den parallellogram som spänns upp av de två faktorerna.

Om man tar dessa tre egenskaper som axiom, kan man ställa frågan om det går att införa vektorprodukter på andra reella vektorrum än $\mathbb{R}^3$. Det visar sig att svaret är ja precis i dimension 0, 1, 3 och 7, och att vektorprodukten är unik (upp till isomorfi) i varje dimension. Vi presenterar ett elementärt och vad det verkar nytt bevis för denna klassiska sats.

Definitioner och resultat

En *reell vektorproduktalgebra* är alltså ett euklidiskt rum[1] $V = (V, \langle\,\rangle)$ utrustat med en bilinjär multiplikationsavbildning

$$V \times V \to V,\ (u, v) \mapsto uv$$

som uppfyller axiomen

1. $\langle uv, v\rangle = 0, \quad \langle uv, u\rangle = 0,$
2. $\|uv\|^2 = \|u\|^2\|v\|^2 - \langle u, v\rangle^2$

för alla $u, v \in V$.[2] En *morfism* mellan två vektorproduktalgebror V och W är en ortogonal[3] avbildning $\varphi : V \to W$ som uppfyller $\varphi(uv) = \varphi(u)\varphi(v)$ för alla

[1] À priori ej nödvändigtvis ändligtdimensionellt

[2] Notera att inga andra krav ställs på multiplikationen än de ovan nämnda. Begreppet *algebra* avser i denna artikel enbart ett vektorrum med en bilinjär multiplikation, som ej förutsätts vara associativ.

[3] En linjär avbildning $\varphi : V \to W$ mellan euklidiska rum sägs vara *ortogonal* om $\langle\varphi(u), \varphi(v)\rangle = \langle u, v\rangle$ för alla $u, v \in V$.

$u, v \in V$. Vektorproduktalgebrorna V och W är *isomorfa* om det existerar en bijektiv morfism $\varphi : V \to W$.

Från villkor 2 följer att $\|u^2\|^2 = \|u\|^2\|u\|^2 - \langle u, u\rangle^2 = 0$, alltså $u^2 = 0$ för alla $u \in V$. Detta ger att $0 = (u+v)^2 = u^2 + uv + vu + v^2 = uv + vu$, så

$$uv = -vu \tag{1}$$

för alla $u, v \in V$, det vill säga att multiplikationen i V är antikommutativ. Detta betyder också de två ekvationerna $\langle uv, v\rangle = 0$ och $\langle uv, u\rangle = 0$ i villkor 1 är ekvivalenta, enbart en av dem är nödvändig för definitionen.

Ekvationen (1) tillsammans med punkt 1 i definitionen ger nu

$$\begin{aligned} 0 = \langle v(u+w), u+w\rangle &= \langle vu, u\rangle + \langle vu, w\rangle + \langle vw, u\rangle + \langle vw, w\rangle = \\ &= \langle vu, w\rangle + \langle vw, u\rangle = -\langle uv, w\rangle + \langle u, vw\rangle, \end{aligned}$$

det vill säga

$$\langle uv, w\rangle = \langle u, vw\rangle \tag{2}$$

för godtyckliga $u, v, w \in V$.

Slutligen ser vi att 2 i definitionen medför att

$$\|uv\| = 1 \quad \text{för varje ortonormalt par } u, v \in V. \tag{3}$$

Det är inte svårt att visa att ekvationerna (1)–(3) (tillsammans med bilinearitet) i själva verket ger en ekvivalent definition av en vektorproduktalgebra.

Vårt huvudresultat ges av Sats 1 nedan. Rummet $\mathbb{R}^n$ anses utrustat med standardskalärprodukten, så att $\langle e_i, e_i\rangle = 1$, och $\langle e_i, e_j\rangle = 0$ om $i \neq j$.

