



ΕΛΛΗΝΙΚΟ ΑΝΟΙΚΤΟ ΠΑΝΕΠΙΣΤΗΜΙΟ

Σχολή Θετικών Επιστημών

Μεταπτυχιακές Σπουδές στα μαθηματικά

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Τα Οκτόνια: Κατασκευή και Ιδιότητες

Ταγγίρης Μιχαήλ

Επιβλέπων Καθηγητής: Αρβανιτογεώργος Ανδρέας

Πάτρα
Ιούνιος, 2026

Η παρούσα εργασία αποτελεί πνευματική ιδιοκτησία του φοιτητή («συγγραφέας/δημιουργός») που την εκπόνησε. Στο πλαίσιο της πολιτικής ανοικτής πρόσβασης ο συγγραφέας/δημιουργός εκχωρεί στο ΕΑΠ, μη αποκλειστική άδεια χρήσης του δικαιώματος αναπαραγωγής, προσαρμογής, δημόσιου δανεισμού, παρουσίασης στο κοινό και ψηφιακής διάχυσής τους διεθνώς, σε ηλεκτρονική μορφή και σε οποιοδήποτε μέσο, για διδακτικούς και ερευνητικούς σκοπούς, άνευ ανταλλάγματος και για όλο το χρόνο διάρκειας των δικαιωμάτων πνευματικής ιδιοκτησίας. Η ανοικτή πρόσβαση στο πλήρες κείμενο για μελέτη και ανάγνωση δεν σημαίνει καθ' οιονδήποτε τρόπο παραχώρηση δικαιωμάτων διανοητικής ιδιοκτησίας του συγγραφέα/δημιουργού ούτε επιτρέπει την αναπαραγωγή, αναδημοσίευση, αντιγραφή, αποθήκευση, πώληση, εμπορική χρήση, μετάδοση, διανομή, έκδοση, εκτέλεση, «μεταφόρτωση» (downloading), «ανάρτηση» (uploading), μετάφραση, τροποποίηση με οποιονδήποτε τρόπο, τμηματικά ή περιληπτικά της εργασίας, χωρίς τη ρητή προηγούμενη έγγραφη συναίνεση του συγγραφέα/δημιουργού. Ο συγγραφέας/δημιουργός διατηρεί το σύνολο των ηθικών και περιουσιακών του δικαιωμάτων.



Σχολή Θετικών Επιστημών

Μεταπτυχιακές Σπουδές στα μαθηματικά

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Τα Οκτόνια: Κατασκευή και Ιδιότητες

Ταγγίρης Μιχαήλ

Επιτροπή Επίβλεψης Διπλωματικής Εργασίας

Επιβλέπων Καθηγητής:

Αρβανιτογεώργος Ανδρέας

Καθηγητής
Πανεπιστημίου Πατρών

Συν-Επιβλέπων Καθηγητής:

Ανούσης Μιχαήλ

Ομότιμος Καθηγητής
Πανεπιστημίου Αιγαίου

Πάτρα
Ιούνιος, 2026

Θα ήθελα να ευχαριστήσω τους επιβλέποντες καθηγητές μου, κ. Ανούση και κ. Αρβανιτογεώργο. Ιδιαίτερα ευχαριστώ τον κ. Αρβανιτογεώργο για τη βοήθεια και την καθοδήγησή του, αλλά και για την υπομονή που επέδειξε απέναντί μου.

Περίληψη

Στην παρούσα διπλωματική εργασία παρουσιάζεται η άλγεβρα των οκτονίων. Αρχικά γίνεται μια ιστορική ανασκόπηση της επέκτασης του συνόλου των πραγματικών αριθμών στους μιγαδικούς, κατόπιν στους υπερμιγαδικούς και τελικά στα οκτόνια. Στη συνέχεια ορίζονται οι composition άλγεβρες και η μέθοδος διπλασιασμού των Cayley–Dickson. Τα τρία σύνολα που επεκτείνουν τους πραγματικούς αριθμούς κατασκευάζονται με τη μέθοδο του διπλασιασμού και με την απόδειξη του Θεωρήματος Hurwitz αποδεικνύεται ότι η διαδικασία επέκτασης δεν μπορεί να συνεχιστεί πέραν των οκτονίων. Οι βασικές ιδιότητες των οκτονίων αποδεικνύονται στο πλαίσιο των ιδιοτήτων των composition αλγεβρών επί του σώματος των πραγματικών αριθμών. Εξετάζεται η επέκταση της έννοιας του ακέραιου αριθμού και της διαιρετότητας στα παραπάνω σύνολα. Η έννοια της διαίρεσης με «μικρό υπόλοιπο» παρουσιάζεται για τους μιγαδικούς και τους υπερμιγαδικούς γεωμετρικά και στα οκτόνια με τη χρήση του πλέγματος E_8 . Οι ακέριοι Gauss παρουσιάζονται συνοπτικά, ενώ για τους ακέριους Hurwitz αποδεικνύονται τα θεωρήματα που μας δίνουν το πλήθος των αναλύσεων σε πρώτους παράγοντες στην περίπτωση του πρωταρχικού και του γενικού ακέριου Hurwitz. Τέλος, αφού κατασκευαστούν οι μέγιστες τάξεις των ακέριων οκτονίων παρουσιάζεται ο αλγόριθμος του Rehm, το πλήθος των αναλύσεων σε πρώτους παράγοντες ενός πρωταρχικού καθώς και σε ειδικές περιπτώσεις μη πρωταρχικού ακέριου οκτονίου.

Λέξεις κλειδιά:

Οκτόνια, Διπλασιασμός Cayley–Dickson, Composition άλγεβρες, Ακέρια οκτόνια.

Abstract

This thesis presents the algebra of octonions. First, a historical review of the extension of the set of real numbers to complex numbers, then to quaternions, and finally to octonions is provided. Next, composition algebras and the Cayley–Dickson doubling process are defined. The three sets that extend the real numbers are constructed using this doubling process, and through the proof of Hurwitz's Theorem, it is demonstrated that this extension process cannot yield composition algebras beyond the octonions. The fundamental properties of octonions are proved within the framework of the properties of composition algebras over the field of real numbers. Furthermore, the extension of the concepts of integers and divisibility to the aforementioned sets is examined. The concept of division with a "small remainder" is presented geometrically for complex numbers and quaternions, and for octonions by utilizing the E_8 lattice. Gaussian integers are briefly introduced, while for Hurwitz integers, we prove the theorems that yield the number of prime factorizations in both the primitive and the general Hurwitz integer cases. Finally, after constructing the maximal orders of integral octonions, Rehm's algorithm is presented, along with the number of prime factorizations of a primitive, as well as specific cases of a non-primitive, integral octonion.

Keywords:

Octonions, Cayley–Dickson construction, Composition algebras, Integral octonions

Περιεχόμενα

Περίληψη	v
Abstract	vi
Κεφάλαιο 1. Η διαδρομή από τους πραγματικούς στα οκτόνια	1
1.1 Οι πραγματικοί αριθμοί ($\mathbb{R}$).....	1
1.2 Οι μιγαδικοί αριθμοί ($\mathbb{C}$)	1
1.3 Οι υπερμιγαδικοί αριθμοί ($\mathbb{H}$)	5
1.4 Τα οκτόνια ($\mathbb{O}$)	8
Κεφάλαιο 2. Composition άλγεβρες – Θεώρημα Hurwitz – Ιδιότητες των οκτονίων	17
2.1 Βασικοί ορισμοί και προτάσεις.....	17
2.2 Η μέθοδος διπλασιασμού Cayley–Dickson.....	22
2.3 Το Θεώρημα Hurwitz	25
2.4 Συνέπειες του Θεωρήματος Hurwitz – Άλλες ιδιότητες των αλγεβρών.....	30
Κεφάλαιο 3. Θεωρία αριθμών και άλγεβρες διαίρεσης.....	41
3.1 Οι ακέραιοι Gauss	41
3.2 Οι ακέραιοι Hurwitz	43
3.3 Τα ακέραια οκτόνια	52
3.3.1 Οι συμβολισμοί των Conway–Smith για τα οκτόνια	52
3.3.2 Ακέραια οκτόνια	54
3.4 Ανάλυση των ακέραιων οκτονίων σε παράγοντες	67
3.4.1 Διαίρεση «με μικρό υπόλοιπο» και ιδεώδη στα ακέραια οκτόνια	67
3.4.2 Οι διαιρέτες ενός ακέραιου οκτονίου	72
3.4.3 Το πλήθος των αναλύσεων των ακέραιων οκτονίων σε παράγοντες	77
4. Συμπεράσματα.....	81
Βιβλιογραφία	83
Διαδικτυακές πηγές	84

Κατάλογος εικόνων

Εικόνα 1.1: Διάγραμμα για τον πολλαπλασιασμό υπερμιγαδικών	6
Εικόνα 1.2: Το άρθρο του Cayley για τα οκτόνια στο Philosophical Magazine	10
Εικόνα 1.3: Διάγραμμα Fano για τον πολλαπλασιασμό οκτονίων.	12
Εικόνα 3.1: Το πλέγμα των ακέραιων του Gauss	41
Εικόνα 3.2: Μέγιστο μέτρο υπολοίπου για τους ακέραιους του Gauss (προσαρμογή από τους Conway–Smith)	42
Εικόνα 3.3: Το τρίγωνο Catalan	50
Εικόνα 3.4: Διάγραμμα Fano για τον πολλαπλασιασμό οκτονίων «κατά τους Conway–Smith»	54
Εικόνα 3.5: Οι 16 τάξεις που περιέχουν τους ακέραιους του Graves, G^8 (προσαρμογή από τους Conway–Smith)	62
Εικόνα 3.6: Τα 8 εξωτερικά 0–σύνολα παράγονται από ένα, με πολλαπλασιασμούς με i_3, i_5 ή i_6 (προσαρμογή από τους Conway–Smith)	64
Εικόνα 3.7: Παραγωγή των n –ακέραιων σύμφωνα με το Λήμμα 3.28β (προσαρμογή από τους Conway–Smith)	65
Εικόνα 3.8: Τα ακέραια οκτόνια που παράγουν το E_8 (επιλογή των κορυφών από τους Conway–Smith)	70
Εικόνα 3.9: Η «ευθεία κατεύθυνση» του αλγόριθμου του Rehm (προσαρμογή από τους Conway–Smith)	72
Εικόνα 3.10: Η «αντίστροφη κατεύθυνση» του αλγόριθμου του Rehm (προσαρμογή από τους Conway–Smith)	74

Κατάλογος πινάκων

Πίνακας 1.1: Πίνακας πολλαπλασιασμού υπερμιγαδικών	6
Πίνακας 1.2: Πίνακας πολλαπλασιασμού οκτονίων	11
Πίνακας 3.1: Πίνακας πολλαπλασιασμού οκτονίων «κατά τους Conway–Smith»	53
Πίνακας 3.2: Πίνακας των ∞ –συνόλων (από τους Conway–Smith)	57
Πίνακας 3.3: Πίνακας των n –συνόλων (από τους Conway–Smith)	58
Πίνακας 3.4: Πίνακας πολλαπλασιασμού των $i_{\infty 356}, i_{0235}, i_{0463}, i_{0156}$	59
Πίνακας 3.5: Πίνακας πολλαπλασιασμού των $i_{\infty 356}, i_{0235}, i_{0463}, i_{0156}$ με τη βάση των οκτονίων	60

Κεφάλαιο 1. Η διαδρομή από τους πραγματικούς στα οκτόνια

1.1 Οι πραγματικοί αριθμοί ($\mathbb{R}$)

Οι πραγματικοί αριθμοί και οι ιδιότητές τους θεωρούνται γνωστοί. Επισημαίνουμε μόνο ότι το σύνολο των πραγματικών αριθμών είναι ένα διατεταγμένο σώμα με τις γνωστές πράξεις της πρόσθεσης και του πολλαπλασιασμού. Επίσης, αν θεωρήσουμε το σύνολό τους ως διανυσματικό χώρο διάστασης 1, τότε σε κάθε πραγματικό αριθμό α μπορεί να αποδοθεί μια έννοια μήκους $|\alpha|$ η οποία ορίζεται από τη σχέση:

$$|\alpha| = \sqrt{\alpha^2}$$

για την οποία ισχύουν οι ιδιότητες:

για κάθε $\alpha, \beta \in \mathbb{R}$

- $|\alpha| = 0 \Leftrightarrow \alpha = 0$
- $|\alpha\beta| = |\alpha||\beta|$.

Τέλος, κάθε μη-μηδενικός πραγματικός αριθμός α έχει έναν πολλαπλασιαστικό αντίστροφο

$$\alpha^{-1} = \frac{1}{\alpha}$$

τέτοιον ώστε: $\alpha\alpha^{-1} = \alpha^{-1}\alpha = 1$.

1.2 Οι μιγαδικοί αριθμοί ($\mathbb{C}$)

Ιστορική ανασκόπηση

Για αιώνες το σύνολο των πραγματικών αριθμών ήταν επαρκές για τα μαθηματικά και τους μαθηματικούς. Δεν ορίζονταν τετραγωνικές ρίζες αρνητικών αριθμών, άρα εξισώσεις όπως η: $x^2 + 1 = 0$ θεωρούνταν αδύνατες.

Στις αρχές του 16^{ου} αι. οι S. del Ferro και N. Tartaglia μελέτησαν ανεξάρτητα την επίλυση της τριτοβάθμιας πολυωνυμικής εξίσωσης και τα αποτελέσματά τους παρουσιάστηκαν από τον G. Cardano στο έργο του «Ars Magna» (1545).

Μια από τις περιπτώσεις που εξέτασε ο Cardano ήταν η εξίσωση: $x^3 = px + q$, βρίσκοντας ότι έχει λύση την:

$$x = \sqrt[3]{\frac{q}{2} + \sqrt{\left(\frac{q}{2}\right)^2 - \left(\frac{p}{3}\right)^3}} + \sqrt[3]{\frac{q}{2} - \sqrt{\left(\frac{q}{2}\right)^2 - \left(\frac{p}{3}\right)^3}}.$$

Το πρόβλημα που παρατήρησε και ο Cardano ήταν στην περίπτωση που ίσχυε:

$$\left(\frac{q}{2}\right)^2 < \left(\frac{p}{3}\right)^3.$$

Σε αυτήν την περίπτωση βρήκε εξισώσεις όπως η $x^3 = 15x + 4$ για την οποία, ενώ έχει προφανή ρίζα το 4, ο τύπος της λύσης έδινε:

$$x = \sqrt[3]{2 + \sqrt{-121}} + \sqrt[3]{2 - \sqrt{-121}}.$$

Ο Cardano συνάντησε παρόμοιες παραστάσεις λύνοντας και άλλες μορφές της τριτοβάθμιας και τις ονόμασε «σοφιστικές» μην μπορώντας να αποδεχθεί την ύπαρξη τετραγωνικών ριζών αρνητικών αριθμών.

Ο R. Bombelli, στο έργο του «L' Algebra» (1572), καθόρισε την εκτέλεση των πράξεων μεταξύ παραστάσεων της μορφής $a \pm \sqrt{-b}$, όπου $\sqrt{-b}$ τετραγωνική ρίζα αρνητικού αριθμού.

Μεταξύ άλλων έδειξε ότι:

$$3 + \sqrt{-16} = (2 + \sqrt{-1})^2.$$

Χρησιμοποιώντας το παραπάνω αποτέλεσμα οδηγήθηκε στις:

$$(3 + \sqrt{-16}) \cdot (2 + \sqrt{-1}) = (2 + \sqrt{-1})^3 = 2 + \sqrt{-121}$$

επομένως,

$$\sqrt[3]{2 + \sqrt{-121}} = 2 + \sqrt{-1} \text{ και με όμοιο τρόπο, } \sqrt[3]{2 - \sqrt{-121}} = 2 - \sqrt{-1},$$

δίνοντας έτσι νόημα στη λύση του Cardano για την $x^3 = 15x + 4$, αφού:

$$x = \sqrt[3]{2 + \sqrt{-121}} + \sqrt[3]{2 - \sqrt{-121}} = 2 + \sqrt{-1} + 2 - \sqrt{-1} = 4.$$

Με την εργασία αυτή θεμελιώθηκε ο λογισμός των μιγαδικών αριθμών και δικαιολογημένα η πατρότητά του αποδίδεται στον Bombelli.

Αν και οι παραστάσεις της μορφής $\alpha + \beta\sqrt{-1}$ χρησιμοποιήθηκαν σε εργασίες πολλών μαθηματικών (L. Euler, L. Lagrange κ.ά.) δεν είχαν γίνει αποδεκτές ως αριθμοί.

Ο Euler το 1777 χρησιμοποίησε το i για να συμβολίσει το $\sqrt{-1}$, από τη λέξη *imaginaire* (φανταστικός). Η λέξη αυτή είχε χρησιμοποιηθεί από τον Descartes υποτιμητικά για τις ρίζες αρνητικών αριθμών.

Οι G. Wessel και J.R. Argand σε εργασίες τους το 1799 και το 1806 έδωσαν γεωμετρική ερμηνεία στις παραστάσεις αυτές ως προσανατολισμένα ευθύγραμμα τμήματα (ο διανυσματικός λογισμός δεν είχε αναπτυχθεί ακόμα).

Ο C.F. Gauss το 1831 καθιέρωσε τον όρο «μιγαδικοί» (complex) για τις παραστάσεις της μορφής $\alpha + \beta i$ και τους έδωσε γεωμετρική υπόσταση.

Η αλγεβρική θεμελίωση του συνόλου των μιγαδικών αριθμών έγινε στην εργασία του W.R. Hamilton «Theory of conjugate functions or algebraic couples» (1837). Ο Hamilton όρισε τους μιγαδικούς αριθμούς ως διατεταγμένα ζεύγη πραγματικών, $\alpha + \beta i = (\alpha, \beta)$ και τις πράξεις μεταξύ τους με τις ακόλουθες σχέσεις:

$$(\alpha_1, \beta_1) + (\alpha_2, \beta_2) = (\alpha_1 + \alpha_2, \beta_1 + \beta_2)$$

$$(\alpha_1, \beta_1) - (\alpha_2, \beta_2) = (\alpha_1 - \alpha_2, \beta_1 - \beta_2)$$

$$(\alpha_1, \beta_1) \cdot (\alpha_2, \beta_2) = (\alpha_1\alpha_2 - \beta_1\beta_2, \alpha_1\beta_2 + \beta_1\alpha_2)$$

$$\frac{(\alpha_1, \beta_1)}{(\alpha_2, \beta_2)} = \left(\frac{\alpha_1\alpha_2 + \beta_1\beta_2}{\alpha_2^2 + \beta_2^2}, \frac{\beta_1\alpha_2 - \alpha_1\beta_2}{\alpha_2^2 + \beta_2^2} \right).$$

Επίσης, αντιστοίχισε κάθε πραγματικό αριθμό α στο ζεύγος $(\alpha, 0)$.

Σχεδόν 300 χρόνια μετά την πρώτη τους εμφάνιση, οι μιγαδικοί έχουν πια θεμελιωθεί ως σύνολο. Η διαδικασία αυτή ήταν ουσιαστικά το έναυσμα για τη φυσιολογική, τουλάχιστον για τα μαθηματικά, πορεία επέκτασης στους υπερμιγαδικούς και τελικά στα οκτόνια.

Οι μιγαδικοί αριθμοί και οι ιδιότητές τους

Μιγαδικός αριθμός ονομάζεται μια παράσταση της μορφής:

$$\alpha + \beta i, \text{ με } \alpha, \beta \in \mathbb{R} \text{ και } i^2 = -1.$$

Η πρόσθεση μιγαδικών ορίζεται από τη σχέση:

$$(\alpha + \beta i) + (\gamma + \delta i) = (\alpha + \gamma) + (\beta + \delta)i,$$

ενώ ο πολλαπλασιασμός από την:

$$(\alpha + \beta i) \cdot (\gamma + \delta i) = (\alpha\gamma - \beta\delta) + (\alpha\delta + \beta\gamma)i.$$

Για κάθε μιγαδικό αριθμό $z = \alpha + \beta i$ ορίζουμε:

- τον συζυγή του $\bar{z} = \alpha - \beta i$.
- το μέτρο του $|z| = \sqrt{\alpha^2 + \beta^2}$
- τη νόρμα του $N(z) = |z|^2 = z\bar{z} = \alpha^2 + \beta^2$.

Άμεσοι υπολογισμοί μας δίνουν ότι:

- $|z| = 0 \Leftrightarrow N(z) = 0 \Leftrightarrow z = 0$
- κάθε μη μηδενικός μιγαδικός z έχει μοναδικό αντίστροφο, τον:

$$z^{-1} = \frac{\bar{z}}{N(z)}$$

Τέλος, είναι εύκολο ναδειχθεί η ταυτότητα των δύο τετραγώνων:

$$(\alpha\gamma - \beta\delta)^2 + (\alpha\delta + \beta\gamma)^2 = (\alpha^2 + \beta^2) \cdot (\gamma^2 + \delta^2),$$

η οποία σημαίνει ότι, για δύο οποιουσδήποτε μιγαδικούς $z_1 = \alpha + \beta i$ και $z_2 = \gamma + \delta i$ ισχύει:

$$N(z_1 \cdot z_2) = N(z_1) \cdot N(z_2). \quad (1.1)$$

1.3 Οι υπερμιγαδικοί αριθμοί (III)

Ιστορική ανασκόπηση

Παρακινημένος από την επιτυχία του στους μιγαδικούς αριθμούς, αλλά και τη στενή τους σχέση με τη γεωμετρία του επιπέδου, ο Hamilton προσπάθησε να επινοήσει μια δομή η οποία θα είχε παρόμοια εφαρμογή στη γεωμετρία του χώρου. Με σύγχρονους όρους, προσπαθούσε να επινοήσει μια άλγεβρα διαίρεσης με νόρμα και διάσταση 3.

Οι προσπάθειές του υπήρξαν ανεπιτυχείς (σήμερα είναι γνωστό ότι τέτοια άλγεβρα δεν υπάρχει) μέχρι τη 16^η Οκτωβρίου 1843 όταν, κατά τη διάρκεια ενός περιπάτου κατά μήκος του «Βασιλικού Καναλιού» στο Δουβλίνο, συνειδητοποίησε ότι στην πραγματικότητα χρειαζόταν μια άλγεβρα τεσσάρων διαστάσεων, όπως επίσης και να εγκαταλείψει την απαίτηση για μεταθετικότητα του πολλαπλασιασμού.

Ο ενθουσιασμός του γι' αυτήν την ανακάλυψη τον οδήγησε να σκαλίζει στη γέφυρα Brougham, κάτω από την οποία περνούσε, τις εξισώσεις:

$$\langle i^2 = j^2 = k^2 = ijk = -1 \rangle.$$

Ο Hamilton αλλά και μεταγενέστεροι μαθηματικοί όπως ο Peter Tait και ο Benjamin Peirce, υποστήριξαν για χρόνια τη χρησιμότητα των υπερμιγαδικών σε εφαρμογές στη γεωμετρία και στη φυσική. Πράγματι, χρησιμοποιήθηκαν αρχικά για την περιγραφή του ηλεκτρομαγνητισμού. Η ανάπτυξη όμως του διανυσματικού λογισμού στα τέλη του 19^{ου} αι. τους παραγκώνισε, αφήνοντας μόνο τον συμβολισμό i, j, k για τα μοναδιαία διανύσματα στα καρτεσιανά συστήματα συντεταγμένων.

Προς το τέλος του 20^{ου} αι. η χρήση των υπερμιγαδικών ανέκαμψε, καθώς διευκολύνει υπολογιστικά την αναπαράσταση περιστροφών στον χώρο και εφαρμόζεται στη ρομποτική, στον προγραμματισμό βιντεοπαιχνιδιών αλλά και στην αεροδιαστημική.

Οι υπερμιγαδικοί αριθμοί και οι ιδιότητές τους

Υπερμιγαδικός αριθμός (quaternion) ονομάζεται μια παράσταση της μορφής:

$$\alpha + \beta i + \gamma j + \delta k, \text{ με } \alpha, \beta, \gamma, \delta \in \mathbb{R}$$

Η πρόσθεση υπερμιγαδικών ορίζεται από τη σχέση:

$$(\alpha_1 + \beta_1 i + \gamma_1 j + \delta_1 k) + (\alpha_2 + \beta_2 i + \gamma_2 j + \delta_2 k)$$

$$= (\alpha_1 + \alpha_2) + (\beta_1 + \beta_2)i + (\gamma_1 + \gamma_2)j + (\delta_1 + \delta_2)k$$

Οι i, j, k ονομάζονται υπερμιγαδικές φανταστικές μονάδες και ικανοποιούν τους παρακάτω κανόνες πολλαπλασιασμού:

$$i^2 = j^2 = k^2 = -1 \quad (1.2)$$

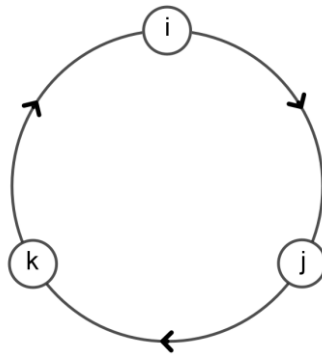
και

$$ijk = -1. \quad (1.3)$$

Από τις δύο τελευταίες σχέσεις, ορίζοντας το $1 = 1 + 0i + 0j + 0k$ ως μοναδιαίο στοιχείο του πολλαπλασιασμού και απαιτώντας αυτός να είναι προσεταιριστικός, έχουμε ότι:

$$ij = k \quad jk = i \quad ki = j \quad ji = -k \quad kj = -i \quad ik = -j. \quad (1.4)$$

Οι σχέσεις αυτές δίνονται συνήθως εποπτικά από το παρακάτω διάγραμμα:



Εικόνα 1.1: Διάγραμμα για τον πολλαπλασιασμό υπερμιγαδικών

Στο διάγραμμα αυτό, πολλαπλασιάζοντας δύο στοιχεία ακολουθώντας τη φορά των βελών παίρνουμε ως αποτέλεσμα το επόμενο στοιχείο. Όταν πολλαπλασιάζουμε δύο στοιχεία ακολουθώντας την αντίθετη φορά, παίρνουμε ως αποτέλεσμα το αντίθετο του επόμενου στοιχείου.

Οι παραπάνω σχέσεις μας δίνουν τον ακόλουθο πίνακα πολλαπλασιασμού:

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

Πίνακας 1.1: Πίνακας πολλαπλασιασμού υπερμιγαδικών

με βάση τον οποίο μπορούμε να ορίσουμε τον πολλαπλασιασμό υπερμιγαδικών ως εξής:

$$\begin{aligned}
 (\alpha_1 + \beta_1 i + \gamma_1 j + \delta_1 k) \cdot (\alpha_2 + \beta_2 i + \gamma_2 j + \delta_2 k) = \\
 (\alpha_1 \alpha_2 - \beta_1 \beta_2 - \gamma_1 \gamma_2 - \delta_1 \delta_2) \\
 + (\alpha_1 \beta_2 + \beta_1 \alpha_2 + \gamma_1 \delta_2 - \delta_1 \gamma_2) i \\
 + (\alpha_1 \gamma_2 - \beta_1 \delta_2 + \gamma_1 \alpha_2 + \delta_1 \beta_2) j \\
 + (\alpha_1 \delta_2 + \beta_1 \gamma_2 - \gamma_1 \beta_2 + \delta_1 \alpha_2) k
 \end{aligned} \tag{1.5}$$

Υπενθυμίζουμε ότι ο πολλαπλασιασμός των υπερμιγαδικών είναι επιμεριστικός (απευθείας υπολογισμοί), προσεταιριστικός (ο πολλαπλασιασμός είναι διγραμμική απεικόνιση άρα αρκεί να ισχύει $(\alpha\beta)\gamma = \alpha(\beta\gamma)$ για $\alpha, \beta, \gamma \in \{1, i, j, k\}$, κάτι που διαπιστώνεται άμεσα από τον πίνακα πολλαπλασιασμού), αλλά όχι μεταθετικός αφού $k = ij \neq ji = -k$.

Για κάθε υπερμιγαδικό $q = \alpha + \beta i + \gamma j + \delta k$ ορίζουμε:

- το πραγματικό του μέρος $Re(q) = \alpha$.
- το φανταστικό του μέρος $Im(q) = \beta i + \gamma j + \delta k$.
- τον συζυγή του $\bar{q} = \alpha - \beta i - \gamma j - \delta k$.
- τη νόρμα του $N(q) = q\bar{q} = \bar{q}q = \alpha^2 + \beta^2 + \gamma^2 + \delta^2$.

Επίσης με απευθείας υπολογισμούς προκύπτουν οι:

- $Re(q) = \frac{1}{2}(q + \bar{q})$
- $Im(q) = \frac{1}{2}(q - \bar{q})$
- $(\overline{pq}) = \bar{q}\bar{p}$
- $N(q) = 0 \Leftrightarrow q = 0$
- κάθε μη μηδενικός υπερμιγαδικός q έχει μοναδικό αντίστροφο, τον:

$$q^{-1} = \frac{\bar{q}}{N(q)}$$

Αν $q_1, q_2 \in \mathbb{H}$ έχουμε:

$$\begin{aligned} N(q_1 q_2) &= (q_1 q_2)(\overline{q_1 q_2}) = (q_1 q_2)(\overline{q_2} \overline{q_1}) = q_1(q_2 \overline{q_2})\overline{q_1} = q_1 N(q_2) \overline{q_1} = \\ &= q_1 \overline{q_1} N(q_2) = N(q_1) N(q_2) \end{aligned} \quad (1.6)$$

Αν $q_1 = \alpha_1 + \beta_1 i + \gamma_1 j + \delta_1 k$ και $q_2 = \alpha_2 + \beta_2 i + \gamma_2 j + \delta_2 k$ τότε, συνδυάζοντας τον ορισμό της νόρμας των υπερμιγαδικών με τις σχέσεις (1.5) και (1.6) παίρνουμε την ταυτότητα των τεσσάρων τετραγώνων:

$$\begin{aligned} (\alpha_1^2 + \beta_1^2 + \gamma_1^2 + \delta_1^2)(\alpha_2^2 + \beta_2^2 + \gamma_2^2 + \delta_2^2) &= \\ &= (\alpha_1 \alpha_2 - \beta_1 \beta_2 - \gamma_1 \gamma_2 - \delta_1 \delta_2)^2 \\ &+ (\alpha_1 \beta_2 + \beta_1 \alpha_2 + \gamma_1 \delta_2 - \delta_1 \gamma_2)^2 \\ &+ (\alpha_1 \gamma_2 - \beta_1 \delta_2 + \gamma_1 \alpha_2 + \delta_1 \beta_2)^2 \\ &+ (\alpha_1 \delta_2 + \beta_1 \gamma_2 - \gamma_1 \beta_2 + \delta_1 \alpha_2)^2. \end{aligned} \quad (1.7)$$

1.4 Τα οκτόνια ($\mathbb{O}$)

Ιστορική ανασκόπηση

Την επόμενη ημέρα της ανακάλυψής του, ο Hamilton έγραψε μια οκτασέλιδη επιστολή στον παλιό του συμφοιτητή στο Trinity College του Δουβλίνου και φίλο του John T. Graves, περιγράφοντας τις ιδέες του για τους υπερμιγαδικούς. Ο Graves, αν και καθηγητής της νομικής επιστήμης, είχε πάθος με τα μαθηματικά και ήταν το δικό του ερευνητικό ενδιαφέρον που παρακίνησε τον Hamilton να ασχοληθεί με τους μιγαδικούς και τις «τριάδες» (triplets).

