



ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ

**Σχολή Εφαρμοσμένων Μαθηματικών και Φυσικών
Επιστημών**

ΘΕΜΑ

**Το Θεμελιώδες Θεώρημα της
Άλγεβρας:
Μια Απόδειξη με τη χρήση της
Θεωρίας *Galois***

Φοιτήτρια:
Βασιλική Μ. Ρουκουνάκη
A.M.: 09120402

Επιβλέπουσα Καθηγήτρια:
Χριστίνα Βασιλακοπούλου
Επίκουρη Καθηγήτρια

Αθήνα, Ιανουάριος 2026

Περιεχόμενα

1	Εισαγωγή	3
1.1	Ιστορική Αναδρομή και Σημασία του Θεμελιώδους Θεωρήματος της Άλγεβρας	3
1.1.1	Ορισμός του Θεμελιώδους Θεωρήματος της Άλγεβρας	3
1.1.2	Η Ιστορία του Προβλήματος και οι Πρώτες Αποδείξεις	3
1.1.3	Η Σημασία του Θεωρήματος στα Μαθηματικά	3
1.2	Επισκόπηση των Διαφορετικών Αποδείξεων	4
1.2.1	Σκοπός της ενότητας και κύριες κατηγορίες προσεγγίσεων	4
1.2.2	Αναλυτικές αποδείξεις: Θεώρημα Liouville και ελάχιστο του $ p $	4
1.2.3	Τοπολογικές/γεωμετρικές αποδείξεις: Αρχή Επιχειρήματος και Θεώρημα Rouché	5
1.2.4	Η αλγεβρική προσέγγιση: στρατηγική μέσω Θεωρίας Galois	5
1.3	Δομή της Εργασίας	6
2	Θεωρία Σωμάτων και Αλγεβρικές Επεκτάσεις	8
2.1	Βασικές Έννοιες της Θεωρίας Σωμάτων	8
2.2	Ο Δακτύλιος των Πολυωνύμων $F[x]$	9
2.3	Επεκτάσεις Σωμάτων	9
2.3.1	Αλγεβρικά και Υπερβατικά Στοιχεία	10
2.3.2	Απλές Επεκτάσεις	11
2.4	Σώματα Ανάλυσης	12
2.4.1	Ύπαρξη και Μοναδικότητα	12
3	Η Θεωρία Galois	14
3.1	Αυτομορφισμοί και Ομάδα Galois	14
3.1.1	Ομομορφισμοί και Ισομορφισμοί Σωμάτων	14
3.1.2	Η Ομάδα Galois $Gal(L/K)$	15
3.2	Κανονικές και Διαχωρίσιμες Επεκτάσεις	16
3.2.1	Κανονικότητα	16
3.2.2	Διαχωρησιμότητα	18
3.3	Επεκτάσεις Galois	18
3.4	Το Θεμελιώδες Θεώρημα της Θεωρίας Galois	19
3.4.1	Προαπαιτούμενα και Συμβολισμοί	20
3.5	Προαπαιτούμενα από τη Θεωρία Ομάδων	22
3.5.1	Θεωρήματα Sylow	23
3.5.2	Ιδιότητες p -ομάδων	23
4	Αναλυτικά Προαπαιτούμενα και η Δομή του \mathbb{C}	24
4.1	Το Σώμα των Μιγαδικών Αριθμών \mathbb{C}	24
4.1.1	Η Κατασκευή $\mathbb{C} = \mathbb{R}(i)$	24
4.1.2	Ο Βαθμός της Επέκτασης $[\mathbb{C} : \mathbb{R}] = 2$	24
4.2	Ιδιότητα 1: Ρίζες Πολυωνύμων Περιττού Βαθμού	25
4.2.1	Το Θεώρημα Ενδιάμεσης Τιμής (Θ.Ε.Τ.)	25
4.2.2	Ιδιότητα 2: Τετραγωνικές Ρίζες στο \mathbb{C}	26
5	Η Απόδειξη του Θεμελιώδους Θεωρήματος της Άλγεβρας	28
5.0.1	Το Κεντρικό Επιχείρημα και η Αναγωγή στο \mathbb{R}	28
5.0.2	Ορισμός της Ομάδας Galois G	29

5.1	Βήμα 1: Η Ομάδα $\text{Gal}(K/R)$ είναι 2-Ομάδα	29
5.1.1	Ανάλυση της Τάξης της Ομάδας G	29
5.1.2	Εφαρμογή του Πρώτου Θεωρήματος Sylow	29
5.1.3	Η Αντιστοιχία Galois και το Ενδιάμεσο Σώμα L	30
5.2	Βήμα 2: Η Ομάδα $\text{Gal}(K/C)$ είναι Τετριμμένη	30
5.2.1	Η Υποομάδα H' και η Τάξη της	30
5.2.2	Η Υπαρξη Υποομάδας Δείκτη 2	31
5.2.3	Η Αντιστοιχία Galois και το Σώμα L'	31
5.3	Συμπέρασμα της Απόδειξης	31
5.3.1	Η Ταύτιση $K = \mathbb{C}$	32
5.3.2	Το \mathbb{C} ως Αλγεβρικά Κλειστό Σώμα	32
6	Συμπεράσματα	33
6.1	Σύνοψη των Κύριων Αποτελεσμάτων	33
6.1.1	Επαναδιατύπωση του Θ.Θ.Α.	33
6.1.2	Ο Ρόλος των Βασικών Θεωρημάτων στην Απόδειξη	33
6.2	Κριτική Σύγκριση	34
	References	35

1 Εισαγωγή

1.1 Ιστορική Αναδρομή και Σημασία του Θεμελιώδους Θεωρήματος της Άλγεβρας

1.1.1 Ορισμός του Θεμελιώδους Θεωρήματος της Άλγεβρας

Το Θεμελιώδες Θεώρημα της Άλγεβρας (Θ.Θ.Α.) αποτελεί έναν από τους κεντρικούς άξονες που συνδέουν την Άλγεβρα με την Ανάλυση και την Τοπολογία. Η κλασική του διατύπωση είναι η εξής:

Θεώρημα. Κάθε μη σταθερό πολυώνυμο $f(z) \in \mathbb{C}[z]$ με μιγαδικούς συντελεστές έχει τουλάχιστον μία ρίζα στο σώμα των μιγαδικών αριθμών \mathbb{C} .

Άμεσο πόρισμα και ισοδύναμη διατύπωση του θεωρήματος αποτελεί το γεγονός ότι κάθε πολυώνυμο $f(z)$ βαθμού $n \geq 1$ παραγοντοποιείται πλήρως σε γινόμενο n γραμμικών παραγόντων στο \mathbb{C} :

$$f(z) = a \prod_{k=1}^n (z - a_k), \quad a_k \in \mathbb{C}.$$

1.1.2 Η Ιστορία του Προβλήματος και οι Πρώτες Αποδείξεις

Η ιστορία της αναζήτησης ριζών είναι πανάρχαια, ξεκινώντας από τους Βαβυλώνιους (1600 π.Χ.) που επέλυαν δευτεροβάθμιες εξισώσεις σε πήλινες πλακέτες. Ωστόσο, η αυστηρή διατύπωση για την ύπαρξη ριζών σε κάθε πολυώνυμο άργησε πολλούς αιώνες.

- **d'Alembert (1746):** Ο Jean le Rond d'Alembert δημοσίευσε την πρώτη σοβαρή προσπάθεια απόδειξης. Η προσέγγισή του βασιζόταν στην ιδέα ότι αν η τιμή $|f(z)|$ δεν είναι μηδέν, τότε μπορεί πάντα να βρεθεί ένα z' τέτοιο ώστε $|f(z')| < |f(z)|$. Παρόλο που η λογική του ήταν σωστή, η απόδειξη θεωρήθηκε ατελής γιατί στηρίχθηκε σε λήμματα (όπως το λήμμα του d'Alembert) που δεν είχαν αποδειχθεί πλήρως με τα εργαλεία της εποχής.
- **Gauss (1799):** Ο Carl Friedrich Gauss, στη διδακτορική του διατριβή, άσκησε κριτική στον d'Alembert και παρουσίασε τη δική του απόδειξη, η οποία ήταν γεωμετρικής φύσεως. Παρόλο που και αυτή η απόδειξη θεωρήθηκε αργότερα ότι είχε κάποια τοπολογικά «κενά» (ως προς τη συνέχεια των καμπυλών στο επίπεδο), ο Gauss επανήλθε με άλλες τρεις αποδείξεις κατά τη διάρκεια της ζωής του, με την τελευταία (1849) να είναι η πιο ώριμη.

1.1.3 Η Σημασία του Θεωρήματος στα Μαθηματικά

Από αλγεβρική σκοπιά, το Θ.Θ.Α. δεν είναι απλώς ένα θεώρημα για τις ρίζες των εξισώσεων, αλλά μια δήλωση για την πληρότητα του συστήματος των μιγαδικών αριθμών.

1. **Αλγεβρικά Κλειστό Σώμα:** Το Θ.Θ.Α. εκφράζει την ιδιότητα ότι το \mathbb{C} είναι **αλγεβρικά κλειστό**. Αυτό σημαίνει ότι δεν υπάρχουν γνήσιες πεπερασμένες αλγεβρικές επεκτάσεις του \mathbb{C} . Κάθε στοιχείο στο \mathbb{C} είναι αλγεβρικό.

2. **Γέφυρα μεταξύ Πεδίων:** Αν και το όνομα του θεωρήματος είναι της Άλγεβρας, όλες οι αυστηρές αποδείξεις απαιτούν αναπόφευκτα κάποιο στοιχείο Ανάλυσης (όπως η συνέχεια ή το Θεώρημα Ενδιάμεσης Τιμής) ή Τοπολογίας.
3. **Χρήση Θεωρίας Galois:** Στη σύγχρονη Άλγεβρα, το Θ.Θ.Α. αποδεικνύεται μέσω του ελέγχου των ομάδων Galois. Αντί να ψάχνουμε τη ρίζα, δείχνουμε ότι η δομή των 2-ομάδων και οι ιδιότητες του \mathbb{R} (όπως οι ρίζες περιττού βαθμού) απαγορεύουν στο \mathbb{C} να έχει οποιαδήποτε επέκταση βαθμού μεγαλύτερου του 1.

Όπως αναφέρουν οι Edwards (1984) και Dummit & Foote (2004), η χρήση της Θεωρίας Galois για την απόδειξη του Θ.Θ.Α. αποτελεί μια από τις πιο κομψές εφαρμογές της μαθηματικής θεωρίας, καθώς μετατρέπει ένα πρόβλημα ύπαρξης σε πρόβλημα δομής ομάδων.

1.2 Επισκόπηση των Διαφορετικών Αποδείξεων

1.2.1 Σκοπός της ενότητας και κύριες κατηγορίες προσεγγίσεων

Το Θεμελιώδες Θεώρημα της Άλγεβρας (Θ.Θ.Α.) έχει ένα ιδιαίτερο χαρακτηριστικό: ενώ διατυπώνεται *αλγεβρικά* (ύπαρξη ριζών πολυωνύμων), οι πιο κλασικές αποδείξεις του αξιοποιούν *αναλυτικές* ή *τοπολογικές* ιδιότητες του μιγαδικού επιπέδου.

Η παρούσα ενότητα δεν στοχεύει να παραθέσει πλήρεις αποδείξεις, αλλά να παρουσιάσει (i) τις βασικές **οικογένειες αποδείξεων**, (ii) τη **μεθοδολογική επιλογή** της εργασίας να αναπτύξει μια δομική και **αλγεβρική** προσέγγιση μέσω Θεωρίας Galois, η οποία συνδέεται οργανικά με τα επόμενα κεφάλαια.

Σε γενικές γραμμές, οι αποδείξεις μπορούν να ομαδοποιηθούν στις εξής κατηγορίες:

- **Αναλυτικές αποδείξεις** (ολόμορφες συναρτήσεις, Liouville, αρχές μεγίστου και ελαχίστου).
- **Τοπολογικές/γεωμετρικές αποδείξεις** (αριθμός περιελίξεων, Αρχή Επιχειρήματος, Rouché).
- **Αλγεβρικές/δομικές προσεγγίσεις** (σώματα, επεκτάσεις, ομάδες Galois και εργαλεία θεωρίας ομάδων).

Σχόλιο. Η ολοκληρωμένη και αυστηρή διατύπωση της αλγεβρικής απόδειξης (μέσω της θεωρίας Galois) αποδίδεται ιστορικά στον Emil Artin (γύρω στο 1940). Ο Emil Artin ήταν ο πρώτος που έδειξε ότι το Θ.Θ.Α. είναι στην πραγματικότητα μια ιδιότητα των Πραγματικά Κλειστών Σωμάτων, αποσυνδέοντάς το από την ανάγκη για μιγαδικά ολοκληρώματα και σειρές.

1.2.2 Αναλυτικές αποδείξεις: Θεώρημα Liouville και ελάχιστο του $|p|$

Μια από τις πιο κλασικές αναλυτικές αποδείξεις στηρίζεται στο **Θεώρημα Liouville**, σύμφωνα με το οποίο κάθε φραγμένη ολόμορφη συνάρτηση στο \mathbb{C} είναι σταθερή. Έστω $p(z) \in \mathbb{C}[z]$ μη σταθερό πολυώνυμο. Αν υποθέσουμε ότι το p δεν έχει ρίζα στο \mathbb{C} , τότε η συνάρτηση

$$f(z) = \frac{1}{p(z)}$$

είναι ολόμορφη σε όλο το \mathbb{C} . Επιπλέον, από τη συμπεριφορά πολυωνύμων στο άπειρο προκύπτει ότι $|p(z)| \rightarrow \infty$ όταν $|z| \rightarrow \infty$, άρα $|f(z)| = |1/p(z)| \rightarrow 0$ όταν $|z| \rightarrow \infty$. Συνεπώς, η f είναι *φραγμένη* στο \mathbb{C} . Το θεώρημα Liouville δίνει ότι η f είναι σταθερή, οπότε και το p θα ήταν σταθερό, άτοπο. Άρα το p έχει ρίζα στο \mathbb{C} .

Στενά συνδεδεμένη είναι η απόδειξη μέσω του **ελαχίστου της** $|p(z)|$. Επειδή $|p(z)| \rightarrow \infty$ όταν $|z| \rightarrow \infty$, υπάρχει $R > 0$ τέτοιο ώστε έξω από τον δίσκο $|z| \leq R$ να ισχύει $|p(z)|$ πολύ μεγάλο. Η συνάρτηση $|p(z)|$ είναι συνεχής και, άρα, λαμβάνει *ελάχιστη* τιμή στον συμπαγή δίσκο $\overline{D(0, R)}$. Αν το ελάχιστο σημείο z_0 ικανοποιούσε $p(z_0) \neq 0$, τότε η τοπική μορφή των ολόμορφων συναρτήσεων (π.χ. ανάπτυγμα Taylor και μη εκφυλισμός του πρώτου μη μηδενικού όρου) επιτρέπει να βρεθούν σημεία κοντά στο z_0 όπου το $|p|$ είναι μικρότερο, αντίφαση. Συνεπώς το ελάχιστο της $|p|$ είναι 0, άρα $p(z_0) = 0$ για κάποιο $z_0 \in \mathbb{C}$.

Σχόλιο. Το πλεονέκτημα αυτών των αποδείξεων είναι ότι χρησιμοποιούν λίγα αλλά ισχυρά εργαλεία της μιγαδικής ανάλυσης και έχουν καθαρή λογική.

1.2.3 Τοπολογικές/γεωμετρικές αποδείξεις: Αρχή Επιχειρήματος και Θεώρημα Rouché

Μια δεύτερη θεμελιώδης οικογένεια αποδείξεων αξιοποιεί τοπολογικές έννοιες στο μιγαδικό επίπεδο, κυρίως τον **αριθμό περιελίξεων** και την **Αρχή Επιχειρήματος**. Η βασική ιδέα είναι ότι, για μεγάλα $R > 0$, το πολυώνυμο

$$p(z) = a_n z^n + a_{n-1} z^{n-1} + \dots + a_0$$

καθορίζεται πάνω στον κύκλο $|z| = R$ από τον κύριο όρο $a_n z^n$. Επομένως, καθώς το z διατρέχει τον κύκλο Re^{it} , $t \in [0, 2\pi]$, η εικόνα $p(Re^{it})$ είναι μια κλειστή καμπύλη που *περιελίσσεται* γύρω από το 0 περίπου n φορές. Η Αρχή Επιχειρήματος συνδέει τον αριθμό περιελίξεων της καμπύλης $p(\partial D(0, R))$ γύρω από το 0 με τον αριθμό των μηδενικών (με πολλαπλότητα) του p μέσα στον δίσκο $D(0, R)$. Άρα, ο αριθμός μηδενικών είναι τουλάχιστον 1 (και, μάλιστα, ισούται με n με πολλαπλότητες για κατάλληλα μεγάλο R).

