Εθνικό Μετσόβιο Πολυτεχνείο

Σχολή Εφαρμοσμένων Μαθηματικών και Φυσικών Επιστημών

Διπλωματική Εργασία

Composition Άλγεβρες

&

Εφαρμογές

Επιμέλεια:

Ελένη Πύλια

Επιβλέπων Καθηγητής:

Ανάργυρος Γ. Φελλούρης

Αθήνα, Ιούλιος 2014

Εθνικό Μετσόβιο Πολυτεχνείο

Σχολή Εφαρμοσμένων Μαθηματικών και Φυσικών Επιστημών

Διπλωματική Εργασία

Composition Άλγεβρες

&

Εφαρμογές

Επιμέλεια: Ελένη Πύλια

Επιβλέπων Καθηγητής: Ανάργυρος Γ. Φελλούρης

Μέλη Επιτροπής:

Σωτήριος Καρανάσιος, Παναγιώτης Ψαρράκος

Αθήνα, Ιούλιος 2014

Περιεχόμενα

Περίληψη

Στην παρούσα διπλωματική εργασία μελετάμε τις Composition Άλγεβρες, την ταξινόμησή τους και κάποιες εφαρμογές αυτών. Στο Κεφάλαιο 1 ορίζουμε κάποιες βασικές αλγεβρικές δομές, διανυσματικούς χώρους και άλγεβρες. Επίσης, γράφουμε σχετικά με διγραμμικές και τετραγωνικές μορφές. Στο Κεφάλαιο 2 ορίζουμε τις Composition Άλγεβρες και μελετάμε κάποιες ιδιότητες αυτών. Επίσης, περιγράφουμε την άλγεβρα των τετράδων και τις οκτάδες, οι οποίες είναι Composition Άλγεβρες διαστάσεων 4, 8 αντίστοιχα. Στο Κεφάλαιο 3 περιγράφουμε την μέθοδο Cayley-Dickson και μελετάμε την ταξινόμηση των Composition Αλγεβρών, η οποία δίνεται από το θεώρημα του Hurwitz. Επιπλέον, δίνουμε κάποιες περαιτέρω ιδιότητες των Composition Αλγεβρών. Στο τελευταίο Κεφάλαιο δίνουμε κάποιες εφαρμογές των τετράδων και των οκτάδων.

Abstract

In this diploma thesis we study Composition Algebras, their classification and some applications of them. In Chapter 1 we define some basic algebraic structures, vector spaces and algebras. Also, we write about bilinear and quadratic forms. In Chapter 2 we define Composition Algebras and we study some properties of them. Also, we describe Quaternions and Octonions which are Composition Algebras with dimensions 4, 8 respectively. In Chapter 3 we describe the Cayley-Dickson process and we study the classification of Composition Algebras, which is given by the Hurwitz theorem . Futhermore, we give some further properties of Composition Algebras. In the last Chapter we give some applications of Quaternions and Octonions.

Κεφάλαιο 1

Άλγεβρες

1.1 Βασικές αλγεβρικές δομές και διανυσματικοί χώροι

Έστω ένα μη κενό σύνολο S. Μία απεικόνιση $\star$ της μορφής $\star : S \times S \to S$ ονομάζεται **εσωτερική πράξη**.

Ορισμός 1.1.1. *Ένα μη κενό σύνολο G εφοδιασμένο με μία εσωτερική πράξη $\circ$ ονομάζεται **ομάδα** αν ισχύουν τα παρακάτω:*

1. $(a \circ b) \circ c = a \circ (b \circ c)$, *για κάθε $a, b, c \in G$ (προσεταιριστική ιδιότητα),*
2. *Υπάρχει $e \in G$ τέτοιο ώστε $a \circ e = e \circ a$, για κάθε $a \in G$ (ύπαρξη ουδετέρου στοιχείου),*
3. *Για κάθε $a \in G$ υπάρχει $a' \in G$ τέτοιο ώστε $a \circ a' = a' \circ a = e$ (ύπαρξη συμμετρικού στοιχείου).*

Η ομάδα G λέγεται **αβελιανή** αν η πράξη $\circ$ είναι μεταθετική. Η αλγεβρική δομή $(G, \circ)$ ονομάζεται **ημιομάδα** αν η πράξη $\circ$ είναι προσεταιριστική.

Ορισμός 1.1.2. *Η αλγεβρική δομή $(R, +, \cdot)$, όπου οι πράξεις $+$ και $\cdot$ είναι εσωτερικές πράξεις στο R, ονομάζεται **δακτύλιος** αν ισχύουν τα ακόλουθα:*

1. *Η αλγεβρική δομή $(R, +)$ είναι αβελιανή ομάδα,*

2. *Η αλγεβρική δομή $(R, \cdot)$ είναι ημιομάδα,*

3. *Η πράξη $\cdot$ είναι επιμεριστική ως προς την πράξη $+$, δηλαδή για κάθε $a, b, c \in R$ ισχύουν οι παρακάτω σχέσεις:*
   $a \cdot (b + c) = a \cdot b + a \cdot c$,
   $(b + c) \cdot a = b \cdot a + c \cdot a$.

Υποδακτύλιος ενός δακτυλίου λέγεται ένα υποσύνολο του δακτυλίου, που είναι δακτύλιος με τις πράξεις που κληρονομεί από το μεγάλο δακτύλιο. Αν για κάποιο δακτύλιο R υπάρχει ένας θετικός ακέραιος n τέτοιος ώστε $n \cdot a = 0$, για κάθε $a \in R$, τότε ο μικρότερος τέτοιος φυσικός αριθμός λέγεται **χαρακτηριστική του δακτυλίου** R. Αν δεν υπάρχει τέτοιος φυσικός αριθμός, λέμε οτι ο R είναι **χαρακτηριστικής** 0.

Ορισμός 1.1.3. *Έστω $R, \;\; R'$ δύο δακτύλιοι. Μία απεικόνιση $\phi : R \to R'$ λέγεται **ομομορφισμός δακτυλίων** αν οι παρακάτω δύο ιδιότητες ικανοποιούνται για κάθε $a, b \in R$:*

1. *$\phi(a + b) = \phi(a) + \phi(b)$,*

2. *$\phi(ab) = \phi(a)\phi(b)$.*

*Αν η ϕ είναι ομομορφισμός δακτυλίων, 1-1 και επί, τότε ονομάζεται **ισομορφισμός δακτυλίων**. Η ϕ είναι 1-1 αν και μόνο αν $ker\phi = \{a \in R | \phi(a) = 0'\} = \{0\}$ (**πυρήνας** της ϕ).*

Ορισμός 1.1.4. *Ένας δακτύλιος R στον οποίο ο πολλαπλασιασμός είναι μεταθετική πράξη λέγεται **μεταθετικός δακτύλιος**. Ένας δακτύλιος με πολλαπλασιαστικό ταυτοτικό στοιχείο 1, για το οποίο ισχύει $1 \cdot x = x \cdot 1 = x$, για κάθε $x \in R$, λέγεται **δακτύλιος με μοναδιαίο στοιχείο**.*

Ορισμός 1.1.5. *Έστω R ένας δακτύλιος με μοναδιαίο στοιχείο. Ένα στοιχείο x του R λέγεται **μονάδα** του R αν έχει πολλαπλασιαστικό αντίστροφο στο R. Αν κάθε μη μηδενικό* *στοιχείο του R είναι μονάδα, τότε ο R λέγεται **δακτύλιος διαίρεσης**. **Σώμα** λέγεται ένας μεταθετικός δακτύλιος διαίρεσης.*

Παράδειγμα 1.1.1. *Η αλγεβρική δομή $(\mathbb{R}, +, \cdot)$ είναι το σώμα των **πραγματικών αριθμών**. Η αλγεβρική δομή $(\mathbb{C}, +, \cdot)$ είναι το σώμα των **μιγαδικών αριθμών**.*

Ορισμός 1.1.6. *Ένα σώμα E λέγεται **επέκταση σώματος** ενός σώματος K αν το K είναι υποσώμα του E (δηλαδή το K είναι υποσύνολο του E, το οποίο αποτελεί σώμα με τις πράξεις που κληρονομεί από το E). Συμβολίζουμε: E/K.*

Ένα μη σταθερό πολυώνυμο $f(x) \in K[x]$ ονομάζεται **ανάγωγο πάνω από το σώμα** K αν δεν μπορούμε να γράψουμε το $f(x)$ σα γινόμενο δύο πολυωνύμων του $K[x]$, τα οποία να έχουν, και τα δύο, βαθμό μικρότερο από το βαθμό του $f(x)$. Το σύνολο $K[x]$ αποτελείται από όλα τα πολυώνυμα μίας μεταβλητής x, τα οποία έχουν συντελεστές από το σώμα K. Ένα στοιχείο a μίας επέκτασης E ενός σώματος K λέγεται **αλγεβρικό πάνω από το** K αν $f(a) = 0$, για κάθε μη μηδενικό πολυώνυμο του $K[x]$. Μία επέκταση E ενός σώματος K λέγεται **αλγεβρική επέκταση** του K αν κάθε στοιχείο του E είναι αλγεβρικό πάνω στο K.

Έστω E μία επέκταση σώματος του σώματος K. Αν το E έχει πεπερασμένη διάσταση σα διανυσματικός χώρος πάνω από το σώμα K, τότε η διάσταση αυτή ονομάζεται **βαθμός της επέκτασης σώματος**. Αν ο βαθμός αυτός ισούται με 2, τότε η επέκταση ονομάζεται **τετραγωνική επέκταση (quadratic extension)**. Μία **διαχωρίσιμη επέκταση σώματος (separable field extension)** είναι μία αλγεβρική επέκταση σώματος E ενός σώματος K, τέτοια ώστε για κάθε $a \in K$, το ελάχιστο (minimal) πολυώνυμο του a, με συντελεστές από το σώμα K, να είναι ένα **διαχωρίσιμο πολυώνυμο (separable polynomial)** (δηλαδή ένα πολυώνυμο που έχει τόσες διακριτές ρίζες όσες ο βαθμός του).

Το **ελάχιστο (minimal)** πολυώνυμο p του a, με συντελεστές από το σώμα K, είναι ένα ανάγωγο πολυώνυμο του $K[x]$, τέτοιο ώστε $p(a) = 0$. Αυτό το ανάγωγο πολυώνυμο είναι μονοσήμαντα ορισμένο , εκτός ίσως από έναν σταθερό παράγοντα στο σώμα K και είναι ένα πολυώνυμο με τον ελάχιστο δυνατό βαθμό ≥ 1 στον $K[x]$, το οποίο έχει το a ως ρίζα.

Ορισμός 1.1.7. *Έστω ότι το μη κενό σύνολο V είναι εφοδιασμένο με δύο πράξεις, μία εσωτερική πράξη, την **πρόσθεση**:*

$$+ : V \times V \to V, (x, y) \mapsto x + y$$

*και μία εξωτερική πράξη με συντελεστές από ένα σώμα K, το **βαθμωτό πολλαπλασιασμό**:*

$$\cdot : K \times V \to V, (\lambda, x) \mapsto \lambda \cdot x = \lambda x$$

έτσι ώστε για κάθε $x, y, z \in V$, $\lambda, \mu \in K$,να ισχύουν:

1. $x + y = y + x$ *(μεταθετική ιδιότητα),*
2. $(x + y) + z = x + (y + z)$ *(προσεταιριστική ιδιότητα),*
3. *Υπάρχει* $0 \in V$ *τέτοιο ώστε:* $x + 0 = x$ *(ουδέτερο στοιχείο),*
4. *Για κάθε* $x \in V$ *υπάρχει* $-x \in V$ *τέτοιο ώστε* $x + (-x) = 0$ *(αντίθετο στοιχείο),*
5. $(\lambda + \mu)x = \lambda x + \mu x$ *(επιμεριστική ιδιότητα ως προς την πρόσθεση του K),*
6. $\lambda(x + y) = \lambda x + \lambda y$ *(επιμεριστική ιδιότητα ως προς την πρόσθεση του V),*
7. $(\lambda\mu)x = \lambda(\mu x)$*,*
8. $1 \cdot x = x$.

*Τότε το σύνολο V ονομάζεται **διανυσματικός χώρος** πάνω στο σώμα K.*

Ορισμός 1.1.8. *Ένα μη κενό υποσύνολο U ενός διανυσματικού χώρου V λέγεται **διανυσματικός υπόχωρος** ή απλά **υπόχωρος** του V αν για κάθε $\lambda \in K$ και $x, y \in U$ ισχύουν τα παρακάτω:*

1. $\lambda x \in U$*,*
2. $x + y \in U$.

Ορισμός 1.1.9. *1. Τα στοιχεία $x_1, x_2, ..., x_n$, όπου $n \in \mathbb{N}^*$, του διανυσματικού χώρου V πάνω στο σώμα K ονομάζονται **γραμμικώς ανεξάρτητα** αν ισχύει η συνεπαγωγή:*

$$\lambda_1 x_1 + \lambda_2 x_2 + ... + \lambda_n x_n = 0, \lambda_1, \lambda_2, ..., \lambda_n \in K \Rightarrow \lambda_1 = \lambda_2 = ... = \lambda_n = 0.$$

*2. Το υποσύνολο $\{x_1, x_2, ..., x_n\}$ του διανυσματικού χώρου V, πάνω στο σώμα K, είναι μία **βάση** του V αν ισχύουν τα ακόλουθα:*

(α΄) Τα $x_1, x_2, ..., x_n$ είναι γραμμικώς ανεξάρτητα,

(β΄) $\{\lambda_1 x_1 + \lambda_2 x_2 + ... + \lambda_n x_n : \lambda_1, \lambda_2, ..., \lambda_n \in K\} = V$, δηλαδή τα $x_1, x_2, ..., x_n$ παράγουν το χώρο V.

*3. Έστω V διανυσματικός χώρος πάνω στο σώμα K. Αν ο V έχει πεπερασμένη βάση, τότε ο κοινός αριθμός που εκφράζει το πλήθος των στοιχείων κάθε βάσης αυτού ονομάζεται **διάσταση** του διανυσματικού χώρου V και συμβολίζεται με dimV. Τότε λέμε ότι ο διανυσματικός χώρος V είναι **πεπερασμένης διάστασης**. Αν ο διανυσματικός χώρος V δεν έχει πεπερασμένη βάση, τότε λέμε ότι ο V είναι **άπειρης διάστασης**.*

Θεώρημα 1.1.1. *Αν ο V είναι διανυσματικός χώρος πάνω στο σώμα K πεπερασμένης διάστασης, έστω n, τότε κάθε γραμμικώς ανεξάρτητο υποσύνολό του επεκτείνεται σε μία βάση του V.*

Ορισμός 1.1.10. *Αν U_1, U_2 είναι υπόχωροι του διανυσματικού χώρου V, τότε και το σύνολο:*

$$U_1 + U_2 := \{x_1 + x_2 | x_1 \in U_1, x_2 \in U_2\}$$

*είναι υπόχωρος του V και ονομάζεται **άθροισμα των υποχώρων** U_1 και U_2.*

Ορισμός 1.1.11. *Αν U_1, U_2 είναι υπόχωροι του διανυσματικού χώρου V, τότε και το σύνολο:*

$$U_1 \cap U_2 := \{x | x \in U_1 \text{ και } x \in U_2\}$$

*είναι υπόχωρος του V και ονομάζεται **τομή των υποχώρων** U_1 και U_2.*

Ορισμός 1.1.12. *Ο διανυσματικός χώρος* V *είναι το* ***ευθύ άθροισμα*** *των υποχώρων* $U_1, U_2, ...U_n$*, όπου* $n \in \mathbb{N}^*$*, αν ισχύουν τα εξής:*

1. $V = U_1 + U_2 + ... + U_n$,

2. *Κάθε* $x \in V$ *μπορεί να γραφεί κατά μοναδικό τρόπο στη μορφή:*

   $x = x_1 + x_2 + ... + x_n$, *με* $x_i \in U_i$*, για κάθε* $i = 1, 2, ..., n$.

Συμβολικά γράφουμε: $V = U_1 \bigoplus U_2 \bigoplus ... \bigoplus U_n$.

Ορισμός 1.1.13. *Έστω οι διανυσματικοί χώροι* X, Y *πάνω στο σώμα* K*. Η απεικόνιση* $f : X \to Y$ *ονομάζεται* ***ομομορφισμός*** *διανυσματικών χώρων (ή* ***γραμμική απεικόνιση****) αν για κάθε* $x, y \in X, \lambda, \mu \in K$ *ισχύει:*

$$f(\lambda x + \mu y) = \lambda f(x) + \mu f(y).$$

Στην περίπτωση που είναι $X = Y$, τότε χρησιμοποιείται και ο όρος **ενδομορφισμός** διανυσματικών χώρων.

1.2 Διγραμμικές και τετραγωνικές μορφές

Έστω K ένα σώμα και V ένας διανυσματικός χώρος πάνω στο σώμα K.

Ορισμός 1.2.1. *Μία απεικόνιση* $f : V \times V \to K$ *ονομάζεται* ***διγραμμική μορφή*** *πάνω στο διανυσματικό χώρο* V *αν για κάθε* $x, y, z \in V$ *και* $\lambda, \mu \in K$ *ισχύουν τα εξής:*

1. $f(\lambda x + \mu y, z) = \lambda f(x, z) + \mu f(y, z)$,

2. $f(x, \lambda y + \mu z) = \lambda f(x, y) + \mu f(x, z)$.

Μία διγραμμική μορφή καλείται ***συμμετρική*** *αν:*

$$f(x, y) = f(y, x),$$

*για κάθε $x, y \in V$ και **αντισυμμετρική** αν:*

$$f(x, y) = -f(y, x),$$

*για κάθε $x, y \in V$. Στην περίπτωση που το σώμα K είναι χαρακτηριστικής 2, η αντισυμμετρική μορφή πρέπει να ικανοποιεί τη συνθήκη $f(x, x) = 0$, για κάθε $x \in V$, επειδή $2f(x, x) = 0$, για κάθε $x \in V$, αφού $f(x, x) \in K$, για κάθε $x \in V$. Αν η χαρακτηριστική του σώματος K δεν είναι 2, τότε οποιαδήποτε συμμετρική ή αντισυμμετρική μορφή είναι **αυτοπαθής ή ανακλαστική**, δηλαδή για κάθε $x, y \in V$ ισχύει ότι:*

$$f(x, y) = 0 \Leftrightarrow f(y, x) = 0.$$

Έστω V ένας διανυσματικός χώρος και $\{u_1, u_2, ...u_n\}$ μία βάση του V πάνω στο σώμα K, όπου $n \in \mathbb{N}^*$. Τότε κάθε διγραμμική μορφή μπορεί να εκφραστεί με συντεταγμένες με τον ακόλουθο τροπο:
Για οποιαδήποτε δύο στοιχεία $x = \sum_{i=1}^{n} x_i u_i$ και $y = \sum_{j=1}^{n} y_j u_j$ του διανυσματικού χώρου V, όπου $x_i, y_j \in K$ για κάθε $i, j \in \{1, ..., n\}$, έχουμε:

$$\begin{aligned} f(x, y) &= f(\sum_{i=1}^{n} x_i u_i, y) \\ &= \sum_{i=1}^{n} x_i f(u_i, y) \\ &= \sum_{i=1}^{n} x_i f(u_i, \sum_{j=1}^{n} y_j u_j) \\ &= \sum_{i,j=1}^{n} f(u_i, u_j) x_i y_j \\ &= \sum_{i,j=1}^{n} a_{ij} x_i y_j, \end{aligned}$$

όπου $a_{ij} = f(u_i, u_j)$. Μπορούμε να γράψουμε την παραπάνω σχέση χρησιμοποιώντας πίνακες, ως εξής:

$$f(x, y) = X^T AY,$$

όπου $X = (x_1, x_2, ..., x_n)^T, Y = (y_1, y_2, ..., y_n)^T$ είναι οι στήλες συντεταγμένων των x και y αντίστοιχα και ο πίνακας $A = (a_{ij}) \in M_n(K)$ καλείται **πίνακας της διγραμμικής μορφής** f στη βάση $\{u_1, u_2, ...u_n\}$.

Αν αλλάξουμε τη βάση $(u'_1, u'_2, ...u'_n) = (u_1, u_2, ...u_n)P$, όπου $P \in M_n(K)$, τότε οι στήλες συντεταγμένων των x και y δίνονται από τις σχέσεις: $X = PX'$ και $Y = PY'$. Επίσης:

$$\begin{aligned} f(x, y) &= X^T AY \\ &= (PX')^T APY' \\ &= X'^T P^T APY', \end{aligned}$$

δηλαδή ο πίνακας της διγραμμικής μορφης f στη βάση $\{u'_1, u'_2, ...u'_n\}$ είναι ο:

$$A' = P^T AP.$$

Παρατηρούμε ότι μια διγραμμική μορφή σε έναν πεπερασμένης διάστασης διανυσματικό χώρο είναι συμμετρική (αντίστοιχα αντισυμμετρική) αν και μόνο αν ο πίνακάς της είναι συμμετρικός $A^T = A$, δηλαδή $a_{ij} = a_{ji}$, για κάθε $i, j \in \{1, ..., n\}$ (αντίστοιχα αντισυμμετρικός $A^T = -A$, δηλαδή $a_{ij} = -a_{ji}$, για κάθε $i, j \in \{1, ..., n\}$). Πράγματι, αν f είναι συμμετρική μορφή, τότε επειδή $f(u_i, u_j) = f(u_j, u_i)$, για κάθε $i, j \in \{1, ..., n\}$, έχουμε ότι ο πίνακας A της f ως προς τη βάση $\{u_1, u_2, ...u_n\}$ είναι συμμετρικός. Αντίστροφα, αν ο πίνακας A της διγραμμικής μορφής f, ως προς τη βάση $\{u_1, u_2, ...u_n\}$ του διανυσματικού χώρου V, είναι συμμετρικός, τότε για κάθε $x, y \in V$ ισχύει:

$$\begin{aligned} f(x,y) &= \sum_{i,j=1}^{n} f(u_i,u_j)x_i y_j \\ &= \sum_{i,j=1}^{n} f(u_j,u_i)x_i y_j \\ &= f(y,x). \end{aligned}$$

Άρα, η f είναι συμμετρική. Με τον ίδιο τρόπο αποδεικνύεται η περίπτωση που η f είναι αντισυμμετρική.

