סמינר בנושא משפט הורוויץ (Hurwitz's Theorem)

בנימין פוקס

מרץ 2014

אדר ב' ה'תשע"ד

עבודה סמינריונית במסגרת הקורס מבנים אלגבריים

מדריך בעבודה: ד"ר עופר הדס

תוכן עניינים

1. הצגת הבעיה

הבעיה היא: לאלו ערכים של n קיימות משוואות מהצורה $(\sum_{i=1}^{n} x_i^2)(\sum_{i=1}^{n} y_i^2)=(\sum_{i=1}^{n} z_i^2)$, כאשר z_i ביטויים בילינאריים במשתנים x , y ?

במקרה $n=1$ יש שוויון טריביאלי: $x_1^2 y_1^2=(x_1 y_1)^2$

במקרה $n=2$ יש את השוויון $(x_1^2+x_2^2)(y_1^2+y_2^2)=(x_1 y_1-x_2 y_2)^2+(x_1 y_2+x_2 y_1)^2$.

גם ידוע שוויון במקרה $n=4$, ולשוויון הזה יש חלק מרכזי בהוכחת המשפט של לגרנז' שכל מספר טבעי הוא הסכום של לא יותר מ-4 ריבועים.

(ניתן לקבל את הנוסחה למקרה $n=4$ מנוסחה (5) בעמוד 37 של פרק 14 בקורס מבנים אלגבריים, יחד עם שאלה 14.27ד ושאלה 14.30.)

גם כן, ידוע שיש שיוויון כזה (די מסובך) גם במקרה $n=8$.

השאלה שנשאלת היא האם יש עוד משוואות כאלה. בשנת 1898, המתמטיקאי הגרמני אדולף הורוויץ הוכיח שהתשובה היא שאין משוואות נוספות כאלה. כדי להוכיח את זה הוא הוכיח משפט הרבה יותר חזק, שמתקיים לא רק על $\mathbb{R}$, אלה מעל שדה כלשהו בעל מאפיין שונה מ-2.

2. למות והגדרות עיקריים

2.1 תבניות

יהי F שדה.

באופן הכי כללי, לכל k טבעי, פונקציה k-לינארית היא פונקציה $f: V_1 \times V_2 \times \ldots \times V_k \rightarrow W$ כאשר $V_1, V_2, \ldots, V_k$ הם מרחבים לינאריים מעל שדה F , וכאשר לכל $j \in \{1,\ldots,k\}$ ולכל $v_1, v_2, \ldots, v_k \in V$ הפונקציה $f(v_1,\ldots,v_{j-1}, x, v_{j+1},\ldots, v_k)$ היא פונקציה לינארית של x . (מהמרחב V_j למרחב W .)

בפרט, עבור $k=1$ זאת פשוט פונקציה לינארית. עבור $k=2$ ו- $W=F$, נקרא לפונקציה כזו תבנית בילינארית. לרוב נשתמש בהוכחה שלנו בפונקציות בילינאריות וריבועיות, שנגדיר אותן כך:

פונקציה Q היא תבנית ריבועית אם יש תבנית בילינארית סימטרית S כך ש- $Q(x)=S(x,x)$ לכל x .
נסמן $B(x,y)=2S(x,y)$, ונקבע ש B היא התבנית הבילינארית של Q , וש- Q הוא התבנית הריבועית של B .
זאת התאמה חד-חד-ערכית, כי

$$Q(x+y)=S(x+y,x+y)=S(x,x)+S(x,y)+S(y,x)+S(y,y)=$$
$$=Q(x)+2S(x,y)+Q(y)$$

ולכן $2S(x,y)=Q(x+y)-Q(x)-Q(y)$, ובכך $B(x,y)=Q(x+y)-Q(x)-Q(y)$, כלומר נוכל גם לעבור מ Q ל- B באופן חד-ערכית.
מכך נסיק גם ש-

$$Q(x+y)=Q(x)+B(x,y)+Q(y) \qquad (2.1.1)$$

אם Q היא תבנית ריבועית, ו- α סקלר, נסיק מהבלינאריות של התבנית הבילינארית שלה כי

$$Q(\alpha x)=\alpha^2 Q(x) \qquad (2.1.2)$$

הגדרה:

תבנית בילינארית $B(x,y)$ נקראת <u>בלתי מנוונת</u> אם לכל $u\neq 0$ יש v כך ש- $B(u,v)\neq 0$. נקרא לתבנית ריבועית בלתי מנוונת אם ורק אם התבנית הבילינארית שלה בלתי מנוונת.

דוגמה:

אם השדה הוא $\mathbb{R}$ ו- Q היא תבנית חיובית לחלוטין ($Q(x)>0$ לכל $x\neq 0$) אז $B(x,x)>0$ לכל $x\neq 0$ ולכן ברור שלכל $x\neq 0$ יש y כך ש- $B(x,y)\neq 0$. במקרה כזה B היא מכפלה פנימית.

טענה: אם B תבנית בילינארית בלתי מנוונת ויש v,w כך ש- $B(u,v)=B(u,w)$ לכל u ,
אז $v=w$. (2.1.3)

הוכחה:

נעביר אגפים, ומהבילינאריות של B , נמצא ש- $B(u,v-w)$ לכל u . כי B בלתי מנוונת, נסיק ש- $v-w=0$, ולכן $v=w$.
מ.ש.ל.

הגדרה: אם C תת-מרחב של A , $C^{\perp}$ היא תת-מרחב המכיל כל איבר x ב- A כך ש- $B(x,y)=0$ לכל $y\in C$.

טענה: אם C תת-מרחב של A , ו- Q בלתי מנוונת על A , אז $dim\,C^{\perp}+dim\,C=dim\,A$.

הוכחה:

נכתוב את התבנית B בכתיבה מטריצית, לפי משפט X.7 בקורס אלגברה לינארית II.

כלומר, $B(x,y)=xMy$ לאיזשהו מטריצה M מסדר $n\times n$, כאשר $n=dim\,A$.

יהי $\{e_1,e_2,..,e_k\}$ בסיס ל- C . נסמן ב- w_i את הוקטור e_iM .

נסמן את המטריצה $N=\begin{bmatrix} \underline{w_i} \\ \underline{w_2} \\ \cdots \\ \underline{w_k} \end{bmatrix}$.

יהי P מרחב הפתרונות של N , כלומר $P=\{y\in A:Ny=0\}$.

אם $y\in C^{\perp}$ אז $B(e_i,y)=0$ לכל e_i , בגלל ש $e_i\in C$.

אם $B(e_i,y)=0$ לכל e_i , אז מפני שנוכל לכתוב כל איבר x ב- C כצירוף לינארי של הבסיס $\{e_1,e_2,..,e_k\}$, אז מהליניאריות של B נקבל ש- $B(x,y)=0$ לכל $x\in C$.

כלומר,

$$C^{\perp}=\{e_1,e_2,..,e_k\}^{\perp}$$

אם $c\in P$, אז $Nc=0$, ולכן $w_ic=0$ לכל i , כלומר $e_iMc=0$ לכל i .

בכך, $B(e_i,c)=e_iMc=0$ לכל i , ולכן
$c\in\{e_1,e_2,..,e_k\}^{\perp}=C^{\perp}$.
לכן מצאנו כי $P\subseteq C^{\perp}$.

אם $c\in\{e_1,e_2,..,e_k\}^{\perp}=C^{\perp}$, אז $0=B(e_i,c)=e_iMc$ לכל i , כלומר $w_ic=0$ לכל i , ולכן $Nc=0$, כלומר $c\in P$.

לכן מצאנו כי $P \supseteq C^{\perp}$.

בכך $P = C^{\perp}$.

לפי משפט V.45 בקורס אלגברה לינארית I, $dim\, P = n - dim\, Sp\{w_{1,} \ldots, w_k\}$, כי המטריצה N בעלת n עמודים.

$$Sp\{w_1, \ldots, w_k\} = \{\alpha_1 w_1 + \ldots + \alpha_k w_k \ : \ \text{סקלרים} \ \alpha_{1,} \ldots, \alpha_k\}$$

$\{w_{1,} \ldots, w_k\}$ פורשת את הקבוצה הזו, ואם $\alpha_1 w_1 + \ldots + \alpha_k w_k = 0$, אז $\sum_{i=i}^{k} \alpha_i e_i M = 0$, ולכן $(\sum_{i=1}^{k} \alpha_i e_i) M = 0$.

אבל מפני ש- B בלתי מנוונת, יש $x \in A$ כך ש $(\sum_{i=1}^{k} \alpha_i e_i) M\, x \neq 0$, כלומר $0\, x \neq 0$, וזה סתירה.

לכן $\{w_{1,} \ldots, w_k\}$ בלתי תלויה לינארית, ולכן $\{w_{1,} \ldots, w_k\}$ בסיס לקבוצה $Sp\{w_{1,} \ldots, w_k\}$, ולכן $dimSp\{w_{1,} \ldots, w_k\} = k$.

בכך, $dim\, C^{\perp} = dimP = n - dimSp\{w_{1,} \ldots, w_k\} = n - k$, ולכן, כי $dimA = n, dimC = k$,

$$dim\, C^{\perp} + dim C = dim\, A$$

מ.ש.ל.

מסקנה:

אם C תת-מרחב של A , ו- Q בלתי מנוונת על A , ו- $C \cap C^{\perp} = \{0\}$, אז $A = C \oplus C^{\perp}$.
(2.1.4)

הוכחה:

לפי הטענה האחרונה, $dim\, C^{\perp} + dim C = dim\, A$,יחד אם הנתון $C \cap C^{\perp} = \{0\}$, נסיק ש- $A = C \oplus C^{\perp}$.
מ.ש.ל.

2.2 האסוציאטור והקומוטטור

אלגברה היא מרחב וקטורי A יחד עם פעולת כפל $A \times A \rightarrow A$ שהיא פונקציה בילינארית.

