ΕΘΝΙΚΟ ΚΑΙ ΚΑΠΟΔΙΣΤΡΙΑΚΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΑΘΗΝΩΝ

ΤΜΗΜΑ ΜΑΘΗΜΑΤΙΚΩΝ
ΤΜΗΜΑ ΜΕΘΟΔΟΛΟΓΙΑΣ ΙΣΤΟΡΙΑΣ ΚΑΙ ΘΕΩΡΙΑΣ ΤΗΣ ΕΠΙΣΤΗΜΗΣ
ΤΜΗΜΑ ΦΙΛΟΣΟΦΙΑΣ - ΠΑΙΔΑΓΩΓΙΚΩΝ - ΨΥΧΟΛΟΓΙΑΣ

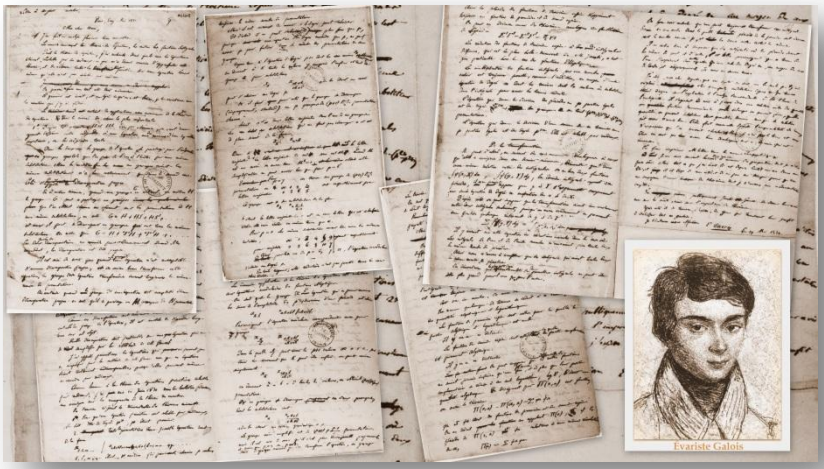
ΠΑΝΕΠΙΣΤΗΜΙΟ ΚΥΠΡΟΥ

ΤΜΗΜΑ ΜΑΘΗΜΑΤΙΚΩΝ ΚΑΙ ΣΤΑΤΙΣΤΙΚΗΣ
ΤΜΗΜΑ ΕΠΙΣΤΗΜΩΝ ΑΓΩΓΗΣ

ΔΙΑΠΑΝΕΠΙΣΤΗΜΙΑΚΟ - ΔΙΑΤΜΗΜΑΤΙΚΟ ΠΡΟΓΡΑΜΜΑ ΜΕΤΑΠΤΥΧΙΑΚΩΝ ΣΠΟΥΔΩΝ
"ΔΙΔΑΚΤΙΚΗ ΚΑΙ ΜΕΘΟΔΟΛΟΓΙΑ ΤΩΝ ΜΑΘΗΜΑΤΙΚΩΝ"

ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

Μια μελέτη της ιστορικής εξέλιξης της Θεωρίας Galois



Παναγιώτης Μαραγκός
Δ200902

Επιβλέπων Καθηγητής:
Ευάγγελος Ράπτης

ΑΘΗΝΑ 2012

Η παρούσα Διπλωματική Εργασία
εκπονήθηκε στα πλαίσια των σπουδών
για την απόκτηση του

Μεταπτυχιακού Διπλώματος Ειδίκευσης

που απονέμει το

Διαπανεπιστημιακό – Διατμηματικό Πρόγραμμα Μεταπτυχιακών Σπουδών

«Διδακτική και Μεθοδολογία των Μαθηματικών»

Εγκρίθηκε την …… από Εξεταστική Επιτροπή
αποτελούμενη από τους :

	Ονοματεπώνυμο	Βαθμίδα	Υπογραφή
1/	Ράπτης Ευάγγελος *(Επιβλέπων)*	Καθηγητής	……
2/	Βάρσος Δημήτριος	Καθηγητής	……
3/	Λάππας Διονύσιος	Αναπληρωτής Καθηγητής	……

Στις γυναίκες της ζωής μου:
τη μητέρα μου Φανή
τη σύζυγό μου Αννέτα
την κόρη μου Ελπίδα.

Περιεχόμενα

Περίληψη **8**

Εισαγωγή **13**

I Ιστορική εξέλιξη της Θεωρίας Galois **15**

1 Πολυώνυμα **17**
1.1 Πολυωνυμικές Εξισώσεις 17
1.1.1 Εξισώσεις 2ου βαθμού 17
Βαβυλώνιοι 17
Έλληνες 19
Άραβες 21
1.1.2 Εξισώσεις 3ου βαθμού 23
Έλληνες 23
Άραβες 24
Ιταλία 26
Casus irreducibilis 29
1.1.3 Εξισώσεις 4ου βαθμού 31
1.2 Συμμετρικά πολυώνυμα 32
Viète 33
Girard 34
Newton 37
1.3 Κυκλοτομικά πολυώνυμα 38
Euler 39
Vandermonde 39
Gauss 41
1.4 Θεμελιώδες Θεώρημα της Άλγεβρας 43

1.4.1 Ιστορική αναφορά 43
1.4.2 Απόδειξη 47

2 Ομάδες **53**
2.1 Ομάδα μεταθέσεων 53
2.1.1 Lagrange 53
2.1.2 Ruffini 64
2.1.3 Abel 67
2.1.4 Cauchy 69
2.2 Ομάδα Galois 71
2.2.1 Galois 71
Τι είχε μελετήσει ο Galois 71
Τα γραπτά του Galois 73
Premier Mémoire 75
Second Mémoire 81
2.3 Επιλύσιμες ομάδες 82
2.3.1 Betti 83
2.3.2 Serret 85
2.3.3 Jordan 90

3 Σώματα **95**
3.1 Επεκτάσεις σωμάτων 95
3.1.1 Kronecker 97
3.1.2 Dedekind 99
3.2 Θεμελιώδες Θεώρημα της Θεωρίας Galois 105
3.2.1 Artin 106

II Θεωρία Galois **111**

4 Θεωρία Galois **113**
4.1 Στοιχειώδης προσέγγιση 113
4.2 Σύγχρονη προσέγγιση 117
4.3 Παραδείγματα 120

Βιβλιογραφία **127**

Περίληψη

Η Θεωρία Galois θεωρείται από πολλούς ως αποκλειστική δημιουργία ενός και μόνο χαρισματικού ανθρώπου. Στην αντίληψη αυτή συμβάλλει τόσο η ονομασία που έχει δοθεί στη Θεωρία αυτή, όσο και το γεγονός ότι σχεδόν σε όλα τα βιβλία και εγχειρίδια που την παρουσιάζουν, περιέχουν και μια βιογραφία του *(θεωρούμενου ως)* ιδρυτή της, κάτι που δεν συναντούμε συνήθως σε άλλα βιβλία Μαθηματικών θεωριών.

Στην παρούσα εργασία παρουσιάζεται η πορεία και η εξέλιξη των εννοιών που βρίσκονται στη Θεωρία Galois, ποιοί άνθρωποι συνέβαλαν και πως απέδωσαν στη γλώσσα των Μαθηματικών τις καινοτόμες ιδέες τους. Εξετάζεται η θεωρία των πολυωνυμικών εξισώσεων, η οποία ήταν το βασικό πεδίο πειραματισμού για τη διαμόρφωση της Θεωρίας Galois, από τους Αρχαίους πολιτισμούς, μέχρι τον 19ο αιώνα, όπου και εμφανίστηκαν οι πρωτοπόρες ιδέες του Galois. Βλέπουμε εν συνεχεία την προσπάθεια των επόμενων γενεών Μαθηματικών να κατανοήσουν αυτές τις νέες αφηρημένες γι αυτούς έννοιες και την τροποποίησή τους, στη μορφή που υπάρχουν σήμερα.

Τέλος παρουσιάζονται, εν συντομία, οι δύο μορφές της Θεωρίας Galois. Η στοιχειώδης προσέγγιση όπως εμφανίστηκε αρχικά από τον Galois και τους άμεσους συνεχιστές του και η σύγχρονη προσέγγιση όπως διαμορφώθηκε από τον Artin μέχρι τις μέρες μας.

Λέξεις κλειδιά

Θεωρία Galois, Ιστορία των Μαθηματικών, Άλγεβρα, Ομάδες, Σώματα.

Abstract

Galois Theory is considered by many to be the sole creation of a single charismatic man. This view is reinforced both by the name given to this theory, and by the fact that almost all relative books and manuals on the theory, contain a biography of the textit (viewed as) founder, something not found usually in other books of Mathematical theories.

This paper presents the progress and evolution of the concepts found in Galois Theory, the people who have contributed and how they manipulated in the language of mathematics their innovative ideas. We examine the theory of polynomial equations, which was the main testing ground for the development of Galois Theory, from Ancient civilizations to the 19th century, where the leading ideas of Galois appeared. We then present the attempts of the next generations of Mathematics to understand these new abstract concepts and to modify them, in today format .

Finally we present briefly the two forms of the Galois Theory. The elementary approach as first appeared by Galois and his immediate successors and the modern approach as formulated by Artin until today.

Keywords

Galois Theory, History of Mathematics, Algebra, Groups, Fields.

Εισαγωγή

> "Στις περισσότερες επιστήμες, η κάθε γενιά γκρεμίζει όσα έχτισε η προηγούμενη. Μόνο στα Μαθηματικά, η κάθε γενιά χτίζει έναν καινούργιο όροφο στο παλιό κτίριο."
>
> Hermann Hankel
> (February 14, 1839 - August 29, 1873)
> *Γερμανός Μαθηματικός*

Η παρούσα εργασία αποτελεί την ολοκλήρωση μιας αναζήτησης η οποία ξεκίνησε πριν από περίπου μια εικοσαετία. Όντας μαθητής της 1ης δέσμης, της τρίτης τάξης του Λυκείου, έπιασα στα χέρια μου το ένα από τα τρία βιβλία των μαθηματικών τα οποία θα διδασκόμουν εκείνη τη χρονιά. Ήταν το βιβλίο με τίτλο "Άλγεβρα"[1]. Ξεφυλλίζοντας το διάβασα στον πρόλογο του 2ου κεφαλαίου: *"Η Άλγεβρα χαρακτηρίζεται από τη μελέτη συνόλων στα οποία έχουν καθοριστεί πράξεις."* Στη διάρκεια της σχολικής χρονιάς έμαθα τη σημασία των εννοιών: *ομάδα, δακτύλιος, σώμα* με κύρια παραδείγματά τους την προσθετική ομάδα των ακεραίων, το δακτύλιο των ακεραίων, το σώμα των ρητών. Τι σχέση είχαν αυτά όμως με την Άλγεβρα; Αυτά ήταν Αριθμητική, στην καλύτερη περίπτωση θα μπορούσαν να βρίσκονται στο βιβλίο της Ανάλυσης όπου αναφερόταν το σώμα των Πραγματικών αριθμών πριν από την εισαγωγή στις Συναρτήσεις. Μέχρι τότε, όλα τα προηγούμενα σχολικά μου χρόνια, ήξερα ότι η Άλγεβρα ασχολείται κυρίως με την

[1]Εκδόσεις ΟΕΔΒ-1989, με συγγραφείς τους: Βαρουχάκη, Αδαμόπουλο, Γιαννίκο, Μπέτση, Νοταρά, Σολδάτο, Φωτόπουλο.

επίλυση εξισώσεων, ανισώσεων ή συστημάτων. Δεν μπορεί όλα τα προηγούμενα βιβλία να έκαναν τέτοια παρανόηση. Από την άλλη όμως ούτε το βιβλίο της Δέσμης θα έκανε ένα τόσο μεγάλο λάθος. Όμως οι δύο αυτές απόψεις για το τι είναι Άλγεβρα φαίνονταν ασυμβίβαστες μεταξύ τους. Πώς συνδέονταν αυτές οι έννοιες;

Απάντηση σ' αυτό το ερώτημα δεν κατάφερα να πάρω εκείνη τη χρονιά. Όμως ούτε και τα επόμενα χρόνια, ως φοιτητής των Μαθηματικών. Χρόνια μετά, όταν έπεσε στην αντίληψή μου η κυκλοφορία κάποιων "εκλαϊκευτικών" βιβλίων σχετικών με την Ιστορία των Μαθηματικών, άρχισα να αντιλαμβάνομαι πως και οι δύο απόψεις για το τι είναι Άλγεβρα είναι σωστές. Απλώς η μία είναι η εξέλιξη της άλλης και αυτό που συνέβη είναι ότι δεν γνώριζα πότε, πως και γιατί η επίλυση των πολυωνυμικών εξισώσεων είχε κατά κάποιο τρόπο μεταλλαχθεί στη μελέτη συνόλων εφοδιασμένων με ορισμένες πράξεις. Στην πορεία της αναζήτησης και κυρίως με την πληθώρα των πληροφοριών που έβρισκα στο ολοένα αναπτυσσόμενο διαδίκτυο, μου έγινε πλήρως αντιληπτό ότι αυτή η "μεταμόρφωση" της Άλγεβρας περνάει υποχρεωτικά μέσα από την εξέλιξη της Θεωρίας Galois. Η ευκαιρία να μελετήσω λοιπόν πιο διεξοδικά, τόσο από πρωτογενείς[2] όσο και από δευτερογενείς[3] πηγές, την Ιστορία της Θεωρίας Galois, ήρθε με την εκπόνηση της διπλωματικής αυτής εργασίας.

Κατά τη διάρκεια της διεξοδικής μελέτης της βιβλιογραφίας, έγινε από μέρους μου μια διαπίστωση, της οποίας βέβαια δεν διεκδικώ την προτεραιότητα: καμία θεωρία στα Μαθηματικά δεν προέρχεται από παρθενογένεση, αλλά οι ήδη υπάρχουσες ιδέες αφού πρώτα κατανοηθούν, στη συνέχεια επεξεργάζονται και εξελίσσονται και πολλές φορές καταλήγουν σε κάτι νέο που δεν θυμίζει σε τίποτα το παλαιό από το οποίο προήλθε. Αυτή τη διαπίστωση προσπαθεί κατά κύριο λόγο να τεκμηριώσει η εργασία αυτή. Ας εξηγήσω τον προηγούμενο ισχυρισμό. Η Θεωρία Galois θεωρείται από πολλούς ως το πιο τρανταχτό παράδειγμα μιας Μαθηματικής θεωρίας που είναι δημιούργημα ενός και μόνο χαρισματικού ανθρώπου. Η άποψη αυτή ενισχύεται από το γεγονός ότι είναι η μόνη θεωρία των Μαθηματικών που έχει το όνομα αυτού που την βρήκε-ανέδειξε, δηλαδή Θεωρία Galois. Για καμία άλλη θεωρία δεν συμβαίνει αυτό, ούτε η Ανάλυση λέγεται Θεωρία Newton-Leibniz, ούτε η θεωρία των Πιθανοτήτων λέγεται Θεωρία Fermat-Pascal, ούτε η Αναλυτική Γεωμετρία λέγεται

[2]πρωτότυπα έργα
[3]άλλες μελέτες

Θεωρία Descartes. Επίσης στην προαναφερόμενη αντίληψη συμβάλλει και το γεγονός ότι σχεδόν σε όλα τα βιβλία και εγχειρίδια που την παρουσιάζουν, περιέχεται και μια βιογραφία του *(θεωρούμενου ως)* ιδρυτή της, κάτι που δεν συναντούμε συνήθως σε άλλα βιβλία Μαθηματικών θεωριών. Όμως όπως θα φανεί στην πορεία της εργασίας, ο Galois πήρε πολλές ιδέες αλλά και το έναυσμα από προγενέστερους Μαθηματικούς των οποίων το έργο τον είχε επηρεάσει σε μεγάλο βαθμό. Θα γίνει επίσης αντιληπτό ότι και η μορφή που βλέπουμε τώρα την Θεωρία Galois είναι εξέλιξη άλλων μεταγενέστερων Μαθηματικών. Αυτό σημαίνει ότι πρέπει να μελετάται η ιστορία για να μην ενισχύονται μύθοι.

Η συμβολή της εργασίας στη διδακτική (αν επιθυμούσαμε να διατυπώσουμε μια διδακτική πρόταση) είναι ακριβώς αυτή η παρουσίαση της ιστορικής εξέλιξης μιας Μαθηματικής ιδέας, αφού δείχνει ότι η ενσωμάτωση της Ιστορίας των Μαθηματικών ενισχύει όχι μόνο την κατανόηση μιας θεωρίας αλλά δικαιολογεί και την ίδια την ύπαρξή της. Ενδεικτικά για παράδειγμα, ο ορισμός της ομάδας μπορεί να γίνει με τρεις ισοδύναμους τρόπους (α)τις μεταθέσεις, (β)τις συμμετρίες και (γ)τα αξιώματα. Αν και σήμερα, σε όλα τα εγχειρίδια, επικρατεί ο (γ) τρόπος, αφού θεωρείται ο πιο ικανοποιητικός ως προς την αυστηρότητα που πρέπει να έχουν τα Μαθηματικά, διδακτικά φαίνεται να είναι πιο προσιτοί οι άλλοι δύο που, ίσως όχι τυχαία, προηγούνται και ιστορικά. Για να γίνουμε πιο πειστικοί ως προς την αναγκαιότητα της χρήσης της Ιστορικής εξέλιξης της Θεωρίας στη διδασκαλία της θα αναφέρουμε την εξής παρομοίωση. Θα μπορούσαμε να παρομοιάσουμε τη Θεωρία Galois ως ένα δέντρο με ρίζες τα έργα των Lagrange, Vandermonde, Gauss κ.λ.π. με κορμό τις ιδέες του Galois και με κλαδιά και φύλλα την εξέλιξη της από τους Jordan, Dedekind, Kronecker, Artin κ.α. Μπορούμε φυσικά να τρώμε μόνο τους καρπούς του δέντρου, δηλαδή τα αποτελέσματα και τις εφαρμογές της θεωρίας, έχοντας επαφή μόνο με τα κλαδιά και τα φύλλα, αν θέλουμε όμως να έχουμε μια βαθιά κατανόηση, τότε πρέπει να κοιτάμε τον κορμό και ίσως και τις ρίζες.

Στην παρούσα εργασία παρουσιάζεται η πορεία και η εξέλιξη των εννοιών που βρίσκονται στη Θεωρία Galois, ποιοί άνθρωποι συνέβαλαν και πως απέδωσαν στη γλώσσα των Μαθηματικών τις καινοτόμες ιδέες τους. Στο πρώτο μέρος της εργασίας, που είναι και το κύριο κομμάτι της, γίνεται μια μελέτη της διαμόρφωσης και εξέλιξης της Θεωρίας Galois, δια μέσου ολόκληρης της γνωστής Ιστορίας των Μαθηματικών. Δηλαδή από την εποχή των Βαβυλωνίων μέχρι τη σύγχρονη εποχή. Αποτελείται από τρία κεφάλαια τα οποία

παρότι ακολουθούν μια χρονολογική εξέλιξη, διαπραγματεύονται αντίστοιχα τα βασικά θέματα της Θεωρίας: τα πολυώνυμα, τις ομάδες και τα σώματα.