Ορισμός 1.2.2. *Έστω η διγραμμική απεικόνιση $f : V \times V \to K$. Το **ριζικό** της διγραμμικής απεικόνισης f είναι ο υπόχωρος:*

$$radf = \{x \in V | f(x,y) = 0, \forall y \in V\}$$

(είναι υπόχωρος αν $radf$ δεν είναι κενό σύνολο).

Ορισμός 1.2.3. *Η διγραμμική μορφή f καλείται **μη εκφυλισμένη** αν $radf = \{0\}$, δηλαδή αν για κάθε $y \in V$ ισχύει ότι $f(x,y) = 0$, τότε $x = 0$.*

Έστω f μία συμμετρική ή αντισυμμετρική διγραμμική μορφή σε ένα διανυσματικό χώρο V πάνω σε ένα σώμα K (χαρακτηριστικής $\neq 2$ στην περίπτωση που είναι αντισυμμετρική).

Ορισμός 1.2.4. *Τα στοιχεία (ή διανύσματα) $x, y \in V$ ονομάζονται **κάθετα** αν $f(x,y) = 0$. Συμβολίζουμε $x \perp y$. Έστω U ένας υπόχωρος του V. Το **ορθογώνιο συμπλήρωμα** του U στο V (σε σχέση με την f) είναι ο υπόχωρος:*

$$U^{\perp} = \{x \in V | x \perp y, \forall y \in U\}$$

(είναι υπόχωρος αν $U^{\perp}$ δεν είναι κενό σύνολο). Συγκεκριμένα, $V^{\perp} = radf$.

Ορισμός 1.2.5. *Ένας υπόχωρος U ενός διανυσματικού χώρου V ονομάζεται* ***μη εκφυλισμένος*** *σε σχέση με τη διγραμμική μορφή f αν ο περιορισμός της f στο U, $f|_U$, είναι μη εκφυλισμένος.*

Πρόταση 1.2.1. *Έστω f μία διγραμμική μορφή σε έναν πεπερασμένης διάστασης διανυσματικό χώρο V, πάνω σε ένα σώμα K. Επίσης, έστω U ένας μη εκφυλισμένος, πεπερασμένης διάστασης υπόχωρος του V. Τότε $V = U \oplus U^{\perp}$. Αν επιπλέον η f είναι μη εκφυλισμένη διγραμμική μορφή, τότε ο $U^{\perp}$ είναι μη εκφυλισμένος.*

Απόδειξη. Ισχύει ότι:

$$U \cap U^{\perp} = \{0\}.$$

Πράγματι, $x \in U \cap U^{\perp} \Rightarrow x \in U$ και $x \in U^{\perp}$. Άρα, $f(x, y) = 0, \forall y \in U \Rightarrow x = 0$, επειδή ο U είναι μη εκφυλισμένος. Αρκεί να δειχθεί ότι:

$$V = U + U^{\perp} \Leftrightarrow dimV = dimU + dimU^{\perp}.$$

Έστω $n = dimV$ και $k = dimU$. Έστω η βάση $\{u_1, u_2, ...u_k\}$ του U και η επέκτασή της σε βάση $\{u_1, u_2, ...u_k, u_{k+1}, ..., u_n\}$ του V. Το τυχαίο $u \in U^{\perp}$ μπορούμε να το γράψουμε ως:

$$u = c_1u_1 + ... + c_nu_n, \text{ όπου } c_1, ..., c_n \in K.$$

Επίσης,

$u \in U^{\perp} \Rightarrow f(u_i, u) = 0, \forall 1 \leq i \leq k$

$\Rightarrow \sum_{j=1}^{n} f(u_i, u_j)c_j = 0$

$\Rightarrow \sum_{j=1}^{n} a_{ij}c_j = 0$

$\Rightarrow$ το u βρίσκεται στον μηδενικό χώρο ενός $k \times n$ πίνακα, ο οποίος βρίσκεται στις πρώτες k γραμμές του πίνακα A της διγραμμικής μορφής f

$\Rightarrow dimU^{\perp} \geq n - k$

$\Rightarrow dimU + dimU^{\perp} = dimU \oplus dimU^{\perp} \geq k + n - k = n$

$\Rightarrow U \oplus U^{\perp} = V.$

Έστω ότι η f είναι μη εκφυλισμένη διγραμμική μορφή και έστω ότι ο υπόχωρος $U^{\perp}$ είναι εκφυλισμένος. Έστω $x \in U^{\perp} \cap (U^{\perp})^{\perp}$. Αν αποδείξουμε ότι $x = 0$, τότε θα έχουμε αποδείξει το ζητούμενο. Έστω $y \in V$. Τότε μπορούμε να γράψουμε το y ως $y = u + u'$, όπου $u \in U, \ \ u' \in U^{\perp}$. Από υπόθεση, $x \in U^{\perp}$ και $x \in (U^{\perp})^{\perp}$, άρα $f(x, u) = 0$ και $f(x, u') = 0$. Λαμβάνοντας υπόψιν ότι η f είναι διγραμμική μορφή έχουμε:

$$f(x,u) + f(x,u') = f(x, u + u') = 0 \ \ \Rightarrow f(x,y) = 0, \forall y \in V \Rightarrow x = 0,$$

αφού η f είναι μη εκφυλισμένη.

$\square$

Πρόταση 1.2.2. *Έστω f μία μη εκφυλισμένη διγραμμική μορφή σε ένα διανυσματικό χώρο V πεπερασμένης διάστασης και έστω U ένας υπόχωρος του V. Τότε $(U^{\perp})^{\perp} = U$.*

Απόδειξη. Ισχύει ότι $x \in U \Rightarrow f(x,y) = 0, \forall y \in U^{\perp} \Rightarrow U \subseteq (U^{\perp})^{\perp}$. Επιπλέον, ισχύει ότι $V = U \oplus U^{\perp} = U^{\perp} \oplus (U^{\perp})^{\perp} \Rightarrow dimU = dim(U^{\perp})^{\perp}$. Άρα $(U^{\perp})^{\perp} = U$. $\square$

Ορισμός 1.2.6. *Έστω V διανυσματικός χώρος πάνω στο σώμα K. Μία απεικόνιση:*

$$n : V \rightarrow K$$

καλείται ***τετραγωνική μορφή*** *αν ισχύουν τα ακόλουθα:*

1. $n(ax) = a^2 n(x), \forall x \in V, \forall a \in K,$
2. *Η απεικόνιση $f(x,y) = n(x+y) - n(x) - n(y)$ είναι διγραμμική μορφή στον V.*

Η διγραμμική μορφή f ονομάζεται ***διγραμμική μορφή αντίστοιχη της*** *n και είναι συμμετρική. Επίσης, εύκολα προκύπτει ότι $n(0) = 0$. Μία τετραγωνική μορφή n ονομάζεται* ***μη εκφυλισμένη*** *αν η αντίστοιχη συμμετρική διγραμμική μορφή f είναι μη εκφυλισμένη. Σε αυτήν την περίπτωση, υπάρχει $x \in V$ ώστε $n(x) \neq 0$.*

Στην αλγεβρική θεωρία των τετραγωνικών μορφών (για σώματα χαρακτηριστικής $\neq 2$) είναι σύνηθες η αντίστοιχη διγραμμική μορφή να ορίζεται ως:

$$f(x,y) = [n(x+y) - n(x) - n(y)]/2.$$

Εδώ γίνεται η σύμβαση ότι ο παράγων $1/2$ δεν εισάγεται στην αντίστοιχη διγραμμική μορφή. Τα πλεονεκτήματα αυτής της σύμβασης, είναι το ότι η αντίστοιχη διγραμμική μορφή είναι καλά ορισμένη και για σώματα χαρακτηριστικής 2 και το ότι όταν το σώμα δεν έχει χαρακτηριστική 2, τότε οι εξισώσεις που προκύπτουν είναι πιο απλές, αφού δεν περιέχουν τον παράγοντα $1/2$ (βλ. [3]). Η σύμβαση αυτή συναντάται συχνά στη βιβλιογραφία ([16],[3], [6],[10], [15]).

1.3 Άλγεβρες

Ορισμός 1.3.1. *Μία* ***K-άλγεβρα*** *A είναι ένας διανυσματικός χώρος πάνω σε ένα σώμα K εφοδιασμένος με ένα διγραμμικό γινόμενο:*

$$\cdot : A \times A \to A, (x,y) \mapsto xy,$$

δηλαδή για κάθε $x, y, z \in A, \alpha, \beta \in K$ ισχύουν:

$$(\alpha x + \beta y)z = \alpha(xz) + \beta(yz),$$

$$x(\alpha y + \beta z) = \alpha(xy) + \beta(xz).$$

Το γινόμενο που ορίστηκε δεν ικανοποιεί κατ'ανάγκη την προσεταιριστική ιδιότητα.

Ορισμός 1.3.2. *Μία K-άλγεβρα A ονομάζεται:*

- ***προσεταιριστική (associative)*** *αν* $[x, y, z] = 0$*, για κάθε* $x, y, z \in A$ *,όπου:*

$$[x, y, z] = (xy)z - x(yz)$$

είναι ο ***προσεταιριστής (associator)*** *των* x, y*.*

- ***μεταθετική (commutative)*** *αν* $[x, y] = 0$*, για κάθε* $x, y \in A$ *,όπου:*

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

είναι ο ***μεταθέτης (commutator)*** *των* x, y*.*

- ***αντιμεταθετική (anticommutative)*** *αν* $x^2 = 0$*, για κάθε* $x \in A$*.*

Ορισμός 1.3.3. *Ως* ***γινόμενο*** *δύο υποσυνόλων* B, C *μιας* K*-άλγεβρας* A *ορίζεται το σύνολο:*

$$BC = \{bc | b \in B, c \in C\}.$$

Ένας ***ομομορφισμός*** $\phi : A \to A'$ *μεταξύ δύο* K*-αλγεβρών* A, A' *είναι ένας ομομορφισμός διανυσματικών χώρων που ικανοποιεί τη σχέση:*

$$\phi(xy) = \phi(x)\phi(y), \forall x, y \in A.$$

Ένας ***ισομορφισμός*** $\phi : A \to A'$ *μεταξύ δύο* K*-αλγεβρών* A, A' *είναι ένας ομομορφισμός* K*-αλγεβρών ο οποίος είναι 1-1 και επί.*
Ένας υπόχωρος B *της* K*-άλγεβρας* A *καλείται* ***υποάλγεβρα*** *της* A *αν είναι κλειστός ως προς τον πολλαπλασιασμό:*

$$\forall x, y \in B \Rightarrow xy \in B.$$

Ισοδύναμα:$BB \subseteq B$*. Ένας υπόχωρος* I *της* K*-άλγεβρας* A *καλείται* ***ιδεώδες*** *της* A *αν είναι κλειστός ως προς τον πολλαπλασιασμό με στοιχεία της* A*:*

$$\forall x \in I, \forall y \in A \Rightarrow xy \in I(\textbf{δεξιό ιδεώδες}) \;\; \textit{και} \;\; yx \in I(\textbf{αριστερό ιδεώδες}).$$

Ισοδύναμα, $AI + IA \subseteq I$. Ο μηδενικός υπόχωρος $\{0\}$ και η K-άλγεβρα A ονομάζονται ***μη γνήσια ιδεώδη****. Ένα στοιχείο $e \in A$ ονομάζεται* ***ταυτοτικό ή μοναδιαίο στοιχείο*** *της K-άλγεβρας A αν για κάθε $x \in A$ ισχύει:*

$$ex = xe = x.$$

Κάθε K-άλγεβρα A έχει το πολύ ένα μοναδιαίο στοιχείο.

Παράδειγμα 1.3.1. *Κάθε σώμα είναι άλγεβρα πάνω στον εαυτό του.*

Παράδειγμα 1.3.2. *Έστω V ένας διανυσματικός χώρος πάνω σε ένα σώμα K. Τότε οι ενδομορφισμοί:*

$$End_K V = \{f : V \to V | f(\alpha x + \beta y) = \alpha f(x) + \beta f(y), x, y \in V, \alpha, \beta \in K\},$$

με πράξεις την πρόσθεση και τη σύνθεση ενδομορφισμών, οι οποίες για κάθε $f, g \in End_K V, x \in V$ ορίζονται ως εξής:

$$(f + g)(x) = f(x) + g(x),$$

$$(f \circ g)(x) = f(g(x)),$$

αποτελούν μία προσεταιριστική άλγεβρα, η οποία δεν είναι μεταθετική. Η άλγεβρα αυτή είναι ισομορφική με την άλγεβρα πινάκων $M_n(K)$, η οποία έχει ως πράξεις την πρόσθεση και τον πολλαπλασιασμό πινάκων, όπου $n = dimV$.

Ορισμός 1.3.4. *'Εστω A μία K-άλγεβρα. Η διάσταση του διανυσματικού χώρου A, πάνω στο σώμα K, ονομάζεται* ***διάσταση της K-άλγεβρας*** *A.*

Ορισμός 1.3.5. *Για κάθε στοιχείο a μίας K-άλγεβρας A ορίζονται δύο γραμμικές απεικονίσεις:*

$$L_a : A \to A, x \mapsto ax,$$

$$R_a : A \to A, x \mapsto xa.$$

Αν $A \neq \{0\}$ και οι απεικονίσεις L_a, R_a είναι 1-1 και επί, για κάθε $a \in A\backslash\{0\}$, τότε η A λέγεται ***άλγεβρα διαίρεσης*** *πάνω στο σώμα K.*

Παράδειγμα 1.3.3. *Τα σώματα $\mathbb{R}$ και $\mathbb{C}$ είναι προσεταιριστικές, μεταθετικές άλγεβρες διαίρεσης διαστάσεων ένα και δύο αντίστοιχα. Θα δείξουμε ότι το $\mathbb{C}$ είναι άλγεβρα διαίρεσης. Πράγματι, αφού ο πολλαπλασιασμός στο $\mathbb{C}$ είναι μεταθετική πράξη έχουμε ότι αν $z_1 \neq 0 + 0i$, τότε η εξίσωση $xz_1 = z_1x = z_2$ έχει μοναδική λύση την:*

$$x = \frac{\overline{z_1}z_2}{|z_1|^2},$$

όπου αν $z_1 = a + bi$, με $a, b \in \mathbb{R}$, τότε ο $\overline{z_1} = a - bi$ είναι ο ***συζυγής μιγαδικός*** *του z_1 και $|z_1| = \sqrt{a^2 + b^2}$ είναι το* ***μέτρο*** *μιγαδικού αριθμού z_1. Επομένως, το $\mathbb{C}$ είναι άλγεβρα διαίρεσης.*

Παράδειγμα 1.3.4. *Οι άλγεβρες πινάκων $M_n(\mathbb{R})$ και $M_n(\mathbb{C})$ δεν είναι άλγεβρες διαίρεσης όταν $n > 1$. Πράγματι, δεν μπορούμε να λύσουμε τις εξισώσεις $AX = Y$ και $YA = B$ όταν ο πίνακας A είναι μη αντιστρέψιμος και ο B είναι αντιστρέψιμος.*

Ορισμός 1.3.6. *Μία K-άλγεβρα A* ***δεν έχει διαιρέτες του μηδενός*** *αν για κάθε $x, y \in A$:*

$$xy = 0 \Rightarrow x = 0 \text{ ή } y = 0.$$

Παράδειγμα 1.3.5. *Κάθε σώμα K δεν έχει διαιρέτες του μηδενός. Πράγματι, έστω $a, b \in K$ και έστω $a \neq 0$. Τότε αν $ab = 0$, έχουμε:*

$$(\frac{1}{a})(ab) = (\frac{1}{a})0 = 0.$$

Όμως, τοτε:

$$0 = (\frac{1}{a})(ab) = \Big[(\frac{1}{a})a\Big]b = 1b = b.$$

Άρα, δείξαμε ότι αν $ab = 0$ και $a \neq 0$, τότε $b = 0$ στο K, επομένως δεν υπάρχουν διαιρέτες του μηδενός στο K.

Πρόταση 1.3.1. *Έστω A μία K-άλγεβρα πεπερασμένης και μη μηδενικής διάστασης. Τότε:*

Η A είναι άλγεβρα διαίρεσης $\Leftrightarrow$ Η A δεν έχει διαιρέτες του μηδενός.

Απόδειξη. Η A είναι άλγεβρα διαίρεσης αν και μόνο αν οι απεικονίσεις L_a, R_a είναι 1-1 και επί για κάθε $a \in A\backslash\{0\}$. Επειδή η άλγεβρα είναι πεπερασμένης διάστασης, αυτό είναι ισοδύναμο με το ότι οι απεικονίσεις L_a, R_a είναι 1-1 για κάθε $a \in A\backslash\{0\}$, το οποίο είναι ισοδύναμο με το ότι η άλγεβρα A δεν έχει διαιρέτες του μηδενός. □

1.4 Τανυστικό γινόμενο διανυσματικών χώρων

Ορισμός 1.4.1. *Έστω V, W δύο διανυσματικοί χώροι πεπερασμένης διάστασης πάνω σε ένα σώμα K χαρακτηριστικής 0. Ένα **τανυστικό γινόμενο** $V \otimes_K W$ (ή $V \otimes W$) πάνω στο σώμα K των διανυσματικών χώρων V, W είναι ένας διανυσματικός χώρος T πάνω στο σώμα K εφοδιασμένος με μία διγραμμική απεικόνιση:*

$$\tau : V \times W \to T,$$

τέτοια ώστε για κάθε διγραμμική απεικόνιση:

$$B : V \times W \to E,$$

όπου E είναι ένας οποιοσδήποτε διανυσματικός χώρος πάνω στο σώμα K, να υπάρχει μοναδικός ομομορφισμός διανυσματικών χώρων:

$$h : T \to E,$$

ο οποίος να ικανοποιεί:

$$h \circ \tau = B.$$

Θεώρημα 1.4.1. *Έστω V, W δύο διανυσματικοί χώροι πάνω σε ένα σώμα K.*

1. *Το τανυστικό γινόμενο των V και W πάνω στο σώμα K υπάρχει.*

2. *Αν (T,τ) και (T',τ') είναι τανυστικά γινόμενα πάνω στο σώμα K των V και W, τότε υπάρχει μοναδικός ισομορφισμός $f : T \to T'$ τέτοιος ώστε $f \circ \tau = \tau'$.*

3. *Αν $\{x_1, ..., x_n\}$ είναι μία βάση του V πάνω στο σώμα K και $\{y_1, ..., y_m\}$ είναι μία βάση του W πάνω στο σώμα K, τότε το σύνολο:*

$$\{\tau(x_i, y_j) : i = 1, ..., n \ \text{και} \ j = 1, ..., m\}$$

   είναι μία βάση του τανυστικού γινομένου T πάνω στο σώμα K. Άρα, ο T είναι πεπερασμένης διάστασης διανυσματικός χώρος πάνω στο σώμα K και $dimT = (dimV)(dimW)$.

Για τα στοιχεία $\tau(x,y)$ του T, $x \in V, y \in W$, χρησιμοποιούμε το συμβολισμό $x \otimes y$.