Ένα ιδιαίτερα ευέλικτο εργαλείο της ίδιας λογικής είναι το **Θεώρημα Rouché**. Αν f, g είναι ολόμορφες σε περιοχή που περιέχει έναν απλό κλειστό κύκλο C και ισχύει

$$|f(z) - g(z)| < |f(z)| \quad \text{για κάθε } z \in C,$$

τότε f και g έχουν τον ίδιο αριθμό μηδενικών (με πολλαπλότητα) στο εσωτερικό του C . Εφαρμόζοντας το θεώρημα στον κύκλο $|z| = R$ με $f(z) = a_n z^n$ και $g(z) = p(z)$, για κατάλληλα μεγάλο R έχουμε ότι $|p(z) - a_n z^n| < |a_n z^n|$ στο σύνορο, άρα p και $a_n z^n$ έχουν τον ίδιο αριθμό μηδενικών μέσα στον κύκλο, δηλαδή ακριβώς n .

Σχόλιο. Οι τοπολογικές αποδείξεις δεν δίνουν μόνο ύπαρξη ρίζας αλλά και την εξής πληροφορία: ο βαθμός του πολυωνύμου εμφανίζεται ως τάξη περιελίξεων, που αντιστοιχεί στον αριθμό ριζών με πολλαπλότητες. Αυτό καθιστά την προσέγγιση εξαιρετικά διαφωτιστική γεωμετρικά.

1.2.4 Η αλγεβρική προσέγγιση: στρατηγική μέσω Θεωρίας Galois

Παρότι οι αναλυτικές/τοπολογικές αποδείξεις είναι οι πιο διαδεδομένες, η παρούσα εργασία υιοθετεί μια **αλγεβρική/δομική** προσέγγιση, η οποία αξιοποιεί τη Θεωρία Galois.

Η βασική ιδέα είναι να μεταφραστεί το Θ.Θ.Α. σε ένα ισοδύναμο δομικό αίτημα για τα σώματα:

Το \mathbb{C} είναι αλγεβρικά κλειστό \iff δεν υπάρχουν γνήσιες πεπερασμένες αλγεβρικές επεκτάσεις του \mathbb{C} .

Η ισοδυναμία αυτή είναι κεντρική στη θεωρία σωμάτων: αν υπήρχε πεπερασμένη αλγεβρική επέκταση K/\mathbb{C} , τότε θα υπήρχε πολυώνυμο στο $\mathbb{C}[x]$ που δεν διασπάται στο \mathbb{C} (και αντιστρόφως).

Η Θεωρία Galois παρέχει οργανωμένο πλαίσιο για να μελετάμε πεπερασμένες κανονικές επεκτάσεις μέσω της **ομάδας Galois** $\text{Gal}(L/K)$, και ιδιαίτερα μέσω της αντιστοιχίας υποομάδων και ενδιάμεσων σωμάτων (Θεμελιώδες Θεώρημα της Θεωρίας Galois). Στη λογική της εργασίας, το ζητούμενο γίνεται: αν K είναι σώμα ανάλυσης κατάλληλου πολυωνύμου πάνω από \mathbb{C} , να αποδειχθεί ότι αναγκαστικά $K = \mathbb{C}$.

Η στρατηγική της απόδειξης (που αναπτύσσεται αναλυτικά στο Κεφάλαιο 5) είναι να θεωρήσουμε μια πεπερασμένη αλγεβρική επέκταση K/\mathbb{C} και να την αναγάγουμε πάνω από το \mathbb{R} :

$$\mathbb{R} \subset \mathbb{C} \subset K.$$

Έπειτα, εξετάζεται η ομάδα $G = \text{Gal}(K/\mathbb{R})$ (σε κατάλληλη κανονική/διαχωριστική περίπτωση). Με χρήση εργαλείων θεωρίας ομάδων (ιδίως επιχειρημάτων για 2-ομάδες και υποομάδες δείκτη 2) και σε συνδυασμό με δύο βασικές *αναλυτικές* ιδιότητες που ισχύουν στον \mathbb{R} και στον \mathbb{C} (ρίζα για πολυώνυμο περιττού βαθμού στο \mathbb{R} , ύπαρξη τετραγωνικής ρίζας για κάθε $z \in \mathbb{C}$), οδηγούμαστε στο ότι δεν μπορεί να υπάρξει γνήσιο ενδιάμεσο σώμα που να αντιστοιχεί σε μη τριμμένη υποομάδα, άρα $\text{Gal}(K/\mathbb{C})$ είναι τριμμένη και τελικά $K = \mathbb{C}$.

Σχόλιο. Η προσέγγιση αυτή είναι «αλγεβρική» ως προς τη βασική της μηχανική (επεκτάσεις σωμάτων, ομάδες Galois, αντιστοιχία υποομάδων), αλλά ενσωματώνει στοχευμένα δύο αναλυτικά γεγονότα ως κρίσιμα σημεία αποκλεισμού ενδιάμεσων σωμάτων. Αυτό είναι συνεπές με τη γενικότερη εικόνα του Θ.Θ.Α. ως αποτελέσματος που βρίσκεται στη διασταύρωση διαφορετικών κλάδων.

1.3 Δομή της Εργασίας

Η παρούσα εργασία είναι διαρθρωμένη με τέτοιο τρόπο ώστε να οικοδομήσει σταδιακά το απαραίτητο θεωρητικό υπόβαθρο, οδηγώντας στην αλγεβρική απόδειξη του Θεμελιώδους Θεωρήματος της Άλγεβρας. Η δομή των κεφαλαίων ορίζεται ως εξής:

- **Στο Κεφάλαιο 2**, παρουσιάζονται οι βασικές έννοιες της θεωρίας σωμάτων και των επεκτάσεων. Εξετάζονται οι αλγεβρικές επεκτάσεις, τα σώματα ανάλυσης πολυωνύμων και οι έννοιες της κανονικότητας και της διαχωρισιμότητας, οι οποίες αποτελούν τους πυλώνες για τη μετάβαση στη θεωρία Galois.
- **Το Κεφάλαιο 3** είναι αφιερωμένο στη Θεωρία Galois. Αναλύεται η αντιστοιχία Galois μεταξύ ενδιάμεσων σωμάτων και υποομάδων της ομάδας Galois. Ιδιαίτερη έμφαση δίνεται στις ιδιότητες των p -ομάδων (και ειδικότερα των 2-ομάδων) και στα Θεωρήματα Sylow, τα οποία θα χρησιμοποιηθούν για την ανάλυση της δομής της ομάδας Galois στην τελική απόδειξη.

- **Στο Κεφάλαιο 4**, εξετάζονται τα αναλυτικά προαπαιτούμενα της εργασίας. Αναλύονται δύο θεμελιώδεις ιδιότητες των πραγματικών αριθμών που βασίζονται στην πληρότητα του \mathbb{R} : η ύπαρξη ριζών σε πολυώνυμα περιττού βαθμού (μέσω του Θεωρήματος Ενδιάμεσης Τιμής) και η ύπαρξη τετραγωνικών ριζών σε κάθε μιγαδικό αριθμό. Οι ιδιότητες αυτές αποτελούν τους αναλυτικούς περιορισμούς που θα επιβάλουν το τελικό αποτέλεσμα.
- **το Κεφάλαιο 5** αποτελεί το κύριο μέρος της εργασίας, όπου πραγματοποιείται η σύνθεση όλων των προηγούμενων εργαλείων. Μέσα από έναν πύργο επεκτάσεων πάνω από το \mathbb{R} και τη χρήση των 2-ομάδων Sylow, αποδεικνύεται ότι κάθε μη σταθερό πολυώνυμο με μιγαδικούς συντελεστές έχει ρίζα στο \mathbb{C} , επιβεβαιώνοντας ότι το σώμα των μιγαδικών αριθμών είναι αλγεβρικά κλειστό.
- **Στο Κεφάλαιο 6**, παρατίθενται τα συμπεράσματα της εργασίας, ανακεφαλαιώνοντας τη σημασία της αλγεβρικής προσέγγισης και εξετάζοντας τη διασύνδεση των διαφορετικών κλάδων των μαθηματικών που επιστρατεύτηκαν για την επίλυση του προβλήματος.

2 Θεωρία Σωμάτων και Αλγεβρικές Επεκτάσεις

Στο κεφάλαιο αυτό θα θέσουμε τις βάσεις της θεωρίας σωμάτων που είναι απαραίτητες για την κατανόηση της δομής των επεκτάσεων Galois. Η μελέτη του Θεμελιώδους Θεωρήματος της Άλγεβρας απαιτεί την εις βάθος κατανόηση του πώς κατασκευάζονται μεγαλύτερα σώματα από μικρότερα μέσω της προσθήκης ριζών πολυωνύμων.

2.1 Βασικές Έννοιες της Θεωρίας Σωμάτων

Η έννοια του σώματος αποτελεί την κεντρική αλγεβρική δομή στην παρούσα εργασία. Ένα σώμα είναι ουσιαστικά ένα σύνολο όπου μπορούμε να εκτελούμε τις τέσσερις βασικές πράξεις της αριθμητικής (πρόσθεση, αφαίρεση, πολλαπλασιασμό και διαίρεση με μη μηδενικά στοιχεία) με τις συνήθεις ιδιότητες.

Ορισμός 2.1.1 (Δακτύλιος) Ένα μη κενό σύνολο F εφοδιασμένο με δύο διμελείς πράξεις, την πρόσθεση (+) και τον πολλαπλασιασμό (\cdot), ονομάζεται **δακτύλιος** αν ικανοποιούνται οι εξής συνθήκες:

- Η δομή $(F, +)$ είναι αντιμεταθετική ομάδα.
- Ο πολλαπλασιασμός είναι προσεταιριστική πράξη: $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ για κάθε $a, b, c \in F$.
- Ισχύουν οι επιμεριστικές ιδιότητες του πολλαπλασιασμού ως προς την πρόσθεση:
 - $a \cdot (b + c) = a \cdot b + a \cdot c$
 - $(b + c) \cdot a = b \cdot a + c \cdot a$

Ορισμός 2.1.2 (Σώμα) Ένα σύνολο F εφοδιασμένο με δύο εσωτερικές πράξεις, την πρόσθεση (+) και τον πολλαπλασιασμό (\cdot), ονομάζεται **σώμα** αν η δομή $(F, +)$ είναι αντιμεταθετική ομάδα με ουδέτερο στοιχείο το 0, η δομή (F^*, \cdot) , όπου $F^* = (F \setminus \{0\}, \cdot)$, είναι αντιμεταθετική ομάδα με ουδέτερο στοιχείο το 1, και ο πολλαπλασιασμός επιμερίζεται ως προς την πρόσθεση.

Παράδειγμα Το \mathbb{Z} δεν είναι σώμα, αφού το 2, για παράδειγμα, δεν έχει πολλαπλασιαστικό αντίστροφο. Ενώ τα $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ είναι σώματα και μάλιστα άπειρων στοιχείων.

Υποσώμα ενός σώματος λέγεται ένα υποσύνολο του σώματος, που είναι σώμα με τις πράξεις που κληρονομεί από το μεγάλο σώμα.

Ορισμός 2.1.3 (Χαρακτηριστική Σώματος) Χαρακτηριστική ενός σώματος F , η οποία συμβολίζεται με $\text{char}(F)$, ονομάζεται ο μικρότερος θετικός ακέραιος n τέτοιος ώστε:

$$n \cdot 1 = \underbrace{1 + 1 + \dots + 1}_{n \text{ φορές}} = 0$$

Αν δεν υπάρχει τέτοιος θετικός ακέραιος, τότε λέμε ότι το σώμα έχει **χαρακτηριστική 0** ($\text{char}(F) = 0$).

Στην εργασία αυτή, εστιάζουμε σε σώματα χαρακτηριστικής 0, όπως το σώμα των πραγματικών αριθμών \mathbb{R} και των μιγαδικών \mathbb{C} .

2.2 Ο Δακτύλιος των Πολυωνύμων $F[x]$

Κάθε αλγεβρική επέκταση ξεκινά από την ανάγκη εύρεσης ριζών για πολυώνυμο που δεν «σπάνε» στο αρχικό σώμα. Ο δακτύλιος όλων των πολυωνύμων με συντελεστές από ένα σώμα F συμβολίζεται με $F[x]$, και αποκτά τη δομή δακτυλίου με τη συνήθη πρόσθεση και πολλαπλασιασμό πολυωνύμων.

Ορισμός 2.2.1 (Ανάγωγο Πολυώνυμο) Ένα μη σταθερό πολυώνυμο $p(x) \in F[x]$ λέγεται **ανάγωγο (irreducible)** πάνω από το F ή ανάγωγο πολυώνυμο στον $F[x]$, αν δεν μπορούμε να γράψουμε το $p(x)$ ως γινόμενο δύο πολυωνύμων του $F[x]$ με βαθμό μικρότερο από τον βαθμό του $p(x)$.

Ο παραπάνω ορισμός να σημειωθεί πως αφορά στην έννοια *ανάγωγο πάνω από το F* και όχι απλώς στην έννοια *ανάγωγο*. Ένα πολυώνυμο $p(x)$ μπορεί να είναι ανάγωγο πάνω από το F , αλλά να μην είναι ανάγωγο αν το θεωρήσουμε πάνω από ένα μεγαλύτερο σώμα K που περιέχει το F .

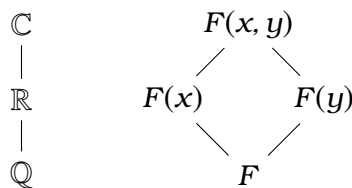
Για παράδειγμα, το $x^2 + 1$ είναι ανάγωγο στο $\mathbb{R}[x]$, διότι δεν έχει πραγματικές ρίζες, αλλά αναγωγίμο στο $\mathbb{C}[x]$, αφού $x^2 + 1 = (x - i)(x + i)$.

2.3 Επεκτάσεις Σωμάτων

Η μελέτη των επεκτάσεων σωμάτων αποτελεί το θεμέλιο της σύγχρονης αλγεβρικής θεωρίας αριθμών. Μια επέκταση σωμάτων μας επιτρέπει να «επεκτείνουμε» ένα σώμα K σε ένα μεγαλύτερο σώμα L , συνήθως με σκοπό την επίλυση εξισώσεων που δεν έχουν λύση στο αρχικό σώμα.

Ορισμός 2.3.1 (Επέκταση σώματος) Έστω K ένα σώμα. Ένα σώμα L ονομάζεται **επέκταση** του K αν το K είναι υποσώμα του L . Στην περίπτωση αυτή γράφουμε L/K (διαβάζεται «το L πάνω από το K »).

Έτσι το \mathbb{R} είναι μια επέκταση σώματος του \mathbb{Q} και το \mathbb{C} είναι μια επέκταση σώματος τόσο του \mathbb{R} όσο και του \mathbb{Q} . Όπως και στην μελέτη ομάδων, θα χρησιμοποιήσουμε δικτυωτά διαγράμματα για να απεικονίσουμε τις επεκτάσεις σωμάτων με το μεγαλύτερο σώμα να βρίσκεται στην κορυφή. Το παραπάνω παράδειγμα φαίνεται στο ακόλουθο διάγραμμα και θα το ορίσουμε (χωρίς κάποιον ακριβή ορισμό) ως **πύργος σωμάτων** (Σχ.2.3.1).