Έτσι το πρώτο κεφάλαιο εξετάζει την θεωρία των πολυωνύμων, η οποία αποτελεί και το βασικό πεδίο πειραματισμού και εφαρμογής της Θεωρίας Galois. Παρουσιάζεται η αντιμετώπιση των δευτεροβάθμιων εξισώσεων από τους Βαβυλώνιους, τους Έλληνες μέχρι και τους Άραβες. Ακολουθεί η τριτοβάθμια και τεταρτοβάθμια εξίσωση και οι προσπάθειες των Ελλήνων και των Αράβων, μέχρι την τελική λύση από τους Ιταλούς Μαθηματικούς του Μεσαίωνα. Επιπλέον γίνεται ιδιαίτερη αναφορά στην ανάγωγη περίπτωση *(casus irreducibilis)* της τριτοβάθμιας, η οποία οδήγησε στην αποδοχή των φανταστικών αριθμών. Επειδή η επόμενη πρόκληση ήταν η επίλυση των πολυωνυμικών εξισώσεων ανώτερων βαθμών, οι Μαθηματικοί στράφηκαν στη μελέτη γενικότερων μορφών όπως τα συμμετρικά πολυώνυμα. Παρουσιάζεται η αναγνώρισή τους από τον Viète και η περαιτέρω μελέτη τους από τους Girard και Newton. Κατόπιν βλέπουμε το πρώτο είδος πολυωνύμων για το οποίο δόθηκε η γενική λύση ανεξαρτήτως βαθμού, που είναι τα κυκλοτομικά πολυώνυμα. Στο τέλος του κεφαλαίου αναφέρεται το "Θεμελιώδες Θεώρημα της Άλγεβρας" μαζί με μια απόδειξή του.

Το δεύτερο κεφάλαιο έχει θέμα του τις ομάδες. Ξεκινάει με την μνημειώδη εργασία του Lagrange για τις πολυωνυμικές εξισώσεις, η οποία εκτός του ότι περιείχε την αρχική ιδέα για τη σχέση μεταξύ των μεταθέσεων των ριζών και της επιλυσιμότητας της εξίσωσης, έδωσε την ώθηση για την απόδειξη της μη-επιλυσιμότητας της πεμπτοβάθμιας και ενέπνευσε τόσο τους βασικούς ερευνητές όπως τους Abel, Ruffini και Galois όσο και το έργο τους. Στη συνέχεια γίνεται μια πιο λεπτομερής μελέτη για την κληρονομιά που άφησε ο Galois στις επόμενες γενιές με το πρωτοπόρο έργο του, μέσα από τα λιγοστά αλλά τόσο σημαντικά γραπτά του. Το κεφάλαιο συμπληρώνεται από τους βασικούς συνεχιστές του έργου του Galois, όπως οι Betti, Serret και Jordan.

Το τρίτο κεφάλαιο ξεκινά με τη συνεισφορά των Γερμανών Μαθηματικών Kronecker και Dedekind, τόσο στη Θεωρία Galois, όσο και γενικότερα στην Άλγεβρα, μέσω της ειδικότερης έρευνάς τους πάνω στα Σώματα. Εν συνεχεία παρουσιάζεται η νέα οπτική ενός Γάλλου, του Emil Artin, ο οποίος έδωσε στη Θεωρία Galois τη σημερινή της μορφή.

Στο δεύτερο μέρος της εργασίας παρουσιάζονται, εν συντομία, οι δύο μορφές της Θεωρίας Galois. Η στοιχειώδης προσέγγιση όπως

εμφανίστηκε αρχικά από τον Galois και τους άμεσους συνεχιστές του και η σύγχρονη προσέγγιση όπως διαμορφώθηκε από τον Artin μέχρι τις μέρες μας. Η εργασία καταλήγει με την απόδειξη της μη επιλυσιμότητας της γενικής πεμπτοβάθμιας πολυωνυμικής εξίσωσης, με χρήση των εργαλείων που παρέχει η Θεωρία Galois.

Στο σημείο αυτό είναι επιβεβλημένο, από ηθική άποψη, να ευχαριστήσω τον επιβλέποντα Καθηγητή κ.Ευάγγελο Ράπτη. Αφ' ενός για την καθοδήγηση και ενθάρρυνση που μου πρόσφερε, με ακαδημαϊκό αλλά ταυτόχρονα και ανθρώπινο τρόπο, καθ' όλη τη διάρκεια της εκπόνησης της εργασίας αυτής. Αφ' ετέρου γιατί είναι το παράδειγμα ενός Δασκάλου[4] ο οποίος μεταχειρίζεται κάθε μέσο, είτε τεχνολογικό είτε επικοινωνιακό, ώστε να μεταδώσει στους μαθητές του τη χαρά της γνώσης. Είναι κάτι που πλέον θα έχω ως οδηγό στις διδασκαλίες μου. Ευχαριστώ τον Καθηγητή κ. Δημήτριο Βάρσο για την τιμή που μου έκανε να συμμετέχει στην τριμελή επιτροπή. Επίσης ευχαριστώ τον Αναπληρωτή Καθηγητή κ Διονύσιο Λάππα, εκτός από την συμμετοχή του στην τριμελή επιτροπή, κυρίως γιατί με έμαθε πως πρέπει να αντιμετωπίζεται η Ιστορία των Μαθηματικών ώστε να αποφεύγεται η απλή ιστοριογραφική προσέγγιση και τι είναι η εγκάρσια έρευνα μιας Μαθηματικής έννοιας, τα οποία πιστεύω αξιοποίησα, όσο μου επέτρεψαν οι δυνατότητές μου, για να φέρω σε πέρας την παρούσα μελέτη. Τέλος ευχαριστώ όλους ανεξαιρέτως τους διδάσκοντες του Προγράμματος γιατί δια μέσου τους, έγινα πλουσιότερος σε εμπειρίες Μαθηματικές, διδακτικές και ανθρώπινες.

[4]το πρώτο γράμμα "Δ" της λέξης, **δεν** είναι κεφαλαίο εκ παραδρομής.

Μέρος Ι

Ιστορική εξέλιξη της Θεωρίας Galois

1

Πολυώνυμα

1.1 Πολυωνυμικές Εξισώσεις

Στην ενότητα αυτή θα δούμε με ποιούς τρόπους αντιμετώπισαν οι Μαθηματικοί, μέχρι την εποχή του Galois, τις πολυωνυμικές εξισώσεις 2^{ου}, 3^{ου} και 4^{ου} βαθμού. Ο λόγος που δεν θα ασχοληθούμε με τη γενική εξίσωση 1^{ου} βαθμού είναι ότι επιλύεται με μια απλή διαίρεση κι έτσι μετά βίας θα μπορούσε να συμπεριληφθεί ως μια ενδιαφέρουσα περίπτωση για τη Θεωρία Galois.

1.1.1 Εξισώσεις 2^{ου} βαθμού

Η γενική μορφή της εξίσωσης 2^{ου} βαθμού είναι:

$$\alpha x^2 + \beta x + \gamma = 0 \ , \alpha \neq 0$$

και σύμφωνα με τη σχολική άλγεβρα οι λύσεις της δίνονται από τον τύπο

$$x_{1,2} = \frac{-\beta \pm \sqrt{\beta^2 - 4\alpha\gamma}}{4\alpha} \tag{1.1}$$

Βαβυλώνιοι

Η πρώτη γνωστή μέθοδος επίλυσης μιας δευτεροβάθμιας εξίσωσης, σύμφωνα με τον Neugebauer (βλέπε [38]) είναι καταγεγραμμένη σε μια Βαβυλωνιακή πήλινη πινακίδα που χρονολογείται περίπου ανάμεσα στο 1.800 και το 1.600 π.Χ. Οι Βαβυλώνιοι δεν χρησιμοποιούσαν έναν αλγεβρικό τύπο για την εύρεση των λυσεων της εξίσωσης, αλλά μια σειρά βημάτων που τους

οδηγούσε στη λύση της. Στις πινακίδες που έχουν διασωθεί μέχρι σήμερα δεν καταγράφεται ο τρόπος με τον οποίο έφτασαν σ'αυτά τα βήματα. Έτσι δεν γνωρίζουμε αν η τεχνική αυτή είχε ανακαλυφθεί από κάποιον "σοφό" της εποχής και οι υπόλοιποι την ακολουθούσαν χωρίς να κατανοούν τι κάνουν ή αν τα κείμενα που έχουμε στη διάθεσή μας είναι απλά ασκήσεις για εξάσκηση μαθητών που γνώριζαν από προφορικές διδασκαλίες τις αιτίες για τις οποίες λειτουργεί η τεχνική που χρησιμοποιούσαν. Ένα παράδειγμα που δίνεται στο βιβλίο του Van der Waerden [38] δείχνει τον τρόπο με τον οποίο οι Βαβυλώνιοι αντιμετώπιζαν τέτοιου είδους προβλήματα.

Πρόβλημα 1. *Αφαιρώ από το εμβαδόν την πλευρά του τετραγώνου και βρίσκω 14.30 . Ποιά είναι η πλευρά;*
Λύση: *Πάρε 1, τον συντελεστή (του x). Διαίρεσε το 1 σε δύο μέρη, θα βρεις 0,30. Πολλαπλασίασε το 0,30 με το 0,30 και θα πάρεις 0,15, πρόσθεσέ το στο 14.30 και η ρίζα του 14.30,15 είναι 29,30. Πρόσθεσε στο 29,30 το 0,30 που πολλαπλασίασες με τον εαυτό του και 30 είναι (η πλευρά) του τετραγώνου.*

Ας δώσουμε τώρα μια εξήγηση[1] στο παραπάνω πρόβλημα με σύγχρονο συμβολισμό. Το πρόβλημα ζητάει ουσιαστικά να βρούμε τη λύση της δευτεροβάθμιας εξίσωσης $x^2 - x = 14.30$. Δεν πρέπει να ξεχνάμε ότι οι Βαβυλώνιοι χρησιμοποιούσαν το εξηκονταδικό σύστημα αρίθμησης κι έτσι ο αριθμός 14.30 είναι στην ουσία ο αριθμός $14 \cdot 60 + 30 = 870$. [2] Σύμφωνα με τα βήματα που ακολουθεί η παραπάνω λύση πρέπει αρχικά να διαιρέσουμε το 1, το οποίο είναι ίσο με $(0,60)_{60}$, διά δύο, οπότε παίρνουμε το$(0,30)_{60}$ το οποίο είναι ίσο με $30 \cdot 60^{-1} = (0,5)_{10}$. Στη συνέχεια υψώνουμε στο τετράγωνο το $(0,30)_{60}$ και βρίσκουμε $(0,15)_{60}$ (ή αλλιώς $(0,25)_{10}$). Έπειτα υπολογίζουμε το άθροισμα $(14.30)_{60} + (0,15)_{60} = (14.30,15)_{60}$ (στο δεκαδικό έχουμε $(870)_{10} + (0,25)_{10} = (870,25)_{10}$). Μετά βρίσκουμε την τετραγωνική ρίζα του $(14.30,15)_{60}$ η οποία είναι η $(29,5)_{60}$ (ή στο δεκαδικό σύστημα $\sqrt{(870,25)_{10}} = (29,5)_{10}$. Τέλος για να βρούμε το x προσθέτουμε $(29,5)_{60} + (0,30)_{60} = (30)_{60}$, δηλαδή x= $(29,5)_{10} + (0,5)_{10} = (30)_{10}$.
Αν θέλαμε να γράψουμε τα παραπάνω βήματα συμπυκνωμένα σε έναν αλγεβρικό τύπο θα είχαμε τον

$$x = \sqrt{\left(\frac{-\beta}{2}\right)^2 - \gamma} + \frac{-\beta}{2} \tag{1.2}$$

[1]Παρόμοια ανάλυση υπάρχει στο βιβλίο [36]

[2]Θα συμβολίζουμε στο εξής με $(14.30)_{60}$ έναν αριθμό στο εξηκονταδικό σύστημα και με $(870)_{10}$ έναν αριθμό στο δεκαδικό σύστημα

ο οποίος αντιστοιχεί στον τύπο (1.1) όπου α=1. Οι Βαβυλώνιοι δεν αναγνώριζαν τους αρνητικούς αριθμούς κι έτσι η άλλη ρίζα της εξίσωσης, η $x = -29$, δεν μπορεί να υπολογιστεί. Για τον ίδιο λόγο δεν είχαν μια ενιαία μορφή για τις δευτεροβάθμιες εξισώσεις όπως έχουμε τώρα, αλλά αντιμετώπιζαν διαφορετικά κάθε έναν τύπο εξισώσεων 2^{ου} βαθμού από τους τρεις που μπορούσαν να χειριστούν:

$$x^2 + \alpha x = \beta, \quad x^2 - \alpha x = \beta \quad \text{και} \quad x^2 + \beta = \alpha x$$

όπου α και β είναι θετικοί αριθμοί. Η τέταρτη μορφή: $x^2 + \alpha x + \beta = 0$ έχει αρνητικές λύσεις και δεν περιλαμβάνεται στις περιπτώσεις που μελετούσαν.

Έλληνες

Οι Αρχαίοι Έλληνες, από την ανακάλυψη των ασύμμετρων αριθμών και μετά, απέφευγαν τη θεωρητική ενασχόληση με τους αριθμούς και ενδιαφέρονταν κυρίως για την ανάπτυξη της θεωρίας ποσοτήτων ή μεγεθών με κύριο εργαλείο τους τη Γεωμετρία. Έτσι τα *"Στοιχεία"* του Ευκλείδη περιέχουν τις μεθόδους που χρησιμοποιούσαν οι Μαθηματικοί εκείνης της περιόδου. Στο ΙΙ^{ο} βιβλίο, αλλά και στο VI^{ο}, παρουσιάζονται προβλήματα σε γεωμετρική γλώσσα που όμως αν μεταφραστούν σε αλγεβρική τότε θα διαπιστώσουμε αλγεβρικά αποτελέσματα όπως ταυτότητες ή επίλυση εξισώσεων. Συγκεκριμένα, μπορούμε να διακρίνουμε τέσσερις μορφές δευτεροβάθμιων εξισώσεων:

- η εξίσωση της μορφής $x^2 = \alpha\beta$, δηλαδή η εύρεση του γεωμετρικού μέσου δύο τμημάτων, που παρουσιάζεται στην πρόταση ΙΙ.14

- η εξίσωση της μορφής $x^2 + \alpha x = \alpha^2$, δηλαδή η διαίρεση τμήματος σε μέσο και άκρο λόγο ή αλλιώς η εύρεση της χρυσής τομής, που παρουσιάζεται στην πρόταση ΙΙ.11

- η εξίσωση της μορφής $\alpha x - x^2 = \beta^2$, που βλέπουμε στην πρόταση ΙΙ.5 αλλά και στην VI.28 σε πιο γενική μορφή

  και τέλος

- η εξίσωση της μορφής $\alpha x + x^2 = \beta^2$, που βλέπουμε στην πρόταση ΙΙ.6 αλλά και σε πιο γενική μορφή στην VI.29

Μια διαφορετική προσέγγιση όμως των εξισώσεων αυτών διαπιστώνουμε στο έργο του Διόφαντου και ειδικότερα στα *"Αριθμητικά"*, όπου αν και ασχολείται όπως και οι άλλοι με συγκεκριμένες περιπτώσεις δευτεροβάθμιων εξισώσεων και όχι με τη γενική μορφή, εντούτοις χρησιμοποιεί έναν αλγεβρικό συμβολισμό με χρήση μεταβλητών, τον πρώτο που εμφανίζεται στην Ιστορία των Μαθηματικών. Βέβαια δεν αντιμετωπίζει με κάποιο γενικό τύπο τη δευτεροβάθμια εξίσωση, όμως η μέθοδός του γίνεται φανερή από την αντιμετώπιση διάφορων προβλημάτων που καταλήγουν σε αυτήν. Σύμφωνα με τον Tomas Heath [18] ο Διόφαντος θέλοντας να λύσει μια εξίσωση της μορφής

$$\alpha x^2 - \beta x + \gamma = 0$$

αντί να διαιρέσει με το συντελεστή του δευτεροβάθμιου όρου, πολλαπλασιάζει με αυτόν και τα δύο μέλη ώστε να φέρει την εξίσωση στη μορφή

$$\alpha^2 x^2 - \alpha\beta x + \alpha\gamma = 0$$

λύνοντάς την παίρνει

$$\alpha x = \frac{1}{2}\beta \pm \sqrt{\frac{1}{4}\beta^2 - \alpha\gamma}$$

και διαιρώντας κατόπιν με το α καταλήγει στη λύση

$$x = \frac{\frac{1}{2}\beta \pm \sqrt{\frac{1}{4}\beta^2 - \alpha\gamma}}{\alpha}$$

Τελικά διακρίνει τρεις περιπτώσεις δευτεροβάθμιων εξισώσεων με θετικούς συντελεστές:

- η εξίσωση της μορφής $mx^2 + px = q$ για την οποία δίνει τη λύση $x = \frac{-\frac{1}{2}p + \sqrt{\frac{1}{4}p^2 + mq}}{m}$
- η εξίσωση της μορφής $mx^2 = px + q$ για την οποία δίνει τη λύση $x = \frac{\frac{1}{2}p + \sqrt{\frac{1}{4}p^2 + mq}}{m}$
- η εξίσωση της μορφής $mx^2 + q = px$ για την οποία δίνει τη λύση $x = \frac{\frac{1}{2}p + \sqrt{\frac{1}{4}p^2 - mq}}{m}$

Ας δούμε ένα παράδειγμα (το πρόβλημα IV.31 με χρήση σύγχρονου συμβολισμού) για το πως αντιμετωπίζει ο Διόφαντος την δεύτερη μορφή δευτεροβάθμιας εξίσωσης που παρουσιάσαμε.

Πρόβλημα 2 (IV.31). *Να διαιρεθεί η μονάδα σε δύο μέρη, ώστε αν προστεθούν σ'αυτά δοσμένοι αριθμοί, τότε το γινόμενο των δύο αθροισμάτων να δίνει τετράγωνο.*
Λύση: *Έστω 3 και 5 οι αριθμοί που θα προστεθούν αντίστοιχα στα μέρη x και 1-x της μονάδας. Οπότε έχουμε*

$$(x+3)(1-x+5) = (x+3)(6-x) = 18+3x-x^2 = \text{τετράγωνο, έστω } = 4x^2$$

Άρα καταλήγουμε στην εξίσωση

$$18 + 3x = 5x^2$$

*η οποία σύμφωνα με σχόλιο του ίδιου του Διόφαντου "*δεν δίνει ρητό αποτέλεσμα*". Επειδή το 5 προέρχεται από ένα τετράγωνο που του έχουμε προσθέσει μια μονάδα, για να έχουμε ρητή λύση πρέπει να αντικαταστήσουμε το τετράγωνο που πήραμε (το 4) με ένα τετράγωνο τέτοιο ώστε:*

$$(\text{τετράγωνο} + 1) \cdot 18 + \left(\frac{3}{2}\right)^2 = \text{ένα τετράγωνο}$$

Θέτουμε

$$(m^2 + 1) \cdot 18 + 2\frac{1}{4} = \text{ένα τετράγωνο}$$

ή

$$72m^2 + 81 = \text{ένα τετράγωνο, έστω } = (8m + 9)^2$$

η οποία γίνεται

$$72m^2 + 81 = 64m^2 + 144m + 81 \Rightarrow 8m^2 = 144m \Rightarrow m = 18 \text{ άρα } m^2 = 324$$

Συνεπώς πρέπει η αρχική εξίσωση του προβλήματος να είναι η

$$(x + 3)(6 - x) = 18 + 3x - x^2 = 324x^2 \Rightarrow 3x + 18 = 325x^2$$

με λύση $x = \frac{6}{25}$. *Έτσι η λύση του προβλήματος είναι το ζεύγος* $\left(\frac{6}{25}, \frac{19}{25}\right)$.