Ορισμός 1.4.2. *Έστω V ένας διανυσματικός χώρος πάνω σε ένα σώμα K και P μία επέκταση σώματος του K, η οποία είναι πεπερασμένης διάστασης διανυσματικός χώρος πάνω στο K. Σχηματίζουμε το τανυστικό γινόμενο $P \otimes_K V$ και το θεωρούμε ως έναν διανυσματικό χώρο πάνω στο σώμα P ορίζοντας:*

$$p(\sum p_i \otimes x_i) = \sum pp_i \otimes x_i.$$

Αυτό είναι καλά ορισμένο και τα αξιώματα για το διανυσματικό χώρο $P \otimes_K V$ πάνω στο σώμα P ισχύουν. Συμβολίζουμε με $V(P)$ αυτό το διανυσματικό χώρο πάνω στο σώμα P και τον ονομάζουμε διανυσματικό χώρο που προέρχεται από τον V ***επεκτείνοντας το σώμα βάση*** *K στο σώμα P.*

Πρόταση 1.4.1. *Έστω V ένας διανυσματικός χώρος πάνω σε ένα σώμα K με βάση $\{x_1, ..., x_m\}$. Τότε τα στοιχεία $1 \otimes x_1, ..., 1 \otimes x_m$ αποτελούν μία βάση του $V(P)$ πάνω στο P, όπου P είναι η επέκταση σώματος του K. Άρα, η διάσταση του V πάνω στο K ισούται με τη διάσταση του $V(P)$ πάνω στο P.*

Απόδειξη. Θέτουμε $\overline{x_i} = 1 \otimes x_i$, όπου $i = 1, ..., m$. Τότε για $p \in P$ έχουμε:

$$p\overline{x_i} = p(1 \otimes x_i) = p \otimes x_i.$$

Άρα, αφού κάθε $x \in V(P)$ έχει τη μορφή $\sum_{i=1}^{m} p_i \otimes x_i$, το x έχει επίσης τη μορφή $\sum_{i=1}^{m} p_i \overline{x_i}$. Άρα τα $\overline{x_i}$, όπου $i = 1, ..., m$, είναι γεννήτορες του διανυσματικού χώρου $V(P)$ πάνω στο σώμα P. Μένει να δειχθεί ότι τα $\overline{x_i}$ είναι γραμμικώς ανεξάρτητα. Πράγματι, έστω $\lambda_1, ...\lambda_m \in P$ τέτοια ώστε:

$$\sum_{i=1}^{m} \lambda_i \overline{x_i} = 0 \Rightarrow 1 \otimes \sum_{i=1}^{m} \lambda_i x_i = 0. \tag{1.1}$$

Για να δείξουμε ότι:

$$\lambda_1 = ... = \lambda_m = 0$$

αρκεί να δείξουμε ότι για τυχαίο $k \in \{1, ..., m\}$ ισχύει $\lambda_k = 0$. Θεωρούμε τον P ως διανυσματικό χώρο πάνω στο σώμα K και ορίζουμε τη διγραμμική απεικόνιση:

$$B : P \times V \to P, \;\; (p, \sum_{i=1}^{m} \mu_i x_i) \mapsto \mu_k.$$

Τότε, από τον ορισμό του τανυστικού γινομένου, υπάρχει μοναδικός ομομορφισμός διανυσματικών χώρων:

$$h : P \otimes_K V \to P \;\text{ ώστε }\; h \circ \tau = B,$$

όπου $\tau : P \times V \to P \otimes_K V$ η διγραμμική μορφή με την οποία είναι εφοδιασμένος ο διανυσματικός χώρος $P \otimes_K V$. Εφαρμόζοντας την h στην (1.1), έχουμε:

$$h(1 \otimes \sum_{i=1}^{m} \lambda_i x_i) = 0 \Rightarrow B(1, \sum_{i=1}^{m} \lambda_i x_i) = 0 \Rightarrow \lambda_k = 0.$$

$\square$

Έστω A μία K-άλγεβρα, P μία επέκταση σώματος του K και $A(P) = P \otimes_K A$ ο διανυσματικός χώρος που προκύπτει από την επέκταση του σώματος βάσης. Τότε ο διανυσματικός χώρος $A(P)$ γίνεται P-άλγεβρα με τον πολλαπλασιασμό:

$$(\sum p_i \otimes x_i)(\sum q_j \otimes y_j) = \sum p_i q_j \otimes x_i y_j.$$

Έστω $\{x_1, ..., x_m\}$ μία βάση της K-άλγεβρας A και έστω οι σταθερές δομής $c_{ij}^k \in K$ που δίνονται από:

$$x_i x_j = \sum_{k=1}^{m} c_{ij}^k x_k.$$

Όπως και πριν, τα στοιχεία $\{\overline{x_1}, ..., \overline{x_m}\}$, με $\overline{x_i} = 1 \otimes x_i, i = 1, ..., m$ αποτελούν βάση της $A(P)$ πάνω στο P και επίσης:

$$\begin{aligned}\overline{x_i}\ \overline{x_j} &= (1 \otimes x_i)(1 \otimes x_j) \\ &= 1 \otimes x_i x_j \\ &= \sum_{k=1}^{m} c_{ij}^k \overline{x_k},\end{aligned}$$

δηλαδή οι σταθερές δομής που είναι αντίστοιχες με τη βάση της $A(P)$ είναι οι ίδιες.

Στη συνέχεια θα θεωρούμε ότι οι K-άλγεβρες έχουν ταυτοτικό στοιχείο. Στη γενική περίπτωση, η έλλειψη ταυτοτικού στοιχείου μπορεί να ξεπεραστεί με τον παρακάτω τροπο: Έστω A μία K-άλγεβρα και $A_1 = K \times A = \{(a, x) | a \in K, x \in A\}$ ένας διανυσματικός χώρος πάνω στο σώμα K εφοδιασμένος με το γινόμενο: για $(a, x), (b, y) \in K \times A$, θέτουμε:

$$(a, x) \cdot (b, y) = (ab, bx + ay + xy) \in K \times A.$$

Τότε η A_1 είναι μία K-άλγεβρα με ταυτοτικό στοιχείο $e = (1, 0)$. Επιπλέον, το $\{0\} \times A$ είναι ένα ιδεώδες στην A_1, το οποίο ως K-άλγεβρα είναι ισομορφικό με την A. Επίσης, η A_1 είναι μεταθετική (αντίστοιχα προσεταιριστική, αντίστοιχα πεπερασμένης διάστασης) αν και μόνο αν η A είναι.

Κεφάλαιο 2

Composition Άλγεβρες

2.1 Ορισμοί-Ιδιότητες

Ορισμός 2.1.1. *Μία K-άλγεβρα $A \neq \{0\}$ με μία τετραγωνική μορφή (συχνά αναφέρεται και ως νόρμα) $n : A \to K$ ονομάζεται* ***composition άλγεβρα*** *αν ισχύουν:*

1. $n(xy) = n(x)n(y), \forall x, y \in A,$
2. *Η τετραγωνική μορφή n είναι μη εκφυλισμένη,*
3. *Υπάρχει μοναδιαίο στοιχείο 1 στην A.*

Ένας μη εκφυλισμένος υπόχωρος B της composition άλγεβρας A καλείται ***υποάλγεβρα*** *της A αν περιέχει το μοναδιαίο στοιχείο 1 της A και αν είναι κλειστός ως προς τον πολλαπλασιασμό, δηλαδή $\forall x, y \in B \Rightarrow xy \in B$.*

Έστω δύο composition άλγεβρες A_1, A_2 με τετραγωνικές μορφές n_1, n_2 αντίστοιχα. Μία γραμμική, 1-1 και επί απεικόνιση $\phi : A_1 \to A_2$ ονομάζεται **ισομορφισμός** αν για κάθε $x, y \in A_1$ ικανοποιείται το ακόλουθο: $\phi(xy) = \phi(x)\phi(y)$.

Παράδειγμα 2.1.1. *Το $\mathbb{R}$ είναι μία composition $\mathbb{R}$-άλγεβρα με τετραγωνική μορφή:*

$$n : \mathbb{R} \to \mathbb{R}, \ \ x \mapsto n(x) := x^2.$$

Πράγματι, υπάρχει το 1 που είναι το μοναδιαίο στοιχείο του $\mathbb{R}$. Επίσης, για $x, y \in \mathbb{R}$ έχουμε:

$$n(xy) = (xy)^2 = x^2y^2 = n(x)n(y).$$

Τέλος, αρκεί να δείξουμε ότι η τετραγωνική μορφή n είναι μη εκφυλισμένη. Θεωρούμε την αντίστοιχη διγραμμική μορφή:

$$f : \mathbb{R} \times \mathbb{R} \to \mathbb{R}, \ \ (x, y) \mapsto f(x, y) := n(x + y) - n(x) - n(y).$$

Έστω ότι $f(x, y) = 0$, για κάθε $y \in \mathbb{R}$. Τότε:

$$n(x + y) - n(x) - n(y) = 0 \Rightarrow (x + y)^2 - x^2 - y^2 = 0 \Rightarrow 2xy = 0 \Rightarrow x = 0.$$

Παράδειγμα 2.1.2. *Το $\mathbb{C}$ είναι μία composition $\mathbb{R}$-άλγεβρα με τετραγωνική μορφή:*

$$n : \mathbb{C} \to \mathbb{R}, \ \ z \mapsto n(z) := z\overline{z} = |z|^2,$$

όπου $\overline{z}$ είναι ο συζυγής μιγαδικός αριθμός του z. Το ουδέτερο στοιχείο του πολλαπλασιασμού μιγαδικών αριθμών είναι ο μιγαδικός $1 + 0i = 1$. Επίσης, λαμβάνοντας υπόψιν ότι ο πολλαπλασιασμός μεταξύ μιγαδικών αριθμών είναι προσεταιριστική και μεταθετική πράξη, έχουμε:

$$\begin{aligned} n(z_1z_2) &= (z_1z_2)(\overline{z_1z_2}) \\ &= z_1z_2\overline{z_1}\ \ \overline{z_2} \\ &= z_1\overline{z_1}z_2\overline{z_2} = n(z_1)n(z_2), \end{aligned}$$

όπου $z_1, z_2 \in \mathbb{C}$. Τέλος, έστω η αντίστοιχη διγραμμική μορφή:

$$f : \mathbb{C} \times \mathbb{C} \to \mathbb{R}, \ \ (z_1, z_2) \mapsto f(z_1, z_2) := n(z_1 + z_2) - n(z_1) - n(z_2).$$

Έστω ότι $f(z_1, z_2) = 0$, για κάθε $z_2 \in \mathbb{C}$. Τότε:

$$
\begin{aligned}
n(z_1 + z_2) - n(z_1) - n(z_2) &= (z_1 + z_2)(\overline{z_1 + z_2}) - z_1\overline{z_1} - z_2\overline{z_2} \\
&= (z_1 + z_2)(\overline{z_1} + \overline{z_2}) - z_1\overline{z_1} - z_2\overline{z_2} \\
&= z_1\overline{z_2} + z_2\overline{z_1} = 0,
\end{aligned}
$$

από το οποίο συνεπάγεται ότι $z_1 = 0 + 0i$.

Έστω A μία composition άλγεβρα πάνω στο σώμα K. Για κάθε $x \in A$ έχουμε:

$$n(x) = n(1x) = n(1)n(x). \tag{2.1}$$

Αφού η τετραγωνική μορφή n είναι μη εκφυλισμένη, υπάρχει $y \in A$, ώστε $n(y) \neq 0$. Από την (2.1) για $x = y$ έχουμε:

$$n(y) = n(1y) = n(1)n(y) \Rightarrow n(y)n(y)^{-1} = n(1) \Rightarrow n(1) = 1.$$

Λήμμα 2.1.1. *Μία K-άλγεβρα A η οποία ικανοποιεί οποιεσδήποτε δύο από τις παρακάτω ιδιότητες, ικανοποιεί επίσης και την τρίτη ιδιότητα:*

1. $[x, x, y] = (xx)y - x(xy) = 0, \forall x, y \in A$,
2. $[x, y, x] = (xy)x - x(yx) = 0, \forall x, y \in A$,
3. $[x, y, y] = (xy)y - x(yy) = 0, \forall x, y \in A$.

*Μία τέτοια άλγεβρα λέγεται **εναλλάσσουσα (alternating)**. Μία άλγεβρα που ικανοποιεί τη συνθήκη (2) ονομάζεται **ευέλικτη (flexible)**.*

Πριν δώσουμε την απόδειξη του λήμματος, θα ορίσουμε ως **(12)-αντισυμμετρική** (αντίστοιχα **(23)-αντισυμμετρική**) την τριγραμμική απεικόνιση $f : A \times A \times A \to A$, για την οποία ισχύει:

$$f(x, y, z) = -f(y, x, z), \forall x, y, z \in A$$

(αντίστοιχα $f(x,y,z) = -f(x,z,y), \forall x,y,z \in A$). Μία τριγραμμική απεικόνιση είναι **αντισυμμετρική** αν και μόνο αν είναι (12)-αντισυμμετρική και (23)-αντισυμμετρική. Παρακάτω δίνεται η απόδειξη του λήμματος, λαμβάνοντας υπόψιν ότι για μία K-άλγεβρα A ο προσεταιριστής είναι μία τριγραμμική απεικόνιση $A \times A \times A \to A$ ([3]):

Απόδειξη. Έστω $x, y \in A$. Αν ισχύει η ιδιότητα (1), τότε:

$$\begin{aligned} 0 &= [x+y, x+y, z] \\ &= [x,x,z] + [x,y,z] + [y,x,z] + [y,y,z] \\ &= [x,y,z] + [y,x,z]. \end{aligned}$$

Άρα,

$$[y,x,z] = -[x,y,z],$$

δηλαδή (12)-αντισυμμετρική. Αν ισχύει η ιδιότητα (3), τότε:

$$\begin{aligned} 0 &= [x, y+z, y+z] \\ &= [x,y,y] + [x,y,z] + [x,z,y] + [x,z,z] \\ &= [x,y,z] + [x,z,y]. \end{aligned}$$

Άρα,

$$[x,z,y] = -[x,y,z],$$

δηλαδή (23)-αντισυμμετρική. Επομένως,

- Αν ισχύουν οι (1) και (3), τότε επειδή η απεικόνιση είναι αντισυμμετρική έχουμε ότι $[x,y,x] = -[x,x,y] = 0$, άρα ισχύει και η (2).
- Αν ισχύουν οι (1) και (2), τότε επειδή η απεικόνιση είναι (12)-αντισυμμετρική έχουμε ότι $[x,y,y] = -[y,x,y] = 0$, άρα ισχύει και η (3).
- Αν ισχύουν οι (2) και (3), τότε επειδή η απεικόνιση είναι (23)-αντισυμμετρική έχουμε ότι $[x,x,y] = -[x,y,x] = 0$, άρα ισχύει και η (1).

$\square$

Έστω $x, y, z \in A$ και A εναλλάσσουσα. Αφού ο προσεταιριστής είναι τριγραμμική απεικόνιση, ισχύουν τα εξής:

$$\begin{aligned}
[x+z, x+z, y] &= [x, x, y] + [x, z, y] + [z, x, y] + [z, z, y] \\
&= [x, z, y] + [z, x, y] = 0, \\
[x, y+z, y+z] &= [x, y, y] + [x, y, z] + [x, z, y] + [x, z, z] \\
&= [x, y, z] + [x, z, y] = 0.
\end{aligned}$$

Ορισμός 2.1.2. *Μία K-άλγεβρα A, με μοναδιαίο στοιχείο 1, καλείται **τετραγωνική πάνω στο σώμα** K **(quadratic over** K**)** αν κάθε στοιχείο x της A ικανοποιεί μία εξίσωση της μορφής:*

$$x^2 - t(x)x + n(x)1 = 0,$$

όπου $t(x), n(x) \in K$.

Για μία K-άλγεβρα A με μοναδιαίο στοιχείο το 1 μπορούμε να "ταυτίσουμε" το σώμα K με την υποάλγεβρα $K \cdot 1$ της άλγεβρας A, όπου 1 είναι το μοναδιαίο στοιχείο της A.

Λήμμα 2.1.2. *Έστω A μία composition άλγεβρα πάνω στο σώμα K. Τότε η A είναι εναλλάσσουσα και τετραγωνική πάνω στο σώμα K.*

Απόδειξη. Γνωρίζουμε ότι για την τετραγωνική μορφή $n : A \to K$ ισχύει:

$$n(xy) = n(x)n(y), \forall x, y \in A. \tag{2.2}$$

Έστω $x, y, w, z \in A$. Θέτουμε στην (2.2) $y = y + w$ και έχουμε:

$$n(x)n(y+w) = n(xy + xw). \tag{2.3}$$

Αφαιρώντας από την (2.3) την (2.2) και την εξίσωση που προκύπτει από την (2.2) αν θέσουμε $y = w$, έχουμε:

$$n(x)n(y+w) - n(x)n(y) - n(x)n(w) = n(xy+xw) - n(xy) - n(xw), \tag{2.4}$$

$$n(x)f(y,w) = f(xy,xw). \tag{2.5}$$

Θέτουμε $x = x + z$ στην εξίσωση (2.5) και προκύπτει:

$$n(x+z)f(y,w) = f(xy+zy, xw+zw). \tag{2.6}$$

Αφαιρώντας από την (2.6) την (2.5) και την εξίσωση που προκύπτει από την (2.5) αν θέσουμε $x = z$, έχουμε:

$$(n(x+z) - n(x) - n(z))f(y,w) = f(xy+zy, xw+zw) - f(xy,xw) - f(zy,zw), \tag{2.7}$$

$$f(x,z)f(y,w) = f(xy,zw) + f(xw,zy). \tag{2.8}$$

Στην (2.8) θέτουμε $z = 1$ και $y = xu$, όπου $u \in A$, και έχουμε:

$$f(x,1)f(xu,w) = f(x(xu),w) + f(xw,xu) \tag{2.9}$$

Αφού $f(xw,xu) = n(x)f(w,u)$, τότε από την (2.9) προκύπτει:

$$f(x(xu),w) + n(x)f(w,u) - f(x,1)f(xu,w) = 0, \tag{2.10}$$

το οποίο, λόγω του ότι η f είναι διγραμμική και συμμετρική, είναι ισοδύναμο με:

$$f(x(xu) + n(x)u - f(x,1)xu, w) = 0. \tag{2.11}$$

Αφού η f είναι μη εκφυλισμένη και το w είναι τυχαίο, συνεπάγεται ότι:

$$x(xu) + n(x)u - f(x,1)xu = 0, \forall x, u \in A. \tag{2.12}$$

Θέτουμε $u = 1$ στην εξίσωση (2.12) και έχουμε:

$$x^2 - f(x,1)x + n(x)1 = 0, \tag{2.13}$$

το οποίο αποδεικνύει ότι η A είναι τετραγωνική πάνω στο σώμα K. Για να δείξουμε ότι η A είναι εναλλάσσουσα, πολλαπλασιάζουμε την εξίσωση (2.13) από δεξιά με u και συγκρίνοντάς την με την εξίσωση (2.12) προκύπτει ότι $x^2u = x(xu)$. Αντίστοιχα, αποδεικνύεται ότι $ux^2 = (ux)x$. $\square$

Λήμμα 2.1.3. *Έστω (A, n), (A, n_1) δύο composition K-άλγεβρες με τετραγωνικές μορφές n, n_1 αντίστοιχα. Τότε $n = n_1$.*

Απόδειξη. Από την (2.13) έχουμε τα εξής για κάθε $x \in A$:

$$x^2 = f(x,1)x - n(x)1,$$
$$x^2 = f_1(x,1)x - n_1(x)1,$$

όπου f, f_1 είναι οι αντίστοιχες διγραμμικές μορφές των n, n_1. Οπότε, έχουμε:

$$f(x,1)x - n(x)1 = f_1(x,1)x - n_1(x)1. \tag{2.14}$$

Αν τα στοιχεία $x, 1$ είναι γραμμικώς ανεξάρτητα, τότε από την (2.14) προκύπτει ότι $n(x) = n_1(x)$. Αν τα στοιχεία $x, 1$ είναι γραμμικώς εξαρτημένα, τότε υπάρχει $\lambda \in K$ ώστε $x = \lambda 1$. Σε αυτήν την περίπτωση ισχύει:

$$n_1(x) = \lambda^2 n_1(1) = \lambda^2 = \lambda^2 n(1) = n(x).$$

Άρα και στις δύο περιπτώσεις ισχύει ότι $n(x) = n_1(x)$.

$\square$

Από το παραπάνω Λήμμα συμπεραίνουμε ότι έχει νόημα το να λέμε ότι ”η τετραγωνική μορφή n σχετίζεται με την composition άλγεβρα A”.

2.2 Η ενέλιξη (involution) μίας K-άλγεβρας

Ορισμός 2.2.1. *Ως **ενέλιξη (involution)** μίας K-άλγεβρας A ορίζεται ο ενδομορφισμός $\rho : A \to A$, ο οποίος ικανοποιεί τα ακόλουθα:*

1. $\rho(\rho(x)) = x$,

2. $\rho(xy) = \rho(y)\rho(x)$,

για κάθε $x, y \in A$.

Ορισμός 2.2.2. *Μία **άλγεβρα με ενέλιξη** (A, ρ) αποτελείται από μία K-άλγεβρα A μαζί με μία ενέλιξη ρ. Ένας **ομομορφισμός αλγεβρών με ενέλιξη** $\phi : (A, \rho) \to (A', \rho')$ είναι ένας ομομορφισμός αλγεβρών $\phi : A \to A'$ για τον οποίο ισχύει:*

$$\phi(\rho(x)) = \rho'(\phi(x)).$$

*Ένα **ιδεώδες μιας άλγεβρας με ενέλιξη** είναι ένα ιδεώδες I της A για το οποίο ισχύει:*

$$\rho(I) \subseteq I.$$

Επίσης,

$$I = \rho(\rho(I)) \subseteq I.$$

Άρα,

$$I = \rho(I).$$

Πρόταση 2.2.1. *Έστω A μία composition άλγεβρα με την τετραγωνική μορφή n και την αντίστοιχη διγραμμική μορφή f. Η απεικόνιση:*

$$x \mapsto \overline{x} = f(1, x)1 - x, \;\; x \in A,$$

όπου 1 είναι το μοναδιαίο στοιχείο της A, είναι μία ενέλιξη της A. Επιπλέον, για $x, y \in A$, ισχύουν τα παρακάτω:

1. $x\overline{x} = \overline{x}x = n(x)1$ *(άρα, $x\overline{x} \in K \cdot 1$),*
2. $n(\overline{x}) = n(x)$,
3. $f(\overline{x}, \overline{y}) = f(x, y)$.