ΣΧΗΜΑ 2.3.1

Σχόλιο Αριστερά του σχήματος απεικονίζεται ο πύργος σωμάτων (όπου ένα μικρότερο

σώμα περιέχεται σε ένα μεγαλύτερο) και δεξιά του σχήματος απεικονίζεται το «διαμάντι» των επεκτάσεων F (όπου αναπαριστά τη σχέση μεταξύ δύο ενδιάμεσων επεκτάσεων ενός σώματος και της σύνθεσής τους).

Μια εξαιρετικά σημαντική παρατήρηση είναι ότι κάθε επέκταση L φέρει μια δομή διανυσματικού χώρου πάνω από το K . Οι πράξεις του διανυσματικού χώρου είναι η πρόσθεση των στοιχείων του L και ο βαθμωτός πολλαπλασιασμός είναι ο συνήθης πολλαπλασιασμός στοιχείων του L με στοιχεία του K .

Ορισμός 2.3.2 (Βαθμός Επέκτασης) Η διάσταση του L ως διανυσματικού χώρου πάνω από το K ονομάζεται **βαθμός της επέκτασης** και συμβολίζεται με $[L : K]$.

Αν $[L : K] = n < \infty$, η επέκταση ονομάζεται πεπερασμένη (π.χ. $[\mathbb{R} : \mathbb{C}] = 2$, όπως αποδεικνύεται και στην ενότητα 4.1.2).

Αν $[L : K] = \infty$, η επέκταση ονομάζεται άπειρη (π.χ. η επέκταση \mathbb{R}/\mathbb{Q} , γιατί κάθε πεπερασμένη επέκταση ενός αριθμήσιμου σώματος παραμένει αριθμήσιμη).

2.3.1 Αλγεβρικά και Υπερβατικά Στοιχεία

Για κάθε στοιχείο a μιας επέκτασης L του K , το $K(a)$ ονομάζεται το υποσώμα του L που παράγεται από το a πάνω από το K . Δομικά, το $K(a)$ αποτελεί την ελάχιστη υποδομή εντός του L η οποία ενσωματώνει το a στο αλγεβρικό πλαίσιο του K .

Ορισμός 2.3.3 Ένα στοιχείο $a \in L$ ονομάζεται **αλγεβρικό** πάνω από το K , αν υπάρχει ένα μη μηδενικό πολυώνυμο $p(x) \in K[x]$ τέτοιο ώστε $p(a) = 0$. Σε αντίθετη περίπτωση, το a ονομάζεται **υπερβατικό**.

Παράδειγμα Το \mathbb{C} είναι μια επέκταση του σώματος του \mathbb{Q} . Αφού το $\sqrt{2}$ είναι ρίζα του $x^2 - 2$, το $\sqrt{2}$ είναι αλγεβρικό στοιχείο πάνω από το \mathbb{Q} .

Παράδειγμα Είναι πολύ γνωστό (δεν θα αποδειχθεί όμως) ότι οι πραγματικοί αριθμοί π και e είναι υπερβατικοί πάνω από το \mathbb{Q} . Ο e εδώ είναι η βάση των φυσικών λογαρίθμων.

Ορισμός 2.3.4 ($\text{irr}(a, K)$) Έστω L μια επέκταση σώματος ενός σώματος K και $a \in L$ αλγεβρικό στοιχείο πάνω από το K . Το μοναδικό μονικό (με ηγετικό στοιχείο 1) πολυώνυμο $p(x)$ λέγεται το **ανάγωγο πολυώνυμο του a πάνω από το K** και θα συμβολίζεται με $\text{irr}(a, K)$. Ο βαθμός του $\text{irr}(a, K)$ λέγεται **βαθμός του a πάνω από το K** και συμβολίζεται με $\text{deg}(a, K)$.

Σχόλιο Το πολυώνυμο αυτό είναι μοναδικό γιατί, οποιοδήποτε άλλο πολυώνυμο μηδενίζει το a , είναι αναγκαστικά πολλαπλάσιο του $\text{irr}(a, K)$.

Παράδειγμα Προφανώς, για το $\text{irr}(\sqrt{2}, \mathbb{Q}) = x^2 - 2$. Επίσης, βλέπουμε ότι για $a = \sqrt{1 + \sqrt{3}}$ στο \mathbb{R} το a είναι ρίζα του $x^4 - 2x^2 - 2$ το οποίο ανήκει στον $\mathbb{Q}[x]$. Αφού το $x^4 - 2x^2 - 2$ είναι ανάγωγο πάνω από το \mathbb{Q} , ισχύει ότι

$$\text{irr}(\sqrt{1 + \sqrt{3}}, \mathbb{Q}) = x^4 - 2x^2 - 2.$$

Άρα το $\sqrt{1 + \sqrt{3}}$ είναι αλγεβρικό στοιχείο βαθμού 4 πάνω από το \mathbb{Q} .

2.3.2 Απλές Επεκτάσεις

Στις προηγούμενες ενότητες εξετάσαμε τις επεκτάσεις σωμάτων γενικά. Ωστόσο, η πιο «ε-ύχρηστη» μορφή μιας επέκτασης είναι αυτή που προκύπτει από την προσθήκη ενός και μόνο στοιχείου στο βασικό σώμα.

Ορισμός 2.3.5 (Απλή επέκταση) Μια επέκταση L ενός σώματος K λέγεται **απλή επέκταση** του K αν $L = K(a)$ για κάποιο $a \in L$.

Το στοιχείο a ονομάζεται **πρωτεύον στοιχείο** της επέκτασης L πάνω από το K .

Στην περίπτωση που το a είναι αλγεβρικό πάνω από το K , η δομή του $K(a)$ είναι πλήρως καθορισμένη από το ανάγωγο πολυώνυμο $\text{irr}(a, K)$. Συγκεκριμένα, αν ο βαθμός του $\text{irr}(a, K)$ είναι n , τότε: Ο βαθμός της επέκτασης είναι $[K(a) : K] = n$. Μια βάση του $K(a)$ ως διανυσματικού χώρου πάνω από το K είναι το σύνολο $\{1, a, a^2, \dots, a^{n-1}\}$.

Ένα από τα πιο εντυπωσιακά αποτελέσματα της θεωρίας σωμάτων είναι ότι οι περισσότερες πεπερασμένες επεκτάσεις που συναντάμε είναι στην πραγματικότητα απλές, ακόμη και αν φαίνεται να δημιουργούνται από πολλά στοιχεία (π.χ. $K(a, \beta)$).

Θεώρημα Πρωτεύοντος Στοιχείου Κάθε πεπερασμένη και διαχωρίσιμη επέκταση (βλ. ενότητα 3.2) L/K είναι απλή.

Ορισμός (Τέλειο Σώμα) Ένα σώμα K ονομάζεται **τέλειο** αν κάθε ανάγωγο πολυώνυμο $f(x) \in K[x]$ είναι διαχωρίσιμο.

Εφόσον κάθε σώμα χαρακτηριστικής 0 (όπως το \mathbb{R} και το \mathbb{C}) είναι **τέλειο σώμα**, όλες οι αλγεβρικές επεκτάσεις τους είναι διαχωρίσιμες. Επομένως, κάθε πεπερασμένη επέκταση του \mathbb{R} ή του \mathbb{Q} είναι απλή.

Παράδειγμα Θεωρούμε την επέκταση $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ πάνω από το \mathbb{Q} . Με μια πρώτη ματιά, η επέκταση παράγεται από δύο στοιχεία. Όμως, σύμφωνα με το θεώρημα, υπάρχει ένα a τέτοιο ώστε $L = \mathbb{Q}(a)$.

Αν επιλέξουμε $a = \sqrt{2} + \sqrt{3}$, μπορούμε να αποδείξουμε ότι:

- $a \in \mathbb{Q}(\sqrt{2}, \sqrt{3})$ (προφανές).
- $\sqrt{2}, \sqrt{3} \in \mathbb{Q}(\sqrt{2} + \sqrt{3})$ (μέσω αλγεβρικών πράξεων).

Συνεπώς, $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$. Το ανάγωγο πολυώνυμο του a είναι το $x^4 - 10x^2 + 1$ και ο βαθμός της επέκτασης είναι 4.

Στην απόδειξη του ΘΘΑ, το Θεώρημα Πρωτεύοντος Στοιχείου μας επιτρέπει να ισχυριστούμε ότι αν είχαμε μια πεπερασμένη επέκταση K του \mathbb{C} , αυτή θα ήταν της μορφής $K = \mathbb{C}(a)$. Αυτό είναι κρίσιμο, διότι αν δείξουμε ότι το ανάγωγο (ή ελάχιστο) πολυώνυμο οποιουδήποτε a πάνω από το \mathbb{C} έχει βαθμό 1, τότε αναγκαστικά $a \in \mathbb{C}$, άρα $K = \mathbb{C}$. Η χρήση της Θεωρίας Galois στην απόδειξη βασίζεται ακριβώς στο να δείξουμε ότι η ομάδα Galois, την οποία θα ορίσουμε παρακάτω, μιας τέτοιας επέκτασης είναι τετριμμένη.

2.4 Σώματα Ανάλυσης

Στην προηγούμενη ενότητα είδαμε ότι αν έχουμε ένα ανάγωγο πολυώνυμο $f(x) \in K[x]$, μπορούμε να κατασκευάσουμε μια επέκταση που περιέχει τουλάχιστον μία ρίζα του. Ωστόσο, για τη μελέτη της ομάδας Galois, χρειαζόμαστε μια επέκταση που να περιέχει όλες τις ρίζες του πολυωνύμου. Αυτή η ανάγκη οδηγεί στην έννοια του σώματος ανάλυσης.

Ορισμός 2.4.1 (Σώμα ανάλυσης) Έστω K ένα σώμα και $f(x) \in K[x]$ ένα πολυώνυμο βαθμού $n \geq 1$.

Μια επέκταση L του K ονομάζεται σώμα ανάλυσης του $f(x)$ πάνω από το K αν ικανοποιούνται οι εξής δύο συνθήκες:

- Το πολυώνυμο $f(x)$ αναλύεται πλήρως σε γινόμενο πρωτοβάθμιων παραγόντων στο $L[x]$. Δηλαδή, υπάρχουν $a_1, a_2, \dots, a_n \in L$ (οι ρίζες) και $c \in K$ τέτοια ώστε:

$$f(x) = c(x - a_1)(x - a_2) \dots (x - a_n)$$

- Το L παράγεται από το K και τις ρίζες a_1, \dots, a_n , δηλαδή $L = K(a_1, a_2, \dots, a_n)$. Αυτό σημαίνει ότι το L είναι το «μικρότερο» δυνατό σώμα που περιέχει όλες τις ρίζες.

2.4.1 Ύπαρξη και Μοναδικότητα

Ένα από τα θεμελιώδη θεωρήματα της θεωρίας σωμάτων (που οφείλεται στον Kronecker) διασφαλίζει ότι για κάθε πολυώνυμο μπορούμε να βρούμε ένα σώμα ανάλυσης.

Θεώρημα (Ύπαρξη) Για κάθε σώμα K και κάθε πολυώνυμο $f(x) \in K[x]$, υπάρχει ένα σώμα ανάλυσης L του $f(x)$ πάνω από το K .

Η ύπαρξη αποδεικνύει ότι, όσο αλγεβρικά περιορισμένο και αν είναι ένα αρχικό σώμα K , μπορούμε πάντα να κατασκευάσουμε μια επέκταση L η οποία να συνιστά το σώμα ανάλυσης του $f(x)$.

Η απόδειξη είναι κατασκευαστική και επαγωγική. Βασίζεται στο Θεώρημα του Kronecker, το οποίο μας λέει ότι αν ένα πολυώνυμο $p(x)$ είναι ανάγωγο στο K , ο δακτύλιος πηλίκου $K[x]/\langle p(x) \rangle$ είναι ένα σώμα που περιέχει τουλάχιστον μία ρίζα του $p(x)$.

Ξεκινάμε με το $f(x)$. Αν αυτό δεν διαθέτει το πλήρες σύνολο των ριζών του εντός του K , προχωρούμε στην επισύναψη μίας ρίζας, κατασκευάζοντας μια κατάλληλη επέκταση του σώματος. Στο νέο αυτό σώμα, το πολυώνυμο παραγοντοποιείται περαιτέρω. Επαναλαμβάνουμε αναδρομικά τη διαδικασία για τους εναπομείναντες παράγοντες, έως ότου το πολυώνυμο διασπαστεί πλήρως σε γινόμενο πρωτοβάθμιων παραγόντων.

Θεώρημα (Μοναδικότητα) Αν L και L' είναι δύο σώματα ανάλυσης του ίδιου πολυωνύμου $f(x)$ πάνω από το K , τότε τα L και L' είναι ισόμορφα μεταξύ τους. Επιπλέον, ο ισομορφισμός αυτός αφήνει τα στοιχεία του K αμετάβλητα.

Παράδειγμα Το σώμα των Μιγαδικών: Το \mathbb{C} είναι το σώμα ανάλυσης του $x^2 + 1$ πάνω από το \mathbb{R} . Περιέχει τις ρίζες $\{i, -i\}$ και $\mathbb{C} = \mathbb{R}(i, -i) = \mathbb{R}(i)$.

Η μοναδικότητα αποδεικνύει ότι, ανεξάρτητα από τη σειρά με την οποία προσθέσαμε τις ρίζες ή τη μέθοδο που χρησιμοποιήσαμε, το τελικό αποτέλεσμα είναι το ίδιο έως ισομορφισμό.

Η απόδειξη δείχνει ότι αν έχουμε δύο σώματα ανάλυσης L και L' για το ίδιο πολυώνυμο, υπάρχει μια αμφιμονοσήμαντη απεικόνιση (ισομορφισμός) που τα συνδέει, η οποία μάλιστα αφήνει τα στοιχεία του αρχικού σώματος K σταθερά.

Η διαδικασία βασίζεται στην επέκταση των ισομορφισμών. Αντιστοιχίζουμε μια ρίζα a στο L με μια ρίζα a' στο L' και δείχνουμε ότι ο ισομορφισμός $K(a) \cong K(a')$ μπορεί να επεκταθεί βήμα-βήμα σε ολόκληρο το σώμα L .

3 Η Θεωρία Galois

Η **Θεωρία Galois** αποτελεί έναν κλάδο των Μαθηματικών που συνδέει μεταξύ τους τη Θεωρία Σωμάτων με τη Θεωρία Ομάδων. Η θεωρία αυτή διαμορφώθηκε από τον Évariste Galois το 1830, ο οποίος υπήρξε ο πρώτος που συνέλαβε την ιδέα ότι η επιλυσιμότητα των αλγεβρικών εξισώσεων εξαρτάται από τη δομή των ομάδων μεταθέσεων των ριζών τους. Η κεντρική φιλοσοφία της Θεωρίας Galois είναι η σύνδεση επεκτάσεων σωμάτων (**επεκτάσεις Galois**) με την Θεωρία Ομάδων και συγκεκριμένα με την **Ομάδα Galois**. Σκοπός του Évariste Galois ήταν να μελετήσει τις μεταθέσεις των ριζών ενός πολυωνύμου που διατηρούν τις αλγεβρικές σχέσεις μεταξύ τους.

3.1 Αυτομορφισμοί και Ομάδα Galois

Η κατανόηση της δομής μιας επέκτασης L/K επιτυγχάνεται μέσω της μελέτης των απεικονίσεων που διατηρούν τις πράξεις του σώματος. Οι απεικονίσεις αυτές μας επιτρέπουν να δούμε πώς τα στοιχεία του σώματος «μετατίθενται» χωρίς να αλλοιώνεται η αλγεβρική τους συμπεριφορά.

3.1.1 Ομομορφισμοί και Ισομορφισμοί Σωμάτων

Όρισμός 3.1.1 (Ομομορφισμός) Έστω L και L' δύο σώματα. Μια απεικόνιση $\sigma : L \rightarrow L'$ ονομάζεται **ομομορφισμός σωμάτων**, αν για κάθε $a, b \in L$ ισχύουν:

1. $\sigma(a + b) = \sigma(a) + \sigma(b)$
2. $\sigma(a \cdot b) = \sigma(a) \cdot \sigma(b)$
3. $\sigma(1_L) = 1_{L'}$

Ιδιότητες

- Κάθε ομομορφισμός σωμάτων είναι αναγκαστικά «ένα προς ένα» (*injection*), καθώς ο πυρήνας του είναι ιδεώδες του σώματος L , και τα μόνα ιδεώδη ενός σώματος είναι το $\{0\}$ και το ίδιο το σώμα.
- Ένας ομομορφισμός $\sigma : L \rightarrow L'$ που είναι «ένα προς ένα» και επί ονομάζεται **ισομορφισμός**.
- Αν $L = L'$, τότε ο ισομορφισμός ονομάζεται **αυτομορφισμός** του L . Το σύνολο όλων των αυτομορφισμών ενός σώματος L συμβολίζεται με $Aut(L)$ και αποτελεί ομάδα υπό τη σύνθεση.