Άραβες

Οι Άραβες μετέφρασαν και μελέτησαν πολλά Μαθηματικά κείμενα των Αρχαίων Ελλήνων, ένα από τα οποία ήταν και τα *Αριθμητικά* του Διόφαντου, κατ' επέκταση όμως ανέπτυξαν τις μεθόδους που μελετούσαν και συνέγραψαν δικές τους πραγματείες. Το πρώτο και βασικότερο σύγγραμμα των Αραβικών Μαθηματικών

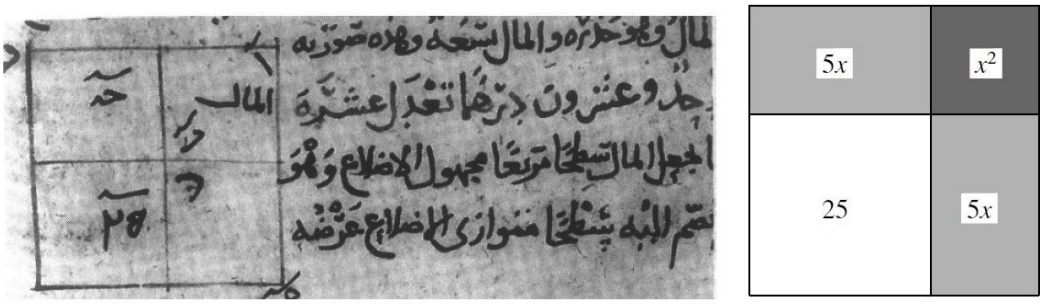
είναι το *"Al-Kitāb al-mukhtasar fī hisāb al-jabr wa-l-muqābala"* που έγραψε το 830 μ.Χ. περίπου ο Muhammad ibn Mūsā al-Khwārizmī. Από το έργο αυτό, ή καλύτερα από μια προσπάθεια λατινοποίησης του τίτλου του, γεννήθηκε από το *"al-jabr"* η λέξη Άλγεβρα. Εκεί ο al-Khwārizmī ασχολείται με την επίλυση εξισώσεων κατηγοριοποιώντας τις σε έξι τύπους:

$$\alpha x^2 = \beta x, \quad \alpha x^2 = \beta, \quad \alpha x = \beta,$$

$$\alpha x^2 + \beta x = \gamma, \quad \alpha x^2 + \gamma = \beta x, \quad \alpha x^2 = \beta x + \gamma$$

Αρχικά εξηγεί τη διαδικασία επίλυσης για κάθε μία δίνοντας οδηγίες, όπως έκαναν και οι Βαβυλώνιοι, όμως κατόπιν δίνει γεωμετρική αιτιολόγηση των βημάτων που ακολουθεί για τους τρεις τελευταίους τύπους χρησιμοποιώντας τη μέθοδο της συμπλήρωσης τετραγώνου.

Πρόβλημα 3. *Επίλυση της εξίσωσης* $x^2 + 10x = 39$
Λύση: *Σχεδιάζουμε ένα τετράγωνο πλευράς x για το* x^2 *και δύο ορθογώνια παραλληλόγραμμα με πλευρές 5 και x για τον όρο 10x, όπως στο σχήμα 1.1. Σύμφωνα με τα δεδομένα της εξίσωσης η γκρι περιοχή ισούται με 39 κι έτσι όλο το τετράγωνο έχει εμβαδό* $39 + 25 = 64 = 8 \cdot 8$ *και επομένως* $5 + x = 8$*, άρα* $x = 3$.

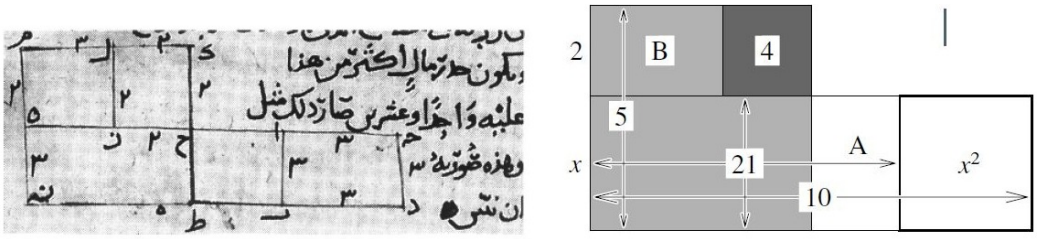


Χειρόγραφο του 1342 ***Σύγχρονο σχήμα***

Σχήμα 1.1: Λύση της $x^2 + 10x = 39$

Πρόβλημα 4. *Επίλυση της εξίσωσης* $x^2 + 21 = 10x$
Λύση: *Σχεδιάζουμε ένα τετράγωνο πλευράς x για το* x^2 *και προσαρτούμε δίπλα του ένα ορθογώνιο παραλληλόγραμμο πλάτους x και αγνώστου μήκους για τον όρο 21x, όπως στο σχήμα 1.2. Σύμφωνα με τα δεδομένα της εξίσωσης το συνολικό σχήμα έχει μήκος 10. Χωρίζουμε το σχήμα στη μέση και τοποθετούμε το μικρό ορθογώνιο (A) που περιέχεται ανάμεσα στο* x^2 *και στη γραμμή που διχοτομεί, στο επάνω μέρος, στη θέση (B).*

Παίρνουμε έτσι ένα σχήμα με ύψος 5. Η γκρι περιοχή ισούται με 21 και το συνολικό τετράγωνο (γκρι και μαύρο) ειναι $5 \cdot 5 = 25$. *Συνεπώς το μαύρο τετράγωνο θα πρέπει να έιναι ίσο με:* $25 - 21 = 4 = 2 \cdot 2$ *και έτσι παίρνουμε ότι* $x = 3$.
Με ένα παρεμφερές σχήμα ο al-Khwārizmī βρίσκει και τη δεύτερη λύση $x = 7$.



Χειρόγραφο του 1342 *Σύγχρονο σχήμα*

Σχήμα 1.2: Λύση της $x^2 + 21 = 10x$

Είναι χρήσιμο να σημειωθεί ότι αν και η γεωμετρία που χρησιμοποιεί ο al-Khwārizmī είναι στοιχειώδης σε σχέση με την γεωμετρία των Αρχαίων Ελλήνων και δεν βασίζεται σε κάποιο αξιωματικό σύστημα αλλά στη διαίσθηση, εντούτοις τα αλγεβρικά εργαλεία και μέθοδοι που αναπτύσσει θα είναι το πρώτο βήμα για την περαιτέρω ανάπτυξη της Άλγεβρας ως κλάδος των Μαθηματικών.

1.1.2 Εξισώσεις 3ου βαθμού

Προβλήματα που οδηγούσαν σε τριτοβάθμιες εξισώσεις εμφανίστηκαν από τα Αρχαία χρόνια και από τους πρώτους οι οποίοι τα αντιμετώπισαν με επιτυχία ήταν οι

Έλληνες

Η παλαιότερη καταγραφή τέτοιου προβλήματος παρουσιάζεται στο έργο του Μέναιχμου (325–375 π.Χ.) ο οποίος θέλοντας να βρει τη λύση της εξίσωσης $x^3 = \alpha^2\beta$ οδηγείται στην εύρεση της τομής της παραβολής $x^2 = \alpha y$ και της έλλειψης $xy = \alpha\beta$. Ένα άλλο γνωστό πρόβλημα που καταλήγει σε τριτοβάθμια εξίσωση είναι η αναζήτηση του Αρχιμήδη της τομής μια σφαίρας ακτίνας R από ένα επίπεδο, με τέτοιο τρόπο, ώστε ο λόγος των όγκων των δύο μερών να ισούται με

δεδομένη τιμή m. Το πρόβλημα καταλήγει τελικά στην αναζητηση του ύψους h του ενός από τα δύο μέρη από την εξίσωση $h^3 + \frac{4m}{m+1}R^3 = 3Rh^2$. Το πιο γνωστό πρόβλημα όμως από το οποίο προκύπτει τριτοβάθμια εξίσωση είναι το Δήλιο πρόβλημα ή ο διπλασιασμός του κύβου, το οποίο καταλήγει στην εξίσωση $x^3 = 2\alpha^3$. Αν και οι Έλληνες δεν μπόρεσαν να βρουν μια λύση (αφού δεν υπάρχει τέτοια) με τους περιορισμούς που είχαν θέσει (κατασκευή μόνο με κανόνα και διαβήτη), κατάφεραν να λύσουν το πρόβλημα με πολλούς τρόπους με χρήση κωνικών τομών και άλλων καμπυλών. Βέβαια όπως ακριβώς και στην περίπτωση της δευτεροβάθμιας εξίσωσης που ήδη αναφέραμε, έτσι και εδώ, οι Αρχαίοι Έλληνες χρησιμοποίησαν καθαρά γεωμετρικές μεθόδους και δούλεψαν ξεχωριστά κάθε περίπτωση που προέκυπτε χωρίς να καταπιαστούν με τη γενική μορφή μιας τριτοβάθμιας εξίσωσης.

Άραβες

Η συμβολή των Αράβων Μαθηματικών στην προσπάθεια επίλυσης της τριτοβάθμιας εξίσωσης εκφράστηκε κυρίως μέσα από το έργο του Πέρση ποιητή, μαθηματικού και αστρονόμου Omar Khayyám γύρω στο 1070 μ.Χ. με τίτλο:*"Risāla fī-l-barāhin 'ala masā'il al-jabr w'al muqābala" (Treatise on Demonstrations of Problems of al-Jabr and al-Muqabala)*. Είναι η πρώτη συστηματική πραγματεία που ασχολείται με τη γεωμετρική επίλυση της τριτοβάθμιας εξίσωσης στη γενική της μορφή, όπου οι λύσεις δεν είναι αριθμητικές αλλά ευθύγραμμα τμήματα. Αναφέρει μαλιστα ρητά ότι το έργο του βασίζεται και μπορεί να κατανοηθεί μέσα από την καλή γνώση των *Στοιχείων* και των *Δεδομένων* του Ευκλείδη καθώς και των *Κωνικών* του Απολλώνιου. Η απαίτηση αυτή γίνεται κατανοητή αφού στο βιβλίο αυτό αποδεικνύει γεωμετρικά ότι οι λύσεις προκύπτουν ως τομές κωνικών τομών. Για να αποφύγει τους αρνητικούς συντελεστές ο Omar Khayyám κατηγοριοποιεί τις εξισώσεις σε 16 είδη. Οι έξι πρώτες είναι αυτές που αναφέρει και ο al-Khwārizmī και οι υπόλοιπες έξι με τις οποίες ασχολείται συστηματικά είναι:

$$x^3 + \alpha x = \beta, \quad x^3 + \beta = \alpha x, \quad \alpha x + \beta = x^3,$$

$$x^3 + \alpha x^2 = \beta, \quad x^3 + \beta = \alpha x^2, \quad \alpha x^2 + \beta = x^3$$

Αίσθηση προκαλεί η φράση που αναφέρει ο ίδιος σχετικά με τη δυνατότητα εύρεσης αριθμητικής λύσης των εξισώσεων αυτών, πως "είναι αδύνατον τόσο για εμάς όσο και για όσους προηγήθηκαν να

βρεθεί τέτοιου είδους λύση. Ίσως κάποιος μεταγενέστερος το πραγματοποιήσει." Για να αντιληφθούμε τον τρόπο με τον οποίο δουλεύει θα εξετάσουμε ως παράδειγμα[3] τη λύση που δίνει για τη μορφή

$$x^3 + \alpha x = \beta \tag{1.3}$$

Ο Omar Khayyám σκέφτεται γεωμετρικά οπότε βλέπει κάθε όρο της εξίσωσης με τη ίδια διάσταση, άρα λόγω της ύπαρξης του x^3 οι όροι είναι τρισδιάστατα στερεά . Έτσι ο συντελεστής α λαμβάνεται ως δισδιάστατη επιφάνεια, έστω ότι είναι ένα τετράγωνο πλευράς ΑΒ όπως στο σχήμα 1.3. Ομοίως ο όρος β είναι παριστάνεται ως ορθογώνιο παραλληλεπίπεδο με ακμές ΑΒ, ΑΒ και ΒΘ. Ο Omar Khayyám φέρει τον κύκλο με διάμετρο ΒΘ και την παραβολή ΓΒΔ με κορυφή το Γ και παράμετρο ΑΒ, δηλαδή την παραβολή με εξίσωση ΒΗ·ΒΗΖ=ΑΒ·ΒΖ ή με σύγχρονο συμβολισμό, αφού $\text{AB}^2 = \alpha \Rightarrow \text{AB} = \sqrt{\alpha}$, είναι η $x^2 = \sqrt{\alpha} \cdot y$. Στη συνέχεια αποδεικνύει ότι το ευθύγραμμο τμήμα ΗΒ που προκύπτει από την τομή του κύκλου και της παραβολής είναι η λύση της τριτοβάθμιας εξίσωσης. Πρώτα γράφει την εξίσωση της παραβολής ως αναλογία:

$$\frac{\text{AB}}{\text{BH}} = \frac{\text{BH}}{\text{BZ}} \tag{i}$$

Για τον κύκλο ισχύει η αναλογία (θεωρώντας το ύψος ΗΔ του ορθογωνίου τριγώνου ΒΔΘ):

$$\Delta\text{H}^2 = \text{BH} \cdot \text{H}\Theta \Longrightarrow \frac{\text{BH}}{\text{H}\Delta} = \frac{\text{H}\Delta}{\text{H}\Theta} \tag{ii}$$

Επειδή όμως ισχύει ότι ΒΖ=ΗΔ, από τις (i) και (ii) παίρνουμε τις σχέσεις:

$$\frac{\text{AB}}{\text{BH}} = \frac{\text{BH}}{\text{H}\Delta} \quad \text{και} \quad \frac{\text{AB}}{\text{BH}} = \frac{\text{H}\Delta}{\text{H}\Theta}$$

οι οποίες πολλαπλασιαζόμενες κατά μέλη δίνουν τη σχέση:

$$\frac{\text{AB}^2}{\text{BH}^2} = \frac{\text{BH} \cdot \text{H}\Delta}{\text{H}\Delta \cdot \text{H}\Theta} \Longrightarrow \text{AB}^2 \cdot \text{H}\Theta = \text{BH}^3 \tag{iii}$$

Αν τώρα και στα δύο μέλη της (iii) προσθέσουμε το ορθογώνιο παραλληλεπίπεδο με ακμές ΑΒ, ΑΒ και ΒΗ, δηλαδή την ποσότητα $\text{AB}^2 \cdot \text{BH}$ τότε παίρνουμε την εξίσωση

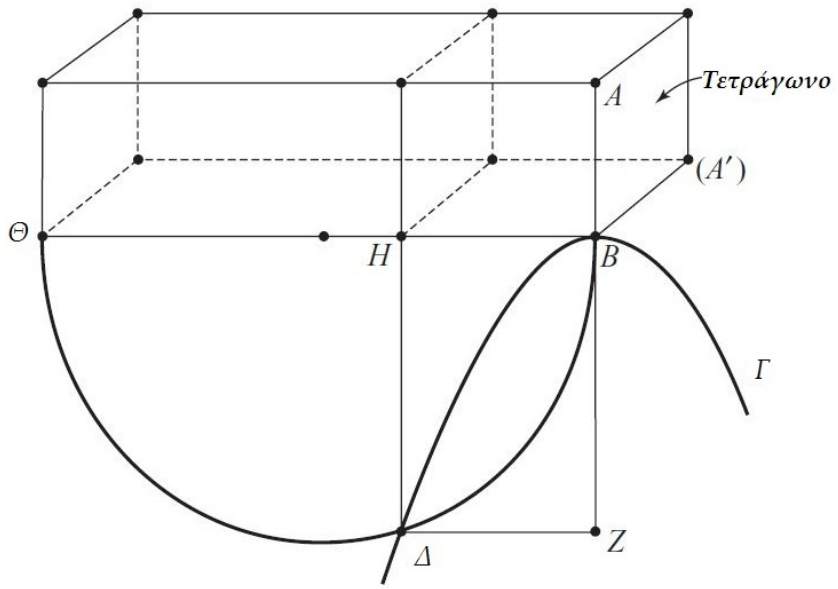
$$\text{AB}^2 \cdot \text{B}\Theta = \text{BH}^3 + \text{AB}^2 \cdot \text{BH}$$

[3]παράδειγμα από το [23]

η οποία μεταφρασμένη στους συντελεστές της αρχικής τριτοβάθμιας εξίσωσης είναι η:

$$\beta = \text{BH}^3 + \alpha \cdot \text{BH}$$

Βλέπουμε λοιπόν ότι το ευθύγραμμο τμήμα BH ικανοποιεί την 1.3 δηλαδη είναι η ζητούμενη λυση.



Σχήμα 1.3: Λύση της $x^3 + \alpha x = \beta$

Ένας άλλος σημαντικός Πέρσης μαθηματικός που εξέλιξε σημαντικά τη μελέτη των τριτοβάθμιων εξισώσεων ήταν ο Sharaf al-Dīn al-Tūsī με το έργο του *"Al-Mu'adalat" (Treatise on Equations)*, όπου βρίσκει αλγεβρικές και αριθμητικές λύσεις τριτοβάθμιων εξισώσεων εισάγοντας την έννοια της παραγώγου του πολυωνύμου τρίτου βαθμού για την εύρεση μεγίστων και ελαχίστων ώστε να μπορέσει να προσδιορίσει τα διαστήματα που περιέχουν τις ρίζες της εξίσωσης.

Ιταλία

Η πλήρης αντιμετώπιση της γενικής μορφής της τριτοβάθμιας εξίσωσης έγινε τελικά τον 16ο αιώνα στην Ιταλία. Συγκεκριμένα παρουσιάστηκε το 1545 από τον Gerolamo Cardano στο έργο του *"Artis magnae, sive de regulis algebraicis"* (γνωστό και ως *Ars magna*). Μια περιληπτική ιστορία της εύρεσης της μεθόδου μας δίνει ο ίδιος ο Cardano στην αρχή του XI κεφαλαίου [4]:

> "Ο Scipio Ferro από την Μπολόνια πριν από σχεδόν τριάντα χρόνια ανακάλυψε αυτόν τον κανόνα και τον παρέδωσε στον Antonio Maria Fior από τη Βενετία, του οποίου ο διαγωνισμός με τον Niccolo Tartaglia της Μπρέσια έδωσε στο Niccolo την ευκαιρία να τον ανακαλύψει εκ νέου. Αυτός [ο Tartaglia] τον έδωσε σε μένα ως ανταπόκριση στις παρακλήσεις μου, αλλά κρατώντας την απόδειξη. Οπλισμένος με αυτή τη βοήθεια, αναζήτησα την απόδειξή της σε [διάφορες] μορφές."