Η «επέκταση» του συνόλου των μιγαδικών εντυπωσίασε τον Graves και φυσικά, τουλάχιστον για όποιον έχει πάθος με τα μαθηματικά, τον έκανε να διερωτηθεί αν αυτή η διαδικασία μπορούσε να συνεχιστεί. Στην απάντησή του στις 26 Οκτωβρίου 1843 γράφει: «Υπάρχει κάτι σε αυτό το σύστημα που με απασχολεί. Δεν έχω ακόμη ξεκάθαρη εικόνα για το μέχρι ποιο σημείο έχουμε την ελευθερία να δημιουργούμε αυθαίρετα φανταστικούς και να τους προικίζουμε με υπερφυσικές ιδιότητες.» (Πρωτότυπο κείμενο: «*There is still something in the*

system which gravels me. I have not yet any clear views as to the extent to which we are at liberty arbitrarily to create imaginaries, and to endow them with supernatural properties.»).

Σε άλλο σημείο της επιστολής του έκανε αυτό το ερώτημα πιο συγκεκριμένο: «*Αν με την αλχημεία σου μπορείς να φτιάξεις τρεις λίβρες χρυσό,*» (πιθανόν να εννοούσε τις τρεις φανταστικές μονάδες των υπερμιγαδικών i, j, k) «*γιατί να σταματήσεις εκεί;*», (Πρωτότυπο κείμενο: «*If with your alchemy you can make three pounds of gold, why should you stop there?*»).

Για τους επόμενους δύο μήνες ο Graves ασχολήθηκε με το τελευταίο ερώτημα και στις 26 Δεκεμβρίου 1843, σε επιστολή του προς τον Hamilton, περιέγραψε μια άλγεβρα διάστασης 8 και διατύπωσε, με κάποια λάθη στα πρόσημα, την ταυτότητα των οκτώ τετραγώνων που θα δούμε στο τέλος αυτής της ενότητας. Ονόμασε το σύνολο αυτό «οκτάβες» (octaves).

Τον Ιανουάριο του 1844 ο Graves επανήλθε με τρεις επιστολές στις οποίες διόρθωσε τα λάθη της επιστολής του Δεκεμβρίου, διερεύνει τη δυνατότητα να επεκταθεί αυτή η διαδικασία για τη δημιουργία αλγεβρών διάστασης 2^n και προσπάθησε να κατασκευάσει μια άλγεβρα διαίρεσης με νόρμα διάστασης 16 (σήμερα γνωστή ως sedenions). Όπως ανέφερε όμως σε αυτές τις επιστολές, απρόσμενα εμπόδια τον έκαναν να αμφιβάλλει για το αν ήταν αυτό δυνατό.

Το πιθανότερο είναι ότι ο Graves δεν είχε αντιληφθεί ότι ο πολλαπλασιασμός στις «οκτάβες» του δεν ήταν προσεταιριστικός ή δεν είχε αξιολογήσει ως σημαντική αυτήν την ιδιότητα. Σε επιστολή του ο Hamilton, τον Ιούλιο του 1844 επισημαίνει ότι η ισότητα « $A \cdot BC = AB \cdot C = ABC$ » ενώ ισχύει στους υπερμιγαδικούς, δεν φαίνεται να ισχύει γενικά στις «οκτάβες». Μάλιστα αυτή είναι μια από τις πρώτες χρήσεις του όρου «προσεταιριστικός» (associative) ο οποίος επινοήθηκε από τον Hamilton.

Αν και ο Hamilton προσφέρθηκε να δημοσιεύσει την ανακάλυψη του Graves, απορροφημένος από την ενασχόλησή του με τους υπερμιγαδικούς το ανέβαλε. Τον Μάρτιο του 1845 στο άρθρο του με τίτλο «*On Jacobi's elliptic functions, in reply to the Rev. Brice Bronwin; and on Quaternions*», που δημοσιεύτηκε στο περιοδικό *Philosophical Magazine*, ο Arthur Cayley συμπεριέλαβε ως υστερόγραφο τη σύντομη περιγραφή των οκτονίων που βλέπουμε στην παρακάτω εικόνα.

P.S. On Quaternions.

It is possible to form an analogous theory with seven imaginary roots of (-1) (? with $v=2^n-1$ roots when v is a prime number). Thus if these be $i_1, i_2, i_3, i_4, i_5, i_6, i_7$, which group together according to the types

123, 145, 624, 658, 725, 734, 176,

i. e. the type 123 denotes the system of equations

$$i_1 i_2 = i_3, \quad i_2 i_3 = i_1, \quad i_3 i_1 = i_2$$

$$i_2 i_1 = -i_3, \quad i_3 i_2 = -i_1, \quad i_1 i_3 = -i_2$$

&c. We have the following expression for the product of two factors:

$$\begin{aligned} & (X_0 + X_1 i_1 + \dots + X_7 i_7) (X'_0 + X'_1 i_1 + \dots + X'_7 i_7) \\ &= X_0 X'_0 - X_1 X'_1 - X_2 X'_2 \dots - X_7 X'_7 \\ &+ [\overline{23} + \overline{45} + \overline{76} + (01)] i_1 \quad \text{where } (01) = X_0 X'_1 + X_1 X'_0 \\ &+ [\overline{31} + \overline{46} + \overline{57} + (02)] i_2 \quad : \\ &+ [\overline{12} + \overline{65} + \overline{47} + (03)] i_3 \quad \overline{12} = X_1 X'_2 - X_2 X'_1 \\ &+ [\overline{51} + \overline{62} + \overline{47} + (04)] i_4 \quad \&c. \\ &+ [\overline{14} + \overline{36} + \overline{72} + (05)] i_5 \\ &+ [\overline{24} + \overline{53} + \overline{17} + (06)] i_6 \\ &+ [\overline{25} + \overline{34} + \overline{61} + (07)] i_7 \end{aligned}$$

And the modulus of this expression is the product of the moduli of the factors. The above system of types requires some care in writing down, and not only with respect to the combinations of the letters, but also their order, it would be vitiated, e. g. by writing 716 instead of 176. A theorem analogous to that which I gave before, for quaternions, is the following:— If $\Lambda = 1 + \lambda_1 i_1 \dots + \lambda_7 i_7$, $X = x_1 i_1 \dots + x_7 i_7$. It is immediately shown that the possible part of $\Lambda^{-1} X \Lambda$ vanishes, and that the coefficients of $i_1, \dots, i_7$ are linear functions of $x_1 \dots x_7$. The modulus of the above expression is evidently the modulus of X ; hence “we may determine seven linear functions of $x_1 \dots x_7$, the sum of whose squares is equal to $x_1^2 + \dots + x_7^2$.” The number of arbitrary quantities is however only seven, instead of twenty-one, as it should be.

Εικόνα 1.2: Το άρθρο του Cayley για τα οκτόνια στο Philosophical Magazine

Θορυβημένος από τη δημοσίευση ο Graves, σε δικό του άρθρο στο ίδιο περιοδικό δήλωσε ότι είχε ανακαλύψει πρώτος τα οκτόνια ήδη από τα Χριστούγεννα του 1843. Σε ένα σημείωμά του στο περιοδικό *Transactions of the Royal Irish Academy*, ο Hamilton επιβεβαίωσε τον ισχυρισμό του. Η μαθηματική κοινότητα όμως είχε πια αποδώσει την πατρότητα των οκτονίων στον Cayley σε τέτοιο βαθμό που τα οκτόνια ονομάστηκαν «αριθμοί Cayley» (Cayley Numbers).

Στην εργασία αυτή υιοθετούμε τον όρο «οκτόνια» ως απευθείας απόδοση του καθιερωμένου πια όρου «octonions», αφού η χρήση του όρου «οκτάβες» έχει καθιερωθεί στη μουσική ενώ η

χρήση του όρου «αριθμοί Cayley» θα συνιστούσε αδικία για τον J.T. Graves ο οποίος, διαπιστωμένα, ήταν ο πρώτος που τα ανακάλυψε.

Το σύνολο των οκτονίων έμεινε ουσιαστικά στην αφάνεια για πάνω από 100 χρόνια αφού δεν είχαν καμία ξεκάθαρη εφαρμογή ή υπολογιστική χρησιμότητα στη γεωμετρία ή στη φυσική. Το ενδιαφέρον γι' αυτά αναζωπυρώθηκε όταν έγινε αντιληπτό ότι θα μπορούσαν να χρησιμοποιηθούν στις θεωρίες χορδών στις οποίες έχουν στραφεί πολλοί φυσικοί από τη δεκαετία του 1980.

Τα οκτόνια και οι ιδιότητές τους

Οκτόνιο (octonion) ονομάζεται μια παράσταση της μορφής:

$$\alpha_0 + \alpha_1 e_1 + \alpha_2 e_2 + \alpha_3 e_3 + \alpha_4 e_4 + \alpha_5 e_5 + \alpha_6 e_6 + \alpha_7 e_7, \text{ με } \alpha_i \in \mathbb{R}, i = 0, 1, \dots, 7$$

Η πρόσθεση οκτονίων ορίζεται από τη σχέση:

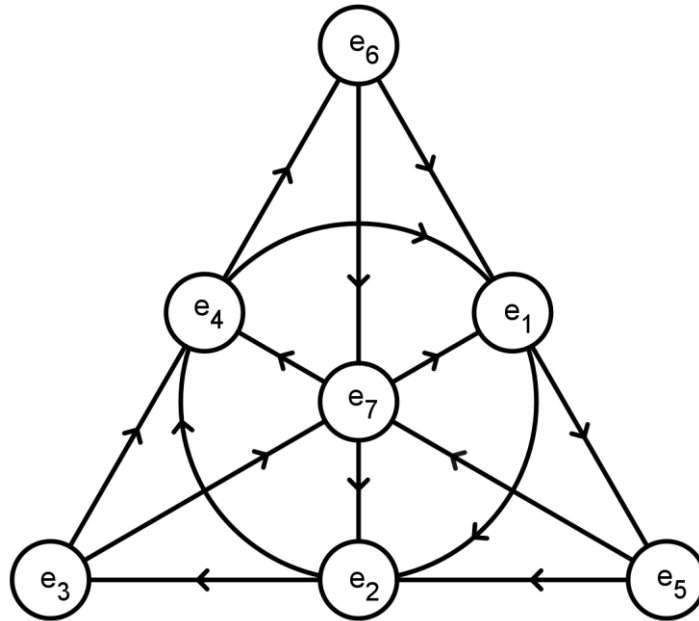
$$\begin{aligned} &(\alpha_0 + \alpha_1 e_1 + \alpha_2 e_2 + \alpha_3 e_3 + \alpha_4 e_4 + \alpha_5 e_5 + \alpha_6 e_6 + \alpha_7 e_7) + \\ &(\beta_0 + \beta_1 e_1 + \beta_2 e_2 + \beta_3 e_3 + \beta_4 e_4 + \beta_5 e_5 + \beta_6 e_6 + \beta_7 e_7) = \\ &(\alpha_0 + \beta_0) + (\alpha_1 + \beta_1)e_1 + (\alpha_2 + \beta_2)e_2 + (\alpha_3 + \beta_3)e_3 + (\alpha_4 + \beta_4)e_4 + (\alpha_5 + \beta_5)e_5 + \\ &+(\alpha_6 + \beta_6)e_6 + (\alpha_7 + \beta_7)e_7. \end{aligned} \quad (1.8)$$

ενώ ο πολλαπλασιασμός οκτονίων ορίζεται από τον παρακάτω πίνακα:

	1	e_1	e_2	e_3	e_4	e_5	e_6	e_7
1	1	e_1	e_2	e_3	e_4	e_5	e_6	e_7
e_1	e_1	-1	e_4	e_7	$-e_2$	e_6	$-e_5$	$-e_3$
e_2	e_2	$-e_4$	-1	e_5	e_1	$-e_3$	e_7	$-e_6$
e_3	e_3	$-e_7$	$-e_5$	-1	e_6	e_2	$-e_4$	e_1
e_4	e_4	e_2	$-e_1$	$-e_6$	-1	e_7	e_3	$-e_5$
e_5	e_5	$-e_6$	e_3	$-e_2$	$-e_7$	-1	e_1	e_4
e_6	e_6	e_5	$-e_7$	e_4	$-e_3$	$-e_1$	-1	e_2
e_7	e_7	e_3	e_6	$-e_1$	e_5	$-e_4$	$-e_2$	-1

Πίνακας 1.2: Πίνακας πολλαπλασιασμού οκτονίων

ή εναλλακτικά από το παρακάτω διάγραμμα Fano:



Εικόνα 1.3: Διάγραμμα Fano για τον πολλαπλασιασμό οκτονίων.

με τους επιπλέον κανόνες:

- το $1 = 1 + 0e_1 + 0e_2 + 0e_3 + 0e_4 + 0e_5 + 0e_6 + 0e_7$ είναι το μοναδιαίο στοιχείο του πολλαπλασιασμού.
- $e_1^2 = e_2^2 = \dots = e_7^2 = -1$

Το διάγραμμα αυτό αποτελείται από 7 «σημεία» τα: $e_1, \dots, e_7$ και 7 «γραμμές» οι οποίες είναι οι πλευρές και τα ύψη του τριγώνου καθώς και ο εγγεγραμμένος κύκλος. Κάθε ζευγάρι διαφορετικών σημείων βρίσκεται σε μοναδική γραμμή. Κάθε γραμμή περιέχει μια τριάδα σημείων. Ο πολλαπλασιασμός δύο σημείων της γραμμής σύμφωνα με τη φορά των βελών έχει ως αποτέλεσμα το επόμενο σημείο (βλέποντάς την κυκλικά), ενώ ο πολλαπλασιασμός με την αντίθετη φορά έχει αποτέλεσμα το αντίθετο του επόμενου σημείου.

Ονομάζοντας τα $e_1, \dots, e_7$ φανταστικές μονάδες των οκτονίων, μπορούμε να βγάλουμε από τα παραπάνω μερικά συμπεράσματα:

- Ο πολλαπλασιασμός των φανταστικών μονάδων e_i και e_j είναι αντισυμμετρικός για $i \neq j$.

$$e_i e_j = -e_j e_i \quad (1.9)$$

- $e_i e_j = e_k \Rightarrow e_{i+1} e_{j+1} = e_{k+1}$ (θεωρούμε ότι $i, j \in \mathbb{Z}_7$)
- $e_i e_j = e_k \Rightarrow e_{2i} e_{2j} = e_{2k}$ (θεωρούμε ότι $i, j \in \mathbb{Z}_7$)
- Ο πολλαπλασιασμός μεταξύ των τριών φανταστικών μονάδων που περιέχονται σε κάθε γραμμή είναι προσεταιριστικός. Μάλιστα, αν e_i, e_j, e_k ανήκουν στην ίδια γραμμή (σύμφωνα με τη φορά των βελών), τότε $e_i e_j e_k = -1$. Έχουμε έτσι 7 τριάδες, τις: $\{e_1, e_2, e_4\}, \{e_1, e_3, e_7\}, \{e_1, e_5, e_6\}, \{e_2, e_3, e_5\}, \{e_2, e_6, e_7\}, \{e_3, e_4, e_6\}, \{e_4, e_5, e_7\}$, οι οποίες «συμπεριφέρονται» όπως ακριβώς η τριάδα $\{i, j, k\}$ του συνόλου των υπερμιγαδικών.

Μπορούμε τώρα να ορίσουμε τον πολλαπλασιασμό των οκτονίων με τη σχέση:

$$\begin{aligned}
 & (\alpha_0 + \alpha_1 e_1 + \alpha_2 e_2 + \alpha_3 e_3 + \alpha_4 e_4 + \alpha_5 e_5 + \alpha_6 e_6 + \alpha_7 e_7) \cdot \\
 & (\beta_0 + \beta_1 e_1 + \beta_2 e_2 + \beta_3 e_3 + \beta_4 e_4 + \beta_5 e_5 + \beta_6 e_6 + \beta_7 e_7) = \\
 & (\alpha_0 \beta_0 - \alpha_1 \beta_1 - \alpha_2 \beta_2 - \alpha_3 \beta_3 - \alpha_4 \beta_4 - \alpha_5 \beta_5 - \alpha_6 \beta_6 - \alpha_7 \beta_7) + \\
 & (\alpha_0 \beta_1 + \alpha_1 \beta_0 + \alpha_2 \beta_4 + \alpha_3 \beta_7 - \alpha_4 \beta_2 + \alpha_5 \beta_6 - \alpha_6 \beta_5 - \alpha_7 \beta_3) e_1 + \\
 & (\alpha_0 \beta_2 - \alpha_1 \beta_4 + \alpha_2 \beta_0 + \alpha_3 \beta_5 + \alpha_4 \beta_1 - \alpha_5 \beta_3 + \alpha_6 \beta_7 - \alpha_7 \beta_6) e_2 + \\
 & (\alpha_0 \beta_3 - \alpha_1 \beta_7 - \alpha_2 \beta_5 + \alpha_3 \beta_0 + \alpha_4 \beta_6 + \alpha_5 \beta_2 - \alpha_6 \beta_4 + \alpha_7 \beta_1) e_3 + \\
 & (\alpha_0 \beta_4 + \alpha_1 \beta_2 - \alpha_2 \beta_1 - \alpha_3 \beta_6 + \alpha_4 \beta_0 + \alpha_5 \beta_7 + \alpha_6 \beta_3 - \alpha_7 \beta_5) e_4 + \\
 & (\alpha_0 \beta_5 - \alpha_1 \beta_6 + \alpha_2 \beta_3 - \alpha_3 \beta_2 - \alpha_4 \beta_7 + \alpha_5 \beta_0 + \alpha_6 \beta_1 + \alpha_7 \beta_4) e_5 + \\
 & (\alpha_0 \beta_6 + \alpha_1 \beta_5 - \alpha_2 \beta_7 + \alpha_3 \beta_4 - \alpha_4 \beta_3 - \alpha_5 \beta_1 + \alpha_6 \beta_0 + \alpha_7 \beta_2) e_6 + \\
 & (\alpha_0 \beta_7 + \alpha_1 \beta_3 + \alpha_2 \beta_6 - \alpha_3 \beta_1 + \alpha_4 \beta_5 - \alpha_5 \beta_4 - \alpha_6 \beta_2 + \alpha_7 \beta_0) e_7 \quad (1.10)
 \end{aligned}$$

Η (1.9) μας δείχνει ότι ο πολλαπλασιασμός των οκτονίων δεν είναι μεταθετικός. Επίσης βλέπουμε ότι δεν είναι προσεταιριστικός αφού, για παράδειγμα:

$$(e_1 e_2) e_3 = e_4 e_3 = -e_6 \quad \text{ενώ} \quad e_1 (e_2 e_3) = e_1 e_5 = e_6.$$

Τέλος, ο πολλαπλασιασμός οκτονίων είναι επιμεριστικός ως προς την πρόσθεση από αριστερά και από δεξιά δηλαδή αν $x, y, z \in \mathbb{O}$ τότε:

$$x(y + z) = xy + xz \quad \text{και} \quad (x + y)z = xz + yz$$

Για κάθε οκτόνιο $x = \alpha_0 + \alpha_1 e_1 + \alpha_2 e_2 + \alpha_3 e_3 + \alpha_4 e_4 + \alpha_5 e_5 + \alpha_6 e_6 + \alpha_7 e_7$ ορίζουμε:

- το πραγματικό του μέρος $Re(x) = \alpha_0$.
- το φανταστικό του μέρος $Im(x) = \alpha_1 e_1 + \alpha_2 e_2 + \alpha_3 e_3 + \alpha_4 e_4 + \alpha_5 e_5 + \alpha_6 e_6 + \alpha_7 e_7$.
- τον συζυγή του $\bar{x} = \alpha_0 - \alpha_1 e_1 - \alpha_2 e_2 - \alpha_3 e_3 - \alpha_4 e_4 - \alpha_5 e_5 - \alpha_6 e_6 - \alpha_7 e_7$.
- τη νόρμα του $N(x) = \alpha_0^2 + \alpha_1^2 + \alpha_2^2 + \alpha_3^2 + \alpha_4^2 + \alpha_5^2 + \alpha_6^2 + \alpha_7^2$.

Με απευθείας υπολογισμούς προκύπτουν οι:

- $Re(x) = \frac{1}{2}(x + \bar{x})$
- $Im(x) = \frac{1}{2}(x - \bar{x})$
- $x\bar{x} = \bar{x}x$, και $N(x) = x\bar{x} = \bar{x}x$

Απόδειξη

$$x = Re(x) + Im(x), \quad \bar{x} = Re(x) - Im(x)$$

$$x\bar{x} = (Re(x) + Im(x))(Re(x) - Im(x))$$

$$= Re^2(x) - Re(x)Im(x) + Im(x)Re(x) - Im(x)Im(x)$$

$$= Re^2(x) - Im(x)Im(x) \quad (\text{αφού } Re(x) \in \mathbb{R} \text{ άρα } Re(x)Im(x) = Im(x)Re(x))$$

$$\bar{x}x = (Re(x) - Im(x))(Re(x) + Im(x)) =$$

$$= Re^2(x) + Re(x)Im(x) - Im(x)Re(x) - Im(x)Im(x)$$

$$= Re^2(x) - Im(x)Im(x)$$

Όμως

$$\begin{aligned} Im(x)Im(x) &= \sum_{i=1}^7 \alpha_i e_i \cdot \sum_{j=1}^7 \alpha_j e_j = \sum_{i=1}^7 \alpha_i^2 e_i^2 + \sum_{1 \leq i < j \leq 7} (\alpha_i \alpha_j e_i e_j + \alpha_j \alpha_i e_j e_i) \\ &= \sum_{i=1}^7 \alpha_i^2 e_i^2 + \sum_{1 \leq i < j \leq 7} \alpha_i \alpha_j (e_i e_j + e_j e_i) \end{aligned}$$

Από την αντισυμμετρικότητα του πολλαπλασιασμού των φανταστικών μονάδων έχουμε ότι το δεύτερο άθροισμα είναι 0 επομένως:

$$Im(x)Im(x) = \sum_{i=1}^7 \alpha_i^2 e_i^2 = - \sum_{i=1}^7 \alpha_i^2 \in \mathbb{R}$$

και

$$x\bar{x} = \bar{x}x = Re^2(x) - Im(x)Im(x) = Re^2(x) + \sum_{i=1}^7 \alpha_i^2 = N(x).$$

■

- Αν $x, y \in \mathbb{O}$ τότε, $(\overline{xy}) = \bar{y}\bar{x}$
- $N(x) = 0 \Leftrightarrow x = 0$
- κάθε μη μηδενικό οκτόνιο x έχει μοναδικό αντίστροφο, τον:

$$x^{-1} = \frac{\bar{x}}{N(x)}$$

Απλοί (αλλά μακροσκελείς) αλγεβρικοί υπολογισμοί μας δίνουν την ταυτότητα των οκτώ τετραγώνων. Όπως είδαμε, η ταυτότητα αυτή περιλαμβανόταν στις επιστολές του Graves προς τον Hamilton, περιγράφεται στο άρθρο του Cayley της εικόνας 1.2, αλλά ο πρώτος που την απέδειξε ήταν ο Δανός μαθηματικός C.F. Degen το 1818 και είναι η παρακάτω:

$$\begin{aligned} &(\alpha_0^2 + \alpha_1^2 + \alpha_2^2 + \alpha_3^2 + \alpha_4^2 + \alpha_5^2 + \alpha_6^2 + \alpha_7^2) \cdot (\beta_0^2 + \beta_1^2 + \beta_2^2 + \beta_3^2 + \beta_4^2 + \beta_5^2 + \beta_6^2 + \beta_7^2) = \\ &(\alpha_0\beta_0 - \alpha_1\beta_1 - \alpha_2\beta_2 - \alpha_3\beta_3 - \alpha_4\beta_4 - \alpha_5\beta_5 - \alpha_6\beta_6 - \alpha_7\beta_7)^2 + \\ &(\alpha_0\beta_1 + \alpha_1\beta_0 + \alpha_2\beta_4 + \alpha_3\beta_7 - \alpha_4\beta_2 + \alpha_5\beta_6 - \alpha_6\beta_5 - \alpha_7\beta_3)^2 + \end{aligned}$$

$$\begin{aligned}
& (\alpha_0\beta_2 - \alpha_1\beta_4 + \alpha_2\beta_0 + \alpha_3\beta_5 + \alpha_4\beta_1 - \alpha_5\beta_3 + \alpha_6\beta_7 - \alpha_7\beta_6)^2 + \\
& (\alpha_0\beta_3 - \alpha_1\beta_7 - \alpha_2\beta_5 + \alpha_3\beta_0 + \alpha_4\beta_6 + \alpha_5\beta_2 - \alpha_6\beta_4 + \alpha_7\beta_1)^2 + \\
& (\alpha_0\beta_4 + \alpha_1\beta_2 - \alpha_2\beta_1 - \alpha_3\beta_6 + \alpha_4\beta_0 + \alpha_5\beta_7 + \alpha_6\beta_3 - \alpha_7\beta_5)^2 + \\
& (\alpha_0\beta_5 - \alpha_1\beta_6 + \alpha_2\beta_3 - \alpha_3\beta_2 - \alpha_4\beta_7 + \alpha_5\beta_0 + \alpha_6\beta_1 + \alpha_7\beta_4)^2 + \\
& (\alpha_0\beta_6 + \alpha_1\beta_5 - \alpha_2\beta_7 + \alpha_3\beta_4 - \alpha_4\beta_3 - \alpha_5\beta_1 + \alpha_6\beta_0 + \alpha_7\beta_2)^2 + \\
& (\alpha_0\beta_7 + \alpha_1\beta_3 + \alpha_2\beta_6 - \alpha_3\beta_1 + \alpha_4\beta_5 - \alpha_5\beta_4 - \alpha_6\beta_2 + \alpha_7\beta_0)^2 \quad (1.11)
\end{aligned}$$

Ο ορισμός του πολλαπλασιασμού οκτονίων που δώσαμε στην (1.10) και η ταυτότητα των οκτώ τετραγώνων, μας δείχνουν ότι η νόρμα που ορίσαμε για τα οκτόνια είναι επίσης πολλαπλασιαστική, δηλαδή:

Αν $x, y \in \mathbb{O}$ και $x = \alpha_0 + \alpha_1 e_1 + \alpha_2 e_2 + \alpha_3 e_3 + \alpha_4 e_4 + \alpha_5 e_5 + \alpha_6 e_6 + \alpha_7 e_7$,

$y = \beta_0 + \beta_1 e_1 + \beta_2 e_2 + \beta_3 e_3 + \beta_4 e_4 + \beta_5 e_5 + \beta_6 e_6 + \beta_7 e_7$, τότε ισχύει:

$$N(xy) = N(x)N(y). \quad (1.12)$$

Σε αυτό το σημείο να σημειώσουμε ότι, σε αντίθεση με τους μιγαδικούς και τους υπερμιγαδικούς, δεν υπάρχει μέχρι σήμερα στη βιβλιογραφία κοινός συμβολισμός για τις φανταστικές μονάδες των οκτονίων. Στην ενότητα αυτή υιοθετήσαμε τον συμβολισμό και τον πίνακα πολλαπλασιασμού από τον Baez J. (2001), από το άρθρο του οποίου αντλήσαμε και τα περισσότερα από τα στοιχεία που δώσαμε στην ιστορική ανασκόπηση.

Κεφάλαιο 2. Composition άλγεβρες – Θεώρημα Hurwitz – Ιδιότητες των οκτονίων

2.1 Βασικοί ορισμοί και προτάσεις

Ο τρόπος με τον οποίο κατασκευάσαμε τα σύνολα $\mathbb{C}, \mathbb{H}, \mathbb{O}$ στην προηγούμενη ενότητα, περιγράφει τη δομή τους και τις βασικές τους ιδιότητες. Ειδικά όμως για το σύνολο των οκτονίων η υπολογιστική πολυπλοκότητα της πράξης του πολλαπλασιασμού κάνει δύσκολη τη διερεύνηση των ιδιοτήτων του. Ένας πιο συστηματικός τρόπος κατασκευής των συνόλων αυτών είναι η μέθοδος των Cayley–Dickson. Πριν την παρουσιάσουμε όμως θα πρέπει να δούμε αυτά τα σύνολα από διαφορετική οπτική γωνία.

Δίνουμε πρώτα τους απαραίτητους ορισμούς και προτάσεις.

Ορισμός 2.1. Ονομάζουμε F -άλγεβρα A ένα διανυσματικό χώρο επί ενός σώματος F , εφοδιασμένο με μια διγραμμική απεικόνιση: $m: A \times A \rightarrow A$,

δηλαδή μια απεικόνιση για την οποία, για κάθε $x, y, z \in A$ και για κάθε $\alpha, \beta \in F$, ισχύουν:

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

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

Θα ονομάζουμε την απεικόνιση m «πολλαπλασιασμό» και θα συμβολίζουμε:

$$m(x, y) = xy.$$

Σημειώνουμε ότι ο πολλαπλασιασμός που ορίσαμε δεν είναι απαραίτητα μεταθετικός ή προσεταιριστικός.

Διάσταση της F -άλγεβρας A θα ονομάζουμε τη διάσταση του διανυσματικού χώρου επί του σώματος F .

Ένα στοιχείο $e \in A$ θα ονομάζεται **μοναδιαίο στοιχείο** της F -άλγεβρας A , αν για κάθε $x \in A$ ισχύει:

$$ex = xe = x.$$

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

Ορισμός 2.2. Ονομάζουμε *άλγεβρα διαίρεσης* μια F -άλγεβρα A όταν για κάθε μη-μηδενικό $\alpha \in A$ οι εξισώσεις:

$$x\alpha = \beta \text{ και } \alpha y = \beta \text{ έχουν μοναδική λύση για κάθε } \beta \in A.$$

Ορισμός 2.3. Ονομάζουμε *composition άλγεβρα* μια F -άλγεβρα $A \neq \{0\}$, εφοδιασμένη με μια μη-εκφυλισμένη τετραγωνική μορφή $N: A \rightarrow F$, (θα την αποκαλούμε *νόρμα*) όταν:

1. η A περιέχει μοναδιαίο στοιχείο,
2. για κάθε $x, y \in A$ ισχύει $N(xy) = N(x)N(y)$.

Ένας μη εκφυλισμένος υπόχωρος της *composition άλγεβρας* A , είναι *υποάλγεβρα της A* όταν περιέχει το μοναδιαίο στοιχείο της A και είναι κλειστός ως προς τον πολλαπλασιασμό της.

Στο εξής θα ασχοληθούμε μόνο με *composition άλγεβρες* επί του $\mathbb{R}$, θα χρησιμοποιούμε τον όρο «άλγεβρα» αντί του « $\mathbb{R}$ -άλγεβρα» και θα συμβολίζουμε το μοναδιαίο στοιχείο με «1».

Δίνουμε παρακάτω μερικούς ορισμούς και προτάσεις που θα μας χρειαστούν για τη μέθοδο διπλασιασμού των Cayley–Dickson ακολουθώντας την προσέγγιση των Conway J. & Smith D. (2003). Σημειώνουμε ότι οι συγγραφείς αναφέρονται στη διαδικασία ως «διπλασιασμός Dickson», αναγνωρίζοντας στον Dickson την πατρότητα της διαδικασίας.

Ορισμός 2.4. Σε μια *composition άλγεβρα* A με νόρμα N , θα ονομάζουμε *εσωτερικό γινόμενο*, τη συσχετισμένη με τη νόρμα συμμετρική διγραμμική μορφή:

$$\langle x, y \rangle = \frac{N(x + y) - N(x) - N(y)}{2} \in \mathbb{R}, \quad \text{για κάθε } x, y \in A.$$

Από τον παραπάνω ορισμό προκύπτουν οι σχέσεις:

$$N(x + y) = N(x) + N(y) + 2\langle x, y \rangle \quad (2.1)$$

$$\langle x, x \rangle = N(x) \quad (2.2)$$

Πρόταση 2.5. Το $\mathbb{R}$ είναι μια *composition άλγεβρα* με τετραγωνική μορφή (νόρμα):

$$N: \mathbb{R} \rightarrow \mathbb{R}, \quad x \mapsto x^2.$$

Απόδειξη

Θα δείξουμε πρώτα ότι η νόρμα είναι μη-εκφυλισμένη.