Sats 1. *Varje vektorproduktalgebra är isomorf med någon av nedanstående algebror:*

- *Den triviala algebran* $\{0\}$.
- *Den 1-dimensionella algebran* $\mathbb{R}$ *med multiplikation* $uv = 0$ *för alla* $u, v \in \mathbb{R}$.
- *Den 3-dimensionella algebran* $\mathbb{R}^3 = \mathrm{span}\{e_1, e_2, e_3\}$ *med multiplikation given av den övre vänsta delen av Tabell 1.*
- *Den 7-dimensionella algebran som ges av Tabell 1.*

Speciellt innebär Sats 1 att varje vektorproduktalgebra är ändligtdimensionell, och att två vektorproduktalgebror av samma dimension är isomorfa.[4]

Beviset för Sats 1 ges i nästa kapitel. Återstoden av detta kapitel ägnas åt sammansättningsalgebror och deras relation till vektorproduktalgebror, samt hur

[4]Det finns även en definition av vektorproduktalgebror över godtycklig grundkropp k av karaktäristik skild från 2 (se exempelvis Brown, Gray [1]). Den allmänna definitionen tillämpad på det reella fallet skiljer sig något från vår (den symmetriska formen $\langle\,\rangle$ förutsätts inte vara positivt definit). Med denna definition kommer det att finnas exakt två isomorfiklasser av vektorproduktalgebror i vardera dimension 1, 3 och 7.

$\cdot$	e_1	e_2	e_3	e_4	e_5	e_6	e_7
e_1	0	e_3	$-e_2$	e_5	$-e_4$	$-e_7$	e_6
e_2	$-e_3$	0	e_1	e_6	e_7	$-e_4$	$-e_5$
e_3	e_2	$-e_1$	0	e_7	$-e_6$	e_5	$-e_4$
e_4	$-e_5$	$-e_6$	$-e_7$	0	e_1	e_2	e_3
e_5	e_4	$-e_7$	e_6	$-e_1$	0	$-e_3$	e_2
e_6	e_7	e_4	$-e_5$	$-e_2$	e_3	0	$-e_1$
e_7	$-e_6$	e_5	e_4	$-e_3$	$-e_2$	e_1	0

Tabell 1: Den 7-dimensionella vektorproduktalgebran

denna relation kan utnyttjas för att bevisa Hurwitz sats om sammansättning av kvadratiska former (se nedan).

En *sammansättningsalgebra* (composition algebra) över $\mathbb{R}$ är ett euklidiskt rum $A \neq 0$ utrustat med en bilinjär multiplikation sådan att $\|uv\| = \|u\|\|v\|$ för alla $u, v \in A$. En morfism $\varphi : A \to B$ mellan sammansättningsalgebror är en ortogonal avbildning som uppfyller $\varphi(ab) = \varphi(a)\varphi(b)$ för alla $a, b \in A$. Sammansättningsalgebror uppstod ur det som idag kallas Hurwitz problem: För vilka $n \in \mathbb{N} \setminus \{0\}$ existerar det bilinjära former

$$\zeta_k = \zeta_k(\xi, \eta) = \sum_{i,j=1}^{n} a_{ij}^{(k)} \xi_i \eta_j, \quad a_{ij}^{(k)} \in \mathbb{R}, \quad k = 1, \ldots, n$$

så att

$$\zeta_1^2 + \cdots + \zeta_n^2 = (\xi_1^2 + \cdots + \xi_n^2)(\eta_1^2 + \cdots + \eta_n^2) \tag{4}$$

för alla $\xi_1, \ldots, \xi_n, \eta_1, \ldots, \eta_n \in \mathbb{R}$?

Givet sådana bilinjära former är det euklidiska rummet $\mathbb{R}^n$ med multiplikationen

$$(x_1, \ldots, x_n)(y_1, \ldots, y_n) = (\zeta_1(x, y), \ldots, \zeta_n(x, y)) \tag{5}$$

en sammansättningsalgebra. Omvänt; givet en sammansättningsalgebrastruktur på $\mathbb{R}^n$ kommer de bilinjära former ζ_k som definieras av (5) att uppfylla (4). Att lösa Hurwitz problem är alltså ekvivalent med att bestämma de $n \in \mathbb{N}$ för vilka det finns en sammansättningsalgebra A med $\dim A = n$.