Ο Cardano στο έργο του, σε αντίθεση με τη σύγχρονη αντίληψή μας, δεν δίνει μια γενική μέθοδο επίλυσης της τριτοβάθμιας εξίσωσης αλλά περιγράφει ξεχωριστές μεθόδους για κάθε περίπτωση (ώστε να εμφανίζονται μόνο θετικοί συντελεστές) σε 13 κεφάλαια. Επιπλέον η επιχειρηματολογία του είναι καθαρά γεωμετρική δηλαδή εμπλέκει στην κυριολεξία κύβους και τους όγκους τους λύνοντας συγκεκριμένα παραδείγματα. Πιο συγκεκριμένα δίνει πρώτα τη λύση εξισώσεων που περιέχουν τον τριτοβάθμιο, τον πρωτοβάθμιο και τον σταθερό όρο, δηλαδή σε ανηγμένη μορφή (depressed cubic) και στις υπόλοιπες περιπτώσεις δίνει τη μέθοδο μετασχηματισμού τους σε αυτές που ήδη έχει αντιμετωπίσει.

Στο XI κεφάλαιο ο Cardano παρουσιάζει τη μέθοδό του για την επίλυση της εξίσωσης $x^3 + \alpha x = \beta$. Φαντάζεται έναν κύβο με πλευρά t η οποία χωρίζεται σε δύο (βοηθητικά) τμήματα μήκους u και t-u όπως φαίνεται στο σχήμα 1.4. Σχηματίζονται έτσι μέσα στον αρχικό κύβο ακμής t, δύο κύβοι με ακμές t-u και u αντίστοιχα και τρία ορθογώνια παραλληλεπίπεδα με ακμές t, u και t-u. Με αλγεβρικό συμβολισμό σύμφωνα με το σχήμα παίρνουμε την ισότητα[4]

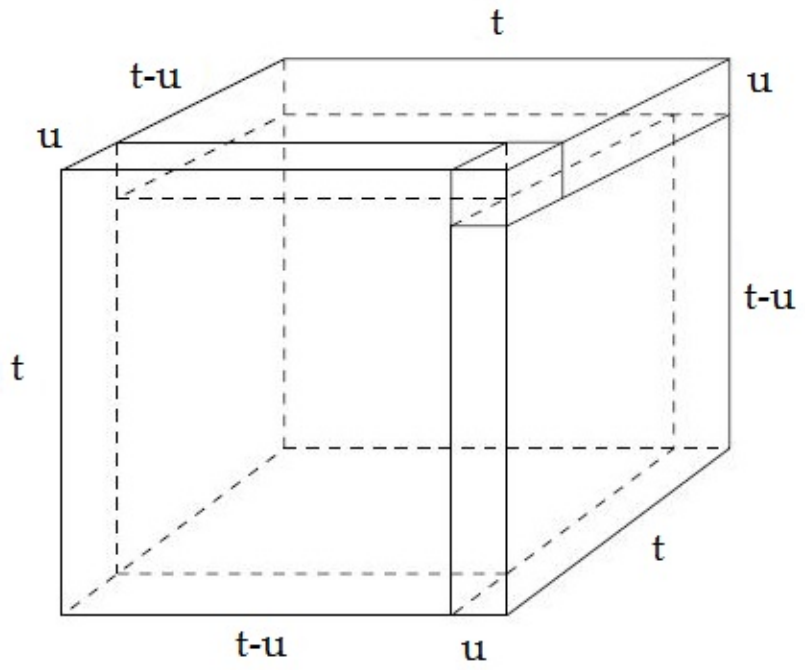
$$(t-u)^3 + 3tu(t-u) = t^3 - u^3 \tag{1.4}$$

Θέτοντας στην παραπάνω εξίσωση $x = t - u$ τότε η (1.4) γίνεται

$$x^3 + 3tux = t^3 - u^3$$

Δηλαδή είναι η ανηγμένη τριτοβάθμια $x^3 + \alpha x = \beta$ όπου όμως έχουμε $3tu = \alpha$ και $t^3 - u^3 = \beta$. Πρέπει να υπολογίσουμε δηλαδή τα t και u από τα γνωστά α και β. Αντικαθιστούμε με $u = \frac{\alpha}{3t}$ στην $t^3 - u^3 = \beta$ και

[4]προφανώς η σχέση αυτή είναι άμεσα φανερή από το αλγεβρικό ανάπτυγμα του κύβου διαφοράς, όμως οι αλγεβρικοί χειρισμοί αυτού του είδους δεν ήταν διαθέσιμοι στους μαθηματικούς του 16ου αιώνα.



Σχήμα 1.4: Λύση του Cardano για την $x^3 + \alpha x = \beta$

καταλήγουμε στην ρητή εξίσωση

$$t^3 - \frac{\alpha^3}{27t^3} = \beta$$

η οποία αν πολλαπλασιαστεί με t^3 γίνεται μια πολυωνυμική εξίσωση έκτου βαθμού

$$t^6 - \beta t^3 - \frac{\alpha^3}{27} = 0$$

Αν και αρχικά φαίνεται ότι, αντί να κάνουμε ένα βήμα προόδου, δυσκολέψαμε την κατάσταση μετασχηματίζοντας μια τριτοβάθμια εξίσωση σε εκτοβάθμια, εν τούτοις μπορούμε να δούμε την τελευταία εξίσωση που προέκυψε ως δευτεροβάθμια με άγνωστο t^3 δηλαδή

$$(t^3)^2 - \beta(t^3) - \frac{\alpha^3}{27} = 0$$

η οποία λύνεται με τον ήδη γνωστό τύπο

$$t^3 = \frac{\beta \pm \sqrt{\beta^2 + \frac{4\alpha^3}{27}}}{2}$$

ή κρατώντας μόνο τη θετική λύση

$$t = \sqrt[3]{\frac{\beta}{2} + \sqrt{\frac{\beta^2}{4} + \frac{\alpha^3}{27}}}$$

Μπορούμε τώρα να υπολογίσουμε και το u αφού $u^3 = t^3 - \beta$ και έτσι παίρνουμε

$$u = \sqrt[3]{-\frac{\beta}{2} + \sqrt{\frac{\beta^2}{4} + \frac{\alpha^3}{27}}}$$

Εφόσον είχαμε θέσει όμως $x = t - u$ παίρνουμε τον λεγόμενο *τύπο του Cardano*

$$x = \sqrt[3]{\frac{\beta}{2} + \sqrt{\frac{\beta^2}{4} + \frac{\alpha^3}{27}}} - \sqrt[3]{-\frac{\beta}{2} + \sqrt{\frac{\beta^2}{4} + \frac{\alpha^3}{27}}} \tag{1.5}$$

Στο XVII κεφάλαιο ο Cardano δείχνει τον τρόπο μετασχηματισμού της πλήρους τριτοβάθμιας $x^3 + \alpha x^2 + \beta x = \gamma$ σε ανηγμένη μορφή, πάλι χρησιμοποιώντας συγκεκριμένο παράδειγμα και γεωμετρική επιχειρηματολογία. Θέτει το μετασχηματισμό[5] $x = y - \frac{\alpha}{3}$ και απαλείφοντας με αυτόν τον τρόπο τον δευτεροβάθμιο όρο, παίρνει την ανηγμένη μορφή που έχει ήδη μελετήσει προηγουμένως στο XI κεφάλαιο.

Casus irreducibilis

Ένα βήμα πιο πέρα από τον Cardano έκανε ο συμπατριώτης του Rafael Bombelli το 1572 στο έργο του με τον απλό τίτλο *Algebra*, όπου παρατηρεί για την τριτοβάθμια εξισωση: $x^3 = 15x + 4$ ότι αν και έχει την προφανή λύση $x = 4$, ο τύπος του Cardano εμφανίζει την ποσότητα

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

η οποία περιέχει την τετραγωνική ρίζα ενός αρνητικού αριθμού και έτσι δεν είναι αποτελεσματικός, για το λόγο αυτό η περιπτωση αυτή ονομάστηκε ανάγωγη περίπτωση, γνωστή και με το λατινικό όνομα *"casus irreducibilis"*. Αν και οι μιγαδικοί αριθμοί δεν ήταν αποδεκτοί εκείνη την εποχή, όπως επίσης και οι αρνητικοί, ο Bombelli παρ' όλα αυτά επιχειρεί να κάνει κάποιους υπολογισμούς και είναι η πρώτη φορά στην Ιστορία των Μαθηματικών που εμφανίζονται σε βιβλίο

[5] για την γενική τριτοβάθμια $\alpha x^3 + \beta x^2 + \gamma x + \delta = 0$ θέτουμε $x = y - \frac{\beta}{3\alpha}$

υπολογισμοί αυτού του είδους. Παρατηρεί λοιπόν, πιθανόν με τη μέθοδο της δοκιμής και λάθους, ότι

$$(2+\sqrt{-1})^3 = 8 + 12\sqrt{-1} - 6 - \sqrt{-1} = 2 + 11\sqrt{-1} = 2 + \sqrt{-121}$$

άρα συμπεραίνει ότι

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

και με παρόμοιο τρόπο ότι

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

κι έτσι καταλήγει στην ήδη γνωστή λύση

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

Αν και η προσέγγιση του Bombelli ήταν ένα βήμα προόδου, δεν έδινε κανένα στοιχείο για το πως θα μπορούσαμε να βρούμε τις κυβικές ρίζες μιγαδικών αριθμών.[6] Αναμφίβολα όμως έδειξε ότι ο δρόμος για την αλγεβρική λύση των πολυωνυμικών εξισώσεων πέρναγε μέσα από τα μονοπάτια των μιγαδικών αριθμών.

Θα δούμε τώρα μια πιο αποτελεσματική αντιμετώπιση του ζητήματος αυτού από τον François Viète σε μια εργασία του με τίτλο *"Ad angulares sectiones theoremata" (Most General Theorems on Divisions of Angles)*, [7] στην οποία μετά από μια ανάλυση για την τριχοτόμηση των γωνιών, συνειδητοποιεί ότι το πρόβλημα της τριχοτόμησης οδηγεί σε μια τριτοβάθμια εξισωση, έτσι προχωράει στην λύση της *casus irreducibilis* με τη βοήθεια της τριγωνομετρίας. Έχουμε την εξίσωση με θετικούς συντελεστές

$$x^3 - 3\alpha x = \beta \tag{1.6}$$

η οποία σύμφωνα με τον τύπο (1.5) είναι ανάγωγη περίπτωση τριτοβάθμιας εφόσον η υπόρριζη ποσότητα κάτω από την τετραγωνική ρίζα είναι αρνητική:

$$\frac{\beta^2}{4} + \frac{(-3\alpha)^3}{27} < 0 \Longrightarrow \frac{\beta^2}{4} < \frac{27\alpha^3}{27} \Longrightarrow \beta^2 < 4\alpha^3$$

[6] Το πρόβλημα αυτό λύθηκε στα μέσα του 18ου αιώνα από τον Ελβετό Μαθηματικό Leonhard Euler.

[7] πληροφορία από [37]

Λόγω του ότι το β είναι θετικό και της παραπάνω σχέσης παιρνουμε ότι $\alpha > 0$ και μπορούμε να θέσουμε $x = 2y\sqrt{\alpha}$ η (1.6) γίνεται

$$8\sqrt{\alpha^3}y^3 - 3\alpha 2y\sqrt{\alpha} = \beta \Longrightarrow 4y^3 - 3y = \frac{\beta}{2\alpha\sqrt{\alpha}} \tag{1.7}$$

Ο Viète παρατήρησε ότι η σχέση (1.7) είναι απλά ένας μετασχηματισμός της τριγωνομετρικής σχέσης

$$4\cos^3\theta - 3\cos\theta = \cos(3\theta)$$

η οποία είχε προέλθει από το πρόβλημα της τριχοτόμησης της γωνίας. Έτσι μπόρεσε να υπολογίσει ότι

$$\cos(3\theta) = \frac{\beta}{2\alpha\sqrt{\alpha}} \Longrightarrow \theta = \frac{\cos^{-1}\left(\frac{\beta}{2\alpha\sqrt{\alpha}}\right)}{3}$$

και έχοντας $y = \cos\theta$ βρήκε μια πραγματική λύση για την (1.6), την

$$x = 2\sqrt{\alpha}\cos\theta \Longrightarrow x = 2\sqrt{\alpha}\cos\left(\frac{\cos^{-1}\left(\frac{\beta}{2\alpha\sqrt{\alpha}}\right)}{3}\right)$$

1.1.3 Εξισώσεις 4ου βαθμού

Στο ίδιο έργο που παρουσιάζεται για πρώτη φορά η λύση για τη γενική τριτοβάθμια, ο Cardano παρουσιάσει και την πλήρης αντιμετώπιση των τεταρτοβάθμιων εξισώσεων. Στο κεφάλαιο XXXIX συγκεκριμένα στον πρόλογο της μεθόδου αναφέρει: *"Υπάρχει και ένας άλλος κανόνας, πιο ευγενής από τον προηγούμενο. Είναι του Lodovico Ferrari, ο οποίος μου τον έδωσε ύστερα από αίτημά μου. Με αυτόν μπορούμε να έχουμε όλες τις λύσεις για τις εξισώσεις τέταρτου βαθμού"*. Ξεκινώντας από τη γενική τεταρτοβάθμια εξίσωση

$$\alpha x^4 + \beta x^3 + \gamma x^2 + \delta x + \epsilon = 0 \tag{1.8}$$

εφαρμόζουμε τον μετασχηματισμό [8] $x = y - \frac{\beta}{4\alpha}$ για να απαλείψουμε τον τριτοβάθμιο όρο. Συνεχίζοντας με χρήση βοηθητικών μεταβλητών, όπως κάναμε και για την τριτοβάθμια, καταφέρνουμε να μετασχηματίσουμε την (1.8) σε τριτοβάθμια και να βρούμε τις λύσεις της.

[8] οι μετασχηματισμοί αυτής της μορφής ονομάζονται μετασχηματισμοί του Tschirnhaus

1.2 Συμμετρικά πολυώνυμα

Ακόμα μετά από την επιτυχημένη αντιμετώπιση των πολυωνυμικών εξισώσεων μέχρι και $4^{ου}$ βαθμού, οι Μαθηματικοί εξακολουθούν να τις μελετούν, να βρίσκουν ιδιότητές τους που δεν ήταν γνωστές και να αποδεικνύουν νέα θεωρήματα. Αυτό είναι πιθανόν να συμβαίνει επειδή έψαχναν το επόμενο βήμα, την λύση της πεμπτοβάθμιας εξίσωσης. Όπως θα φανεί πολύ αργότερα οι τεχνικές που χρησιμοποίησαν για τις εξισώσεις $3^{ου}$ και $4^{ου}$ βαθμού ήταν εξαρχής καταδικασμένες να αποτύχουν, έτσι στράφηκαν σε άλλους τρόπους προσέγγισης και πιο συγκεκριμένα στην μελέτη της σχέση των ριζών μιας εξίσωσης με τους συντελεστές της, ελπίζοντας ότι θα τους βοηθήσει να ανακαλύψουν τον τύπο που δίνει τις λύσεις. Αυτή την πορεία θα δούμε σ'αυτήν την παράγραφο η οποία καταλήγει ουσιαστικά στα λεγόμενα συμμετρικά πολυώνυμα. [9]

Ο πρώτος που αναγνωρίζει μια σχέση τέτοιου είδους είναι ο Cardano στο έργο που ήδη έχουμε αναφέρει [4, Κεφ.1 §8]. Εκεί αναφέρει με παράδειγμα την εξίσωση $x^3 + 72 = 11x^2$ και τις ρίζες[10] της, $\sqrt{40} - 4$ η αρνητική (ή πλασματική όπως την ονομάζει), 3 και $\sqrt{40} + 4$ οι θετικές, ότι η διαφορά θετικών και αρνητικών ριζών δίνει τον συντελεστή του δευτεροβάθμιου όρου. Πράγματι $\left[3 + (\sqrt{40} + 4)\right] - (\sqrt{40} - 4) = 7 + \sqrt{40} - \sqrt{40} + 4 = 11$.

Μια δεύτερη αναφορά στη σχέση ριζών και συντελεστών υπάρχει στην Άλγεβρα του Γάλλου Jacques Peletier το 1554 με τίτλο *De occulta parte numerorum, quam algebram vocant, libri duo*. Παρουσιάζεται μια μέθοδος εύρεσης των ριζών μιας εξίσωσης μεταξύ των διαιρετών του σταθερού όρου, όταν η ρίζα είναι ρητός αριθμός, είτε ακέραιος είτε κλάσμα. Ο Peletier παρατηρεί ότι η ρίζα είναι πάντα "κρυμμένη" σ'αυτόν τον όρο αφού είναι κάποιος από τους διαιρέτες του.

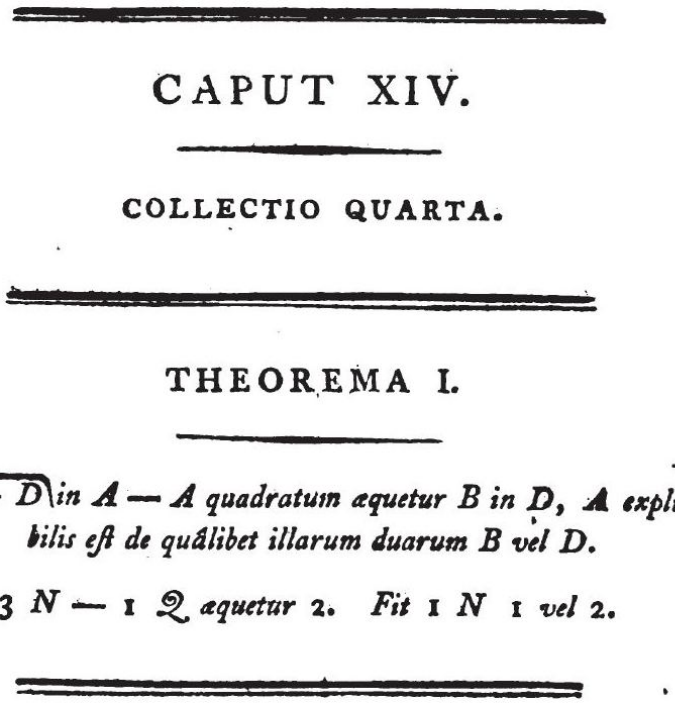
Όμως μέχρι τότε οι Μαθηματικοί δεν είχαν τη δυνατότητα να διακρίνουν βαθύτερες σχέσεις μεταξύ ριζών και συντελεστών όταν η εξίσωση και η λύση της δίνονταν με λεκτικό τρόπο. Έτσι στην αναζήτηση αυτή τον βασικότερο ίσως ρόλο έπαιξε η καθιέρωση και η βελτίωση της συμβολικής αλγεβρικής γλώσσας. Ως γνωστό ο πρωτοπόρος στον αλγεβρικό συμβολισμό ήταν ο François Viète, ο οποίος είδε λίγο πιο βαθιά από τους προγενέστερούς του.