Θεωρούμε την αντίστοιχη της νόρμας διγραμμική μορφή $\langle \cdot \rangle: \mathbb{R} \times \mathbb{R} \rightarrow \mathbb{R}$ με:

$$\langle x, y \rangle = \frac{N(x+y) - N(x) - N(y)}{2}$$

Έστω ότι για κάθε $y \in \mathbb{R}$ ισχύει, $\langle x, y \rangle = 0$. Τότε:

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

Υπάρχει μοναδιαίο στοιχείο αφού, για κάθε $x \in \mathbb{R}$, $1x = x1 = x$.

Τέλος, για κάθε $x, y \in \mathbb{R}$:

$$N(xy) = (xy)^2 = x^2y^2 = N(x)N(y). \quad \blacksquare$$

Θα αποδείξουμε στη συνέχεια μερικές προτάσεις για τις *composition άλγεβρες*, οι οποίες πηγάζουν από την πολλαπλασιαστική ιδιότητα της νόρμας:

$$N(xy) = N(x)N(y) \quad (2.3)$$

Έστω A μια *composition άλγεβρα* με νόρμα N .

Λήμμα 2.6. Για κάθε $x, y, z \in A$ ισχύει:

$$\langle xy, xz \rangle = N(x)\langle y, z \rangle \text{ και } \langle xz, yz \rangle = N(z)\langle x, y \rangle \quad (2.4)$$

Απόδειξη

Αντικαθιστώντας στην (2.3) το y με $y+z$ και χρησιμοποιώντας την (2.1) έχουμε:

$$N(x(y+z)) = N(xy+xz) \Rightarrow$$

$$N(x)N(y+z) = N(xy) + N(xz) + 2\langle xy, xz \rangle \Rightarrow$$

$$N(x)(N(y) + N(z) + 2\langle y, z \rangle) = N(xy) + N(xz) + 2\langle xy, xz \rangle \Rightarrow$$

$$N(x)N(y) + N(x)N(z) + 2N(x)\langle y, z \rangle = N(xy) + N(xz) + 2\langle xy, xz \rangle \Rightarrow$$

$$N(x)\langle y, z \rangle = \langle xy, xz \rangle.$$

Με τον ίδιο τρόπο αποδεικνύεται και η δεύτερη σχέση. ■

Λήμμα 2.7. Για κάθε $x, y, u, z \in A$ ισχύει:

$$\langle xy, uz \rangle = 2\langle x, u \rangle \langle y, z \rangle - \langle xz, uy \rangle \quad (2.5)$$

Απόδειξη

Αντικαθιστώντας στην (2.4) το x με $x + u$, παίρνουμε:

$$\langle (x + u)y, (x + u)z \rangle = N(x + u)\langle y, z \rangle \Rightarrow$$

$$\langle xy + uy, xz + uz \rangle = (N(x) + N(u) + 2\langle x, u \rangle)\langle y, z \rangle \Rightarrow$$

$$\langle xy, xz \rangle + \langle xy, uz \rangle + \langle uy, xz \rangle + \langle uy, uz \rangle = (N(x) + N(u) + 2\langle x, u \rangle)\langle y, z \rangle \stackrel{(2.4)}{\Rightarrow}$$

$$N(x)\langle y, z \rangle + \langle xy, uz \rangle + \langle uy, xz \rangle + N(u)\langle y, z \rangle = N(x)\langle y, z \rangle + N(u)\langle y, z \rangle + 2\langle x, u \rangle \langle y, z \rangle \Rightarrow$$

$$\langle xy, uz \rangle = 2\langle x, u \rangle \langle y, z \rangle - \langle uy, xz \rangle \Rightarrow$$

$$\langle xy, uz \rangle = 2\langle x, u \rangle \langle y, z \rangle - \langle xz, uy \rangle. \quad \blacksquare$$

Ορισμός 2.8. Σε μια *composition άλγεβρα* A με νόρμα N , θα ονομάζουμε **συζυγές στοιχείο** του $x \in A$, το:

$$\bar{x} = 2\langle x, 1 \rangle - x \in A.$$

Παρατηρούμε ότι, αν $x \in \mathbb{R}$, τότε:

$$\bar{x} = 2\langle x, 1 \rangle - x = N(x + 1) - N(x) - N(1) - x = x^2 + 2x + 1 - x^2 - 1 - x = x.$$

Πρόταση 2.9. Για κάθε $x, y, z \in A$ ισχύει:

$$\langle xy, z \rangle = \langle y, \bar{x}z \rangle \quad \text{και} \quad \langle xy, z \rangle = \langle x, z\bar{y} \rangle \quad (2.6)$$

Απόδειξη

Θέτοντας στην (2.5) $u = 1$, παίρνουμε:

$$\langle xy, z \rangle = 2\langle x, 1 \rangle \langle y, z \rangle - \langle xz, y \rangle \quad (*)$$

Έχουμε:

$$\begin{aligned}\langle y, \bar{x}z \rangle &= \langle y, (2\langle x, 1 \rangle - x)z \rangle = \langle y, 2\langle x, 1 \rangle z - xz \rangle = \langle y, 2\langle x, 1 \rangle z \rangle - \langle y, xz \rangle \\ &= 2\langle x, 1 \rangle \langle y, z \rangle - \langle y, xz \rangle = 2\langle x, 1 \rangle \langle y, z \rangle - \langle xz, y \rangle \stackrel{(*)}{\Rightarrow} \langle y, \bar{x}z \rangle = \langle xy, z \rangle\end{aligned}$$

Η δεύτερη σχέση αποδεικνύεται ομοίως. ■

Λήμμα 2.10. Για $x, y \in A$ ισχύει:

$$\langle x, z \rangle = \langle y, z \rangle, \text{ για κάθε } z \in A \Rightarrow x = y \quad (2.7)$$

Απόδειξη

$$\langle x, z \rangle = \langle y, z \rangle, \text{ για κάθε } z \in A \Rightarrow$$

$$\langle x, z \rangle - \langle y, z \rangle = 0, \text{ για κάθε } z \in A \Rightarrow$$

$$\langle x - y, z \rangle = 0, \text{ για κάθε } z \in A$$

Επειδή η νόρμα της A είναι μη εκφυλισμένη η τελευταία σχέση σημαίνει ότι:

$$x - y = 0 \Rightarrow x = y. \quad \blacksquare$$

Πρόταση 2.11. Για κάθε $x \in A$ ισχύει:

$$\bar{\bar{x}} = x \quad (2.8)$$

Απόδειξη

Θέτοντας στην (2.6) $y = 1$, παίρνουμε:

$$\langle x, z \rangle = \langle x1, z \rangle = \langle 1, \bar{x}z \rangle = \langle \bar{x}z, 1 \rangle = \langle z, \bar{\bar{x}}1 \rangle = \langle \bar{\bar{x}}, z \rangle, \text{ για κάθε } z \in A.$$

Επομένως, από την (2.7), $\bar{\bar{x}} = x$. ■

Πρόταση 2.12. Για κάθε $x, y \in A$ ισχύει:

$$\overline{xy} = \bar{y}\bar{x} \quad (2.9)$$

Απόδειξη

Εφαρμόζοντας τις (2.6) και την (2.8), παίρνουμε:

$$\begin{aligned} \langle \bar{y}\bar{x}, z \rangle &= \langle \bar{x}, \bar{y}z \rangle = \langle \bar{x}, yz \rangle = \langle yz, \bar{x} \rangle = \langle y, \bar{x}\bar{z} \rangle = \langle \bar{x}\bar{z}, y \rangle = \langle \bar{z}, \bar{x}y \rangle = \langle \bar{z}, xy \rangle = \\ &= \langle (xy)1, \bar{z} \rangle = \langle 1, (\overline{xy})\bar{z} \rangle = \langle (\overline{xy})\bar{z}, 1 \rangle = \langle \overline{xy}, 1\bar{z} \rangle = \langle \overline{xy}, z \rangle, \text{ για κάθε } z \in A. \end{aligned}$$

Από την (2.7) λοιπόν έχουμε ότι $\overline{xy} = \bar{y}\bar{x}$. ■

2.2 Η μέθοδος διπλασιασμού Cayley–Dickson

Είμαστε τώρα έτοιμοι να δώσουμε τους κανόνες που διέπουν τη μέθοδο διπλασιασμού Cayley–Dickson.

Έστω μια *composition άλγεβρα* A με μοναδιαίο στοιχείο 1 και μια τετραγωνική μορφή N ως νόρμα. Η τετραγωνική νόρμα και η ύπαρξη μοναδιαίου στοιχείου μας επιτρέπουν να ορίσουμε εσωτερικό γινόμενο όπως στον Ορισμό 2.4 και συζυγή όπως στον Ορισμό 2.8.

Ορίζουμε πρώτα την ορθογωνιότητα στην A .

Ορισμός 2.13. Τα στοιχεία $x, y \in A$ θα ονομάζονται **κάθετα** όταν $\langle x, y \rangle = 0$. Αν H είναι μια υποάλγεβρα της A , θα λέμε ότι το $x \in A$ είναι **κάθετο στην H** όταν $\langle x, y \rangle = 0$, για κάθε $y \in H$.

Θεωρούμε τώρα μια υποάλγεβρα H διάστασης n , η οποία περιέχει το 1 και ένα μοναδιαίο διάνυσμα i ($N(i) = 1$), κάθετο στην H .

Τότε ισχύουν οι σχέσεις: $\bar{i} = 2\langle i, 1 \rangle - i = -i$, αφού $\langle i, 1 \rangle = 0$ και

$$\langle i, x \rangle = 0, \text{ για κάθε } x \in H.$$

Τότε το σύνολο $B = H + iH$ είναι επίσης μια άλγεβρα με στοιχεία:

$$(\alpha, \beta) = \alpha + i\beta, \quad \alpha, \beta \in H.$$

Την άλγεβρα B θα την ονομάζουμε στο εξής «**διπλασιασμό Dickson της H** ».

Οι επόμενες τρεις σχέσεις ορίζουν το εσωτερικό γινόμενο, τον συζυγή και τον πολλαπλασιασμό στη B με όρους της H .

Πρόταση 2.14. Για κάθε $\alpha, \beta, \gamma, \delta \in H$ ισχύει:

$$\langle \alpha + i\beta, \gamma + i\delta \rangle = \langle \alpha, \gamma \rangle + \langle \beta, \delta \rangle \quad (2.10)$$

Απόδειξη

$$\langle \alpha + i\beta, \gamma + i\delta \rangle = \langle \alpha, \gamma \rangle + \langle \alpha, i\delta \rangle + \langle i\beta, \gamma \rangle + \langle i\beta, i\delta \rangle$$

Όμως,

$$\langle \alpha, i\delta \rangle = \langle i\delta, \alpha \rangle = \langle i, \alpha\bar{\delta} \rangle = 0, \text{ αφού } \alpha\bar{\delta} \in H.$$

$$\langle i\beta, \gamma \rangle = \langle i, \gamma\bar{\beta} \rangle = 0, \text{ αφού } \gamma\bar{\beta} \in H.$$

$$\langle i\beta, i\delta \rangle = N(i)\langle \beta, \delta \rangle = \langle \beta, \delta \rangle \text{ αφού } i \text{ μοναδιαίο.}$$

Επομένως,

$$\langle \alpha + i\beta, \gamma + i\delta \rangle = \langle \alpha, \gamma \rangle + \langle \beta, \delta \rangle. \quad \blacksquare$$

Όπως θα δείξουμε στην ενότητα 2.4, η απαίτηση $N(i) = 1$ σημαίνει ότι, αν η νόρμα της H είναι θετικά ορισμένη τότε ισχύει το ίδιο και για τη νόρμα της B . Στις άλγεβρες λοιπόν που θα μας απασχολήσουν, ξεκινώντας από το $\mathbb{R}$ το οποίο έχει θετικά ορισμένη νόρμα, θα παίρνουμε άλγεβρες με την ίδια ιδιότητα.

Πρόταση 2.15. Για κάθε $\alpha, \beta \in H$ ισχύει:

$$\overline{\alpha + i\beta} = \bar{\alpha} - i\beta \quad (\text{συνεπώς για } \alpha = 0, i\beta = -i\bar{\beta} = -\bar{\beta}i = \bar{\beta}i) \quad (2.11)$$

Απόδειξη

$$\begin{aligned} \overline{\alpha + i\beta} &= 2\langle \alpha + i\beta, 1 \rangle - (\alpha + i\beta) = 2\langle \alpha, 1 \rangle + 2\langle i\beta, 1 \rangle - \alpha - i\beta \\ &= 2\langle \alpha, 1 \rangle - \alpha - i\beta = \bar{\alpha} - i\beta. \quad \blacksquare \end{aligned}$$

Πρόταση 2.16. Για κάθε $\alpha, \beta, \gamma, \delta \in H$ ισχύει:

$$(\alpha + i\beta)(\gamma + i\delta) = (\alpha\gamma - \delta\bar{\beta}) + i(\gamma\beta + \bar{\alpha}\delta) \quad (2.12)$$

Απόδειξη

$$(\alpha + i\beta)(\gamma + i\delta) = \alpha\gamma + \alpha(i\delta) + (i\beta)\gamma + (i\beta)(i\delta)$$

Όμως για κάθε $z \in B$ έχουμε:

$$\langle \alpha(i\delta), z \rangle = \langle i\delta, \bar{\alpha}z \rangle = 2\langle i, \bar{\alpha} \rangle \langle \delta, z \rangle - \langle iz, \bar{\alpha}\delta \rangle = -\langle iz, \bar{\alpha}\delta \rangle = -\langle z, \bar{i}(\bar{\alpha}\delta) \rangle = \langle z, i(\bar{\alpha}\delta) \rangle$$

Επομένως, $\alpha(i\delta) = i(\bar{\alpha}\delta)$.

Επίσης, από την (2.11) για $\alpha = 0$ παίρνουμε $i\beta = -\bar{i}\bar{\beta} = -\bar{\beta}i = \bar{\beta}i$, για κάθε $\beta \in H$ και για κάθε $z \in B$ έχουμε:

$$\begin{aligned} \langle (i\beta)\gamma, z \rangle &= \langle i\beta, z\bar{\gamma} \rangle = \langle \bar{\beta}i, z\bar{\gamma} \rangle = 2\langle \bar{\beta}, z \rangle \langle i, \bar{\gamma} \rangle - \langle \bar{\beta}\bar{\gamma}, zi \rangle = -\langle \bar{\beta}\bar{\gamma}, zi \rangle = -\langle zi, \bar{\beta}\bar{\gamma} \rangle \\ &= -\langle z, (\bar{\beta}\bar{\gamma})\bar{i} \rangle = \langle (\bar{\beta}\bar{\gamma})i, z \rangle = \langle (\bar{\gamma}\beta)i, z \rangle = \langle i(\gamma\beta), z \rangle \end{aligned}$$

Επομένως, $(i\beta)\gamma = i(\gamma\beta)$.

Τέλος, για κάθε $z \in B$ έχουμε:

$$\begin{aligned} \langle (i\beta)(i\delta), z \rangle &= \langle i\beta, z(i\delta) \rangle = -\langle i\beta, z(i\delta) \rangle = -\langle z(i\delta), i\beta \rangle = -2\langle z, i \rangle \langle i\delta, \beta \rangle + \langle z\beta, i(i\delta) \rangle \\ &= -2\langle z, i \rangle \langle i, \beta\bar{\delta} \rangle + \langle z\beta, i(i\delta) \rangle = \langle i(i\delta), z\beta \rangle = \langle i\delta, \bar{i}(z\beta) \rangle = -\langle i\delta, i(z\beta) \rangle \\ &= -N(i)\langle \delta, z\beta \rangle = -\langle z\beta, \delta \rangle = -\langle z, \delta\bar{\beta} \rangle = \langle -\delta\bar{\beta}, z \rangle \end{aligned}$$

Επομένως, $(i\beta)(i\delta) = -\delta\bar{\beta}$.

Από τις παραπάνω παίρνουμε:

$$(\alpha + i\beta)(\gamma + i\delta) = \alpha\gamma + i(\bar{\alpha}\delta) + i(\gamma\beta) - \delta\bar{\beta} = (\alpha\gamma - \delta\bar{\beta}) + i(\gamma\beta + \bar{\alpha}\delta). \quad \blacksquare$$

Είναι εύκολο να δούμε ότι, αν $\dim(H) = n$, τότε $\dim(B) = 2n$ (επί του $\mathbb{R}$).

Πράγματι, αν $\{1, e_1, \dots, e_{n-1}\}$ είναι μια βάση της H , τότε η $\{1, e_1, \dots, e_{n-1}, i, ie_1, \dots, ie_{n-1}\}$ είναι μια βάση της B , αφού:

$$\langle ie_k, e_j \rangle = \langle i, e_j \overline{e_k} \rangle = 0, \quad j, k = 1, \dots, n-1 \quad \text{και}$$

$$\langle ie_k, ie_j \rangle = N(i) \langle e_k, e_j \rangle = \langle e_k, e_j \rangle = 0, \quad \text{για } j \neq k$$

Η διγραμμική σχέση που αποκαλούσαμε στα παραπάνω «εσωτερικό γινόμενο» έχει τις ιδιότητες:

$$\langle x, x \rangle \geq 0 \quad \text{και} \quad \langle x, x \rangle = 0 \Leftrightarrow x = 0$$

για κάθε x που ανήκει σε μια από τις πραγματικές άλγεβρες που κατασκευάσαμε με τον διπλασιασμό Cayley–Dickson (όπως τον δώσαμε στα προηγούμενα). Επομένως, αν δούμε τις παραπάνω άλγεβρες σαν διανυσματικούς χώρους, αυτοί είναι Ευκλείδειοι.

Αυτό σημαίνει ότι, αν μια άλγεβρα Γ με πεπερασμένη διάσταση, περιέχει μια γνήσια υποάλγεβρα B τότε ισχύει $\Gamma = B \oplus B^\perp$, με $B^\perp \neq \{0\}$.

Επομένως η Γ περιέχει διάνυσμα κάθετο στη B , το οποίο μπορούμε να θεωρήσουμε ότι έχει νόρμα ίση με 1 (αλλιώς μπορούμε να το κανονικοποιήσουμε).

Τα παραπάνω δείχνουν ότι, αν μια *composition* άλγεβρα Γ περιέχει μια γνήσια υποάλγεβρα B , τότε θα περιέχει (ή, στην περίπτωση που η B δεν περιέχεται σε άλλη γνήσια υποάλγεβρα, θα είναι ίση με) τον διπλασιασμό Dickson της B .

Μια πεπερασμένης διάστασης *composition* άλγεβρα A επί του $\mathbb{R}$, όπως αυτές που μελετάμε, αν δεν είναι το σύνολο $\mathbb{R}$, περιέχει μια υποάλγεβρα A_1 , η οποία με τη σειρά της μπορεί να περιέχει μια υποάλγεβρα A_2 , διαδικασία που συνεχίζεται ώσπου να καταλήξει στη μικρότερη υποάλγεβρα, το $\mathbb{R}$.

Αυτό σημαίνει ότι οι πεπερασμένης διάστασης *composition* άλγεβρες έχουν διάσταση 2^n , $n = 0, 1, 2, \dots$

2.3 Το Θεώρημα Hurwitz

Το συμπέρασμα της προηγούμενης υποενότητας είναι ότι, κάθε πεπερασμένης διάστασης *composition* άλγεβρα επί του $\mathbb{R}$ δημιουργείται ξεκινώντας από το $\mathbb{R}$ και εφαρμόζοντας επανειλημμένα τον διπλασιασμό Cayley–Dickson.

Το ερώτημα που ανακύπτει άμεσα είναι: «πόσες φορές μπορούμε να επαναλάβουμε το βήμα, ώστε ο διπλασιασμός να έχει ως αποτέλεσμα μια composition άλγεβρα;».

Η διατυπώνοντάς το διαφορετικά, ποια είναι η μεγαλύτερη τιμή που μπορεί να πάρει το n (αν υπάρχει τέτοια);

Η απάντηση είναι ότι, ξεκινώντας από το $\mathbb{R}$, μπορούμε να εφαρμόσουμε τον διπλασιασμό Cayley–Dickson το πολύ τρεις φορές ώστε το αποτέλεσμα να είναι composition άλγεβρα και δίνεται από το Θεώρημα Hurwitz. Οι επόμενες τρεις προτάσεις θα μας επιτρέψουν να το αποδείξουμε.

Με i_{A_n} συμβολίζουμε μοναδιαίο διάνυσμα της άλγεβρας A_n κάθετο στην A_{n-1} .

Πρόταση 2.17. Η $A_3 = A_2 + i_{A_3}A_2$ είναι composition άλγεβρα αν και μόνο αν η A_2 είναι προσεταιριστική composition άλγεβρα.

Απόδειξη

(Χρησιμοποιούμε αρκετές φορές την : $x, y \in A_2 \Rightarrow \langle x, i_{A_3}y \rangle = \langle x\bar{y}, i_{A_3} \rangle = 0$.)

A_3 composition άλγεβρα $\Leftrightarrow$

για κάθε $\alpha, \beta, \gamma, \delta \in A_2$,

$$N(\alpha + i_{A_3}\beta)N(\gamma + i_{A_3}\delta) = N((\alpha\gamma - \delta\bar{\beta}) + i_{A_3}(\gamma\beta + \bar{\alpha}\delta)) \Leftrightarrow$$

$$\begin{aligned} & \left(2\langle \alpha, i_{A_3}\beta \rangle + N(\alpha) + N(i_{A_3}\beta)\right) \left(2\langle \gamma, i_{A_3}\delta \rangle + N(\gamma) + N(i_{A_3}\delta)\right) \\ &= 2\langle \alpha\gamma - \delta\bar{\beta}, i_{A_3}(\gamma\beta + \bar{\alpha}\delta) \rangle + N(\alpha\gamma - \delta\bar{\beta}) + N(i_{A_3}(\gamma\beta + \bar{\alpha}\delta)) \Leftrightarrow \end{aligned}$$

$$\begin{aligned} & \left(N(\alpha) + N(i_{A_3}\beta)\right) \left(N(\gamma) + N(i_{A_3}\delta)\right) = \\ &= 2\langle \alpha\gamma - \delta\bar{\beta}, i_{A_3}(\gamma\beta) + i_{A_3}(\bar{\alpha}\delta) \rangle + 2\langle \alpha\gamma, -\delta\bar{\beta} \rangle + N(\alpha\gamma) + N(\delta\bar{\beta}) + N(\gamma\beta + \bar{\alpha}\delta) \Leftrightarrow \end{aligned}$$

$$\begin{aligned} & (N(\alpha) + N(\beta))(N(\gamma) + N(\delta)) = \\ &= -2\langle \alpha\gamma, \delta\bar{\beta} \rangle + N(\alpha)N(\gamma) + N(\delta)N(\bar{\beta}) + 2\langle \gamma\beta, \bar{\alpha}\delta \rangle + N(\gamma\beta) + N(\bar{\alpha}\delta) \Leftrightarrow \end{aligned}$$

$$\begin{aligned} & (N(\alpha) + N(\beta))(N(\gamma) + N(\delta)) = \\ &= -2\langle \alpha\gamma, \delta\bar{\beta} \rangle + N(\alpha)N(\gamma) + N(\delta)N(\bar{\beta}) + 2\langle \gamma\beta, \bar{\alpha}\delta \rangle + N(\gamma\beta) + N(\bar{\alpha}\delta) \Leftrightarrow \end{aligned}$$

$$\begin{aligned} N(\alpha)N(\gamma) + N(\alpha)N(\delta) + N(\beta)N(\gamma) + N(\beta)N(\delta) &= \\ &= -2\langle \alpha\gamma, \delta\bar{\beta} \rangle + N(\alpha)N(\gamma) + N(\delta)N(\bar{\beta}) + 2\langle \gamma\beta, \bar{\alpha}\delta \rangle + N(\gamma)N(\beta) + N(\bar{\alpha})N(\delta) \Leftrightarrow \end{aligned}$$

$$\begin{aligned} N(\alpha)N(\gamma) + N(\alpha)N(\delta) + N(\beta)N(\gamma) + N(\beta)N(\delta) &= \\ &= -2\langle \alpha\gamma, \delta\bar{\beta} \rangle + N(\alpha)N(\gamma) + N(\delta)N(\beta) + 2\langle \gamma\beta, \bar{\alpha}\delta \rangle + N(\gamma)N(\beta) + N(\alpha)N(\delta) \Leftrightarrow \end{aligned}$$

$$0 = -2\langle \alpha\gamma, \delta\bar{\beta} \rangle + 2\langle \gamma\beta, \bar{\alpha}\delta \rangle \Leftrightarrow$$

$$\langle \alpha\gamma, \delta\bar{\beta} \rangle = \langle \gamma\beta, \bar{\alpha}\delta \rangle \Leftrightarrow$$

$$\langle (\alpha\gamma)\beta, \delta \rangle = \langle \alpha(\gamma\beta), \delta \rangle, \text{ για κάθε } \alpha, \beta, \gamma, \delta \in A_2 \Leftrightarrow$$

$$(\alpha\gamma)\beta = \alpha(\gamma\beta), \text{ για κάθε } \alpha, \beta, \gamma \in A_2. \quad \blacksquare$$

Η επόμενη πρόταση είναι μάλλον αναμενόμενη.

Πρόταση 2.18. Η $A_2 = A_1 + i_{A_2}A_1$ είναι προσεταιριστική composition άλγεβρα αν και μόνο αν η A_1 είναι μεταθετική και προσεταιριστική composition άλγεβρα.

Απόδειξη

Από την (2.12) έχουμε ότι για κάθε $\alpha, \beta \in A_1$:

$$(i_{A_2}\alpha)\beta = (0 + i_{A_2}\alpha)(\beta + i_{A_2}0) = (0\beta - 0\bar{\alpha}) + i_{A_2}(\beta\alpha + \bar{0}0) = i_{A_2}(\beta\alpha)$$

Όμως η A_2 είναι προσεταιριστική composition άλγεβρα, άρα η υποάλγεβρά της A_1 έχει επίσης αυτές τις ιδιότητες. Έχουμε λοιπόν:

$$(i_{A_2}\alpha)\beta = i_{A_2}(\alpha\beta) = i_{A_2}(\beta\alpha), \text{ για κάθε } \alpha, \beta \in A_1$$

Η τελευταία σχέση δείχνει ότι για να είναι η A_2 προσεταιριστική composition άλγεβρα θα πρέπει να ισχύει:

$$\alpha\beta = \beta\alpha, \text{ για κάθε } \alpha, \beta \in A_1$$

δηλαδή η A_1 θα πρέπει να είναι και μεταθετική.

Αντίστροφα, αν $\alpha, \beta, \gamma, \delta, \varepsilon, \zeta \in A_1$, έχουμε:

$$\begin{aligned}
 & [(\alpha + i_{A_2}\beta)(\gamma + i_{A_2}\delta)](\varepsilon + i_{A_2}\zeta) = [(\alpha\gamma - \delta\bar{\beta}) + i_{A_2}(\gamma\beta + \bar{\alpha}\delta)](\varepsilon + i_{A_2}\zeta) \\
 & = [(\alpha\gamma - \delta\bar{\beta})\varepsilon - \zeta(\bar{\beta}\bar{\gamma} + \bar{\delta}\alpha)] + i_{A_2}[\varepsilon(\gamma\beta + \bar{\alpha}\delta) + (\bar{\gamma}\bar{\alpha} - \beta\bar{\delta})\zeta] \\
 & = [(\alpha\gamma)\varepsilon - (\delta\bar{\beta})\varepsilon - \zeta(\bar{\beta}\bar{\gamma}) - \zeta(\bar{\delta}\alpha)] + i_{A_2}[\varepsilon(\gamma\beta) + \varepsilon(\bar{\alpha}\delta) + (\bar{\gamma}\bar{\alpha})\zeta - (\beta\bar{\delta})\zeta]
 \end{aligned}$$

και,

$$\begin{aligned}
 & (\alpha + i_{A_2}\beta)[(\gamma + i_{A_2}\delta)(\varepsilon + i_{A_2}\zeta)] = (\alpha + i_{A_2}\beta)[(\gamma\varepsilon - \zeta\bar{\delta}) + i_{A_2}(\varepsilon\delta + \bar{\gamma}\zeta)] \\
 & = [\alpha(\gamma\varepsilon - \zeta\bar{\delta}) - (\varepsilon\delta + \bar{\gamma}\zeta)\bar{\beta}] + i_{A_2}[(\gamma\varepsilon - \zeta\bar{\delta})\beta + \bar{\alpha}(\varepsilon\delta + \bar{\gamma}\zeta)] \\
 & = [\alpha(\gamma\varepsilon) - \alpha(\zeta\bar{\delta}) - (\varepsilon\delta)\bar{\beta} - (\bar{\gamma}\zeta)\bar{\beta}] + i_{A_2}[(\gamma\varepsilon)\beta - (\zeta\bar{\delta})\beta + \bar{\alpha}(\varepsilon\delta) + \bar{\alpha}(\bar{\gamma}\zeta)]
 \end{aligned}$$

Αν η A_1 είναι μεταθετική και προσεταιριστική composition άλγεβρα, οι δύο παραστάσεις είναι ίσες και η A_2 είναι προσεταιριστική composition άλγεβρα. ■

Μένει ένα τελευταίο βήμα για να ολοκληρώσουμε την πορεία μας για το Θεώρημα Hurwitz. Πριν από αυτό θα δώσουμε όνομα σε μια ήδη γνωστή ιδιότητα του $\mathbb{R}$.

Ορισμός 2.19. Άλγεβρα με τετριμμένο συζυγή, ονομάζεται μια άλγεβρα στην οποία ισχύει:

$$\bar{x} = x, \text{ για κάθε } x \in A$$

Στον Ορισμό 2.8 είδαμε ότι το $\mathbb{R}$ είναι άλγεβρα με τετριμμένο συζυγή.

Πρόταση 2.20. Η $A_1 = A_0 + i_{A_1}A_0$ είναι μεταθετική και προσεταιριστική composition άλγεβρα αν και μόνο αν η A_0 είναι μεταθετική και προσεταιριστική composition άλγεβρα με τετριμμένο συζυγή.

Απόδειξη

Από την (2.11) έχουμε:

$$i_{A_1}\alpha = -\overline{i_{A_1}\alpha} = -\bar{\alpha}\overline{i_{A_1}} = \bar{\alpha}i_{A_1}$$

Αν η A_1 είναι μεταθετική και προσεταιριστική composition άλγεβρα, η υποάλγεβρά της A_0 έχει τις ίδιες ιδιότητες και η $i_{A_1}\alpha = \bar{\alpha}i_{A_1} = i_{A_1}\bar{\alpha}$, για κάθε $\alpha \in A_0$, σημαίνει ότι θα πρέπει να ισχύει $\alpha = \bar{\alpha}$, για κάθε $\alpha \in A_0$, δηλαδή η άλγεβρα A_0 θα πρέπει να έχει τετριμμένο συζυγή.

Αντίστροφα, αν $\alpha, \beta, \gamma, \delta \in A_0$ έχουμε:

$$(\alpha + i_{A_1}\beta)(\gamma + i_{A_1}\delta) = (\alpha\gamma - \delta\bar{\beta}) + i_{A_1}(\gamma\beta + \bar{\alpha}\delta)$$

και

$$(\gamma + i_{A_1}\delta)(\alpha + i_{A_1}\beta) = (\gamma\alpha - \beta\bar{\delta}) + i_{A_1}(\alpha\delta + \bar{\gamma}\beta)$$

Αν η A_0 είναι μεταθετική, προσεταιριστική και με τετριμμένο συζυγή composition άλγεβρα, οι δύο παραστάσεις είναι ίσες και η A_1 είναι μεταθετική και προσεταιριστική composition άλγεβρα. ■

Φτάσαμε τελικά στον στόχο της ενότητας:

Θεώρημα 2.21. (Hurwitz) Οι μόνες composition άλγεβρες επί των πραγματικών αριθμών με θετικά ορισμένη νόρμα είναι αυτές με διάσταση 1, 2, 4, 8 (επί του $\mathbb{R}$).