*Επίσης, το στοιχείο $t(x)1 = x+\overline{x}$ ανήκει στην $K\cdot 1$ και κάθε $x \in A$ ικανοποιεί την εξίσωση $x^2 - t(x)x + n(x)1 = 0$. Το στοιχείο $\overline{x}$ ονομάζεται **συζυγής** του x και η απεικόνιση:*

$$t : A \to K, \;\; x \mapsto t(x) := f(1, x)$$

*ονομάζεται **ίχνος**.*

Απόδειξη. Αρχικά, θα δείξουμε ότι η απεικόνιση που ορίστηκε είναι ενέλιξη της A. Πράγματι, για $x, y \in A, a \in K$, ισχύουν τα ακόλουθα:

$$\begin{aligned} \overline{x+y} &= f(1, x+y)1 - (x+y) = f(1, x)1 + f(1, y)1 - x - y = \overline{x} + \overline{y}, \\ \overline{ax} &= f(1, ax)1 - ax = a(f(1, x)1 - x) = a\overline{x}. \end{aligned}$$

Άρα, η απεικόνιση είναι ενδομορφισμός. Επίσης,

$$\begin{aligned} f(1, 1) &= n(1+1) - n(1) - n(1) = n(2 \cdot 1) - n(1) - n(1) \\ &= 4n(1) - n(1) - n(1) = 2n(1) = 2 \end{aligned}$$

και:

$$\begin{aligned}\overline{\overline{x}} &= f(1,\overline{x})1-\overline{x}\\ &= f(1,f(1,x)1-x)1-f(1,x)1+x\\ &= f(1,1)f(1,x)1-f(1,x)1-f(1,x)1+x=x.\end{aligned}$$

Θα δείξουμε ότι για $x,y\in A$ ισχύει $\overline{x}\ \ \overline{y}=\overline{yx}$. Θέτουμε $x=y=1,\ \ z=x,\ \ ,w=y$ στην εξίσωση (2.8) και έχουμε:

$$f(1,x)f(1,y)=f(1,xy)+f(x,y), \tag{2.15}$$

$$f(1,xy)=f(1,yx). \tag{2.16}$$

Στη συνέχεια, αντικαθιστούμε στην (2.13) το x με $x+y,x,y$ και αφαιρούμε τις δύο τελευταίες εξισώσεις που προκύπτουν από την πρώτη. Λαμβάνοντας υπόψιν την (2.15), προκύπτει:

$$\begin{aligned}0 &= (x+y)^2-f(x+y,1)(x+y)+n(x+y)1-[x^2-f(x,1)x+n(x)1]-[y^2-f(y,1)y+n(y)1]\\ &= xy+yx-f(1,x)y-f(1,y)x+f(x,y)1\\ &= xy+yx-f(1,x)y-f(1,y)x+f(1,x)f(1,y)1-f(1,xy)1,\end{aligned} \tag{2.17}$$

οπότε:

$$\begin{aligned}\overline{x}\ \ \overline{y} &= (f(1,x)1-x)(f(1,y)1-y)\\ &= xy-f(1,x)y-f(1,y)x+f(1,x)f(1,y)1\\ &= f(1,xy)1-yx\\ &= f(1,yx)1-yx=\overline{yx}.\end{aligned}$$

Για το (1):

$$\begin{aligned} x\overline{x} &= x(f(1,x)1 - x) \\ &= f(1,x)x - x^2 \\ &= (f(1,x)1 - x)x = \overline{x}x. \end{aligned}$$

Επίσης,

$$\begin{aligned} x\overline{x} &= x(f(1,x)1 - x) \\ &= -(x^2 - f(1,x)x) = n(x)1. \end{aligned}$$

Η τελευταία ισότητα προκύπτει από την εξίσωση (2.13). Για το (2):

$$n(\overline{x})1 = \overline{x}\ \overline{\overline{x}} = \overline{x}x = n(x)1.$$

Άρα, $n(x) = n(\overline{x})$. Για το (3):

$$\begin{aligned} f(\overline{x}, \overline{y}) &= n(\overline{x} + \overline{y}) - n(\overline{x}) - n(\overline{y}) \\ &= n(\overline{x + y}) - n(\overline{x}) - n(\overline{y}) \\ &= n(x + y) - n(x) - n(y) = f(x, y). \end{aligned}$$

Τέλος, έχουμε ότι $t(x)1 = x + \overline{x} = f(1,x)1 \in K \cdot 1$ και από την (2.13):

$$x^2 - t(x)x + n(x)1 = x^2 - f(1,x)x + n(x)1 = 0.$$

□

Παράδειγμα 2.2.1. *Έχουμε ήδη δείξει ότι το $\mathbb{C}$ είναι μία composition $\mathbb{R}$-άλγεβρα με τετραγωνική μορφή:*

$$n : \mathbb{C} \to \mathbb{R}, \;\; z \mapsto n(z) := z\overline{z} = |z|^2.$$

Παρατηρούμε ότι:

$$a - bi = \overline{z} = f(1 + 0i, z)(1 + 0i) - z, \;\; z \in \mathbb{C},$$

όπου η f είναι η αντίστοιχη διγραμμική μορφή της n. Παρόμοια, για το $\mathbb{R}$ (το οποίο δείξαμε ότι είναι μία composition $\mathbb{R}$-άλγεβρα) έχουμε ότι:

$$x = \overline{x} = f(1, x)1 - x, \;\; x \in \mathbb{R}.$$

2.3 Η άλγεβρα των τετράδων (Quaternions)

Το 1833 ο Hamilton συνέλαβε την ιδέα της παράστασης των μιγαδικών αριθμών με διατεταγμένα ζεύγη πραγματικών αριθμών. Έτσι, θεώρησε τον ισομορφισμό:

$$\phi : \mathbb{C} \to \mathbb{R}^2, \;\; a + bi \mapsto (a, b)$$

και μέσω αυτού όρισε τη δομή αλγεβρικού σώματος πάνω στο $\mathbb{R}^2$ με τις παρακάτω πράξεις:

$$(a, b) + (c, d) = (a + b, c + d),$$
$$(a, b)(c, d) = (ac - bd, ad + bc).$$

Επίσης, θεώρησε το $\mathbb{R}^2$ σα διανυσματικό χώρο πάνω στο $\mathbb{R}$ με την πράξη:

$$\lambda(a, b) = (\lambda a, \lambda b), \;\; \text{όπου} \;\; \lambda \in \mathbb{R}.$$

Το σώμα $\mathbb{R}^2$ περιέχει μία ισομορφική εικόνα του σώματος των πραγματικών αριθμών μέσω της απεικόνισης:

$$\phi : \mathbb{R} \to \mathbb{C}, \;\; x \mapsto (x, 0).$$

Ενθουσιασμένος από τη σχέση μεταξύ των μιγαδικών αριθμών και της γεωμετρίας 2 διαστάσεων, ο Hamilton προσπάθησε για πολλά χρόνια να ορίσει τη δομή αλγεβρικού σώματος πάνω στο $\mathbb{R}^3$, το οποίο να περιέχει μία ισόμορφη εικόνα του $\mathbb{R}^2$. Προσπάθησε, δηλαδή, να εφεύρει μία "μεγαλύτερη" άλγεβρα η οποία να έχει παρόμοιο ρόλο στη γεωμετρία 3 διαστάσεων. Συγκεκριμένα, θεώρησε τις πράξεις:

$$(a_1, a_2, a_3) + (b_1, b_2, b_3) = (a_1 + b_1, a_2 + b_2, a_3 + b_3),$$

$$\lambda(a_1, a_2, a_3) = (\lambda a_1, \lambda a_2, \lambda a_3),$$

όπου $a_1, a_2, a_3, b_1, b_2, b_3, \lambda \in \mathbb{R}$. Επίσης, χρησιμοποίησε τους παρακάτω συμβολισμούς:

$$x_1 = (1, 0, 0), \ \ x_2 = (0, 1, 0), \ \ x_3 = (0, 0, 1),$$

$$(a_1, a_2, a_3) = a_1x_1 + a_2x_2 + a_3x_3.$$

O Hamilton προσπάθησε, χωρίς επιτυχία, να βρει έναν καλά ορισμένο πολλαπλασιασμό μεταξύ των τριπλετών (a_1, a_2, a_3), με $a_1, a_2, a_3 \in \mathbb{R}$, ο οποίος να ικανοποιεί την μεταθετική και την προσεταιριστική ιδιότητα. Συγκεκριμένα, χρησιμοποιώντας την επιμεριστική ιδιότητα έγραψε την ισότητα:

$$(a_1x_1 + a_2x_2 + a_3x_3)(b_1x_1 + b_2x_2 + b_3x_3) = \sum_{i=1}^{3} \sum_{j=1}^{3} a_ib_jx_ix_j,$$

από την οποία παρατήρησε ότι ο πολλαπλασιασμός ορίζεται πλήρως αν είναι γνωστά τα γινόμενα x_ix_j, με $i, j \in \{1, 2, 3\}$, όπου το x_1 είναι το μοναδιαίο στοιχείο και ισχύει $x_2x_3 = x_3x_2$. Ο πίνακας πολλαπλασιασμού που κατασκεύασε είναι ο εξής:

	x_1	x_2	x_3
x_1	x_1	x_2	x_3
x_2	x_2	$x_1 + (\beta - \beta^{-1})x_2$	βx_3
x_3	x_3	βx_3	$x_1 + \beta x_2 + \gamma x_3$

όπου $\beta, \gamma \in \mathbb{R}^*$. Παρατήρησε ότι:

$$(a, \beta a, \beta)(-\beta\gamma, \gamma, 0) = (0, 0, 0),$$

δηλαδή υπάρχουν διαιρέτες του μηδενός, το οποίο δεν ισχύει σε ένα σώμα. O Hamilton το 1843 θεώρησε τα $1, i, j$ στη θέση των x_1, x_2, x_3 και τον πίνακα:

	1	i	j
1	1	i	j
i	i	-1	
j	j		-1

Στον πίνακα αυτό άφησε τα γινόμενα ij, ji απροσδιόριστα, αλλά πάλι δεν είχε επιτυχία η προσπάθειά του, επειδή θεώρησε ότι η πράξη είναι μεταθετική, το οποίο οδηγεί σε άτοπο όπως φαίνεται παρακάτω. Πράγματι, έστω ότι $ij = ji = x1 + yi + zj$, όπου $x, y, z \in \mathbb{R}$. Τότε έχουμε:

$$\begin{aligned}
(ji)i &= j(ii) = j(-1) = -j, \\
(ji)i &= (x1 + yi + zj)i = xi + yi^2 + z(ji) \\
&= xi + y(-1) + z(x1 + yi + zj) \\
&= (zx - y)1 + (x + zy)i + z^2 j.
\end{aligned}$$

Άρα, έχουμε ότι $z^2 = -1, z \in \mathbb{R}$, το οποίο είναι άτοπο. Τελικά, την ίδια χρονιά θεώρησε τις τετράδες συμβολίζοντας:

$$1 = (1, 0, 0, 0), i = (0, 1, 0, 0), j = (0, 0, 1, 0), k = (0, 0, 0, 1).$$

Θεώρησε το 1 ως μοναδιαίο στοιχείο και:

$$ij = k, ji = -k,$$

$$i^2 = j^2 = k^2 = ijk = -1.$$

Επίσης, από την προσεταιριστική ιδιότητα:

$$\begin{aligned}
&k^2 = (ij)(ij) = i(ji)j = i(-ij)j = -i^2j^2 = -(-1)(-1) = -1,\\
&ik = i(ij) = i^2j = -j,\\
&ki = (ij)i = -ji^2 = j,\\
&jk = j(ij) = (ji)j = -ij^2 = (-i)(-1) = i.
\end{aligned}$$

Έτσι, θεώρησε τον πίνακα:

	1	i	j	k
1	1	i	j	k
i	i	-1	k	$-j$
j	j	$-k$	-1	i
k	k	j	$-i$	-1

Με αυτόν τον τρόπο ο Hamilton εισήγαγε την **άλγεβρα των τετράδων (quaternions)** η οποία είναι μία προσεταιριστική, αλλά όχι μεταθετική άλγεβρα πάνω στο σώμα των πραγματικών αριθμών. Με την κατασκευή αυτής της άλγεβρας, ο Hamilton άνοιξε το δρόμο για τη θεώρηση αλγεβρικών δομών στις οποίες δεν ισχύει η μεταθετικότητα. Η άλγεβρα των τετράδων είναι η εξής:

$$\mathbb{H} = \{a + bi + cj + dk | a, b, c, d \in \mathbb{R}\},$$

με πράξεις:

$$(a + bi + cj + dk) + (a' + b'i + c'j + d'k) = (a + a') + (b + b')i + (c + c')j + (d + d')k,$$

$$\lambda(a + bi + cj + dk) = \lambda a + (\lambda b)i + (\lambda c)j + (\lambda d)k,$$

$$(a + bi + cj + dk)(a' + b'i + c'j + d'k) = a'' + b''i + c''j + d''k,$$

όπου

$$a'' = aa' - bb' - cc' - dd',$$

$$b'' = ab' + ba' + cd' - dc',$$

$$c'' = ac' + ca' + db' - bd',$$

$$d'' = ad' + da' + bc' - cb'.$$

Η **συζυγής τετράδα** μίας τετράδας $q = a + bi + cj + dk$ είναι η $\overline{q} = a - bi - cj - dk$. Ισχύει ότι $q + \overline{q} = 2a \in \mathbb{R}$ και $q\overline{q} = a^2 + b^2 + c^2 + d^2 \in \mathbb{R}$. Η **νόρμα (ή μέτρο) της τετράδας** q είναι ο μη αρνητικός πραγματικός αριθμός $||q|| = \sqrt{a^2 + b^2 + c^2 + d^2}$. Ισχύει ότι $q\overline{q} = ||q||^2$ και για $\lambda \in \mathbb{R}$:

$$||\lambda q|| = |\lambda| \; ||q||.$$

Επίσης, για $q_1, q_2 \in \mathbb{H}$ ισχύουν τα εξής:

- $\overline{q_1 + q_2} = \overline{q_1} + \overline{q_2}$,
- $\overline{\overline{q}}_1 = q_1$,
- $\overline{q_1 q_2} = \overline{q_2} \; \overline{q_1}$.

Για να αποδειχθεί η τελευταία ισότητα, αρκεί να δειχθεί ότι ισχύει για την περίπτωση που τα q_1, q_2 είναι οποιεσδήποτε δύο από τις τετράδες i, j, k, το οποίο προκύπτει άμεσα χρησιμοποιώντας τον πίνακα πολλαπλασιασμού των τετράδων. Από τα παραπάνω προκύπτει ότι η συζυγία σαν απεικόνιση είναι ενέλιξη της άλγεβρας $\mathbb{H}$. Έστω q_1, q_2 δύο τετράδες. Τότε από τις παραπάνω σχέσεις και από την προσεταιριστικότητα του πολλαπλασιασμού των τετράδων, προκύπτει ότι:

$$\begin{aligned} ||q_1 q_2||^2 &= (q_1 q_2)(\overline{q_1 q_2}) \\ &= (q_1 q_2)(\overline{q_2}\ \overline{q_1}) \\ &= q_1(q_2 \overline{q_2})\overline{q_1} = ||q_1||^2 ||q_2||^2, \end{aligned} \tag{2.18}$$

οπότε, $||q_1 q_2|| = ||q_1||\ \ ||q_2||$.

Υπάρχει μία βασική διαφορά μεταξύ της διαίρεσης των τετράδων και της διαίρεσης των μιγαδικών αριθμών. Αφού ο πολλαπλασιασμός τετράδων δεν είναι μεταθετική πράξη, έχουμε δύο εξισώσεις:

$$q_2 x = q_1 \ \text{ και } \ y q_2 = q_1, q_2 \neq 0 + 0i + 0j + 0k,$$

άρα, δύο λύσεις:

$$x = \frac{\overline{q_2} q_1}{||q_2||^2}, \ \ y = \frac{q_1 \overline{q_2}}{||q_2||^2}.$$

Επίσης, κάθε τετράδα $q = a + bi + cj + dk \neq 0 + 0i + 0j + 0k$ έχει την **αντίστροφή** της που ορίζεται ως εξής:

$$q^{-1} = \frac{1}{a^2 + b^2 + c^2 + d^2}(a - bi - cj - dk).$$

Από τα παραπάνω γίνεται σαφές ότι η άλγεβρα των τετράδων είναι άλγεβρα διαίρεσης και η μοναδική ιδιότητα που δεν ικανοποιεί για να είναι σώμα, είναι η μεταθετικότητα του πολλαπλασιασμού.

Χρησιμοποιώντας τη σχέση $ij = k$, μπορούμε να γράψουμε οποιαδήποτε τετράδα $q =$

$a + bi + cj + dk$ με τη μορφή:

$$q = (a + bi) + (c + di)j, \text{ ή } q = z_1 + z_2 j,$$

όπου $z_1 = a + bi, \; z_2 = c + di$. Με αυτόν τον τρόπο, μπορέσαμε να γράψουμε μία τετράδα ως ένα ζεύγος μιγαδικών αριθμών. Αυτό αποτελεί μία γενίκευση της κατασκευής των μιγαδικών αριθμών σα ζεύγη πραγματικών αριθμών. Παρατηρούμε ότι:

$$(a + bi)j = j(a - bi)$$

και $j^2 = -1$. Αντίστοιχα, για τους μιγαδικούς αριθμούς ισχύει ότι $a + bi = a + ib$ και $i^2 = -1$. Άρα στην περίπτωση των τετράδων, ισχύει:

$$z_1 + z_2 j = z_1 + j\overline{z_2}$$

και ο πολλαπλασιασμός δύο τετράδων μπορεί να γραφτεί ως εξής (λαμβάνοντας υπόψιν ότι ο πολλαπλασιασμός των τετράδων είναι προσεταιριστική πράξη και ο πολλαπλασιασμός των μιγαδικών αριθμών είναι μεταθετική πράξη):

$$\begin{aligned}(z_1 + jz_2)(w_1 + jw_2) &= (z_1 + \overline{z_2}j)(w_1 + \overline{w_2}j) \\ &= (z_1 w_1 - w_2\overline{z_2}) + j(\overline{z_1}w_2 + w_1 z_2).\end{aligned}$$

Η παρατήρηση αυτή είναι απαραίτητο να γίνει, ώστε να είναι κατανοητή η μέθοδος Cayley-Dickson, η οποία θα οριστεί στο επόμενο κεφάλαιο.

Η συζυγής της q είναι η:

$$\overline{q} = a - bi - cj - dk = a - bi - (c + di)j = \overline{z_1} - z_2 j.$$

Έστω η τετραγωνική μορφή:

$$n : \mathbb{H} \to \mathbb{R}, \;\; q \mapsto n(q) := ||q||^2 = q\overline{q}.$$

Για την n δείξαμε ότι ισχύει $n(q_1 q_2) = n(q_1)n(q_2)$ (βλ. εξίσωση (2.18)), άρα η άλγεβρα των τετράδων $\mathbb{H}$ είναι μία composition $\mathbb{R}$-άλγεβρα.

2.4 Οι οκτάδες ή αριθμοί του Cayley (Octonions)

Οι οκτάδες ανακαλύφτηκαν το 1843 από τον John T.Graves. Το 1845 ο Arthur Cayley δημοσίευσε σε άρθρο του μία παρόμοια κατασκευή. Οι **οκτάδες (octonions)** $\mathbb{O}$ είναι μία μη προσεταιριστική, μη μεταθετική άλγεβρα διαίρεσης. Μπορούμε να θεωρήσουμε ότι με την άλγεβρα αυτή έχουμε το πρώτο παράδειγμα μη προσεταιριστικής άλγεβρας. Μία βάση της αποτελούν τα στοιχεία $1, i, j, k, l, li, lj, lk$, για τα οποία ισχύει:

$$i^2 = j^2 = k^2 = l^2 = (li)^2 = (lj)^2 = (lk)^2 = -1,$$

όπου το 1 είναι το μοναδιαίο στοιχείο του πολλαπλασιασμού. Δηλαδή έχουμε μία γενίκευση των μιγαδικών αριθμών με επτά φανταστικές μονάδες. Έχουμε:

$$\mathbb{O} = \{a_1 1 + a_2 i + a_3 j + a_4 k + a_5 l + a_6 li + a_7 lj + a_8 lk | a_s \in \mathbb{R}, s \in \{1, 2, ..., 8\}\},$$

με πράξεις την πρόσθεση και το βαθμωτό πολλαπλασιασμό που ορίζονται ως εξής:
Αν $x = a_1 1 + a_2 i + a_3 j + a_4 k + a_5 l + a_6 li + a_7 lj + a_8 lk, \;\; y = b_1 1 + b_2 i + b_3 j + b_4 k + b_5 l + b_6 li + b_7 lj + b_8 lk \in \mathbb{O}$,$\lambda \in \mathbb{R}$,

$$x+y = (a_1+b_1)1+(a_2+b_2)i+(a_3+b_3)j+(a_4+b_4)k+(a_5+b_5)l+(a_6+b_6)li+(a_7+b_7)lj+(a_8+b_8)lk,$$

$$\lambda x = (\lambda a_1)1 + (\lambda a_2)i + (\lambda a_3)j + (\lambda a_4)k + (\lambda a_5)l + (\lambda a_6)li + (\lambda a_7)lj + (\lambda a_8)lk.$$

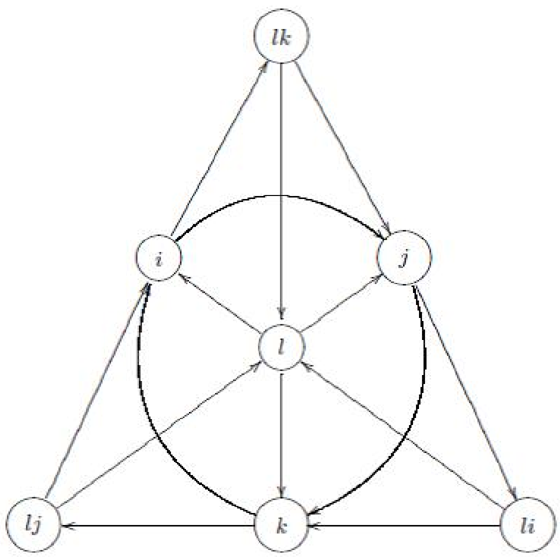
Ισχύει:

$$a_1 1 + a_2 i + a_3 j + a_4 k + a_5 l + a_6 li + a_7 lj + a_8 lk$$
$$= a_1 1 + a_2 i + a_3 j + a_4 k + l(a_5 + a_6 i + a_7 j + a_8 k) = q_1 + lq_2.$$

Άρα, μπορούμε να θεωρήσουμε τις οκτάδες ως εκφράσεις της μορφής $q_1 + lq_2$, όπου $q_1 = a_1 1 + a_2 i + a_3 j + a_4 k, q_2 = a_5 1 + a_6 i + a_7 j + a_8 k$ είναι δύο τετράδες. Έστω οι οκτάδες $q_1 + lq_2$ και $p_1 + lp_2$, όπου q_1, q_2, p_1, p_2 είναι τετράδες. Τότε, ο πολλαπλασιασμός τους ορίζεται ως εξής:

$$(q_1 + lq_2)(p_1 + lp_2) = (q_1 p_1 - p_2 \overline{q_2}) + l(\overline{q_1} p_2 + p_1 q_2).$$

Παρακάτω δίνεται ένα προβολικό επίπεδο επτά σημείων μέσω του οποίου μπορεί να καθοριστεί πλήρως ο πίνακας πολλαπλασιασμού των οκτάδων, ως εξής:



Κάθε ζευγάρι από τα στοιχεία της βάσης (εκτός από το 1) βρίσκεται σε μία μοναδική γραμμή και κάθε γραμμή περιέχει τρία στοιχεία. Το γινόμενο δύο οποιονδήποτε από τα επτά στοιχεία i, j, k, l, li, lj, lk δίνεται από το τρίτο στοιχείο της ευθείας που τα συνδέει, με πρόσημο το οποίο καθορίζεται από τα βέλη (ακολουθώντας κυκλική φορά όπως δείχνουν τα βέλη). Δηλαδή, αν τα a, b, c είναι στην ίδια γραμμή και με αυτή τη σειρά κυκλικά ταξινομημένα τότε $ab = c$ και $ba = -c$.