[9] αναφορά από το [14]

[10] αν και βρίσκει λάθος λύσεις της εξίσωσης αφού οι σωστές είναι 3, $-\sqrt{40} + 4$ και $\sqrt{40} + 4$ αυτό δεν τον εμποδίζει να δει τη σχέση ριζών και συντελεστών

Viète

Τα αποτελέσματά του στο πεδίο που εξετάζουμε, βρίσκονται σε μια έκδοση μετά το θάνατό του, το 1615 με τίτλο *Francisci Vietae Fontenaeensis de aequationum recognitione et emendatione* που επιμελήθηκε ο Alexander Anderson. Στο 14ο κεφάλαιο της έκδοσης αυτής υπάρχουν χωρίς απόδειξη τέσσερα θεωρήματα για τη γενική σχέση των ριζών πολυωνυμικών εξισώσεων και των συντελεστών τους, όταν οι ρίζες είναι θετικές. Το πρώτο θεώρημα παρουσιάζεται με την αυθεντική του μορφή (στα Λατινικά) στην εικόνα 1.5. Σε σύγχρονο συμβολισμό



CAPUT XIV.

COLLECTIO QUARTA.

THEOREMA I.

Si $\overline{B + D}$ *in A — A quadratum æquetur B in D, A explicabilis eſt de quâlibet illarum duarum B vel D.*

3 *N* — 1 ♀ *æquetur* 2. *Fit* 1 *N* 1 *vel* 2.

Σχήμα 1.5: Θεώρημα του Viète για τη σχέση ριζών και συντελεστών της δευτεροβάθμιας εξίσωσης

διατυπώνεται ως εξής:

Θεώρημα 1.2.1. *Αν* $(\alpha + \beta)x - x^2 = \alpha\beta$ *τότε* $x = \alpha$ *ή* β

$$\textit{Παράδειγμα} \quad 3x - x^2 = 2 \Longrightarrow x = 1 \text{ ή } 2$$

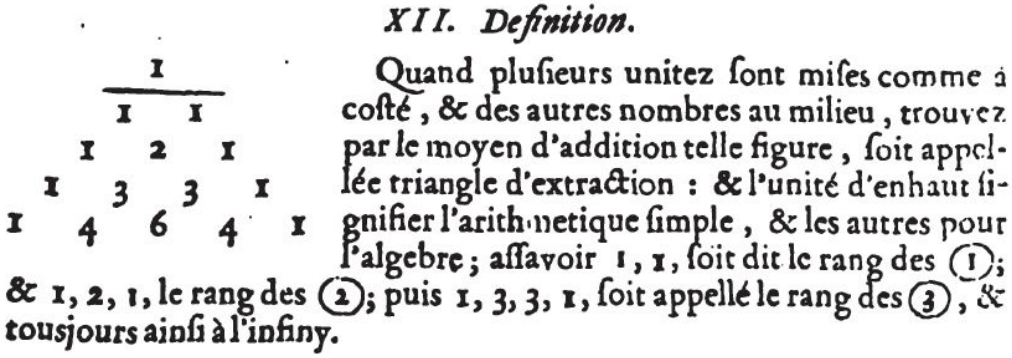
Με παρόμοιο τρόπο στα υπόλοιπα θεωρήματα δίνει τους τύπους για την κυβική και την τεταρτοβάθμια εξίσωση. Αυτό δείχνει ότι ο Viète είχε μια ξεκάθαρη αντίληψη για τη σχέση των ριζών και των

συντελεστών ενός πολυωνύμου, αν και η απόρριψη των ριζών που δεν ήταν θετικές τον εμπόδισε να επεκταθεί στη γενική μελέτη των συμμετρικών συναρτήσεων των ριζών πολυωνύμων. Όμως άνοιξε το δρόμο στον επόμενο Μαθηματικό του οποίου το έργο είναι η πρώτη ολοκληρωμένη μελέτη αυτού του αντικειμένου.

Girard

Σε ένα φυλλάδιο με τίτλο *"Invention Nouvelle en l'Algèbre"*[16] που εκδόθηκε το 1629 στο Amsterdam, ο Albert Girard αποδεικνύει ότι ήταν ο πρώτος που κατανόησε τη γενική θεωρία του σχηματισμού των συντελεστών μιας εξίσωσης από τα αθροίσματα των ριζών της και τα γινόμενά τους. Ο Girard ξεκινάει από το γνωστό σε μας ως τρίγωνο του Pascal και το χρησιμοποιεί για να αναπτύξει ένα θεώρημά του σχετικό με τα συμμετρικά πολυώνυμα, αν και δεν τα κατονομάζει με αυτόν τον όρο. Στο σχήμα 1.6 ο Girard διατυπώνει την κατασκευή του "Τριγώνου του Pascal". Συγκεκριμένα αναφέρει:

> "Όταν δοθούν πολλές μονάδες όπως δίπλα (εννοεί το σχήμα) και οι υπόλοιποι αριθμοί στο μέσο βρίσκονται με την πράξη της πρόσθεσης (εννοεί των δύο από πάνω τους) τότε αυτό το σχήμα ονομάζεται "τρίγωνο εξαγωγής" (triangle d'extraction). Η μονάδα της κορυφής αντιστοιχεί στην απλή αριθμητική και οι υπόλοιπες στην άλγεβρα και ειδικότερα η πρώτη γραμμή με τα 1,1 στις πρωτοβάθμιες, η σειρά με 1,2,1 στις δευτεροβάθμιες και η γραμμή 1,3,3,1 στις τριτοβάθμιες εξισώσεις. Συνεχιζοντας με τον ίδιο τρόπο μέχρι το άπειρο."


XII. Definition.

1
1 1
1 2 1
1 3 3 1
1 4 6 4 1

Quand plusieurs unitez sont mises comme à costé, & des autres nombres au milieu, trouvez par le moyen d'addition telle figure, soit appellée triangle d'extraction : & l'unité d'enhaut signifier l'arithmetique simple, & les autres pour l'algebre; assavoir 1, 1, soit dit le rang des (1); & 1, 2, 1, le rang des (2); puis 1, 3, 3, 1, soit appellé le rang des (3), & tousjours ainsi à l'infiny.

Σχήμα 1.6: Ορισμός του Girard για το "Τρίγωνο του Pascal"

Ονομάζοντας ως *""première faction"(πρώτη τάξη)* το άθροισμα μιας ομάδας αριθμών, ως *""deuxième faction"(δεύτερη τάξη)* το άθροισμα των γινομένων τους ανά δύο και ούτω καθεξής, διατυπώνει το παρακάτω θεώρημα, το οποίο με τη βοήθεια του "τριγώνου εξαγωγής" καθορίζει πόσους προσθετέους έχει κάθε τέτοια τάξη:

Θεώρημα 1.2.2. *Δεδομένου ενός πλήθους αριθμών, τότε το πλήθος των γινομένων κάθε τάξης μπορεί να βρεθεί από το "τρίγωνο εξαγωγής" από την σειρά εκείνη που είναι και το πλήθος των αριθμών.*

Αμέσως μετά ο ίδιος ο Girard δίνει ένα παράδειγμα όπου γίνεται κατανοητό το νόημα του θεωρήματος. Συγκεκριμένα αναφέρει:

> "Έστω 4 αριθμοί. Πρέπει να πάρουμε την 4η σειρά του τριγώνου εξαγωγής η οποία είναι η 1,4,6,4,1. Το πρώτο 1 σημαίνει τη μονάδα (εννοεί ως συντελεστή) του μέγιστου (εννοεί του μεγιστοβάθμιου όρου). Το 4 σημαίνει ότι η πρώτη τάξη είναι το άθροισμα των τεσσάρων αριθμών που δοθηκαν. Το 6 σημαίνει ότι η δεύτερη τάξη αποτελείται από το άθροισμα έξι γινομένων αν τους πάρουμε ανά δύο. Και με τον ίδιο τρόπο τα υπόλοιπα."

Συνεχίζει με το δεύτερο θεώρημά του το οποίο αφορά τα συμμετρικά πολυώνυμα (αλλά περιέχει και το Θεμελιώδες Θεώρημα της Άλγεβρας):

Θεώρημα 1.2.3. *Όλες οι εξισώσεις της άλγεβρας δέχονται τόσες λύσεις όσες και η πιο μεγάλη ποσότητα (βαθμός του αγνώστου), εκτός από τις μη πλήρεις εξισώσεις. Η πρώτη τάξη των λύσεων ισούται με τον συντελεστή του όρου που έχει τον αμέσως μικρότερο βαθμό από τον μεγιστοβάθμιο, η δεύτερη τάξη με τον συντελεστή του αμέσως μικρότερου , κ.λ.π με τέτοιο όμως τρόπο ώστετα πρόσημα να διατάσσονται εναλλάξ.*

Όπως και με το προηγούμενο θεώρημα, δεν το αποδεικνύει σύμφωνα με τη σύγχρονη πρακτική, αλλά εξηγεί την ουσία του θεωρήματος δίνοντας συγκεκριμένο παράδειγμα το οποίο αναφέρουμε με σύγχρονο συμβολισμό. Για την εξίσωση $x^4 = 4x^3 + 7x^2 - 34x + 24$ ο Girard αρχικά σημειώνει ότι έχει τέσσερις ρίζες εφόσον ο βαθμός του μέγιστου όρου είναι ο 4. Κατόπιν όπως λέει *"Για να δούμε τα πράγματα με την τελειότητά τους, πρέπει να πάρουμε τα πρόσημα με εναλλασσόμενη διάταξη"*, έτσι γράφει την εξίσωση με τη μορφή $x^4 - 7x^2 - 24 = 4x^3 - 34x$ και άρα οι αριθμοί $4, -7, -34, -24$ είναι οι τέσσερις τάξεις των λύσεων. Δηλαδή το 4 είναι

το άθροισμα των λύσεων, το -7 είναι το άθροισμα των γινομένων των ζευγών των λύσεων, το -34 είναι το άθροισμα των γινομένων των τριάδων των λύσεων και το -24 είναι το γινόμενο των τεσσάρων λύσεων. Προχωράει όμως και στην περίπτωση εξίσωσης όπως η $x^4 = 4x - 3$ η οποία έχει και μιγαδικές ρίζες, ή *αδύνατες* όπως τις χαρακτηρίζει ο Girard, και δείχνει ότι το θεώρημά του ισχύει και σ'αυτήν την περίπτωση. Ο Girard προχωρώντας τη μελέτη του φτάνει μάλλον τυχαία στην ανακάλυψη των αθροισμάτων των δυνάμεων των ριζών συναρτήσει των συντελεστών της εξίσωσης. Συγκεκριμένα αναφέρει ότι αν κάποιος χάριν απλότητας στα παραπάνω θεωρήματα αντί για άθροισμα ριζών, άθροισμα γινομένων των ριζών ανά δύο, άθροισμα γινομένων των ριζών ανά τρεις, κ.λ.π, πει άθροισμα ριζών, άθροισμα τετραγώνων των ριζών, άθροισμα κύβων των ριζών, κ.λ.π τότε θα κάνει λάθος. Για να δείξει ότι οι εκφράσεις αυτές αντιπροσωπεύουν διαφορετικές ποσότητες αναφέρει ότι:

$$\text{Έστω} \begin{cases} A & \text{ο συντελεστής του δεύτερου (σε βαθμό) όρου} \\ B & \text{ο συντελεστής του τρίτου όρου} \\ \Gamma & \text{ο συντελεστής του τέταρτου όρου} \\ \text{κ.λ.π.} & \end{cases}$$

τότε για κάθε βαθμού εξίσωση τα αθροίσματα

$$\text{είναι ίσα με:} \begin{cases} A & \text{των ριζών} \\ A^2 - 2B & \text{των τετραγώνων} \\ A^3 - 3AB + 3\Gamma & \text{των κύβων} \\ A^4 - 4A^2B + 4A\Gamma + 2B^2 - 4\Delta & \text{στην τέταρτη δύναμη} \end{cases}$$

δίνοντας στη συνέχεια ως παράδειγμα την εξίσωση $x^4 + 35x^2 + 24 = 10x^3 + 50x$ με άθροισμα ριζών ίσο με 10 αφού αυτές είναι οι $1, 2, 3, 4$, κατόπιν υπολογίζοντας βρίσκει $A^2 - 2B = 10^2 - 2 \cdot 35 = 30$ το άθροισμα των τετραγώνων των ριζών: $1^2 + 2^2 + 3^2 + 4^2 = 30$ και ούτω καθεξής.

Όπως συμβαίνει καμιά φορά στην Ιστορία της Επιστήμης, ο άνθρωπος που κάνει γνωστή μια ανακάλυψη λόγω πιο πρόσφορων συνθηκών ή λόγω του επιστημονικού του κύρους, έχει και την τιμή να δοθεί το όνομά του στην ανακάλυψη αυτή ακόμα και αν αυτή έχει γίνει από κάποιον προγενέστερό του. Κάπως έτσι συνέβη και με την περίπτωση του Girard όσον αφορά το θεώρημα για τα συμμετρικά πολυώνυμα. Έτσι το αποτέλεσμα που μόλις αναφέραμε είναι γνωστό

σε μας σήμερα ως Θεώρημα του Newton για τα συμμετρικά πολυώνυμα.

Newton

Σχεδόν έναν αιώνα μετά την εργασία του Girard, το 1707 εκδόθηκε το *Arithmetica Universalis* από τον ήδη αναγνωρισμένο τότε στην επιστημονική κοινότητα Isaac Newton. Ο Newton αποσκοπούσε[11] στον προσδιορισμό των συνθηκών ώστε δύο τριτοβάθμιες πολυωνυμικές εξισώσεις να έχουν τις ίδιες ρίζες. Παίρνοντας μια τριτοβάθμια εξίσωση

$$x^3 + bx^2 + cx + d = 0 \text{ με ρίζες } t_i,\ i = 1, 2, 3$$

χωρίς να αναφέρει τη διαδικασια που ακολούθησε καταλήγει σε δεκαεννέα σχέσεις στις οποίες συσχετίζει δυνάμεις των ριζών της εξίσωσης με τους συντελεστές της:

$$\sum_{i=1}^{3} t_i = -b\ ,\ \sum_{i=1}^{3} {t_i}^2 = b^2 - 2c\ ,\ \sum_{i=1}^{3} {t_i}^3 = -b^3 + 3bc - 3d\ ,\quad \cdots$$

$$\cdots\quad ,\ \cdots\quad ,\ \sum_{\substack{i,j,k=1\\ i\neq j\neq k}}^{3} {t_i}^3 {t_j}^3 {t_k}^2 = cd^2\ ,\quad \prod_{i=1}^{3} {t_i}^3 = -d^3$$

Σε άλλες σημειώσεις του εκφράζει παρόμοιους τύπους για τις ρίζες ενός πολυωνύμου $8^{ου}$ βαθμού, γεγονός που σημαίνει πως ο Newton γνώριζε ότι μπορούν να βρεθούν τέτοιοι τύποι για κάθε βαθμού πολυωνυμική εξισωση. Είναι πιθανόν όμως, όπως σημειώνει ο Whiteside πως δεν γνώριζε την ύπαρξη της εργασίας του Girard κι έτσι η ανακάλυψη του θεωρήματος από τον Newton θεωρείται ανεξάρτητη. Ο τρόπος με τον οποίο διατυπώνει το θεώρημά του στο *Arithmetica Universalis* είναι ο έξης:

Θεώρημα 1.2.4. *Ας υποθέσουμε ότι οι γνωστές ποσότητες των όρων κάθε εξίσωσης, μετά την κατάλληλη αλλαγή των προσήμων, ότι είναι p,q,r,s,t,v δηλαδη του δεύτερου όρου το p, του τρίτου το q, του τέταρτου το r, του πέμπτου το s, και ούτω καθεξής. Αν τα προσέξουμε ώστε να έχουμε τα σωστά πρόσημα τότε έχουμε* $p = a$, $pa + 2q = b$, $pb + qa + 3r = c$, $pc + qb + ra + 4s = d$, $pd + qc + rb + ca + 5t = e$ *κ.λ.π. ως σειρές προόδων. Όπου το a είναι το άθροισμα των ριζών, το b*

[11]σύμφωνα με τον Derek Whiteside που μελέτησε και εξέδωσε τα ανέκδοτα χειρόγραφα του Newton (όπως αναφέρεται στο [11])

είναι το άθροισμα των τετραγώνων των ριζών, το c είναι το άθροισμα των κύβων, το d είναι το άθροισμα των τετάρτων δυνάμεων κ.λ.π.

Ο Newton δεν αναφέρει στο έργο του αυτό, ούτε πως οδηγήθηκε σ'αυτό το συμπέρασμα, ούτε όμως δίνει κάποια απόδειξή του.

Οι Μαθηματικοί των επόμενων ετών διαδέχθηκαν τον Newton στην αναζήτηση αυτή και ενδιαφέρθηκαν για την απόδειξη και τη εύρεση και άλλων σχέσεων συμμετρικών πολυωνύμων. Ανάμεσα σ'αυτούς συγκαταλέγονται ο Maclaurin, ο Euler, ο Edward Waring στο *Meditationes Algebraicae* το 1770, ο Vandermonde στο *Mémoire sur la résolution des équations*, ο Lagrange στο *Traité de la Résolution des Equations Numériques de tous les Degrés* το 1798 , και άλλοι. Ιδιάιτερη αναφορά ωστόσο ίσως πρέπει να γίνει στον Meyer Hirsch ο οποίος στην Άλγεβρά του το 1809, αφού αποδείξει με διάφορους τρόπους τους τύπους του Newton για συμμετρικές συναρτήσεις, δίνει πρώτη φορά τη σύγχρονη γενική διατύπωση του θεωρήματος με μια απόδειξη του και τους πρώτους πιο γνωστούς πίνακες συμμετρικών συναρτήσεων που προέρχονται από πολυωνυμικές εξισώσεις μέχρι και $10^{ου}$ βαθμού.

1.3 Κυκλοτομικά πολυώνυμα

Ένα πολυώνυμο της μορφής $x^n - 1 = 0$, ονομάζεται κυκλοτομικό πολυώνυμο επειδή όπως προκύπτει από τον τύπο του de Moivre

$$(\cos\alpha + i\cdot\sin\alpha)^n = \cos n\alpha + i\cdot\sin n\alpha$$

οι n το πλήθος ρίζες του έχουν συντεταγμένες $(cos\frac{2\pi k}{n}, \sin\frac{2\pi k}{n})$ όπου $k = 0, \cdots, n-1$ και βρίσκονται στις κορυφές ενός κανονικού n-γώνου εγγεγραμμένου στον μοναδιαίο κύκλο. Η σημασία των κυκλοτομικών πολυωνύμων για την εξέλιξη της θεωρίας Galois βρίσκεται σε δύο κυρίως σημεία:

- αν γνωρίζουμε μια ν-στη ρίζα u, κάποιου μιγαδικού αριθμού z, τότε μέσω των ν-στων ριζών ω_i της μονάδας μπορούμε να προσδιορίζουμε και τις υπόλοιπες ρίζες του αφού ισχύει ότι:

$$(\omega_i u)^\nu = \omega_i^\nu u^\nu = 1\cdot u^\nu = z$$

- τα κυκλοτομικά πολυώνυμα ήταν τα πρώτα πολυώνυμα για τα οποία δόθηκε μια γενική (για οποιοδήποτε βαθμό) λύση με ριζικά. Οι μέθοδοι αντιμετώπισής τους μάλιστα περιείχαν ιδέες οι οποίες χρησιμοποιήθηκαν ύστερα και από τον Galois στην ανάπτυξη της θεωρίας του.