Παράδειγμα Έστω η επέκταση σωμάτων $L = \mathbb{Q}(\sqrt{2})$ πάνω από το σώμα των ρητών αριθμών \mathbb{Q} . Κάθε στοιχείο του L έχει τη μοναδική μορφή $a + b\sqrt{2}$, όπου $a, b \in \mathbb{Q}$. Ορίζουμε την απεικόνιση:

$$\sigma : \mathbb{Q}(\sqrt{2}) \rightarrow \mathbb{Q}(\sqrt{2})$$

με τον τύπο:

$$\sigma(a + b\sqrt{2}) = a - b\sqrt{2}, \quad \forall a, b \in \mathbb{Q}$$

Η σ αποτελεί αυτομορφισμό του σώματος L που αφήνει σταθερό το υποσώμα \mathbb{Q} (K -αυτομορφισμός), καθώς ικανοποιεί τις ιδιότητες:

Έστω $z_1 = a + b\sqrt{2}$ και $z_2 = c + d\sqrt{2}$. Τότε

- $\sigma(z_1 + z_2) = \sigma((a + c) + (b + d)\sqrt{2}) = (a + c) - (b + d)\sqrt{2} = (a - b\sqrt{2}) + (c - d\sqrt{2}) = \sigma(z_1) + \sigma(z_2)$
- $\sigma(z_1 \cdot z_2) = \sigma((ac + 2bd) + (ad + bc)\sqrt{2}) = (ac + 2bd) - (ad + bc)\sqrt{2} = \sigma(z_1) \cdot \sigma(z_2)$
- Για κάθε $q \in \mathbb{Q}$ (όπου $b = 0$), έχουμε $\sigma(q) = \sigma(q + 0\sqrt{2}) = q - 0\sqrt{2} = q$.
- Παρατηρούμε ότι ο σ μεταθέτει τις ρίζες του ανάγωγου πολυωνύμου $p(x) = x^2 - 2 \in \mathbb{Q}[x]$, καθώς $\sigma(\sqrt{2}) = -\sqrt{2}$ και $\sigma(-\sqrt{2}) = \sqrt{2}$.

Άρα,

$$\text{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) = \{\text{id}, \sigma\} \cong \mathbb{Z}_2$$

3.1.2 Η Ομάδα Galois $\text{Gal}(L/K)$

Όρισμός 3.1.2 (K-αυτομορφισμός) Έστω L/K μια επέκταση σωμάτων. Ένας αυτομορφισμός $\sigma \in \text{Aut}(L)$ ονομάζεται **K-αυτομορφισμός**, αν για κάθε $k \in K$ ισχύει:

$$\sigma(k) = k$$

Δηλαδή, ο σ δρα ως η ταυτοτική απεικόνιση πάνω στο K .

Παράδειγμα Στους μιγαδικούς αριθμούς \mathbb{C} , όπου σ ένας αυτομορφισμός του \mathbb{C} υπεράνω του \mathbb{R} . Για κάθε τέτοιο αυτομορφισμό προκύπτει ότι $\sigma(0) = 0, \sigma(1) = 1, \sigma(-1) = -1$. Επομένως $\sigma(i^2) = (\sigma(i))^2 = -1$ και έτσι $\sigma(i) = \pm i$. Επειδή τα 1 και i σχηματίζουν μια βάση του \mathbb{C} υπεράνω του \mathbb{R} , οι εικόνες τους προσδιορίζουν πλήρως έναν αυτομορφισμό. Συνεπώς, υπάρχουν ακριβώς 2 αυτομορφισμοί του \mathbb{C} , οι:

- $\sigma_1 : 1, i \rightarrow i$ ο ταυτοτικός αυτομορφισμός, και
- $\sigma_2 : 1, i \rightarrow -i$

Όρισμός 3.1.3 (Ομάδα Galois) Έστω L/K μια επέκταση σωμάτων. Το σύνολο όλων των αυτομορφισμών του L που αφήνουν σταθερό κάθε στοιχείο του K ονομάζεται ομάδα των K -αυτομορφισμών του L και συμβολίζεται με $\text{Aut}(L/K)$. Στην περίπτωση που η επέκταση L/K είναι επέκταση Galois, η ομάδα αυτή ονομάζεται Ομάδα Galois της επέκτασης και συμβολίζεται με $\text{Gal}(L/K)$.

$$\text{Gal}(L/K) = \{\sigma \in \text{Aut}(L) \mid \sigma(a) = a, \forall a \in K\}$$

Η ομάδα αυτή είναι υποομάδα της $\text{Aut}(L)$. Η σημασία της έγκειται στο γεγονός ότι αν ένα πολυώνυμο $f(x)$ έχει συντελεστές στο K , τότε κάθε στοιχείο της $\text{Gal}(L/K)$ μεταθέτει τις ρίζες του $f(x)$ που βρίσκονται στο L . Αυτό συνδέει άμεσα τις αλγεβρικές ιδιότητες των ριζών με τη δομή της ομάδας.

Όρισμός 3.1.4 (Σταθερό Σώμα) Αν σ είναι ένας ισομορφισμός ενός σώματος K πάνω σε κάποιο σώμα, τότε ένα στοιχείο a του K **μένει σταθερό** από τον σ , αν $\sigma(a)=a$. Μια οικογένεια H ισομορφισμών του K **αφήνει ένα υπόσωμα F του K σταθερό**, αν κάθε $a \in F$ μένει σταθερό από κάθε $\sigma \in H$. Αν το $\{\sigma\}$ αφήνει το F σταθερό, τότε λέμε ότι ο σ **αφήνει το F σταθερό**.

Θεώρημα Έστω $\{\sigma_i | i \in I\}$ είναι μια οικογένεια αυτομορφισμών ενός σώματος K . Τότε το σύνολο $K_{\{\sigma_i\}}$ όλων των $a \in K$, που μένουν σταθερά από κάθε $\sigma_i, i \in I$, είναι ένα υπόσωμα του K .

Απόδειξη. Αν $\sigma_i(a) = a$ και $\sigma_i(b) = b$ για κάθε $i \in I$, τότε

- $\sigma_i(a \pm b) = \sigma_i(a) \pm \sigma_i(b) = a \pm b$ και
- $\sigma_i(ab) = \sigma_i(a)\sigma_i(b) = ab$ για κάθε $i \in I$. Επίσης, αν $b \neq 0$, τότε
- $\sigma_i(a/b) = \sigma_i(a)/\sigma_i(b) = a/b$ για κάθε $i \in I$. Αφού οι σ_i είναι αυτομορφισμοί, έχουμε
- $\sigma_i(0) = 0$ και $\sigma_i(1) = 1$ για κάθε $i \in I$. Επομένως $0, 1 \in K_{\{\sigma_i\}}$. Άρα το $K_{\{\sigma_i\}}$ είναι υπόσωμα του K .

□

3.2 Κανονικές και Διαχωρίσιμες Επεκτάσεις

Στην ενότητα αυτή θα ορίσουμε τις έννοιες της κανονικότητας και της διαχωρισιμότητας, οι οποίες αποτελούν τις αναγκαίες και ικανές συνθήκες για να χαρακτηριστεί μια επέκταση σωμάτων ως επέκταση Galois. Οι ιδιότητες αυτές είναι καθοριστικές για την απόδειξη του Θεμελιώδους Θεωρήματος της Άλγεβρας, καθώς μας επιτρέπουν να χρησιμοποιήσουμε τη δομή των ομάδων Galois για να αντλήσουμε πληροφορίες για τα σώματα \mathbb{R} και \mathbb{C} .

3.2.1 Κανονικότητα

Ένα κεντρικό πρόβλημα στην Άλγεβρα είναι η ύπαρξη ριζών για πολυώνυμα $p(t) \in K[t]$ που δεν έχουν λύση στο βασικό σώμα K . Ο απώτερος στόχος μας είναι να δείξουμε ότι κάθε τέτοιο πολυώνυμο στο $\mathbb{C}[t]$ αναλύεται πλήρως.

Για τον σκοπό αυτό, χρησιμοποιούμε την έννοια του Σώματος Ανάλυσης του $f(x)$ πάνω από το K , το οποίο, όπως ορίστηκε προηγουμένως (Ορισμός 2.4.1), αποτελεί την ελάχιστη επέκταση L στην οποία το πολυώνυμο διασπάται πλήρως σε γραμμικούς παράγοντες.

Ορισμός 3.2.1(Κανονική Επέκταση) Μια πεπερασμένη επέκταση L/K ονομάζεται **κανονική**, αν είναι σώμα ανάλυσης κάποιου πολυωνύμου $f(x) \in K[x]$. Ισοδύναμα, η επέκταση είναι κανονική αν κάθε ανάγωγο πολυώνυμο του $K[x]$ που έχει μία ρίζα στο L , αναλύεται πλήρως εντός του L .

Η κανονικότητα διασφαλίζει ότι η ομάδα Galois διακρίνει όλες τις δυνατές συμμετρίες των ριζών, καθιστώντας την αντιστοιχία Galois αμφιμονοσήμαντη.

Παράδειγμα Η επέκταση $\mathbb{C} : \mathbb{R}$ είναι κανονική, καθώς κάθε πολυώνυμο (ανάγωγο ή μη) αναλύεται πλήρως στο \mathbb{C} .

Αντιπαράδειγμα Έστω a η πραγματική κυβική ρίζα του 2 και θεωρούμε την επέκταση $\mathbb{Q}(a) : \mathbb{Q}$. Το ανάγωγο πολυώνυμο $t^3 - 2$ έχει μία ρίζα, συγκεκριμένα το a , στο $\mathbb{Q}(a)$, αλλά δεν αναλύεται πλήρως στο $\mathbb{Q}(a)$. Αν αναλυόταν, τότε θα υπήρχαν τρεις πραγματικές κυβικές ρίζες του 2, μη όλες ίσες μεταξύ τους. Αυτό είναι άτοπο.

Θεώρημα Μια πεπερασμένη επέκταση $L : K$ είναι κανονική αν και μόνο αν το L αποτελεί σώμα ανάλυσης κάποιου πολυωνύμου $f(x) \in K[x]$.

Απόδειξη. (\Rightarrow) Έστω ότι η επέκταση $L : K$ είναι κανονική και πεπερασμένη.

Εφόσον είναι πεπερασμένη, επιλέγουμε ένα σύνολο γεννητόρων a_1, a_2, \dots, a_s τέτοιο ώστε $L = K(a_1, a_2, \dots, a_s)$. Για κάθε γεννήτορα a_i , θεωρούμε το ελάχιστο πολυώνυμο $m_i(x)$ πάνω από το K .

Εφόσον κάθε $m_i(x)$ είναι ανάγωγο και έχει τουλάχιστον μία ρίζα (το a_i) στο σώμα L , από ιδιότητα της κανονικότητας το $m_i(x)$ να αναλύεται πλήρως σε γραμμικούς παράγοντες εντός του L .

Θεωρούμε το πολυώνυμο

$$f(x) = m_1(x) \cdot m_2(x) \cdots m_s(x)$$

Είναι σαφές ότι το $f(x)$ αναλύεται πλήρως στο L , και εφόσον το L παράγεται από τις ρίζες αυτών των πολυωνύμων, το L είναι εξ ορισμού το σώμα ανάλυσης του $f(x)$ πάνω από το K .

(\Leftarrow) Υποθέτουμε ότι το L είναι σώμα ανάλυσης ενός πολυωνύμου $g(x) \in K[x]$. Θέλουμε να δείξουμε ότι η επέκταση είναι κανονική.

Έστω $f(x)$ ένα ανάγωγο πολυώνυμο στο $K[x]$ που διαθέτει μια ρίζα θ_1 στο L . Πρέπει να αποδείξουμε ότι όλες οι υπόλοιπες ρίζες του $f(x)$ ανήκουν επίσης στο L .

Έστω M μια επέκταση του L που περιέχει όλες τις ρίζες του $f(x)$. Αν θ_2 είναι μια άλλη ρίζα του $f(x)$ στο M , θεωρούμε τους πύργους επεκτάσεων:

1. $K \subseteq K(\theta_1) \subseteq L(\theta_1)$
2. $K \subseteq K(\theta_2) \subseteq L(\theta_2)$

Από πολλαπλασιαστική ιδιότητα του βαθμού, έχουμε:

$$[L(\theta_j) : K] = [L(\theta_j) : L] \cdot [L : K] = [L(\theta_j) : K(\theta_j)] \cdot [K(\theta_j) : K]$$

Λόγω της αναγωγικότητας του f , οι επεκτάσεις $K(\theta_1)$ και $K(\theta_2)$ είναι ισόμορφες. Επειδή το L είναι σώμα ανάλυσης του g πάνω από το K , το $L(\theta_j)$ είναι σώμα ανάλυσης του g πάνω από το $K(\theta_j)$.

Από τη μοναδικότητα των σωμάτων ανάλυσης, οι επεκτάσεις $L(\theta_1) : K(\theta_1)$ και $L(\theta_2) : K(\theta_2)$ έχουν τον ίδιο βαθμό.

Συνεπώς, $[L(\theta_1) : L] = [L(\theta_2) : L]$. Εφόσον $\theta_1 \in L$, ο βαθμός είναι 1, άρα και $[L(\theta_2) : L] = 1$, γεγονός που συνεπάγεται ότι $\theta_2 \in L$. Η επέκταση είναι λοιπόν κανονική.

□

Για την πλήρη κατανόηση του παραπάνω θεωρήματος θα δοθεί το ακόλουθο παράδειγμα:

Παράδειγμα Θεωρούμε το πολυώνυμο $g(x) = (x^2 - 2)(x^2 + 1) \in \mathbb{Q}[x]$. Οι ρίζες του είναι οι $\{\sqrt{2}, -\sqrt{2}, i, -i\}$. Το μικρότερο σώμα που περιέχει όλες αυτές τις ρίζες είναι το $L = \mathbb{Q}(\sqrt{2}, i)$. Επομένως, το L είναι σώμα ανάλυσης του $g(x)$. Με βάση το παραπάνω θεώρημα η επέκταση $L : \mathbb{Q}$ πρέπει να είναι κανονική. Αυτό σημαίνει ότι αν πάρουμε οποιοδήποτε ανάγωγο πολυώνυμο, π.χ. το $x^2 - 2$, εφόσον έχει μία ρίζα στο L ($\sqrt{2}$), πρέπει να έχει και την άλλη ($-\sqrt{2}$). Πράγματι, $-\sqrt{2} = (-1) \cdot \sqrt{2} \in L$.

3.2.2 Διαχωρησιμότητα

Η διαχωρισιμότητα αποτελεί την δεύτερη απαραίτητη προϋπόθεση για τον χαρακτηρισμό μιας επέκτασης ως *Galois*. Ενώ η κανονικότητα εξασφαλίζει ότι το σώμα περιέχει όλες τις ρίζες ενός πολυωνύμου, η διαχωρισιμότητα εξασφαλίζει ότι οι ρίζες αυτές είναι διακριτές μεταξύ τους.

Ορισμός 3.2.2 Ένα ανάγωγο πολυώνυμο $f(x) \in K[x]$ ονομάζεται **διαχωρίσιμο**, αν όλες οι ρίζες του σε ένα σώμα ανάλυσης είναι απλές. Αντίστοιχα, ένα στοιχείο a ονομάζεται διαχωρίσιμο αν το ελάχιστο πολυώνυμό του είναι διαχωρίσιμο.

Αν το $f(x)$ είναι διαχωρίσιμο βαθμού n , τότε στο σώμα ανάλυσής του λαμβάνει τη μορφή:

$$f(x) = k(x - a_1)(x - a_2) \dots (x - a_n)$$

όπου $a_j \neq a_i$ για κάθε $i \neq j$.