Ως **συζυγής οκτάδα** της οκτάδας x, ορίζεται η οκτάδα:

$$\overline{x} = a_1 1 - a_2 i - a_3 j - a_4 k - a_5 l - a_6 li - a_7 lj - a_8 lk.$$

και αν γράψουμε το x στη μορφή $x = q_1 + lq_2$, $q_1, q_2 \in \mathbb{H}$, τότε $\overline{x} = \overline{q_1} - lq_2$. Ισχύει ότι $x + \overline{x} = 2a_1 1 \in \mathbb{R}$. Επίσης, για $x, y \in \mathbb{O}$, ισχύουν:

1. $\overline{\overline{x}} = x$,
2. $\overline{x + y} = \overline{x} + \overline{y}$,
3. $\overline{xy} = \overline{y}\ \overline{x}$,

άρα η συζυγία σαν απεικόνιση είναι ενέλιξη της άλγεβρας $\mathbb{O}$.Για να αποδειχθεί η τελευταία ισότητα, αρκεί να δειχθεί ότι ισχύει για την περίπτωση που τα x, y είναι οποιεσδήποτε δύο από τις οκτάδες i, j, k, l, li, lj, lk, το οποίο προκύπτει άμεσα χρησιμοποιώντας το προβολικό επίπεδο για τον πολλαπλασιασμό των στοιχείων της βάσης των οκτάδων. Η **νόρμα μιας οκτάδας** x είναι ο μη αρνητικός πραγματικός αριθμός:

$$\begin{aligned} ||x|| &= \sqrt{x\overline{x}} \\ &= \sqrt{a_1^2 + a_2^2 + a_3^2 + a_4^2 + a_5^2 + a_6^2 + a_7^2 + a_8^2}. \end{aligned}$$

Για $x, y \in \mathbb{O}$ ισχύει ότι:

$$||xy|| = ||x||\ ||y||. \tag{2.19}$$

Κάθε μη μηδενική οκτάδα x έχει την **αντίστροφή** της που ορίζεται ως εξής:

$$x^{-1} = \frac{1\overline{x}}{||x||^2}.$$

Το ότι οι οκτάδες είναι άλγεβρα διαίρεσης, αποδεικνύεται με τον ίδιο τρόπο που αποδείξαμε ότι η άλγεβρα των τετράδων είναι άλγεβρα διαίρεσης, λαμβάνοντας πάλι υπόψιν ότι δεν ισχύει η μεταθετικότητα του πολλαπλασιασμού. Έστω η τετραγωνική απεικόνιση:

$$n : \mathbb{O} \to \mathbb{R}, \;\; x \mapsto n(x) := ||x||^2 = x\overline{x}.$$

Για την n ισχύει ότι $n(xy) = n(x)n(y)$ (βλ. (2.19)), άρα η άλγεβρα $\mathbb{O}$ είναι μία composition $\mathbb{R}$-άλγεβρα.

Κεφάλαιο 3

Το θεώρημα Hurwitz-Ταξινόμηση Composition Αλγεβρών

3.1 Η μέθοδος Cayley-Dickson

Έστω A μία K-άλγεβρα με μοναδιαίο στοιχείο το 1 και με ενέλιξη $a \mapsto \overline{a}$, όπου $a + \overline{a} \in K \cdot 1, a\overline{a} \in K \cdot 1$, για κάθε $a \in A$.

Με τη **μέθοδο Cayley-Dickson** κατασκευάζουμε μία νέα άλγεβρα με ενέλιξη, η οποία περιέχει την A σαν υποάλγεβρα. Επιπλέον, αν η διάσταση της A είναι m, τότε η διάσταση της νέας άλγεβρας είναι $2m$.

Έστω $0 \neq \mu \in K$. Η νέα άλγεβρα συμβολίζεται με (A, μ) και αποτελείται από όλα τα διατεταγμένα ζεύγη $(a_1, a_2) \in A \times A$, με πράξεις την πρόσθεση και το βαθμωτό πολλαπλασιασμό, οι οποίες ορίζονται κατά τις συνιστώσες, και τον πολλαπλασιασμό:

$$(a_1, a_2)(a_3, a_4) = (a_1 a_3 + \mu a_4 \overline{a_2}, \overline{a_1} a_4 + a_3 a_2).$$

Ο πολλαπλασιασμός που ορίστηκε είναι διγραμμική πράξη και η (A, μ) είναι μία K-άλγεβρα με μοναδιαίο στοιχείο το 1=(1,0). Επίσης, το σύνολο $A' = \{(a, 0) | a \in A\}$ είναι υποάλγεβρα της άλγεβρας (A, μ):

$$(a_1, 0)(a_3, 0) = (a_1 a_3, 0),$$

η οποία είναι ισομορφική με την A.

Για το στοιχείο $u = (0, 1) \in (A, \mu)$ ισχύει ότι $u^2 = \mu(1, 0) = \mu 1$ και η (A, μ) είναι το ευθύ άθροισμα των m-διάστατων διανυσματικών χώρων A', uA'. Συμβολίζουμε:

$$(A, \mu) = A' \oplus uA'.$$

Αν ταυτίσουμε την A' με την A, τότε τα στοιχεία της άλγεβρας (A, μ) είναι της μορφής:

$$x = a_1 + ua_2,$$

όπου τα $a_1, a_2 \in A$ καθορίζονται με μοναδικό τρόπο από το x και ο πολλαπλασιασμός στοιχείων της (A, μ) δίνεται από:

$$(a_1 + ua_2)(a_3 + ua_4) = (a_1 a_3 + \mu a_4 \overline{a_2}) + u(\overline{a_1} a_4 + a_3 a_2),$$

για κάθε $a_i \in A$.

Για ένα τυχαίο στοιχείο $x = a_1 + ua_2 \in (A, \mu)$ ορίζουμε:

$$\overline{x} = \overline{a_1} - ua_2.$$

Λήμμα 3.1.1. *Η απεικόνιση $x \mapsto \overline{x}$, που ορίστηκε παραπάνω, ειναι μία ενέλιξη της άλγεβρας (A, μ). Επιπλέον,*

$$x + \overline{x} = t(x)1 \in K \cdot 1 \ \textit{ και } \ x\overline{x} (= \overline{x}x) = n(x)1 \in K \cdot 1,$$

για κάθε $x \in (A, \mu)$. Αν η τετραγωνική μορφή, για την οποία ισχύει $n(a)1 = a\overline{a}$, είναι μη *εκφυλισμένη στην A, τότε η τετραγωνική μορφή, για την οποία ισχύει $n(x)1 = x\overline{x}$, είναι μη εκφυλισμένη στην (A, μ).*

Απόδειξη. Η απεικόνιση $x \mapsto \overline{x}$ είναι γραμμική, επειδή η ενέλιξη στην A είναι γραμμική. Επίσης, ισχύει ότι $\overline{\overline{x}} = x$, για κάθε $x \in (A, \mu)$, λόγω του ότι $\overline{\overline{a_1}} = a_1$, για κάθε $a_1 \in A$. Έστω $x = a_1 + ua_2, \;\; y = a_3 + ua_4 \in (A, \mu)$. Τότε έχουμε:

$$\begin{aligned}\overline{y}\;\overline{x} &= (\overline{a_3} - ua_4)(\overline{a_1} - ua_2) \\ &= (\overline{a_3}\;\overline{a_1} + \mu a_2\overline{a_4}) - u(a_3a_2 + \overline{a_1}a_4) = \overline{xy}.\end{aligned}$$

Άρα, η απεικόνιση $x \mapsto \overline{x}$ ειναι μία ενέλιξη της άλγεβρας (A, μ). Επιπλέον,

$$t(x)1 = x + \overline{x} = a_1 + \overline{a_1} = t(a_1)1 \in K \cdot 1$$

και:

$$\begin{aligned}x\overline{x} &= (a_1\overline{a_1} - \mu a_2\overline{a_2}) + u(-\overline{a_1}a_2 + \overline{a_1}a_2) \\ &= n(a_1)1 - \mu n(a_2)1 = n(x)1 \in K \cdot 1,\end{aligned}$$

όπου:

$$n(x) = n(a_1) - \mu n(a_2). \tag{3.1}$$

Έστω η μη εκφυλισμένη τετραγωνική μορφή στην A για την οποία ισχύει $n(a)1 = a\overline{a}$, για κάθε $a \in A$. Θα δείξουμε ότι η τετραγωνική μορφή στην (A, μ) για τη οποία ισχύει $n(x)1 = x\overline{x}$, για κάθε $x \in (A, \mu)$, είναι μη εκφυλισμένη. Έστω η αντίστοιχη διγραμμική της μορφή f, για την οποία ισχύει:

$$\begin{aligned}f(x, y)1 &= n(x + y)1 - n(x)1 - n(y)1 \\ &= n(a_1 + a_3)1 - \mu n(a_2 + a_4)1 - n(a_1)1 + \mu n(a_2)1 - n(a_3)1 + \mu n(a_4)1 \\ &= (a_1 + a_3)(\overline{a_1 + a_3}) - \mu((a_2 + a_4)(\overline{a_2 + a_4})) - a_1\overline{a_1} + \mu a_2\overline{a_2} - a_3\overline{a_3} + \mu a_4\overline{a_4} \\ &= (a_1\overline{a_3} + a_3\overline{a_1}) - \mu(a_2\overline{a_4} + a_4\overline{a_2})\end{aligned}$$

και έστω $f(x, y) = 0$, για κάθε $y \in (A, \mu)$. Θέτουμε $y = a_3 \in A$, οπότε έχουμε:

$$\begin{aligned} f(x, y)1 &= a_1\overline{a_3} + a_3\overline{a_1} \\ &= f(a_1, a_3)1. \end{aligned}$$

Άρα, δεδομένου ότι η διγραμμική μορφή f είναι μη εκφυλισμένη στην A και $f(a_1, a_3) = 0$, για κάθε $a_3 \in A$, προκύπτει ότι $a_1 = 0$. Επίσης, με ανάλογο τρόπο προκύπτει ότι $a_2 = 0$, δεδομένου ότι $\mu \neq 0$. Άρα, $x = 0$. □

Παρακάτω ακολουθούν κάποιοι κανόνες, οι οποίοι ονομάζονται **κανόνες γινομένου Cayley-Dickson**, για τον πολλαπλασιασμό στοιχείων της άλγεβρας (A, μ), που βοηθούν στο να θυμόμαστε πώς γίνεται αυτός ο πολλαπλασιασμός. Έστω $a, b \in A$. Τότε:

$$\begin{aligned} au &= u\overline{a}, \\ a(ub) &= u(\overline{a}b), \\ (ub)a &= u(ab), \\ (ua)(ub) &= \mu b\overline{a}. \end{aligned}$$

3.2 Το θεώρημα Hurwitz

Έστω A μία composition άλγεβρα, πάνω στο σώμα K, με τετραγωνική μορφή n. Από την Πρόταση 2.2.1, υπάρχει μία ενέλιξη $a \mapsto \overline{a}$ στην A τέτοια ώστε $n(a)1 = a\overline{a} \in K \cdot 1$ και $t(a)1 = a + \overline{a} \in K \cdot 1$, για κάθε $a \in A$. Άρα, μπορούμε να εφαρμόσουμε στην A τη μέθοδο Cayley-Dickson.
Παρακάτω αποδεικνύεται τι πρέπει να ικανοποιείται ώστε η άλγεβρα (A, μ), που προκύπτει, να είναι μία composition άλγεβρα.

Λήμμα 3.2.1. *Έστω A μία composition άλγεβρα. Τότε η (A, μ) είναι composition άλγεβρα αν και μόνο αν η A είναι προσεταιριστική.*

Απόδειξη. Έχει δειχθεί παραπάνω ότι η άλγεβρα (A, μ) έχει μοναδιαίο στοιχείο. Επίσης, από το Λήμμα 3.1.1, η τετραγωνική μορφή n, για την οποία ισχύει $n(x)1 = x\overline{x}$, $x \in (A,\mu)$, είναι μη εκφυλισμένη στην (A,μ). Επομένως, η (A,μ) είναι composition άλγεβρα αν και μόνο αν για κάθε $x, y \in (A,\mu)$ ισχύει $n(xy) = n(x)n(y)$. Έστω $x = a_1 + ua_2 \in (A,\mu)$, τότε:

$$n(x) = n(a_1) - \mu n(a_2).$$

Έστω $y = a_3 + ua_4 \in (A,\mu)$. Τότε:

$$\begin{aligned} n(xy) - n(x)n(y) &= n(a_1a_3 + \mu a_4\overline{a_2}) - \mu n(\overline{a_1}a_4 + a_3a_2) - (n(a_1) - \mu n(a_2))(n(a_3) - \mu n(a_4)) \\ &= n(a_1a_3) + \mu^2 n(a_4\overline{a_2}) + \mu f(a_1a_3, a_4\overline{a_2}) \\ &- \mu n(\overline{a_1}a_4) - \mu n(a_3a_2) - \mu f(\overline{a_1}a_4, a_3a_2) \\ &- n(a_1)n(a_3) + \mu n(a_1)n(a_4) + \mu n(a_2)n(a_3) - \mu^2 n(a_2)n(a_4). \end{aligned}$$

Γνωρίζουμε ότι για κάθε $a, b \in A$ ισχύουν:

$$n(ab) = n(a)n(b) \text{ και } n(\overline{a}) = n(a),$$

οπότε:

$$n(xy) - n(x)n(y) = \mu f(a_1a_3, a_4\overline{a_2}) - \mu f(\overline{a_1}a_4, a_3a_2).$$

Χρησιμοποιώντας την εξίσωση (2.8), έχουμε:

$$\begin{aligned} f(a_1a_3, a_4\overline{a_2}) &= f((a_1a_3)1, a_4\overline{a_2}) \\ &= -f((a_1a_3)\overline{a_2}, a_4) + f(a_1a_3, a_4)f(1, \overline{a_2}) \\ &= f((a_1a_3)(f(1,\overline{a_2})1 - \overline{a_2}), a_4) \\ &= f((a_1a_3)a_2, a_4). \end{aligned}$$

Με ανάλογο τρόπο προκύπτει ότι:

$$f(\overline{a_1}a_4, a_3a_2) = f(a_4, a_1(a_3a_2)).$$

Επομένως, αφού $\mu \neq 0$ και η συμμετρική διγραμμική μορφή f είναι μη εκφυλισμένη, έπεται ότι για κάθε $x, y \in (A, \mu)$ ισχύει $n(xy) = n(x)n(y)$ αν και μόνο αν η A είναι προσεταιριστική. $\square$

Έχουμε δείξει ότι το $\mathbb{R}$ είναι μία composition $\mathbb{R}$-άλγεβρα. Εφαρμόζουμε διαδοχικά τη μέθοδο Cayley-Dickson και λαμβάνουμε τις εξής composition $\mathbb{R}$-άλγεβρες:

1. $\mathbb{C} = (\mathbb{R}, -1) = \mathbb{R} \oplus i\mathbb{R},\ \ i^2 = -1,$

2. $\mathbb{H} = (\mathbb{C}, -1) = \mathbb{C} \oplus j\mathbb{C},\ \ j^2 = -1,$

3. $\mathbb{O} = (\mathbb{H}, -1) = \mathbb{H} \oplus l\mathbb{H},\ \ l^2 = -1.$

Η κατασκευή αυτή σταματάει στις οκτάδες λόγω του Λήμματος 3.2.1 και του ότι οι οκτάδες είναι μία μη προσεταιριστική composition $\mathbb{R}$-άλγεβρα.

Πρόταση 3.2.1. *Έστω A μία K-άλγεβρα με μοναδιαίο στοιχείο το 1 και μία ενέλιξη $a \mapsto \overline{a}$, όπου $a + \overline{a},\ \ a\overline{a} \in K \cdot 1$, για κάθε $a \in A$. Έστω (A, μ) η άλγεβρα που προκύπτει όταν εφαρμόσουμε στην A τη μέθοδο Cayley-Dickson. Τότε ισχύουν τα παρακάτω:*

1. *Η άλγεβρα (A, μ) είναι μεταθετική αν και μόνο αν η A είναι μεταθετική με την τετριμμένη ενέλιξη (δηλαδή $\overline{a} = a$, για κάθε $a \in A$),*

2. *Η άλγεβρα (A, μ) είναι προσεταιριστική αν και μόνο αν η A είναι προσεταιριστική και μεταθετική,*

3. *Η άλγεβρα (A, μ) είναι εναλλάσσουσα αν και μόνο αν η A είναι προσεταιριστική.*

Απόδειξη. Έστω $x = a_1 + ua_2,\ \ , y = a_3 + ua_4,\ \ , z = a_5 + ua_6 \in (A, \mu)$.
Για το (1): Αν η (A, μ) είναι μεταθετική, τότε και η υποάλγεβρα A' είναι μεταθετική, άρα και η A, η οποία είναι ισομορφική με την A'. Επίσης,

$$xy = (a_1a_3 + \mu a_4\overline{a_2}) + u(\overline{a_1}a_4 + a_3a_2),$$

$$yx = (a_3a_1 + \mu a_2\overline{a_4}) + u(\overline{a_3}a_2 + a_1a_4).$$

Από τα παραπάνω, είναι σαφές ότι $xy = yx$ αν η A είναι μεταθετική.

Για το (2): Για να είναι η (A, μ) προσεταιριστική, είναι απαραίτητο η A να είναι προσεταιριστική (ως ισομορφική με την υποάλγεβρα A') και μεταθετική. Η μεταθετικότητα της A χρειάζεται για να μηδενίζεται ο προσεταιριστής στην (A, μ). Πράγματι, έστω $a, b \in A$:

$$[u, a, b] = (ua)b - u(ab) = u(ba - ab).$$

Βλέπουμε ότι για να ισχύει $[u, a, b] = 0$, πρέπει $ab = ba$, δηλαδή πρέπει η A να είναι μεταθετική. Αντίστροφα:

$$\begin{aligned}
(xy)z &= ((a_1a_3 + \mu a_4\overline{a_2}) + u(\overline{a_1}a_4 + a_3a_2))(a_5 + ua_6) \\
&= (a_1a_3)a_5 + \mu(a_4\overline{a_2})a_5 + \mu a_6(\overline{a_2}\ \ \overline{a_3}) + \mu a_6(\overline{a_4}a_1) \\
&+ u((\overline{a_3}\ \ \overline{a_1})a_6 + \mu(a_2\overline{a_4})a_6 + a_5(\overline{a_1}a_4) + a_5(a_3a_2)), \\
x(yz) &= (a_1 + ua_2)((a_3a_5 + \mu a_6\overline{a_4}) + u(\overline{a_3}a_6 + a_5a_4)) \\
&= a_1(a_3a_5) + \mu a_1(a_6\overline{a_4}) + \mu(\overline{a_3}a_6)\overline{a_2} + \mu(a_5a_4)\overline{a_2} \\
&+ u(\overline{a_1}(\overline{a_3}a_6) + \overline{a_1}(a_5a_4) + (a_3a_5)a_2 + \mu(a_6\overline{a_4})a_2),
\end{aligned}$$

και $(xy)z = x(yz)$ αν η A είναι προσεταιριστική και μεταθετική.