Lösningen gavs av Hurwitz [5] år 1898, som visade att sådana former existerar precis när $n \in \{1, 2, 4, 8\}$. Vi skall visa att samma resultat följer från Sats 1, tillsammans med Sats 2 nedan, som ger ett starkt samband mellan vektorproduktalgebror och sammansättningsalgebror med identitetselement[5].

Först ser man, att givet en ändligtdimensionell sammansättningsalgebra A kan man konstruera en sammansättningsalgebra med etta av samma dimension: Betrakta ett godtyckligt element $a \in A$ med $\|a\| = 1$. Eftersom $\|ax\| = \|xa\| = \|a\|\|x\| = \|x\|$ för alla $x \in A$, så är de linjära avbildningarna $L_a : A \to A$, $x \mapsto ax$ och $R_a : A \to A$, $x \mapsto xa$ ortogonala, och därmed även inverterbara. Definiera

[5] Ett identitetselement (eller etta) i en algebra A är ett element $1_A \in A$ som uppfyller $1_A u = u 1_A = u$ för alla $u \in A$.

$x * y = R_a^{-1}(x)L_a^{-1}(y)$. Nu är $(A, *)$ en sammansättningsalgebra, ty $\|x * y\| = \|R_a^{-1}(x)L_a^{-1}(y)\| = \|R_a^{-1}(x)\|\|L_a^{-1}(y)\| = \|x\|\|y\|$. Vidare är $\dim(A, *) = \dim A$, och $a^2 * x = x = x * a^2$ för alla $x \in A$, så a^2 är en etta i $(A, *)$. För att lösa Hurwitz problem räcker det alltså att betrakta sammansättningsalgebror med etta.

Givet en vektorproduktalgebra V definieras en multiplikation på rummet $\mathbb{R} \times V$ enligt

$$(\alpha, v) \cdot (\beta, w) = (\alpha\beta - \langle v, w\rangle, \alpha w + \beta v + vw),$$

och en skalärprodukt $\langle(\alpha, v), (\beta, w)\rangle = \alpha\beta + \langle v, w\rangle$ (där $\langle v, w\rangle$ avser skalärprodukten i V). Vi använder $\mathcal{H}(V)$ som beteckning för $\mathbb{R}\times V$ utrustat med dessa strukturer.

Antag att A är en sammansättningsalgebra med identitetselement 1_A. Sätt $A_0 = 1_A^{\perp} = \{x \in A \mid \langle x, 1_A\rangle = 0\}$ och låt $P : A \to A_0$ vara den ortogonala projektionen av A på underrummet A_0. Vi definierar $\mathcal{I}(A) = (A_0, \times)$, där multiplikationen '$\times$' ges av $u\times v = P(uv)$. Rummet $\mathcal{I}(A)$ är euklidiskt, med den inducerade skalärprodukten från A. Följande sats säger att sammansättningsalgebror med etta och vektorprodukter väsentligen är ekvivalenta koncept. Den visades först av Brown och Gray [1, Theorem 4.1].

Sats 2.

1. *Om V är en vektorproduktalgebra, så är $\mathcal{H}(V)$ en sammansättningsalgebra med etta. Varje sammansättningsalgebra med etta är isomorf med $\mathcal{H}(V)$ för någon vektorproduktalgebra V.*

2. *Om A är en sammansättningsalgebra med etta, så är $\mathcal{I}(A)$ en vektorproduktalgebra. För varje vektorproduktalgebra V finns en sammansättningsalgebra A så att $\mathcal{I}(A)$ är isomorf med V.*

3. *För varje vektorproduktalgebra V gäller att $\mathcal{IH}(V)$ är isomorf med V, och för varje sammansättningsalgebra A med etta gäller att $\mathcal{HI}(A)$ är isomorf med A.*

Det är inte svårt att visa, att $\mathcal{H}$ och $\mathcal{I}$ i själva verket är funktorer, som definierar en kategoriekvivalens.