Απόδειξη

Κάθε composition άλγεβρα επί του $\mathbb{R}$ είναι ίση με αυτό ή το περιέχει ως την «μικρότερη» υποάλγεβρά της.

Αν η άλγεβρά μας είναι η $A_0 = \mathbb{R}$, τότε $\dim(A_0) = 1$.

Διαφορετικά, ξεκινώντας από την $A_0 = \mathbb{R}$, η οποία είναι μεταθετική, προσεταιριστική και με τετριμμένο συζυγή composition άλγεβρα, εφαρμόζοντας τον διπλασιασμό Cayley–Dickson, παίρνουμε την A_1 η οποία είναι μεταθετική, προσεταιριστική (αλλά χωρίς τετριμμένο συζυγή) composition άλγεβρα, για την οποία όπως είδαμε ισχύει $\dim(A_1) = 2$.

Εφαρμόζοντας στην A_1 , η οποία είναι μεταθετική και προσεταιριστική composition άλγεβρα, τον διπλασιασμό Cayley–Dickson, παίρνουμε την A_2 η οποία είναι προσεταιριστική composition άλγεβρα, η οποία έχει διάσταση $\dim(A_2) = 4$.

Εφαρμόζοντας στην A_2 , η οποία είναι προσεταιριστική composition άλγεβρα, τον διπλασιασμό Cayley–Dickson, παίρνουμε την A_3 η οποία είναι composition άλγεβρα, η οποία έχει διάσταση $\dim(A_3) = 8$.

Η άλγεβρα A_3 δεν είναι προσεταιριστική, άρα ο διπλασιασμός της δεν μας δίνει composition άλγεβρα. ■

Στην επόμενη ενότητα θα δείξουμε ότι οι άλγεβρες του παραπάνω Θεωρήματος είναι οι άλγεβρες $\mathbb{R}, \mathbb{C}, \mathbb{H}, \mathbb{O}$ ή είναι ισομορφικές με αυτές. Στην περίπτωση που η νόρμα δεν είναι θετικά ορισμένη, οι άλγεβρες (διάστασης 2, 4, 8) που προκύπτουν από τον διπλασιασμό Cayley–Dickson είναι composition αλλά δεν είναι άλγεβρες διαίρεσης.

2.4 Συνέπειες του Θεωρήματος Hurwitz – Άλλες ιδιότητες των αλγεβρών

Στις ενότητες 2.1 και 2.2 ακολουθήσαμε έναν μακρύ και κάπως πολύπλοκο τρόπο για να ορίσουμε τις composition άλγεβρες και να διερευνήσουμε κάποιες από τις ιδιότητές τους. Σε αυτήν την ενότητα θα δείξουμε ότι η κατασκευή των μιγαδικών, των υπερμιγαδικών και των οκτονίων επιτυγχάνεται πιο σύντομα και κομψά ακολουθώντας αυτήν την προσέγγιση. Επίσης θα δείξουμε μερικές ακόμη ιδιότητες, ιδιαίτερα χρήσιμες στον χειρισμό των οκτονίων.

Πρόταση 2.22. Αν $\alpha, \beta \in A_{n-1}$ και $(\alpha + i_{A_n}\beta) \in A_n$ τότε:

$$N_{A_n}(\alpha + i_{A_n}\beta) = N_{A_{n-1}}(\alpha) + N_{A_{n-1}}(\beta) \quad (2.13)$$

Απόδειξη

Από τις (2.1) και (2.10) έχουμε:

$$N_{A_n}(\alpha + i_{A_n}\beta) = \langle \alpha + i_{A_n}\beta, \alpha + i_{A_n}\beta \rangle = \langle \alpha, \alpha \rangle + \langle \beta, \beta \rangle = N_{A_{n-1}}(\alpha) + N_{A_{n-1}}(\beta) \quad \blacksquare$$

Στην απόδειξη της (2.10) απαιτήσαμε $N_{A_n}(i_{A_n}) = 1$. Από την (2.13) διαπιστώνουμε ότι αυτή η απαίτηση «κληροδοτεί» τη θετικά ορισμένη νόρμα της A_{n-1} στην A_n .

Η κατασκευή και οι βασικές ιδιότητες των συνόλων $\mathbb{C}, \mathbb{H}, \mathbb{O}$ προκύπτουν τώρα φυσιολογικά.

- Ξεκινάμε από το $A_0 = \mathbb{R}$.

Είναι μια μεταθετική, προσεταιριστική και με τετριμμένο συζυγή composition άλγεβρα.

Η νόρμα του ορίζεται ως: $N(x) = x^2$.

- Εφαρμόζοντας στο $\mathbb{R}$ τον διπλασιασμό Cayley–Dickson, παίρνουμε την άλγεβρα:

$$A_1 = \mathbb{R} + i\mathbb{R} = \{\alpha + i\beta : \alpha, \beta \in \mathbb{R}\} = \mathbb{C}$$

Το $\mathbb{C}$ είναι μια μεταθετική και προσεταιριστική composition άλγεβρα

Από τους κανόνες του διπλασιασμού παίρνουμε:

$$\text{Αν } z = \alpha + i\beta, w = \gamma + i\delta \in \mathbb{C}$$

- Η νόρμα βρίσκεται από την (2.13):

$$N_{\mathbb{C}}(z) = N_{\mathbb{C}}(\alpha + i\beta) = N_{\mathbb{R}}(\alpha) + N_{\mathbb{R}}(\beta) = \alpha^2 + \beta^2.$$

- Ο συζυγής ορίζεται από την (2.11): $\bar{z} = \overline{\alpha + i\beta} = \bar{\alpha} - i\beta = \alpha - i\beta$

- Το γινόμενο ορίζεται από την (2.12):

$$zw = (\alpha + i\beta)(\gamma + i\delta) = (\alpha\gamma - \delta\bar{\beta}) + i(\gamma\beta + \bar{\alpha}\delta) = (\alpha\gamma - \beta\delta) + i(\alpha\delta + \beta\gamma)$$

- «Διπλασιάζοντας» το $\mathbb{C}$, παίρνουμε την άλγεβρα:

$$A_2 = \mathbb{C} + j\mathbb{C} = \{z + jw : z, w \in \mathbb{C}\} = \{\alpha + \beta i + \gamma j + \delta ji : \alpha, \beta, \gamma, \delta \in \mathbb{R}\} = \mathbb{H}$$

Το $\mathbb{H}$ είναι μια προσεταιριστική composition άλγεβρα

- Από την (2.13): $N_{\mathbb{H}}(q) = N_{\mathbb{C}}(\alpha + i\beta) + N_{\mathbb{C}}(\gamma + i\delta) = \alpha^2 + \beta^2 + \gamma^2 + \delta^2$.

- Ο συζυγής ορίζεται από την (2.11): $\bar{q} = \overline{\alpha + \beta i + \gamma j + \delta ji} = \alpha - \beta i - \gamma j - \delta ji$

- Το γινόμενο ορίζεται από την (2.12).

Επισημαίνουμε εδώ ότι ο τρόπος με τον οποίο κατασκευάσαμε το σύνολο των υπερμιγαδικών παραπάνω, διαφέρει από αυτόν του Hamilton ($\mathbb{H} = \mathbb{C} + \mathbb{C}j$), δίνοντας μια ισόμορφη άλγεβρα.

Αν $\mathbb{H} = \mathbb{C} + \mathbb{C}j$ η άλγεβρα των υπερμιγαδικών όπως την ορίσαμε στην ενότητα 1.3 και $\mathbb{H}' = \mathbb{C} + j\mathbb{C}$ η αντίστοιχη από τον διπλασιασμό Cayley–Dickson που δώσαμε παραπάνω, αποδεικνύεται εύκολα ότι η απεικόνιση

$$f: \mathbb{H}' \rightarrow \mathbb{H}, f(\alpha + \beta i + \gamma j + \delta ji) = \alpha + \beta i + \gamma j - \delta ij$$

είναι ισομορφισμός.

- Τέλος, «διπλασιάζοντας» το $\mathbb{H}$, παίρνουμε την άλγεβρα:

$$A_3 = \mathbb{H} + l\mathbb{H} = \{q + lp: q, p \in \mathbb{H}\} =$$

$$= \{\alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 ji + \alpha_4 l + \alpha_5 li + \alpha_6 lj + \alpha_7 l(ji): \alpha_0, \dots, \alpha_7 \in \mathbb{R}\} = \mathbb{O}$$

Το $\mathbb{O}$ είναι μια composition άλγεβρα

- Η νόρμα είναι: $N(x) = \alpha_0^2 + \alpha_1^2 + \alpha_2^2 + \alpha_3^2 + \alpha_4^2 + \alpha_5^2 + \alpha_6^2 + \alpha_7^2$.

- Ο συζυγής είναι: $\bar{x} = \overline{\alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 ji + \alpha_4 l + \alpha_5 li + \alpha_6 lj + \alpha_7 l(ji)} =$
 $= \alpha_0 - \alpha_1 i - \alpha_2 j - \alpha_3 ji - \alpha_4 l - \alpha_5 li - \alpha_6 lj - \alpha_7 l(ji)$

- Το γινόμενο ορίζεται από την (2.12).

Οι επόμενες δύο προτάσεις δείχνουν πόσο βαθιά συνυφασμένη με τη δομή μιας composition άλγεβρας είναι η νόρμα της.

Πρόταση 2.23. Η άλγεβρα A_n , $n = 0, 1, 2, 3$, είναι **τετραγωνική (quadratic)** επί του $\mathbb{R}$ δηλαδή, κάθε στοιχείο x της A_n ικανοποιεί μια εξίσωση της μορφής:

$$x^2 - t(x)x + n(x)1 = 0, \quad t(x), n(x) \in \mathbb{R}. \quad (2.14)$$

Απόδειξη

Για κάθε $x, y, w, z \in A_n$ έχουμε:

$$\langle (x + z)y, (x + z)w \rangle = N(x + z)\langle y, w \rangle \Leftrightarrow \langle xy + zy, xw + zw \rangle = N(x + z)\langle y, w \rangle$$

$$\langle xy, xw \rangle = N(x)\langle y, w \rangle$$

$$\langle zy, zw \rangle = N(z)\langle y, w \rangle$$

Αφαιρώντας από την πρώτη τις δύο τελευταίες παίρνουμε:

$$\langle xy + zy, xw + zw \rangle - \langle xy, xw \rangle - \langle zy, zw \rangle = \langle y, w \rangle (N(x + z) - N(x) - N(z))$$

Χρησιμοποιώντας την γραμμικότητα του εσωτερικού γινομένου στο 1^ο μέλος και τον ορισμό του εσωτερικού γινομένου στο 2^ο παίρνουμε:

$$\langle xy, zw \rangle + \langle zy, xw \rangle = 2\langle x, z \rangle \langle y, w \rangle$$

Θέτουμε $z = 1$ και $y = xu$, $u \in A_n$ παίρνουμε:

$$\langle x(xu), w \rangle + \langle xu, xw \rangle = 2\langle x, 1 \rangle \langle xu, w \rangle \quad \text{ή}$$

$$\langle x(xu), w \rangle + N(x) \langle u, w \rangle - 2\langle x, 1 \rangle \langle xu, w \rangle = 0 \quad \text{ή}$$

$$\langle x(xu), w \rangle + \langle N(x)u, w \rangle - \langle 2\langle x, 1 \rangle(xu), w \rangle = 0$$

Πάλι από την γραμμικότητα του εσωτερικού γινομένου:

$$\langle x(xu) + N(x)u - 2\langle x, 1 \rangle(xu), w \rangle = 0$$

Αφού το εσωτερικό γινόμενο είναι μη εκφυλισμένο έχουμε:

$$x(xu) + N(x)u - 2\langle x, 1 \rangle(xu) = 0, \quad \text{για κάθε } x, u \in A_n$$

Θέτοντας $u = 1$ παίρνουμε:

$$x^2 - 2\langle x, 1 \rangle x + N(x)1 = 0, \quad \text{για κάθε } x \in A_n \quad \blacksquare$$

Η παραπάνω πρόταση μας επιτρέπει να δείξουμε ότι:

Πρόταση 2.24. Αν (A_n, N) και (A_n, N_1) , $n = 0, 1, 2, 3$, οι άλγεβρες με νόρμες N και N_1 αντίστοιχα, τότε $N = N_1$.

Απόδειξη

Συμβολίζουμε με $\langle \cdot \rangle$ και $\langle \cdot \rangle_1$ τα συσχετισμένα με τις νόρμες εσωτερικά γινόμενα.

Από την (2.14) έχουμε:

$$x^2 = 2\langle x, 1 \rangle x - N(x)1 \quad \text{και,}$$

$$x^2 = 2\langle x, 1 \rangle_1 x - N_1(x)1, \quad \text{επομένως}$$

$$2\langle x, 1 \rangle x - N(x)1 = 2\langle x, 1 \rangle_1 x - N_1(x)1$$

Αν τα στοιχεία $x, 1$ είναι γραμμικά ανεξάρτητα τότε προκύπτει αμέσως ότι $N(x) = N_1(x)$.

Αν είναι γραμμικά εξαρτημένα τότε υπάρχει $\lambda \in \mathbb{R}$ τέτοιο ώστε $x = \lambda 1$ επομένως έχουμε:

$$N(x) = N(\lambda 1) = \lambda^2 N(1) = \lambda^2 1 = \lambda^2 N_1(1) = N_1(\lambda 1) = N_1(x)$$

Επομένως η νόρμα στις composition άλγεβρες μας είναι μοναδική. ■

Θα δείξουμε τώρα ότι οι άλγεβρες $A_0 \dots A_3$ είναι άλγεβρες διαίρεσης. Θα χρειαστούμε πρώτα την παρακάτω πρόταση.

Πρόταση 2.25. Αν A μια composition άλγεβρα πεπερασμένης διάστασης, τότε:

$$A \text{ άλγεβρα διαίρεσης} \Leftrightarrow (\text{για κάθε } x, y \in A, \quad xy = 0 \Leftrightarrow x = 0 \text{ ή } y = 0)$$

Απόδειξη

($\Rightarrow$)

Έστω ότι A άλγεβρα διαίρεσης.

Αν $xy = 0$ και $x \neq 0$, τότε η $y = 0$ είναι λύση και από τον ορισμό 2.2. μοναδική.

Αντίστοιχα αν $y \neq 0$, τότε η $x = 0$ είναι μοναδική λύση.

Επομένως ισχύει η $xy = 0 \Leftrightarrow x = 0 \text{ ή } y = 0$.

(Αν μια άλγεβρα περιέχει στοιχεία $x \neq 0$ και $y \neq 0$ τέτοια ώστε $xy = 0$, τότε αυτά τα στοιχεία λέγονται **διαιρέτες του μηδενός**.)

($\Leftarrow$)

Έστω ότι για κάθε $x, y \in A$, $xy = 0 \Leftrightarrow x = 0 \text{ ή } y = 0$.

Θα δείξουμε ότι, αν $a \in A$, με $a \neq 0$ τότε οι εξισώσεις

$$xa = \beta \text{ και } ay = \beta$$

έχουν μοναδική λύση για κάθε $\beta \in A$, επομένως η A είναι άλγεβρα διαίρεσης.

Ορίζουμε τη γραμμική απεικόνιση $R_\alpha: A \rightarrow A$, $R_\alpha(x) = x\alpha$.

$$R_\alpha(x) = 0 \Rightarrow x\alpha = 0.$$

Αφού $\alpha \neq 0$ και σύμφωνα με την υπόθεση η άλγεβρα A δεν έχει διαιρέτες του μηδενός έχουμε:

$$x = 0.$$

Άρα, $\ker(R_\alpha) = \{0\}$ και η R_α είναι 1-1.

Αφού η A έχει πεπερασμένη διάσταση, η R_α είναι και επί (αφού $\dim A = \dim(\operatorname{Im}(R_\alpha)) + \dim(\ker(R_\alpha))$).

Επομένως, για κάθε $\beta \in A$, υπάρχει $x \in A$ τέτοιο ώστε $x\alpha = \beta$.

Αφού η R_α είναι 1-1 αυτό το x είναι μοναδικό.

Η ύπαρξη μοναδικής λύσης για την $\alpha y = \beta$ είναι όμοια και παραλείπεται. ■

Σε όλες τις άλγεβρες που κατασκευάστηκαν με τον παραπάνω τρόπο, η νόρμα είναι θετικά ορισμένη άρα:

$$N(x) = 0 \Leftrightarrow x = 0.$$

Αυτή η ιδιότητα, σε συνδυασμό με το γεγονός ότι η νόρμα είναι πολλαπλασιαστική κάνει τις παραπάνω άλγεβρες διαίρεσης.

Πράγματι, αν σε κάποια από αυτές τις άλγεβρες είχαμε $x \neq 0 \neq y$ με $xy = 0$, τότε θα ίσχυε:

$$0 = N(xy) = N(x)N(y) \neq 0$$

Επισημαίνουμε εδώ ότι η απαίτηση για θετικά ορισμένη νόρμα είναι ουσιαστική προκειμένου μια composition άλγεβρα να είναι και άλγεβρα διαίρεσης. Μια άλγεβρα η οποία περιέχει διαιρέτες του μηδενός και έχει θετικά ορισμένη νόρμα δεν μπορεί να είναι composition, αφού η νόρμα της δεν θα μπορούσε να είναι πολλαπλασιαστική. Όταν η νόρμα μιας composition άλγεβρας επί των πραγματικών αριθμών δεν είναι θετικά ορισμένη, προκύπτουν οι λεγόμενες **split composition άλγεβρες**, οι οποίες περιέχουν διαιρέτες του μηδενός (Dray & Manogue (2015)).

Επίσης σε κάθε μια από τις παραπάνω άλγεβρες ισχύει:

$$x\bar{x} = \bar{x}x = N(x) \quad (2.15)$$

Πράγματι:

Αν $x \in A_0 = \mathbb{R}$ τότε $x\bar{x} = \bar{x}x = xx = x^2 = N(x)$.

Μέσω των κανόνων διπλασιασμού η ιδιότητα αυτή «κληροδοτείται» στις άλγεβρες που παράγονται από αυτόν αφού:

Αν για κάθε $y \in A_{n-1}$ ισχύει $y\bar{y} = N_{A_{n-1}}(y)$ τότε:

για κάθε στοιχείο της επόμενης άλγεβρας $x = \alpha + i_{A_n}\beta$, $\alpha, \beta \in A_{n-1}$

$$\begin{aligned} x\bar{x} &= (\alpha + i_{A_n}\beta)\overline{(\alpha + i_{A_n}\beta)} \stackrel{(2.11)}{=} (\alpha + i_{A_n}\beta)(\bar{\alpha} - i_{A_n}\bar{\beta}) \\ &\stackrel{(2.12)}{=} (\alpha\bar{\alpha} - (-\beta)\bar{\beta}) + i_{A_n}(\bar{\alpha}\beta + \bar{\alpha}(-\bar{\beta})) = \alpha\bar{\alpha} + \beta\bar{\beta} = N_{A_{n-1}}(\alpha) + N_{A_{n-1}}(\beta) \\ &\stackrel{(2.13)}{=} N_{A_n}(x). \end{aligned}$$

Με όμοιο τρόπο αποδεικνύεται και ότι $\bar{x}x = N(x)$.

Αν $n = 0, 1, 2, 3$, με βάση τα παραπάνω, για κάθε $0 \neq x \in A_n$ μπορούμε να ορίσουμε μοναδικό και αμφίπλευρο αντίστροφο, τον:

$$x^{-1} = \frac{\bar{x}}{N(x)} \quad (2.16)$$

Η μοναδικότητα του αντιστρόφου που ορίστηκε στην (2.16) αποδεικνύεται εύκολα για τις άλγεβρες των μιγαδικών και των υπερμιγαδικών. Για τα οκτόνια όμως απαιτεί την παρακάτω:

Πρόταση 2.26. Αν $x, y \in A_n$, $n = 0, 1, 2, 3$ τότε:

$$\bar{x}(xy) = N(x)y = (yx)\bar{x} \quad (2.17)$$

Απόδειξη

Για κάθε $t \in A_n$ έχουμε:

$$\langle \bar{x}(xy), t \rangle \stackrel{(2.6)}{=} \langle xy, \bar{x}t \rangle = \langle xy, xt \rangle = N(x)\langle y, t \rangle = \langle N(x)y, t \rangle \Rightarrow \bar{x}(xy) = N(x)y$$

$$\langle (yx)\bar{x}, t \rangle \stackrel{(2.6)}{=} \langle yx, t\bar{x} \rangle = \langle yx, tx \rangle = N(x)\langle y, t \rangle = \langle N(x)y, t \rangle \Rightarrow (yx)\bar{x} = N(x)y \quad \blacksquare$$

Αν $x \neq 0$ τότε $N(x) \neq 0$ και διαιρώντας την (2.17) με $N(x)$ παίρνουμε:

$$x^{-1}(xy) = y = (yx)x^{-1} \quad (2.18)$$

Τώρα μπορούμε να αποδείξουμε την μοναδικότητα του αντιστρόφου της (2.16).

Έστω $0 \neq x \in A_n$ και $x' \in A_n$ τέτοιος ώστε $x'x = 1$.

Πολλαπλασιάζοντας από δεξιά με x^{-1} παίρνουμε:

$$(x'x)x^{-1} = x^{-1} \stackrel{(2.18)}{\implies} x' = x^{-1}.$$

Αντίστοιχα αποδεικνύουμε και για την περίπτωση $xx' = 1$.

Στο 4^ο βήμα του διπλασιασμού Cayley–Dickson κατασκευάζεται η άλγεβρα των **sedenions** ($\mathbb{S}$). Με βάση τους κανόνες διπλασιασμού που δώσαμε παραπάνω, αν συμβολίσουμε με m το κάθετο στην $\mathbb{O}$ διάνυσμα με νόρμα $N(m) = 1$, τότε κάθε sedenion s γράφεται στη μορφή $s = \alpha + m\beta$ με $\alpha, \beta \in \mathbb{O}$ και για κάθε $\alpha, \beta, \gamma, \delta \in \mathbb{O}$ έχουμε τις σχέσεις:

$$\langle \alpha + m\beta, \gamma + m\delta \rangle = \langle \alpha, \gamma \rangle + \langle \beta, \delta \rangle$$

$$\overline{\alpha + m\beta} = \bar{\alpha} - m\beta$$

$$(\alpha + m\beta)(\gamma + m\delta) = (\alpha\gamma - \delta\bar{\beta}) + m(\gamma\beta + \bar{\alpha}\delta)$$

Χρησιμοποιώντας το συμβολισμό του Baez (στην υποενότητα 3.3.1 θα δείξουμε την αντιστοιχία των e_i με τα i, j, k, l και τα γινόμενά τους) έχουμε:

$$\begin{aligned} (e_6 + me_4)(e_5 + me_2) &= (e_6e_5 - e_2\bar{e}_4) + m(e_5e_4 + \bar{e}_6e_2) \\ &= (e_6e_5 + e_2e_4) + m(e_5e_4 - e_6e_2). \end{aligned}$$

Από το διάγραμμα Fano της Εικόνας 1.3 η τελευταία παράσταση είναι ίση με:

$$(-e_1 + e_1) + m(-e_7 + e_7) = 0.$$

Επομένως η άλγεβρα των sedenions, ενώ έχει θετική νόρμα περιέχει διαιρέτες του μηδενός άρα, όπως δείξαμε παραπάνω δεν είναι composition άλγεβρα.

Ο Moreno (1997) απέδειξε ότι το σύνολο των διαιρετών του μηδενός (α, β) της άλγεβρας των sedenions $\mathbb{S}$, με $N(\alpha) = N(\beta) = 1$, είναι ομοιομορφικό με την εξαιρετική ομάδα Lie G_2 .

Είδαμε παραπάνω ότι ο πολλαπλασιασμός οκτονίων δεν έχει την προσεταιριστική ιδιότητα. Παρακάτω θα αποδείξουμε κάποιες ιδιότητες οι οποίες, ως ένα βαθμό, την υποκαθιστούν.

Η προσεταιριστική ιδιότητα του πολλαπλασιασμού τις κάνει τετριμμένες για τις άλγεβρες $\mathbb{R}, \mathbb{C}, \mathbb{H}$, οπότε θα διατυπωθούν μόνο για τα οκτόνια.

Πρόταση 2.27. (Νόμοι του Moufang) Αν $x, y, z \in \mathbb{O}$, τότε:

$$1. (xy)(zx) = (x(yz))x = x((yz)x) \quad (2.19)$$

$$2. x(y(xz)) = (x(yx))z \quad (2.20)$$

$$3. y(x(zx)) = ((yx)z)x \quad (2.21)$$

Απόδειξη

1. Για κάθε $t \in \mathbb{O}$ έχουμε:

$$\begin{aligned} \langle (xy)(zx), t \rangle &\stackrel{(2.6)}{=} \langle xy, t(\overline{xz}) \rangle \stackrel{(2.5)}{=} 2\langle x, t \rangle \langle y, \overline{xz} \rangle - \langle x(\overline{xz}), ty \rangle \stackrel{(2.6)}{=} \\ &\stackrel{(2.6)}{=} 2\langle x, t \rangle \langle \overline{xz}, y \rangle - \langle \overline{xz}, \overline{x}(ty) \rangle \stackrel{(2.6)}{=} 2\langle x, t \rangle \langle \overline{x}, yz \rangle - \langle \overline{xz}, \overline{x}(ty) \rangle = \\ &= 2\langle x, t \rangle \langle yz, \overline{x} \rangle - N(\overline{x}) \langle \overline{z}, ty \rangle = 2\langle x, t \rangle \langle yz, \overline{x} \rangle - N(x) \langle \overline{z}, ty \rangle = \\ &= 2\langle yz, \overline{x} \rangle \langle x, t \rangle - N(x) \langle z, \overline{ty} \rangle = 2\langle yz, \overline{x} \rangle \langle x, t \rangle - N(x) \langle z, \overline{y}t \rangle \stackrel{(2.6)}{=} \\ &\stackrel{(2.6)}{=} 2\langle yz, \overline{x} \rangle \langle x, t \rangle - N(x) \langle yz, \overline{t} \rangle = 2\langle yz, \overline{x} \rangle \langle x, t \rangle - \langle x(yz), x\overline{t} \rangle \stackrel{(2.6)}{=} \\ &\stackrel{(2.6)}{=} 2\langle x(yz), 1 \rangle \langle x, t \rangle - \langle (x(yz))t, x \rangle \stackrel{(2.5)}{=} \langle (x(yz))x, 1t \rangle = \\ &= \langle (x(yz))x, t \rangle \implies (xy)(zx) = (x(yz))x \end{aligned}$$

Οι αποδείξεις για τις: $(xy)(zx) = x((yz)x)$, 2,3 είναι όμοιες και παραλείπονται. ■

Θέτοντας στις (2.19) και (2.20) $y = 1$ και στην 3. $z = 1$ παίρνουμε ότι:

Πρόταση 2.28. (Alternative laws) Αν $x, y, z \in \mathbb{O}$, τότε:

$$1. \quad x(yx) = (xy)x \quad (2.22)$$

$$2. \quad x(xz) = (xx)z \quad (2.23)$$

$$3. \quad (yx)x = y(xx) \quad (2.24)$$

Μια άλγεβρα που ικανοποιεί τις παραπάνω ιδιότητες ονομάζεται **εναλλάσσουσα (alternative)**.

Το γεγονός ότι η άλγεβρα των οκτονίων είναι εναλλάσσουσα συνεπάγεται άμεσα το Θεώρημα του Artin, το οποίο διατυπωμένο για τα οκτόνια είναι:

Θεώρημα 2.29. (Artin) Η υποάλγεβρα που παράγεται από δύο οποιαδήποτε οκτόνια είναι προσεταιριστική.

Ολοκληρώνοντας το κεφάλαιο, αποδεικνύουμε μερικές απλές αλλά ιδιαίτερα χρήσιμες ιδιότητες των οκτονίων.

Λήμμα 2.30. Αν $x = \alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 ji + \alpha_4 l + \alpha_5 li + \alpha_6 lj + \alpha_7 l(ji)$: $\alpha_0, \dots, \alpha_7 \in \mathbb{R}$ τότε:

$$\langle x, 1 \rangle = \alpha_0$$

Απόδειξη

$$\langle x, 1 \rangle = \langle \alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 ji + \alpha_4 l + \alpha_5 li + \alpha_6 lj + \alpha_7 l(ji), 1 \rangle$$

$$= \langle \alpha_0, 1 \rangle + \langle \alpha_1 i, 1 \rangle + \langle \alpha_2 j, 1 \rangle + \langle \alpha_3 ji, 1 \rangle + \langle \alpha_4 l, 1 \rangle + \langle \alpha_5 li, 1 \rangle + \langle \alpha_6 lj, 1 \rangle + \langle \alpha_7 l(ji), 1 \rangle$$

$$= \langle \alpha_0, 1 \rangle = \alpha_0 \quad \blacksquare$$

Λήμμα 2.31. $x \in Im\mathbb{O} \Leftrightarrow x^2 = -N(x)$

Απόδειξη

Για $x = 0$ η ισότητα ισχύει προφανώς.

Για $x \neq 0$ έχουμε:

$$x \in Im\mathbb{O} \Leftrightarrow x = -\bar{x} \Leftrightarrow xx = -\bar{x}x \Leftrightarrow x^2 = -N(x) \quad \blacksquare$$

Κλείνοντας το κεφάλαιο, πρέπει να τονίσουμε ότι όσα παρουσιάσαμε σε αυτό έχουν στη βάση τους τη νόρμα των composition αλγεβρών, η οποία μάλιστα καθορίζεται μοναδικά από τη δομή της άλγεβρας, και την πολλαπλασιαστική της ιδιότητα. Η πολλαπλασιαστική ιδιότητα λοιπόν αποδεικνύεται αρκετά ισχυρή ώστε να δώσει στις composition άλγεβρες την πλούσια δομή της οποίας παρουσιάσαμε μόνο ένα μέρος.

Κεφάλαιο 3. Θεωρία αριθμών και άλγεβρες διαίρεσης

3.1 Οι ακέραιοι Gauss

Ορισμός 3.1. Ονομάζουμε **ακέραιο του Gauss (Gaussian integer)** ένα μιγαδικό αριθμό της μορφής:

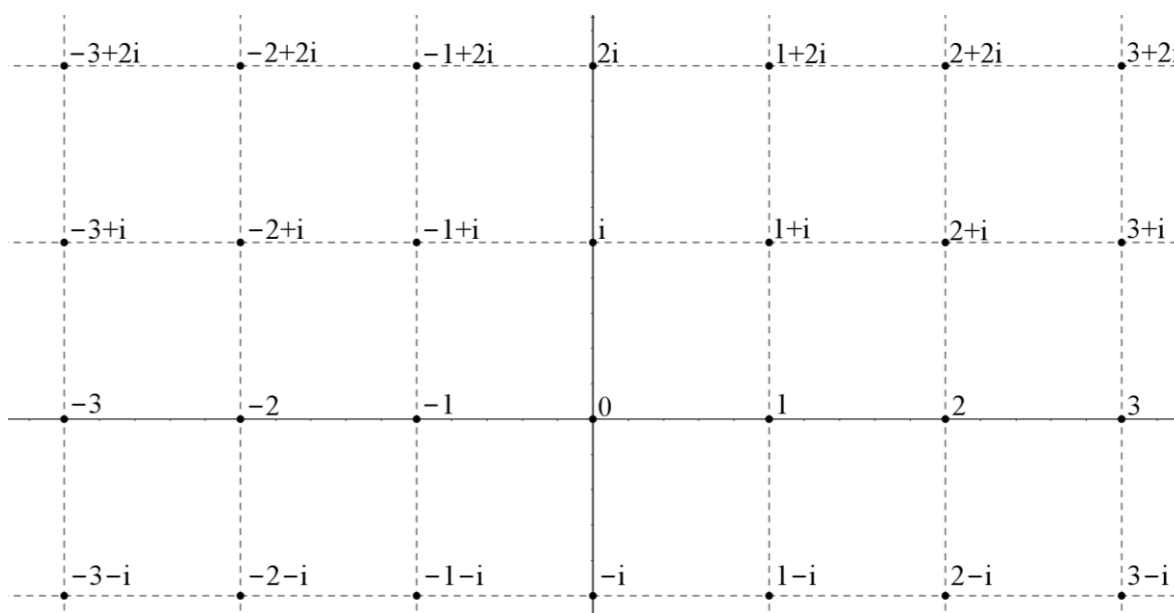
$$\alpha + i\beta, \quad \alpha, \beta \in \mathbb{Z}. \quad (3.1)$$

Εύκολα βλέπουμε ότι το σύνολο των ακεράιων του Gauss είναι κλειστό ως προς την πρόσθεση, την αφαίρεση και τον πολλαπλασιασμό και σχηματίζει έναν δακτύλιο.