Όπως σημειώνεται στην κλασική βιβλιογραφία, ο Évariste Galois δεν όρισε ρητά τη διαχωρισιμότητα, καθώς εργάστηκε αποκλειστικά με το σώμα των μιγαδικών αριθμών \mathbb{C} . Στο \mathbb{C} , όπως και σε κάθε σώμα χαρακτηριστικής 0, η διαχωρισιμότητα είναι μια αυτόματη ιδιότητα.

Στην παρούσα εργασία, η διασφάλιση της διαχωρισιμότητας είναι κρίσιμη για την απόδειξη του Θεμελιώδους Θεωρήματος της Άλγεβρας. Εφόσον το βασικό μας σώμα είναι το \mathbb{R} (ή το \mathbb{C}), ισχύουν τα εξής:

1. Κάθε ανάγωγο πολυώνυμο $f(x) \in \mathbb{R}[x]$ έχει μέγιστο κοινό διαιρέτη με την παράγωγό του $f'(x)$ ίσο με τη μονάδα ($\gcd(f, f') = 1$).
2. Αυτό συνεπάγεται ότι το $f(x)$ δεν μπορεί να έχει πολλαπλές ρίζες.

Επειδή εργαζόμαστε σε σώματα χαρακτηριστικής 0, κάθε κανονική επέκταση που θα κατασκευάσουμε στην πορεία της απόδειξης είναι αυτόματα διαχωρίσιμη.

Παράδειγμα Το πολυώνυμο $t^4 + t^3 + t^2 + t + 1$ είναι διαχωρίσιμο πάνω από το \mathbb{Q} , καθώς οι ρίζες του στο \mathbb{C} είναι οι $e^{2\pi i/5}, e^{4\pi i/5}, e^{6\pi i/5}, e^{8\pi i/5}$, οι οποίες είναι όλες διαφορετικές μεταξύ τους.

3.3 Επεκτάσεις Galois

Στις προηγούμενες ενότητες εξετάσαμε τις έννοιες της κανονικότητας και της διαχωρισιμότητας. Μια επέκταση που συγκεντρώνει και τα δύο αυτά χαρακτηριστικά ονομάζεται επέκταση Galois. Οι επεκτάσεις αυτές είναι οι πλέον «συμμετρικές» επεκτάσεις σωμάτων, καθώς διαθέτουν τον μέγιστο δυνατό αριθμό αυτομορφισμών σε σχέση με τον βαθμό τους.

Ορισμός 3.3.1 (Επέκταση Galois) Μια πεπερασμένη επέκταση σωμάτων L/K ονομάζεται **επέκταση Galois** εάν είναι ταυτόχρονα κανονική και διαχωρίσιμη.

Στην περίπτωση των σωμάτων χαρακτηριστικής 0 (όπως το \mathbb{R} και το \mathbb{C}), ο ορισμός απλοποιείται: μια επέκταση είναι Galois αν και μόνο αν είναι κανονική (δηλαδή σώμα ανάλυσης κάποιου πολυωνύμου).

Ισοδύναμοι ορισμοί μιας επέκτασης Galois:

1. Το σώμα σταθερών της ομάδας Galois $Gal(L/K)$ είναι ακριβώς το βασικό σώμα K (δηλαδή $L^{Gal(L/K)} = K$).
2. Η τάξη της ομάδας Galois ισούται με τον βαθμό της επέκτασης: $|Gal(L/K)| = [L : K]$.
3. Το L είναι το σώμα ανάλυσης ενός διαχωρίσιμου πολυωνύμου πάνω από το K .

Οι επεκτάσεις Galois παρουσιάζουν ορισμένες ιδιότητες που τις καθιστούν «σταθερές» αλγεβρικές δομές:

1. **Μεταβατικότητα:** Αν L/K είναι μια επέκταση Galois και M είναι ένα ενδιάμεσο σώμα ($K \subset M \subset L$), τότε η επέκταση L/M είναι πάντα Galois.
2. **Διατήρηση υπό σύνθεση:** Αν οι L_1/K και L_2/K είναι επεκτάσεις Galois, τότε και η σύνθεσή τους (το μικρότερο υποσώμα του L που περιέχει ταυτόχρονα τα σώματα L_1 και L_2) L_1L_2/K είναι επέκταση Galois.

Παράδειγμα Η επέκταση \mathbb{C}/\mathbb{R} είναι η πλέον θεμελιώδης επέκταση για το $\Theta\Theta A$. Είναι σώμα ανάλυσης του

$$x^2 + 1 \in \mathbb{R}[x]$$

Με βαθμό $[\mathbb{C} : \mathbb{R}] = 2$. Η ομάδα Galois είναι $Gal(\mathbb{C}/\mathbb{R}) = \{id, \sigma\}$, όπου σ είναι η μιγαδική συζυγία. Επειδή $|Gal| = 2 = [\mathbb{C} : \mathbb{R}]$, η επέκταση είναι Galois.

Παράδειγμα Η επέκταση $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$ είναι σώμα ανάλυσης του

$$(x^2 - 2)(x^2 - 3) \in \mathbb{Q}[x]$$

Με βαθμό $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$ και βάση $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$. Η ομάδα Galois έχει 4 στοιχεία που καθορίζονται από τις εναλλαγές προσήμων των $\sqrt{2}$ και $\sqrt{3}$. Είναι ισόμορφη με την ομάδα Klein V_4 . Άρα είναι επέκταση Galois.

Παράδειγμα Η επέκταση $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$. Το ελάχιστο πολυώνυμο είναι το

$$x^3 - 2$$

Με βαθμό επέκτασης 3. Ωστόσο, η ομάδα Galois $Gal(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})$ έχει μόνο ένα στοιχείο (την ταυτοτική απεικόνιση), διότι οι άλλες δύο ρίζες του $x^3 - 2$ είναι μιγαδικές και δεν ανήκουν στο σώμα $\mathbb{Q}(\sqrt[3]{2})$. Επειδή $1 \neq 3$, η επέκταση **δεν** είναι Galois (στερείται κανονικότητας).

3.4 Το Θεμελιώδες Θεώρημα της Θεωρίας Galois

Το Θεμελιώδες Θεώρημα της Θεωρίας Galois ($\Theta\Theta\Theta G$) αποτελεί το αποκορύφωμα της θεωρίας μας, καθώς μετατρέπει το πρόβλημα της εύρεσης ενδιάμεσων σωμάτων σε ένα πρόβλημα ταξινόμησης υποομάδων μιας πεπερασμένης ομάδας. Στην παρούσα εργασία, το θεώρημα αυτό θα μας επιτρέψει να αποδείξουμε την ανυπαρξία επεκτάσεων του \mathbb{C} αναλύοντας τη δομή της ομάδας Galois.

3.4.1 Προαπαιτούμενα και Συμβολισμοί

Έστω L/K μια επέκταση σωμάτων στο \mathbb{C} με ομάδα Galois G , η οποία αποτελείται από όλους τους K -αυτομορφισμούς του L . Έστω \mathcal{F} το σύνολο των ενδιάμεσων σωμάτων M ($K \subseteq M \subseteq L$) και \mathcal{G} το σύνολο όλων των υποομάδων H της G . Ορίζουμε δύο απεικονίσεις:

- Αν $M \in \mathcal{F}$, τότε M^* είναι η ομάδα όλων των M -αυτομορφισμών του L . Συμβολίζεται

$$M^* = \text{Gal}(L/M)$$

- Αν $H \in \mathcal{G}$, τότε H^\dagger είναι το σώμα σταθερών της H . Δηλαδή, είναι το σύνολο όλων των στοιχείων του L που παραμένουν αναλλοίωτα υπό τη δράση κάθε αυτομορφισμού της H .

Λήμμα Έστω L/K μια επέκταση σωμάτων, M ένα ενδιάμεσο σώμα και τ ένας K -αυτομορφισμός του L . Τότε $\tau(M)^* = \tau M^* \tau^{-1}$.

Απόδειξη. Θέτουμε $M' = \tau(M) = \{\tau(m) \mid m \in M\}$. Σύμφωνα με τον ορισμό, η ομάδα M'^* (δηλαδή η $\text{Gal}(L/M')$) αποτελείται από όλους τους αυτομορφισμούς $\sigma \in \text{Gal}(L/K)$ που αφήνουν σταθερό κάθε στοιχείο του M' .

(\Rightarrow) Έστω ένα τυχαίο στοιχείο της μορφής $\tau\gamma\tau^{-1}$, όπου $\gamma \in M^*$. Θέλουμε να δείξουμε ότι αυτός ο αυτομορφισμός αφήνει σταθερό κάθε στοιχείο $x' \in M'$. Από τον ορισμό του M' , κάθε $x' \in M'$ γράφεται ως $x' = \tau(x)$ για κάποιο $x \in M$. Εφαρμόζουμε τον αυτομορφισμό $\tau\gamma\tau^{-1}$ στο x' :

$$(\tau\gamma\tau^{-1})(x') = (\tau\gamma\tau^{-1})(\tau(x)) = \tau(\gamma(\tau^{-1}(\tau(x)))) = \tau(\gamma(x))$$

Επειδή $x \in M$ και $\gamma \in M^*$, ο γ αφήνει το x σταθερό ($\gamma(x) = x$). Επομένως:

$$\tau(\gamma(x)) = \tau(x) = x'$$

Αφού ο $\tau\gamma\tau^{-1}$ αφήνει σταθερό ένα τυχαίο στοιχείο $x' \in M'$, συμπεραίνουμε ότι $\tau\gamma\tau^{-1} \in M'^*$.

(\Leftarrow) Έστω τώρα ένας αυτομορφισμός $\sigma \in M'^*$. Θέλουμε να δείξουμε ότι ο σ μπορεί να γραφτεί στη μορφή $\tau\gamma\tau^{-1}$ για κάποιο $\gamma \in M^*$. Αυτό ισοδυναμεί με το να δείξουμε ότι ο αυτομορφισμός $\gamma = \tau^{-1}\sigma\tau$ ανήκει στο M^* . Για να ανήκει ο γ στο M^* , πρέπει να αφήνει σταθερό κάθε $x \in M$. Έχουμε:

$$\gamma(x) = (\tau^{-1}\sigma\tau)(x) = \tau^{-1}(\sigma(\tau(x)))$$

Επειδή $\tau(x) \in M'$ και ο σ ανήκει στο M'^* , ο σ αφήνει το $\tau(x)$ σταθερό, δηλαδή $\sigma(\tau(x)) = \tau(x)$. Επομένως:

$$\tau^{-1}(\tau(x)) = x$$

Άρα $\gamma \in M^*$, γεγονός που συνεπάγεται ότι $\sigma = \tau\gamma\tau^{-1} \in \tau M^* \tau^{-1}$. Συμπέρασμα Από τα δύο παραπάνω βήματα προκύπτει η ισότητα των συνόλων:

$$\tau(M)^* = \tau M^* \tau^{-1}$$

□

Θεώρημα (Θεμελιώδες Θεώρημα της Θεωρίας Galois) Έστω L/K μια πεπερασμένη, κανονική επέκταση σωμάτων εντός του \mathbb{C} , με ομάδα Galois G . Τότε ισχύουν τα εξής:

1. Η ομάδα Galois G έχει τάξη ίση με τον βαθμό της επέκτασης, δηλαδή $|G| = [L : K]$.
2. Οι απεικονίσεις $*$ και \dagger είναι αντίστροφες μεταξύ τους και ορίζουν μια αμφιμονοσήμαντη αντιστοιχία που αναστρέφει τη διάταξη (εγκλεισμό) μεταξύ των συνόλων \mathcal{F} και \mathcal{G} .
3. Αν M είναι ένα ενδιάμεσο σώμα, τότε:
 - $[L : M] = |M^*|$
 - $[M : K] = |G|/|M^*|$
4. Ένα ενδιάμεσο σώμα M είναι κανονική επέκταση του K αν και μόνο αν η ομάδα M^* είναι κανονική υποομάδα της G .
5. Αν το M είναι κανονική επέκταση του K , τότε η ομάδα Galois της επέκτασης M/K είναι ισόμορφη με την ομάδα πηλίκο G/M^* .

Απόδειξη. 1. **Τάξη της Ομάδας $|G| = [L : K]$**

Η πρόταση αυτή αποτελεί τον ορισμό των επεκτάσεων Galois. Εφόσον η επέκταση L/K είναι διαχωρίσιμη και κανονική (σώμα ανάλυσης ενός διαχωρίσιμου πολυωνύμου), ο αριθμός των K -αυτομορφισμών του L ισούται ακριβώς με τον βαθμό της επέκτασης. Αυτό προκύπτει από το γεγονός ότι κάθε K -αυτομορφισμός $\sigma \in \text{Gal}(L/K)$ καθορίζεται μονοσήμαντα από τις τιμές του στις ρίζες του πολυωνύμου $f(x)$. Συγκεκριμένα, εφόσον το σώμα ανάλυσης L παράγεται από το σώμα βάσης K και τις ρίζες $\{a_1, a_2, \dots, a_n\}$ του $f(x)$, κάθε στοιχείο του L μπορεί να εκφραστεί ως πολυωνυμική έκφραση των ριζών με συντελεστές από το K . Επειδή κάθε K -αυτομορφισμός σ οφείλει να απεικονίζει μια ρίζα a_i σε μια άλλη ρίζα a_j του ίδιου ανάγωγου πολυωνύμου (διατηρώντας τις αλγεβρικές σχέσεις), η δράση του σ σε ολόκληρο το σώμα L καθορίζεται μονοσήμαντα μόλις οριστεί η μετάθεση που προκαλεί στο σύνολο των ριζών. Στην περίπτωση διαχωρίσιμων επεκτάσεων, οι ρίζες είναι όλες διακριτές, γεγονός που εξασφαλίζει ότι υπάρχουν ακριβώς $[L : K]$ διαφορετικοί τρόποι να μεταταθούν οι ρίζες διατηρώντας τη δομή του σώματος, οδηγώντας έτσι στην ισότητα $|\text{Gal}(L/K)| = [L : K]$.

2. **Οι απεικονίσεις $*$ και \dagger είναι αντίστροφες**

Πρέπει να δείξουμε ότι $M^{*\dagger} = M$ και $H^{\dagger*} = H$.

- **Για το $M^{*\dagger} = M$:** Από τον ορισμό, το $M^{*\dagger}$ είναι το σταθερό σώμα της ομάδας $\text{Gal}(L/M)$. Είναι γνωστό ότι αν η L/K είναι επέκταση Galois, τότε κάθε ενδιάμεση επέκταση L/M είναι επίσης Galois, καθώς η κανονικότητα και η διαχωριστικότητα διατηρούνται για υποσώματα M που περιέχουν το K . Σύμφωνα με το θεώρημα του Artin για τις επεκτάσεις Galois, το σταθερό σώμα της ομάδας Galois $\text{Gal}(L/M)$ ταυτίζεται με το σώμα βάσης της επέκτασης, δηλαδή το M . Επομένως, $M^{*\dagger} = M$.
- **Για το $H^{\dagger*} = H$:** Έστω $M = H^\dagger$ το σώμα σταθερών της υποομάδας H . Από το Θεώρημα του Artin, γνωρίζουμε ότι αν H είναι μια πεπερασμένη ομάδα αυτομορφισμών, τότε $[L : H^\dagger] = |H|$. Όμως, από το μέρος (3) που έπεται, $[L : M] = |M^*|$. Συνεπώς $|H| = |M^*|$. Επειδή προφανώς $H \subseteq M^*$, η ισότητα των πληθαιρίμων συνεπάγεται $H = M^*$, δηλαδή $H = H^{\dagger*}$.