Euler

Σύμφωνα με τον Neumann [26], ο πρώτος που έδωσε λύσεις με ριζικά στο κυκλοτομικό πολυώνυμο $x^n - 1 = 0$ ήταν ο Ελβετός Leonhard Euler[12], ο οποίος αντιμετώπισε ξεχωριστά κάθε περίπτωση για $1 \leq n \leq 10$. Δεν κατάφερε να συνεχίσει για $n = 11$ λέγοντας:

> "Πράγματι, οι έντεκα ρίζες της εξίσωσης $x^{11} - 1 = 0$ δεν μπορούν να υπολογιστούν μέσω της βοηθητικής εξίσωσης αφού αυτή είναι πεμπτοβάθμια, εφόσον η λύση της είναι κρυφή μέχρι τώρα θα πρέπει να σταματήσουμε εδώ."

Για να δούμε πως εργάστηκε ο Euler θα μελετήσουμε την περίπτωση $x^5 - 1 = 0$. Μία προφανής ριζα είναι το $x = 1$, έτσι παραγοντοποιώντας έχουμε τη σχέση $x^5 - 1 = (x-1)(x^4 + x^3 + x^2 + x + 1)$. Επομένως πρέπει να λυθεί η εξίσωση $x^4 + x^3 + x^2 + x + 1 = 0$ η οποία είναι μια αντίστροφη εξίσωση. Θέτοντας $u = -(x + x^{-1})$ παίρνουμε, μετά από ύψωση στο τετράγωνο, $u^2 - 2 = x^2 + x^{-2}$. Προσθέτοντας κατά μέλη βρίσκουμε την δευτεροβάθμια εξίσωση $u^2 - u - 1 = 0$ με ρίζες: $p = \frac{1+\sqrt{5}}{2}$ και $q = \frac{1-\sqrt{5}}{2}$. Άρα οι υπόλοιπες τέσσερις ρίζες της μονάδας υπολογίζονται από τις εξισώσεις $x^2 + px + 1 = 0$ και $x^2 + qx + 1 = 0$. Προκύπτει ότι οι ρίζες αυτές είναι ρητές συναρτήσεις των $\sqrt{5}$ και $\sqrt{-10 + 2\sqrt{5}}$. Ειδικότερα έχουμε:

$$x = \frac{1}{4}\left[-1 - \delta_1\sqrt{5} + \delta_2\sqrt{-10 - \delta_1 2\sqrt{5}}\right] \text{ με } \delta_{1,2} = \pm 1$$

Vandermonde

Ο Alexandre-Théophile Vandermonde στην εργασία που παρουσίασε στην Ακαδημία των Παρισίων το Νοέμβριο του 1770 με τίτλο *Mémoire sur la résolution des équations*, ξεπέρασε τη δυσκολία επίλυσης της κυκλοτομικής εξίσωσης $x^{11} - 1 = 0$ χρησιμοποιώντας τις λεγόμενες επιλύουσες Vandermonde (ή Lagrange).

Και στην εξίσωση $x^{11} - 1 = 0$, μία προφανής ρίζα είναι το $x = 1$, έτσι παραγοντοποιώντας έχουμε τη σχέση

$$x^{11} - 1 = (x-1)(x^{10} + x^9 \cdots + x^3 + x^2 + x + 1)$$

Επομένως για τις υπόλοιπες ρίζες πρέπει να λυθεί η εξίσωση

$$x^{10} + x^9 \cdots + x^2 + x + 1 = 0 \tag{1.9}$$

[12]κατά τον Tignol[36] οι περιπτώσεις αυτές μελετήθηκαν από τον de Moivre

η οποία είναι μια αντίστροφη εξίσωση. Ο Vandermonde όπως και παρπάνω ο Euler έθεσε $u = -(x + x^{-1})$ και κατέληξε στην βοηθητική πεμπτοβάθμια εξίσωση

$$x^5 - x^4 - 4x^3 + 3x^2 + 3x - 1 = 0 \tag{1.10}$$

Επειδή όμως οι ρίζες της (1.9) είναι οι ενδέκατες ρίζες της μονάδας δηλαδή $x_k = e^{\frac{2k\pi i}{11}}$ όπου $k = 1, \cdots, 10$ συμπεραίνουμε ότι οι πέντε ρίζες της εξίσωσης (1.10) θα είναι οι $u_k = -\left(e^{\frac{2k\pi i}{11}} + e^{-\frac{2k\pi i}{11}}\right) = -2\cos\frac{2k\pi}{11}$ όπου $k = 1, \cdots, 5$
Ο Vandermonde χρησιμοποιώντας τον τριγωνομετρικό τύπο:

$$2\cos\alpha\cos\beta = \cos(\alpha + \beta) + \cos(\alpha - \beta)$$

κατάφερε να γράψει όλες τις σχέσεις μεταξύ των ριζών. Για παράδειγμα αντικαθιστώντας όπου $\alpha = \beta = \frac{2\pi}{11}$ πήρε τη σχέση

$$2\cos^2\frac{2\pi}{11} = \cos\frac{4\pi}{11} + \cos 0$$

δηλαδή την

$$u_1^2 = -u_2 + 2$$

Εν συνεχεία αντικαθιστώντας όπου $\alpha = \frac{2\pi}{11}$ και $\beta = \frac{4\pi}{11}$ βρήκε τη σχέση

$$2\cos\frac{2\pi}{11}\cos\frac{4\pi}{11} = \cos\frac{6\pi}{11} + \cos\frac{-2\pi}{11}$$

δηλαδή την

$$u_1u_2 = -u_3 - u_1$$

Συνεχίζοντας με αυτόν τον τρόπο κατέληξε σε μια σειρά από σχέσεις για όλες τις ρίζες της εξίσωσης (1.10):

$$u_1^2 = -u_2 + 2,\ u_2^2 = -u_4 + 2,\ u_3^2 = -u_5 + 2,\ u_4^2 = -u_3 + 2,\ u_5^2 = -u_1 + 2 \tag{1.11}$$

$$u_1u_2 = -u_3 - u_1,\ u_2u_3 = -u_1 - u_5,\ u_3u_4 = -u_1 - u_4,\ u_4u_5 = -u_1 - u_2 \tag{1.12}$$

$$u_1u_3 = -u_2 - u_4,\ u_2u_4 = -u_2 - u_5,\ u_3u_5 = -u_2 - u_3 \tag{1.13}$$

$$u_1u_4 = -u_3 - u_5,\ u_2u_5 = -u_3 - u_4 \tag{1.14}$$

$$u_1u_5 = -u_4 - u_5 \tag{1.15}$$

$$u_1 + u_2 + u_3 + u_4 + u_5 - 1 = 0 \tag{1.16}$$

Ο Vandermonde έκανε την βασική για τη συνέχεια παρατήρηση ότι οι παραπάνω σχέσεις μετατίθενται μεταξύ τους αν εφαρμόσουμε την κυκλική μετάθεση $(12435) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 4 & 3 & 5 \end{pmatrix}$ στους δείκτες k των ριζών u_k. Για παράδειγμα η σχέση $u_1^2 = -u_2 + 2$ γίνεται $u_2^2 = -u_4 + 2$ η οποία είναι επίσης αληθής.
Ο Vandermonde στην εργασία που προαναφέραμε, προσεγγίζει τη λύση των πολυωνυμικών εξισώσεων n-στου βαθμού με τη σχέση

$$x = \frac{1}{n}\left[(x_1 + \cdots + x_n) + \sqrt[n]{(\Delta^{(1)})^n} + \cdots + \sqrt[n]{(\Delta^{(n-1)})^n}\right]$$

όπου $\Delta^{(i)} = \rho_1^i x_1 + \cdots + \rho_n^i x_n$, $1 \leq i \leq n$ οι επιλύουσες Vandermonde (ή Lagrange) αν $\rho_1, \cdots, \rho_n$ είναι οι n-στες ρίζες της μονάδας.
Έτσι ειδικότερα για την περίπτωση της εξίσωσης (1.9), ύστερα από μακροσκελής αλλά σαφείς υπολογισμούς, παρατηρεί ότι οι επιλύουσες $\Delta^{(i)}$ είναι γραμμικοί συνδυασμοί των 5-ων ριζών της μονάδας και μέσω των σχέσεων (1.11) έως (1.16) παραμένουν αναλλοίωτες κάτω από την κυκλική μετάθεση (12435). Καταλήγει στην εύρεση των λύσεων με ριζικά από την σχέση

$$x = \frac{1}{5}\left[1 + \sqrt[5]{(\Delta^{(1)})^5} + \sqrt[5]{(\Delta^{(2)})^5} + \sqrt[5]{(\Delta^{(3)})^5} + \sqrt[5]{(\Delta^{(4)})^5}\right]$$

στην οποία περιέχονται η $\sqrt{5}$, άλλες τετραγωνικές ρίζες, ρίζες πέμπτης τάξης και οι πέμπτες ρίζες της μονάδας.

Ο Vandermonde δεν προχώρησε στην επίλυση περιπτώσεων κυκλοτομικών εξισώσεων μεγαλύτερου του ενδεκάτου βαθμού, αλλά αρκέστηκε μόνο να σημειώσει ότι χρειάζεται να βρίσκουμε κάθε φορά την ποσότητα που μένει αμετάβλητη για κάθε μια από τις ρίζες.

Gauss

Τελικά ο Γερμανός Carl Friedrich Gauss στο μνημειώδες έργο του *Disquisitiones arithmeticae* που εξέδωσε το 1801, παρουσίασε μια πλήρως ανεπτυγμένη θεωρία για την επίλυση των κυκλοτομικών πολυωνύμων με ριζικά, βασισμένη αποκλειστικά στη Θεωρία Αριθμών και ειδικότερα σε ισοϋπόλοιπα ($\bmod p$) πρώτων αριθμών, χωρίς να κάνει καμία αναφορά σε προηγούμενες εργασίες που ασχολούνται με το ίδιο θέμα από αλγεβρική σκοπιά.[13] Η συμβολή του

[13]αναφορές από τα [20] και [27]

Gauss στην εξέλιξη της θεωρίας των εξισώσεων, πέρα από τη γενική λύση με ριζικά μιας μορφής πολυωνυμικών εξισώσεων (των κυκλοτομικών), βρίσκεται στην ανάδειξη του ρόλου της αναγωγιμότητας των πολυωνύμων, δηλαδή στη μελέτη εκείνων των πολυωνύμων που δεν μπορούν να παραγοντοποιηθούν σε γινόμενα πολυωνύμων μικρότερου βαθμού. Ξεκινάει λοιπόν τη μελέτη του για τα κυκλοτομικά πολυώνυμα

$$X = \frac{x^n - 1}{x - 1} = x^{n-1} + \cdots + x + 1$$

με n περιττό πρώτο αριθμό αποδεικνύοντας με αυστηρότητα ότι το πολυώνυμο X είναι ανάγωγο στο σώμα $\mathbb{Q}$ των ρητών αριθμών. Αυτό το πετυχαίνει με τη χρήση του "Λήμματος Gauss" σύμφωνα με το οποίο η παραγοντοποίηση στους ρητούς περιορίζεται στην παραγοντοποίηση στο σώμα των ακεραίων. Στη συνέχεια ο Gauss επιχειρεί να αναλύσει την εξίσωση X σε όσο δυνατόν μικρότερης τάξης παράγοντες. Χρησιμοποιεί ένα Λήμμα που έχει ήδη αποδείξει: "υπάρχουν πάντοτε αριθμοί g τέτοιοι ώστε οι δυνάμεις $1 = g^0, g, \cdots, g^{n-2} \mod n$ να εξαντλούν όλες τις πρώτες κλάσεις υπολοίπων $\mod n$." Οι αριθμοί g ονομάζονται πρωταρχικές ρίζες $\mod n$. Για κάθε ανάλυση σε γινόμενο $n - 1 = f \cdot e$ ο Gauss σχηματίζει τις λεγόμενες περιόδους με f όρους

$$\eta_i = \zeta^i + \zeta^{ih} + \cdots + \zeta^{ih^{f-1}} = \sum_{j=0}^{f-1} \zeta^{ih^j} \quad (0 \leq i \leq e - 1)$$

με $h = g^e$. Αυτά τα αθροίσματα είναι ανεξάρτητα από την εκλογή του g και ικανοποιούν μια εξίσωση με βαθμού e στο σώμα των ρητών στο οποίο είναι ανάγωγες. Επιπλέον οι περίοδοι $\eta_0, \cdots, \eta_{e-1}$ είναι ρητές συναρτήσεις μεταξύ τους με ρητούς συντελεστές και κάθε n-στη πρωταρχική ρίζα της μονάδας ικανοποιεί μια εξίσωση βαθμού f με συντελεστές ρητές συναρτήσεις οποιασδηποτε περιόδου με f όρους. Επαναλαμβάνοντας την ίδια διαδικασία περαιτέρω παραγοντοποίησης του f βρίσκει μια σειρά από βοηθητικές εξισώσεις. Ισχυρίζεται ότι αυτές οι εξισώσεις μπορούν να επιλυθούν λέγοντας ότι, αν για παράδειγμα έχουμε μια παραγοντοποίηση του $n - 1$ =αβγ με τρείς παράγοντες, τότε οι εξισώσεις β βαθμού των περιόδων με γ όρους μπορούν να επιλυθούν από ένα ριζικό β τάξης, εφόσον οι περίοδοι με βγ όρους και οι β-στες ρίζες της μονάδας θεωρηθούν γνωστές. Ο Gauss δίνει μόνο ένα σχεδιάγραμμα της

απόδειξης του ισχυρισμού του χρησιμοποιώντας ως κύριο εργαλείο τα *"αθροίσματα Gauss"*:

$$(\zeta, \alpha^i) = \zeta + \alpha^i \cdot \zeta^g + \alpha^{2i} \cdot \zeta^{g^2} + \cdots + \alpha^{(n-2)i} \cdot \zeta^{g^{n-2}}$$

τα οποία στην ουσία είναι επιλύουσες του Lagrange (ή Vandermonde). Η διαφορά στο χειρισμό τους όμως σε σχέση με τον Lagrange είναι ότι αντί να χρησιμοποιήσει όλες τις μεταθέσεις των ριζών, αρκείται στο να πολλαπλασιάσει κάθε τέτοια σχέση με μία μόνο ρίζα ή με ένα άθροισμά τους, το οποίο βέβαια πάλι πραγματοποιεί μια μετάθεση.[14]

1.4 Θεμελιώδες Θεώρημα της Άλγεβρας

1.4.1 Ιστορική αναφορά

Το Θεμελιώδες Θεώρημα της Άλγεβρας λέει ότι κάθε πολυώνυμο ν-στου βαθμού έχει ν ρίζες.[15] Ο χαρακτηρισμός του θεωρήματος ως θεμελιώδες για την Άλγεβρα δικαιολογείται από το γεγονός ότι την εποχή που του δόθηκε, η Άλγεβρα ήταν συνώνυμη με την επίλυση πολυωνυμικών εξισώσεων με πραγματικούς ή μιγαδικούς συντελεστές, σε αντίθεση με τη σύγχρονη θεώρηση της αφηρημένης Άλγεβρας ως μελέτης των δομών.

Μέχρι τον 16ο αιώνα δεν γινόταν καμία σκεψη για την ύπαρξη ενός τέτοιου θεωρήματος αφού ούτε καν οι αρνητικοί αριθμοί δεν ήταν αποδεκτοί ως έγκυρες λύσεις. Η διαίσθηση ότι το Θεώρημα αυτό μπορεί να ισχύει, άρχισε να υπάρχει στους μαθηματικούς μετά από την δημοσίευση των τύπων για την επίλυση της τριτοβάθμιας και τεταρτοβάθμιας εξίσωσης από τον Cardano (και τον Ferrari) και κυρίως μετά την διαπίστωσή του ότι μπορούμε να χειριστούμε και ποσότητες πέρα από τους πραγματικούς αριθμούς για να καταλήξουμε σε αποδεκτά αποτελέσματα. Ο Bombelli ενίσχυσε αυτή την άποψη με τους κανόνες που διατύπωσε στην Άλγεβρά του για τις πράξεις μεταξύ των ποσοτήτων αυτών. Ο Peter Roth στο βιβλίο του *Arithmetica Philosophica* που εκδόθηκε το 1608 ισχυρίζεται ότι μια πολυωνυμική εξίσωση ν-στου βαθμού μπορεί να έχει το πολύ ν ρίζες.

Η πρώτη διατύπωση του Θεμελιώδους Θεωρήματος της Άλγεβρας με τη μορφή που το γνωρίζουμε σήμερα, ότι δηλαδή υπάρχουν

[14]μια πιο αναλυτική παρουσίαση της θεωρίας του Gauss στα κυκλοτομικά πολυώνυμα βρίσκεται στο [36, Κεφ.12]

[15]Στη συνέχεια θα διατυπώσουμε και άλλες ισοδύναμες και πιο ακριβείς διατυπώσεις του θεωρήματος. Αναφορές από τα [10] και [15]

II. Theoreme.

Toutes les equations d'algebre reçoivent autant de ſolutions, que la denomination de la plus haute quantité le demonſtre, excepté les incomplettes: & la premiere faction des ſolutions eſt eſgale au nombre du premier meſlé, la ſeconde faction des meſmes, eſt eſgale au nombre du deuxieſme meſlé; la troiſieſme, au troiſieſme, & tousjours ainſi, tellement que la derniere faction eſt eſgale à la fermeture, & ce ſelon les ſignes qui ſe peuvent remarquer en l'ordre alternatif.

Εικόνα 1.7: Η διατύπωση του Θεμελιώδους Θεωρήματος της Άλγεβρας από τον Albert Girard στο έργο του *Invention Nouvelle en l'Algèbre.*

ακριβώς ν ρίζες, έγινε το 1629 από τον Albert Girard στο έργο του *Invention Nouvelle en l'Algèbre* όπου αναφέρει: *"Όλες οι εξισώσεις της Άλγεβρας δέχονται τόσες λύσεις, όσες δείχνει και ο δείκτης της πιο μεγάλης ποσότητας, εκτός αυτών που είναι ελλιπείς.* (βλέπε Εικόνα 1.7) Δεν ισχυρίζεται όμως ότι οι λύσεις είναι αποκλειστικά της μορφής $x + yi$, αφήνοντας ανοικτό το ενδεχόμενο να είναι και πέρα από το σύνολο των μιγαδικών αριθμών. Ο Girard δεν δίνει κάποια απόδειξη του θεωρήματος που διατυπώνει αλλά αναφέρει παραδείγματα εξισώσεων για τις οποίες αυτό ισχύει. Ο Descartes το 1637 στο τρίτο και τελευταίο βιβλίο της: *La géométrie* κάνει μια σύντομη περίληψη στα μέχρι τότε γνωστά αποτελέσματα σχετικά με τις εξισώσεις. Εκεί αναφέρει ότι μπορούμε να "φανταστούμε" ν ρίζες για κάθε εξισωση ν-στού βαθμού, αλλά αυτές δεν θα αντιστοιχούν σε κάποιες πραγματικές ποσότητες.