הגדרה:

באלגברה (לא בהכרח אסוציאטיבית) A , נגדיר לכל $a, b, c \in A$ את האסוציאטור

$$[a, b, c] = (ab)c - a(bc)$$

$[a, b, c] = 0$ לכל $a, b, c \in A$ אם ורק אם A אסוציאטיבית.

האסוציאטור הוא פונקציה טרילינארית, כלומר:

$$[a, b, \alpha c] = [a, \alpha b, c] = [\alpha a, b, c] = \alpha [a, b, c]$$

(2.2.1)

$$[a+d, b, c] = [a, b, c] + [d, b, c]$$
$$[a, b+d, c] = [a, b, c] + [a, d, c]$$
$$[a, b, c+d] = [a, b, c] + [a, b, d]$$

הגדרה: באלגברה A , נגדיר לכל $a, b \in A$ את הקומוטטור $[a, b] = ab - ba$. (2.2.2)

$[a, b] = 0$ לכל $a, b \in A$ אם ורק אם A קומוטטיבית. הקומוטטור הוא פונקציה בילינארית.

אם יש ל- A יחידה, אז ברור כי

(2.2.3)

$$[x, y, 1] = [x, 1, y] = [1, x, y] = 0 \quad \text{לכל} \quad x, y \in A$$

וש- $[1, x] = [x, 1] = 0$ לכל $x \in A$. (2.2.4)

לכל סקלר α , נסיק כי $[x, y, \alpha 1] = [x, \alpha 1, y] = [\alpha 1, x, y] = 0$ לכל $x, y \in A$, (2.2.5)

וש- $[\alpha 1, x] = [x, \alpha 1] = 0$ לכל $x \in A$. (2.2.6)

2.3 אלגברה אלטרנטיבית

הגדרה: נגדיר אלגברה אלטרנטיבית כאלגברה שמקיימת את המשוואות $[x, x, y] = [y, x, x] = 0$ לכל $x, y \in A$. (2.3.1)

דוגמה:

כל אלגברה אסוציאטיבית היא אלגברה אלטרנטיבית.

טענה:

באלגברה אלטרנטיבית, האסוציאטור משנה סימן תחת חילוף של שני איברים סמוכים.

הוכחה:

מ-2.3.1, 2.2.1:

$$[x,x,z]+[x,y,z]+[y,y,z]+[y,x,z]=[x+y,x+y,z]=0$$

ולכן,

$$[x,y,z]+[y,x,z]=0$$

גם כן,

$$0=[y,x+z,x+z]=[y,x,x]+[y,z,z]+[y,x,z]+[y,z,x]=[y,z,x]+[y,x,z]$$

בזאת הוכחנו שחילוף של שני איברים סמוכים משנה את הסימן.

מ.ש.ל.

מסקנה:

לכל $\sigma\in S_3$:

$$[x_1,x_2,x_3]=(-1)^{\sigma}[x_{\sigma 1},x_{\sigma 2},x_{\sigma 3}]$$

כאשר $(-1)^{\sigma}$ הוא הסימן של σ.

הוכחה:

מהטענה הקודמת, ידוע שהתמורות $(1,2)$ ו- $(2,3)$ מחליפות את הסימן של האסוציאטור. אבל $\{(1,2),(2,3)\}$ יוצר את S_3 , ולכן הסימן מוחלף מספר פעמים המתאים לסימן של σ.

מ.ש.ל.

משפט: ב-A (אלגברה אלטרנטיבית כלשהי):

אם $x,y,u\in A$:

א)

$$x^2 y=x(xy) \tag{2.3.2}$$

ב)

$$yx^2=(yx)x \tag{2.3.3}$$

ג)

$$(xy)x=x(yx) \tag{2.3.4}$$

ובכך נסמן $xyx=(xy)x=x(yx)$.

ד)

$$(ux)y+x(yu)=u(xy)+(xy)u \tag{2.3.5}$$

ה)

$$(u^2 x) y+(ux)(yu)=u((ux) y)+((ux) y)u \tag{2.3.6}$$

ו)

$$(ux)(yu)+x(yu^2)=u(x(yu))+(x(yu))u \tag{2.3.7}$$

ז)

$$(u^2 x) y+2(ux)(yu)+x(yu^2)=u^2(xy)+2u(xy)u+(xy)u^2 \tag{2.3.8}$$

ח)

$$(ux)(yu)=u(xy)u \tag{2.3.9}$$

השוויון האחרון נקרא שוויון מופנג, על שם רות מופנג, מתמטיקאית גרמנייה שגילתה את השוויון הזה.

הוכחה:

מ-2.3.1 נקבל ש $[x,x,y]=[y,x,x]=0$.

ולכן נסיק מהמסקנה שלפני המשפט ש $[x,y,x]=-[y,x,x]=-[x,x,y]=0$.

בכך יש לנו את הזהויות 2.3.2, 2.3.3, 2.3.4:

$$x^2 y=x(xy) \Leftarrow x^2 y-x(xy)=0 \Leftarrow [x,x,y]=0$$
$$y x^2=(yx)x \Leftarrow (yx)x-yx^2=0 \Leftarrow [y,x,x]=0$$
$$(xy)x=x(yx) \Leftarrow (xy)x-x(yx)=0 \Leftarrow [x,y,x]=0$$

תמורה באורך 3 היא זוגית, ולכן $[u,x,y]=[x,y,u]$, כלומר $(ux)y+x(yu)=u(xy)+(xy)u$, שזה 2.3.5.

כדי לקבל את 2.3.6, נציב ב-2.3.5 את ux במקום x ונקבל

$$(u^2 x) y+(ux)(yu)=u((ux) y)+((ux) y)u$$

כדי לקבל את 2.3.7, נציב ב-2.3.5 את yu במקום y ונקבל

$$(ux)(yu)+x(yu^2)=u(x(yu))+(x(yu))u$$

נקבל את 2.3.8 אם נוסיף את 2.3.6 ו-2.3.7 זו לזו:

$$(u^2 x) y+2(ux)(yu)+x(yu^2)=u((ux) y)+((ux) y)u+u(x(yu))+(x(yu))u$$

ואז נקבל:

$$(u^2 x) y+2(ux)(yu)+x(yu^2)=u[(ux) y+x(yu)]+[(ux) y+x(yu)]u$$

נסיק מכך, לפי 2.3.5, כי

$$(u^2 x) y+2(ux)(yu)+x(yu^2)=u[u(xy)+(xy)u]+[u(xy)+(xy)u]u$$

ולכן

$$(u^2 x)\,y+2(ux)(yu)+x(yu^2)=u^2(xy)+2u(xy)u+(xy)u^2$$

שזאת 2.3.8.

אם נציב ב-2.3.5 את u^2 במקום u, נקבל ש- $(u^2 x)\,y+x(y\,u^2)=u^2(xy)+(xy)u^2$.

נחסיר את זה מ 2.3.8 ונקבל ש-

$$2(ux)(yu)=2u(xy)u$$

ולכן מצאנו ש- $(ux)(yu)=u(xy)u$, שזה 2.3.9.

מ.ש.ל.

3. הגדרת "אלגברת הרכבה"

תהי A מרחב וקטורי מממד סופי עם מאפיין שונה מ-2, ותהי Q תבנית ריבועית בלתי מנוונת מעל A.

הגדרה: Q נקראת תבנית מאפשרת הרכבה אם ורק אם יתכן להגדיר מכפלה בלינארית כך ש $Q(x)Q(y)=Q(xy)$ לכל $x,y\in A$.

הגדרה: נגדיר אלגברת הרכבה כזוג (A,Q) כאשר A אלגברה עם יחידה, ו- Q תבנית בלתי מנוונת עליה, כך ש- $Q(x)Q(y)=Q(xy)$ לכל $x,y\in A$.

טענה: אם Q מאפשר הרכבה, אז ניתן להגדיר מכפלה בלינארית עם יחידה כך ש- $Q(x)Q(y)=Q(xy)$ לכל $x,y\in A$.

הוכחה:

Q מאפשר הרכבה, ולכן קיים אלגברה A כך ש $Q(x)Q(y)=Q(xy)$ לכל $x,y\in A$. אבל לא בהכרח יש ל- A יחידה.

נבנה מכפלה על איברי A כך שתהיה לנו אלגברה עם יחידה על איברי A שעדיין תקיים את התנאי על Q ביחס למכפלה החדשה.

נבחר $v\in A$ כלשהי כך ש $Q(v)\neq 0$, ונגדיר $u=(Q(v))^{-1}v^2$.

בכך, $Q(u)=Q((Q(v))^{-1}v^2)=Q(v)^{-2}Q(v^2)$ לפי 2.1.2,

ולכן, כי $Q(v)Q(v)=Q(vv)=Q(v^2)$, נסיק ש $Q(u)=Q(v)^{-2}Q(v)^2=1$.

בכך, $Q(xu)=Q(x)Q(u)=Q(x)=Q(u)Q(x)=Q(ux)$ לכל x .

לכן, לכל $x, y\in A$,

$$B(ux,uy)=Q(u(x+y))-Q(ux)-Q(uy)=Q(x+y)-Q(x)-Q(y)=B(x,y)$$

אם $ux=0$ אז נסיק ש- $B(x,y)=B(ux,uy)=B(0,uy)=0$ לכל y, וכי B בלתי מנוונת, נובע ש- $x=0$.

לכן, $ker\, u_L(x)=\{0\}$, כאשר u_L הוא הטרנספורמציה הלינארית $u_L(x)=ux$, ולכן u_L הפיכה.
באופן דומה, גם $u_R=xu$ טרנספורמציה לינארית הפיכה.

נגדיר: $x*y=(u_R^{-1}x)(u_L^{-1}y)$.