Ορισμός 3.2. Ονομάζουμε **μονάδα του Gauss (Gaussian unit)** έναν ακέραιο του Gauss ο οποίος έχει πολλαπλασιαστικό αντίστροφο.

Υπάρχουν τέσσερις μονάδες του Gauss και είναι οι μιγαδικοί: $1, -1, i, -i$.

Γεωμετρικά οι ακέραιοι του Gauss σχηματίζουν ένα τετραγωνικό πλέγμα όπως φαίνεται στην παρακάτω εικόνα:



Εικόνα 3.1: Το πλέγμα των ακεράιων του Gauss

Είναι γνωστό ότι για οποιουσδήποτε ακέραιους Δ, δ με $\delta \neq 0$ υπάρχουν ακέραιοι π, υ με $0 \leq \upsilon < |\delta|$ τέτοιοι ώστε:

$$\Delta = \pi\delta + \upsilon \quad (3.2)$$

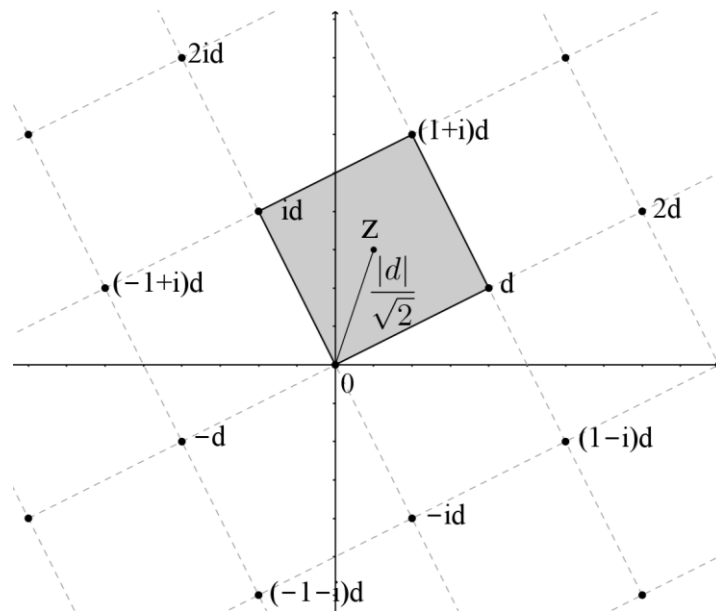
Μας ενδιαφέρει να διαπιστώσουμε αν ισχύει αντίστοιχη ιδιότητα στο σύνολο των ακεραίων του Gauss το οποίο θα συμβολίζουμε στο εξής με $\mathbb{Z}[i]$. Δηλαδή, αν για $Z, d \in \mathbb{Z}[i]$ με $d \neq 0$, υπάρχουν $Q, r \in \mathbb{Z}[i]$ τέτοιοι ώστε:

$$Z = Qd + r, \quad N(r) < N(d) \Leftrightarrow |r| < |d| \quad (3.3)$$

όπου $|\cdot|$ είναι το μέτρο μιγαδικού αριθμού $|\alpha + i\beta| = \sqrt{\alpha^2 + \beta^2}$.

Η (3.3) γίνεται: $Z - Qd = r$, $|r| < |d|$, δηλαδή μας αρκεί κάθε ακεραίος του Gauss να απέχει από κάποιο «ακέραιο» πολλαπλάσιο του d απόσταση μικρότερη από $|d|$.

Όπως βλέπουμε στο παρακάτω σχήμα:



Εικόνα 3.2: Μέγιστο μέτρο υπολοίπου για τους ακεραίους του Gauss (προσαρμογή από τους Conway–Smith)

τα ακεραία πολλαπλάσια του d σχηματίζουν ένα πλέγμα από τετράγωνα πλευράς $|d|$, άρα οποιοσδήποτε ακεραίος του Gauss απέχει από ένα πολλαπλάσιο του d , απόσταση με μέγιστη τιμή $\frac{|d|}{\sqrt{2}} < |d|$.

Ορισμός 3.3. Ένας μη μηδενικός ακεραίος του Gauss π ονομάζεται **πρώτος του Gauss (Gaussian prime)** αν δεν είναι μονάδα και για κάθε παραγοντοποίησή του

$$\pi = \alpha\beta$$

είτε η α είτε η β είναι μονάδα του Gauss.

Το γεγονός ότι στους ακέραιους του Gauss μπορούμε να ορίσουμε διαίρεση με υπόλοιπο «μικρότερο του διαιρέτη» μας επιτρέπει να αποδείξουμε ότι κάθε ακέραιος του Gauss αναλύεται σε γινόμενο πρώτων του Gauss.

Θεώρημα 3.4. Κάθε μη μηδενικός ακέραιος του Gauss ο οποίος δεν είναι μονάδα του Gauss, αναλύεται σε γινόμενο $\pi_1 \pi_2 \dots \pi_k$, όπου $\pi_1, \pi_2, \dots, \pi_k$ πρώτοι του Gauss. Δύο αναλύσεις ενός ακέραιου του Gauss προκύπτουν η μία από την άλλη με:

- αναδιάταξη των πρώτων ή
- πολλαπλασιασμό με μονάδες του Gauss u , της μορφής:

$$\pi_1 \dots \pi_n \pi_{n+1} \pi_k = \pi_1 \dots (\pi_n u) (\bar{u} \pi_{n+1}) \pi_k$$

3.2 Οι ακέραιοι Hurwitz

Σε αυτήν την ενότητα θα μας απασχολήσει το ερώτημα ποιοι υπερμιγαδικοί μπορούν να χαρακτηριστούν «ακέραιοι».

Σε μια φυσιολογική επέκταση των ακεράιων του Gauss ο Lipschitz το 1886 όρισε τους ακέραιους Lipschitz να είναι το σύνολο $\mathbb{L} = \{\alpha + \beta i + \gamma j + \delta k : \alpha, \beta, \gamma, \delta \in \mathbb{Z}\}$.

Μας ενδιαφέρει να διαπιστώσουμε αν μπορεί να οριστεί στο σύνολο $\mathbb{L}$ διαίρεση με υπόλοιπο «μικρότερο του διαιρέτη» δηλαδή, αν διαιρέσουμε έναν ακέραιο Lipschitz Z , με έναν επίσης ακέραιο Lipschitz z (και οι δύο μη μηδενικοί), μπορούμε να βρούμε «πηλίκο» Q και υπόλοιπο R , τέτοιους ώστε:

$$Z = Qz + R, \quad N(R) < N(z)$$

ή

$$Zz^{-1} - Q = Rz^{-1}, \quad N(Zz^{-1} - Q) = N(Rz^{-1}) < 1$$

Είναι γνωστό ότι, αν επιτρέψουμε στο υπόλοιπο μιας ευκλείδειας διαίρεσης να πάρει αρνητικές τιμές, τότε για κάθε ζευγάρι μη-μηδενικών ακεράιων Δ, δ , υπάρχει ένα ζευγάρι ακεράιων π, ν , τέτοιων ώστε:

$$\Delta = \pi\delta + \nu, \quad |\nu| \leq \frac{|\delta|}{2}$$

ή

$$\frac{\Delta}{\delta} - \pi = \frac{v}{\delta}, \quad \left| \frac{\Delta}{\delta} - \pi \right| = \left| \frac{v}{\delta} \right| \leq \frac{1}{2}$$

όπου π είναι ο πλησιέστερος προς τον $\frac{\Delta}{\delta}$ ακέραιος.

Έστω τώρα ότι $Zz^{-1} = a + \beta i + \gamma j + \delta k$ και $Q = A + Bi + \Gamma j + \Delta k$ όπου A, B, Γ, Δ οι πλησιέστεροι στους $\alpha, \beta, \gamma, \delta$ ακέραιοι. Τότε:

$$N(Rz^{-1}) = N(Zz^{-1} - Q) = (\alpha - A)^2 + (\beta - B)^2 + (\gamma - \Gamma)^2 + (\delta - \Delta)^2 \leq$$

$$\left(\frac{1}{2}\right)^2 + \left(\frac{1}{2}\right)^2 + \left(\frac{1}{2}\right)^2 + \left(\frac{1}{2}\right)^2 = 1 \Rightarrow N(R) \leq N(z).$$

Στους ακέραιους του Lipschitz λοιπόν δεν μπορούμε να ορίζουμε διαίρεση με υπόλοιπο «μικρότερο του διαιρέτη» κάτι που αποδεικνύεται μεγάλο εμπόδιο στην προσπάθεια να αναλύσουμε τέτοιους αριθμούς σε γινόμενα πρώτων παραγόντων.

Το πρόβλημα παρουσιάζεται ακριβώς όταν $(\alpha - A) = (\beta - B) = (\gamma - \Gamma) = (\delta - \Delta) = \frac{1}{2}$

δηλαδή όταν $\alpha, \beta, \gamma, \delta \in \mathbb{Z} + \frac{1}{2}$, και η λύση του δίνεται από τον ορισμό που έδωσε για τους «ακέραιους» υπερμιγαδικούς ο Hurwitz.

Ορισμός 3.5. Ονομάζουμε **ακέραιους του Hurwitz (Hurwitz integers ή Hurwitz integral quaternions)** το σύνολο:

$$H = \{\alpha + \beta i + \gamma j + \delta k : \alpha, \beta, \gamma, \delta \in \mathbb{Z}\} \cup \left\{ \alpha + \beta i + \gamma j + \delta k : \alpha, \beta, \gamma, \delta \in \mathbb{Z} + \frac{1}{2} \right\} \quad (3.4)$$

Αν τώρα ορίσουμε τους Z και z να είναι ακέραιοι Hurwitz και τους Q και R όπως παραπάνω, τότε έχουμε:

$$Z = Qz + R \text{ με } N(R) < N(z) \text{ ή}$$

$$N(R) = N(z).$$

Αν $N(R) = N(z)$ έχουμε ότι Zz^{-1} είναι ακέραιος Hurwitz και επιλέγοντας $Q = Zz^{-1}$, παίρνουμε $R = 0$ και έχουμε τέλεια διαίρεση $Z = Qz + 0$ στην οποία ισχύει $N(0) < N(z)$.

Μπορούμε τώρα να ασχοληθούμε με την ανάλυση ενός ακέραιου Hurwitz σε πρώτους παράγοντες, αφού πρώτα δώσουμε μερικούς απαραίτητους ορισμούς.

Ορισμός 3.6. Ονομάζουμε **πρώτο ακέραιο Hurwitz (prime Hurwitz integer)** έναν ακέραιο του Hurwitz P τέτοιον ώστε η νόρμα του να είναι ίση με έναν συνήθη πρώτο (rational prime) αριθμό p .

Ορισμός 3.7. Ονομάζουμε **μονάδα Hurwitz (Hurwitz unit)** έναν ακέραιο του Hurwitz τέτοιον ώστε η νόρμα του να είναι ίση με 1.

Θεώρημα 3.8. Υπάρχουν ακριβώς 24 μονάδες Hurwitz οι οποίες είναι, οι 8 μονάδες Lipschitz $\pm 1, \pm i, \pm j, \pm k$, και οι 16 της μορφής $\frac{1}{2}(\pm 1 \pm i \pm j \pm k)$ (στην ομάδα των 16 έχουμε όλους τους συνδυασμούς προσήμων).

Απόδειξη

Έστω υπερμιγαδικός $P = \alpha + \beta i + \gamma j + \delta k$.

Αν αυτός είναι Lipschitz θα πρέπει τουλάχιστον ένα από τα $|\alpha|, |\beta|, |\gamma|, |\delta| \geq 1$.

Για να είναι μονάδα θα πρέπει $N(P) = \alpha^2 + \beta^2 + \gamma^2 + \delta^2 = 1$, που σημαίνει ότι ένα ακριβώς από τα $\alpha, \beta, \gamma, \delta$ είναι ίσο με ± 1 , ενώ τα υπόλοιπα είναι 0.

Αν $\alpha, \beta, \gamma, \delta \in \mathbb{Z} + \frac{1}{2}$, τότε για να ισχύει $\alpha^2 + \beta^2 + \gamma^2 + \delta^2 = 1$, θα πρέπει όλα να έχουν τιμή $\pm \frac{1}{2}$. ■

Τώρα μπορούμε να ασχοληθούμε με τους πρώτους Hurwitz.

Όπως ένας συνήθης πρώτος αριθμός p μπορεί να γραφεί μόνο στις μορφές:

$$p = 1p \text{ ή } p = p1$$

απαιτούμε ένας πρώτος Hurwitz P να μπορεί να γραφεί μόνο ως:

$$P = P'U \text{ ή } P = VP'',$$

με $N(P') = N(P'') = p$ και $N(U) = N(V) = 1$.

Επομένως, οι μόνοι τρόποι γραφής ενός πρώτου Hurwitz είναι:

$$P = (PU^{-1})U \text{ και } P = V(V^{-1}P)$$

με U, V , να είναι οποιεσδήποτε από τις 24 μονάδες Hurwitz.

Σημειώνουμε ότι αν U είναι μονάδα Hurwitz τότε U^{-1} είναι επίσης μονάδα Hurwitz, επομένως και οι $PU^{-1}, V^{-1}P$ είναι ακέραιοι Hurwitz.

Η παραγοντοποίηση ενός ακεραίου Hurwitz εξαρτάται από το αν αυτός διαιρείται από φυσικό αριθμό $n > 1$, γεγονός που οδηγεί στον ακόλουθο ορισμό

Ορισμός 3.9. Ονομάζουμε **πρωταρχικό (primitive)** έναν ακέραιο του Hurwitz:

$$P = \alpha + \beta i + \gamma j + \delta k, \alpha, \beta, \gamma, \delta \in \mathbb{Z} \text{ ή}$$

$$P = \frac{1}{2}(\alpha + \beta i + \gamma j + \delta k), \text{ με } \alpha, \beta, \gamma, \delta \text{ της μορφής } 2\kappa + 1, \kappa \in \mathbb{Z},$$

$$\text{όταν } MK\Delta(\alpha, \beta, \gamma, \delta) = 1.$$

Αλλιώς τον ονομάζουμε **μη-πρωταρχικό (imprimitive)**.

Για την ανάλυση σε πρώτους παράγοντες των πρωταρχικών ακεραίων Hurwitz ισχύει το παρακάτω θεώρημα.

Θεώρημα 3.10. Αν Q πρωταρχικός ακέραιος Hurwitz με νόρμα $N(Q) = q$ τότε, για κάθε ανάλυση σε πρώτους $p_0 p_1 \dots p_k$ της νόρμας, υπάρχει μια ανάλυση

$$Q = P_0 P_1 \dots P_k$$

του Q σε γινόμενο πρώτων Hurwitz με νόρμες $N(P_0) = p_0, N(P_1) = p_1, \dots, N(P_k) = p_k$.

Θα λέμε ότι η ανάλυση $P_0 P_1 \dots P_k$ του Q είναι **με πρότυπο την ανάλυση** $p_0 p_1 \dots p_k$ της $N(Q)$.

Αν $Q = P_0 P_1 \dots P_k$ είναι οποιαδήποτε ανάλυση του Q σε πρώτους παράγοντες με πρότυπο την $p_0 p_1 \dots p_k$, τότε οι άλλες έχουν τη μορφή

$$Q = P_0 U_1 \cdot U_1^{-1} P_1 U_2 \cdot \dots \cdot U_k^{-1} P_k.$$

Απόδειξη

Είναι εύκολο να δούμε ότι το H είναι δακτύλιος.

Επίσης για κάθε $0 \neq x \in H$, $N(x) \geq 1$.

Άρα για κάθε $0 \neq x, y \in H$ έχουμε ότι: $N(xy) \geq N(x)$.

Τα παραπάνω μαζί με τη δυνατότητα ορισμού «με μικρό υπόλοιπο» κάνουν το H ευκλείδειο δακτύλιο.

Άρα κάθε ιδεώδες του (αριστερό ή δεξιό) είναι κύριο (Nagata (1987), van der Waerden) και το ιδεώδες

$$p_0H + QH$$

πρέπει να παράγεται από ένα στοιχείο του H έστω P_0 .

Επομένως θα πρέπει $p_0H + QH = P_0H$.

Παίρνοντας στο αριστερό μέλος τα $1, 0 \in H$ έχουμε ότι $p_0 \in P_0H$, άρα υπάρχει $R \in H$ τέτοιο ώστε $p_0 = P_0R$ και ο $N(P_0)$ θα πρέπει να είναι διαιρέτης του $N(p_0) = p_0^2 N(1) = p_0^2$. Δηλαδή θα πρέπει $N(P_0)$ να είναι ίσο με 1 ή p_0 ή p_0^2 .

Αν $N(P_0) = 1$, τότε θα ήταν $p_0H + QH = H$.

Αυτό όμως είναι άτοπο καθώς η νόρμα ενός τυχαίου στοιχείου $p_0x + Qy$ του ιδεώδους είναι:

$$\begin{aligned} N(p_0x + Qy) &= N(p_0x) + N(Qy) + 2\langle p_0x, Qy \rangle = \\ &= p_0^2 N(x) + p_0 p_1 \dots p_k N(y) + 2p_0 \langle x, Qy \rangle \end{aligned}$$

και διαιρείται με το p_0 .

Επίσης δεν μπορεί να ισχύει $N(P_0) = p_0^2$.

Παίρνοντας πάλι στο αριστερό μέλος τα $1, 0 \in H$ έχουμε ότι $p_0 \in P_0H$, άρα υπάρχει $R \in H$

τέτοιο ώστε $p_0 = P_0R \Rightarrow N(p_0) = N(P_0)N(R) \Rightarrow p_0^2 = p_0^2 N(R) \Rightarrow N(R) = 1$.

Τότε όμως θα είχαμε $p_0 = P_0U$ όπου U μονάδα Hurwitz, άρα $p_0U^{-1} = P_0$ και το p_0 θα διαιρούσε το Q . Αυτό όμως είναι άτοπο καθώς Q είναι πρωταρχικός ακέραιος Hurwitz.

Επομένως $N(P_0) = p_0$, δηλαδή ο P_0 είναι πρώτος Hurwitz ο οποίος διαιρεί τον Q .

Έτσι έχουμε ότι $Q = P_0Q_1$ με τον P_0 να είναι μοναδικός με εξαίρεση τον πολλαπλασιασμό του από δεξιά με μονάδα Hurwitz και $N(Q_1) = p_1 \dots p_k$.

Επαναλαμβάνοντας το βήμα άλλες k φορές φτάνουμε στο: $Q = P_0P_1 \dots P_kQ'$, με το Q' να είναι μονάδα Hurwitz (άρα να μπορεί να «ενσωματωθεί» στο P_k). ■

Παράδειγμα 3.11. Ένας πρωταρχικός ακέραιος Hurwitz Q , με $N(Q) = 84$, έχει (με την εξαίρεση του πολλαπλασιασμού με μονάδες) 12 αναλύσεις σε πρώτους παράγοντες, κάθε μια από αυτές με πρότυπο μια από τις παρακάτω αναλύσεις της νόρμας σε ρητούς πρώτους:

$$\begin{array}{cccccc} 2 \cdot 2 \cdot 3 \cdot 7 & 2 \cdot 2 \cdot 7 \cdot 3 & 2 \cdot 3 \cdot 2 \cdot 7 & 2 \cdot 7 \cdot 2 \cdot 3 & 2 \cdot 3 \cdot 7 \cdot 2 & 2 \cdot 7 \cdot 3 \cdot 2 \\ 3 \cdot 2 \cdot 2 \cdot 7 & 7 \cdot 2 \cdot 2 \cdot 3 & 3 \cdot 2 \cdot 7 \cdot 2 & 7 \cdot 2 \cdot 3 \cdot 2 & 3 \cdot 7 \cdot 2 \cdot 2 & 7 \cdot 3 \cdot 2 \cdot 2 \end{array}$$

Υπάρχουν τρεις θέσεις σε κάθε μια από αυτές τις αναλύσεις σε πρώτους στις οποίες μπορούμε να πολλαπλασιάσουμε με οποιαδήποτε από τις 24 μονάδες Hurwitz, άρα ο συνολικός αριθμός αναλύσεων σε πρώτους είναι: $24^3 \cdot 12 = 165.888$.

Δίνουμε παρακάτω κάποια στοιχεία από την θεωρία αριθμών που είναι απαραίτητα για να συνεχίσουμε την μελέτη μας στην ανάλυση των ακεραίων Hurwitz σε πρώτους παράγοντες.

Έστω p περιττός πρώτος.

Ορισμός 3.12. Ονομάζουμε **τετραγωνικό υπόλοιπο (mod p)** έναν ακέραιο r ο οποίος ικανοποιεί την $r \equiv a^2 \pmod{p}$. Αν ένας ακέραιος $s \not\equiv 0 \pmod{p}$ δεν ικανοποιεί την παραπάνω εξίσωση θα λέμε ότι **δεν είναι τετραγωνικό υπόλοιπο (mod p)** ή ότι είναι **μη-τετραγωνικό υπόλοιπο (mod p)**.

Λήμμα 3.13. Υπάρχουν ακριβώς $\frac{p-1}{2}$ (μη-ισοδύναμα και μη-μηδενικά) τετραγωνικά υπόλοιπα (mod p) και ακριβώς $\frac{p-1}{2}$ που δεν είναι τετραγωνικά υπόλοιπα.

Λήμμα 3.14. Αν n ένα μη-τετραγωνικό υπόλοιπο (mod p), τότε το σύνολο των μη-τετραγωνικών υπολοίπων είναι το $\{nr : r \text{ μη-μηδενικό τετραγωνικό υπόλοιπο (mod } p)\}$.

Λήμμα 3.15. Αν n ένα μη-τετραγωνικό υπόλοιπο (mod p), τότε ικανοποιεί την $n \equiv \alpha^2 + \beta^2 \pmod{p}$, για κάποια $\alpha, \beta \not\equiv 0 \pmod{p}$.

Απόδειξη

Έστω n' το μικρότερο μη-τετραγωνικό υπόλοιπο (mod p). Τότε $n' = r + 1$ με r τετραγωνικό υπόλοιπο, δηλαδή $r \equiv a^2 \pmod{p}$. Τότε $n' \equiv a^2 + 1^2 \pmod{p}$ και από το Λήμμα 3.14 έχουμε ότι κάθε μη-τετραγωνικό υπόλοιπο έχει την μορφή $n'r'$ με

$r' \equiv \gamma^2 \pmod{p}$. Επομένως κάθε μη-τετραγωνικό υπόλοιπο έχει την μορφή $n \equiv (\alpha\gamma)^2 + \gamma^2 \pmod{p}$. ■

Λήμμα 3.16. Υπάρχουν $\alpha, \beta, \gamma \in \mathbb{Z}$ όχι όλοι $0 \pmod{p}$ οι οποίοι ικανοποιούν την $0 \equiv \alpha^2 + \beta^2 + \gamma^2 \pmod{p}$.

Απόδειξη

Έχουμε ότι $0 = -1 + 1^2$.

Αν το -1 είναι τετραγωνικό υπόλοιπο $\pmod{p}$ τότε $-1 \equiv a^2 \pmod{p}$ και $0 \equiv a^2 + 1^2 \pmod{p}$.

Αν το -1 δεν είναι τετραγωνικό υπόλοιπο $\pmod{p}$ τότε, από το Λήμμα 3.15 $-1 \equiv a^2 + \beta^2 \pmod{p}$ και $0 \equiv a^2 + \beta^2 + 1^2 \pmod{p}$. ■

Θεώρημα 3.17. Κάθε ρητός πρώτος p έχει μια τουλάχιστον παραγοντοποίηση σε υπερμιγαδικούς, της μορφής:

$$p = P_0 \overline{P_0}.$$

Απόδειξη

Αφού $\kappa^2 = (p - \kappa)^2 \pmod{p}$, μπορούμε να υποθέσουμε ότι οι α, β, γ του Λήμματος 3.16 είναι μικρότεροι ή ίσοι του $\frac{p}{2}$.

Άρα έχουμε ότι $\alpha^2 + \beta^2 + \gamma^2 = mp$, και αφού $\alpha, \beta, \gamma \leq \frac{p}{2}$,

$$\alpha^2 + \beta^2 + \gamma^2 \leq \left(\frac{p}{2}\right)^2 + \left(\frac{p}{2}\right)^2 + \left(\frac{p}{2}\right)^2 = \frac{3p^2}{4} < p^2.$$

Επομένως $0 < m < p$.

Παίρνουμε τώρα τον υπερμιγαδικό $Q = \alpha + \beta i + \gamma j$ με νόρμα $N(Q) = mp$.

Όπως και στην απόδειξη του θεωρήματος 3.10 από το ιδεώδες $p\mathbf{H} + Q\mathbf{H} = P_0\mathbf{H}$ συμπεραίνουμε (με όμοιο τρόπο) ότι $N(P_0) = p$.

Άρα, $P_0 \overline{P_0} = N(P_0) = p$.

Το θεώρημα ισχύει και για $p = 2$, αφού $2 = (1 + i)(1 - i)$. ■

Οι Conway–Smith αναφέρουν πως χρησιμοποιώντας μεθόδους της αναλυτικής θεωρίας αριθμών αποδεικνύεται πως το συνολικό πλήθος των αναλύσεων είναι $24(p + 1)$ αν $p > 2$ και 24 αν $p = 2$.

Πριν ολοκληρώσουμε την ενότητα μελετώντας την ανάλυση των μη–πρωταρχικών ακέραιων Hurwitz, πρέπει να ορίσουμε το τρίγωνο Catalan και τα πολώνυμα Catalan.

Το τρίγωνο Catalan δημιουργείται όπως το τρίγωνο του Pascal, χωρίς όμως το «αριστερό μέρος», και από αυτό μπορούμε να βρούμε τους συντελεστές των αντίστοιχων πολωνύμων $C_n(x)$.

C_0	1									
C_1		1								
C_2	1		1							
C_3		2		1						
C_4	2		3		1					
C_5		5		4		1				
C_6	5		9		5		1			
C_7		14		14		6		1		
C_8	14		28		20		7		1	
C_9		42		48		27		8		1

Εικόνα 3.3: Το τρίγωνο Catalan

Δίνουμε τα πρώτα πολώνυμα Catalan για να ξεκαθαρίσουμε την χρήση του τριγώνου.

$$C_0(x) = C_1(x) = 1$$

$$C_2(x) = x + 1$$

$$C_3(x) = 2x + 1$$

$$C_4(x) = 2x^2 + 3x + 1$$

$$C_5(x) = 5x^2 + 4x + 1$$

Ορισμός 3.18. Ονομάζουμε **περικομμένο (truncated)** πολυώνυμο Catalan $C_{n,s}(x)$, το πολυώνυμο που αποτελείται από τους όρους του $C_n(x)$ που έχουν βαθμό μικρότερο ή ίσο του s .

Τα περικομμένα πολυώνυμα Catalan ικανοποιούν την αναδρομική σχέση:

$$C_{n,s}(x) = C_{n-1,s}(x) + xC_{n-1,s-1}(x) \quad (3.5)$$

Έστω τώρα ακέραιος Hurwitz Q με νόρμα $N(Q)$, με ανάλυση σε πρώτους παράγοντες $N(Q) = 2^{n_0} p_1^{n_1} p_2^{n_2} \dots p_k^{n_k}$, ο οποίος διαιρείται από τον ρητό ακέραιο $2^{s_0} p_1^{s_1} p_2^{s_2} \dots p_k^{s_k}$.

(Κάθε ένας από τους εκθέτες $s_0, s_1, \dots, s_k$, είναι ο μέγιστος, ώστε το παραπάνω γινόμενο να διαιρεί τον Q .)

Θεώρημα 3.19. Το πλήθος των αναλύσεων σε πρώτους Hurwitz (με εξαίρεση τους πολλαπλασιασμούς με μονάδες) ενός μη-πρωταρχικού ακέραιου Hurwitz Q , με πρότυπο μια δεδομένη ανάλυση της $N(Q)$ σε ρητούς πρώτους είναι το γινόμενο

$$\prod_{i \geq 1} C_{n_i, s_i}(p_i)$$

των αριθμητικών τιμών των περικομμένων πολυωνύμων Catalan υπολογισμένων στους περιττούς πρώτους της ανάλυσης της $N(Q)$.

Περιγράφουμε τα βήματα της απόδειξης ακολουθώντας τους Conway–Smith.

Θα μετρήσουμε το πλήθος των αναλύσεων της μορφής

$$Q = P_1 P_2 \dots P_n$$

ενός ακέραιου Hurwitz Q με νόρμα $N(Q) = p^n$, όπου $N(P_1) = N(P_2) = \dots = N(P_n) = p$.

Υποθέτουμε ότι ο Q διαιρείται από τον p^s αλλά όχι από τον p^{s+1} , άρα $Q = p^s P$ όπου ο P είναι πρωταρχικός. Αυτό σημαίνει ότι υπάρχει μοναδική (με εξαίρεση τους πολλαπλασιασμούς με μονάδες) ανάλυση του P :

$$P = P'_1 P'_2 \dots P'_{n-2s}$$

Γνωρίζουμε ότι υπάρχουν $p+1$ υπερμιαδικοί με νόρμα p (με εξαίρεση τους πολλαπλασιασμούς με μονάδες).

Αν $P_1 = P'_1$ τότε, αφαιρώντας τον από τα αριστερά της ανάλυσης του Q μένουμε με ένα πρόβλημα ανάλυσης ενός ακέрайου Hurwitz με νόρμα p^{n-1} , ο οποίος διαιρείται από τον p^s , το οποίο επαγωγικά έχει $C_{n-1,s}(p)$ λύσεις.

Στις p στο πλήθος περιπτώσεις στις οποίες $P_1 \neq P'_1$, μένουμε με ένα πρόβλημα ανάλυσης ενός ακέрайου Hurwitz με νόρμα p^{n-1} , ο οποίος διαιρείται από τον p^{s-1} , το οποίο επαγωγικά έχει $C_{n-1,s-1}(p)$ λύσεις. Επομένως σε αυτήν την περίπτωση έχουμε $pC_{n-1,s-1}(p)$.

Αρα έχουμε συνολικά $C_{n-1,s}(p) + pC_{n-1,s-1}(p) \stackrel{(3.5)}{=} C_{n,s}(p)$ λύσεις.

Επειδή η διαδικασία αυτή γίνεται ανεξάρτητα για κάθε παράγοντα του Q με νόρμα της μορφής p^n με p περιττό πρώτο τελικά το πλήθος των λύσεων είναι:

$$\prod_{i \geq 1} C_{n_i, s_i}(p_i).$$

Ο παράγοντας του Q που έχει νόρμα 2^{n_0} , δεν επηρεάζει την καταμέτρησή μας καθώς οι ακέрайοι Hurwitz με νόρμα 2 είναι οι $u(1+i)$ όπου u μονάδα, άρα μας δίνει μια μόνο επιλογή (με εξαίρεση τους πολλαπλασιασμούς με μονάδες). ■

3.3 Τα ακέрайα οκτόνια

Στην ενότητα αυτή θα διερευνήσουμε το ερώτημα, ποια οκτόνια μπορούν να χαρακτηριστούν «ακέрайα».