Για το (3): Γνωρίζουμε ότι ισχύει $\overline{y} = f(1, y)1 - y$, οπότε:

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

άρα οι συνθήκες $(xy)y = xy^2$ και $(xy)\overline{y} = x(y\overline{y})$ είναι ισοδύναμες.Έστω ότι η (A, μ)

είναι εναλλάσσουσα και έστω $a, b, c \in A$. Τότε:

$$\begin{aligned}
0 &= [ua+b, ua+b, c] \\
&= [ua, b, c] + [b, ua, c] \\
&= (u(ba))c - (ua)(bc) + (u(\bar{b}a))c - b(u(ca)) \\
&= u(c(ba)) - u((bc)a) + u(c(\bar{b}a)) - u(\bar{b}(ca)) \\
&= u[c(t(b)a) - [b, c, a] - t(b)(ca)] \\
&= -u[b, c, a],
\end{aligned}$$

άρα η A είναι προσεταιριστική. Αντίστροφα, έστω ότι η A είναι προσεταιριστική. Τότε έχουμε:

$$\begin{aligned}
(xy)\overline{y} &= ((a_1a_3 + \mu a_4\overline{a_2}) + u(\overline{a_1}a_4 + a_3a_2))(\overline{a_3} - ua_4) \\
&= (a_1a_3)\overline{a_3} + \mu(a_4\overline{a_2})\overline{a_3} - \mu a_4(\overline{a_2}\ \overline{a_3}) - \mu a_4(\overline{a_4}a_1) \\
&+ u[-(\overline{a_3}\ \overline{a_1})a_4 - \mu(a_2\overline{a_4})a_4 + \overline{a_3}(\overline{a_1}a_4) + \overline{a_3}(a_3a_2)] \\
&= a_1n(a_3) - \mu n(a_4)a_1 + u[-\mu a_2n(a_4) + n(a_3)a_2] \\
&= (a_1 + ua_2)(n(a_3) - \mu n(a_4)) \\
&= xn(y) = x(y\overline{y}).
\end{aligned}$$

Η συνθήκη $x^2y = x(xy)$ αποδεικνύεται με ανάλογο τρόπο. □

Λήμμα 3.2.2. *Έστω A μία composition K-άλγεβρα με τετραγωνική μορφή n και B μία υποάλγεβρα αυτής. Τότε $B^\perp B \subseteq B^\perp$ και $BB^\perp \subseteq B^\perp$. Επίσης, για κάθε $a, b \in B$ και $u \in B^\perp$ ισχύουν οι παρακάτω σχέσεις:*

$$\overline{u} = -u, \qquad au = u\overline{a}, \tag{3.2}$$

$$a(ub) = u(\overline{a}b), \qquad (ub)a = u(ab), \tag{3.3}$$

$$(ua)(ub) = -n(u)b\overline{a}. \tag{3.4}$$

Απόδειξη. Από τον ορισμό της υποάλγεβρας, έχουμε ότι $1 \in B$. Επίσης,

$$f(u,1) = 0, \;\; f(u,a) = f(u,b) = 0.$$

Χρησιμοποιώντας την εξίσωση (2.8), έχουμε:

$$f(a, ub) = f(a1, ub) = -f(ab, u) + f(a, u)f(1, b) = 0$$

και ανάλογα αποδεικνύεται ότι $f(a, bu) = 0$. Επομένως, αφού τα στοιχεία $a, b \in B$ και $u \in B^\perp$ είναι τυχαία, συμπεραίνουμε ότι $B^\perp B \subseteq B^\perp$ και $BB^\perp \subseteq B^\perp$. Επιπλέον,

$$u + \overline{u} = f(1, u)1 = 0$$

και χρησιμοποιώντας την (2.17), έχουμε:

$$\begin{aligned} u\overline{a} + a\overline{u} &= u(f(1,a)1 - a) + a(f(1,u)1 - u) \\ &= f(1,a)u - ua + f(1,u)a - au \\ &= f(1,a)f(1,u)1 - f(1,au)1 = 0 \\ &\Rightarrow u\overline{a} - au = 0, \end{aligned}$$

άρα αποδείξαμε τις εξισώσεις (3.2).

Έστω $x, y, z \in A$. Από το Λήμμα 2.1.2, έχουμε ότι η A είναι εναλλάσσουσα άλγεβρα, οπότε ισχύει η εξίσωση $x(xy) = x^2y$. Έχουμε:

$$\begin{aligned} x(\overline{x}y) - (x\overline{x})y &= x(f(1,x)y - xy) - (f(1,x)x - x^2)y \\ &= f(1,x)xy - x(xy) - f(1,x)xy + x^2y \\ &= x^2y - x(xy) = 0, \end{aligned} \tag{3.5}$$

άρα:

$$x(\overline{x}y) = (x\overline{x})y = n(x)y. \tag{3.6}$$

Θέτοντας $x = x + z$ στην (3.6) προκύπτει:

$$\begin{aligned} n(x+z)y &= (x+z)[(\overline{x+z})y] = (x+z)(\overline{x}y + \overline{z}y) \\ &= n(x)y + x(\overline{z}y) + z(\overline{x}y) + n(z)y \end{aligned} \tag{3.7}$$

και:

$$x(\overline{z}y) + z(\overline{x}y) = f(x,z)y. \tag{3.8}$$

Θέτουμε $x = a, y = b, z = u$ στην (3.8) και έχουμε:

$$a(\overline{u}b) + u(\overline{a}b) = 0 \Rightarrow -a(ub) + u(\overline{a}b) = 0. \tag{3.9}$$

Εφαρμόζοντας στην εξίσωση (3.9) την ενέλιξη και λαμβάνοντας υπόψιν τις εξισώσεις (3.2), λαμβάνουμε:

$$\begin{aligned} \overline{a(\overline{u}b) + u(\overline{a}b)} &= \overline{a(\overline{u}b)} + \overline{u(\overline{a}b)} \\ &= (\overline{b}u)\overline{a} + (\overline{b}a)\overline{u} = (ub)\overline{a} - u(\overline{a}b) = 0, \end{aligned} \tag{3.10}$$

άρα αποδείξαμε τις εξισώσεις (3.3).

Τέλος, από την εξίσωση (3.8), χρησιμοποιώντας τις εξισώσεις (2.5),(3.6), (3.3) προκύπτει:

$$\begin{aligned} (ua)(ub) &= -\overline{u}((\overline{ua})b) + f(ua, \overline{u})b = u((\overline{a}\ \ \overline{u})b) - f(ua, u)b \\ &= -u((\overline{a}u)b) - n(u)f(a,1)b = -u((ua)b) - n(u)f(a,1)b \\ &= u(\overline{u}(ba)) - n(u)f(a,1)b = n(u)[ba - f(a,1)b] = -n(u)b\overline{a}. \end{aligned}$$

$\square$

Πρόταση 3.2.2. *Έστω A μία composition άλγεβρα με τετραγωνική μορφή n και έστω $x \in A$. Αν το x έχει αντίστροφο το x^{-1}, τότε ισχύει:*

$$n(x^{-1}) = n(x)^{-1}.$$

Συγκεκριμένα, τα $n(x^{-1}), n(x)^{-1}$ είναι διάφορα του μηδενός.

Απόδειξη.
$$1 = n(1) = n(xx^{-1}) = n(x)n(x^{-1}),$$

άρα $n(x^{-1}) = n(x)^{-1}$. □

Πρόταση 3.2.3. *Έστω A μία composition άλγεβρα με τετραγωνική μορφή n. Για κάθε $x \in A$, τα επόμενα είναι ισοδύναμα:*

1. *Το x έχει αντίστροφο,*

2. *$n(x) \neq 0$.*

Σε αυτήν την περίπτωση, $x^{-1} = n(x)^{-1}\overline{x}$. Αν το x έχει αντίστροφο, τότε το αντίστροφο αυτό είναι μοναδικό.

Απόδειξη. (1) $\Rightarrow$ (2): Προκύπτει από την Πρόταση 3.2.2.
(2) $\Rightarrow$ (1): Έστω ότι $n(x) \neq 0$. Θέτουμε $y = n(x)^{-1}\overline{x}$. Έχουμε:

$$xy = x(n(x)^{-1}\overline{x}) = n(x)^{-1}(x\overline{x}) = n(x)^{-1}n(x)1 = 1.$$

Η ισότητα $yx = 1$ αποδεικνύεται με ανάλογο τρόπο. Άρα, $xy = yx = 1$. Έστω ότι to x έχει κι άλλο αντίστροφο, δηλαδή έστω ότι υπάρχει $z \in A$, τέτοιο ώστε $xz = zx = 1$. Τότε, χρησιμοποιώντας την εξίσωση (3.6), προκύπτει:

$$\begin{aligned} y = y(xz) &= n(x)^{-1}\overline{x}(xz) = n(x)^{-1}(\overline{x}x)z \\ &= n(x)^{-1}n(x)z = z. \end{aligned}$$

□

Λήμμα 3.2.3. *Έστω A μία composition άλγεβρα με τετραγωνική μορφή n. Αν D είναι ένας πεπερασμένης διάστασης γνήσιος και μη εκφυλισμένος υπόχωρος της A, τότε υπάρχει ένα στοιχείο $u \in D^{\perp}\backslash\{0\}$ τέτοιο ώστε $n(u) \neq 0$.*

Απόδειξη. Έστω ότι $n(x) = 0$, για κάθε $x \in D^{\perp}$. Από την Πρόταση 1.2.1 έχουμε ότι $A = D \oplus D^{\perp}$ και ο $D^{\perp}$ είναι μη εκφυλισμένος. Επίσης, γνωρίζουμε ότι $D \neq A$, άρα $D^{\perp} \neq \{0\}$. Έστω u ένα μη μηδενικό στοιχείο του $D^{\perp}$. Τότε:

$$f(u, x) = n(u + x) - n(u) - n(x) = 0, \;\; \forall x \in D^{\perp}$$

και αφού ο $D^{\perp}$ είναι μη εκφυλισμένος, $u = 0$ το οποίο είναι άτοπο. □

Θεώρημα 3.2.1 (Hurwitz). *Έστω A μία composition άλγεβρα πάνω σε ένα σώμα K χαρακτηριστικής $\neq 2$. Τότε ισχύει ακριβώς ένα από τα παρακάτω:*

1. *$A = K \cdot 1$, με τετραγωνική μορφή:*

$$n(x)1 = x^2,$$

2. *Η A είναι ισομορφική με την composition άλγεβρα $(K \cdot 1, \mu)$, όπου $\mu \neq 0$, με τετραγωνική μορφή:*

$$n(x)1 = x_1^2 - \mu x_2^2,$$

3. *Η A είναι ισομορφική με την composition άλγεβρα $\mathbb{H}(\mu, \beta) = ((K \cdot 1, \mu), \beta)$, όπου $\beta \neq 0$ **(γενικευμένη άλγεβρα των τετράδων)**, με τετραγωνική μορφή:*

$$n(x)1 = x_1^2 - \mu x_2^2 - \beta x_3^2 + \mu\beta x_4^2,$$

4. *Η A είναι ισομορφική με την composition άλγεβρα $\mathbb{O}(\mu, \beta, \gamma) = (\mathbb{H}(\mu, \beta), \gamma)$, όπου $\gamma \neq 0$ **(Cayley άλγεβρα)**, με τετραγωνική μορφή:*

$$n(x)1 = x_1^2 - \mu x_2^2 - \beta x_3^2 + \mu\beta x_4^2 - \gamma x_5^2 + \mu\gamma x_6^2 + \beta\gamma x_7^2 - \mu\beta\gamma x_8^2.$$

Άρα η διάσταση της A είναι 1 ή 2 ή 4 ή 8.

Απόδειξη. Έστω A μία composition άλγεβρα πάνω σε ένα σώμα K χαρακτηριστικής $\neq 2$, με τετραγωνική μορφή n και με την αντίστοιχη διγραμμική μορφή f. Έστω B μία πεπερασμένης διάστασης composition υποάλγεβρα της άλγεβρας A με $B \neq A$ (δηλαδή γνήσια υποάλγεβρα της A). Από τον ορισμό της υποάλγεβρας, το B είναι ένας μη εκφυλισμένος υπόχωρος της άλγεβρας A, που περιέχει το μοναδιαίο στοιχείο της A και είναι κλειστός ως προς τον πολλαπλασιασμό. Όπως είναι γνωστό, μπορούμε να γράψουμε την A ως το ευθύ άθροισμα των υποχώρων:

$$A = B \oplus B^{\perp}.$$

Έστω $\{b_1, ..., b_n\}$ μία βάση του B. Τότε για κάθε $a \in A$, έχουμε ότι:

$$a = x_1 b_1 + ... + x_n b_n + a^{\perp}, \text{ όπου } x_1, ..., x_n \in K, \ a^{\perp} \in B^{\perp}$$

και τα $x_1, ..., x_n$ μπορούν να βρεθούν λύνοντας το παρακάτω σύστημα:

$$f(a^{\perp}, b_i) = f(a - x_1 b_1 - ... - x_n b_n, b_i) = 0, \ i = 1, ..., n.$$

Επιπλέον, ο περιορισμός της f στο $B^{\perp}$ είναι επίσης μη εκφυλισμένος (βλ. Πρόταση 1.2.1). Αφού υποθέσαμε ότι $B \neq A$ (άρα $B^{\perp} \neq \{0\}$) και αφού ο $B^{\perp}$ είναι μη εκφυλισμένος υπόχωρος, μπορούμε να βρούμε ένα στοιχείο $u \in B^{\perp} \backslash \{0\}$ (βλ. Λήμμα 3.2.3), τέτοιο ώστε:

$$n(u) = -\mu \neq 0.$$

Από την (2.5), έχουμε:

$$f(ua, ub) = n(u) f(a, b) = -\mu f(a, b). \tag{3.11}$$

Από την εξίσωση (3.11) προκύπτει ότι ο υπόχωρος uB είναι μη εκφυλισμένος ως προς την f.Από το Λήμμα 3.2.2, ισχύει ότι $uB \subseteq B^{\perp}$, άρα $B \cap uB = \{0\}$, αφού ο B είναι μη εκφυλισμένος. Αυτό σημαίνει ότι ο υπόχωρος:

$$B_1 = B \oplus uB,$$

είναι το ευθύ άθροισμα δύο μη εκφυλισμένων υπόχωρων. Επίσης, $dimB_1 = 2dimB$. Πράγματι, ας θεωρήσουμε την απεικόνιση

$$L : B \to uB, \ \ x \mapsto ux.$$

Αφού $n(u) \neq 0$, έχουμε ότι το u έχει αντίστροφο (βλ. Πρόταση 3.2.3). Άρα η απεικόνιση L είναι 1-1 και επί. Επίσης, από το ευθύ άθροισμα έχουμε ότι $dimB_1 = dimB + dim(uB) = 2dimB$.

Ο υπόχωρος B_1 προέκυψε από την B με την εφαρμογή της μεθόδου Cayley-Dickson. Συμβολίζουμε $B_1 = (B, \mu)$. Από το Λήμμα 3.1.1 προκύπτει ότι ο B_1 είναι μη εκφυλισμένος υπόχωρος. Οι σχέσεις (3.3),(3.4) δείχνουν ότι ο υπόχωρος $B_1 = B \oplus uB$ είναι composition υποάλγεβρα της άλγεβρας A. Από το Λήμμα 3.2.2, ισχύει ότι $\overline{u} = -u$, άρα

$$\overline{a + ub} = \overline{a} - \overline{b}u = \overline{a} - ub, \ \ \text{όπου} \ \ a, b \in B.$$

Από το παραπάνω, προκύπτει ότι η ενέλιξη που ορίστηκε στην B_1, μέσω της ενέλιξης της A, συμπίπτει με την ενέλιξη που ορίζεται από τη μέθοδο Cayley-Dickson. Τέλος, η υποάλγεβρα B_1 ικανοποιεί τις ίδιες συνθήκες με την B και αν $B_1 \neq A$, τότε μπορούμε να επαναλάβουμε την ίδια μέθοδο με την B_1.

Έχουμε πει ότι το σώμα K είναι χαρακτηριστικής $\neq 2$, άρα ο υπόχωρος $K \cdot 1$ της composition άλγεβρας A είναι μη εκφυλισμένος ως προς την f, οπότε είναι composition υποάλγεβρα της A . Αν το σώμα K ήταν χαρακτηριστικής 2, τότε για κάθε $x, y \in K \cdot 1$ θα ίσχυε $f(x, y) = (x + y)^2 - x^2 - y^2 = 0$ και άρα η διγραμμική μορφή f θα ήταν εκφυλισμένη. Με βάση τα παραπάνω, μπορούμε να θέσουμε $B = K \cdot 1$.

Αν $B \neq A$, τότε υπάρχει $u_1 \in B^{\perp} \backslash \{0\}$, ώστε $n(u_1) = -a_1 \neq 0$. Τότε η άλγεβρα:

$$B_1 = (B, a_1) = B \oplus u_1 B$$

είναι μία composition υποάλγεβρα της A. Η B_1 είναι διάστασης 2 και είναι ισομορφική με την άλγεβρα (2) που δίνεται στη διατύπωση του Θεωρήματος. Αν $B_1 \neq A$, τότε υπάρχει $u_2 \in B_1^{\perp} \backslash \{0\}$, ώστε $n(u_2) = -a_2 \neq 0$. Τότε η άλγεβρα:

$$B_2 = ((B, a_1), a_2) = B_1 \oplus u_2 B_1$$

είναι μία composition υποάλγεβρα της A. Η B_2 είναι προσεταιριστική, αλλά όχι μεταθετική. Επίσης, είναι διάστασης 4 και είναι ισομορφική με την άλγεβρα (3) που δίνεται στη διατύπωση του Θεωρήματος. Αν $B_2 \neq A$, τότε υπάρχει $u_3 \in B_2^{\perp} \backslash \{0\}$, ώστε $n(u_3) = -a_3 \neq 0$. Τότε η άλγεβρα:

$$B_3 = (((B, a_1), a_2), a_3) = B_2 \oplus u_3 B_2$$

είναι μία composition υποάλγεβρα της A. Η B_3 είναι διάστασης 8, είναι ισομορφική με την άλγεβρα (4) που δίνεται στη διατύπωση του Θεωρήματος και δεν είναι μεταθετική. Επίσης, δεν είναι προσεταιριστική. Πράγματι, αφού η B_2 δεν είναι μεταθετική, υπάρχουν $q_1, q_2 \in B_2$, τέτοια ώστε $[q_1, q_2] \neq 0$. Οπότε,με τη βοήθεια του Λήμματος 3.2.2, έχουμε:

$$[u_3, q_1, q_2] = (u_3 q_1) q_2 - u_3 (q_1 q_2) = -u_3 [q_1, q_2] \neq 0.$$

Η διαδικασία αυτή δε μπορεί να συνεχιστεί. Αν συνεχιζόταν, θα υπήρχε μέσα στην A μία υποάλγεβρα B_4 η οποία δε θα ήταν composition άλγεβρα (σύμφωνα με το Λήμμα 3.2.1), το οποίο είναι άτοπο. Άρα, $A = B_3$.

Έστω τώρα ότι $A = K \cdot 1$ και $x = \lambda 1 \in K \cdot 1, \ \lambda \in K$.Τότε, γνωρίζουμε ότι $n(x)1 = x\overline{x}$.

Θα δείξουμε ότι $\overline{x} = x$, οπότε $n(x)1 = x^2$. Πράγματι,

$$\begin{aligned}\overline{x} = \overline{\lambda 1} &= f(1, \lambda 1)1 - \lambda 1 \\ &= \lambda f(1, 1)1 - \lambda 1 = 2(\lambda 1) - \lambda 1 = \lambda 1 = x.\end{aligned}$$

Οι υπόλοιπες τετραγωνικές μορφές που δίνονται στη διατύπωση του Θεωρήματος, βγαίνουν από την εξίσωση (3.1) και ικανοποιούν την εξίσωση (2.13). $\square$

Για την άλγεβρα $(K \cdot 1, \mu)$, όπου $\mu \neq 0$ και η χαρακτηριστική του K δεν είναι 2 (βλ. διατύπωση Θεωρήματος 3.2.1) ισχύει:
Αν το πολυώνυμο $x^2 - \mu$ είναι ανάγωγο στον $K[x]$, τότε η $(K \cdot 1, \mu)$ είναι ένα σώμα (μία διαχωρίσιμη, τετραγωνική επέκταση του σώματος K), αλλιώς ειναι το ευθύ άθροισμα $K \oplus K$ (βλ. [16]). Θα δώσουμε ένα παράδειγμα για την πρώτη περίπτωση.
Έστω ότι $K = \mathbb{R}$ και $\mu = -1$. Τότε, το πολυώνυμο $x^2 - \mu$ είναι ανάγωγο στον $\mathbb{R}[x]$ (επειδή $\sqrt{-1} \notin \mathbb{R}$) και η άλγεβρα $(\mathbb{R} \cdot 1, -1)$ είναι το σώμα των μιγαδικών αριθμών,

$$\mathbb{C} = \{a + \sqrt{\mu} b | a, b \in \mathbb{R}\} = \{a + \sqrt{-1} b = a + ib | a, b \in \mathbb{R}\}.$$

Το παραπάνω Θεώρημα αποδείχτηκε για σώματα χαρακτηριστικής $\neq 2$. Δείξαμε ότι αν η A είναι composition K-άλγεβρα διάστασης 1, τότε το σώμα K δε μπορεί να έχει χαρακτηριστική 2. Αποδεικνύεται ότι αν η A είναι composition K-άλγεβρα, όπου K είναι σώμα χαρακτηριστικής 2, τότε η διάσταση της A είναι 2 ή 4 ή 8 ([13],[10],[15]). Στην απόδειξη αυτή γίνεται χρήση της μεθόδου Cayley-Dickson.
Έχουμε δείξει ότι οι άλγεβρες $\mathbb{R}, \mathbb{C}, \mathbb{H}, \mathbb{O}$ είναι composition άλγεβρες διαίρεσης πάνω στο σώμα των πραγματικών αριθμών. Επομένως, υπάρχουν εναλλάσσουσες άλγεβρες διαίρεσης πάνω στο $\mathbb{R}$ διαστάσεων 1,2,4,8, αφού κάθε composition άλγεβρα είναι εναλλάσσουσα. Το 1958 αποδείχτηκε ότι οι πεπερασμένης διάστασης άλγεβρες διαίρεσης πάνω στο $\mathbb{R}$ μπορούν να έχουν αυτές μόνο τις διαστάσεις. Όμως, δεν αληθεύει το ότι οι πεπερασμένης διάστασης άλγεβρες διαίρεσης πάνω στο $\mathbb{R}$ είναι μόνο οι τέσσερις που δόθηκαν

παραπάνω. Αυτές οι τέσσερις είναι οι μόνες εναλλάσσουσες (βλ. [13]).