המכפלה הזאת מתקיימת את התנאי $Q(x*y)=Q(x)Q(y)$, כי

$$Q(x*y)=Q(u_R^{-1}x)Q(u_L^{-1}y)=Q(x)Q(y).$$

בגלל ש- $u_L^{-1}u^2=u_L^{-1}(u_L u)=u$ ו- $u_R^{-1}u^2=u_R^{-1}(u_R u)=u$, נסיק ש:

$$u^2*x=(u_R^{-1}u^2)(u_L^{-1}x)=u(u_L^{-1}x)=x$$

$$x*u^2=(u_R^{-1}x)(u_L^{-1}u^2)=(u_R^{-1}x)u=x$$

ובכך u^2 היא יחידה ביחס לכפל הזה.

כלומר, מצנאו שקיימת מכפלה בלינארית עם יחידה כך ש $Q(x*y)=Q(x)Q(y)$ לכל $x, y\in A$.
לכן, מצאנו אלגברה A' כך ש- (A',Q) אלגברת הרכבה.
מ.ש.ל.

תהי (A,Q) אלגברת הרכבה. נמצא כמה זהויות לגבי אלגברת ההרכבה הזו.

למה: הזהויות האלה קיימות בכל אלגברת הרכבה (A,Q) , כאשר B היא התבנית הבילינארית של Q (כלומר $B(x,y)=Q(x+y)-Q(x)-Q(y)$):

$$Q(1)=1 \tag{3.1}$$

$$Q(x+z)Q(y)=Q(xy+zy) \tag{3.2}$$

(3.3) $$B(xy,zy)=B(x,z)Q(y)$$

(3.4) $$B(xy,xw)=Q(x)B(y,w)$$

(3.5) $$B(xy,zw)+B(zy,xw)=B(x,z)B(y,w)$$

(3.6) $$B(yx,wz)+B(yz,wx)=B(x,z)B(y,w)$$

הוכחה:

מהנוסחה ש- $Q(x)Q(y)=Q(xy)$, נסיק כי $Q(x)Q(1)=Q(x)$ לכל $x\in A$, ולכן $Q(1)=1$.
($Q(x)\neq 0$ לאיזשהו x , כי ידוע ש- Q בלתי מנוונת.) בכך הוכחנו את 3.1.

מהנוסחה $Q(x)Q(y)=Q(xy)$ נסיק גם כי $Q(x+z)Q(y)=Q((x+z)y)=Q(xy+zy)$, שזה 3.2.

נקבל מכך ש-

$$\begin{aligned}
B(xy,zy)&=Q(xy+zy)-Q(xy)-Q(zy)=\\
&=Q(x+z)Q(y)-Q(x)Q(y)-Q(z)Q(y)=\\
&=(Q(x+z)-Q(x)-Q(z))Q(y)=\\
&=B(x,z)Q(y)
\end{aligned}$$

ובכך הוכחנו את 3.3. בדרך סימטרית ניתן להוכיח את 3.4.

ניקח את משוואה 3.3 ונציב $y+w$ במקום y , ונקבל

$$B(x(y+w),z(y+w))=B(x,z)Q(y+w)$$

B בילינארית, ולכן

$$B(xy,zy)+B(xw,zy)+B(xy,zw)+B(xw,zw)=B(x,z)Q(y+w)$$

אבל מ-3.3 ו-3.4 נובע מזה ש-

$$B(x,z)Q(y)+B(xw,zy)+B(xy,zw)+B(x,z)Q(w)=B(x,z)Q(y+w)$$.

נעביר אגפים, ונציב $B(y+w)=Q(y+w)-Q(y)-Q(w)$, ונקבל

$$B(xy,zw)+B(zy,xw)=B(x,z)B(y,w)$$

שזה 3.5, והצד הימיני לא משתנה כשנחליף את x עם y ו- z עם w , ולכן:

$$B(x,z)B(y,w)=B(yx,wz)+B(yz,wx)$$

שזה 3.6.
מ.ש.ל.

4. מציאת אינוולוציה על האלגברה

תחילה נגדיר את המושג של אינוולוציה.

הגדרה: אינוולוציה היא פונקציה לינארית, שהיא אנטיהומומורפיזם, והיא הפונקציה הנגדית של עצמה:
כלומר $j:A\rightarrow A$ אינוולוציה של האלגברה A מעל השדה F , אם ורק אם j טרנספורמציה לינארית כך שלכל $x,y\in A$, $j(xy)=j(y)j(x)$, ולכל $x\in A$, $j(j(x))=x$.

הגדרה: כאשר Q היא תבנית ריבועית על אלגברה עם יחידה A , ו- B התבנית הבילינארית המתאימה, נסמן $T(x)=B(x,1)$, שזה תבנית לינארית על A .

לצורך ההוכחה בסעיף הבא של האלטרנטיביות של אלגברת הרכבה, נצטרך פונקציה שהיא הרחבה של הרעיון הידוע של הצמוד על המספרים המרוכבים.

נגדיר אותה כך:

הגדרה: תהי (A,Q) אלגברת הרכבה.
נסמן $\bar{x}=j(x)=T(x)1-x$

(כלומר $\bar{x}=B(x,1)1-x$.)

נוכיח כי יש לזה את התכונות הידועות של הצמוד, כאשר $Q(x)1$ היא מתפקדת כ-"הנורמה בריבוע של x " ($|x|^2$) . בפרט נראה כי היא אינוולוציה.

משפט: j היא אינוולוציה, כלומר:

א) j היא לינארית.

ב) $x=j(j(x))=\bar{\bar{x}}$ (4.1)

ג) $\overline{xy}=\bar{y}\,\bar{x}$ (כלומר j אנטיהומומורפיזם.)

הוכחה:

ברור ש- j לינארית. נוכיח כי $x=j(j(x))=\bar{\bar{x}}$.

$$\begin{aligned}j(j(x))&=j(T(x)1-x)=j(T(x)1)-j(x)=\\&=(T(T(x)1)1-T(x)1)-(T(x)1-x)=\\&=T(T(x)1)1-T(x)(1+1)+x=\\&=T(x)T(1)1-2\cdot T(x)1+x=x\end{aligned}$$

כאשר השיוויונות האחרונים נובעים מהלינאריות של T , $T(T(x)1)=T(x)T(1)$, ומהזהות

$$\begin{aligned}T(1)&=B(1,1)=Q(1+1)-Q(1)-Q(1)=Q(1\cdot 2)-2Q(1)=\\&=2^2Q(1)-2Q(1)=2Q(1)=2\end{aligned}$$.

לפני שנוכיח כי ל- j יש גם את שאר התכונות של אינוולוציה, נוכיח טענה, למה, ומשפט חשוב.

טענה: $Q(x)=Q(\bar{x})$ לכל $x\in A$. (4.2)

הוכחה:

$$\begin{aligned}Q(j(x))&=Q(T(x)1-x)=\\&=Q(T(x)1)+B(T(x),-x)+Q(-x)=\\&=T(x)^2Q(1)-T(x)B(1,x)+Q(x)=\\&=T(x)^2-T(x)T(x)+Q(x)=Q(x)\end{aligned}$$

מ.ש.ל.

למה:

$$B(x,\bar{y}z)=B(yx,z) \tag{4.3}$$
$$B(x,z\bar{y})=B(xy,z) \tag{4.4}$$

הוכחה:

$$B(x,j(y)z)=B(x,B(y,1)z-yz)=B(y,1)B(x,z)-B(x,yz)=$$
$$=B(yx,z)+B(yz,x)-B(x,yz)= \quad \text{(לפי 3.5)}$$
$$=B(yx,z)$$

וזה 4.3. בדרך סימטרית נוכל להוכיח את 4.4.

מ.ש.ל.

בדומה לכך שמספר מרוכב כפול הצמוד שלו הוא הנורמה שלו בריבוע, נוכיח את המשפט הבא:

משפט:

$$x\bar{x}=\bar{x}x=Q(x)1 \tag{4.5}$$

הוכחה:

מ 4.3 ו-3.4, נמצא כי $Q(x)B(1,y)=B(x,xy)=B(\bar{x}x,y)$.

לכן $B(Q(x)1,y)=B(\bar{x}x,y)$ (כי B בילינארית).

זה נכון לכל y , וכי Q אינה מנוונת, B אינה מנוונת, ולכן נסיק לפי 2.1.3 כי $\bar{x}x=Q(x)1$.

אם נציב $\bar{x}$ במקום x , נקבל מ-4.2 ש- $x\bar{x}=\bar{\bar{x}}\bar{x}=Q(\bar{x})1=Q(x)1$.

לכן, $x\bar{x}=\bar{x}x=Q(x)1$.

מ.ש.ל.

מסקנה:

$$(\bar{x}x)y=Q(x)y=\bar{x}(xy) \tag{4.6}$$
$$y(x\bar{x})=Q(x)y=(yx)\bar{x} \tag{4.7}$$

הוכחה:

$B(\bar{x}(xy),z)=B(xy,xz)=Q(x)B(y,z)=B(Q(x)y,z)$, לפי 3.4 ו-4.3.

שוב נשתמש ב-2.1.3, ונקבל ש- $Q(x)y=\bar{x}(xy)$, ולכן מ-4.5 ,
$(\bar{x}x)y=Q(x)y=\bar{x}(xy)$.

שזה 4.6, ובאופן סימטרי נוכל להוכיח את 4.7.

מ.ש.ל.

לבסוף, נסיים את ההוכחה ש- j היא אינוולוציה, על ידי הוכחת הזהות $\overline{xy}=\bar{y}\,\bar{x}$.

באמצעות 4.3 ו- 4.4 לסירוגין, נמצא ש-

$$B(\bar{y}\,\bar{x},z)=B(\bar{x},yz)=B(\bar{x}\,\bar{z},y)=B(\bar{z},xy)=B(1,(xy)z)=B(\overline{xy},z)$$

ושוב, מ 2.1.3 נקבל ש- $\overline{xy}=\bar{y}\,\bar{x}$.

בכך, הוכחנו את המשפט ומצאנו כי j היא אינוולוציה.
מ.ש.ל.