Bevis (skiss): Att visa att $\mathcal{H}(V)$ är en sammansättningsalgebra med identitetselement $(1, 0) \in \mathbb{R} \times V$, om V är en vektorproduktalgebra, är en ren rutinverifikation. För att visa att $\mathcal{I}(A)$ är en vektorproduktalgebra krävs lite förarbete.

Låt A vara en godtycklig sammansättningsalgbra, och $x, y, z \in A$. Då är

$$\begin{aligned}\|(x + y)z\|^2 = \|x + y\|^2\|z\|^2 &= (\|x\|^2 + \|y\|^2 + 2\langle x, y\rangle)\|z\|^2 = \\ &= \|x\|^2\|z\|^2 + \|y\|^2\|z\|^2 + 2\langle x, y\rangle\|z\|^2\end{aligned}$$

men även

$$\begin{aligned}\|(x + y)z\|^2 = \|xz + yz\|^2 &= \|xz\|^2 + \|yz\|^2 + 2\langle xz, yz\rangle = \\ &= \|x\|^2\|z\|^2 + \|y\|^2\|z\|^2 + 2\langle xz, yz\rangle.\end{aligned}$$

Således gäller

$$\langle xz, yz\rangle = \langle x, y\rangle\|z\|^2.$$

På samma sätt kan man linearisera denna identitet genom att ersätta z med $z+w$ och utveckla höger- och vänsterled var för sig. Detta ger identiteten

$$\langle xz, yw\rangle + \langle xw, yz\rangle = 2\langle x, y\rangle\langle z, w\rangle \quad \text{för alla } x, y, z, w \in A. \tag{6}$$

Låt nu A vara en sammansättningsalgebra med etta. Vi skall visa att $\mathcal{I}(A) = (A_0, \times)$ är en vektorproduktalgebra. Genom att sätta $y = w = 1_A$ i (6) får man för alla $x, z \in A_0$ att $\langle xz, 1_A\rangle = -\langle x, z\rangle$. Av detta följer att $\langle x^2, 1_A\rangle = -\|x\|^2 = -\|x^2\|$ och därmed

$$x^2 = -\|x\|^2 1_A, \quad x \times x = P(x^2) = 0. \tag{7}$$

Det senare implicerar anti-kommutativitet för '$\times$', vilket är villkor (1) i vår alternativa definition av en vektorproduktalgebra. Om istället $x, z \in A_0$ är ortonormala fås $\langle xz, 1_A\rangle = 0$ och därmed $\|x \times z\| = \|P(xz)\| = \|xz\| = \|x\|\|z\| = 1$, så även villkor (3) är uppfyllt. Ekvationen $\langle u \times v, w\rangle = \langle u, v \times w\rangle$ fås genom att sätta $z = 1_A,\ x, y, z \in A_0$ i (6).

En morfism $\varphi : A \to B$ mellan sammansättningsalgebror är i synnerhet en ortogonal avbildning, och $\varphi(1_A) = 1_B$. Därför inducerar φ en avbildning $\varphi_0 : A_0 \to B_0,\ v \mapsto \varphi(v)$ mellan de ortogonala komplementen till 1_A respektive 1_B. Man visar lätt att φ_0 är en morfism $\mathcal{I}(A) \to \mathcal{I}(B)$ av vektorproduktalgebror, som är bijektiv om och endast om φ är bijektiv. På samma ger varje morfism $f : V \to W$ mellan vektorproduktalgebror upphov till en morfism $\bar{f} : \mathcal{H}(V) \to \mathcal{H}(W),\ (\alpha, v) \mapsto (\alpha, f(v))$ som är bijektiv precis när f är det.

Om A är en sammansättningsalgebra med etta så är definierar $(\alpha, v) \mapsto \alpha 1_A + v$ en isomorfism $\mathcal{HI}(A) \to A$. För varje vektorproduktalgebra V gäller $\mathcal{IH}(V) = V$. □

Korollarium 3.