Θα ακολουθήσουμε σε μεγάλο βαθμό την προσέγγιση των Conway–Smith και, για να αποφύγουμε την εισαγωγή νέων συμβολισμών, δίνουμε πρώτα αυτούς που χρησιμοποιούν στο βιβλίο τους «On Quaternions and Octonions».

3.3.1 Οι συμβολισμοί των Conway–Smith για τα οκτόνια

Οι Conway–Smith κατασκευάζουν το σύνολο των οκτονίων με τη διαδικασία που περιγράψαμε στο κεφάλαιο 2, έτσι ώστε κάθε $x \in \mathbb{O}$ να γράφεται στη μορφή:

$$x = \alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 ji + \alpha_4 l + \alpha_5 li + \alpha_6 lj + \alpha_7 l(ji): \alpha_0, \alpha_1, \dots, \alpha_7 \in \mathbb{R}$$

Αφού διαπιστώσουν ότι $ji = -k$, ορίζουν:

$$i_1 = i, \quad i_2 = j, \quad i_4 = -ji = k, \quad i_0 = l.$$

Ορίζοντας τη σχέση $i_0 i_n = i_{3n}$ (οι δείκτες $(\text{mod } 7)$), παίρνουν:

$$i_3 = i_0 i_1 = li, \quad i_6 = i_0 i_2 = lj, \quad i_5 = i_0 i_4 = lk = l(-ji) = -l(ji)$$

και τελικά γράφουν κάθε οκτόνιο στη μορφή:

$$x = \alpha_\infty + \alpha_0 i_0 + \alpha_1 i_1 + \alpha_2 i_2 + \alpha_3 i_3 + \alpha_4 i_4 + \alpha_5 i_5 + \alpha_6 i_6: \alpha_\infty, \alpha_0, \dots, \alpha_6 \in \mathbb{R}.$$

Κάθε τριάδα της μορφής $i_{n+1}, i_{n+2}, i_{n+4}$ (οι δείκτες $(\text{mod } 7)$) δημιουργεί μαζί με τη μονάδα 1, μια υποάλγεβρα που «συμπεριφέρεται» όπως οι υπερμιγαδικοί.

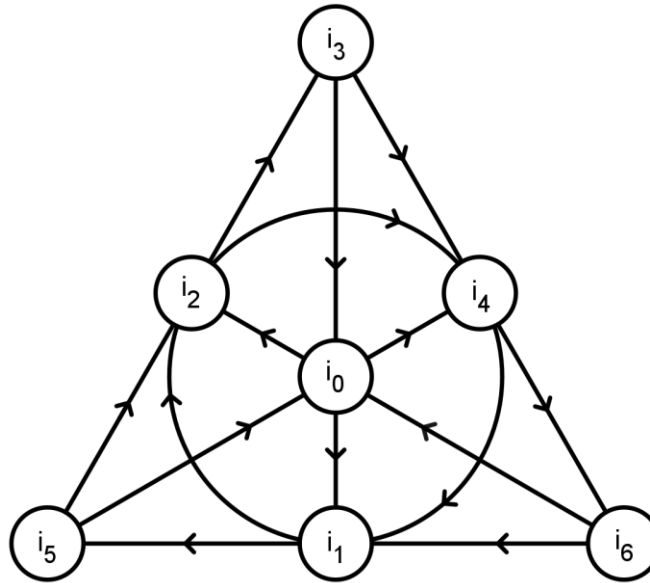
Οι αποδείξεις για τα παραπάνω παραλείπονται καθώς ξεφεύγουν από τον σκοπό της ενότητας (ο αναγνώστης μπορεί να τις βρει στο εν λόγω βιβλίο).

Τα παραπάνω μας δίνουν τον πίνακα πολλαπλασιασμού:

	1	i_0	i_1	i_2	i_3	i_4	i_5	i_6
1	1	i_0	i_1	i_2	i_3	i_4	i_5	i_6
i_0	i_0	-1	i_3	i_6	$-i_1$	i_5	$-i_4$	$-i_2$
i_1	i_1	$-i_3$	-1	i_4	i_0	$-i_2$	i_6	$-i_5$
i_2	i_2	$-i_6$	$-i_4$	-1	i_5	i_1	$-i_3$	i_0
i_3	i_3	i_1	$-i_0$	$-i_5$	-1	i_6	i_2	$-i_4$
i_4	i_4	$-i_5$	i_2	$-i_1$	$-i_6$	-1	i_0	i_3
i_5	i_5	i_4	$-i_6$	i_3	$-i_2$	$-i_0$	-1	i_1
i_6	i_6	i_2	i_5	$-i_0$	i_4	$-i_3$	$-i_1$	-1

Πίνακας 3.1: Πίνακας πολλαπλασιασμού οκτονίων «κατά τους Conway-Smith»

ο οποίος, ως συνήθως, παριστάνεται καλύτερα στο ακόλουθο διάγραμμα Fano.



Εικόνα 3.4: Διάγραμμα Fano για τον πολλαπλασιασμό οκτονίων «κατά τους Conway–Smith»

Απλή παρατήρηση στις εικόνες 1.3 και 3.4 μας δείχνει ότι, αν $\mathbb{O}'$ το σύνολο των οκτονίων που κατασκευάστηκε στην ενότητα 1.4 και $\mathbb{O}$ αυτό των Conway–Smith, η απεικόνιση:

$$f: \mathbb{O}' \rightarrow \mathbb{O}, \quad f(\alpha_\infty + \alpha_4 e_1 + \alpha_1 e_2 + \alpha_5 e_3 + \alpha_2 e_4 + \alpha_6 e_5 + \alpha_3 e_6 + \alpha_0 e_7) = \\ = \alpha_\infty + \alpha_0 i_0 + \alpha_1 i_1 + \alpha_2 i_2 + \alpha_3 i_3 + \alpha_4 i_4 + \alpha_5 i_5 + \alpha_6 i_6$$

είναι ισομορφισμός.

3.3.2 Ακέραια οκτόνια

Η έννοια του «ακέραιου» στην άλγεβρα σημαίνει συνήθως στοιχείο ενός υποδακτύλιου το οποίο ικανοποιεί μια εξίσωση της μορφής:

$$x^n + \alpha_{n-1}x^{n-1} + \dots + \alpha_0 = 0, \quad \alpha_0, \dots, \alpha_{n-1} \in \mathbb{Z}. \quad (3.6)$$

με τον υποδακτύλιο να μην περιέχεται γνήσια σε κάποιον άλλον (Dickson (1923)).

Το σύνολο των οκτονίων βέβαια δεν είναι δακτύλιος αφού ο πολλαπλασιασμός δεν είναι προσεταιριστικός, αλλά θα προσαρμόσουμε τις απαιτήσεις μας στον παρακάτω ορισμό.

Ορισμός 3.20. Ονομάζουμε **τάξη (order)** το σύνολο των στοιχείων μιας composition άλγεβρας το οποίο έχει τις ιδιότητες:

1. είναι κλειστό ως προς την αφαίρεση και τον πολλαπλασιασμό.

2. περιέχει τη μονάδα 1 της άλγεβρας.
3. κάθε στοιχείο του ικανοποιεί μια εξίσωση της μορφής (3.6).

Αν η τάξη δεν περιέχεται γνήσια σε καμία άλλη τάξη της άλγεβρας τότε θα ονομάζεται **μέγιστη τάξη (maximal order)** ή **αριθμητική (arithmetic)**. Στη συνέχεια περιορίζουμε τη μελέτη μας στον «δακτύλιο» $\mathbb{Q}(i_0, i_1, \dots, i_6)$.

Έχουμε δείξει ότι κάθε οκτόνιο $\alpha = \alpha_\infty + \alpha_0 i_0 + \alpha_1 i_1 + \alpha_2 i_2 + \alpha_3 i_3 + \alpha_4 i_4 + \alpha_5 i_5 + \alpha_6 i_6$ ικανοποιεί την εξίσωση:

$$x^2 - 2\alpha_\infty x + (\alpha_\infty^2 + \alpha_0^2 + \dots + \alpha_6^2) = 0 \quad (3.7)$$

Το παραπάνω μάλιστα μπορεί να χαρακτηριστεί ελάχιστο πολυώνυμο αφού για να ικανοποιεί μια γραμμική εξίσωση ένα οκτόνιο θα πρέπει να έχει μηδενικό φανταστικό μέρος.

Για να ανήκει λοιπόν ένα οκτόνιο σε μια τάξη θα πρέπει να απαιτήσουμε το $2\alpha_\infty$ και η νόρμα $(\alpha_\infty^2 + \alpha_0^2 + \dots + \alpha_6^2)$ να είναι συνήθεις ακέραιοι.

Μια προφανής τάξη οκτονίων είναι τα οκτόνια των οποίων όλες οι συντεταγμένες $\alpha_\infty, \dots, \alpha_6$ είναι συνήθεις ακέραιοι. Αυτά τα οκτόνια ονομάζονται **ακέραιοι Graves**, προς τιμήν του πρώτου ανθρώπου που κατασκεύασε το σύνολο των οκτονίων.

Οι μέγιστες τάξεις που ψάχνουμε λοιπόν πρέπει να περιέχουν τους ακέραιους Graves.

Παρατηρούμε ότι, για να ανήκει ένα οκτόνιο σε μια τάξη πρέπει να ισχύει:

$$2\alpha_\infty \in \mathbb{Z} \Leftrightarrow \alpha_\infty \in \frac{1}{2}\mathbb{Z}$$

Επειδή θα αναφερόμαστε συχνά σε οκτόνια των οποίων κάποιες από τις συντεταγμένες είναι της μορφής $\alpha_r = \frac{2k+1}{2}, k \in \mathbb{Z}$, (θα ονομάζουμε αυτούς τους αριθμούς **ημιακέραιους**) θα αποκαλούμε το σύνολο των δεικτών των συντεταγμένων αυτής της μορφής, **halving-σύνολο** για το οκτόνιο αυτό.

Η επόμενη πρόταση είναι σημαντική για τη συνέχεια της διερεύνησής μας.

Πρόταση 3.21. Αν ένα οκτόνιο α ανήκει σε μια τάξη που περιέχει τους ακέραιους Graves, τότε το διπλάσιο κάθε συντεταγμένης του α_r είναι ακέραιος αριθμός και το πλήθος των στοιχείων του halving-συνόλου του είναι πολλαπλάσιο του 4.

Απόδειξη

Προφανώς οι φανταστικές μονάδες ανήκουν στην τάξη του α (αφού είναι ακέραιοι Graves). Έστω τώρα ότι η συντεταγμένη $\alpha_r \notin \frac{1}{2}\mathbb{Z}$. Πολλαπλασιάζοντας το α με i_r , παίρνουμε το οκτόνιο $\alpha' = -\alpha_r + \dots$ με πραγματικό μέρος $-\alpha_r \notin \frac{1}{2}\mathbb{Z}$, που είναι άτοπο αφού η τάξη είναι κλειστή ως προς τον πολλαπλασιασμό και το διπλάσιο του πραγματικού μέρους των στοιχείων της πρέπει να είναι ακέραιος αριθμός.

Επομένως κάθε οκτόνιο που ανήκει σε μια τέτοια τάξη έχει συντεταγμένες που ανήκουν στο $\frac{1}{2}\mathbb{Z}$.

Επίσης για κάθε ημιακέραια συντεταγμένη α_r του α έχουμε ότι:

$$\alpha_r \equiv \kappa + \frac{1}{2}, \quad \kappa \in \mathbb{Z} \Rightarrow \alpha_r \equiv \frac{1}{2} \pmod{1} \Rightarrow \alpha_r^2 \equiv \frac{1}{4} \pmod{1}.$$

Για κάθε ακέραια συντεταγμένη α_r του α έχουμε ότι:

$$\alpha_r \equiv 0 \pmod{1} \Rightarrow \alpha_r^2 \equiv 0 \pmod{1}.$$

Αν λοιπόν το πλήθος των ημιακέραιων συντεταγμένων είναι m , τότε ισχύει:

$$\alpha_\infty^2 + \alpha_0^2 + \dots + \alpha_6^2 \equiv \frac{m}{4} \pmod{1}$$

Όμως $\alpha_\infty^2 + \alpha_0^2 + \dots + \alpha_6^2 \in \mathbb{Z}$, άρα m πολλαπλάσιο του 4. ■

Επομένως το halving-σύνολο ενός ακέραιου οκτονίου έχει 0, 4 ή 8 στοιχεία.

Αν το ακέραιο οκτόνιο είναι ακέραιος Graves θα λέμε ότι το halving-σύνολό του είναι το κενό σύνολο $\emptyset$.

Αν και οι 8 συντεταγμένες του ακέραιου οκτονίου είναι ημιακέραιες, τότε θα λέμε ότι το halving-σύνολό του είναι το Ω .

Τα οκτόνια που είναι είτε ακέραιοι Graves είτε με όλες τις συντεταγμένες τους ημιακέραιες, θα τα ονομάζουμε **οκτόνια Klein**.

Σε ό,τι αφορά τα ακέραια οκτόνια με μέγεθος halving-συνόλου 4, για ακέραια οκτόνια με halving-σύνολο $\{\alpha, \beta, \gamma, \delta\}$ (αβγδ στο εξής) θα χρησιμοποιούμε τον συμβολισμό:

$$i_{\alpha\beta\gamma\delta} \text{ για το } \frac{1}{2}(i_{\alpha} + i_{\beta} + i_{\gamma} + i_{\delta}) \text{ και } i_{\alpha\bar{\beta}\gamma\bar{\delta}} \text{ για το } \frac{1}{2}(i_{\alpha} - i_{\beta} + i_{\gamma} - i_{\delta})$$

Στον παραπάνω συμβολισμό με i_{∞} θα εννοούμε τη μονάδα 1.

Σύμφωνα με τους Conway–Smith, ο Kirmse το 1925 υπέθεσε ότι τα οκτόνια με halving–σύνολο το $\emptyset$ ή το Ω ή μια από τις τετράδες που σχηματίζουν υπερμιγαδικές υποάλγεβρες στο σύνολο των οκτονίων όπως φαίνεται στον παρακάτω πίνακα :

$\infty 124$	0356
$\infty 235$	1460
$\infty 346$	2501
$\infty 450$	3612
$\infty 561$	4023
$\infty 602$	5134
$\infty 013$	6245
$\emptyset$	Ω
∞ – σύνολα	

Πίνακας 3.2: Πίνακας των ∞ –συνόλων (από τους Conway–Smith)

είναι μια μέγιστη τάξη.

Όμως αυτό δεν ισχύει αφού το σύνολο αυτό (θα ονομάζεται στο εξής ∞ –ακέραιοι) δεν είναι κλειστό ως προς τον πολλαπλασιασμό αφού:

$$i_{\infty 026} i_{\infty 013} = \frac{1}{2}(i_{\infty} + i_0 + i_2 + i_6) \frac{1}{2}(i_{\infty} + i_0 + i_1 + i_3) = \frac{1}{2}(i_0 + i_2 + i_3 + i_5) = i_{0235}.$$

Αυτή μάλιστα η λανθασμένη υπόθεση είναι πια γνωστή ως «λάθος του Kirmse».

Ο πίνακας 3.2 ορίζει και τους ∞ –ακέραιους. Σε κάθε κελί εμφανίζεται το halving–σύνολο που μπορεί να έχει ένα στοιχείο τους.

Για παράδειγμα ο $\alpha = \frac{1}{2}(i_{\infty} + i_0 + i_2 + i_6) + (i_1 + i_3 + i_4 + i_5)$ είναι ∞ –ακέραιος.

Αργότερα ο Dickson ανακάλυψε πώς να διορθώσει το λάθος του Kirmse και η εργασία του στα ακέραια οκτόνια συμπληρώθηκε από τον Bruck.

Ορίζουμε τα n –σύνολα και τους αντίστοιχους n –ακέραιους εναλλάσσοντας στα ∞ –σύνολα το ∞ με το n , όπως φαίνεται στον παρακάτω πίνακα.

∞124	0356	0124	∞356	∞124	0356	∞124	0356
∞235	1460	0235	146∞	1235	∞460	∞235	1460
∞346	2501	0346	25∞1	1346	250∞	2346	∞501
∞450	3612	∞450	3612	1450	36∞2	2450	361∞
∞561	4023	0561	4∞23	∞561	4023	2561	40∞3
∞602	5134	∞602	5134	1602	5∞34	∞602	5134
∞013	6245	∞013	6245	∞013	6245	2013	6∞45
∅	Ω	∅	Ω	∅	Ω	∅	Ω
∞ – σύνολα		0 – σύνολα		1 – σύνολα		2 – σύνολα	

3124	0∞56	∞124	0356	5124	03∞6	6124	035∞
∞235	1460	4235	1∞60	∞235	1460	6235	14∞0
∞346	2501	∞346	2501	5346	2∞01	∞346	2501
3450	∞612	∞450	3612	∞450	3612	6450	3∞12
3561	402∞	4561	∞023	∞561	4023	∞561	4023
3602	51∞4	4602	513∞	5602	∞134	∞602	5134
∞013	6245	4013	62∞5	5013	624∞	6013	∞245
∅	Ω	∅	Ω	∅	Ω	∅	Ω
3 – σύνολα		4 – σύνολα		5 – σύνολα		6 – σύνολα	

Πίνακας 3.3: Πίνακας των n -συνόλων (από τους Conway–Smith)

Τα σύνολα των n -ακέραιων περιέχουν τη μονάδα και τα στοιχεία τους ικανοποιούν την εξίσωση (3.7).

Λήμμα 3.22. Το σύνολο των n -ακέραιων $\mathbf{O}_n$ είναι κλειστό ως προς την αφαίρεση για $n = 0, 1, \dots, 6$.

Απόδειξη

Οι επτά δομές των n -ακέραιων είναι ισομορφικές.

Αρκεί να παρατηρήσουμε ότι η απεικόνιση $n \mapsto n + k \pmod{7}$, απεικονίζει κάθε n -σύνολο σε ακριβώς ένα $n + k$ -σύνολο. Επίσης από το διάγραμμα Fano της εικόνας 3.4 μπορούμε να δούμε ότι οι προσανατολισμένες τριάδες είναι της μορφής:

$$(i_{n+1}, i_{n+2}, i_{n+4}) \pmod{7}, \quad n = 0, \dots, 6$$

και η απεικόνιση $n \mapsto n + k \pmod{7}$ είναι αυτομορφισμός αφού απεικονίζει κάθε μια από αυτές στην τριάδα $(i_{n+k+1}, i_{n+k+2}, i_{n+k+4}) \pmod{7}$, $n, k = 0, \dots, 6$ η οποία είναι της ίδιας μορφής.

Άρα θα αποδείξουμε την πρόταση μόνο για τους 0-ακέραιους.

Αρκεί να παρατηρήσουμε ότι, αγνοώντας τα πρόσημα, $i_A - i_B = i_{A \Delta B}$, όπου $A \Delta B$ η συμμετρική διαφορά των A και B . Αν $A = \emptyset$ τότε $A \Delta B = B$, αν $A = \Omega$ τότε $A \Delta B = B^c$, αν $A = B^c$ τότε $A \Delta B = \Omega$, ενώ στις υπόλοιπες περιπτώσεις αρκεί να παρατηρήσουμε από τον πίνακα 3.3 ότι οι συμμετρικές διαφορές όλων των υπόλοιπων ζευγών 0-συνόλων, ανήκουν στα 0-σύνολα.

Αυτό ισχύει σε όλα τα n σύνολα για $n = 0, 1, \dots, 6$. ■

Η επόμενη πρόταση μετατρέπει τα 0-σύνολα σε τάξεις.

Πρόταση 3.23. Το σύνολο των n -ακέραιων $\mathbf{O}_n$ είναι κλειστό ως προς τον πολλαπλασιασμό για $n = 0, 1, \dots, 6$.

Απόδειξη

Θα αποδείξουμε την πρόταση μόνο για τους 0-ακέραιους.

Άμεσοι υπολογισμοί δίνουν τους παρακάτω πίνακες πολλαπλασιασμού:

	$i_{\infty 356}$	i_{0235}	i_{0463}	i_{0156}
$i_{\infty 356}$	$i_{\infty 356}$	$i_{\infty 234}$	$i_{\infty 461}$	$i_{\infty 152}$
i_{0235}	$i_{\infty 045}$	-1	$i_{\infty 125}$	$i_{\infty 416}$
i_{0463}	$i_{\infty 013}$	$i_{\infty 125}$	-1	$i_{\infty 243}$
i_{0156}	$i_{\infty 026}$	$i_{\infty 416}$	$i_{\infty 243}$	-1

Πίνακας 3.4: Πίνακας πολλαπλασιασμού των $i_{\infty 356}, i_{0235}, i_{0463}, i_{0156}$

και

	1	i_0	i_1	i_2	i_3	i_4	i_5	i_6
$i_{\infty 356}$	$i_{\infty 356}$	i_{0142}	$i_{1\overline{065}}$	$i_{2\overline{530}}$	$i_{3\overline{\infty 24}}$	$i_{4\overline{603}}$	$i_{5\overline{2\infty 1}}$	$i_{6\overline{41\infty}}$
i_{0235}	i_{0235}	$i_{\overline{\infty 614}}$	$i_{3\overline{406}}$	$i_{6\overline{\infty 53}}$	$i_{\overline{15\infty 2}}$	$i_{5\overline{160}}$	$i_{\overline{432\infty}}$	$i_{\overline{2041}}$
i_{0463}	i_{0463}	$i_{\overline{\infty 521}}$	$i_{3\overline{250}}$	$i_{6\overline{105}}$	$i_{\overline{164\infty}}$	$i_{5\overline{\infty 36}}$	$i_{\overline{4012}}$	$i_{\overline{23\infty 4}}$
i_{0156}	i_{0156}	$i_{\overline{\infty 342}}$	$i_{3\overline{\infty 65}}$	$i_{6\overline{430}}$	$i_{\overline{1024}}$	$i_{5\overline{203}}$	$i_{\overline{46\infty 1}}$	$i_{\overline{251\infty}}$

Πίνακας 3.5: Πίνακας πολλαπλασιασμού των $i_{\infty 356}, i_{0235}, i_{0463}, i_{0156}$ με τη βάση των οκτονίων

Παρατηρούμε ότι αν θέσουμε

$$p_1 = i_{\infty 356}, \quad p_2 = i_{0235}, \quad p_3 = i_{0463}, \quad p_4 = i_{0156}$$

Έχουμε:

$$p_1 + p_2 = i_{\infty 356} + i_{0235} = i_{\infty 026}$$

$$p_1 + p_3 = i_{\infty 356} + i_{0463} = i_{\infty 045}$$

$$p_1 + p_4 = i_{\infty 356} + i_{0156} = i_{\infty 013}$$

$$p_2 + p_3 = i_{0235} + i_{0463} = i_{2456}$$

$$p_2 + p_4 = i_{0235} + i_{0156} = i_{1236}$$

$$p_3 + p_4 = i_{0463} + i_{0156} = i_{1345}$$

$$p_1 + p_2 + p_3 = i_{\infty 026} + i_{0463} = i_{\infty 234}$$

$$p_1 + p_2 + p_4 = i_{\infty 026} + i_{0156} = i_{\infty 125}$$

$$p_1 + p_3 + p_4 = i_{\infty 045} + i_{0156} = i_{\infty 146}$$

$$p_2 + p_3 + p_4 = i_{2456} + i_{0156} = i_{0124}$$

$$p_1 + p_2 + p_3 + p_4 = i_{\infty 026} + i_{1345} = i_{\Omega}$$

Παρατηρούμε ότι για κάθε 0-σύνολο ο αντιπρόσωπός του γράφεται σαν άθροισμα των p_1, p_2, p_3, p_4 .

Κάθε 0-ακέραιος α , με halving-σύνολο $A \neq \emptyset$ γράφεται ως:

$$\alpha = g + i_A = g + \alpha_1 p_1 + \alpha_2 p_2 + \alpha_3 p_3 + \alpha_4 p_4, \quad \alpha_i \in \{0,1\}, i = 1, \dots, 4$$

όπου g ακέραιος Graves και $\alpha_i, i = 1, \dots, 4$ όχι όλοι μηδέν.

Επομένως κάθε 0-ακέραιος γράφεται ως:

$$\alpha = g + \alpha_1 p_1 + \alpha_2 p_2 + \alpha_3 p_3 + \alpha_4 p_4, \quad \alpha_i \in \{0,1\}, i = 1, \dots, 4, \quad g \text{ ακέραιος Graves.}$$

Έστω τώρα δύο 0-ακέραιοι,

$$\alpha = g + \alpha_1 p_1 + \alpha_2 p_2 + \alpha_3 p_3 + \alpha_4 p_4 \text{ και}$$

$$\beta = g' + \beta_1 p_1 + \beta_2 p_2 + \beta_3 p_3 + \beta_4 p_4, \quad \alpha_i, \beta_i \in \{0,1\}, \quad i = 1, \dots, 4$$

Παρατηρούμε ότι στο γινόμενο τους $\alpha\beta$ υπάρχουν μόνο όροι της μορφής:

$$(gg'), (g'g), (gp_i), (p_i g), (p_i p_j), \quad i, j = 1, \dots, 4.$$

Το γινόμενο δύο ακέραιων Graves είναι προφανώς 0-ακέραιος και ο πίνακας 3.4 μας δίνει ότι το ίδιο ισχύει και για τα γινόμενα $(p_i p_j)$.

Επομένως, για να δείξουμε ότι το γινόμενο $\alpha\beta$ είναι 0-ακέραιος αρκεί να αποδείξουμε ότι τα γινόμενα $(gp_i), (p_i g), i, j = 1, \dots, 4$, είναι 0-ακέραιοι.

$$\text{Για κάθε ακέραιο Graves } g = \alpha_\infty + \alpha_0 i_0 + \alpha_1 i_1 + \alpha_2 i_2 + \alpha_3 i_3 + \alpha_4 i_4 + \alpha_5 i_5 + \alpha_6 i_6$$

με $\alpha_\infty, \alpha_0, \dots, \alpha_6 \in \mathbb{Z}$.

Για $i = 1, \dots, 4$ έχουμε:

$$p_i g = p_i(\alpha_\infty + \alpha_0 i_0 + \alpha_1 i_1 + \alpha_2 i_2 + \alpha_3 i_3 + \alpha_4 i_4 + \alpha_5 i_5 + \alpha_6 i_6)$$

$$= p_i \alpha_\infty + \alpha_0 p_i i_0 + \alpha_1 p_i i_1 + \alpha_2 p_i i_2 + \alpha_3 p_i i_3 + \alpha_4 p_i i_4 + \alpha_5 p_i i_5 + \alpha_6 p_i i_6$$

Από τον πίνακα 3.5 παρατηρούμε ότι τα γινόμενα που εμφανίζονται σε όλους τους όρους είναι 0-ακέραιοι για $i = 1, \dots, 4$, επομένως τα γινόμενα $p_i g$ είναι 0-ακέραιοι για $i = 1, \dots, 4$.

Για τα γινόμενα gp_i ισχύει το ίδιο επιχείρημα καθώς ο αντίστοιχος του πίνακα 3.5 για τα γινόμενα gp_i παράγει τα ίδια αποτελέσματα αλλάζοντας μόνο κάποιες από τις παύλες στους δείκτες. ■

Δείξαμε λοιπόν ότι οι n -ακέραιοι είναι τάξεις.

Πριν δώσουμε το σχήμα που θα μας καθοδηγήσει να αποδείξουμε ότι είναι μέγιστες τάξεις δίνουμε την παρακάτω πρόταση.

Λήμμα 3.24. Η τομή δύο τάξεων είναι τάξη.

Απόδειξη

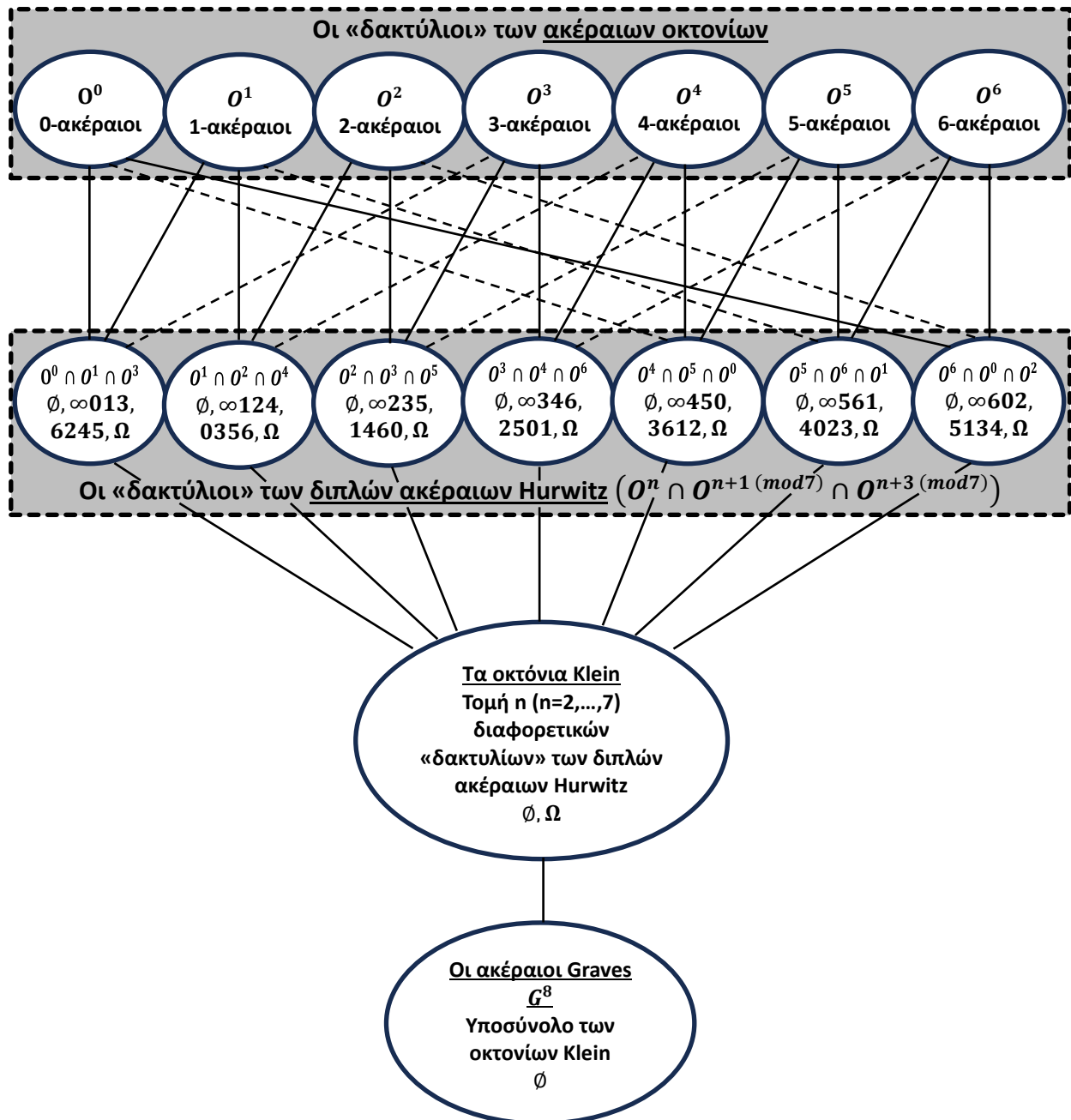
Αν $\mathbf{O}_1, \mathbf{O}_2$ τάξεις μιας άλγεβρας τότε $1 \in \mathbf{O}_1$ και $1 \in \mathbf{O}_2$ επομένως $1 \in \mathbf{O}_1 \cap \mathbf{O}_2$.