הגדרה: תהי A אלגברה עם יחידה מעל שדה F , ו- Q תבנית ריבועית בלתי מנוונת עליה ו- $j(x)=\bar{x}$ אינוולוציה עליה כך ש- $x\,\bar{x}=Q(x)1$. נקרא לאלגברה כזאת אלגברת $Q*$.

דוגמה:

כל אלגברת הרכבה היא אלגברת $Q*$.

משפט: תהי A אלגברת $Q*$.

לכל $x,y\in A$

א)

$$B(x,y)1=x\,\bar{y}+y\,\bar{x} \tag{4.8}$$

ב)

$$x+\bar{x}=T(x)1 \tag{4.9}$$

ג)

$$Q(x)=Q(\bar{x}) \tag{4.10}$$

ד)

$$\bar{x}\,x=Q(x)1 \tag{4.11}$$

הוכחה:

לכל x , $x\,\bar{x}=Q(x)1$, ולכן $Q(x+y)1=(x+y)\overline{(x+y)}=x\,\bar{x}+x\,\bar{y}+y\,\bar{x}+y\,\bar{y}$.

בכך, $B(x,y)1=(Q(x+y)-Q(x)-Q(y))1=x\,\bar{y}+y\,\bar{x}$.

נציב $y=1$ ונקבל $x\cdot\bar{1}+1\cdot\bar{x}=T(x)1$.

מכך ש- $\bar{1}=\bar{1}\cdot 1=\overline{(1\cdot\bar{1})}=\bar{\bar{1}}=1$ נסיק ש- $x\cdot 1+1\cdot\bar{x}=T(x)1$, כלומר $x+\bar{x}=T(x)1$.

באמצעות הנוסחה הזו, נוכל להוכיח את 4.10 באותו הדרך שהוכחנו את 4.2, כי השתמשנו רק בנוסחה $x+\bar{x}=T(x)1$ להוכחה הזו.
נציב $\bar{x}$ במקום x ב- $x\bar{x}=Q(x)1$ ונקבל ש- $\bar{x}\bar{\bar{x}}=Q(\bar{x})1$.

לפי 4.10, נקבל ש- $\bar{x}\bar{\bar{x}}=Q(x)1$, ולכן, מאחר ו- $\bar{\bar{x}}=x$, נובע ש- $\bar{x}x=Q(x)1$.
מ.ש.ל.

מסקנה: באלגברת $Q*$:
א)

$$[x,x,y]=-[\bar{x},x,y]$$

ב)

$$[y,x,x]=-[y,x,\bar{x}]$$

הוכחה:

$$[x,x,y]=[T(x)1-\bar{x},x,y]=T(x)[1,x,y]-[\bar{x},x,y]$$

ולכן לפי 2.2.4,

$$[x,x,y]=T(x)0-[\bar{x},x,y]=-[\bar{x},x,y]$$

הוכחת סעיף ב' סימטרית.
מ.ש.ל.

משפט:
אלגברה $Q*$ היא אלטרנטיבית אם ורק אם $[y,x,\bar{x}]=[\bar{x},x,y]=0$ לכל x,y באלגברה. (4.12)

הוכחה:
באלגברה אלטרנטיבית, $[y,x,x]=[x,x,y]=0$ לפי 2.3.1, ולכן מהמסקנה האחרונה,

$$[y,x,\bar{x}]=[\bar{x},x,y]=0$$

אם $[y,x,\bar{x}]=[\bar{x},x,y]=0$, אז מהמסקנה הזו נסיק ש- $[y,x,x]=[x,x,y]=0$.
כלומר, לפי 2.3.1, האלגברה היא אלטרנטיבית.
מ.ש.ל.

5. הוכחת האלטרנטיביות של אלגברת הרכבה

נשתמש באינוולוציה j כדי להוכיח כי אלגברת הרכבה A כלשהי היא אלטרנטיבית.

משפט: כל אלגברת הרכבה היא אלטרנטיבית.

הוכחה:

תהי (A,Q) אלגברת הרכבה. A הוא אלגברת $Q*$, ולכן מ-4.6 ו-4.7, נסיק מיד כי לכל x,y באלגברה,

$$[y,x,\bar{x}]=[\bar{x},x,y]=0$$

לכן, מהמשפט האחרון, ידוע ש- A אלטרנטיבית.

מ.ש.ל.

סיכום ביניים:

מצאנו שאם (A,Q) אלגברת הרכבה, אזי היא אלגברת $Q*$, והיא אלטרנטיבית.

בהמשך נוכיח את המשפט ההפוך.

6. c-הכפלה של אלגבראות (c-doubling)

נגדיר תהליך "הכפלה" של אלגברת $Q*$, ונקבל אלגברה $Q*$ חדשה עם ממד שווה פי שניים הממד של האלגברה הראשון. הבנייה הזאת נקראת גם בניית קיילי-דיקסון.

זאת הכללה לצורת הבנייה של המספרים המרוכבים מהמספרים הממשיים.

יהי c איבר של F כלשהו שאינו 0. בעזרת c נבנה אלגברה $Q*$ חדשה ונקרה לה ה-"c-הכפלה" של A. נסמן אותה ב- $D_c A$, או ב- DA כאשר ברור לאיזה c אנו מתכוונים.

יהי $D=A^2$ המרחב הוקטורי של זוגות סדורות של איברים מ- A. נגדיר הכפלה ב- D אל ידי הנוסחה:

$$(u,v)(x,y)=(ux+c\bar{y}v,\ yu+v\bar{x}) \tag{6.1}$$

נגדיר, כרגיל: $(u,v)+(x,y)=(u+x,v+y)$

טענה: $D=A^2$ יחד עם הכפל והסכום האלה היא אלגברה עם יחידה.

הוכחה:

פעולת הכפל הזו היא פעולה בילינארית, כמו שהיגדרנו בסעיף 2.2, כי אם
$\alpha,\beta\in F,\ \ (u,v),(x,y),(z,w)\in D$:

1)

$$((x,y)+(z,w))(u,v)=(x+z,y+w)(u,v)=$$
$$=(xu+zu+c\bar{v}y+c\bar{v}w,vx+vz+x\bar{u}+z\bar{u})=$$
$$=(xu+c\bar{v}y,vx+x\bar{u})+(zu+c\bar{v}w,vz+z\bar{u})=(x,y)(u,v)+(z,w)(u,v)$$

2)

$$(u,v)((x,y)+(z,w))=(u,v)(x+z,y+w)=$$
$$=(ux+uz+c\overline{(y+w)}v,yu+wu+v\overline{(x+z)})=$$
$$=(ux+c\bar{y}v,yu+v\bar{x})+(uz+c\bar{w}z,wu+v\bar{z})=((u,v)(x,y)+(u,v)(z,w))$$

3)

$$(\alpha(u,v))(\beta(x,y))=((\alpha u)(\beta x)+c\overline{(\beta y)}(\alpha v),(\beta y)(\alpha u)+(\alpha v)\overline{(\beta x)})=$$
$$=(\alpha\beta(ux+c\bar{y}v),\alpha\beta(yu+v\bar{x}))=$$
$$=\alpha\beta(ux+c\bar{y}v,yu+v\bar{x})=\alpha\beta(u,v)(x,y)$$

בכך, D יחד עם פעולת הכפל הזו היא אלגברה.

לכל $(x,y)\in D$,

$$(1,0)(x,y)=(1x+c\bar{y}0,y1+0\bar{x})=(x,y)$$
$$(x,y)(1,0)=(x1+c\bar{0}y,1y+\bar{x}0)=(x,y)$$

ולכן יש ל- D איבר יחידה, שהוא $(1,0)$.

גם כן, לכל $x,y\in A$, $(u,0)(v,0)=(uv+c\bar{0}0,0u+0\bar{v})=(uv,0)$, ובכך נסיק שהפונקציה $x\to(x,0)$ הוא מונומורפיזם של A לתוך D . כלומר A איזומורפית לתת-אלגברה $\{(x,0):x\in A\}$. נוכל לזהות את $x\in A$ עם $(x,0)\in D$.

אם נסמן $t=(0,1)$, אז $t^2=(0+c\cdot\bar{1}\cdot1,0+0)=(c,0)$. ואם נזהה את $(c,0)$ עם c , אז מצאנו ש- $t^2=c$, כלומר יש שורש ריבועי ל- c ב- D .

דוגמה: בבניית המספרים המורכבים בקורס אלגברה לינארית I, בנינו את C כ- $D_c R$, כאשר $c=-1$.
שם, $i=(0,1)$ הוא השורש של $c=-1$.

נרחיב את j ל- $D_c A$:

נגדיר

$$j:(x,y)\rightarrow\overline{(x,y)}=(\bar{x},-y) \tag{6.2}$$

ברור שזהו הרחבה של j , כי $\overline{(x,0)}=(\bar{x},-0)=(\bar{x},0)$, וזיהינו את $(\bar{x},0)$ עם $\bar{x}$.

טענה: ההרחבה של j היא אינוולוציה על $D_c A$.

הוכחה:

1) j אנטיהומומורפיזם, כי:

$$\overline{(u,v)(x,y)}=\overline{(ux+c\,\bar{y}v,\,yu+v\bar{x})}=(\overline{(ux)}+c\,\overline{(\bar{y}v)},-yu-v\bar{x})=(\bar{x}\bar{u}+c\bar{v}\,y,-yu-v\bar{x})=$$
$$=(\bar{x},-y)(\bar{u},-v)=\overline{(x,y)}\,\overline{(u,v)}$$

ובכך $\overline{(x,y)}\cdot\overline{(u,v)}=(\overline{(u,v)\cdot(x,y)})$.