1. *Varje reell sammansättningsalgebra med etta är isomorf någon av följande algebror: De rella talen $\mathbb{R}$, de komplexa talen $\mathbb{C}$, kvaternionerna $\mathbb{H}$ och oktonionerna $\mathbb{O}$.*

2. *Det existerar bilinjära former $\zeta_k = \zeta_k(\xi, \eta),\ k = 1, \ldots, n$ som uppfyller (4) om och endast om $n \in \{1, 2, 4, 8\}$.*

Bevis. Enligt Sats 2 kommer varje sammansättningsalgebra med etta vara isomorf med $\mathcal{H}(V)$, där V är någon av de vektorproduktalgebror som anges i Sats 1. De algebror som uppkommer på detta sätt är precis $\mathbb{R}$, $\mathbb{C}$, $\mathbb{H}$ och $\mathbb{O}$.

Bilinjära former som uppfyller (4) existerar om och endast om det finns en sammansättningsalgebra A med etta sådan att $\dim A = n$, det vill säga om och endast om $n \in \{1, 2, 4, 8\}$. □

Klassen av reella sammansättningsalgebror med identitetselement sammanfaller med klassen av reella ändligtdimensionella alternativa[6] divisionsalgebror. Därmed ger vårt studium även ett nytt bevis för satsen att varje sådan divisionsalgebra är

[6] En algebra kallas *alternativ* om varje underalgebra som genereras av två element är associativ.

isomorf någon av $\mathbb{R}$, $\mathbb{C}$, $\mathbb{H}$ och $\mathbb{O}$. Originalbeviset till denna sats går tillbaka till Zorn [10].

Varje sammansättningsalgebra A med etta är utrustad med en naturlig involution: För $a = \alpha 1_A + x \in \mathbb{R}1_A \oplus A_0 = A$ definieras $\bar{a} = \alpha 1_A - x$. Enligt ekvation (7) är $x^2 = -\|x\|^2 1_A$ och därmed

$$a\bar{a} = (\alpha 1_A + x)(\alpha 1_A - x) = \alpha^2 1_A - x^2 = \alpha^2 1_A + \|x\|^2 1_A = \|a\|^2 \, 1_A.$$

Om vi identifierar $\mathbb{R}1_A \subset A$ med kroppen av skalärer $\mathbb{R}$, får vi alltså

$$\|a\| = \sqrt{a\bar{a}} \quad \text{för alla } a \in A.$$

Av Sats 2 följer att

$$vw = -\langle v, w\rangle 1_A + P(vw) \quad \text{för alla } v, w \in A_0.$$

Därmed gäller

$$v \times w = P(vw) = \frac{1}{2}[v, w] \tag{8}$$

där $[v, w] = vw - wv$ är kommutatormultiplikationen. Vektorprodukten på A_0 ges alltså av kommutatorn på A. Om A är associativ är den en Liealgebra under $[\ ]$, och av (8) följer då att även $\mathcal{I}(A) = (A_0, \times)$ är en Liealgebra.[7] I fallet $A = \mathbb{H}$ är $\mathcal{I}(A)$ isomorf med $\mathfrak{so}_3\mathbb{R}$.[8]

Den sjudimensionella vektorprodukten (här betecknad V_7) är i motsats till de lägredimensionella inte en Liealgebra. För att se detta, låt $u, v, w \in V_7$ vara ortonormala, och w även ortogonal mot uv (sådana vektorer existerar eftersom $\dim V_7 > 3$). Av Lemma 4:3 nedan följer att $(uv)w = (vw)u = (wu)v$. Dessutom är $\|(uv)w\| = 1$, och således

$$(uv)w + (vw)u + (wu)v = 3(uv)w \neq 0.$$

Den sjudimensionella vektorprodukten uppfyller alltså inte Jacobiidentiteten.