Αν $x \in \mathbf{O}_1 \cap \mathbf{O}_2$ τότε $x \in \mathbf{O}_1$ επομένως ικανοποιεί την (3.6).

Αν $x, y \in \mathbf{O}_1 \cap \mathbf{O}_2$ τότε $x, y \in \mathbf{O}_1$ άρα $x - y, xy, yx \in \mathbf{O}_1$ και $x, y \in \mathbf{O}_2$ άρα

$x - y, xy, yx \in \mathbf{O}_2$ επομένως $x - y, xy, yx \in \mathbf{O}_1 \cap \mathbf{O}_2$. ■

Στο παρακάτω σχήμα φαίνονται οι 16 τάξεις που περιέχουν τους ακέριους Graves.



Εικόνα 3.5: Οι 16 τάξεις που περιέχουν τους ακέριους του Graves, G^8 (προσαρμογή από τους Conway–Smith)

Από το παραπάνω σχήμα βλέπουμε ότι η τομές συγκεκριμένων ζευγών (ή τριάδων) των $\mathbf{O}_n$ παράγουν τα επτά συστήματα των «διπλών ακέραιων Hurwitz». Οι Conway–Smith αναφέρουν ότι καθένα από αυτά παράγεται εφαρμόζοντας τον διπλασιασμό Cayley–Dickson σε έναν δακτύλιο ακέραιων Hurwitz.

Η τομή όλων των $\mathbf{O}_n$ ή δύο οποιωνδήποτε συστημάτων διπλών ακέραιων Hurwitz μας δίνει τα οκτόνια (ή ακέрайους) Klein, οι οποίοι προκύπτουν από τους ακέрайους Graves, με την προσθήκη του $\frac{1}{2}(1 + i_0 + \dots + i_6)$.

Οι επόμενες προτάσεις θα μας επιτρέψουν να αποδείξουμε ότι, όπως υπονοεί η εικόνα 3.5, οι n –ακέрайοι είναι μέγιστες τάξεις.

Ορισμός 3.25. Ονομάζουμε **εσωτερικό** ένα halving–σύνολο των n –συνόλων που ανήκει και στα ∞ –σύνολα. Αλλιώς το ονομάζουμε **εξωτερικό**.

Από τον πίνακα 3.3 παρατηρούμε ότι:

Λήμμα 3.26. Κάθε εσωτερικό n –σύνολο είναι συμμετρική διαφορά δύο εξωτερικών n –συνόλων για $n = 0, 1, \dots, 6$ (και ο αντιπρόσωπος κάθε εσωτερικού συνόλου είναι το άθροισμα των αντιπροσώπων δύο εξωτερικών).

Λήμμα 3.27. Οι ακέрайοι Graves και ένα οκτόνιο α του οποίου το halving–σύνολο είναι ένα εξωτερικό n –σύνολο παράγουν όλους τους n –ακέрайους.

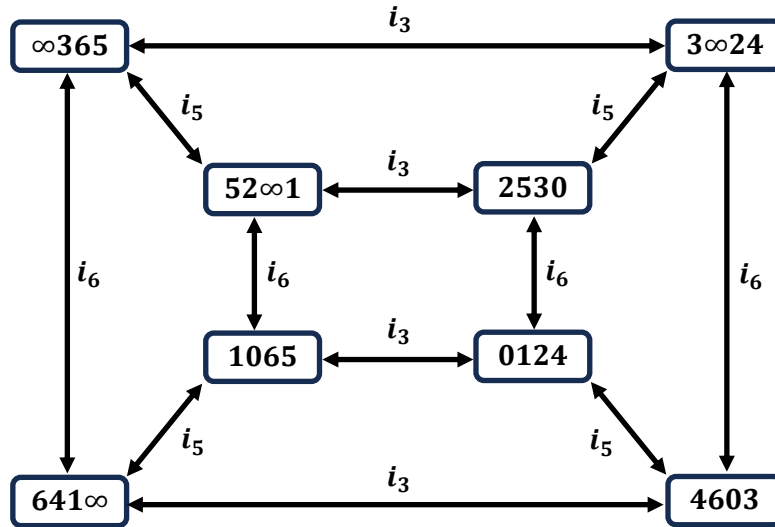
Απόδειξη

Θα αποδείξουμε την πρόταση για τους 0–ακέрайους. Αν το halving–σύνολο του α είναι το κλμν, τότε αφαιρώντας κατάλληλο ακέрайο Graves παίρνουμε το οκτόνιο

$$\alpha' = \frac{1}{2}(i_\kappa + i_\lambda + i_\mu + i_\nu) = i_{\kappa\lambda\mu\nu}$$

Πολλαπλασιάζοντας τώρα με κατάλληλες φανταστικές μονάδες (που ανήκουν στους ακέрайους Graves) παίρνουμε και τα 8 εξωτερικά 0–σύνολα.

Στο επόμενο σχήμα δείχνουμε πως γίνεται η διαδικασία, αγνοώντας τα πρόσημα αφού μας ενδιαφέρουν μόνο τα halving–σύνολα.



Εικόνα 3.6: Τα 8 εξωτερικά 0–σύνολα παράγονται από ένα, με πολλαπλασιασμούς με i_3 , i_5 ή i_6 (προσαρμογή από τους Conway–Smith).

Από το Λήμμα 3.26 έχουμε ότι κάθε εσωτερικό 0 σύνολο είναι το άθροισμα δύο εξωτερικών, επομένως τα οκτόνια με halving–σύνολα αυτά της εικόνας 3.6 παράγουν προσθετικά τους 0–ακέραιους. ■

Σε ό,τι αφορά τα εσωτερικά n –σύνολα ισχύει η παρακάτω πρόταση:

Λήμμα 3.28. Αν μια τάξη περιέχει τους ακέραιους Graves και

- δύο ακέραια οκτόνια με halving–σύνολα τα οποία είναι συμπληρωματικά ∞ –σύνολα τεσσάρων στοιχείων, τότε κάθε ένα από αυτά παράγει το άλλο.
- δύο ακέραια οκτόνια με halving–σύνολα τα οποία είναι διαφορετικά, μη συμπληρωματικά ∞ –σύνολα τεσσάρων στοιχείων, τότε αυτά παράγουν τους n –ακέραιους για κάποιο n .

Απόδειξη

Θα αποδείξουμε την πρόταση για τους 0–ακέραιους.

- Μπορούμε να δούμε ότι ο πολλαπλασιασμός του i_A με μια φανταστική μονάδα i_k , όπου $k \notin A$, μας δίνει το i_{A^c} (αγνοώντας τα πρόσημα).

Για παράδειγμα, $i_0 \frac{1}{2} (1 + i_1 + i_2 + i_4) = \frac{1}{2} (i_0 + i_3 + i_6 + i_5)$.

- Από το α. βλέπουμε ότι μπορούμε να υποθέσουμε ότι και τα δύο σύνολα περιέχουν το ∞ (αν όχι αντικαθιστούμε όποιο χρειάζεται με το συμπλήρωμά του).

Από τον πίνακα 3.3 παρατηρούμε ότι το ένα από αυτά μπορεί να προκύψει από το άλλο προσθέτοντας στους δείκτες 1, 2, ή 4 (mod 7).

Στο διάγραμμα Fano της εικόνας 3.4, παρατηρούμε ότι αν διπλασιάσουμε τους δείκτες των φανταστικών μονάδων (mod 7) προκύπτει διάγραμμα Fano ισοδύναμο με το αρχικό, άρα ο διπλασιασμός των δεικτών των μονάδων (mod 7) είναι αυτομορφισμός στο σύνολο των οκτονίων.

Αν οι δείκτες μας διαφέρουν κατά 2 ή 4, εφαρμόζοντας δύο ή μια φορά αντίστοιχα διπλασιασμό δεικτών παίρνουμε σύνολα των οποίων οι δείκτες διαφέρουν κατά 1.

Επομένως χρειάζεται να εξετάσουμε μόνο αυτήν την περίπτωση.

Έχουμε δείξει ότι η απεικόνιση $n \mapsto n + t \pmod{7}$ είναι αυτομορφισμός αφού δίνει τριάδες της ίδιας μορφής.

Άρα μπορούμε να εξετάσουμε μόνο την περίπτωση που τα halving-σύνολα είναι τα $\infty 602$ και $\infty 013$. Όπως έχουμε δει $i_{\infty 602} i_{\infty 013} = i_{0235}$, το οποίο έχει halving-σύνολο ένα εξωτερικό 0-σύνολο και το συμπέρασμά μας προκύπτει από το Λήμμα 3.27. ■

Στο παρακάτω σχήμα δείχνουμε ζεύγη οκτονίων της περίπτωσης β, τα οποία παράγουν τα σύνολα n-ακέραιων για $n = 0, \dots, 6$.

0^0	$\infty 013 - 6245$	$\infty 450 - 3612$	$\infty 602 - 5134$
0^1	$\infty 013 - 6245$	$\infty 124 - 0356$	$\infty 561 - 4023$
0^2	$\infty 124 - 0356$	$\infty 235 - 1460$	$\infty 602 - 5134$
0^3	$\infty 013 - 6245$	$\infty 235 - 1460$	$\infty 346 - 2501$
0^4	$\infty 124 - 0356$	$\infty 346 - 2501$	$\infty 450 - 3612$
0^5	$\infty 235 - 1460$	$\infty 450 - 3612$	$\infty 561 - 4023$
0^6	$\infty 346 - 2501$	$\infty 561 - 4023$	$\infty 602 - 5134$

Εικόνα 3.7: Παραγωγή των n-ακέραιων σύμφωνα με το Λήμμα 3.28β (προσαρμογή από τους Conway-Smith)

Στο σχήμα, κάθε παραλληλόγραμμο («σημείο») παριστάνει ένα οκτόνιο με halving-σύνολο ένα από αυτά του παραλληλογράμμου (είναι συμπληρωματικά). Το γινόμενο δύο «σημείων» της ίδιας γραμμής παράγει το αντίστοιχο σύνολο των n -ακέραιων.

Φτάσαμε στον τελικό στόχο της ενότητας που είναι το παρακάτω θεώρημα.

Θεώρημα 3.29. Οι τάξεις που περιέχουν τους ακέραιους Graves είναι τα 16 συστήματα ακέραιων της εικόνας 3.5 και μόνο αυτά.

Απόδειξη

Αν η τάξη δεν είναι οι ακέραιοι Graves ή οι ακέραιοι Klein τότε πρέπει να περιέχει τουλάχιστον ένα οκτόνιο με halving-σύνολο μεγέθους 4 άρα από την απόδειξη του Λήμματος 3.28α και ένα οκτόνιο με halving-σύνολο το συμπληρωματικό του. Επίσης πρέπει να περιέχει και οκτόνια με halving-σύνολο το Ω (αφού πρέπει να είναι κλειστή ως προς την πρόσθεση).

Αν δεν περιέχει άλλης μορφής οκτόνια τότε είναι μια από τις τάξεις των διπλών ακέραιων Hurwitz.

Αν περιέχει και άλλο οκτόνιο, αυτό θα είναι ή εξωτερικό ή εσωτερικό, διαφορετικό από αυτό που περιέχει η τάξη Hurwitz.

Και στις δύο περιπτώσεις, από τα Λήμματα 3.27 και 3.28 η τάξη περιέχει τους n -ακέραιους για κάποιο $n = 0, \dots, 6$.

Αν υπήρχε μια μεγαλύτερη τάξη Λ , τότε αυτή θα έπρεπε να περιέχει μία τουλάχιστον τάξη n -ακεραίων και ένα ακέραιο οκτόνιο x από μια τάξη l -ακεραίων ($l \neq n$) με halving-σύνολο 4 στοιχείων που δεν είναι n -σύνολο.

Αν το halving-σύνολο του x είναι εξωτερικό τότε, λόγω του Λήμματος 3.27 η τάξη Λ περιέχει και τους l -ακέραιους.

Από τον Πίνακα 3.3 μπορούμε να δούμε ότι η τομή δύο οποιωνδήποτε τάξεων n -ακεραίων περιέχει τουλάχιστον ένα εσωτερικό halving-σύνολο A και το συμπλήρωμά του A^c .

Αν το halving-σύνολο του x είναι εσωτερικό τότε είναι διαφορετικό από το A και το A^c . Τότε λόγω του Λήμματος 3.28 β η τάξη Λ περιέχει και μια τάξη m -ακεραίων για ($n \neq m$).

Επιλέγοντας όμως κατάλληλα στοιχεία από κάθε τάξη των n -ακεραίων όπως βλέπουμε στον παρακάτω πίνακα διαπιστώνουμε ότι κάθε ζεύγος τάξεων n -ακεραίων περιέχει στοιχεία των

οποίων το γινόμενο δεν είναι ακέραιο οκτόνιο (ενδεικτικά σημειώνουμε στον πίνακα την πρώτη από τις συντεταγμένες των γινομένων που δεν είναι ακέραιες ούτε ημιακέραιες).

		O^0	O^1	O^2	O^3	O^4	O^5	O^6
		i_{0124}	i_{1235}	i_{2346}	i_{3124}	i_{4235}	i_{5124}	i_{6124}
O^0	i_{0124}		$\frac{1}{4}i_2$	$-\frac{1}{4}i_1$	$-\frac{3}{4}i_\infty$	$-\frac{1}{4}i_1$	$-\frac{3}{4}i_\infty$	$-\frac{3}{4}i_\infty$
O^1	i_{1235}			$\frac{1}{4}i_0$	$-\frac{3}{4}i_\infty$	$-\frac{3}{4}i_\infty$	$-\frac{3}{4}i_\infty$	$-\frac{1}{4}i_0$
O^2	i_{2346}				$-\frac{3}{4}i_\infty$	$-\frac{3}{4}i_\infty$	$-\frac{1}{4}i_0$	$-\frac{3}{4}i_\infty$
O^3	i_{3124}					$-\frac{3}{4}i_\infty$	$-\frac{3}{4}i_\infty$	$-\frac{3}{4}i_\infty$
O^4	i_{4235}						$-\frac{3}{4}i_\infty$	$-\frac{1}{4}i_0$
O^5	i_{5124}							$-\frac{3}{4}i_\infty$

Από τα παραπάνω διαπιστώνουμε ότι η τάξη Λ δεν μπορεί να περιέχει δύο διαφορετικές τάξεις n –ακεραίων.

Επομένως οι τάξεις των n –ακεραίων O_n είναι μέγιστες για $n = 0, \dots, 6$.

Ορίσαμε λοιπόν τα ακέραια οκτόνια να είναι ακριβώς οι τάξεις των n –ακεραίων. Αφού αυτές είναι ισομορφικές, στη συνέχεια θα ονομάζουμε ακέραιο οκτόνιο ένα O –ακέραιο.

3.4 Ανάλυση των ακέραιων οκτονίων σε παράγοντες

Στην ενότητα αυτή θα υπολογίσουμε το πλήθος των αναλύσεων ενός ακέραιου οκτονίου σε παράγοντες. Θα ονομάζουμε ακέραια οκτόνια τους O –ακέραιους και θα τους συμβολίζουμε με O^8 .

3.4.1 Διαίρεση «με μικρό υπόλοιπο» και ιδεώδη στα ακέραια οκτόνια

Στην ενότητα 3.2 δώσαμε τα θεωρήματα για την ανάλυση των ακέραιων Hurwitz, αφού πρώτα αποδείξαμε ότι ορίζεται σε αυτούς διαίρεση με μικρό υπόλοιπο, άρα όλα τα αριστερά ή δεξιά ιδεώδη τους είναι κύρια.

Ακολουθώντας την ίδια προσέγγιση και για τα ακέραια οκτόνια δίνουμε μερικούς γεωμετρικούς ορισμούς, που θα μας χρειαστούν για να δείξουμε ότι μπορούμε να ορίσουμε διαίρεση «με μικρό υπόλοιπο».

Ορισμός 3.30. Ονομάζουμε n -διάστατο **κανονικό simplex** την κυρτή θήκη $n + 1$ σημείων, τα οποία ισαπέχουν ανά δύο. Το n -διάστατο **πλέγμα simplex** A_n (**simplex lattice** A_n), παράγεται από τα διανύσματα των ακμών ενός τέτοιου simplex.

Αν θεωρήσουμε ότι οι κορυφές του simplex έχουν διάνυσμα θέσης:

$$u_i = (0, 0, \dots, \underbrace{1}_i, \dots, 0, 0)$$

στον χώρο των $n + 1$ διαστάσεων, τότε τα διανύσματα που παράγουν το πλέγμα στον χώρο A_n είναι:

$$u_i - u_j = (0, 0, \dots, \underbrace{1}_i, \dots, \underbrace{-1}_j, \dots, 0, 0).$$

Από τα παραπάνω, μπορούμε να ορίσουμε το πλέγμα A_n , ως το σύνολο των διανυσμάτων $(x_0, \dots, x_n)$, τα οποία έχουν ακέραιες συντεταγμένες με άθροισμα 0.

Παραδείγματα simplex είναι το τρίγωνο (2-simplex) και το τετράεδρο (3-simplex).

Ορισμός 3.31. Ονομάζουμε n -διάστατο **σταυρωτό πολύτοπο** ή **κανονικό orthoplex** (**regular orthoplex**, ονομασία που προτείνεται από τους Conway–Smith) την κυρτή θήκη των σημείων με διανύσματα θέσης αυτά της ορθοκανονικής βάσης του $\mathbb{R}^n$ ή τα αντίθετά τους. Το n -διάστατο **πλέγμα orthoplex** D_n παράγεται από τα διανύσματα των ακμών του n -διάστατου σταυρωτού πολύτοπου.

Οι κορυφές λοιπόν του σταυρωτού πολύτοπου έχουν τα σημεία του $\mathbb{R}^n$ με διάνυσμα θέσης:

$$u_i = (0, 0, \dots, \underbrace{1}_i, \dots, 0, 0) \text{ ή } \overline{u_i} = (0, 0, \dots, \underbrace{-1}_i, \dots, 0, 0)$$

ενώ τα διανύσματα που παράγουν το D_n , είναι τα διανύσματα:

$$\left(0, 0, \dots, \underbrace{\pm 1}_i, \dots, \underbrace{\pm 1}_j, \dots, 0, 0 \right), \quad i, j = 1, \dots, n, \quad i \neq j.$$

Το πλέγμα D_n λοιπόν είναι το σύνολο των διανυσμάτων $(x_1, \dots, x_n)$ με ακέραιες συντεταγμένες οι οποίες έχουν άθροισμα $0 \pmod{2}$.

Παραδείγματα σταυρωτών πολύτοπων είναι, το τετράγωνο στις 2 διαστάσεις και το οκτάεδρο στις 3.

Ορισμός 3.32. Ονομάζουμε **κέντρο** ενός simplex ή ενός σταυρωτού πολύτοπου το βαρύκεντρο των κορυφών του.

Παρατηρούμε ότι τα σημεία ενός κανονικού simplex ή ενός κανονικού σταυρωτού πολύτοπου με την μέγιστη απόσταση από το κέντρο τους είναι οι κορυφές.

Αυτές οι μέγιστες αποστάσεις είναι $\frac{2\sqrt{2}}{3}$ και 1 για τα (διάστασης 8) S και O αντίστοιχα, όπως αυτά ορίστηκαν παραπάνω.

Στο εξής θα αναφερόμαστε στα κανονικά simplex και στα κανονικά σταυρωτά πολύτοπα όπως αυτά ορίστηκαν παραπάνω χρησιμοποιώντας τους όρους simplex και σταυρωτό πολύτοπο και συμβολίζοντας με S και O , αντίστοιχα.

Ορισμός 3.33. Ονομάζουμε **πλέγμα E_8** το πλέγμα $\langle S, O \rangle$, το οποίο παράγεται από τα διανύσματα με άκρα τις κορυφές ενός simplex S (διάστασης 8) και ενός σταυρωτού πολύτοπου O , το οποίο έχει μια κοινή 7-έδρα με το S .

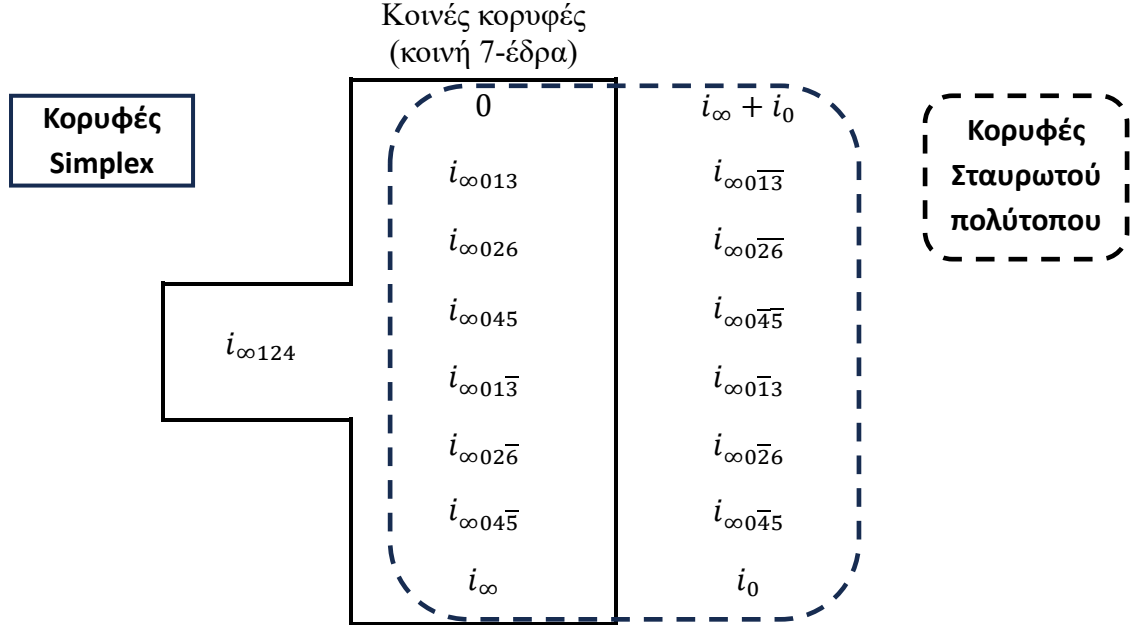
Τα πλέγματα A_8 και D_8 περιέχονται στο E_8 . Ο $\mathbb{R}^8$ καλύπτεται από 8-simplex και 8-διάστατα σταυρωτά πολύτοπα χωρίς κενά και ξένα ανά δύο εσωτερικά, επομένως:

Λήμμα 3.34. Για κάθε στοιχείο α ενός 8-διάστατου (ευκλείδειου) χώρου υπάρχει στοιχείο β του πλέγματος E_8 , τέτοιο ώστε $N(\alpha - \beta) \leq 1$.

Απόδειξη

Το α ανήκει σε ένα simplex ή σε ένα σταυρωτό πολύτοπο. Η μέγιστη απόσταση από τις κορυφές του πολύτοπου επιτυγχάνεται στο κέντρο του και όπως είδαμε παραπάνω είναι ίση με $\frac{2\sqrt{2}}{3}$ και 1 αντίστοιχα. Άρα υπάρχει κορυφή β του πολύτοπου, δηλαδή σημείο του E_8 τέτοια ώστε $N(\alpha - \beta) \leq 1$. ■

Το παρακάτω σχήμα δείχνει στοιχεία του $\mathbf{O}^8$ που είναι κορυφές ενός simplex και ενός σταυρωτού πολύτοπου που έχουν κοινή μια 7-έδρα, άρα παράγουν ένα «υπό κλίμακα» αντίγραφο του E_8 αφού τα διανύσματα των κορυφών δεν είναι πια μοναδιαία των αξόνων.



Εικόνα 3.8: Τα ακέραια οκτόνια που παράγουν το E_8 (επιλογή των κορυφών από τους Conway-Smith)

Για το simplex με κορυφές αυτές της Εικόνας 3.8 έχουμε ότι το κέντρο του έχει διάνυσμα θέσης:

$$\begin{aligned} C_s &= \frac{1}{9}(0 + i_{\infty 124} + i_{\infty 013} + i_{\infty 026} + i_{\infty 045} + i_{\infty 01\bar{3}} + i_{\infty 02\bar{6}} + i_{\infty 04\bar{5}} + i_{\infty}) \\ &= \frac{1}{2}i_{\infty} + \frac{1}{3}i_0 + \frac{1}{6}i_1 + \frac{1}{6}i_2 + \frac{1}{6}i_4. \end{aligned}$$

Η μέγιστη απόσταση ενός σημείου του simplex από το κέντρο του επιτυγχάνεται στις κορυφές v_i , $i = 1, \dots, 9$ και μπορούμε να υπολογίσουμε ότι:

$$|C_s - v_i| = \frac{2}{3} \Rightarrow N(C_s - v_i) = \frac{4}{9}.$$

Με τον ίδιο τρόπο βρίσκουμε ότι το κέντρο του σταυρωτού πολύτοπου είναι:

$$C_o = \frac{1}{2}i_{\infty} + \frac{1}{2}i_0$$

με τη μέγιστη απόσταση ενός σημείου του από το κέντρο να επιτυγχάνεται επίσης στις κορυφές και ισχύει ότι:

$$|C_o - v_i| = \frac{1}{\sqrt{2}} \Rightarrow N(C_o - v_i) = \frac{1}{2}, \quad i = 1, \dots, 16.$$

Στο «υπό κλίμακα» αντίγραφο του E_8 της Εικόνας 3.8, κάθε οκτόνιο α ανήκει σε ένα simplex ή σε ένα σταυρωτό πολύτοπο των οποίων οι κορυφές είναι ακέραια οκτόνια, επομένως:

Λήμμα 3.35. Για κάθε οκτόνιο α υπάρχει ακέραιο οκτόνιο β , τέτοιο ώστε $N(\alpha - \beta) \leq \frac{1}{2}$.

Μπορούμε τώρα να αποδείξουμε ότι:

Θεώρημα 3.36. Αν α και δ ακέραια οκτόνια με $\delta \neq 0$, τότε υπάρχουν ακέραια οκτόνια β και ρ , τέτοια ώστε $\alpha = \delta\beta + \rho$ και $N(\rho) \leq \frac{1}{2}N(\delta)$.

Απόδειξη

Έστω α και δ ακέραια οκτόνια με $\delta \neq 0$. Από το Λήμμα 3.35 έχουμε ότι υπάρχει ακέραιο οκτόνιο β , τέτοιο ώστε:

$$N(\delta^{-1}\alpha - \beta) \leq \frac{1}{2} \Rightarrow N(\delta(\delta^{-1}\alpha) - \delta\beta) \leq \frac{1}{2}N(\delta) \text{ και από την (2.18) παίρνουμε:}$$

$$N(\alpha - \delta\beta) \leq \frac{1}{2}N(\delta)$$

Θέτοντας $\rho = \alpha - \delta\beta \in \mathbf{O}^8$ έχουμε ότι:

$$\alpha = \delta\beta + \rho \text{ και } N(\rho) \leq \frac{1}{2}N(\delta). \quad \blacksquare$$

Ανάλογα αποδεικνύεται ότι υπάρχουν ακέραια οκτόνια β και ρ ώστε να ισχύει: $\alpha = \beta\delta + \rho$.

Το επόμενο θεώρημα δίνεται χωρίς απόδειξη, ο αναγνώστης μπορεί να ανατρέξει στους Conway–Smith (χωρισμένο σε τρεις προτάσεις) ή στον Allcock (1999) για την απόδειξή του.

Θεώρημα 3.37. Κάθε αριστερό ή δεξιό ιδεώδες Λ του $\mathbf{O}^8$, είναι αμφίπλευρο και έχει την μορφή $n\mathbf{O}^8 = \mathbf{O}^8n$, για κάποιον συνήθη ακέραιο n .

Οι Conway–Smith αναφέρουν ότι οι Mahler, van der Blij & Springer και Lamont, με διαφορετική συνεισφορά ο καθένας, απέδειξαν ότι αυτή η ιδιότητα των ιδεωδών του $\mathbf{O}^8$ δεν μας επιτρέπει να τα χρησιμοποιήσουμε προκειμένου να μελετήσουμε την ανάλυση των ακέραιων οκτονίων σε παράγοντες.

3.4.2 Οι διαιρέτες ενός ακέραιου οκτονίου

Στην προηγούμενη ενότητα καταλήξαμε στο συμπέρασμα ότι η θεωρία των ιδεωδών δεν μπορεί να χρησιμοποιηθεί για την ανάλυση των ακέραιων οκτονίων σε παράγοντες. Η δυνατότητα διαίρεσης με «μικρό υπόλοιπο» του Θεωρήματος 3.36 όμως μας επιτρέπει την κατασκευή μιας «αντιστροφής» του ευκλείδειου αλγορίθμου, η οποία προτάθηκε από τον Rehm (1993).

Περιγράφουμε πρώτα την «ευθεία κατεύθυνση» του αλγορίθμου.

Αυτή ξεκινάει με ένα ζεύγος r_1, d_1 , όπου r_1 είναι ένα ακέραιο οκτόνιο του οποίου η νόρμα διαιρείται από τον θετικό συνήθη ακέραιο d_1 . Θέτοντας $N(r_1) = d_0 d_1$ και από το Θεώρημα 3.36 παίρνουμε διαδοχικά θετικούς συνήθεις ακέραιους d_i και ακέραια οκτόνια g_i, r_i όπως φαίνεται στην επαναληπτική διαδικασία που περιγράφεται παρακάτω:

$$\begin{array}{lll}
 r_1 = g_1 d_1 + \overline{r_2} & N(r_1) = d_0 d_1 & \\
 r_2 = g_2 d_2 + \overline{r_3} & N(r_2) = d_1 d_2 & d_1 > d_2 \\
 \vdots & \vdots & \vdots \\
 r_{n-1} = g_{n-1} d_{n-1} + \overline{r_n} & N(r_{n-1}) = d_{n-2} d_{n-1} & d_{n-2} > d_{n-1} \\
 r_n = g_n d_n & N(r_n) = d_{n-1} d_n & d_{n-1} > d_n > 0
 \end{array}$$

Εικόνα 3.9: Η «ευθεία κατεύθυνση» του αλγορίθμου του Rehm (προσαρμογή από τους Conway–Smith)

Δείχνουμε ότι η διαδικασία που περιγράφεται παραπάνω είναι καλά ορισμένη.

Πρόταση 3.38. Στην επαναληπτική διαδικασία της εικόνας 3.9 ισχύει ο θετικός ακέραιος d_{i-1} διαιρεί τη νόρμα $N(r_i)$ για $i = 2, \dots, n$.

Απόδειξη

$$\begin{aligned}
 N(\overline{r_i}) &= N(r_{i-1} - g_{i-1} d_{i-1}) = N(r_{i-1}) + N(-g_{i-1} d_{i-1}) + 2\langle r_{i-1}, -g_{i-1} d_{i-1} \rangle \\
 &= N(r_{i-1}) + d_{i-1}^2 N(g_{i-1}) - d_{i-1} (2\langle r_{i-1}, g_{i-1} \rangle)
 \end{aligned} \tag{3.8}$$

Ο d_{i-1} διαιρεί όλους τους όρους της τελευταίας παράστασης. ■

Πρόταση 3.39. Στην επαναληπτική διαδικασία της εικόνας 3.9 ισχύει ότι $d_{i-1} > d_i$ για $i = 2, \dots, n$.

Απόδειξη

$$d_{i-1}d_i = N(r_i) \leq \frac{N(d_{i-1})}{2} = \frac{d_{i-1}^2}{2} \Rightarrow d_i \leq \frac{d_{i-1}}{2} < d_{i-1}$$

■

Τέλος, έχουμε τους θετικούς ακέραιους αριθμούς $d_1 > d_2 > d_3 > \dots$.