2) j לינארית, כי:

$$\overline{(\alpha x+\beta z,\alpha y+\beta w)}=(\alpha\bar{x}+\beta\bar{z},-\alpha y-\beta w)=$$
$$=(\alpha\bar{x},-\alpha y)+(\beta\bar{z},-\beta w)=\alpha\overline{(x,y)}+\beta\overline{(z,w)}$$

3) j^2 היא פונקציית הזהות, כי:

$$\overline{\overline{(x,y)}}=\overline{(\bar{x},-y)}=(\bar{\bar{x}},-(-y))=(x,y)$$

משלושת השיקולים האלו, מצאנו שגם ה- j המורחב היא אינוולוציה.
מ.ש.ל.

טענה: $D_c A$ היא אלגברת Q^* ממימד $2\,dim\,A$ שהיא הרחבה של A .

הוכחה:

נוכיח ש- $D_c A$ היא אלגברת Q^* :

$$\overline{(x,y)}(x,y)=(\bar{x},-y)(x,y)=(\bar{x}x+c\,\bar{y}(-y),\,yx+(-y)\bar{x})=(\bar{x}x-c\,\bar{y}\,y,0)=$$
$$=(Q(x)1-c\,Q(y)1,0)=(Q(x)-c\,Q(y))(1,0) \quad \text{(מ-4.9)}$$

שזהו $Q(x)-cQ(y)$ כפול היחידה של D. אבל נמצא כי $Q(x)-cQ(y)$ היא תבנית ריבועית מעל D.

$Q(x)-cQ(y)=2B(x,x)-2cB(y,y)$, וכי B בילינארית, נמצא ש-
$E((x,y),(z,w))=B(x,z)-cB(y,w)$ גם תבנית בילינארית, הפעם על $D_c A$.
בכך, $R((x,y))=E((x,y),(x,y))$ תבנית ריבועית, שזה $R((x,y))=Q(x)-c\,Q(y)$.

לכל $(0,0)\neq(x,y)\in D_c A$, אם $x\neq 0$ אז מכך ש- B בלתי מנוונת קיים $z\in A$ כך ש-
$B(x,z)\neq 0$, ואז $E((x,y),(z,0))=B(x,z)-cB(y,0)=B(x,z)\neq 0$.
אחרת $y\neq 0$, ואז יש $w\in A$ כך ש- $B(x,w)\neq 0$.
במקרה הזה, $E((x,y),(0,w))=B(x,0)-c\,B(y,w)=-c\,B(y,w)\neq 0$.

בכל מקרה יש $(z,w)\in D_c A$ כך ש- $E((x,y),(z,w))\neq 0$, ולכן E תבנית בילינארית בלתי מנוונת על $D_c A$, ולכן התבנית הריבועית המתאימה R תבנית ריבועית בלתי מנוונת על $D_c A$.

בכך, D, יחד אם האינוולוציה הזו והתבנית הריבועית $R(x,y)=Q(x)-c\,Q(y)$, היא אלגברת $Q*$ שהיא הרחבה של A.

גם כן, $\dim D_c A=\dim(A\times A)=2\dim A$, ובכך הוכחנו את הטענה.
מ.ש.ל.

נוכיח טענה נוספת מעניינת, שלא קשורה למשפט הכללי, אבל מעניינת מאוד לגבי מכפלות פנימיות ב- $\mathbb{R}$:

טענה: מעל השדה $\mathbb{R}$, בהנתן ש- Q חיובית לחלוטין, (כלומר $Q(v)>0$ לכל $v\neq 0$. או בניסוח אחר, B מכפלה פנימית.), ו- $c<0$, אז גם D בעלת תבנית ריבועית חיובית לחלוטין.

הוכחה:

אם $(x,y)\neq(0,0)$, $Q(x),Q(y)$ שניהם אי-שליליים, ולפחות אחד מהם חיובי.

לכן $Q(x),-c\,Q(y)$ שניהם אי-שליליים, ולפחות אחד מהם חיובי, ולכן $Q(x)-c\,Q(y)>0$.

לכן, $Q(x)-cQ(y)$ היא תבנית חיובית לחלוטין.
מ.ש.ל.

דוגמה: עבור $\mathbb{R}$ עם התבנית $Q(x)=x^2$ נקבל $\mathbb{C}=D_{-1}\mathbb{R}$ עם התבנית $R((x,y))=x^2+y^2$.

7. משהו הולך לאיבוד בכל הכפלה

משפט: תהי A אלגברת Q^* , $c\in F\setminus\{0\}$ ו- $D=D_c A$ ה-c-הכפלה של A .

א) D היא קומוטטיבית ואסוציאטיבית אם ורק אם A קומוטטיבית ואסוציאטיבית ו - j היא פונקציית הזהות. (7.1)

ב) D היא אסוציאטיבית אם ורק אם A קומוטטיבית ואסוציאטיבית. (7.2)

ג) D היא אלטרנטיבית אם ורק אם A אסוציאטיבית. (7.3)

לפני שנוכיח את המשפט, נוכיח שתי טענות עזר.

נסמן $X=(x,y),U=(u,v),Z=(z,t)$ ל- $x,y,u,v,z,t\in A$.

טענה: $$[U,X]=([u,x]+c(\bar{y}v-\bar{v}y),y(u-\bar{u})+v(\bar{x}-x)) \quad (7.4)$$

הוכחה:

$$\begin{aligned}[U,X]&=UX-XU=\\&=(ux+c\bar{y}v,yu+v\bar{x})-(xu+c\bar{v}y,vx+y\bar{u})=\\&=(ux-xu+c(\bar{y}v-\bar{v}y),y(u-\bar{u})+v(\bar{x}-x))=\\&=([u,x]+c(\bar{y}v-\bar{v}y),y(u-\bar{u})+v(\bar{x}-x))\end{aligned}$$

מ.ש.ל.

טענה:

$$[U,X,Z]=([u,x,z]+c(\bar{t}(yu)-u(\bar{t}y)+\bar{t}(v\bar{x})-(\bar{x}\bar{t})v+(\bar{y}v)z-(z\bar{y})v),$$
$$t(ux)-(tx)u+(yu)\bar{z}-(y\bar{z})u+(v\bar{x})\bar{z}-v(\bar{z}\bar{x})+c(t(\bar{y}v)-v(\bar{y}t))) \tag{7.5}$$

הוכחה:

$$[U,X,Z]=(UX)Z-U(XZ)=$$
$$=(ux+c\bar{y}v,\ yu+v\bar{x})(z,t)-(u,v)(xz+c\bar{t}y,\ tx+y\bar{z})=$$

$$=((ux)z+c(\bar{y}v)z+c\bar{t}(yu+v\bar{x}),t(ux+c\bar{y}v)+(yu)\bar{z}+(v\bar{x})\bar{z})+$$
$$+(-u(xz)-cu(\bar{t}y)-c\overline{(tx+y\bar{z})}v,-(tx)u-(y\bar{z})u-v\overline{(xz+c\bar{t}y)})=$$

$$=((ux)z-u(xz)+c(\bar{t}(yu)-u(\bar{t}y)+\bar{t}(v\bar{x})-(\bar{x}\bar{t})v+(\bar{y}v)z-(z\bar{y})v),$$
$$t(ux)-(tx)u+(yu)\bar{z}-(y\bar{z})u+(v\bar{x})\bar{z}-v(\bar{z}\bar{x})+c(t(\bar{y}v)-v(\bar{y}t)))=$$

$$=([u,x,z]+c(\bar{t}(yu)-u(\bar{t}y)+\bar{t}(v\bar{x})-(\bar{x}\bar{t})v+(\bar{y}v)z-(z\bar{y})v),$$
$$t(ux)-(tx)u+(yu)\bar{z}-(y\bar{z})u+(v\bar{x})\bar{z}-v(\bar{z}\bar{x})+c(t(\bar{y}v)-v(\bar{y}t)))$$

מ.ש.ל.

הוכחת המשפט:

יש אלגברה איזומורפית ל- A (שהיא מורכבת מ- $(x,0)$ לכל $x\in A$) שהיא תת-אלגברה של D , ולכן נסיק כי אם D קומוטטיבית, אסוציאטיבית, או אלטרנטיבית, אז גם A קומוטטיבית, אסוציאטיבית, או אלטרנטיבית בהתאמה.

נוכיח כיוון אחד של 7.1:

אם D קומוטטיביות ואסוציאטיבית, אז A קומוטטיבית ואסוציאטיבית, ומ-7.4 נסיק (על ידי ההצבה $u=x=0, v=1$) כי:

$$[U,X]=(0+c(\bar{y}1-\bar{1}y),\ y(0-\bar{0})+1(\bar{0}-0))=(c(\bar{y}-y),0)$$

מהקומוטטיביות של D , $[U,X]=0$, ולכן בגלל ש- $c\neq 0$, נסיק ש- $y=\bar{y}$ (ל- y כלשהו). בכך, מצאנו ש- $j(x)$ היא פונקציית הזהות.

הוכחנו את הכיוון הראשון של 7.1.

נוכיח כיוון אחד של 7.2:

אם D אסוציאטיבית, אז $[U,X,Z]=0$ ולכן מ-7.5, אם ניקח $v=x=z=0, t=1$:

$$0=[U,X,Z]=(c(yu-uy),0)$$

ולכן $yu=uy$ (ל- u,y כלשהם), ולכן הקומוטטיביות של A נובע מהאסוציאטיביות של D .
בכך, יש לנו שאם D האסוציאטיבית, אז A גם קומוטטיבית וגם אסוציאטיבית, ולכן גם הוכחנו כיוון אחד של 7.2.

הכיוון השני של 7.1: אם A קומוטטיבית ואסוציאטיבית, ו- j היא פונקציית הזהות, אז D קומוטטיבית ואסוציאטיבית.

הוכחה:

אם A קומוטטיבית ואסוציאטיבית, ו- j היא פונקציית הזהות, אז מ-7.4, לכל $U,X\in D$:

$$\begin{aligned}[U,X]&=([u,x]+c(\bar{y}v-\bar{v}y),y(u-\bar{u})+v(\bar{x}-x))=\\&=(0+c(yv-yv),y(u0u)+v(x-x))=(0,0)\end{aligned}$$

בכך D קומוטטיבית. נוכיח ש- D אסוציאטיבית כשנוכיח את הכיוון השני של 7.2.