Vektorproduktalgebror studerades, och klassificerades, först av Eckmann [4] med hjälp av topologiska metoder. Sambandet med sammansättningsalgebror utnyttjas för en klassifikation av Massey [8], som även ger ett alternativt bevis baserat på resultat från algebraisk topologi. Vektorprodukter över allmänna kroppar av karaktäristik skild från två har behandlats av Brown och Gray [1] (av dem kallade “two-fold vector products”), som även de använder sambandet med sammansättningsalgebror för att nå en klassifikation. Rost [9] har bevisat att om d är dimensionen hos en vektorproduktalgebra över en kropp k, $\operatorname{char} k \neq 2$, så är $d(d-1)(d-3)(d-7) = 0$ i k. Till detta kan läggas ett flertal artiklar som behandlar sammansättningsalgebror, såsom [7], [6] och [2]. Se även författarens kommande artikel [3].

[7] En *Liealgebra* $\mathfrak{g} = (\mathfrak{g}, [\,])$ är en algebra vars multiplikation uppfyller $[x, x] = 0$ och $[[x, y], z] + [[y, z]x] + [[z, y], x] = 0$ (Jacobiidentiteten) för alla $x, y, z \in \mathfrak{g}$. Det är ett generellt resultat, att varje associativ algebra A är en Liealgebra under sin kommutator.

[8] En isomorfism $\mathcal{I}(\mathbb{H}) \to \mathfrak{so}_3\mathbb{R}$ ges av $x_1 i + x_2 j + x_3 k \mapsto \begin{pmatrix} 0 & x_3 & x_2 \\ -x_3 & 0 & x_1 \\ -x_2 & -x_1 & 0 \end{pmatrix}$.

Bevis för Sats 1

Idén i vårt bevis skiljer sig från de i de ovan nämnda publikationerna. Framställningen är elementär, och oberoende av sambandet med sammansättningsalgebror. Tanken är att konceptet med multiplikativt oberoende mängder som introduceras skall göra vektorproduktalgebror mer intiutivt lättförståeliga.

I återstoden av denna artikel kommer V och W alltid att beteckna reella vektorproduktalgebror. Nedanstående lemma är grundläggande för att förstå strukturen hos en vektorproduktalgebra.

Lemma 4. *Antag att $u, v \in V$ är ortonormala. Då gäller följande:*

1. $u(uv) = -v$,

2. $v(uv) = u$.

Om därutöver $w \in V$ är ortogonal mot u och v, så gäller även

3. $u(vw) = -(uv)w = (vu)w$.

I synnerhet är $\operatorname{span}\{u, v, uv\}$ *slutet under multiplikation, och därmed en underalgebra till V.*

Bevis. Eftersom u är en enhetsvektor, så följer från ekvationen (3) att den linjära avbildningen $u^\perp \to u^\perp$, $x \mapsto ux$ ortogonal.[9] Således gäller för alla $x \in V$ att

$$\langle x, u(uv)\rangle = \langle xu, uv\rangle = -\langle ux, uv\rangle = \langle ux, u(-v)\rangle = \langle x, -v\rangle.$$

Detta betyder att $u(uv) = -v$. Identiteten 2 är en omformulering av 1 med hjälp av antikommutativitetsvillkoret (1).

Från 1 får vi att

$$\begin{aligned}-\|u+w\|^2 v &= (u+w)\left((u+w)v\right) = (u+w)(uv+wv) = \\ &= u(uv) + u(wv) + w(uv) + w(wv) = \\ &= -\|u\|^2 v + u(wv) + w(uv) - \|w\|^2 v = \\ &= -\|u+w\|^2 v - u(vw) - (uv)w.\end{aligned}$$

Alltså gäller $u(vw) = -(uv)w$. □

Vårt grundläggande verktyg för att förstå vektorproduktalgebror är *multiplikativt oberoende mängder*. Vi säger att en ändlig delmängd $E \subset V$ är multiplikativt oberoende om varje $e \in E$ är normerad och ortogonal mot underalgebran $\langle E_e\rangle \subset V$ som genereras av $E_e = E \setminus \{e\}$.