Μια τέτοια ακολουθία ακέραιων αριθμών έχει πεπερασμένο πλήθος όρων, άρα σε κάποιο σημείο καταλήγουμε σε ένα $d_{n+1} = 0$.

Η αντιστροφή της διαδικασίας μας επιτρέπει να βρίσκουμε αριστερούς ή δεξιούς διαιρέτες ενός ακεραίου οκτονίου και να μετράμε το πλήθος τους.

Στο τελευταίο στάδιο της «ευθείας κατεύθυνσης» είχαμε καταλήξει σε συνήθη ακέραιο d_n και ακεραία οκτόνια g_n, r_n τέτοια ώστε $r_n = g_n d_n$.

Επιλέγουμε δ_n οποιοδήποτε ακέραιο οκτόνιο με νόρμα d_n . Τότε από την (2.17) έχουμε:

$$r_n = g_n d_n = g_n (\delta_n \overline{\delta_n}) = (g_n \delta_n) \overline{\delta_n}$$

Θέτουμε $\delta_{n-1} = g_n \delta_n$, ώστε το δ_{n-1} να είναι αριστερός διαιρέτης του r_n με νόρμα d_{n-1} .

Τότε ο $\overline{\delta_{n-1}}$ είναι δεξιός διαιρέτης του $\overline{r_n}$ και διαιρέτης του d_{n-1} , επομένως και του r_{n-1} αφού:

$$\begin{aligned} r_{n-1} &= g_{n-1} d_{n-1} + \overline{r_n} = (g_{n-1} \delta_{n-1}) \overline{\delta_{n-1}} + \delta_n \overline{\delta_{n-1}} \\ &= (g_{n-1} \delta_{n-1} + \delta_n) \overline{\delta_{n-1}} \end{aligned}$$

Στο βήμα αυτό γίνεται φανερός και ο λόγος για τον οποίο στην «ευθεία κατεύθυνση» γράψαμε τα υπόλοιπα των διαιρέσεων ως συζυγείς ακέραιων οκτονίων.

Θέτοντας τώρα $\delta_{n-2} = g_{n-1} \delta_{n-1} + \delta_n$, παίρνουμε έναν αριστερό διαιρέτη του r_{n-1} με νόρμα d_{n-2} .

Συνεχίζοντας με τον ίδιο τρόπο, δηλαδή ακολουθώντας από κάτω προς τα πάνω την αριστερή στήλη της ευθείας διαδικασίας και παραγοντοποιώντας, καταλήγουμε να γράψουμε το ακέραιο οκτόνιο $r = r_1$ στη μορφή $r_1 = \delta_0 \overline{\delta_1}$ έχοντας βρει έναν αριστερό του διαιρέτη δ_0 με νόρμα $m = d_0$ και έναν δεξιό του διαιρέτη $\overline{\delta_1}$ με νόρμα $n = d_1$.

Η παραπάνω διαδικασία περιγράφεται συνοπτικά στην παρακάτω εικόνα:

		$N(\delta_n) = d_n$
$r_n = \delta_{n-1} \overline{\delta_n}$	$\delta_{n-1} = g_n \delta_n$	$N(\delta_{n-1}) = d_{n-1}$
$r_{n-1} = \delta_{n-2} \overline{\delta_{n-1}}$	$\delta_{n-2} = g_{n-1} \delta_{n-1} + \delta_n$	$N(\delta_{n-2}) = d_{n-2}$
$r_{n-2} = \delta_{n-3} \overline{\delta_{n-2}}$	$\delta_{n-3} = g_{n-2} \delta_{n-2} + \delta_{n-1}$	$N(\delta_{n-3}) = d_{n-3}$
$\vdots$	$\vdots$	$\vdots$
$r_2 = \delta_1 \overline{\delta_2}$	$\delta_1 = g_2 \delta_2 + \delta_3$	$N(\delta_1) = d_1$
$r_1 = \delta_0 \overline{\delta_1}$	$\delta_0 = g_1 \delta_1 + \delta_2$	$N(\delta_0) = d_0$

Εικόνα 3.10: Η «αντίστροφη κατεύθυνση» του αλγόριθμου του Rehm (προσαρμογή από τους Conway–Smith)

Επισημαίνουμε ότι σε όλα τα στάδια του αλγορίθμου, τα γινόμενα τριών παραγόντων που προκύπτουν είναι προσεταιριστικά λόγω της Πρότασης 2.26.

Επίσης η αντιστοίχιση $\delta_n \rightarrow \delta_{n-1} \rightarrow \dots \rightarrow \delta_1 \rightarrow \delta_0$ «αντιστρέφεται». Στο τέλος του αλγορίθμου έχουμε $r_1 = \delta_0 \overline{\delta_1}$. Από τα δ_0, δ_1 μπορούμε να υπολογίσουμε όλα τα υπόλοιπα δ_i της διαδικασίας σύμφωνα με την παρακάτω:

$$\delta_2 = \delta_0 - g_1 \delta_1 \rightarrow \dots \rightarrow \delta_i = \delta_{i-2} - g_{i-1} \delta_{i-1} \rightarrow \dots \rightarrow \delta_n.$$

Αρα δύο διαφορετικά δ_n δεν μπορούν να καταλήξουν στο ίδιο ζεύγος δ_0, δ_1 και η αντιστοίχιση είναι 1–1.

Αυτό σημαίνει ότι κάθε διαφορετική επιλογή του ακέραιου οκτονίου δ_n με νόρμα d_n μας δίνει έναν διαφορετικό αριστερό και έναν διαφορετικό δεξιό διαιρέτη του $r = r_1$.

Επομένως το πλήθος των αριστερών διαιρετών νόρμας d_0 , όπως και το πλήθος των δεξιών διαιρετών νόρμας d_1 του ακέραιου οκτονίου $r = r_1$ είναι ίσο με το πλήθος των ακεραίων οκτονίων με νόρμα d_n .

Η επόμενη πρόταση θα μας επιτρέψει να υπολογίσουμε το πλήθος των αριστερών και δεξιών διαιρετών ενός πρωταρχικού ακέραιου οκτονίου. Κατ' αναλογία με τον ορισμό που δώσαμε

στους ακέραιους Hurwitz, ονομάζουμε ένα ακέραιο οκτόνιο πρωταρχικό, όταν αυτό δεν διαιρείται από κανένα φυσικό αριθμό μεγαλύτερο του 1.

Αν r ακέραιο οκτόνιο και d_1, d_2 συνήθεις ακέραιοι, με $MK\Delta(r, d_1, d_2)$ θα συμβολίζουμε τον $MK\Delta(m, d_1, d_2)$, όπου m είναι ο μεγαλύτερος φυσικός αριθμός που διαιρεί τον r .

Πρόταση 3.40. Αν $\kappa_i = MK\Delta(r_i, d_{i-1}, d_i)$ για $1 \leq i \leq n$, τότε $\kappa_i = \kappa_{i+1} = d_n$ για $1 \leq i \leq n-1$.

Απόδειξη

Παρατηρούμε ότι ο κ_i διαιρεί τον $\overline{r_{i+1}} = r_i - g_i d_i$, αφού διαιρεί τους r_i, d_i . Επομένως διαιρεί και τον r_{i+1} .

Επίσης έχουμε:

$$d_{i+1} = \frac{N(r_{i+1})}{d_i} \stackrel{(3.8)}{=} \frac{1}{d_i} (N(r_i) + d_i^2 N(g_i) - d_i (2\langle r_i, g_i \rangle)) = d_{i-1} + d_i N(g_i) - 2\langle r_i, g_i \rangle$$

Παρατηρούμε ότι ο κ_i διαιρεί κάθε όρο της τελευταίας παράστασης, άρα ο κ_i διαιρεί τον d_{i+1} , επομένως και τον $\kappa_{i+1} = MK\Delta(r_{i+1}, d_i, d_{i+1})$.

Ο $\kappa_{i+1} = MK\Delta(r_{i+1}, d_i, d_{i+1})$ διαιρεί τον r_{i+1} άρα και τον $\overline{r_{i+1}}$, επομένως διαιρεί τον $r_i = g_i d_i + \overline{r_{i+1}}$.

Από τη σχέση $d_{i+1} = d_{i-1} + d_i N(g_i) - 2\langle r_i, g_i \rangle$ παίρνουμε ότι:

$$d_{i-1} = d_{i+1} - d_i N(g_i) + 2\langle r_i, g_i \rangle$$

Άρα ο κ_{i+1} διαιρεί και τον d_{i-1} , επομένως και τον κ_i .

Συνεπώς ισχύει $\kappa_i = \kappa_{i+1}$ για $1 \leq i \leq n-1$.

Όμως $\kappa_n = MK\Delta(r_n, d_{n-1}, d_n) = d_n$, επομένως $\kappa_i = \kappa_{i+1} = d_n$ για $1 \leq i \leq n-1$. ■

Η παραπάνω πρόταση σημαίνει ότι το πλήθος των αριστερών και των δεξιών διαιρετών ενός ακέραιου οκτονίου είναι ίσο με το πλήθος των ακέραιων οκτονίων με νόρμα d_n .

Στην περίπτωση που το ακέραιο οκτόνιο $r = r_1$ είναι πρωταρχικό, τότε $d_n = 1$.

Άρα οι αριστεροί και οι δεξιοί του διαιρέτες που προκύπτουν από τον αλγόριθμο του Rehm, είναι τόσοι στο πλήθος όσα και τα ακέραια οκτόνια με νόρμα 1.

Τα ακέραια οκτόνια με νόρμα 1 είναι οι ακέραιοι Graves με μια από τις συντεταγμένες τους ± 1 και τις υπόλοιπες ίσες με 0 και αυτά με 4 ημιακέραιες συντεταγμένες $\pm \frac{1}{2}$ και τις υπόλοιπες ίσες με 0. Η πρώτη κατηγορία δίνει 16 «μονάδες» ενώ η δεύτερη $14 \cdot 2^4 = 224$.

Επομένως, κάθε πρωταρχικό ακέραιο οκτόνιο έχει 240 αριστερούς και 240 δεξιούς διαιρέτες.

Οι επόμενες δύο προτάσεις μας δείχνουν ότι η σχέση των διαιρετών του ακέραιου οκτονίου r με τα ακέραια οκτόνια με νόρμα d_n δεν περιορίζεται στο πλήθος τους.

Λήμμα 3.41. Έστω ότι το ακέραιο οκτόνιο g μπορεί να γραφεί ως γινόμενο με δύο τρόπους $g = \alpha\beta = \alpha'\beta'$, όπου $N(\alpha) = N(\alpha') \neq 0$ και $N(\beta) = N(\beta') \neq 0$. Τότε η γωνία θ_α μεταξύ των α και α' είναι ίση με τη γωνία θ_β μεταξύ των β και β' .

Απόδειξη

Υπολογίζουμε το εσωτερικό γινόμενο των g και $\alpha\beta'$ με δύο τρόπους:

$$\langle g, \alpha\beta' \rangle = \langle \alpha\beta, \alpha\beta' \rangle = N(\alpha)\langle \beta, \beta' \rangle$$

$$\langle g, \alpha\beta' \rangle = \langle \alpha'\beta', \alpha\beta' \rangle = N(\beta')\langle \alpha, \alpha' \rangle$$

Επομένως

$$\cos\theta_\alpha = \frac{\langle \alpha, \alpha' \rangle}{N(\alpha)} = \frac{\langle \beta, \beta' \rangle}{N(\beta)} = \cos\theta_\beta \quad \blacksquare$$

Συμβολίζουμε με $\{\delta_n\}, \{\delta_{n-1}\}, \dots, \{\delta_0\}$ τα σύνολα όλων των δ_k που μπορούν να εμφανιστούν στην «αντίστροφη κατεύθυνση» του αλγόριθμου του Rehm. Έχουμε δείξει ότι το $\{\delta_n\}$ είναι το σύνολο των ακέραιων οκτονίων με νόρμα d_n .

Θέτοντας στο Λήμμα 3.41: $g = d_n = \delta_n \overline{\delta_n} = \delta'_n \overline{\delta'_n}$, παίρνουμε ότι το $\{\delta_n\}$ είναι όμοιο με το σύνολο των συζυγών $\{\overline{\delta_n}\}$. Συμβολίζουμε αυτή τη σχέση με:

$$\{\delta_n\} \stackrel{d_n}{\sim} \{\overline{\delta_n}\}.$$

Θέτοντας τώρα $g = r_n$ παίρνουμε $\{\overline{\delta_n}\} \stackrel{r_n}{\sim} \{\delta_{n-1}\}$.

Συνεχίζοντας με τον ίδιο τρόπο παίρνουμε τελικά τις ομοιότητες:

$$\{\delta_n\} \stackrel{d_n}{\sim} \{\overline{\delta_n}\} \stackrel{r_n}{\sim} \{\delta_{n-1}\} \stackrel{d_{n-1}}{\sim} \{\overline{\delta_{n-1}}\} \stackrel{r_{n-1}}{\sim} \dots \stackrel{d_1}{\sim} \{\overline{\delta_1}\} \stackrel{r_1}{\sim} \{\delta_0\}.$$

Το παραπάνω συμπέρασμα σε συνδυασμό με την πρόταση 3.40 μας δίνουν το παρακάτω:

Θεώρημα 3.42. Έστω ένα ακέραιο οκτόνιο r με νόρμα mn , όπου m, n θετικοί συνήθεις ακέραιοι και κ ο μέγιστος κοινός διαιρέτης των r, m, n . Τότε το σύνολο των αριστερών διαιρετών (δ_0) του r με νόρμα m και το σύνολο των δεξιών διαιρετών $(\overline{\delta_1})$ του r με νόρμα n είναι γεωμετρικά όμοιο με το σύνολο των ακεραίων οκτονίων (δ_n) με νόρμα $\kappa (= d_n)$.

3.4.3 Το πλήθος των αναλύσεων των ακεραίων οκτονίων σε παράγοντες

Στην ενότητα 3.2, η έλλειψη της μεταθετικότητας του πολλαπλασιασμού υπερμιγαδικών, οδηγούσε σε διαφορετικές αναλύσεις ενός ακεραίου Hurwitz σε παράγοντες, με κάθε μια από αυτές να έχει ως πρότυπο μια ανάλυση της νόρμας του σε πρώτους παράγοντες.

Ένας πρωταρχικός ακεραίος Hurwitz με νόρμα ίση με 84, έχει (με την εξαίρεση του πολλαπλασιασμού με μονάδες) 12 αναλύσεις σε πρώτους παράγοντες, κάθε μια από αυτές με πρότυπο μια από τις παρακάτω αναλύσεις της νόρμας σε ρητούς πρώτους:

$$\begin{array}{cccccc} 2 \cdot 2 \cdot 3 \cdot 7 & 2 \cdot 2 \cdot 7 \cdot 3 & 2 \cdot 3 \cdot 2 \cdot 7 & 2 \cdot 7 \cdot 2 \cdot 3 & 2 \cdot 3 \cdot 7 \cdot 2 & 2 \cdot 7 \cdot 3 \cdot 2 \\ 3 \cdot 2 \cdot 2 \cdot 7 & 7 \cdot 2 \cdot 2 \cdot 3 & 3 \cdot 2 \cdot 7 \cdot 2 & 7 \cdot 2 \cdot 3 \cdot 2 & 3 \cdot 7 \cdot 2 \cdot 2 & 7 \cdot 3 \cdot 2 \cdot 2 \end{array}$$

Ο πολλαπλασιασμός των οκτονίων δεν είναι προσεταιριστικός, γεγονός το οποίο αλλάζει την ανάλυσή μας με δύο τρόπους.

Οι τρόποι με τους οποίους μπορούμε να γράψουμε τη νόρμα, τώρα είναι $5 \cdot 12 = 60$, όπως φαίνεται παρακάτω:

$$\begin{array}{cccccc} ((2 \cdot 2) \cdot 3) \cdot 7 & (2 \cdot (2 \cdot 3)) \cdot 7 & (2 \cdot 2) \cdot (3 \cdot 7) & 2 \cdot ((2 \cdot 3) \cdot 7) & 2 \cdot (2 \cdot (3 \cdot 7)) & \\ ((2 \cdot 2) \cdot 7) \cdot 3 & (2 \cdot (2 \cdot 7)) \cdot 3 & (2 \cdot 2) \cdot (7 \cdot 3) & \dots & & \end{array}$$

Οι αναλύσεις σε παράγοντες ενός ακεραίου οκτονίου με πρότυπο μια ανάλυση της νόρμας από τις παραπάνω δεν συνδέονται μεταξύ τους με τον πολλαπλασιασμό με μονάδες αφού στα οκτόνια ισχύει γενικά $(\alpha u)(u^{-1}\beta) \neq \alpha\beta$.

Μια αλλαγή όμως που επηρεάζει δύο γειτονικούς παράγοντες, όπως για παράδειγμα η αντικατάσταση του γινομένου P_1P_2 από το $P'_1P'_2$, όπου P'_1, P'_2 είναι όπως στο Λήμμα 3.41, θα την ονομάζουμε **metamigration**. Αν το P_1P_2 είναι πρωταρχικό (όπως συμβαίνει αν το γινόμενο P_1P_2 εμφανίζεται στην ανάλυση σε παράγοντες ενός πρωταρχικού ακέραιου οκτονίου) αποδείξαμε ότι αυτή η αντικατάσταση μπορεί να γίνει με 240 τρόπους.

Τέλος, κάθε ανάλυση σε k πρώτους παράγοντες περιέχει $k-1$ γινόμενα αυτής της μορφής.

Καταλήγουμε λοιπόν στο παρακάτω:

Θεώρημα 3.43. Έστω ένα πρωταρχικό ακέραιο οκτόνιο Q . Το πλήθος των αναλύσεων σε παράγοντες, με πρότυπο μια δεδομένη ανάλυση της νόρμας του σε πρώτους παράγοντες (όπως για παράδειγμα, της μορφής $Q = ((P_1P_2)(P_3(P_4 \dots P_k)))$) είναι ίσο με 240^{k-1} . Αν κρατήσουμε σταθερούς όλους τους παράγοντες εκτός από δύο, τους P_i και P_j , τότε τα σύνολα των δυνατών τιμών των P_i και P_j είναι γεωμετρικά όμοια με το σύνολο των 240 μονάδων του $\mathcal{O}^8$.

Μένει να εξετάσουμε την περίπτωση του μη πρωταρχικού οκτονίου.

Θεώρημα 3.44. Ένα ακέραιο οκτόνιο με νόρμα $p_1^{n_1}p_2^{n_2} \dots p_k^{n_k}$, του οποίου ο μέγιστος φυσικός διαιρέτης είναι ο $p_1^{s_1}p_2^{s_2} \dots p_k^{s_k}$ έχει

$$240^{n-1} \prod_{i=1}^k C_{n_i, s_i}(p_i^3)$$

αναλύσεις σε πρώτους παράγοντες, με πρότυπο μια δεδομένη ανάλυση της νόρμας του σε πρώτους παράγοντες. Με τον όρο πρώτους παράγοντες εννοούμε πρωταρχικά ακέραια οκτόνια με νόρμα ρητό πρώτο αριθμό. Επίσης, $C_{n,s}(x)$ είναι τα περικομμένα πολυώνυμα Catalan, όπως αυτά ορίστηκαν στην ενότητα 3.2, και $n = n_1 + \dots + n_k$.

Απόδειξη

Όπως και με τους ακέραιους Hurwitz, θα μετρήσουμε το πλήθος των αναλύσεων της μορφής:

$$(P_1(P_2(\dots (P_{n-1}P_n) \dots)))$$

όπου όλοι οι παράγοντες έχουν νόρμα τον ρητό πρώτο p .

Η απόδειξη είναι ανάλογη αυτής του θεωρήματος 3.19 με τις παρακάτω διαφορές.

Στους υπερμιγαδικούς ταυτίζαμε τις αναλύσεις που διέφεραν κατά πολλαπλασιασμό με μονάδες, κάτι που δεν ισχύει στα οκτόνια, άρα σε κάθε βήμα πρέπει να υπολογίζουμε τις 240 διαφορετικές επιλογές που προκύπτουν από το Θεώρημα 3.43. Αφού η ανάλυση σε n πρώτους παράγοντες έχει $n - 1$ τέτοια βήματα προκύπτει ο παράγοντας

$$240^{n-1}.$$

Καθώς υπάρχουν $240(p^3 + 1)$ ακέραια οκτόνια νόρμας p , το όρισμα p στα πολυώνυμα Catalan αντικαθίσταται από το p^3 .

Τέλος, ενώ στους ακέραιους Hurwitz ο πρώτος 2 δεν επηρέαζε την καταμέτρησή μας, στην περίπτωση των ακέραιων οκτονίων αντιμετωπίζεται όπως και οι υπόλοιποι πρώτοι παράγοντες της νόρμας. ■

Οι Conway–Smith αναφέρουν ότι:

με ανάλογα επιχειρήματα αποδεικνύεται ότι το θεώρημα ισχύει και για αναλύσεις σε παράγοντες της μορφής:

$$P_1((P_2P_3)P_4)$$

ενώ για αναλύσεις σε παράγοντες της μορφής

$$(P_1P_2)(P_3P_4)$$

παίρνουμε το ίδιο αποτέλεσμα χρησιμοποιώντας το αποκαλούμενο «metassociation lemma», σύμφωνα με το οποίο, όταν τα ακέραια οκτόνια κάθε ενός από τα ζεύγη (A, A') , (B, B') , (C, C') έχουν την ίδια νόρμα και διαιρούνται από τους ίδιους συνήθεις ακέραιους, τότε το πλήθος των αναλύσεων των μορφών $(AB)C$ και $A'(B'C')$ είναι το ίδιο.

4. Συμπεράσματα

Σκοπός της παρούσας εργασίας ήταν η συστηματική παρουσίαση της άλγεβρας των οκτονίων, μιας από τις μη προσεταιριστικές άλγεβρες που εμφανίζονται στα μαθηματικά.

Η μελέτη ξεκίνησε με μια ιστορική ανασκόπηση της διαδικασίας επέκτασης του συνόλου των πραγματικών αριθμών αρχικά στους μιγαδικούς, κατόπιν στους υπερμιγαδικούς και τελικά στα οκτόνια. Δόθηκε έμφαση στους μιγαδικούς αριθμούς, η κατασκευή των οποίων θεωρήθηκε το σημείο έναρξης της εν λόγω διαδικασίας. Η διαδικασία αυτή παρουσιάστηκε ως μια φυσιολογική για τα μαθηματικά αναζήτηση με βάση το ερώτημα: μέχρι ποιο σημείο μπορεί να επεκταθεί η έννοια του αριθμού διατηρώντας κάποιες βασικές αλγεβρικές ιδιότητες.

Στο 1^ο κεφάλαιο της εργασίας εκτός από τα ιστορικά στοιχεία, αναδείχθηκε η σταδιακή απώλεια αυτών των αλγεβρικών ιδιοτήτων κατά τα βήματα επέκτασης. Στη μετάβαση από τους πραγματικούς αριθμούς στους μιγαδικούς χάνεται η διάταξη. Οι υπερμιγαδικοί χάνουν την μεταθετική ιδιότητα του πολλαπλασιασμού, ενώ στα οκτόνια χάνεται και η προσεταιριστική. Σε επόμενα βήματα εμφανίζονται διαιρέτες του μηδενός.

Το 2^ο κεφάλαιο είναι η βάση για τη συστηματική παρουσίαση των οκτονίων που αναφέραμε στην αρχή. Παρουσιάστηκαν οι composition άλγεβρες και αποδείχθηκαν οι ιδιότητές τους, στις οποίες θεμελιώνεται η μέθοδος διπλασιασμού των Cayley–Dickson. Η διαδικασία αυτή ξεκινάει από τη νόρμα μιας composition άλγεβρας και την πολλαπλασιαστική της ιδιότητα, οι οποίες βρίσκονται στη βάση των αποτελεσμάτων που παρουσιάστηκαν.

Χρησιμοποιώντας την μέθοδο Cayley–Dickson κατασκευάστηκαν με ενιαίο τρόπο τα σύνολα των μιγαδικών, των υπερμιγαδικών και των οκτονίων. Η απόδειξη του θεωρήματος Hurwitz έδειξε ότι οι μοναδικές πεπερασμένης διάστασης άλγεβρες διαίρεσης, με μονάδα και πολλαπλασιαστική νόρμα έχουν διαστάσεις 1, 2, 4 και 8. Επομένως η άλγεβρα των οκτονίων είναι το τελικό σημείο της διαδικασίας επέκτασης των πραγματικών αριθμών, αν έχουμε την απαίτηση να διατηρούνται συγκεκριμένες αλγεβρικές ιδιότητες, όπως η μη-ύπαρξη διαιρετών του μηδενός.

Στη συνέχεια αποδείχθηκαν κάποιες βασικές αλλά ιδιαίτερα σημαντικές ιδιότητες των οκτονίων, όπως οι νόμοι του Moufang και η εναλλακτικότητα στο πλαίσιο των ιδιοτήτων μιας composition άλγεβρας. Οι παραπάνω ιδιότητες δείχνουν ότι, παρά την έλλειψη της προσεταιριστικότητας, η πολλαπλασιαστική ιδιότητα της νόρμας δίνει στα οκτόνια μια αρκετά

πλούσια δομή ώστε να διατηρούν, με κατάλληλες προσαρμογές, αρκετές από τις ιδιότητες του πολλαπλασιασμού.

Τέλος, στο 3^ο κεφάλαιο συνδέθηκαν οι άλγεβρες που μελετήθηκαν στα προηγούμενα με την θεωρία αριθμών. Ορίστηκαν οι ακέрайοι Gauss, Hurwitz και τα ακέрайα οκτόνια ως μορφές επέκτασης της έννοιας του ακέрайου αριθμού στις παραπάνω άλγεβρες. Η μελέτη για τη δυνατότητα διαίρεσης με «μικρό υπόλοιπο» στα σύνολα αυτά ανέδειξε τη σύνδεση των αλγεβρικών δομών που μελετήθηκαν με γεωμετρικές δομές. Η δυνατότητα διαίρεσης με «μικρό υπόλοιπο» αποδείχθηκε γεωμετρικά. Στην περίπτωση των ακέрайων Gauss, ουσιαστικά με τη βοήθεια του πλέγματος $\mathbb{Z}^2$, σε αυτή των Hurwitz με τη βοήθεια του πλέγματος D_4 και σε αυτήν των ακέрайων οκτονίων με τη βοήθεια του E_8 .

Στους ακέрайους Hurwitz μετρήθηκε το πλήθος των αναλύσεων σε «πρώτους» παράγοντες με τη χρήση ιδεωδών. Στην περίπτωση των ακέрайων οκτονίων χρησιμοποιήθηκε ο αλγόριθμος του Rehm, ο οποίος είναι σχετικά καινούργια συνεισφορά στην θεωρία των ακέрайων οκτονίων.

Στην εργασία αυτή δεν μελετήθηκε, παρά την αρχική πρόθεση, η σχέση των υπερμιγαδικών και των οκτονίων με γεωμετρικούς μετασχηματισμούς σε χώρους διάστασης 3, 4, 7 και 8.

Οι περιστροφές στον $\mathbb{R}^3$ είναι ενεργό πεδίο εφαρμογής των υπερμιγαδικών, ενώ οι περιστροφές στους $\mathbb{R}^7$ και $\mathbb{R}^8$ είναι πιθανό πεδίο εφαρμογής των οκτονίων στη φυσική, καθώς η σύγχρονη θεωρητική φυσική μελετά χώρους με διάσταση μεγαλύτερη του 4.

Επίσης δε μελετήθηκε η σύνδεση των οκτονίων με ομάδες Lie (όπως η $G_2 = \text{Aut}(\mathbb{O})$), οι οποίες αποτελούν ενεργό τομέα των μαθηματικών.

Τα παραπάνω μπορούν να αποτελέσουν το αντικείμενο μελλοντικής εργασίας καθώς ερευνούν πεδία στα οποία θα μπορούσαν τα οκτόνια να βρουν εφαρμογές και τα οποία αποτελούν αντικείμενα της σύγχρονης έρευνας.

Βιβλιογραφία

- [1] Loria, G. (1971). *Ιστορία των Μαθηματικών*. Αθήνα: Εκδόσεις ΕΜΕ.
- [2] Θωμαΐδης, Γ. (1981). Ιστορική Αναδρομή στους Μιγαδικούς Αριθμούς. *Μαθηματική Επιθεώρηση*, 21, 95–109.
- [3] Fraleigh, J.B. (1999). *Εισαγωγή στην Άλγεβρα*. Ηράκλειο: Πανεπιστημιακές Εκδόσεις Κρήτης.
- [4] Dray, T. & Manogue, C. (2015). *The Geometry of the Octonions*. Singapore: World Scientific Publishing Co. Pte. Ltd.
- [5] Baez, J.C. (2001). The Octonions. *Bulletin of the American Mathematical Society*, 39, 145–205.
- [6] Conway, J. & Smith, D. (2003). *On Quaternions and Octonions*. Canada: A K Peters Ltd.
- [7] Cayley, A. (1845). On Jacobi's Elliptic Functions, in reply to the Rev. Brice Bronwin; and on Quaternions. *Philosophical Magazine*, 26, 208–211.
- [8] Moreno, G.R. (1997). The zero divisors of the Cayley–Dickson algebras over the real numbers. [arXiv:q-alg/9710013v1](https://arxiv.org/abs/q-alg/9710013v1)
- [9] Schafer, R.D. (1966). *An Introduction to Nonassociative Algebras*. New York: Academic Press Inc.
- [10] Αντωνιάδης, Γ. & Κοντογεώργης, Α. (2015). *Θεωρία Αριθμών και Εφαρμογές*. Αθήνα: Σύνδεσμος Ελληνικών Ακαδημαϊκών Βιβλιοθηκών.
- [11] Dickson, L.E. (1923). *Algebras and their Arithmetics*. Chicago, Illinois: University of Chicago Press.
- [12] Allcock, D. (1999). Ideals in the Integral Octonions. *Journal of Algebra*, 220 (2), 396–400.
- [13] Rehm, H.P. (1993). Prime factorization of integral Cayley octaves. *Annales de la faculté des sciences de Toulouse*. 2(2), 271–289.
- [14] Nagata, M. (1987). On the Definition of a Euclid Ring. *Advanced Studies in Pure Mathematics*. 11, 167–171.

[15] Πύλια, Ε. (2014). Composition Άλγεβρες & Εφαρμογές. Αθήνα: Εθνικό Μετσόβιο Πολυτεχνείο.

Διαδικτυακές πηγές

[1] O'Connor, J.J. & Robertson, E.F. (2016). John Thomas Graves. *MacTutor History of Mathematics*. University of St Andrews, Scotland

http://mathshistory.st-andrews.ac.uk/Biographies/Graves_John

[2] O'Connor, J.J. & Robertson, E.F. (2016). The Eight Squares Identity and Graves–Cayley Numbers. *MacTutor History of Mathematics*. University of St Andrews, Scotland

http://mathshistory.st-andrews.ac.uk/Extras/Eight_Squares_Identity/

Υπεύθυνη Δήλωση Συγγραφέα

Δηλώνω ρητά ότι, σύμφωνα με το άρθρο 8 του Ν.1599/1986, η παρούσα εργασία αποτελεί αποκλειστικά προϊόν προσωπικής μου εργασίας, δεν προσβάλλει κάθε μορφής δικαιώματα διανοητικής ιδιοκτησίας, προσωπικότητας και προσωπικών δεδομένων τρίτων, δεν περιέχει έργα/εισφορές τρίτων για τα οποία απαιτείται άδεια των δημιουργών/δικαιούχων και δεν είναι προϊόν μερικής ή ολικής αντιγραφής, οι πηγές δε που χρησιμοποιήθηκαν περιορίζονται στις βιβλιογραφικές αναφορές και μόνον και πληρούν τους κανόνες της επιστημονικής παράθεσης.