הכיוון השני של 7.2: אם A קומוטטיבית ואסוציאטיבית (בין אם j היא פונקציית הזהות או לא), אז D אסוציאטיבית.

הוכחה:

אם A קומוטטיבית ואסוציאטיבית, מ-7.5, לכל $U,X,Z\in D$:

$$\begin{aligned}[U,X,Z]=(&[u,x,z]+c(\bar{t}(yu)-u(\bar{t}y)+\bar{t}(v\bar{x})-(\bar{x}\bar{t})v+(\bar{y}v)z-(z\bar{y})v),\\&t(ux)-(tx)u+(yu)\bar{z}-(y\bar{z})u+(v\bar{x})\bar{z}-v(\bar{z}\bar{x})+c(t(\bar{y}v)-v(\bar{y}t)))=\end{aligned}$$

$$\begin{aligned}&=(0+c(\bar{t}yu-u\bar{t}y+\bar{t}v\bar{x}-\bar{x}\bar{t}v+\bar{y}vz-z\bar{y}v),\\&tux-txu+yu\bar{z}-y\bar{z}u+v\bar{x}\bar{z}-v\bar{z}\bar{x}+c(t\bar{y}v-v\bar{y}t))=\\&=(0,0)\end{aligned}$$

בכך D אסוציאטיבית.

לכן, גם הוכחנו את הכיוון השני של 7.2 , וזה משלים את הכיוון השני של 7.1.

נוכיח את 7.3:

טענה: אם ניקח $U=\bar{X}=(\bar{x},-y)$ ($x,y,z,t\in A$ כלשהם):

$$[\bar{X},X,Z]=([\bar{x},x,z]+c[\bar{x},\bar{t},y],-[y,\bar{z},\bar{x}]) \tag{7.6}$$

$$[Z,X,\bar{X}]=([z,x,\bar{x}]+c[y,\bar{z},\bar{x}],-[\bar{x},\bar{t},y]) \tag{7.7}$$

הוכחה:

נציב ל-7.5:

$$[\bar{X},X,Z]=$$
$$=([\bar{x},x,z]+c(\bar{t}(y\bar{x})-\bar{x}(\bar{t}\,y)+\bar{t}(-y\bar{x})-(\bar{x}\,\bar{t})(-y)+(\bar{y}(-y))z-(z\bar{y})(-y)),$$
$$t(\bar{x}\,x)-(t\,x)\bar{x}+(y\bar{x})\bar{z}-(y\bar{z})\bar{x}+(-y\bar{x})\bar{z}-(-y)(\bar{z}\,\bar{x})+c(t(\bar{y}(-y))-(-y)(\bar{y}\,t)))=$$

$$=([\bar{x},x,z]+c(\bar{t}(y\bar{x})-\bar{x}(\bar{t}\,y)-\bar{t}(y\bar{x})+(\bar{x}\,\bar{t})y-(\bar{y}\,y)z+(z\bar{y})y),$$
$$t(\bar{x}\,x)-(t\,x)\bar{x}+(y\bar{x})\bar{z}-(y\bar{z})\bar{x}-(y\bar{x})\bar{z}+y(\bar{z}\,\bar{x})+c(-t(\bar{y}\,y)+y(\bar{y}t)))=$$

$$=([\bar{x},x,z]+c([\bar{x},\bar{t},y]-(\bar{y}\,y)z+(z\bar{y})y),t(\bar{x}\,x)-(t\,x)\bar{x}-[y,\bar{z},\bar{x}]+c(-t(\bar{y}\,y)+y(\bar{y}\,t)))=$$
$$=([\bar{x},x,z]+c([\bar{x},\bar{t},y]-Q(y)z+Q(\bar{y})z,Q(x)t-Q(x)t-[y,\bar{z},\bar{x}]+c(-Q(\bar{y})t+Q(\bar{y})t)))=$$
$$=([\bar{x},x,z]+c([\bar{x},\bar{t},y],-[y,\bar{z},\bar{x}]))$$

(השוויון השני מהאחרון נובע מ-4.7, 4.6)

בכך קיבלנו את 7.6. באופן דומה נקבל 7.7.

מ.ש.ל.

טענה: אם A אסוציאטיבית, D אלטרנטיבית. (הכיוון השני של 7.3)

הוכחה:

מ-7.6, אם A אסוציאטיבית, $[\bar{X},X,Z]=(0+c\cdot 0,-0)=(0,0)$.

באופן דומה, אם ניקח $Z=\bar{X}=(\bar{x},-y)$ במקום $U=\bar{X}$, נמצא כי $[Z,X,\bar{X}]=0$.

לכן, לפי 4.12, מצאנו כי D אלטרנטיבית.

הוכחנו את הכיוון השני של 7.3.

מ.ש.ל.

נותר להוכיח את הכוון הראשון של 7.3:

טענה: אם D אלטרנטיבית, אז A אסוציאטיבית.

הוכחה:

אם D אלטרנטיבית, בפרט A אלטרנטיבית, כי יש תת-אלגברה ל- D האיזומורפית ל- A .
כי D אלטרנטיבית, לפי 4.12, $[\bar{X}, X, Z]=0$.

נובע מזה לפי 7.6 ש:

$$0=([\bar{x}, x, z]+c[\bar{x}, \bar{t}, y], -[y, \bar{z}, \bar{x}])$$

בכך,

$$[\bar{x}, x, z]+c[\bar{x}, \bar{t}, y]=-[y, \bar{z}, \bar{x}]=0$$

וכי A אלטרנטיבית,

$$[\bar{x}, x, z]=0 .$$

לכן,

$$c[\bar{x}, \bar{t}, y]=[y, \bar{z}, \bar{x}]=0$$

ולכן ($c\neq 0$)

$$[\bar{x}, \bar{t}, y]=[y, \bar{z}, \bar{x}]=0$$

לכל $x, y, t, z\in A$.

בכך, אם נסמן $v=\bar{x}, u=\bar{t}$, נמצא כי $[v, u, y]=0$ לכל $v, u, y\in A$, ובכך מצאנו כי A אסוציאטיבית.
מ.ש.ל.

בכך הוכחנו גם את 7.3.

8. אלטרנטיביות היא תנאי מספיק לאלגברת הרכבה

מצאנו כי כל אלגברת הרכבה (A, Q) היא אלגברת $Q*$ אלטרנטיבית. נוכיח כי התנאים האלה מספיקים.

למה:

תהי A אלגברה $Q*$ אלטרנטיבית . לכל $x, y\in A$:

$$(y x)\bar{x}=y(x\bar{x})=\bar{x}(x y)=(\bar{x} x) y=Q(x) y \quad (8.1)$$

הוכחה:

מ-4.12:

$$[\bar{x}, x, y]=0=[y, x, \bar{x}]$$

לכן,

$$(\bar{x}\,x)\,y-\bar{x}(x\,y)=0=(y\,x)\,\bar{x}-y(x\,\bar{x})$$

ובכך

$$\bar{x}(x\,y)=(\bar{x}\,x)\,y$$
$$(yx)\,\bar{x}=y(x\,\bar{x})$$

לכן, הגדרת אלגברת Q^* ומ-4.11:

$$(yx)\,\bar{x}=y(x\,\bar{x})=Q(x)\,y$$
$$\bar{x}(x\,y)=(\bar{x}\,x)\,y=Q(x)\,y$$

מ.ש.ל.

טענה: כל אלגברת Q^* אלטרנטיבית היא אלגברת הרכבה.

הוכחה:

מ- 4.5:

$$Q(xy)\,1=\overline{(xy)}(xy)=(\bar{y}\,\bar{x})(x\,y)$$

מהעובדה ש- j היא אנטיהומומורפיזם (בגלל שהיא אינוולוציה), ומ-4.9, נקבל ש-

$$Q(xy)\,1=[(T(y)1-y)\bar{x}](xy)$$

בכך,

$$Q(xy)\,1=(T(y)\bar{x}-y\,\bar{x})(xy)=T(y)\bar{x}(x\,y)-(y\,\bar{x})(x\,y)$$

מ- 2.3.9, 8.1, 4.5:

$$Q(xy)\,1=T(y)Q(x)\,y-y(\bar{x}\,x)\,y=$$
$$=Q(x)\,T(y)\,y-Q(x)\,y^2=$$
$$=Q(x)\,\bar{y}\,y=Q(x)Q(y)\,1$$

ובכך מצאנו ש- $Q(xy)=Q(x)Q(y)$ ובכך (A,Q) היא אלגברת הרכבה.

מ.ש.ל.

נסכם מה שמצאנו אד כה במשפט:

משפט: Q היא תבנית המאפשרת הרכבה על מרחב A אם ורק אם יש מכפלה בילינארית על A כך ש- (A,Q) אלגברת Q^* אלטרנטיבית.

9. היררכיה של אלגברות הרכבה

נתחיל בבניית היררכיה של אלגברות הרכבה, ואז נוכיח למה שבעזרתה נוכיח בסעיף 11 שההיררכיה הזו כוללת את כל אלגברות ההרכבה.

נתחיל ב- F שדה כלשהו בעל אפיין השונה מ-2. כדי ש- F תהיה אלגברת הרכבה, ניקח תבנית ריבועית בלתי מנוונת עליו. הכרחי ש- $Q(1)=1$, ולכן לכל $x\in F$, $Q(x)=Q(x\cdot 1)=x^2Q(1)=x^2\cdot 1=x^2$.

בכך (Q,F) , כאשר $Q(x)=x^2$, היא האלגברת הרכבה הפשוטה ביותר, עם ממד 1.

במקרה הזה, לכל $x\in F$,

$$\begin{aligned}\bar{x}&=T(x)1-x=B(x,1)1-x=\\&=Q(x+1)-Q(x)-Q(1)-x=(x+1)^2-x^2-1^2-x=\\&=x^2+2x+1-x^2-1-x=x\end{aligned}$$

כלומר האינוולציה $\bar{x}$ היא אינוולציית הזהות.