3. Βαθμοί και Τάξεις $[L : M] = |M^*|$ και $[M : K] = |G|/|M^*|$

- Η πρώτη ισότητα $[L : M] = |Gal(L/M)| = |M^*|$ προκύπτει άμεσα από το γεγονός ότι η L/M είναι επέκταση Galois (ως υπο-επέκταση μιας Galois).
- Η δεύτερη ισότητα προκύπτει από την πολλαπλασιαστική ιδιότητα του βαθμού :

$$[L : K] = [L : M] \cdot [M : K] \implies |G| = |M^*| \cdot [M : K] \implies [M : K] = \frac{|G|}{|M^*|}$$

4. Κανονικότητα Επέκτασης και Κανονικότητα Υποομάδας

Χρησιμοποιούμε το παραπάνω **Λήμμα** ($\tau(M)^* = \tau M^* \tau^{-1}$):

- (\implies): Αν η M/K είναι κανονική, τότε για κάθε $\tau \in G$ ισχύει $\tau(M) = M$. Τότε από το λήμμα έχουμε $M^* = \tau M^* \tau^{-1}$ για κάθε $\tau \in G$, που είναι ο ορισμός της κανονικής υποομάδας.
- (\impliedby): Αν M^* είναι κανονική υποομάδα, τότε $\tau M^* \tau^{-1} = M^*$. Από το λήμμα, $\tau(M)^* = M^*$. Επειδή η αντιστοιχία είναι 1-1, προκύπτει $\tau(M) = M$. Αυτό σημαίνει ότι κάθε K -αυτομορφισμός του L περιορίζεται σε έναν αυτομορφισμό του M , άρα η M/K είναι κανονική.

5. Ισομορφισμός $Gal(M/K) \cong G/M^*$

Ορίζουμε την απεικόνιση περιορισμού $\phi : Gal(L/K) \rightarrow Gal(M/K)$ με $\phi(\sigma) = \sigma|_M$.

- Η ϕ είναι καλά ορισμένη επειδή η M/K είναι κανονική (άρα ο σ στέλνει το M στον εαυτό του).
- Η ϕ είναι ομομορφισμός ομάδων (προφανές από τη σύνθεση).
- Ο πυρήνας $Ker(\phi)$ είναι το σύνολο των $\sigma \in G$ που δρουν ως ταυτότητα στο M . Αυτό είναι εξ ορισμού η ομάδα M^* .
- Από το Πρώτο Θεώρημα Ισομορφισμών: $Im(\phi) \cong G/M^*$. Επειδή $|Im(\phi)| = [M : K] = |G/M^*|$, η ϕ είναι επιμορφισμός. Άρα $Gal(M/K) \cong G/M^*$.

□

3.5 Προαπαιτούμενα από τη Θεωρία Ομάδων

Στην υποενότητα αυτή θα συγκεντρώσουμε τα εργαλεία από τη Θεωρία Ομάδων που είναι απολύτως απαραίτητα για την απόδειξη του Θεμελιώδους Θεωρήματος της Άλγεβρας. Η στρατηγική μας βασίζεται στο γεγονός ότι η ομάδα Galois μιας επέκτασης των πραγματικών αριθμών είναι μια 2-ομάδα, και τα θεωρήματα Sylow μας διαβεβαιώνουν ότι αν μια δύναμη ενός πρώτου αριθμού διαιρεί την τάξη $|G|$ (όπου G μια πεπερασμένη αβελιανή ομάδα), τότε θα υπάρχει υποομάδα της G , που θα έχει τάξη αυτή τη δύναμη του πρώτου αριθμού. Ακόμη μας δίνουν πληροφορίες και για το πλήθος αυτών των υποομάδων.

Ορισμός 3.5.1 (p -ομάδα) Μια ομάδα G λέγεται p -ομάδα αν κάθε στοιχείο της G έχει τάξη κάποια δύναμη του πρώτου αριθμού p . Μια υποομάδα H της ομάδας G λέγεται p -υποομάδα της G αν η H είναι p -ομάδα.

Θεώρημα (Cauchy) Έστω G μια πεπερασμένη ομάδα· υποθέτουμε ότι ο p διαιρεί την $|G|$. Τότε η G έχει ένα στοιχείο τάξης p , επομένως και μια υποομάδα τάξης p .

Πόρισμα Έστω G μια πεπερασμένη ομάδα. Η G είναι p -ομάδα τότε και μόνον τότε όταν η τάξη της είναι δύναμη του p , δηλαδή $|G| = p^n$ για κάποιο φυσικό αριθμό $n \geq 1$.

Στην απόδειξη του ΘΘΑ, θα εστιάσουμε αποκλειστικά στις 2-ομάδες ($|G| = 2^n$). Αυτό συμβαίνει διότι η επέκταση \mathbb{C}/\mathbb{R} έχει βαθμό 2, και κάθε περαιτέρω επέκταση που θα εξετάσουμε θα δειχθεί ότι σχετίζεται με δυνάμεις του 2.

3.5.1 Θεωρήματα Sylow

Τα θεωρήματα Sylow αποτελούν τη βάση για τη μελέτη των υποομάδων μιας πεπερασμένης ομάδας. Μας εξασφαλίζουν την ύπαρξη υποομάδων με συγκεκριμένες τάξεις.

1ο Θεώρημα Sylow (Ύπαρξη) Έστω G μια πεπερασμένη ομάδα και $|G| = p^n \cdot m$, όπου ο πρώτος p δεν διαιρεί το m . Τότε η G περιέχει τουλάχιστον μία υποομάδα τάξης p^k για κάθε $1 \leq k \leq n$.

3ο Θεώρημα Sylow (Πλήθος) Το πλήθος n_p των Sylow p -υποομάδων της G ικανοποιεί τις συνθήκες:

- $n_p \equiv 1 \pmod{p}$
- n_p διαιρεί την τάξη $|G|$.

3.5.2 Ιδιότητες p -ομάδων

Οι p -ομάδες έχουν μια πολύ αυστηρή ιεραρχική δομή, η οποία είναι το κλειδί για να δείξουμε ότι μια επέκταση μπορεί να αναλυθεί σε διαδοχικές επεκτάσεις βαθμού p .

Ιδιότητα 1 (Μη τετριμμένο κέντρο) Κάθε μη τετριμμένη p -ομάδα G έχει μη τετριμμένο κέντρο $Z(G) \neq \{e\}$. Αυτό μας επιτρέπει να χρησιμοποιούμε επαγωγή στην τάξη της ομάδας.

Ιδιότητα 2 (Ύπαρξη υποομάδας δείκτη p) Αν G είναι μια p -ομάδα τάξης p^n , τότε για κάθε $k \in \{0, 1, \dots, n\}$ η G περιέχει μια κανονική υποομάδα τάξης p^k . Ειδικότερα, μια ομάδα τάξης p^n περιέχει πάντα μια υποομάδα H με δείκτη p ($[G : H] = p$).

4 Αναλυτικά Προαπαιτούμενα και η Δομή του \mathbb{C}

Τώρα ήρθε η ώρα να θεμελιώσουμε τη δομή του σώματος των μιγαδικών αριθμών ως την κύρια επέκταση των πραγματικών. Αυτή η ενότητα λειτουργεί ως το σημείο εκκίνησης για την απόδειξη του ΘΘΑ, καθώς ορίζει τον «χώρο» στον οποίο θα δείξουμε ότι κάθε πολυώνυμο έχει ρίζα.

Πριν προχωρήσουμε στην αλγεβρική απόδειξη, είναι απαραίτητο να ορίσουμε με ακρίβεια το σώμα των μιγαδικών αριθμών και να αναδείξουμε τις ιδιότητες εκείνες του σώματος των πραγματικών αριθμών \mathbb{R} οι οποίες καθιστούν το \mathbb{C} «σχεδόν» αλγεβρικά κλειστό, δηλαδή κάθε μη σταθερό πολυώνυμο $f(x) \in \mathbb{C}[x]$ έχει τουλάχιστον μία ρίζα στο \mathbb{C} .

4.1 Το Σώμα των Μιγαδικών Αριθμών \mathbb{C}

Το σώμα των μιγαδικών αριθμών \mathbb{C} μπορεί να οριστεί αλγεβρικά ως η επέκταση του σώματος των πραγματικών αριθμών \mathbb{R} μέσω της προσθήκης μιας ρίζας του ανάγωγου πολυωνύμου $x^2 + 1 \in \mathbb{R}[x]$.

4.1.1 Η Κατασκευή $\mathbb{C} = \mathbb{R}(i)$

Σύμφωνα με τη θεωρία σωμάτων, εφόσον το $x^2 + 1$ δεν έχει πραγματικές ρίζες (καθώς $x^2 + 1 \geq 1$ για κάθε $x \in \mathbb{R}$), είναι ανάγωγο πάνω από το \mathbb{R} . Ορίζουμε ως φανταστική μονάδα i το στοιχείο εκείνο για το οποίο ισχύει $i^2 = -1$.

Το σώμα των μιγαδικών αριθμών είναι η απλή αλγεβρική επέκταση:

$$\mathbb{C} = \mathbb{R}(i) = \{a + bi \mid a, b \in \mathbb{R}\}$$

Θεωρούμε λοιπόν, το \mathbb{R} ως υποσύνολο των μιγαδικών αριθμών, ταυτίζοντας κάθε πραγματικό αριθμό r με τον μιγαδικό $r + 0i$.

Για παράδειγμα, γράφουμε τον $3 + 0i$ ως 3 , τον $-\pi + 0i$ ως $-\pi$ κ.ο.κ.. Ομοίως, γράφουμε τους $0 + 1i$ ως i και γενικότερα τον $0 + si$ ως si .

4.1.2 Ο Βαθμός της Επέκτασης $[\mathbb{C} : \mathbb{R}] = 2$

Ένα από τα πιο κρίσιμα δεδομένα για την απόδειξη με τη θεωρία Galois είναι ο βαθμός της επέκτασης. Το στοιχείο i είναι ρίζα του πολυωνύμου $f(x) = x^2 + 1 \in \mathbb{R}[x]$.

- Το $x^2 + 1$ είναι **ανάγωγο** πάνω από το \mathbb{R} , διότι είναι πολυώνυμο 2ου βαθμού χωρίς πραγματικές ρίζες (η διακρίνουσα είναι $\Delta = -4 < 0$).
- Εφόσον το $x^2 + 1$ είναι μονικό (με μεγιστοβάθμιο συντελεστή τη μονάδα) και ανάγωγο, αποτελεί το **ελάχιστο πολυώνυμο του i** πάνω από το \mathbb{R} .
- Ο **βαθμός** της απλής αλγεβρικής επέκτασης ισούται με τον βαθμό του ελάχιστου πολυωνύμου:

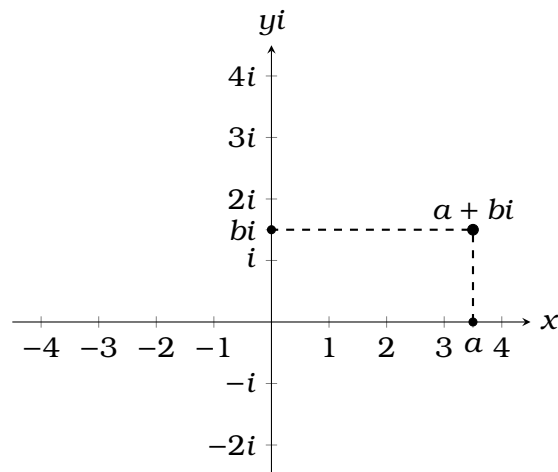
$$[\mathbb{R}(i) : \mathbb{R}] = \deg(x^2 + 1) = 2$$

Από γεωμετρικής σκοπιάς, ως διανυσματικός χώρος πάνω από το \mathbb{R} , το \mathbb{C} έχει διάσταση 2. Αυτό σημαίνει ότι κάθε μιγαδικός αριθμός z μπορεί να εκφραστεί ως μοναδικός γραμμικός

συνδυασμός δύο βασικών στοιχείων. Η κανονική βάση είναι το σύνολο $\{1, i\}$.

$$z = a \cdot 1 + b \cdot i, \quad a, b \in \mathbb{R}$$

Η δομή αυτή ταυτίζει το σώμα των μιγαδικών αριθμών με το Ευκλείδειο επίπεδο \mathbb{R}^2 , όπου ο άξονας των x αντιστοιχεί στο πραγματικό μέρος και ο άξονας των y στο φανταστικό.



4.2 Ιδιότητα 1: Ρίζες Πολυωνύμων Περιττού Βαθμού

Η πρώτη αναλυτική ιδιότητα που απαιτείται για την απόδειξη του Θεμελιώδους Θεωρήματος της Άλγεβρας αφορά τη συμπεριφορά των πολυωνυμικών συναρτήσεων περιττού βαθμού. Η ιδιότητα αυτή βασίζεται στην **πληρότητα** των πραγματικών αριθμών.

4.2.1 Το Θεώρημα Ενδιάμεσης Τιμής (Θ.Ε.Τ.)

Για την απόδειξη της ύπαρξης ριζών, βασίζομαστε σε ένα από τα κεντρικότερα θεωρήματα της Πραγματικής Ανάλυσης:

Θεώρημα (Bolzano / Ενδιάμεσης Τιμής) Έστω μια συνεχή συνάρτηση $f : [a, b] \rightarrow \mathbb{R}$. Αν ο αριθμός y βρίσκεται μεταξύ των $f(a)$ και $f(b)$, τότε υπάρχει τουλάχιστον ένα $c \in [a, b]$ τέτοιο ώστε $f(c) = y$. Ειδικότερα, αν $f(a) \cdot f(b) < 0$ (δηλαδή οι τιμές στα άκρα είναι ετερόσημες), τότε υπάρχει τουλάχιστον μία ρίζα $c \in (a, b)$ τέτοια ώστε $f(c) = 0$.

Πρόταση (Ρίζες Πολυωνύμων Περιττού Βαθμού) Κάθε πολυώνυμο $P(x) \in \mathbb{R}[x]$ περιττού βαθμού έχει τουλάχιστον μία πραγματική ρίζα.

Απόδειξη. Έστω $P(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_0$ με n περιττό και $a_n \neq 0$. Χωρίς βλάβη της γενικότητας, υποθέτουμε $a_n > 0$.

- $x \rightarrow +\infty$: ο μεγιστοβάθμιος όρος $a_n x^n$ κυριαρχεί, άρα $P(x) \rightarrow +\infty$. Επομένως, υπάρχει ένας πολύ μεγάλος θετικός αριθμός b τέτοιος ώστε $P(b) > 0$.
- $x \rightarrow -\infty$: επειδή ο εκθέτης n είναι περιττός, ο όρος x^n διατηρεί το αρνητικό πρόσημο. Επομένως $P(x) \rightarrow -\infty$. Άρα, υπάρχει ένας πολύ μικρός (μεγάλος αρνητικός) αριθμός a τέτοιος ώστε $P(a) < 0$.

Η πολυωνυμική συνάρτηση $P(x)$ είναι συνεχής σε όλο το \mathbb{R} . Στο διάστημα $[a, b]$, έχουμε $P(a) < 0$ και $P(b) > 0$. Σύμφωνα με το Θεώρημα Ενδιάμεσης Τιμής, υπάρχει τουλάχιστον ένα $c \in (a, b)$ τέτοιο ώστε $P(c) = 0$. \square

Η παραπάνω πρόταση έχει ισχυρή αλγεβρική συνέπεια :

Δεν υπάρχουν επεκτάσεις του \mathbb{R} περιττού βαθμού μεγαλύτερου του 1.

Αν υπήρχε μια επέκταση L/\mathbb{R} με $[L : \mathbb{R}] = n$ (όπου n περιττός και $n > 1$), τότε για κάθε στοιχείο $\vartheta \in L \setminus \mathbb{R}$, το ελάχιστο πολυώνυμό του θα έπρεπε να έχει βαθμό που διαιρεί το n . Άρα θα υπήρχε ένα ανάγωγο πολυώνυμο περιττού βαθμού > 1 . Όμως, η παραπάνω πρόταση μας λέει ότι κάθε τέτοιο πολυώνυμο έχει πραγματική ρίζα, άρα δεν μπορεί να είναι ανάγωγο.

Αυτός ο περιορισμός είναι που θα αναγκάσει την ομάδα *Galois* στην τελική απόδειξη να είναι μια 2-ομάδα.

4.2.2 Ιδιότητα 2: Τετραγωνικές Ρίζες στο \mathbb{C}

Η δεύτερη αναλυτική ιδιότητα που απαιτείται είναι η δυνατότητα επίλυσης κάθε δευτεροβάθμιας εξίσωσης εντός του σώματος των μιγαδικών αριθμών. Αυτό βασίζεται στην ύπαρξη τετραγωνικών ριζών για κάθε στοιχείο του \mathbb{C} .