Το 1702 ο Leibniz, σε μια δημοσίευσή του στο *Acta Eruditorum*, που αφορούσε την μέθοδο ολοκλήρωσης ρητών παραστάσεων μέσω απλών κλασμάτων, ισχυρίστηκε ότι το Θεμελιώδες Θεώρημα της Άλγεβρας δεν ισχύει εφόσον το γινόμενο δύο πρωτοβάθμιων πολυωνύμων με συντελεστές από το σώμα των μιγαδικών, δεν δίνει πάντα ένα πολυώνυμο δευτέρου βαθμού με πραγματικούς συντελεστές. Για να αποδείξει τον ισχυρισμό του έδωσε το παρακάτω παράδειγμα παραγοντοποίησης:

$$x^4 + a^4 = (x^2 - a^2 i)(x^2 + a^2 i) = (x + a\sqrt{i})(x - a\sqrt{i})(x + a\sqrt{-i})(x - a\sqrt{-i})$$

Η αδυναμία του Leibniz βρίσκεται στο ότι δεν παρατήρησε πως το γινόμενο του πρώτου και του τρίτου παράγοντα, όπως και το

γινόμενο του δεύτερου με τον τέταρτο δίνουν:

$$(x^2 + a\sqrt{2}x + a^2)(x^2 - a\sqrt{2}x + a^2) = x^4 + a^4$$

δηλαδή πολυώνυμα δευτέρου βαθμού με πραγματικούς συντελεστές. Αν και το λάθος εντοπίστηκε αργότερα από άλλους μαθηματικούς όπως ο Jean(I) Bernoulli, ο Jacob Hermann, ο Roger Cotes, παρ' όλα αυτά για τους μαθηματικούς η ισχύς του Θεωρήματος δεν ήταν ακόμα δεδομένη, εφόσον εξακολουθούσε να λείπει μια έγκυρη απόδειξη. Η διαπίστωση αυτή γίνεται φανερή από την αλληλογραφια μεταξύ των Euler, Nicolas(I) Bernoulli και Christian Goldbach όπου γίνεται λόγος ακριβώς για αυτό το θέμα. Ο Nicolas Bernoulli για να ενισχύσει τον ισχυρισμό του Leibniz δίνει το δικό του "αντιπαράδειγμα", το πολυώνυμο: $x^4 - 4x^3 + 2x^2 + 4x + 4$ με ρίζες

$$x_{1,2} = 1 \pm \sqrt{2 + i\sqrt{3}}\,,\ x_{3,4} = 1 \pm \sqrt{2 - i\sqrt{3}}$$

Όμως κι εδώ ο Euler εντοπίζει το λάθος απαντώντας ότι πολλαπλασιάζοντας μεταξύ τους τους παράγοντες που περιέχουν την πρώτη και τρίτη ρίζα παίρνουμε

$$(x - x_1)(x - x_3) = \left(x^2 - \left(2 + \sqrt{4 + 2\sqrt{7}}\right)x + 1 + \sqrt{7} + \sqrt{4 + 2\sqrt{7}}\right)$$

και αντίστοιχα αυτούς με την δεύτερη και τέταρτη

$$(x - x_2)(x - x_4) = \left(x^2 - \left(2 + \sqrt{4 + 2\sqrt{7}}\right)x + 1 + \sqrt{7} + \sqrt{4 + 2\sqrt{7}}\right)$$

δηλαδή δευτεροβάθμια πολυώνυμα με πραγματικούς συντελεστές. Ο Euler καταφέρνει να αποδείξει το Θεμελιώδες Θεώρημα της Άλγεβρας για πολυώνυμα μέχρι και 6ου βαθμού, αλλά αποτυγχάνει να αποδείξει την γενική περίπτωση αφού η προσπάθειά του που δημοσιεύτηκε το 1749 με τίτλο *Recherches sur les racines imaginaires des équations* περιέχει ελλείψεις όπως διαπιστώνει αργότερα, το 1772, ο Lagrange ο οποίος προσπαθεί να καλύψει τα κενά. Άλλοι που προσπάθησαν να αποδείξουν το Θεώρημα ήταν ο de Foncenex (1759) και ο Laplace (1795). Και οι τέσσερις τους, σύμφωνα με την κριτική του Gauss, έκαναν το σφάλμα της a priori ύπαρξης των ριζών του πολυωνύμου και στην απόδειξή τους έδειχναν μόνο ότι αυτές ήταν της μορφής $x + yi$.

Τρία χρόνια πριν την προσπάθεια του Euler, το 1746, προηγήθηκε αυτή του Jean Le Rond d'Alembert με τίτλο *Recherches sur le calcul*

intégral που παρουσιάστηκε στην Ακαδημία του Βερολίνου. Αυτή ήταν η πρώτη προσπάθεια που έγινε για να αποδειχθεί το Θεμελιώδες Θεώρημα της Άλγεβρας. Όμως όπως διαπίστωσε ο Gauss αργότερα και αυτή περιείχε κενά, αλλά η ιδέα της απόδειξης δεν επηρεάζεται και μπορεί να χρησιμοποιηθεί για μια πλήρης απόδειξη. Οι βασικές παραλείψεις στην απόδειξη του d'Alembert ήταν δύο. Πρώτον, χρησιμοποιεί ένα λήμμα που αποδείχθηκε πολύ αργότερα (το 1851) από τον Victor Puiseux, όμως η απόδειξη του χρησιμοποιεί το Θεμελιώδες Θεώρημα της Άλγεβρας. Και δεύτερον, στην εποχή του δεν υπήρχαν οι απαραίτητες γνώσεις σχετικές με την πυκνότητα των πραγματικών ώστε να καταλήξει στην απαραίτητη για την απόδειξη σύγκλιση.

Τελικά ο Gauss ήταν αυτός ο οποίος έδωσε την αυστηρή απόδειξη και μάλιστα όχι μία αλλά τέσσερις. Η πρώτη απόδειξη παρουσιάστηκε στη διδακτορική διατριβή του, που υπέβαλλε το 1799, όταν ήταν 22 ετών, με τον κάπως μακροσκελή τίτλο: *"Demonstratio nova altera theorematis omnem functionem algebraicam rationalem integram unius variabilis in factores reales primi vel secundi gradus resolvi posse."*[16]. Ξεκινάει τη διατριβή του με μια λεπτομερή κριτική εξέταση όλων των προηγούμενων προσπαθειών για την απόδειξη του θεωρήματος. Η βασική διαφορά της απόδειξης του Gauss από τις προηγούμενες ήταν ότι αντί να προσπαθήσει να υπολογίσει μια ρίζα, αποδείκνυε την ύπαρξή της με επιχειρήματα τοπολογικής φύσης. Με τα σημερινά κριτήρια και αυτή η απόδειξη είχε ένα τοπολογικό κενό, το οποίο συμπλήρωσε το 1920 ο Alexander Ostrowski. Το 1816 ο Gauss έδωσε μια δεύτερη απόδειξη η οποία είναι σχεδόν εξ' ολοκλήρου αλγεβρική. Η μόνη πρόταση που δανείζεται από την Ανάλυση είναι ότι κάθε πραγματικό πολυώνυμο περιττού βαθμού έχει πάντοτε τουλάχιστον μια πραγματική ρίζα. Η απόδειξη αυτή αν και υπερβολικά τεχνική, είναι ακόμα και με τα σημερινά στάνταρντς, απόλυτα ορθή. Την ίδια χρονιά δημοσίευσε και την τρίτη, κατά χρονολογική σειρά, απόδειξη του ίδιου θεωρήματος τοπολογικής πάλι φύσης. Η τέταρτη και τελευταία απόδειξη που έδωσε ο Gauss στο Θεμελιώδες Θεώρημα της Άλγεβρας ήταν λίγα χρόνια πριν το θάνατό του, το 1849, η οποία ήταν παραλλαγή της πρώτης, αλλά η υπόθεση του θεωρήματος τώρα ήταν ότι το πολυώνυμο έχει μιγαδικούς συντελεστές και όχι μόνο πραγματικούς. Σ' αυτή την εργασία ήταν και η πρώτη φορά που το θεώρημα εμφανίστηκε με την ονομασία που διατηρεί μέχρι και

[16] *"Μια νέα απόδειξη του θεωρήματος ότι κάθε ακέραια ρητή αλγεβρική συνάρτηση μπορεί να αναλυθεί σε πραγματικούς παράγοντες πρώτου ή δευτέρου βαθμού."*

σήμερα ως: "Θεμελιώδες Θεώρημα της Άλγεβρας".

1.4.2 Απόδειξη

Το Θεμελιώδες Θεώρημα της Άλγεβρας συναντάται στη βιβλιογραφία με διαφορετικές διατυπώσεις, που όμως είναι ισοδύναμες μεταξύ τους. Οι παρακάτω προτάσεις είναι κάποιες από αυτές.

1. Κάθε μη σταθερό πολυώνυμο με μιγαδικούς συντελεστές έχει τουλάχιστον μία μιγαδική ρίζα.

2. Κάθε μη σταθερό πολυώνυμο με μιγαδικούς συντελεστές παραγοντοποιείται πλήρως (με πρωτοβάθμιους παράγοντες) στο σώμα των μιγαδικών αριθμών.

3. Κάθε μη σταθερό πολυώνυμο με μιγαδικούς συντελεστές ν βαθμού έχει ακριβώς ν μιγαδικές ρίζες (λαμβάνοντας υπ'όψιν την πολλαπλότητα κάθε ρίζας).

4. Το σώμα των μιγαδικών αριθμών είναι αλγεβρικά κλειστό.

Θα ήταν παράλογο να αναζητήσουμε μια καθαρά αλγεβρική απόδειξη του θεωρήματος, εφόσον οι πραγματικοί αριθμοί (και συνεπώς και οι μιγαδικοί αριθμοί) ορίζονται με βάση αναλυτικές έννοιες όπως οι ακολουθίες Cauchy, οι τομές Dedekind ή η πληρότητα της διάταξης. Η απόδειξη[17] που παραθέτουμε παρακάτω βασίζεται σε μια πρόταση γνωστή στη σχολική βιβλιογραφία ως θεώρημα του Bolzano. Πρώτα θα χρειαστεί να αποδείξουμε τέσσερα λήμματα και στη συνέχεια θα δοθεί η απόδειξη του Θεμελιώδους Θεωρήματος της Άλγεβρας.

Λήμμα 1.4.1. *Κάθε πολυώνυμο περιττού βαθμού με πραγματικούς συντελεστές έχει τουλάχιστον μία πραγματική ρίζα.*

Απόδειξη. Έστω πολυώνυμο $P(x) \in \mathbb{R}[x]$ βαθμού $n = 2k+1, k \in \mathbb{N}$ και ας υποθέσουμε ότι ο συντελεστής του μεγιστοβάθμιου όρου είναι θετικός, δηλαδή $a_n > 0$ (η απόδειξη είναι παρόμοια για $a_n < 0$). Τότε το πολυώνυμο γράφεται

$$P(x) = a_n x^n + (\text{μικρότερου βαθμού όροι})$$

[17]είναι μία από τις πολλές που υπάρχουν, βρίσκεται στο [13], στο [6] και στο [36]

όπου n περιττός. Οπότε έχουμε:

$$\lim_{x\to+\infty} P(x) = \lim_{x\to+\infty} a_n x^n = +\infty \quad \text{εφόσον} \quad a_n > 0 \tag{1.17}$$

$$\lim_{x\to-\infty} P(x) = \lim_{x\to-\infty} a_n x^n = -\infty \quad \text{εφόσον } a_n > 0 \text{ και n περιττός} \tag{1.18}$$

Λόγω της (1.17) το $P(x)$ παίρνει απείρως μεγάλες τιμές και έτσι υπάρχει x_1 ώστε $P(x_1) > 0$. Ομοίως λόγω της (1.18) το $P(x)$ παίρνει απείρως μικρές τιμές και έτσι υπάρχει x_2 ώστε $P(x_2) < 0$. Κάθε πολυώνυμο όμως με συντελεστές από το σώμα των πραγματικών αριθμών είναι συνεχής συνάρτηση σε όλο το $\mathbb{R}$. Εφόσον όμως ισχύει και ότι $P(x_1)P(x_2) < 0$, από το θεώρημα του Bolzano συμπεραίνουμε ότι υπάρχει $x_3 \in \mathbb{R}$ ανάμεσα στα x_1 και x_2 τέτοιο ώστε $P(x_3) = 0$. □

Λήμμα 1.4.2. *Κάθε πολυώνυμο δευτέρου βαθμού με μιγαδικούς συντελεστές έχει μιγαδικές ρίζες.*

Απόδειξη. Έστω το πολυώνυμο $P(x) = \alpha x^2 + \beta x + \gamma$. Οι ρίζες του είναι οι $x_{1,2} = \frac{-\beta\pm\sqrt{\beta^2-4\alpha\gamma}}{2\alpha}$. Όμως από τον τύπο του DeMoivre γνωρίζουμε ότι η τετραγωνική ρίζα κάθε μιγαδικού είναι μιγαδικός αριθμός. Συνεπώς $x_1, x_2 \in \mathbb{C}$. □

Λήμμα 1.4.3. *Αν κάθε μη σταθερό πολυώνυμο με πραγματικούς συντελεστές έχει τουλάχιστον μία μιγαδική ρίζα, τότε και κάθε μη σταθερό πολυώνυμο με μιγαδικούς συντελεστές έχει τουλάχιστον μία μιγαδική ρίζα.*

Απόδειξη. Έστω πολυώνυμο $P(x) \in \mathbb{C}[x]$ και υποθέτουμε ότι κάθε μη σταθερό πολυώνυμο με πραγματικούς συντελεστές έχει τουλάχιστον μία μιγαδική ρίζα. Αν συμβολίσουμε με $\overline{P}(x)$ το συζυγές πολυώνυμο του $P(x)$, ορίζουμε το πολυώνυμο $H(x) = P(x)\overline{P}(x)$. Τότε ισχύει

$$\overline{H}(x) = \overline{P(x)\overline{P}(x)} = \overline{P}(x)\overline{\overline{P}} = \overline{P}(x)P(x) = P(x)\overline{P}(x) = H(x)$$

Δηλαδή το $H(x)$ είναι πολυώνυμο με πραγματικούς συντελεστές και από την υπόθεση υπάρχει $z_0 \in \mathbb{C}$ τέτοιο ώστε $H(z_0) = 0 \Rightarrow P(x)\overline{P}(x) = 0$. Επειδή όμως το σώμα $\mathbb{C}$ είναι ακέραια περιοχή και δεν έχει διαιρέτες του μηδενός, θα ισχύει είτε $P(z_0) = 0$ οπότε αποδείχθηκε, είτε $\overline{P}(z_0) = 0$. Σ' αυτήν την περίπτωση

$$\overline{P}(z_0) = 0 \Rightarrow \overline{\overline{P}(z_0)} = \overline{0} \Rightarrow \overline{\overline{P}}(\overline{z_0}) = 0 \Rightarrow P(\overline{z_0}) = 0$$

που σημαίνει ότι ο μιγαδικός $\overline{z_0}$ είναι ρίζα του πολυωνύμου $P(x)$. □

Λήμμα 1.4.4. *Έστω πολυώνυμο $p(x) \in F[x]$ με ρίζες $\rho_1, \cdots, \rho_n$ που βρίσκονται σε ένα σώμα αναλύσεως $F'[x]$.*
Αν υποθέσουμε ότι το $g(x) = g(x, \rho_1, \cdots, \rho_n) \in F'[x]$ είναι συμμετρικό πολυώνυμο ως προς τις ρίζες $\rho_1, \cdots, \rho_n$ τότε $g(x) \in F[x]$.

Απόδειξη. Αν το $g(x) = g(x, \rho_1, \cdots, \rho_n)$ είναι συμμετρικό πολυώνυμο ως προς τις ρίζες $\rho_1, \cdots, \rho_n$ τότε σύμφωνα με το Θεμελιώδες Θεώρημα των συμμετρικών πολυωνύμων[18] μπορεί να γραφεί ως συμμετρικό πολυώνυμο συναρτήσει των στοιχειωδών συμμετρικών πολυωνύμων. Αυτά όμως , σύμφωνα με το Θεώρημα 1.2.3 του Newton για τα συμμετρικά πολυώνυμα , είναι και συντελεστές του $p(x)$, επομένως ανήκουν στο αρχικό σώμα F. Έτσι αφού οι συντελεστές του $g(x)$ ανήκουν στο F, τότε $g(x) \in F[x]$. □

Φτάνουμε τελικώς στην απόδειξη του θεωρήματος η οποία ακολουθεί μία στρατηγική που χρησιμοποίησε ο Euler μαζί με μια ιδέα του Laplace.

Θεώρημα 1.4.1 (Θεμελιώδες Θεώρημα της Άλγεβρας)**.** *Κάθε μη σταθερό πολυώνυμο με μιγαδικούς συντελεστές έχει τουλάχιστον μία μιγαδική ρίζα.*

Απόδειξη. Σύμφωνα με το προηγούμενο Λήμμα 1.4.3 αρκεί να δείξουμε ότι το πολυώνυμο

$$P(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{R}[x] \quad \text{με} \quad n \geq 1,\ a_n \neq 0$$

έχει τουλάχιστον μία μιγαδική ρίζα. Η στρατηγική του Euler είναι να εφαρμόσουμε τη μέθοδο της μαθηματικής επαγωγής πάνω στο βαθμό του πολυωνύμου.

Μπορούμε να γράψουμε το βαθμό n του πολυωνύμου με μοναδικό τρόπο ως $n = 2^m q$ όπου q περιττός. Εφαρμόζουμε επαγωγή στον m. Αν $m = 0$, τότε το $P(x)$ είναι περιττού βαθμού και το θεώρημα αποδείχτηκε σύμφωνα με το Λήμμα 1.4.1. Υποθέτουμε τώρα ότι το θεώρημα ισχύει για όλα τα πολυώνυμα βαθμού $d = 2^k q'$, όπου $k < m$ και q' περιττός. Θα δείξουμε ότι ισχύει και για το πολυώνυμο $P(x) \in \mathbb{R}[x]$ βαθμού $n = 2^m q$ όπου q περιττός. Έστω F' το σώμα αναλύσεως του $P(x)$ πάνω στο $\mathbb{R}[x]$ στο οποίο έχει ρίζες $\rho_1. \cdots, \rho_n$.[19]

[18]Κάθε συμμετρικό πολυώνυμο μπορεί να γραφεί ως πολυώνυμο των στοιχειωδών συμμετρικών πολυωνύμων.