לפי 7.1, אם נכפיל (לפי איזשהו c) את F , נקבל אלגברה אסוציאטיבית וקומוטטיבית, שהיא בכך אלטרנטיבית, ולכן אלגברת הרכבה. (נקרא לה אלגברה ריבועית מעל F .)
במקרה הזה לפי 6.2, לכל $(x,y)\in D_cF$,

$$\overline{(x,y)}=(\bar{x},-y)=(x,-y)$$

אבל ידוע ש- $\overline{(0,1)}=(0,-1)\neq(0,1)$, כי F בעל אפיין השונה מ-2, ולכן $-1\neq 1$.
כלומר האינוולציה $\overline{(x,y)}$ **לא** יכולה להיות אינוולציית הזהות.

לפי 7.2, אם נכפיל את האלגברה DF הזו, נקבל אלגברה אסוציאטיבית DDF , שהיא בכך אלטרנטיבית, ולכן אלגברת הרכבה. (נקרא לה אלגברת הקווטרניונים מעל F .)

לעומת זאת, אם DDF היא גם קומוטטיבית, ידוע מ-7.1 שהאינוולציה של DF הוא הזהות, והוכחנו שזה לא המצב.
לכן DDF אסוציאטיבית ולא קומוטטיבית.

לפי 7.3, אם נכפיל את האלגברה DDF , נקבל אלגברה אלטרנטיבית $DDDF$, ולכן היא אלגברת הרכבה. (נקרא לה אלגברת קיילי מעל F .)

לעומת זאת, אם היא אסוציאטיבית, ידוע מ-7.2 ש- DDF קומוטטיבית, והוכחנו שזה לא המצב.
לכן $DDDF$ לא אסוציאטיבית.

בכך, לא נוכל לקבל אלגברת הרכבה נוספת אל ידי הכפלה של $DDDF$. אילו $DDDDF$ היתה אלגברת הרכבה, היא היתה אלטרנטיבית, ואז מ-7.3 $DDDF$ אסוציאטיבית, והוכחנו שזה לא המצב.

בכך, מצאנו היררכיה מגודל 4 של אלגברות הרכבה, שכל אחד פרט לראשון הוא ההכפלה של האלגברה שמעליו.

10. אלגברת הרכבה מכילה הכפלות של תת-אלגברות מסויימות

טענה: אם A אלגברת הרכבה ו- C תת-אלגברה כך שהצימצום של Q ל- C בלתי מנוונת ו- $1\in C$, אז C אלגברת הרכבה.

אם A אלגברת הרכבה:
לכל $x, y\in C$ מתקיים $Q(x)Q(y)=Q(xy)$ (כי זה נכון לכל $x, y\in A\supseteq C$).

מכך, ומכך של- C יש יחידה (בגלל ש- $1\in C$), C היא אלגברת הרכבה.
מ.ש.ל.

טענה: אם A אלגברת- $Q*$ ו- C תת-אלגברה שהצימצום של Q ל- C בלתי מנוונת ו- $1\in C$, אז C אלגברת $Q*$.

הוכחה:

אם A אלגברת $Q*$, לכל $x\in C$, ידוע לפי 4.9 ש $\bar{x}=T(x)1-x\in C$ (בגלל ש- $1,x\in C$).
בכך $\bar{x}$ אינוולציה על איברי C .

בגלל שלכל $x\in C\subseteq A$ מתקיים $x\bar{x}=Q(x)1$, C אלגברת $Q*$.
מ.ש.ל.

משפט: בהינתן אלגברת הרכבה A , (מעל שדה F , Q התבנית הריבועית עליה, $j(x)=\bar{x}$ האינוולוציה שלה) שיש לה תת-אלגברה C כך ש $1\in C$ שהצימצום של Q ל- C בלתי מנוונת ו- $C\neq A$, אז יש תת-אלגברה $C\subseteq D\subseteq A$ כך ש- D איזומורפית להכפלה של C .

הוכחה:

נניח בשלילה ש $C\cap C^{\perp}\neq\{0\}$. אז יש $0\neq v\in C\cap C^{\perp}$. בגלל ש- $v\in C^{\perp}$, מתקיים $B(v,x)=0$ לכל $x\in C$. בגלל ש $0\neq v\in C$, זה סתירה לכך שהצימצום של Q ל- C בלתי מנוונת.

לכן, מצאנו ש - $C\cap C^{\perp}=\{0\}$.

בכך, לפי 2.1.4, $A=C\oplus C^{\perp}$.

מהשוויון הזה ומהנחת המשפט ש- $A\neq C$, נובע ש $C^{\perp}\neq\{0\}$.

אם $0\neq x\in C^{\perp}$, אז בפרט x איבר של A השונה מ-0, ולכן יש $v\in A$ כך ש- $B(x,v)\neq 0$, כי B בלתי מנוונת מעל A .

מהסכום $A=C\oplus C^{\perp}$, קיימים איזשהם $a\in C^{\perp}$ ו- $b\in C$ יחידים כך ש $v=a+b$.
לכן,

$$B(x,a)+B(x,b)=B(x,a+b)=B(x,v)\neq 0$$

אבל $b\in C$ ו- $x\in C^{\perp}$, ולכן $B(x,b)=0$. לכן $B(x,a)\neq 0$, כלומר מצאנו $a\in C^{\perp}$ כך ש $B(x,a)\neq 0$ עבור כל $0\neq x\in C^{\perp}$, כלומר הצימצום של B ל- $C^{\perp}$ בלתי מנוונת.

לכן הצימצום של Q ל- $C^{\perp}$ בלתי מנוונת, ובפרט היא לא פונקציית האפס.
לכן יש $t\in C^{\perp}$ כך ש- $Q(t)\neq 0$.
נסמן $c=-Q(t)$.

$1\in C$ ולכן מהגדרת $C^{\perp}$, $T(t)=B(t,1)=0$.
בכך,

$$\bar{t}=T(t)1-t=-t$$

ולכן

$$t^2=t\,t=-\bar{t}\,t=-Q(t)1=c\,1 \qquad (10.1)$$

לכל $x\in C$, $B(x,t)=0$, ולכן מ-4.8, $\bar{x}\,t+\bar{t}\,x=0$, ובכך לכל $x\in C$,

$$t\,x=\bar{x}\,t \qquad (10.2)$$

ל- $x,y\in C$, ידוע ש- $\bar{y}\,x\in C$, ולכן $B(x,yt)=B(\bar{y}\,x,t)=0$ (השוויון הראשון הוא מ-4.3).

מכך נסיק כי המרחב $Ct=\{y\,t:y\in C\}$ הוא תת-מרחב של $C^{\perp}$, ולכן אם נגדיר $D=C+Ct$, נמצא שזהו סכום ישר, $D=C\oplus Ct$.

טענה: ב- A מתקיים הזהות $\bar{x}(z\,y)+\bar{z}(x\,y)=B(x,z)\,y$.

הוכחה:

זה נובע מהזהות שב-8.1, $\bar{x}(x\,y)=Q(x)\,y$. נציב $x+z$ במקום x , ונקבל את הזהות $\bar{x}((x+z)\,y)+\bar{z}((x+z)\,y)=Q(x+z)\,y$, ובכך $\bar{x}(x\,y)+\bar{x}(z\,y)+\bar{z}(x\,y)+\bar{z}(z\,y)=Q(x+z)\,y$.
נשתמש שוב בזהות הזו מ-2.1 ונמצא כי $Q(x)\,y+\bar{x}(z\,y)+\bar{z}(x\,y)+Q(z)\,y=Q(x+z)\,y$. נעביר אגפים, ובזאת הוכחנו את הזהות.
מ.ש.ל.

אם $z=t$, $x,y\in C$ נמצא ש- $\bar{x}(t\,y)+\bar{t}(x\,y)=B(x,t)\,y$, ובכך $\bar{x}(t\,y)-t(x\,y)=0\cdot y=0$.
לכן, $\bar{x}(t\,y)=t(x\,y)$. מ-10.2, נמצא כי $\bar{x}(\bar{y}\,t)=(\bar{y}\,\bar{x})\,t$. בכך נסיק אל ידי ההצבה של $\bar{x}$ במקום x ו- $\bar{y}$ במקום y שלכל $x,y\in C$:

$$x(y\,t)=(yx)\,t \tag{10.3}$$

על זה נפעיל את האינוולוציה, ונקבל $\overline{(y\,t)}\,\bar{x}=\bar{t}\,\overline{(yx)}$, כלומר $-(t\,\bar{y})\,\bar{x}=-t(\bar{x}\,\bar{y})$,
כלומר $(t\,\bar{y})\,\bar{x}=t(\bar{x}\,\bar{y})$.

מ-10.2, נמצא ש- $(y\,t)\,\bar{x}=(y\,x)\,t$ לכל $x,y\in C$. נציב $\bar{x}$ במקום x ונמצא שלכל $x,y\in C$,

$$(y\,t)\,x=(y\,\bar{x})\,t \tag{10.4}$$

גם כן, משוויון מופנג (נוסחה 2.3.9), $(x\,t)(y\,t)=(t\,\bar{x})(y\,t)=t(\bar{x}\,y)\,t$,ובכך (מ-10.1, 10.2),

$$(x\,t)(y\,t)=(\bar{y}\,x)\,t^2=c\,\bar{y}\,x \tag{10.5}$$

מ 10.1-5, נסיק לכל $x,y,u,v\in C$ את המשוואה:

$$(u+vt)(x+yt)=(u\,x+c\,\bar{y}\,v)+(y\,u+v\,\bar{x})\,t \tag{10.6}$$

בכך, מצאנו שאם נכפיל שני איברים מ- $D=C+Ct$, נקבל איבר מ- D , ולכן מצאנו ש- D היא תת-אלגברה של A . (המכילה את C .)