Πρόταση (Ύπαρξη Τετραγωνικών Ριζών) Κάθε μιγαδικός αριθμός $z = a + bi \in \mathbb{C}$ έχει μια τετραγωνική ρίζα $w = u + vi \in \mathbb{C}$ τέτοια ώστε $w^2 = z$.

Απόδειξη. Αναζητούμε πραγματικούς αριθμούς u, v τέτοιους ώστε $(u + vi)^2 = a + bi$. Αναπτύσσοντας το τετράγωνο και εξισώνοντας πραγματικά και φανταστικά μέρη, προκύπτει το σύστημα :

$$\begin{cases} u^2 - v^2 = a \\ 2uv = b \\ u^2 + v^2 = \sqrt{a^2 + b^2} \end{cases}$$

Λύνοντας το σύστημα ως προς u^2 και v^2 (προσθέτοντας και αφαιρώντας την 1 και την 3), καταλήγουμε στον γενικό τύπο για τις τετραγωνικές ρίζες :

$$w = \pm \left(\sqrt{\frac{\sqrt{a^2 + b^2} + a}{2}} + i \cdot \operatorname{sgn}(b) \sqrt{\frac{\sqrt{a^2 + b^2} - a}{2}} \right)$$

Όπου $\operatorname{sgn}(b)$ είναι το πρόσημο του b (με $\operatorname{sgn}(0) = 1$). Επειδή η υπόριζη ποσότητα $\sqrt{a^2 + b^2} \pm a$ είναι πάντα μη αρνητική για κάθε $a, b \in \mathbb{R}$, οι τιμές των u, v είναι πάντα πραγματικοί αριθμοί.

Συνεπώς, $w \in \mathbb{C}$. \square

Πόρισμα Το σώμα των μιγαδικών αριθμών \mathbb{C} δεν έχει επεκτάσεις βαθμού 2.

Απόδειξη. Έστω L μια επέκταση του \mathbb{C} με $[L : \mathbb{C}] = 2$. Τότε η επέκταση αυτή παράγεται από τη ρίζα ενός τριωνύμου $f(z) = az^2 + \beta z + \gamma$ με $a, \beta, \gamma \in \mathbb{C}$. Οι ρίζες αυτού του πολυωνύμου δίνονται από τον γνωστό τύπο :

$$z = \frac{-\beta \pm \sqrt{\Delta}}{2a}, \quad \text{όπου } \Delta = \beta^2 - 4a\gamma$$

Εφόσον η διακρίνουσα Δ είναι ένας μιγαδικός αριθμός, από την προηγούμενη πρόταση γνωρίζουμε ότι η $\sqrt{\Delta}$ υπάρχει και ανήκει στο \mathbb{C} . Επομένως, και οι δύο ρίζες z_1, z_2 ανήκουν στο \mathbb{C} . Αυτό σημαίνει ότι το πολυώνυμο $f(z)$ δεν είναι ανάγωγο πάνω από το \mathbb{C} , και συνεπώς δεν μπορεί να δημιουργήσει επέκταση βαθμού 2. \square

Η σημασία της ύπαρξης τετραγωνικών ριζών στο σώμα των μιγαδικών αριθμών υπερβαίνει την απλή επίλυση δευτεροβάθμιων εξισώσεων, καθώς αποτελεί το θεμέλιο για τον περιορισμό της δομής των επεκτάσεων *Galois* πάνω από το \mathbb{R} .

Στο τελικό στάδιο της απόδειξης του Θεμελιώδους Θεωρήματος της Άλγεβρας, ο ρόλος αυτής της ιδιότητας είναι διττός:

1. Η θεωρία των p -ομάδων (εν προκειμένω των 2-ομάδων) ορίζει ότι κάθε μη τετριμμένη ομάδα G περιέχει μια υποομάδα με δείκτη $p = 2$. Μέσω της αντιστοιχίας Galois, η ύπαρξη μιας τέτοιας υποομάδας θα συνεπαγόταν την ύπαρξη μιας ενδιάμεσης επέκτασης M του \mathbb{C} με βαθμό $[M : \mathbb{C}] = 2$. Ωστόσο, η Ιδιότητα 2 αποδεικνύει ότι κάθε πολυώνυμο δεύτερου βαθμού στο $\mathbb{C}[x]$ έχει τις ρίζες του εντός του \mathbb{C} . Συνεπώς, δεν υφίσταται ανάγωγο πολυώνυμο βαθμού 2, γεγονός που ακυρώνει την πιθανότητα ύπαρξης τέτοιας επέκτασης.
2. Εφόσον αποδεικνύεται ότι το \mathbb{C} δεν επιδέχεται καμία επέκταση βαθμού 2, και έχοντας ήδη αποκλείσει επεκτάσεις περιττού βαθμού (μέσω της Ιδιότητας 1), οδηγούμαστε στο συμπέρασμα ότι η ομάδα *Galois* μιας οποιασδήποτε αλγεβρικής επέκτασης του \mathbb{R} που περιέχει το \mathbb{C} πρέπει να είναι τετριμμένη.

Κατά συνέπεια, η δυνατότητα εξαγωγής τετραγωνικής ρίζας από κάθε μιγαδικό αριθμό είναι αυτή που καθιστά το σώμα \mathbb{C} ως το μέγιστο δυνατό αλγεβρικό οικοδόμημα πάνω από τους πραγματικούς αριθμούς, ολοκληρώνοντας έτσι την απόδειξη ότι το \mathbb{C} είναι αλγεβρικά κλειστό.

5 Η Απόδειξη του Θεμελιώδους Θεωρήματος της Άλγεβρας

Στο σημείο αυτό, η εργασία ολοκληρώνεται με την απόδειξη του Θεμελιώδους Θεωρήματος της Άλγεβρας, αξιοποιώντας το θεωρητικό υπόβαθρο που αναπτύχθηκε στα προηγούμενα κεφάλαια. Έχοντας ήδη αποσαφηνίσει τις έννοιες των επεκτάσεων Galois και της αντιστοιχίας σωμάτων-ομάδων (Κεφάλαιο 3), καθώς και τις κρίσιμες αναλυτικές ιδιότητες του \mathbb{R} και του \mathbb{C} (Κεφάλαιο 4), περνάμε τώρα στο κεντρικό επιχείρημα. Η στρατηγική μας παραμένει σε εκκρεμότητα ως προς την τελική της υλοποίηση, η οποία θα διεξαχθεί στη χρήση των θεωρημάτων Sylow για ναδειχθεί ότι η ομάδα Galois της επέκτασης είναι μια 2-ομάδα (αποκλείοντας την ύπαρξη περιττών βαθμών λόγω του Θ.Ε.Τ.) και στην απόδειξη ότι η ομάδα αυτή είναι τριμμένη (αποκλείοντας επεκτάσεις βαθμού 2 λόγω της ύπαρξης τετραγωνικών ριζών στο \mathbb{C}).

Θεώρημα (Το Θεμελιώδες Θεώρημα της Άλγεβρας) *Το σώμα των μιγαδικών αριθμών \mathbb{C} είναι αλγεβρικά κλειστό, δηλαδή κάθε μη σταθερό μιγαδικό πολυώνυμο διαθέτει μια θέση μηδενισμού στο \mathbb{C} .*

5.0.1 Το Κεντρικό Επιχείρημα και η Αναγωγή στο \mathbb{R}

Ένας ορισμός του **αλγεβρικά κλειστού** σώματος είναι ότι κάθε πολυώνυμο $f(x) \in \mathbb{C}[x]$ βαθμού $n \geq 1$ έχει n ρίζες στο \mathbb{C} . Ισοδύναμα, το \mathbb{C} είναι **αλγεβρικά κλειστό** αν κάθε πεπερασμένη αλγεβρική επέκταση K του \mathbb{C} έχει βαθμό $[K : \mathbb{C}] = 1$, δηλαδή $K = \mathbb{C}$.

Η δυσκολία στην απευθείας μελέτη μιας επέκτασης K/\mathbb{C} έγκειται στο ότι χάνουμε τις πληροφορίες που μας παρέχει το σώμα των πραγματικών αριθμών \mathbb{R} , το οποίο διαθέτει την ιδιότητα της διάταξης και την έννοια της συνέχειας (μέσω της πληρότητας). Για να αξιοποιήσουμε αυτά τα αναλυτικά εργαλεία, αναγάγουμε την επέκταση K σε μια ευρύτερη δομή πάνω από το \mathbb{R} .

Έστω K μια πεπερασμένη επέκταση του \mathbb{C} . Για να διασφαλίσουμε ότι η ομάδα Galois θα περιλαμβάνει όλες τις απαραίτητες συμμετρίες, κατασκευάζουμε μια επέκταση που να είναι Galois πάνω από το \mathbb{R} . Αν το K παράγεται από μια ρίζα a ενός πολυωνύμου $f(x) \in \mathbb{C}[x]$, τότε θεωρούμε το πολυώνυμο:

$$g(x) = f(x) \cdot \bar{f}(x)$$

όπου $\bar{f}(x)$ είναι το πολυώνυμο που προκύπτει αν αντικαταστήσουμε κάθε συντελεστή c_i του $f(x)$ με τον συζυγή του \bar{c}_i .

Λήμμα Το πολυώνυμο $g(x)$ ανήκει στο $\mathbb{R}[x]$.

Απόδειξη. Η μιγαδική συζυγία είναι ένας αυτομορφισμός του \mathbb{C} που αφήνει σταθερό το \mathbb{R} . Επειδή ο συζυγής του γινομένου, $f(x) \cdot \bar{f}(x)$, είναι πάλι το $f(x) \cdot \bar{f}(x)$, οι συντελεστές του $g(x)$ είναι αναλλοίωτοι υπό τη συζυγία, άρα είναι πραγματικοί. \square

Θεωρούμε πλέον το σώμα K ως το σώμα ανάλυσης του $g(x) \in \mathbb{R}[x]$ πάνω από το \mathbb{R} . Αυτή η επιλογή είναι καθοριστική για δύο λόγους:

- Ως σώμα ανάλυσης, η επέκταση K/\mathbb{R} είναι κανονική.
- Σε σώματα χαρακτηριστικής 0 (όπως το \mathbb{R}), κάθε επέκταση είναι διαχωρίσιμη.

Συνεπώς, η επέκταση K/\mathbb{R} είναι Galois, γεγονός που μας επιτρέπει να χρησιμοποιήσουμε την πλήρη ισχύ της Αντιστοιχίας Galois και των Θεωρημάτων Sylow.

5.0.2 Ορισμός της Ομάδας Galois G

Ορίζουμε την ομάδα Galois της επέκτασης ως:

$$G = \text{Gal}(K/\mathbb{R})$$

Η τάξη της ομάδας G ισούται με τον βαθμό της επέκτασης, δηλαδή $|G| = [K : \mathbb{R}]$. Λόγω της πολλαπλασιαστικής ιδιότητας του βαθμού επεκτάσεων, έχουμε:

$$[K : \mathbb{R}] = [K : \mathbb{C}] \cdot [\mathbb{C} : \mathbb{R}] = 2 \cdot [K : \mathbb{C}]$$

Συνεπώς, η τάξη της G είναι οπωσδήποτε **άρτιος** αριθμός.

5.1 Βήμα 1: Η Ομάδα $\text{Gal}(K/\mathbb{R})$ είναι 2-Ομάδα

Στην προηγούμενη ενότητα ορίσαμε την ομάδα $G = \text{Gal}(K/\mathbb{R})$ και διαπιστώσαμε ότι η τάξη της είναι άρτιος αριθμός, καθώς $[K : \mathbb{R}] = [K : \mathbb{C}] \cdot [\mathbb{C} : \mathbb{R}] = 2[K : \mathbb{C}]$. Στόχος αυτού του βήματος είναι να αποδείξουμε ότι η τάξη της G είναι δύναμη του 2.

5.1.1 Ανάλυση της Τάξης της Ομάδας G

Έστω ότι η τάξη της ομάδας G γράφεται στη γενική μορφή:

$$|G| = 2^k \cdot m$$

όπου ο $k \geq 1$ είναι ο μέγιστος εκθέτης του 2 που διαιρεί την τάξη της ομάδας και ο m είναι ένας περιττός φυσικός αριθμός. Για να δείξουμε ότι η G είναι μια 2-ομάδα, αρκεί να αποδείξουμε ότι $m = 1$.

5.1.2 Εφαρμογή του Πρώτου Θεωρήματος Sylow

Ας υποθέσουμε, προς άτοπο, ότι ο περιττός παράγοντας είναι $m > 1$. Σύμφωνα με το **Πρώτο Θεώρημα Sylow** (βλ. Ενότητα 3.5), για κάθε πρώτο διαιρέτη p της τάξης μιας ομάδας, υπάρχει μια αντίστοιχη p -υποομάδα Sylow. Στην περίπτωσή μας, θεωρούμε την 2-υποομάδα Sylow, έστω H , η οποία έχει τάξη:

$$|H| = 2^k$$

Ο δείκτης της υποομάδας H στην ομάδα G είναι:

$$[G : H] = \frac{|G|}{|H|} = \frac{2^k \cdot m}{2^k} = m$$

5.1.3 Η Αντιστοιχία Galois και το Ενδιάμεσο Σώμα L

Από το Θεμελιώδες Θεώρημα της Θεωρίας Galois, στην υποομάδα H αντιστοιχεί ένα ενδιάμεσο σώμα σταθερών $L = K^H$, τέτοιο ώστε $\mathbb{R} \subseteq L \subseteq K$. Οι βαθμοί της επέκτασης ικανοποιούν τη σχέση:

$$[L : \mathbb{R}] = [G : H] = m$$

Εφόσον υποθέσαμε ότι $m > 1$, το L είναι μια γνήσια επέκταση του \mathbb{R} με **περιττό βαθμό** m .

Έστω ένα στοιχείο $a \in L$ το οποίο δεν ανήκει στο \mathbb{R} (τέτοιο στοιχείο υπάρχει αφού $[L : \mathbb{R}] = m > 1$). Θεωρούμε το ελάχιστο πολυώνυμο του a πάνω από το \mathbb{R} , έστω $p(x) \in \mathbb{R}[x]$.

- Ο βαθμός του $p(x)$, έστω d , πρέπει να διαιρεί τον βαθμό της επέκτασης $[L : \mathbb{R}] = m$.
- Εφόσον ο m είναι περιττός, έπεται ότι και ο d είναι **περιττός αριθμός** μεγαλύτερος της μονάδας ($d > 1$).
- Επιπλέον, το $p(x)$ είναι εξ ορισμού **ανάγωγο** πάνω από το \mathbb{R} .

Ωστόσο, σύμφωνα με την **Ιδιότητα 1** (βλ. Ενότητα 4.2), κάθε πολυώνυμο περιττού βαθμού στο $\mathbb{R}[x]$ έχει τουλάχιστον μία πραγματική ρίζα. Η ύπαρξη ρίζας συνεπάγεται ότι το πολυώνυμο έχει έναν γραμμικό παράγοντα της μορφής $(x - c)$, γεγονός που έρχεται σε άμεση αντίθεση με την αναγωγικότητα του $p(x)$ για βαθμό $d > 1$.

Οπότε, η μοναδική περίπτωση που δεν οδηγεί σε άτοπο είναι ο περιττός παράγοντας να είναι η μονάδα, δηλαδή $m = 1$. Συνεπώς:

$$|G| = 2^k$$

Αποδείχθηκε λοιπόν ότι η ομάδα Galois $G = Gal(K/\mathbb{R})$ είναι μια **2-ομάδα**.

5.2 Βήμα 2: Η Ομάδα $Gal(K/\mathbb{C})$ είναι Τετριμμένη

Μετά την απόδειξη ότι η ομάδα Galois $G = Gal(K/\mathbb{R})$ είναι μια **2-ομάδα τάξης** $|G| = 2^k$, το επόμενο βήμα είναι να εξετάσουμε τη σχέση του σώματος K με το σώμα των μιγαδικών αριθμών \mathbb{C} . Θα αποδείξουμε ότι **ο βαθμός της επέκτασης** $[K : \mathbb{C}]$ είναι **ίσος με τη μονάδα**, γεγονός που συνεπάγεται ότι $K = \mathbb{C}$.