Låt $E \subset V$ vara en multiplikativt oberoende mängd, och $e \in E$. Av Lemma 4 följer att $\langle E_e\rangle + \langle e\rangle + \langle E_e\rangle e \subset V$ är en underalgebra:

[9] Med $u^\perp$ avses det ortogonala komplementet till u i V, alltså $u^\perp = \{v \in V \mid \langle u, v\rangle = 0\}$.

Antag att $x, y \in \langle E_e \rangle$, $x = \alpha y + x'$ där $\alpha \in \mathbb{R}$ och $\langle x', y \rangle = 0$. Nu gäller

$$\begin{aligned}
xy &\in \langle E_e \rangle, \\
xe &\in \langle E_e \rangle e, \\
x(ye) &= (\alpha y + x')(ye) = -\alpha \|y\|^2 e - (x'y)e \in \langle e \rangle + \langle E_e \rangle e, \\
ee &= 0, \\
e(ye) &= y \in \langle E_e \rangle, \\
(xe)(ye) &= (ye)(ex) = ((ye)e)x = (-y)x = xy \in \langle E_e \rangle.
\end{aligned}$$

Alltså är $\langle E_e \rangle + \langle e \rangle + \langle E_e \rangle e$ slutet under multiplikation, och således en underalgebra i V. Eftersom $E \subset \langle E_e \rangle + \langle e \rangle + \langle E_e \rangle e \subset \langle E \rangle$ så betyder detta att $\langle E \rangle = \langle E_e \rangle + \langle e \rangle + \langle E_e \rangle e$.

Enligt antagande är $\langle e \rangle$ ortogonal mot $\langle E_e \rangle$. Dessutom gäller, för $x, y \in E_e$, att $\langle x, ye \rangle = \langle xy, e \rangle = 0$ och $\langle e, xe \rangle = -\langle e, ex \rangle = -\langle e^2, x \rangle = 0$. Alltså är även $\langle E_e \rangle e$ ortogonal mot både $\langle E_e \rangle$ och $\langle e \rangle$. Sammanfattningsvis gäller alltså att

$$\langle E \rangle = \langle E_e \rangle \oplus \langle e \rangle \oplus \langle E_e \rangle e \tag{9}$$

med summanderna i högerledet parvis ortogonala.

Lemma 5. *Om $E \subset V$ är en multiplikativt oberoende mängd och $f \in V$ normerad och ortogonal mot $\langle E \rangle$, så är även $E \cup \{f\}$ multiplikativt oberoende.*

Bevis. Enligt antagande är f ortogonal mot $\langle E \rangle$. Återstår att visa att varje $e \in E$ är ortogonal mot $\langle E_e \cup \{f\} \rangle$. Men $\langle E_e \cup \{f\} \rangle = \langle E_e \rangle \oplus \langle f \rangle \oplus \langle E_e \rangle f$. Vi vet enligt antagande att e är ortogonal mot $\langle E_e \rangle$, och mot f. Dessutom är $\langle e, xf \rangle = \langle ex, f \rangle = 0$ för alla $x \in \langle E_e \rangle$, varför e är ortogonal även mot $\langle E_e \rangle f$. □

Som konsekvens av lemmat får vi att om V är ändligtdimensionell, så finns en multiplikativt oberoende mängd $E \subset V$ sådan att $V = \langle E \rangle$. En sådan mängd kallar vi en *multiplikativ bas* för V.

Den tomma mängden är multiplikativt oberoende, och $\langle \emptyset \rangle = \{0\}$, det vill säga $\dim\langle \emptyset \rangle = 0$. Av (9) följer att $\dim\langle E \rangle = 2\dim\langle E_e \rangle + 1$ för varje multiplikativt oberoende mängd E och varje vektor $e \in E$. Därför gäller att $\dim\langle E \rangle = 2^n - 1$, där n är antalet element i E.