גם כן, ל- $u,v\in C$, $\overline{u+vt}=\bar{u}+\bar{t}\,\bar{v}=\bar{u}-t\,\bar{v}=\bar{u}-vt\in C+Ct=D$, ובכך D סגורה ביחס ל- j .

טענה: הצמצומים של Q ל- Ct ול- $D=C+Ct$ בלתי מנוונים.

הוכחה:

הצמצום של Q ל- C בלתי מנוונת, כלומר אם B התבנית הבילינארית המתאימה ל- Q , לכל $0\neq u\in C$, יש $v\in C$ כך ש- $B(u,v)\neq 0$. לכן, לכל $w\in Ct$, ($w=ut$, $u\in C$), יש $v\in C$ כך ש- $B(u,v)\neq 0$, ולכן (לפי 3.3), $B(w,vt)=B(ut,ut)=Q(t)B(u,v)\neq Q(t)0=0$. לכן, יש $vt\in Ct$ ($v\in C$) כך ש- $B(w,vt)\neq 0$.

בכך, הצמצום של B ל- Ct בלתי מנוונת, ולכן הצמצום של Q ל- Ct בלתי מנוון.

תהי $0\neq u+xt\in D=C+Ct$.

נחלק ל-3 מקרים:

א) אם $u=0$ אז $x\neq 0$, ולכן מפני שהצימצום של Q ל- Ct לא מוונת, קיים $y\in C$ כך ש $B(xt,yt)\neq 0$. בכך $w=0+yt$ הוא איבר ב D כך ש $B(u+xt,w)\neq 0$.

ב) אם $x=0$ אז $u\neq 0$, ולכן מפני שהצימצום של Q ל- C לא מוונת,
קיים $y\in C$ כך ש $B(x,y)\neq 0$. בכך $y=y+0t$ הוא איבר ב D כך ש $B(u+xt,y)\neq 0$.

ג) אם $u\neq 0, x\neq 0$:

מפני שהצימצום של Q ל- C בלתי מנוון, קיים $v\in C$ כך ש $B(u,v)\neq 0$.

מפני שהצימצום של Q ל- Ct בלתי מנוון, קיים $y\in C$ כך ש $B(xt,yt)\neq 0$.

אם $B(xt,yt)=-B(u,v)$, נסמן $z=2y$, אחרת $z=y$. בכל מקרה, $z\in C$.

נחשב את $B(u+xt,v+zt)$:

$$B(u+xt,v+zt)=B(u,v+zt)+B(xt,v+zt)=$$
$$=B(u,v)+B(u,zt)+B(xt,v)+B(xt,zt)=$$
$$=B(u,v)+B(xt,zt)$$

ההסבר לשיוויון האחרון הוא ש $Ct\subseteq C^{\perp}$, ולכן $B(u,zt)=B(xt,v)=0$, מפני ש- $u,v\in C, zt,xt\in Ct$.

נחלק לשני מקרים:

1) אם $B(xt,yt)\neq -B(u,v)$ אז $z=y$, ולכן $B(u,v)+B(xt,zt)=B(u,v)+B(xt,yt)\neq 0$.

2) אם $B(xt,yt)=-B(u,v)$ אז $z=2y$, ולכן

$$B(u,v)+B(xt,zt)=B(u,v)+B(xt,2yt)=$$
$$=(B(u,v)+B(xt,yt))+B(xt,yt)=0+B(xt,yt)\neq 0$$

בשני המקרים, $B(u+xt,v+zt)=B(u,v)+B(xt,zt)\neq 0$.

בכך, מצאנו בכל אחד משלושת המקרים האפשריים, א ,ב ,ו-ג, איבר $a+bt\in D$ כך ש-
$B(u+zt\,,a+bt)\neq 0$, ובכך הצמצום של B ל- D בלתי מנוונת, ולכן הצמצום של Q ל- D בלתי מנוון.
מ.ש.ל.

נשאר עכשיו רק להוכיח ש- D איזומורפית ל- $D_c C$. מהשוואה פשוטה של 10.6 עם 6.1, יחד עם העובדה ש- $(x+yt)+(u+vt)=(x+u)+(y+v)t$ לכל $x+yt\,,u+vt\in D$, וש- $\alpha(x+yt)=\alpha x+\alpha yt$ לכל $x+yt\in D$, α סקלר, נובע שההתאמה $(x\,,y)\rightarrow x+yt$ מ- $D_c C$ ל- D היא הומומורפיזם ביניהם.

אם $x+yt=0$ לאיזשהו $x\,,y\in C$, אז $-x=yt\in Ct$, ולכן $x\in Ct\subseteq C^{\perp}$.
אבל $C\cap C^{\perp}=\{0\}$, ולכן $x=0$. בכך $y=0$, ולכן הגרעין של ההומומורפיזם $(x\,,y)\rightarrow x+yt$ הוא בדיוק $\{0\}$.

כלומר, ההתאמה היא חד-חד-ערכית, ולפי ההגדרה של D כ- $C+Ct$ זאת התאמה על D , ולכן זאת איזומורפיזם.
מ.ש.ל.

11. ההיררכיה של אלגברות הרכבה היא שלמה

אם A אלגברת הרכבה מעל F , אז A מכיל שדה האיזומורפי ל- F , שהוא השדה $\{\alpha\cdot 1:\alpha\in F\}$.
גם כן, הצמצום של Q לשדה הזה בלתי מנוון.

נניח בשלילה ש- A אלגברת הרכבה שאינה בהיררכיה שבסעיף 9.

מההנחה הזו, $A\neq F$, ולכן מתקיימים כל תנאי הלמה בסעיף 10, כאשר $C=F$.

לכן, A מכילה שדה D_1 שהוא הכפלה של F .
$D_1=DF$ היא בהיררכיה, ולכן היא אינה שקולה ל- A .
בכך, שוב מתקיימים כל תניי הלמה, כאשר $C=D_1$.

לכן, A מכילה אלגברה D_2 שהיא הכפלה של D_1 .
$D_2=D\,D_1=D\,D\,F$ היא בהיררכיה, ולכן היא אינה שקולה ל- A .
בכך, שוב מתקיימים כל תנאי הלמה, כאשר $C=D_2$.

לכן, A מכילה אלגברה D_3 שהיא הכפלה של D_2 .
$D_3=D\,D_2=D\,D\,D_1=D\,D\,D\,F$ היא בהיררכיה, ולכן היא אינה שקולה ל- A .
בכך, שוב מתקיימים כל תניא הלמה, כאשר $C=D_3$.

לכן, A מכילה אלגברה $D_4 = D\,D_3 = D\,D\,D_2 = D\,D\,D\,D_1 = D\,D\,D\,D\,F$ שהיא הכפלה של D_3 .

מסעיף 7, מפני ש- D_3 אינה אסוציאטיבית, D_4 אינה אלטרנטיבית. (מצאנו בסעיף 9 ש- D_3 (אלגברת קיילי) אינה אסוציאטיבית.)

בכך, A מכילה אלגברה לא אלטרנטיבית, ולכן לא יתכן ש- A אלטרנטיבית.
בכך היגענו לסתירה, ולכן מצאנו שלא יתכן ש- A אינה בהירככיה.

12. סיום הוכחת משפט הורוויץ

בכך הוכחנו את המשפט הזו:

משפט הורוויץ

מעל שדה F כלשהי, אלגברות ההרכבה היחידות הן F עצמה, האלגברות הריבועיות מעל F , אלגברות הקווטרניוניות מעל F , ואלגברות קיילי מעל F .

בפרט, במקרה ש- $F=\mathbb{R}$, נקבל את המסקנה הזו :

משפט הורוויץ הקלסי

מעל $\mathbb{R}$, הסכום $Q(x)=\sum_{i=1}^{n} x_i^2$ הוא תבנית ריבועית המאפשרת הרכבה אם ורק אם $n\in\{1,2,4,8\}$.

הוכחה:

מבניית ההירככיה שבסעיף 9, ידוע שנוכל לבנות $\mathbb{R}, D\mathbb{R}, DD\mathbb{R}, DDD\mathbb{R}$.
בסעיף 9 מצאנו שמעל $F=\mathbb{R}$, $Q(x)=x^2$.

אם נשתמש ב- $c=-1$, נקבל שמעל $DF=D\mathbb{R}$, $Q(x)=x_1^2+x_2^2$.

שוב, אם נשתמש ב- $c=-1$, נקבל שמעל $DDF=DD\mathbb{R}$, $Q(x)=x_1^2+x_2^2+x_3^2+x_4^2$,

ושוב, אם נשתמש ב- $c=-1$, נקבל שמעל $DDF=DD\mathbb{R}$,
$Q(x)=x_1^2+x_2^2+x_3^2+x_4^2+x_5^2+x_6^2+x_7^2+x_8^2$.

לכן הצלחנו לבנות אלגברות הרכבה עם Q מהצורה $Q(x)=\sum_{i=1}^{n} x_i^2$ כאשר $n\in\{1,2,4,8\}$.

כלומר, אם $n\in\{1,2,4,8\}$, מצאנו ש- $Q(x)=\sum_{i=1}^{n} x_i^2$ מאפשרת הרכבה.

ממשפט הורוויץ (הכללי) נקבל שלא ניתן בכלל לבנות אלגברת הרכבה עם ממד שאינו אחד מ-1, 2, 4, או 8.

לכן אם $n\notin\{1,2,4,8\}$, לא ייתכן ש- (Q,A) כאשר A מעל IR ו- $Q(x)=\sum_{i=1}^{n} x_i^2$ היא אלגברת הרכבה, ובכך מצאנו ש- $Q(x)=\sum_{i=1}^{n} x_i^2$ לא מאפשרת הרכבה אם $n\notin\{1,2,4,8\}$.

מ.ש.ל.

ביבליוגרפיה

Basic Algebra I מאת Nathan Jacobson, סעיף 7.6.