5.2.1 Η Υποομάδα H' και η Τάξη της

Θεωρούμε την υποομάδα $H' = Gal(K/\mathbb{C})$. Από το Θεμελιώδες Θεώρημα της Θεωρίας Galois, γνωρίζουμε ότι η υποομάδα αυτή αντιστοιχεί στο σώμα \mathbb{C} μέσα στον πύργο επεκτάσεων $\mathbb{R} \subseteq \mathbb{C} \subseteq K$. Η τάξη της H' δίνεται από τη σχέση:

$$|H'| = [K : \mathbb{C}] = \frac{[K : \mathbb{R}]}{[\mathbb{C} : \mathbb{R}]} = \frac{2^k}{2} = 2^{k-1}$$

Εφόσον η H' είναι υποομάδα της 2-ομάδας G , είναι και η ίδια μια **2-ομάδα**.

5.2.2 Η Ύπαρξη Υποομάδας Δείκτη 2

Ας υποθέσουμε, προς άτοπο, ότι η επέκταση είναι γνήσια, δηλαδή $k - 1 \geq 1$ (που σημαίνει $|H'| > 1$). Μία από τις θεμελιώδεις ιδιότητες των p -ομάδων (βλ. Ενότητα 3.5.3) είναι ότι κάθε μη τριμμένη p -ομάδα διαθέτει μια σειρά υποομάδων τέτοια ώστε να υπάρχει πάντα μια υποομάδα N με δείκτη ίσο με τον πρώτο p . Στην περίπτωση μας ($p = 2$), η H' πρέπει να περιέχει μια υποομάδα N τέτοια ώστε:

$$[H' : N] = 2$$

Αυτή η υποομάδα N είναι αναγκαστικά κανονική στην H' , αν και για την απόδειξή μας αρκεί η ύπαρξή της και ο δείκτης της.

5.2.3 Η Αντιστοιχία Galois και το Σώμα L'

Εφαρμόζοντας ξανά την αντιστοιχία Galois για την υποομάδα N εντός της H' , προκύπτει η ύπαρξη ενός ενδιάμεσου σώματος $L' = K^N$, το οποίο βρίσκεται ανάμεσα στο \mathbb{C} και το K ($\mathbb{C} \subseteq L' \subseteq K$). Ο βαθμός της επέκτασης L'/\mathbb{C} ισούται με τον δείκτη της υποομάδας:

$$[L' : \mathbb{C}] = [H' : N] = 2$$

Μια επέκταση βαθμού 2 πάνω από το \mathbb{C} παράγεται από τη ρίζα ενός τετραγωνικού πολυωνύμου $f(x) = x^2 + bx + c$, όπου $b, c \in \mathbb{C}$. Σύμφωνα με τον κλασικό αλγεβρικό τύπο, οι ρίζες αυτού του πολυωνύμου εξαρτώνται από την ύπαρξη της τετραγωνικής ρίζας της διακρίνουσας $\Delta = b^2 - 4c$.

Ωστόσο, στην **Ιδιότητα 2** (βλ. Ενότητα 4.3), αποδείξαμε αναλυτικά ότι κάθε μιγαδικός αριθμός διαθέτει τετραγωνική ρίζα εντός του \mathbb{C} . Αυτό σημαίνει ότι:

- Το πολυώνυμο $f(x)$ έχει ήδη τις ρίζες του στο \mathbb{C} .
- Το πολυώνυμο $f(x)$ είναι αναγώγιμο (διασπάται σε γραμμικούς παράγοντες) πάνω από το \mathbb{C} .
- Δεν μπορεί να υπάρξει ανάγωγο πολυώνυμο βαθμού 2 πάνω από το \mathbb{C} .

Επομένως, η ύπαρξη του σώματος L' με $[L' : \mathbb{C}] = 2$ είναι αδύνατη.

Η αντίφαση που προέκυψε μας αναγκάζει να απορρίψουμε την υπόθεση $|H'| > 1$. Συνεπώς, πρέπει:

$$k - 1 = 0 \implies k = 1$$

Αυτό σημαίνει ότι η τάξη της ομάδας H' είναι $2^0 = 1$, άρα η H' είναι η τριμμένη ομάδα $\{id\}$. Κατά συνέπεια:

$$[K : \mathbb{C}] = 1$$

5.3 Συμπέρασμα της Απόδειξης

Με την ολοκλήρωση των δύο προηγούμενων βημάτων, ο κύκλος της απόδειξης κλείνει, οδηγώντας μας στο τελικό συμπέρασμα για τη φύση του σώματος των μιγαδικών αριθμών.

5.3.1 Η Ταύτιση $K = \mathbb{C}$

Στην ενότητα 5.3 αποδείξαμε ότι ο βαθμός της επέκτασης $[K : \mathbb{C}]$ είναι αναγκαστικά ίσος με τη μονάδα. Στη θεωρία σωμάτων, η συνθήκη $[K : \mathbb{C}] = 1$ συνεπάγεται άμεσα ότι:

$$K = \mathbb{C}$$

Αυτό σημαίνει ότι το σώμα ανάλυσης K οποιουδήποτε πολυωνύμου $f(x) \in \mathbb{C}[x]$ (ή του κατασκευασμένου $g(x) \in \mathbb{R}[x]$ που περιέχει τις ρίζες του f) δεν είναι μεγαλύτερο από το ίδιο το σώμα των μιγαδικών αριθμών. Συνεπώς, όλες οι ρίζες του πολυωνύμου $f(x)$, οι οποίες εξ ορισμού περιέχονται στο σώμα ανάλυσής του K , ανήκουν στην πραγματικότητα στο \mathbb{C} .

5.3.2 Το \mathbb{C} ως Αλγεβρικά Κλειστό Σώμα

Η απόδειξη ότι κάθε πεπερασμένη αλγεβρική επέκταση του \mathbb{C} συμπίπτει με το ίδιο το \mathbb{C} αποτελεί τον ορισμό του αλγεβρικά **κλειστού σώματος**. Καταλήγουμε λοιπόν στην επιβεβαίωση του Θεμελιώδους Θεωρήματος της Άλγεβρας:

Κάθε μη σταθερό πολυώνυμο $f(x) \in \mathbb{C}[x]$ έχει τουλάχιστον μία ρίζα στο \mathbb{C} .

Ως άμεση συνέπεια, κάθε τέτοιο πολυώνυμο βαθμού n μπορεί να γραφεί ως γινόμενο n πρωτοβάθμιων παραγόντων:

$$f(x) = a_n(x - a_1)(x - a_2) \dots (x - a_n)$$

όπου $a_1, a_2, \dots, a_n \in \mathbb{C}$ είναι οι ρίζες του.

6 Συμπεράσματα

6.1 Σύνοψη των Κύριων Αποτελεσμάτων

Στην παρούσα εργασία εξετάστηκε μία από τις πιο κομψές και βαθιές αποδείξεις του Θεμελιώδους Θεωρήματος της Άλγεβρας, η οποία συνδυάζει την Θεωρία *Galois* με τις θεμελιώδεις αναλυτικές ιδιότητες των πραγματικών αριθμών. Η προσέγγιση αυτή έχει τις ρίζες της στις πρώιμες προσπάθειες των Euler και Lagrange κατά τον 18ο αιώνα, οι οποίοι επιχειρήσαν να αποδείξουν το θεώρημα χρησιμοποιώντας τις συμμετρίες των ριζών. Ωστόσο, η απόδειξη ολοκληρώθηκε και διατυπώθηκε τον 19ο αιώνα, βασισμένη στο έργο του Έvariste Galois, ενώ η συγκεκριμένη μορφή της που χρησιμοποιεί την αντιστοιχία σωμάτων και ομάδων διδάσκεται σήμερα ως μέρος της θεωρίας του Emil Artin.

6.1.1 Επαναδιατύπωση του Θ.Θ.Α.

Το Θεμελιώδες Θεώρημα της Άλγεβρας (Θ.Θ.Α.) επιβεβαιώνει ότι το σώμα των μιγαδικών αριθμών \mathbb{C} είναι **αλγεβρικά κλειστό**. Όπως αναλύθηκε, αυτό σημαίνει ότι κάθε μη σταθερό πολυώνυμο $f(z) \in \mathbb{C}[z]$ βαθμού $n \geq 1$ διαθέτει τουλάχιστον μία ρίζα στο \mathbb{C} . Κατά συνέπεια, κάθε τέτοιο πολυώνυμο διασπάται πλήρως σε γινόμενο n γραμμικών παραγόντων της μορφής $(z - a_i)$. Το αποτέλεσμα αυτό δεν αποτελεί απλώς μια διαπίστωση για τις πολυωνυμικές εξισώσεις, αλλά ορίζει το \mathbb{C} ως το τελικό στάδιο της αλγεβρικής εξέλιξης των αριθμητικών συστημάτων, όπου κάθε αλγεβρική οντότητα βρίσκει τη λύση της.

6.1.2 Ο Ρόλος των Βασικών Θεωρημάτων στην Απόδειξη

Η ισχύς της απόδειξης που αναπτύχθηκε στα προηγούμενα κεφάλαια βασίστηκε στη συνεργασία τριών διαφορετικών μαθηματικών πυλώνων:

1. **Θεμελιώδες Θεώρημα της Θεωρίας Galois (Θ.Θ.Θ.Γ):** Λειτουργήσε ως ο συνδετικός κρίκος που επέτρεψε τη μετάφραση ενός προβλήματος σωμάτων σε πρόβλημα θεωρίας ομάδων. Μέσω της αντιστοιχίας *Galois*, η αναζήτηση ενδιάμεσων σωμάτων αντικαταστάθηκε από τη μελέτη των υποομάδων της ομάδας $\text{Gal}(K/\mathbb{R})$. Η ικανότητα να ερμηνεύουμε τη δομή μιας επέκτασης σωμάτων μέσα από τη δομή μιας ομάδας ήταν η απαραίτητη προϋπόθεση για τον έλεγχο των δυνατών βαθμών επέκτασης.
2. **Θεωρήματα Sylow και p -ομάδες:** Τα θεωρήματα Sylow παρείχαν τα εργαλεία για την αποδόμηση της ομάδας *Galois*. Το 1ο Θεώρημα Sylow μας επέτρεψε να απομονώσουμε μια 2-υποομάδα και να δείξουμε ότι η ομάδα *Galois* μιας οποιασδήποτε επέκτασης του \mathbb{R} πρέπει να είναι μια 2-ομάδα. Επιπλέον, η ιδιότητα των p -ομάδων να διαθέτουν πάντα υποομάδες δείκτη p (στην περίπτωσή μας δείκτη 2) ήταν αυτή που οδήγησε στην τελική αντίφαση, αποδεικνύοντας ότι δεν υπάρχει χώρος για περαιτέρω επεκτάσεις πάνω από το \mathbb{C} .
3. **Αναλυτικές Ιδιότητες του \mathbb{R} και του \mathbb{C} :** Παρά τον αλγεβρικό προσανατολισμό της αποδεικτικής διαδικασίας, οι αναλυτικές ιδιότητες των πραγματικών αριθμών αποτέλεσαν το αναγκαίο υπόβαθρο για την οικοδόμηση του τελικού επιχειρήματος.
 - Η **Ιδιότητα 1** (πολυώνυμα περιττού βαθμού στο \mathbb{R} έχουν ρίζα), βασισμένη στο Θεώρημα Ενδιάμεσης Τιμής, απέκλεισε την ύπαρξη επεκτάσεων περιττού βαθμού.

- Η **Ιδιότητα 2** (ύπαρξη τετραγωνικών ριζών στο \mathbb{C}) απέκλεισε την ύπαρξη επεκτάσεων βαθμού 2.

6.2 Κριτική Σύγκριση

Η απόδειξη του Θεμελιώδους Θεωρήματος της Άλγεβρας (Θ.Θ.Α.) μπορεί να επιτευχθεί μέσω ποικίλων μεθόδων, από τη Μιγαδική Ανάλυση (Θεώρημα *Liouville*) έως την Τοπολογία (Αριθμός Στροφής). Ωστόσο, η αλγεβρική προσέγγιση μέσω της Θεωρίας *Galois* παρουσιάζει διακριτά πλεονεκτήματα και προσφέρει μια μοναδική οπτική στη φύση του προβλήματος.

Ενώ οι περισσότερες αποδείξεις βασίζονται σε προχωρημένες έννοιες της Μιγαδικής Ανάλυσης (όπως οι ολόμορφες συναρτήσεις, τα επικαμπύλια ολοκληρώματα ή η αρχή του μεγίστου), η απόδειξη μέσω *Galois* απαιτεί μόνο δύο βασικά αποτελέσματα της Ανάλυσης: ότι κάθε πολυώνυμο περιττού βαθμού στο $\mathbb{R}[x]$ έχει ρίζα και ότι κάθε μιγαδικός αριθμός έχει τετραγωνική ρίζα. Αυτό καθιστά την απόδειξη πιο διαφανή ως προς το πού ακριβώς εισέρχεται η ιδιότητα της πληρότητας των πραγματικών αριθμών.

Η συγκεκριμένη μέθοδος αντιμετωπίζει το \mathbb{C} ως ένα σώμα, όπου μέσω της χρήσης των p -ομάδων Sylow, αποκαλύπτεται ότι η αιτία που το \mathbb{C} είναι αλγεβρικά κλειστό κρύβεται στη δομή των πεπερασμένων ομάδων.

Η μέθοδος *Galois* δείχνει ότι αν ένα σώμα F έχει τις ίδιες αναλυτικές ιδιότητες με το \mathbb{R} , τότε η επέκταση $F(i)$ θα είναι πάντα αλγεβρικά κλειστή. Αυτή η γενίκευση είναι αδύνατη με μεθόδους της Μιγαδικής Ανάλυσης, οι οποίες είναι αυστηρά περιορισμένες στο σώμα \mathbb{C} .

Καταλήγουμε, λοιπόν, στο συμπέρασμα ότι η απόδειξη μέσω της Θεωρίας *Galois* είναι μία διαδικασία που συνδέει οργανικά την Άλγεβρα με την Ανάλυση. Αναδεικνύει ότι το Θ.Θ.Α. είναι στην πραγματικότητα ένα θεώρημα για την ακαμπτία των επεκτάσεων του \mathbb{R} . Η επιλογή της στην παρούσα εργασία δικαιώνεται από το γεγονός ότι προσφέρει τη βαθύτερη δυνατή κατανόηση του γιατί το μιγαδικό σώμα αποτελεί το φυσικό όριο της αλγεβρικής διαδικασίας.

References

- [1] Lars Valerian Ahlfors. *Complex Analysis: An Introduction to the Theory of Analytic Functions of One Complex Variable*. McGraw-Hill, 3rd edition, 1979.
- [2] Michael Artin. *Algebra*. Pearson Prentice Hall, 2nd edition, 2011.
- [3] Gerhard Rosenberger Benjamin Fine. *The Fundamental Theoren of Algebra*. Springer, 1997.
- [4] John B. Conway. *Functions of One Complex Variable I*. Springer, 2nd edition, 1978.
- [5] David A. Cox. *Galois Theory*. John Wiley & Sons, 2nd edition, 2012.
- [6] David S. Dummit and Richard M. Foote. *Abstract Algebra*. John Wiley & Sons, 3rd edition, 2004.
- [7] Harold M. Edwards. *Galois Theory*, volume 101 of *Graduate Texts in Mathematics*. Springer-Verlag, 1984.
- [8] Jhon B. Fraleigh. *An Introduction in Algebra*. Graduate Texts in Mathematics. Crete University Press (CUP), 11th edition, 2019.
- [9] John M. Howie. *Fields and Galois Theory*. Graduate Texts in Mathematics. Springer, 2006.
- [10] Serge Lang. *Algebra*, volume 211 of *Graduate Texts in Mathematics*. Springer, 3rd edition, 2002.
- [11] Joseph Rotman. *Galois Theory*. Graduate Texts in Mathematics. Leader Books, 1st edition, 2000.
- [12] Ian Stewart. *Galois Theory*. CRCPress Taylor Francis Group, 4th edition, 2015.
- [13] Theophilos Tsantilas. *Grothendieck's Galois Theory*. MSc Thesis, Dept. of Mathematics. University of Athens.