3.3 Ιδιότητες των Composition Αλγεβρών

Πρόταση 3.3.1. *Σε κάθε εναλλάσσουσα K-άλγεβρα A ισχύουν οι παρακάτω σχέσεις, για κάθε $x, y, z \in A$. Οι σχέσεις αυτές ονομάζονται **ταυτότητες Moufang**.*

$$x(yzy) = ((xy)z)y,$$
$$(yzy)x = y(z(yx)),$$
$$(xy)(zx) = x(yz)x.$$

Πρόταση 3.3.2. *Σε κάθε εναλλάσσουσα άλγεβρα A ικανοποιούνται οι παρακάτω ταυτότητες:*

$$[x, xy, z] = [x, y, z]x,$$
$$[x, yx, z] = x[x, y, z],$$
$$[x^2, y, z] = [x, xy + yx, z],$$
$$[x^2, y, z] = x[x, y, z] + [x, y, z]x,$$

όπου $x, y, z \in A$.

Ορισμός 3.3.1. *Μία K-άλγεβρα A ονομάζεται **απλή (simple)** αν ισχύουν τα παρακάτω:*

- *Τα μόνα ιδεώδη της A είναι το $\{0\}$ και η A, δηλαδή δεν έχει γνήσια ιδεώδη,*
- $AA \neq \{0\}$.

Θεώρημα 3.3.1. *Έστω A μία τετραγωνική K-άλγεβρα, η οποία περιέχει τουλάχιστον τρία στοιχεία. Τότε το ίχνος $t(x) : A \to K$ είναι μία γραμμική απεικόνιση και η νόρμα $n(x) : A \to K$ είναι τετραγωνική μορφή. Επιπλέον, αν η άλγεβρα A είναι εναλλάσσουσα, τότε η τετραγωνική μορφή n ικανοποιεί τη σχέση $n(xy) = n(x)n(y)$,για κάθε $x, y \in A$.*

Θεώρημα 3.3.2. *Έστω A μία απλή, τετραγωνική, εναλλάσσουσα K-άλγεβρα που περιέχει τουλάχιστον τρία στοιχεία. Τότε είτε η A είναι composition άλγεβρα, είτε είναι κάποιο σώμα χαρακτηριστικής 2.*

Απόδειξη. Από το Θεώρημα 3.3.1, πάνω στην άλγεβρα A είναι ορισμένη μία τετραγωνική μορφή n για την οποία ισχύει $n(xy) = n(x)n(y), \ \ x, y \in A$. Έστω f η αντίστοιχη διγραμμική μορφή της n. Έστω το σύνολο $radf = \{a \in A | f(a, y) = 0, \ \ \forall y \in A\}$, που είναι το ριζικό της f. Θα δείξουμε ότι το $radf$ είναι ιδεώδες της A. Ισχύει ότι $0 \in radf$, το οποίο συνεπάγεται ότι $radf \neq \emptyset$. Το ριζικό της f είναι υπόχωρος του διανυσματικού χώρου A. Έστω $a \in radf$, $x, y \in A$. Χρησιμοποιώντας την εξίσωση (2.8), έχουμε:

$$f(ax, y) = f(ax, y1) = -f(a, yx) + f(a, y)f(x, 1) = 0,$$

άρα το $radf$ είναι δεξιό ιδεώδες της άλγεβρας A. Με ανάλογο τρόπο αποδεικνύεται ότι το $radf$ είναι αριστερό ιδεώδες της άλγεβρας A. Αφού η A είναι απλή άλγεβρα, είτε $radf = \{0\}$, είτε $radf = A$. Στην πρώτη περίπτωση η τετραγωνική μορφή n είναι μη εκφυλισμένη και η άλγεβρα A είναι μία composition άλγεβρα. Έστω ότι $radf = A$. Σε αυτήν την περίπτωση η συνάρτηση f είναι παντού μηδέν στην άλγεβρα A, οπότε ισχύει:

$$n(x + y) = n(x) + n(y), \forall x, y \in A.$$

Επομένως, η απεικόνιση:

$$\phi : A \to K, \ \ x \mapsto \phi(x) := n(x)$$

είναι ομομορφισμός των δακτυλίων A και K. Είναι εύκολο να δούμε ότι ο πυρήνας αυτού του ομομορφισμού είναι ιδεώδες της A. Αφού η A είναι απλή και $n(1) = 1 \neq 0$, ο πυρήνας αυτός είναι το σύνολο $\{0\}$, άρα η απεικόνιση ϕ είναι 1-1. Επομένως, ο δακτύλιος A είναι ισομορφικός με κάποιον υποδακτύλιο του δακτυλίου K. Επιπλέον, από την ισότητα $0 = f(1, 1) = 2$ προκύπτει ότι το σώμα K είναι χαρακτηριστικής 2. Τέλος, είναι σαφές ότι ο δακτύλιος A είναι υποσώμα του σώματος K. $\square$

Λήμμα 3.3.1. *Έστω A μία composition άλγεβρα με τετραγωνική μορφή n. Τα επόμενα είναι ισοδύναμα:*

1. *$n(x) = 0$ για κάποιο $0 \neq x \in A$,*

2. *Υπάρχουν διαιρέτες του μηδενός στην A.*

Απόδειξη. $(1) \Rightarrow (2)$: Αν $0 \neq x \in A$ και $n(x)1 = x\overline{x} = 0$, τότε το x είναι διαιρέτης του μηδενός.
$(2) \Rightarrow (1)$: Έστω $xy = 0$, όπου $x, y \in A$ και $x \neq 0, y \neq 0$. Τότε έχουμε $0 = n(xy) = n(x)n(y)$, οπότε είτε $n(x) = 0$ είτε $n(y) = 0$. $\square$

Ορισμός 3.3.2. *Αν σε μία composition άλγεβρα A ικανοποιείται μία από τις δύο συνθήκες του Λήμματος 3.3.1, τότε η A καλείται **διαχωρίσιμη (split)**. Δηλαδή, η A είναι διαχωρίσιμη αν δεν είναι άλγεβρα διαίρεσης.*

Λήμμα 3.3.2. *Μία composition άλγεβρα A είναι διαχωρίσιμη αν και μόνο αν περιέχει ένα στοιχείο $e \neq 0, 1$, για το οποίο ισχύει $e^2 = e$. Το στοιχείο αυτό ονομάζεται **ταυτοδύναμο (idempotent)**.*

Απόδειξη. Αν υπάρχει στην A ένα στοιχείο $e \neq 0, 1$, για το οποίο ισχύει $e^2 = e$, τότε $n(e) = 0$ και η A είναι διαχωρίσιμη. Αντίστροφα, έστω ότι η A είναι διαχωρίσιμη. Τότε μπορούμε να βρούμε ένα στοιχείο $x \in A$, τέτοιο ώστε $n(x) = 0$ και $t(x) = a \neq 0$, οπότε το στοιχείο $a^{-1}x$ είναι το ζητούμενο ταυτοδύναμο. Έστω ότι δε μπορεί να βρεθεί ένα τέτοιο στοιχείο. Δηλαδή, έστω ότι για κάθε $x \in A$ η ισότητα $n(x) = 0$ συνεπάγεται ότι $t(x) = 0$. Τότε αφού η A είναι διαχωρίσιμη έπεται ότι υπάρχει $0 \neq a \in A$ τέτοιο ώστε $n(a) = 0$. Για κάθε $x \in A$ έχουμε:

$$n(ax) = n(a)n(x) = 0 \Rightarrow t(ax) = 0.$$

Θέτουμε στην εξίσωση (2.8) $x = y = 1, z = a, w = x$ και προκύπτει:

$$f(1,a)f(1,x) = f(1,ax) + f(x,a) \Rightarrow f(a,x) = t(a)t(x) - t(ax) = 0.$$

Αφού η f είναι μη εκφυλισμένη, έπεται ότι $a = 0$, το οποίο είναι άτοπο. $\square$

Λήμμα 3.3.3. *Οποιεσδήποτε δύο διαχωρίσιμες composition K-άλγεβρες ίδιας διάστασης είναι ισομορφικές.*

Κεφάλαιο 4

Εφαρμογές

4.1 Εφαρμογές των τετράδων (Quaternions)

Η θεωρία των τετράδων (quaternions), που εισήχθη στα μέσα του 19ου αιώνα, είχε πολλές εφαρμογές στην κλασσική μηχανική, στην κβαντομηχανική και στη θεωρία της σχετικότητας. Οι τετράδες αργότερα χρησιμοποιήθηκαν σε αεροδιαστημικές εφαρμογές και σε προσομοιώσεις πτήσεων. Πιο μετά, οι προγραμματιστές γραφικών και παιχνιδιών ανακάλυψαν τις δυνατότητες που τους παρείχαν οι τετράδες και ξεκίνησαν να τις χρησιμοποιούν ως ισχυρά εργαλεία για την περιγραφή περιστροφών γύρω από έναν τυχαίο άξονα. Το πεδίο των εφαρμογών αυτών επεκτάθηκε με τον καιρό σε πεδία όπως αυτά των fractals και της εικονικής πραγματικότητας [9].

4.1.1 Περιστροφή γύρω από έναν τυχαίο άξονα

Ορισμός 4.1.1. *Έστω τα διανύσματα* $x = (x_1, x_2, x_3), \;\; y = (y_1, y_2, y_3) \in \mathbb{R}^3$ *και έστω* θ *η επίπεδη, κυρτή γωνία μεταξύ των ευθειών που ενώνουν ένα τυχόν σημείο O του* $\mathbb{R}^3$ *με τα σημεία* (x_1, x_2, x_3) *και* (y_1, y_2, y_3)*. Ορίζουμε τα παρακάτω:*

- *Το **μέτρο** του διανύσματος x είναι ο μη αρνητικός πραγματικός αριθμός:*

$$||x|| = \sqrt{x_1^2 + x_2^2 + x_3^2}.$$

- *Το **εσωτερικό γινόμενο** των διανυσμάτων x, y είναι ο πραγματικός αριθμός:*

$$\begin{aligned} x \cdot y &= ||x|| \ \ ||y|| cos\theta \\ &= x_1 y_1 + x_2 y_2 + x_3 y_3. \end{aligned}$$

- *Το **εξωτερικό γινόμενο** των διανυσμάτων x, y είναι το διάνυσμα $x \times y$, το οποίο έχει μέτρο:*

$$||x \times y|| = ||x|| \ \ ||y|| sin\theta.$$

*Το διάνυσμα αυτό είναι κάθετο στα x, y. Έστω ένα σύστημα συντεταγμένων στον $\mathbb{R}^3$ που αποτελείται από τα στοιχεία $V_1, V_2, V_3 \in \mathbb{R}^3$. Το σύστημα συντεταγμένων ονομάζεται **δεξιόστροφο** αν $(V_1 \times V_2) \cdot V_3 > 0$ και **αριστερόστροφο** αν $(V_1 \times V_2) \cdot V_3 < 0$. Το διάνυσμα $x \times y$ έχει τέτοια φορά, ώστε το σύστημα των διανυσμάτων $\{x, y, x \times y\}$ να είναι δεξιόστροφο. Το εξωτερικό γινόμενο $x \times y$ μπορεί να γραφτεί και με τον παρακάτω τρόπο:*

$$x \times y = \begin{bmatrix} 0 & -x_3 & x_2 \\ x_3 & 0 & -x_1 \\ -x_2 & x_1 & 0 \end{bmatrix} \begin{bmatrix} y_1 \\ y_2 \\ y_3 \end{bmatrix}. \tag{4.1}$$

Έστω τα διανύσματα $x, y \in \mathbb{R}^3$. Ισχύει το παρακάτω:

$$x \times (y \times x) = (x \cdot x)y - (x \cdot y)x. \tag{4.2}$$

Πολλές φορές χρειάζεται να ανάλυσουμε ένα διάνυσμα x σε μία κάθετη και μία παράλληλη συνιστώσα ως προς ένα άλλο διάνυσμα y. Η παράλληλη συνιστώσα ονομάζεται **προβολή** του διανύσματος x στο y και είναι το παρακάτω διάνυσμα:

$$proj_y x = \frac{x \cdot y}{||y||^2} y. \tag{4.3}$$

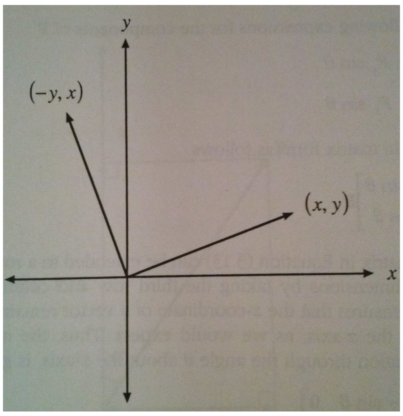
Σε μορφή πινάκων μπορεί να γραφτεί ως εξής:

$$proj_y x = \frac{1}{||y||^2} \begin{bmatrix} y_1^2 & y_1 y_2 & y_1 y_3 \\ y_1 y_2 & y_2^2 & y_2 y_3 \\ y_1 y_3 & y_2 y_3 & y_3^2 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix}. \tag{4.4}$$

Η κάθετη συνιστώσα του x ως προς το διάνυσμα y είναι το εξής διάνυσμα :

$$perp_y x = x - \frac{x \cdot y}{||y||^2} y. \tag{4.5}$$

Θεωρούμε το επίπεδο του $\mathbb{R}^2$. Επίσης, θεωρούμε ως περιστροφή ενός διανύσματος, κατά θετική γωνία θ, ως προς έναν άξονα A να είναι αυτή η οποία πραγματοποιεί μία περιστροφή με φορά αντίθετη των δεικτών του ρολογιού, όταν ο άξονας A έχει φορά προς τα εμάς. Όπως φαίνεται στο σχήμα 4.1, μπορούμε να πραγματοποιήσουμε μία περιστροφή 90



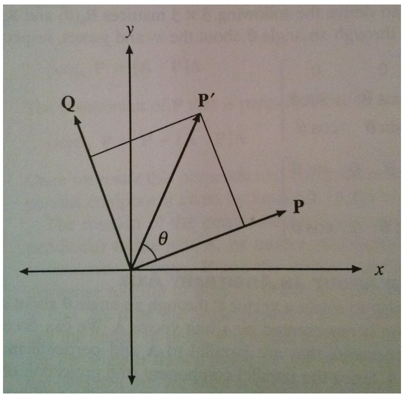
Σχήμα 4.1: Περιστροφή κατά 90 μοίρες στο επίπεδο $x - y$.

μοιρών, με φορά αντίθετη των δεικτών του ρολογιού, ενός διανύσματος $P \in \mathbb{R}^2$, ανταλλάσοντας τις x, y συντεταγμένες και προσθέτοντας έναν μείον στην καινούρια x συντεταγμένη. Δηλαδή, αν $P = (x, y)$, τότε το διάνυσμα που προκύπτει από την περιστροφή είναι το $Q = (-y, x)$. Ισχύει ότι:

$$P \cdot Q = x(-y) + yx = 0,$$

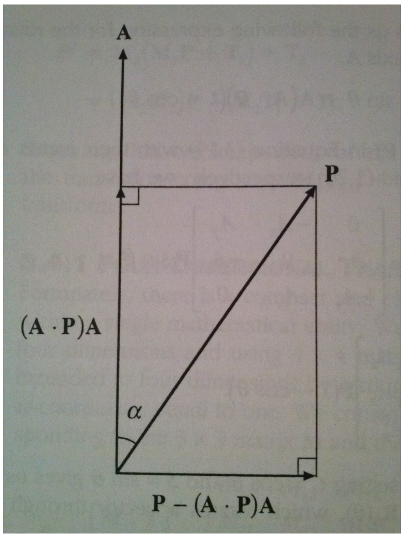
άρα τα P, Q σχηματίζουν μία ορθογώνια βάση στο επίπεδο $x - y$. Επομένως, κάθε διάνυσμα στο επίπεδο αυτό μπορεί να γραφτεί σα γραμμικός συνδυασμός των P, Q. Συγκεκριμένα, όπως φαίνεται στο σχήμα 4.2, οποιοδήποτε διάνυσμα P' που προκύπτει από περιστροφή του P κατά γωνία θ μπορεί να εκφραστεί με τον παρακάτω τρόπο:

$$P' = Pcos\theta + Qsin\theta. \tag{4.6}$$



Σχήμα 4.2:

Έστω ότι θέλουμε να περιστρέψουμε ένα διάνυσμα P του $\mathbb{R}^3$ κατά μία γωνία θ, γύρω από έναν τυχαίο άξονα του οποίου η κατεύθυνση δηλώνεται από το διάνυσμα A, το οποίο έχει μέτρο 1. Έστω ότι το διάνυσμα που προκύπτει από την περιστροφή ονομάζεται P'. Μπορούμε να χωρίσουμε το διάνυσμα P σε δύο συνιστώσες: μία παράλληλη με το A (η προβολή του P στο A) και μία κάθετη στο A, όπως φαίνεται στο σχήμα 4.3. Λαμβάνοντας



Σχήμα 4.3: Περιστροφή γύρω από τυχαίο άξονα.

υπόψιν ότι το διάνυσμα A έχει μέτρο 1, προκύπτει ότι:

$$prop_A P = (A \cdot P)A \text{ και } perp_A P = P - (A \cdot P)A.$$

Κατά την περιστροφή η παράλληλη συνιστώσα δε μεταβάλλεται. Η περιστροφή της κάθετης συνιστώσας γίνεται στο επίπεδο που είναι κάθετο στον άξονα A. Όπως πριν, θα γράψουμε το περιστρεφόμενο διάνυσμα σα γραμμικό συνδυασμό του $perp_A P$ και ενός διανύσματος, το οποίο προκύπτει από περιστροφή 90 μοιρών, με φορά αντίθετη από αυτή του ρολογιού, του $perp_A P$ γύρω από το A.Το μήκος του διανύσματος $perp_A P$ ισούται με $||P||sin\alpha$.Ένα διάνυσμα ίδιου μήκους, το οποίο έχει την κατεύθυνση που επιθυμούμε είναι το $A \times P$. Επομένως, μπορούμε να περιγράψουμε την περιστροφή του $perp_A P$, κατά γωνία θ ως εξής:

$$[P - (A \cdot P)A]cos\theta + (A \times P)sin\theta. \tag{4.7}$$

Προσθέτοντας στο παραπάνω αποτέλεσμα το $prop_A P$ έχουμε:

$$P' = Pcos\theta + (A \times P)sin\theta + A(A \cdot P)(1 - cos\theta). \tag{4.8}$$

4.1.2 Περιστροφή με τις τετράδες

Έχουμε αναφέρει ότι αν $q \in \mathbb{H}$, τότε το q είναι της μορφής $q = a+bi+cj+dk,\ \ a, b, c, d \in \mathbb{R}$. Συχνά, χρησιμοποιείται η γραφή $q = s+v$, όπου $s = a$ (**βαθμωτό μέρος του** q) και $v = bi + cj + dk$ (**διανυσματικό μέρος του** q). Σε αυτήν την περίπτωση ο πολλαπλασιασμός μεταξύ δύο τετράδων q_1, q_2 γράφεται ως:

$$q_1 q_2 = s_1 s_2 - v_1 \cdot v_2 + s_1 v_2 + s_2 v_1 + v_1 \times v_2.$$

Ορισμός 4.1.2. *Μία **περιστροφή** στις τρεις διαστάσεις μπορεί να θεωρηθεί ότι είναι μία συνάρτηση $f : \mathbb{R}^3 \to \mathbb{R}^3$, η οποία διατηρεί τα μήκη, τις γωνίες και την ιδιότητα "αριστερόστροφο ή δεξιόστροφο" του συστήματος συντεταγμένων.*

Έστω $P, P_1, P_2 \in \mathbb{R}^3$. Η f διατηρεί τα μήκη αν ικανοποιεί τη σχέση:

$$||f(P)|| = ||P||. \tag{4.9}$$

Η f διατηρεί τη γωνία μεταξύ των P_1, P_2 αν ικανοποιεί τη σχέση:

$$f(P_1) \cdot f(P_2) = P_1 \cdot P_2. \tag{4.10}$$

Τέλος, η f διατηρεί την ιδιότητα "αριστερόστροφο ή δεξιόστροφο" του συστήματος συντεταγμένων αν ικανοποιεί τη σχέση:

$$f(P_1) \times f(P_2) = f(P_1 \times P_2). \tag{4.11}$$

Επεκτείνουμε τη συνάρτηση f σε μία συνάρτηση που απεικονίζει το $\mathbb{H}$ στο $\mathbb{H}$, ζητώντας να ισχύει:

$$f(s + v) = s + f(v),\ \ q = s + v \in \mathbb{H}.$$

Με βάση τα προηγούμενα μπορούμε να ξαναγράψουμε την εξίσωση 4.10 ως εξής:

$$f(P_1) \cdot f(P_2) = f(P_1 \cdot P_2). \tag{4.12}$$

Αν θεωρήσουμε ότι τα P_1, P_2 είναι τετράδες με μηδενικά βαθμωτά μέλη, τότε μπορούμε να συνδυάσουμε τις εξισώσεις 4.11,4.12, αφού ισχύει ότι $P_1 P_2 = -P_1 \cdot P_2 + P_1 \times P_2$. Επομένως, η γωνία μεταξύ των P_1, P_2 και η ιδιότητα "αριστερόστροφο ή δεξιόστροφο" του συστήματος συντεταγμένων διατηρούνται αν ισχύει η σχέση:

$$f(P_1)f(P_2) = f(P_1 P_2). \tag{4.13}$$

Μία συνάρτηση που ικανοποιεί την ιδιότητα αυτή ονομάζεται, όπως έχουμε ήδη αναφέρει, ομομορφισμός. Το σύνολο των συναρτήσεων που δίνονται από τον τύπο:

$$f_q(P) = qPq^{-1}, \tag{4.14}$$

όπου q είναι μία μη μηδενική τετράδα, ικανοποιεί τις εξισώσεις (4.9),(4.13) και άρα αποτελεί ένα σύνολο περιστροφών. Πράγματι, η f_q διατηρεί τα μήκη, επειδή ισχύει:

$$||f_q(P)|| = ||qPq^{-1}|| = ||q|| \ ||P|| \ ||q^{-1}|| = ||P|| \frac{||q|| \ ||\overline{q}||}{||q||^2} = ||P||. \tag{4.15}$$

Επίσης, η f_q είναι ομομορφισμός, επειδή ισχύει:

$$f_q(P_1)f_q(P_2) = qP_1q^{-1}qP_2q^{-1} = qP_1P_2q^{-1} = f_q(P_1P_2). \tag{4.16}$$

Στη συνέχεια, θα βρούμε έναν τύπο για μία τετράδα q, η οποία αντιστοιχεί σε μία περιστροφή κατά γωνία θ, γύρω από έναν άξονα A. Εύκολα αποδεικνύεται ότι για $0 \neq \alpha \in \mathbb{R}$ ισχύει $f_{\alpha q} = f_q$. Στη συνέχεια θα ασχοληθούμε με τετράδες που έχουν μέτρο 1. Έστω $q = s + v$ μία τετράδα μέτρου 1. Τότε $q^{-1} = s - v$. Έστω και ένα σημείο $P \in \mathbb{R}^3$. Τότε έχουμε:

$$qPq^{-1} = (s+v)P(s-v) = \tag{4.17}$$

$$= (-v \cdot P + sP + v \times P)(s-v) \tag{4.18}$$

$$= -s(v \cdot P) + s^2 P + s(v \times P) + (v \cdot P)v - s(Pv) - (v \times P)v \tag{4.19}$$

$$= s^2 P + 2s(v \times P) + (v \cdot P)v - v \times (P \times v). \tag{4.20}$$

Χρησιμοποιώντας τη σχέση (4.2) έχουμε ότι:

$$qPq^{-1} = (s^2 - v \cdot v)P + 2s(v \times P) + 2(v \cdot P)v. \tag{4.21}$$

Θέτουμε $v = tA$, όπου $t \in \mathbb{R}$ και A ένα διάνυσμα μέτρου 1 και προκύπτει:

$$qPq^{-1} = (s^2 - t^2)P + 2st(A \times P) + 2t^2(A \cdot P)A. \tag{4.22}$$

Αν συγκρίνουμε την εξίσωση (4.22) με την εξίσωση (4.8), έχουμε τις παρακάτω ισότητες:

$$s^2 - t^2 = cos\theta, \tag{4.23}$$

$$2st = sin\theta, \tag{4.24}$$

$$2t^2 = 1 - cos\theta. \tag{4.25}$$

Η τρίτη εξίσωση συνεπάγεται ότι $t = \sqrt{\frac{1-cos\theta}{2}} = sin\frac{\theta}{2}$. Η πρώτη και η τρίτη εξίσωση συνεπάγονται ότι $s^2 + t^2 = 1$, οπότε έχουμε ότι $s = cos\frac{\theta}{2}$.