Antag nu att $E = \{u, v, w, z\} \subset V$ är en multiplikativt oberoende mängd (så $\dim\langle E \rangle = 15$). Vi får

$$u(v(wz)) = u((wv)z) = ((wv)u)z = -((vw)u)z$$

men även

$$u(v(wz)) = (vu)(wz) = (w(vu))z = ((vw)u)z.$$

Alltså är $u(v(wz)) = 0$, vilket motsäger att E är multiplikativt oberoende. Således kan ingen multiplikativt oberoende mängd innehålla mer än 3 element. Detta utesluter existensen av oändligtdimensionella vektorproduktalgebror, eftersom i en sådan algebra skulle det vara möjligt att konstruera multiplikativt oberoende mängder med godtyckligt många element. Vidare betyder det att varje vektorproduktalgebra har dimension 0, 1, 3 eller 7.

Vi visar nu med induktion att två vektorproduktalgebror av samma dimension måste vara isomorfa. Basfallet $V = W = \langle\emptyset\rangle = \{0\}$ är klart. Låt E och F vara multiplikativa baser för V respektive W, $\dim V = \dim W$, och $e \in E$, $f \in F$. Det följer att E och F har samma antal element. Enligt induktionsantagandet finns det en isomorfism $\varphi : \langle E_e\rangle \to \langle F_f\rangle$. Vi definierar nu $\tilde{\varphi} : V \to W$ genom $\tilde{\varphi}(x + \lambda e + ye) = \varphi(x) + \lambda f + \varphi(y)f$, för $x, y \in \langle E_e\rangle$, $\lambda \in \mathbb{R}$. Man verifierar direkt att $\tilde{\varphi}$ är en morfism. Eftersom φ är bijektiv så följer av konstruktionen att $\tilde{\varphi}$ också är det. Avbildningen $\tilde{\varphi} : V \to W$ är alltså en isomorfism.

Å andra sidan är det inte svårt att kontrollera att $V = \mathbb{R}^7$ med multiplikation given av Tabell 1 uppfyller axiomen för en vektorproduktalgebra. Givet detta är det också klart att $\operatorname{span}\emptyset$, $\operatorname{span}\{e_1\}$ och $\operatorname{span}\{e_1, e_2, e_3\}$ är underalgebror (och därmed själva vektorproduktalgebror) av de typer som anges i satsen.

Vi har visat att varje vektorproduktalgebra har samma dimension som någon av de ovan nämnda (nämligen 0, 1, 3 eller 7), och att två vektorproduktalgebror av samma dimension är isomorfa. Därför måste varje vektorproduktalgebra vara isomorf med någon av dessa fyra, vilket är påståendet Sats 1.

Referenser

[1] Robert B. Brown and Alfred Gray. Vector cross products. *Commentarii Mathematici Helvetici*, 42:222–236, 1967.

[2] J. A. Cuenca Mira. On composition and absolute-valued algebras. *Proceedings of the Royal Society of Edinburgh*, 136A(4):717–731, 2006.

[3] Erik Darpö. Vector product algebras. To appear.

[4] Beno Eckmann. Stetige Lösungen linearer Gleichungssysteme. *Commentarii Mathematici Helvetici*, 15:318–339, 1942–43.

[5] B. Hurwitz. Über die Komposition der quadratischen Formen. *Mathematische Annalen*, 88:1–25, 1922.

[6] Nathan Jacobson. Composition algebras and their automorphisms. *Rend. Circ. Mat. Palermo*, 7(2):55–80, 1958.

[7] I. Kaplansky. Infinite-dimensional quadratic forms admitting composition. *Proceedings of the American mathematical society*, 4(6):956–960, 1953.

[8] W.S. Massey. Cross products of vectors in higher dimensional spaces. *American mathematical monthly*, 90(10):697–701, 1983.

[9] Markus Rost. On the dimension of a composition algebra. *Documenta Mathematica*, 1:209–214, 1996.

[10] Max Zorn. Theorie der alternativen Ringe. *Abh. Math. Sem. Hamburg*, 8:123–147, 1931.