Με βάση τα παραπάνω, έχουμε προσδιορίσει ότι η τετράδα q (μέτρου 1), που αντιστοιχεί σε μία περιστροφή κατά γωνία θ γύρω από έναν άξονα A, δίνεται από τον παρακάτω τύπο:

$$q = cos\frac{\theta}{2} + sin\frac{\theta}{2}A. \tag{4.26}$$

Παρατηρούμε ότι αν πολλαπλασιάσουμε την τετράδα q με έναν πραγματικό αριθμό α, αποκτούμε πάλι την ίδια περιστροφή αφού ισχύει το παρακάτω:

$$(\alpha q)P(\alpha q)^{-1} = \alpha q P \frac{q^{-1}}{\alpha} = qPq^{-1}.$$

Το γινόμενο δύο τετράδων q_1, q_2 αναπαριστά επίσης μία περιστροφή. Συγκεκριμένα, το γινόμενο q_1q_2 αναπαριστά την περιστροφή που προκύπτει αν περιστρέψουμε πρώτα με το q_2 και μετά με το q_1. Αφού ισχύει η εξίσωση:

$$q_1(q_2Pq_2^{-1})q_1^{-1} = (q_1q_2)P(q_1q_2)^{-1},$$

μπορούμε να παραθέσουμε όσες τετράδες θέλουμε για να παραχθεί μία τετράδα, η οποία θα αντιστοιχεί σε μία ολόκληρη σειρά περιστροφών.

Πολλές φορές, για να περιγράψουμε μία περιστροφή ενός τρισδιάστατου διανύσματος κατά μία γωνία γύρω από ένα άξονα, χρησιμοποιούμε έναν 3×3 πίνακα ο οποίος ονομάζεται **πίνακας περιστροφής**. Αν πολλαπλασιάσουμε τον πίνακα αυτό με το αρχικό διάνυσμα, τότε παίρνουμε το διάνυσμα που προκύπτει από την περιστροφή. Για να πολλαπλασιάσουμε δύο τετράδες χρειαζόμαστε 16 πράξεις ενώ αν χρησιμοποιήσουμε τον πίνακα περιστροφής, θέλουμε 27 πράξεις. Από αυτό συμπεραίνουμε ότι αν θέλουμε να περιστρέψουμε πολλές φορές ένα τρισδιάστατο αντικείμενο, είναι υπολογιστικά πιο αποδοτικό να χρησιμοποιήσουμε τις τετράδες.

Σε κάποιες περιπτώσεις, είναι απαραίτητο να μετατρέψουμε μία τετράδα στον ισοδύναμο 3×3 πίνακα περιστροφής, για παράδειγμα, για να εισάγουμε το μετασχηματισμό ενός αντικειμένου σε μία βιβλιοθήκη 3D γραφικών. Έστω ότι P είναι το αρχικό διάνυσμα το οποίο θα περιστραφεί κατά γωνία θ γύρω από τον άξονα A. Θεωρούμε το A ως διάνυσμα μέτρου 1 και $A = (A_x, A_y, A_z)$. Τέλος, έστω ότι P' είναι το τελικό διάνυσμα και R_P ο

3×3 πίνακας περιστροφής. Τότε $P' = R_P P$, με:

$$R_P = \begin{bmatrix} 1-2y^2-2z^2 & 2xy-2wz & 2xz+2wy \\ 2xy+2wz & 1-2x^2-2z^2 & 2yz-2wx \\ 2xz-2wy & 2yz+2wx & 1-2x^2-2y^2 \end{bmatrix},$$

όπου $q = w + xi + yj + zk = s + tA$, $w = s,\ \ x = tA_x,\ \ y = tA_y,\ \ z = tA_z.$

4.2 Εφαρμογές των οκτάδων (Octonions)

Γνωρίζουμε ότι $\mathbb{O} = \mathbb{H} \oplus l\mathbb{H}$. Από τις εξισώσεις (3.2) συμπεραίνουμε ότι η άλγεβρα των οκτάδων μπορεί να παρασταθεί ως $\mathbb{O} = \mathbb{H} \oplus \mathbb{H}l$ ([15]). Έστω $a \in \mathbb{O}$ με:

$$a = a_0 + a_1 i + a_2 j + a_3 k + a_4 l + a_5 il + a_6 jl + a_7 kl.$$

Θα συμβολίζουμε:

$$Re(a) = a_0,\ \ Im(a) = a_1 i + a_2 j + a_3 k + a_4 l + a_5 il + a_6 jl + a_7 kl.$$

4.2.1 Αναπαράσταση των οκτάδων με πίνακες

Ισχύει ότι οποιαδήποτε πεπερασμένης διάστασης, προσεταιριστική άλγεβρα πάνω σε ένα τυχαίο σώμα K είναι ισομορφική με μία υποάλγεβρα μίας άλγεβρας πινάκων πάνω στο σώμα αυτό. Δηλαδή, οποιοδήποτε στοιχείο μίας πεπερασμένης διάστασης, προσεταιριστικής άλγεβρας πάνω στο K έχει μία αναπαράσταση με πίνακα, του οποίου τα στοιχεία ανήκουν στο K ([14]). Για την άλγεβρα των τετράδων $\mathbb{H}$, ισχύει ότι μέσω της 1-1 και επί απεικόνισης:

$$\phi : q = q_0 + q_1 i + q_2 j + q_3 k \in \mathbb{H} \mapsto \phi(q) = \begin{bmatrix} q_0 & -q_1 & -q_2 & -q_3 \\ q_1 & q_0 & -q_3 & q_2 \\ q_2 & q_3 & q_0 & -q_1 \\ q_3 & -q_2 & q_1 & q_0 \end{bmatrix}, \tag{4.27}$$

η $\mathbb{H}$ είναι ισομορφική με την άλγεβρα πινάκων:

$$M = \left\{ \begin{bmatrix} q_0 & -q_1 & -q_2 & -q_3 \\ q_1 & q_0 & -q_3 & q_2 \\ q_2 & q_3 & q_0 & -q_1 \\ q_3 & -q_2 & q_1 & q_0 \end{bmatrix} : q_0, q_1, q_2, q_3 \in \mathbb{R} \right\}. \tag{4.28}$$

Η $\phi(q)$ είναι η αναπαράσταση με πίνακα της τετράδας q. Την αναπαράσταση της τετράδας q με πίνακα μπορούμε να τη γράψουμε και ως εξής:

$$\tau(q) = D\phi^T(q)D = \begin{bmatrix} q_0 & -q_1 & -q_2 & -q_3 \\ q_1 & q_0 & q_3 & -q_2 \\ q_2 & -q_3 & q_0 & q_1 \\ q_3 & q_2 & -q_1 & q_0 \end{bmatrix}, \tag{4.29}$$

όπου $D = diag(1, -1, -1, -1)$.

Λήμμα 4.2.1. *Έστω $x = x_0 + x_1 i + x_2 j + x_3 k \in \mathbb{H}$ και έστω το στοιχείο:*

$$\overrightarrow{x} = [x_0, x_1, x_2, x_3]^T,$$

το οποίο καλείται ***διανυσματική αναπαράσταση*** *του x. Τότε για κάθε $a, b, x \in \mathbb{H}$, ισχύουν* *τα παρακάτω:*

$$\overrightarrow{ax} = \phi(a)\overrightarrow{x}, \tag{4.30}$$

$$\overrightarrow{xb} = \tau(b)\overrightarrow{x}, \tag{4.31}$$

$$\overrightarrow{axb} = \phi(a)\tau(b)\overrightarrow{x} = \tau(b)\phi(a)\overrightarrow{x}, \tag{4.32}$$

$$\phi(a)\tau(b) = \tau(b)\phi(a). \tag{4.33}$$

Ορισμός 4.2.1. *Έστω $a = a' + a''l \ \in \mathbb{O}, \ a', a'' \in \mathbb{H}$, όπου $a' = a_0 + a_1 i + a_2 j + a_3 k$, $a'' = a_4 + a_5 i + a_6 j + a_7 k$. Τότε ο παρακάτω 8×8 πίνακας, με στοιχεία από το $\mathbb{R}$:*

$$\omega(a) := \begin{bmatrix} \phi(a') & -\tau(a'')D_4 \\ \phi(a'')D_4 & \tau(a') \end{bmatrix}, \tag{4.34}$$

*καλείται **αριστερή αναπαράσταση με πίνακα** του a πάνω στο $\mathbb{R}$, όπου $D_4 = diag(1, -1, -1, -1)$.*

Θεώρημα 4.2.1. *Έστω $x = x_0 + x_1 i + x_2 j + x_3 k + x_4 l + x_5 il + x_6 jl + x_7 kl \in \mathbb{O}$ και έστω το στοιχείο:*

$$\overrightarrow{x} = [x_0, x_1, x_2, ..., x_7]^T,$$

*το οποίο καλείται **διανυσματική αναπαράσταση** του x. Τότε για κάθε $a, x \in \mathbb{O}$, ισχύει το παρακάτω:*

$$\overrightarrow{ax} = \omega(a)\overrightarrow{x}. \tag{4.35}$$

Απόδειξη. Έστω ότι $a = a' + a''l, \ x = x' + x''l \in \mathbb{O}$, όπου $a', a'', x', x'' \in \mathbb{H}$. Γνωρίζουμε ότι:

$$ax = (a'x' - \overline{x''}a'') + (x''a' + a''\overline{x'})l.$$

Με τη βοήθεια των εξισώσεων (4.30),(4.31),(4.32) έχουμε:

$$\overrightarrow{ax} = \begin{bmatrix} \overrightarrow{a'x' - \overline{x''}a''} \\ \overrightarrow{x''a' + a''\overline{x'}}. \end{bmatrix} = \begin{bmatrix} \overrightarrow{a'x'} - \overrightarrow{\overline{x''}a''} \\ \overrightarrow{x''a'} + \overrightarrow{a''\overline{x'}}. \end{bmatrix}$$

$$= \begin{bmatrix} \phi(a')\overrightarrow{x'} - \tau(a'')D_4\overrightarrow{x''} \\ \tau(a')\overrightarrow{x''} + \phi(a'')D_4\overrightarrow{x'} \end{bmatrix}$$

$$= \begin{bmatrix} \phi(a') & -\tau(a'')D_4 \\ \phi(a'')D_4 & \tau(a') \end{bmatrix} \begin{bmatrix} \overrightarrow{x'} \\ \overrightarrow{x''} \end{bmatrix}$$

□

Ορισμός 4.2.2. *Έστω* $a = a' + a''l \ \in \mathbb{O}, \ a', a'' \in \mathbb{H}$, *όπου* $a' = a_0 + a_1 i + a_2 j + a_3 k$, $a'' = a_4 + a_5 i + a_6 j + a_7 k$. *Τότε ο παρακάτω* 8×8 *πίνακας, με στοιχεία από το* $\mathbb{R}$*:*

$$\nu(a) := \begin{bmatrix} \tau(a') & -\phi(\overline{a''}) \\ \phi(a'') & \tau(\overline{a'}) \end{bmatrix}, \tag{4.36}$$

καλείται ***δεξιά αναπαράσταση με πίνακα*** *του* a *πάνω στο* $\mathbb{R}$.

Θεώρημα 4.2.2. *Έστω* $a, x \in \mathbb{O}$. *Τότε ισχύει το παρακάτω:*

$$\overrightarrow{xa} = \nu(a)\overrightarrow{x}. \tag{4.37}$$

Απόδειξη. Έστω ότι $a = a' + a''l, \ x = x' + x''l \in \mathbb{O}$, όπου $a', a'', x', x'' \in \mathbb{H}$. Γνωρίζουμε ότι:

$$xa = (x'a' - \overline{a''}x'') + (a''x' + x''\overline{a'})l.$$

Με τη βοήθεια των εξισώσεων (4.30),(4.31),(4.32) έχουμε:

$$\begin{aligned}
\overrightarrow{xa} = \begin{bmatrix} \overrightarrow{x'a' - \overline{a''}x''} \\ \overrightarrow{a''x' + x''\overline{a'}}. \end{bmatrix} &= \begin{bmatrix} \overrightarrow{x'a'} - \overrightarrow{\overline{a''}x''} \\ \overrightarrow{a''x'} + \overrightarrow{x''\overline{a'}}. \end{bmatrix} \\
&= \begin{bmatrix} \tau(a')\overrightarrow{x'} - \phi(\overline{a''})\overrightarrow{x''} \\ \phi(a'')\overrightarrow{x'} + \tau(\overline{a'})\overrightarrow{x''} \end{bmatrix} \\
&= \begin{bmatrix} \tau(a') & -\phi(\overline{a''}) \\ \phi(a'') & \tau(\overline{a'}) \end{bmatrix} \begin{bmatrix} \overrightarrow{x'} \\ \overrightarrow{x''} \end{bmatrix}
\end{aligned}$$

□

Θεώρημα 4.2.3. *Έστω $a \in \mathbb{O}$. Ισχύουν τα ακόλουθα:*

$$\omega(a^2) = \omega^2(a), \tag{4.38}$$

$$\nu(a^2) = \nu^2(a), \tag{4.39}$$

$$\omega(a)\nu(a) = \nu(a)\omega(a). \tag{4.40}$$

4.2.2 Γραμμικές εξισώσεις με συντελεστές από το $\mathbb{O}$

Ισχύουν τα παρακάτω Θεωρήματα (βλ. [14]).

Θεώρημα 4.2.4. *Έστω $a, b \in \mathbb{O}$ και έστω $a = a_0+a_1i+a_2j+a_3k+a_4l+a_5il+a_6jl+a_7kl$. Τότε η γραμμική εξίσωση $ax = xb$ έχει μη μηδενική λύση αν και μόνο αν:*

$$Re(a) = Re(b) \ \ \textit{και} \ \ ||Im(a)|| = ||Im(b)||.$$

1. *Αν $b \neq \overline{a}$, δηλαδή αν $Im(a) + Im(b) \neq 0$, τότε η γενική λύση της εξίσωσης $ax = xb$ μπορεί να εκφραστεί ως εξής:*

$$x = (Im(a))p + p(Im(b)),$$

όπου το p είναι ένα τυχαίο στοιχείο της υποάλγεβρας που παράγουν τα a, b. Ισοδύναμα,

$$x = \lambda_1(Im(a) + Im(b)) + \lambda_2[||Im(a)||\ ||Im(b)|| - (Im(a))(Im(b))],$$

όπου λ_1, λ_2 είναι τυχαίοι πραγματικοί αριθμοί.

2. *Αν $b = \overline{a}$, τότε η γενική λύση της εξίσωσης $ax = xb$ είναι η:*

$$x = x_1 i + x_2 j + x_3 k + x_4 l + x_5 il + x_6 jl + x_7 kl,$$

όπου τα $x_1, ..., x_7$ ικανοποιούν την ισότητα:

$$a_1 x_1 + a_2 x_2 + ... + a_7 x_7 = 0.$$

Θεώρημα 4.2.5. *Έστω $a, b \in \mathbb{O}$ με $a \notin \mathbb{R}$. Τότε η γραμμική εξίσωση:*

$$ax - xa = b$$

έχει λύση στο $\mathbb{O}$ αν και μόνο αν $ab = b\overline{a}$. Σε αυτήν την περίπτωση, η γενική λύση της εξίσωσης $ax - xa = b$ είναι:

$$x = \frac{1}{4||Im(a)||^2}(ba - ab) + p - \frac{1}{||Im(a)||^2}(Im(a))p(Im(a)),$$

όπου p είναι ένα τυχαίο στοιχείο του $\mathbb{O}$.

Θεώρημα 4.2.6. *Έστω $a, b \in \mathbb{O}$ με $a \notin \mathbb{R}$ και $a = a_0 + a_1 i + a_2 j + a_3 k + a_4 l + a_5 il + a_6 jl + a_7 kl$. Τότε η εξίσωση:*

$$ax - x\overline{a} = b \tag{4.41}$$

έχει λύση αν και μόνο αν υπάρχουν $\lambda_0, \lambda_1 \in \mathbb{R}$*, τέτοια ώστε:*

$$b = \lambda_0 + \lambda_1 a.$$

Σε αυτήν την περίπτωση η γενική λύση της εξίσωσης (4.41) *είναι η:*

$$x = \frac{\lambda_1}{2} + x_1 i + ... + x_7 kl,$$

όπου τα $x_1, ..., x_7$ *ικανοποιούν την ισότητα:*

$$a_1 x_1 + ... + a_7 x_7 = -\frac{1}{2} Re(b).$$

Βιβλιογραφία

[1] Ανάργυρος Γ. Φελλούρης, Γραμμική Άλγεβρα και Αναλυτική Γεωμετρία, Αθήνα 2006

[2] Ανάργυρος Γ. Φελλούρης, Θέματα Άλγεβρας, Σημειώσεις παραδόσεων, Εθνικό Μετσόβιο Πολυτεχνείο, Αθήνα

[3] Pete L. Clark, Nonassociative Algebras

[4] Keith Conrad, Tensor Products

[5] Ernst Dieterich, A General Approach to Finite Dimensional Division Algebras, Uppsala University, Department of Mathematics, 2011

[6] Alberto Elduque, Composition Algebras and their Gradings, Universidad de Zaragoza, Spain

[7] John B. Fraleigh, Εισαγωγή στην Άλγεβρα, Πανεπιστημιακές Εκδόσεις Κρήτης, Ηράκλειο 2010

[8] Eric Lengyel, Mathematics for 3D Game Programming and Computer Graphics, Charles River Media, Inc, 2002

[9] R. Mukundan, Quaternions: From Classical Mechanics to Computer Graphics and Beyond, University of Canterbury, Department of Computer Science, New Zealand, Proceedings of the 7^{th} Asian Technology Conference in Mathematics, 2002

[10] Rasmus Précenth, The (1,2,4,8)-Theorem for Composition Algebras, Uppsala University, Department of Mathematics, 2013

[11] Eitan Reich, Bilinear Forms, February 2005

[12] A. Sagle, R. Walde, Introduction to Lie Groups and Lie Algebras, Academic Press, 1973

[13] Richard D. Schafer, An Introduction to Nonassociative Algebras, Dover Publications, New York 1994

[14] Yongge Tian, Matrix Representations of Octonions and their Applications, Queen's University, Department of Mathematics and Statistics, April 2000

[15] K. A. Zhevlakov, A. M. Slinko, I. P. Shestakov, A. I. Shirshov, Rings that are nearly associative, Academic Press, New York 1982

[16] Natalia Zhukavets, Composition Algebras, Lecture notes, Finland, April 2007

Ηλεκτρονική Βιβλιογραφία

[A] Composition Algebra, Wikipedia, Free Encyclopedia

[B] Field Extension, Wikipedia, Free Encyclopedia

[C] Octonion, Wikipedia, Free Encyclopedia

[D] Quaternion, Wikipedia, Free Encyclopedia

[E] Separable Extension, Wikipedia, Free Encyclopedia

[F] Separable Polynomial, Wikipedia, Free Encyclopedia