[19]Η ύπαρξη του σώματος ανάλυσης αποδεικνύεται με επαγωγή στο Θεώρημα του Kronecker: *Κάθε πολυώνυμο $p(x) \in F[x]$ έχει μία ρίζα σε ένα σώμα επέκτασης $E \supset F$.*

Η έξυπνη ιδέα του Laplace ήταν για έναν $h \in \mathbb{Z}$ να σχηματίσουμε το πολυώνυμο

$$H(x) = \prod_{1 \leq i < j \leq n} (x - (\rho_i + \rho_j + h\rho_i\rho_j)) \quad \in F'[x]$$

Η ισότητα

$$x - (\rho_i + \rho_j + h\rho_i\rho_j) = x - (\rho_j + \rho_i + h\rho_j\rho_i)$$

δείχνει ότι το $H(x)$ είναι γινόμενο που καθορίζεται από ζεύγη ριζών και μένει αναλλοίωτο από τις μεταθέσεις τους. Έτσι για να σχηματίσουμε το $H(x)$ παίρνουμε ζεύγη ριζών (ρ_i, ρ_j), ούτως ώστε το πλήθος αυτών των ζευγών να ισούται με τον αριθμό των επιλογών δύο στοιχείων από $n = 2^m q$ στοιχεία. Το πλήθος αυτό είναι ίσο με

$$\frac{n(n-1)}{2} = \frac{(2^m q)(2^m q - 1)}{2} = 2^{m-1} q(2^m q - 1) = 2^{m-1} q'$$

με q' περιττό ως γινόμενο δύο περιττών. Επομένως ο βαθμός του $H(x)$ είναι $2^{m-1}q'$.

Το $H(x)$ είναι συμμετρικό πολυώνυμο των ριζών $\rho_1, \cdots, \rho_n$. Επειδή όμως αυτές είναι ρίζες πολυωνύμου με πραγματικούς συντελεστές, από το Λήμμα 1.4.4 κάθε πολυώνυμο συμμετρικό ως προς τις ρίζες του, στο σώμα αναλύσεώς του, έχει πραγματικούς συντελεστές. Επομένως $H(x) \in \mathbb{R}[x]$ με βαθμό $2^{m-1}q'$. Από τη υπόθεση της μαθηματικής επαγωγής, το $H(x)$ θα έχει μία μιγαδική ρίζα. Το οποίο σημαίνει πως, λόγω της κατασκευής του $H(x)$, υπάρχει ζεύγος (ρ_i, ρ_j) με

$$\rho_i + \rho_j + h\rho_i\rho_j \in \mathbb{C}$$

Εφόσον ο h είναι τυχαίος ακέραιος, για κάθε ακέραιο h_i θα πρέπει να υπάρχει τέτοιο ζεύγος (ρ_i, ρ_j) με

$$\rho_i + \rho_j + h_i\rho_i\rho_j \in \mathbb{C}$$

Ο h_i μεταβάλλεται στο σύνολο των ακεραίων. Επειδή όμως τα ζεύγη (ρ_i, ρ_j) είναι πεπερασμένα σε πλήθος θα πρέπει να υπάρχουν τουλάχιστον δύο διαφορετικοί ακέραιοι h_1, h_2 τέτοιοι ώστε

$$z_1 = \rho_i + \rho_j + h_1\rho_i\rho_j \in \mathbb{C} \text{ και } z_2 = \rho_i + \rho_j + h_2\rho_i\rho_j \in \mathbb{C}$$

Τότε $z_1 - z_2 = (h_1 - h_2)\rho_i\rho_j \in \mathbb{C}$ και αφού $h_1, h_2 \in \mathbb{Z} \subset \mathbb{C}$ συμπεραίνουμε ότι $\rho_i, \rho_j \in \mathbb{C}$ Όμως τότε και $h_1\rho_i\rho_j \in \mathbb{C}$, οπότε $\rho_i + \rho_j \in \mathbb{C}$. Έτσι το πολυώνυμο

$$p(x) = (x - \rho_i)(x - \rho_j) = x^2 - (\rho_i + \rho_j)x + \rho_i\rho_j \quad \in \mathbb{C}[x]$$

Το $p(x)$ όμως είναι ένα δευτεροβάθμιο πολυώνυμο κι έτσι από το Λήμμα 1.4.2 έχει μιγαδικές ρίζες οι οποίες εμφανώς είναι οι ρ_i και ρ_j. Οπότε $\rho_i, \rho_j \in \mathbb{C}$, δηλαδη και το αρχικό πολυώνυμο $P(x)$ έχει τουλάχιστον μία μιγαδική ρίζα. $\square$

2

Ομάδες

2.1 Ομάδα μεταθέσεων

Ο Galois δεν εισέβαλε από το πουθενά στον κόσμο των Μαθηματικών. Το έργο του, μπορεί να φαινόταν στους μαθηματικούς της εποχής του πρωτοπόρο και εκπληκτικό, όμως εκ των υστέρων μπορεί να θεωρηθεί ως το φυσικό, ίσως ακόμα και απαραίτητο, αποκορύφωμα αιώνων ανάπτυξης των ιδεών αυτών. Ο ίδιος ο Galois άλλωστε στις εργασίες του αναφέρει ονόματα μαθηματικών, των οποίων το έργο είχε μελετήσει, όπως τον Lagrange, τον Gauss και τον Abel.

2.1.1 Lagrange

Η έρευνα του Joseph Louis Lagrange[1] στην θεωρία των εξισώσεων μπορεί να χωριστεί σε δύο κατηγορίες[2]: η μία αφορά την αλγεβρική επίλυση πολυωνυμικών εξισώσεων με πράξεις μεταξύ των συντελεστών και των ριζών τους (δηλαδή την εύρεση ενός γενικού τύπου) και η άλλη αφορά τις τεχνικές για την αριθμητική επίλυση συγκεκριμένων εξισώσεων (κυρίως προσεγγιστικές μεθόδους). Όπως εξηγεί ο ίδιος, αυτές οι δύο κατηγορίες θα πρέπει να είναι θεωρηθούν ως διακεκριμένες. Τα αποτελέσματα για την πρώτη κατηγορία της έρευνάς του ο Lagrange τα παρουσίασε στην Ακαδημία του Βερολίνου με τίτλο: *"Réflexions sur la résolution algébrique des équations"*[24] και

[1]το όνομά του ήταν Giuseppe Lodovico (Luigi) Lagrangia, εφόσον γεννήθηκε στο Τορίνο της βορειοδυτικής Ιταλίας.

[2]όπως αναφέρει ο Hamburg στο [17]

δημοσιεύτηκαν στο περιοδικό της Ακαδημίας, τα δύο πρώτα μέρη το 1770 και τα υπόλοιπα το 1771. Τα αποτελέσματα της δεύτερης κατηγορίας της έρευνάς του δημοσιεύτηκαν το 1798 σε ένα βιβλίο με τίτλο *"Traité de la résolution des équations numériques de tous les degrés"*.

Αν και είναι πιθανό ο Galois να είχε μελετήσει όλα τα προαναφερόμενα έργα του Lagrange, αυτό που τον επηρέασε σαφώς όσο κανένα άλλο είναι η μελέτη του για την αλγεβρική επίλυση των εξισώσεων, όπου όπως θα διαπιστώσουμε περιέχει τους σπόρους των ιδεών τις οποίες ανάπτυξε περαιτέρω στη θεωρία του. Αξίζει βέβαια να αναφερθεί ότι το ίδιο έργο[24] του Lagrange επηρέασε και έδωσε την απαραίτητη ώθηση στους Ruffini και Abel για την απόδειξη της μη επιλυσιμότητας της πεμπτοβάθμιας εξίσωσης με ριζικά. Στην εισαγωγή του *"Réflexions sur la résolution algébrique des équations"* ο Lagrange εξηγεί τους σκοπούς της μελέτης του:

> Σε αυτή την εργασία προτίθεμαι να εξετάσω τις διάφορες μεθόδους που έχουν βρεθεί για την αλγεβρική λύση των εξισώσεων, να τις ελαττώσω σε γενικές αρχές, και να δείξω εκ των προτέρων *(a priori)* γιατί αυτές οι μέθοδοι πετυχαίνουν για την εξίσωση τρίτου και τετάρτου βαθμού και αποτυγχάνουν για υψηλότερους βαθμούς. Η μελέτη αυτή θα έχει ένα διπλό όφελος: πρώτον, θα χρησιμεύσει για να ρίξει περισσότερο φως στις γνωστές λύσεις των περιπτώσεων τρίτου και τετάρτου βαθμού, δεύτερον, θα είναι χρήσιμη σε όσους σκοπεύουν να ασχοληθούν με την επίλυση των εξισώσεων υψηλότερου βαθμού, με την παράθεση διαφορετικών απόψεων για το σκοπό αυτό και την εξάλειψη ενός ιδιαίτερα μεγάλου αριθμό άχρηστων ενεργειών και υποθέσεων.

Τα δύο πρώτα μέρη της εργασίας ήταν αφιερωμένα στις μέχρι τότε γνωστές μεθόδους επίλυσης των εξισώσεων τρίτου και τετάρτου βαθμού. Στην τρίτη ενότητα εξεταζόταν η δυνατότητα εφαρμογής τους σε εξισώσεις με υψηλότερο βαθμό. Η τέταρτη ενότητα περιλάμβανε το συμπέρασμα του προηγούμενου προβληματισμού, με αρκετές γενικές παρατηρήσεις σχετικά με τη μετατροπή των εξισώσεων και η μείωσή τους σε χαμηλότερο βαθμό.

Ο Lagrange ξεκινάει τη μελέτη του αφιερώνοντας το πρώτο μέρος της αποκλειστικά στην τριτοβάθμια εξίσωση. Αρχικά αναφέρει ότι από

τη γενική της μορφή[3]

$$x^3 + mx^2 + nx + p = 0 \tag{2.1}$$

μπορούμε να απαλείψουμε τον δευτεροβάθμιο όρο και διαιρώντας με τον συντελεστή του x^3 να φέρουμε την εξίσωση στη μορφή

$$x^3 + nx + p = 0 \tag{2.2}$$

Για την συντμημένη αυτή μορφή ο Lagrange σημειώνει ότι με αυτή τη μορφή τριτοβάθμιας ασχολήθηκαν και κατάφεραν την επίλυσή της ο delFerro και ο Tartaglia χωρίς όμως να γνωρίζουμε το μονοπάτι που ακολούθησαν. Η πρώτη μέθοδο επίλυσης που εξετάζει είναι αυτή του Hudde[4] η οποία του φαίνεται και η πιο φυσική. Η μέθοδος αυτή παριστάνει τη ρίζα της εξίσωσης ως άθροισμα δύο μεταβλητών οι οποίες συμμετέχουν με τέτοιο τρόπο ώστε να οδηγούν σε μια εξίσωση δευτέρου βαθμού που είναι εύκολο να επιλυθεί. Έτσι θέτοντας $x = y + z$ και αντικαθιστώντας στην (2.2) παίρνουμε τις ισότητες

$$y^3+3y^2z+3yz^2+z^3+n(y+z)+p = 0 \Leftrightarrow y^3+z^3+p+(y+z)(3yz+n) = 0 \tag{2.3}$$

Από την τελευταία μπορούμε να εξάγουμε ένα σύστημα δύο εξισώσεων

$$y^3 + z^3 + p = 0 \text{ και } 3yz + n = 0 \tag{2.4}$$

Λύνοντας τη δεύτερη ως προς z παίρνουμε $z = -\frac{n}{3y}$ και αντικαθιστώντας στην πρώτη βρίσκουμε

$$y^3 - \frac{n^3}{27y^3} + p = 0 \Leftrightarrow y^6 + py^3 - \frac{n^3}{27} = 0 \tag{2.5}$$

Η εξίσωση αυτή είναι βεβαίως 6ου βαθμού αλλά επειδή έχει μόνο δύο δυνάμεις του αγνώστου, μια στην τρίτη και μια στην έκτη δύναμη, μπορούμε να τη λύσουμε σαν δευτέρου βαθμού ως προς y^3 και έτσι να πάρουμε

$$y^3 = -\frac{p}{2} \pm \sqrt{\frac{p^2}{4} + \frac{n^3}{27}} \Leftrightarrow y = \sqrt[3]{\frac{p^2}{4} + \frac{n^3}{27}} \tag{2.6}$$

[3]χάριν την κομψότητας του αρχικού κειμένου του 1770, κρατούμε τον συμβολισμό και τις μεταβλητές που χρησιμοποιεί ο Lagrange, σημειώνοντας επιπλέον ότι με x', x'', x''', x^{IV} συμβολίζει αντίστοιχα τις μεταβλητές με δείκτες x_1, x_2, x_3, x_4

[4]όπως την ονομάζει ο Lagrange, αλλά όταν ολοκληρώνει τη μελέτη της μεθόδου αυτής την αναφέρει ως "Régle de Cardan" δηλαδή Κανόνα του Καρντάν.

Οπότε βρίσκουμε και τη λύση για την αρχική εξίσωση (2.2)

$$x = y + z = y - \frac{n}{3y} \tag{2.7}$$

Φτάνοντας σ' αυτή τη λύση, ο Lagrange κάνει ορισμένες παρατηρήσεις. Επειδή το y είναι ρίζα εξίσωσης 6ου βαθμού πρέπει να παίρνει 6 τιμές και συνεπώς και το x θα πρέπει επίσης να λαμβάνει κι αυτό 6 τιμές αφού υπολογίζεται από τη σχέση $x = y - \frac{n}{3y}$. Όμως το x είναι ρίζα της τριτοβάθμιας εξίσωσης (2.2) και άρα πρέπει να παίρνει το πολύ τρεις διαφορετικές τιμές. Συνεπώς συμπεραίνει ότι ο x θα πρέπει μέσω του y να παίρνει τρεις διαφορετικές τιμές. Αναφέρει στη συνέχεια ότι αυτό επιβεβαιώνεται πλήρως αν απαλείψουμε το y από τις δύο εξισώσεις $y^6 + py^3 - \frac{n^3}{27} = 0$ και $x = y - \frac{n}{3y}$ και χειριζόμενος δεξιοτεχνικά τους αλγεβρικούς υπολογισμούς καταλήγει στην εξίσωση $(x^3 + nx + p)^2 = 0$ δηλαδή την αρχική τριτοβάθμια (2.2) υψωμένη όμως στο τετράγωνο η οποία έχει τις ίδιες ακριβώς λύσεις αλλά διπλές.

Παρά τις έξι τιμές που παίρνει ο y, συνεχίζει στη μελέτη του ο Lagrange, υπάρχουν μόνο τρεις που δίνουν διαφορετικές τιμές για το x. Μένει λοιπόν να ξεχωρίσουμε αυτές τις τιμές. Άρα χρειάζεται να εκφράσουμε ακριβώς κάθε μία από αυτές τις έξι λύσεις για το y. Για συντομία συμβολίζει με 1, α και β τις κυβικές ρίζες της μονάδας, δηλαδή τις λύσεις της εξίσωσης $x^3 - 1 = 0$ και θέτει $q = \frac{p^2}{4} + \frac{n^3}{27}$. Έτσι αναφέρει πως οι έξι τιμές που παίρνει το y είναι:

$$\sqrt[3]{-\frac{p}{2} \pm \sqrt{q}},\ \alpha\sqrt[3]{-\frac{p}{2} \pm \sqrt{q}},\ \beta\sqrt[3]{-\frac{p}{2} \pm \sqrt{q}} \tag{2.8}$$

όμως επειδή

$$\sqrt[3]{-\frac{p}{2} \pm \sqrt{q}} \cdot \sqrt[3]{-\frac{p}{2} \mp \sqrt{q}} = \sqrt[3]{(-\frac{p}{2})^2 - (\sqrt{q})^2} = \sqrt[3]{\frac{p^2}{4} - q} = \sqrt[3]{-\frac{n^3}{27}} = -\frac{n}{3} \tag{2.9}$$

άρα

$$\sqrt[3]{-\frac{p}{2} \mp \sqrt{q}} = -\frac{n}{3\sqrt[3]{-\frac{p}{2} \pm \sqrt{q}}} \tag{2.10}$$

και αφού είναι $z = -\frac{n}{3y}$ παίρνουμε τις έξι στο πλήθος τιμές για το z:

$$\sqrt[3]{-\frac{p}{2} \mp \sqrt{q}},\ \frac{1}{\alpha}\sqrt[3]{-\frac{p}{2} \mp \sqrt{q}},\ \frac{1}{\beta}\sqrt[3]{-\frac{p}{2} \mp \sqrt{q}} \tag{2.11}$$

όμως επειδή τα 1,α, και β είναι ρίζες της εξίσωσης $x^3 - 1 = 0$, το γινόμενό τους, σύμφωνα με τους τύπους του Viéte, θα είναι ίσο με τον σταθερό

όρο, δηλαδή $1 \cdot \alpha \cdot \beta = 1 \rightarrow \alpha \cdot \beta = 1$ οπότε $\alpha = \frac{1}{\beta}$ ή και $\beta = \frac{1}{\alpha}$ έτσι τελικά οι έξι τιμές για το z γίνονται:

$$\sqrt[3]{-\frac{p}{2} \mp \sqrt{q}}, \beta\sqrt[3]{-\frac{p}{2} \mp \sqrt{q}}, \alpha\sqrt[3]{-\frac{p}{2} \mp \sqrt{q}} \tag{2.12}$$

Μπορούμε πλέον να υπολογίσουμε τις τιμές για τις ρίζες της αρχικής εξίσωσης (2.2) χρησιμοποιώντας τον αρχικό μετασχηματισμό $x = y + z$. Έτσι βλέπουμε ότι οι έξι τιμές που παίρνει ο x είναι:

$$\begin{array}{c} \sqrt[3]{-\frac{p}{2} \pm \sqrt{q}} + \sqrt[3]{-\frac{p}{2} \mp \sqrt{q}} \\ \alpha\sqrt[3]{-\frac{p}{2} \pm \sqrt{q}} + \beta\sqrt[3]{-\frac{p}{2} \mp \sqrt{q}} \\ \beta\sqrt[3]{-\frac{p}{2} \pm \sqrt{q}} + \alpha\sqrt[3]{-\frac{p}{2} \mp \sqrt{q}} \end{array} \tag{2.13}$$

από τις παραπάνω σχέσεις είναι εύκολο να διαπιστώσουμε ότι όλοι οι συνδυασμοί των προσήμων (+ και -) του $\sqrt{q}$ μας δίνουν τρεις μόνο διαφορετικές τιμές για το x.

Ο Lagrange συνεχίζοντας ονομάζει την εξίσωση που προέκυψε $y^6 + py^3 - \frac{n^3}{27} = 0$ ως "ελαττωμένη" *(réduite)* της τριτοβάθμιας αφού με την επίλυσή της σαν δευτέρου βαθμού (δηλαδή μικρότερου) οδηγούμαστε στις λύσεις της ζητούμενης. Αμέσως μετά, αφού έχει ήδη δείξει πως οι ρίζες της αρχικής εξαρτώνται από τις λύσεις της ελαττωμένης, εξετάζει το αντίστροφο, δηλαδή πως οι ρίζες της ελαττωμένης εξαρτώνται από αυτές της αρχικής τριτοβάθμιας.
Στη μελέτη αυτή αρχίζει παίρνοντας την πλήρη τριτοβάθμια

$$x^3 + mx^2 + nx + p = 0 \tag{2.14}$$

ονομάζοντας a, b και c τις ρίζες της. Με το μετασχηματισμό $x = x' - \frac{m}{3}$ και κάνοντας χρήση των συντομογραφιών $n' = n - \frac{m^2}{3}, p' = p - \frac{mn}{3} + \frac{2m^3}{27}$ απαλείφει τον δευτεροβάθμιο όρο και η 2.14 γίνεται

$$x'^3 + n'x' + p' = 0 \tag{2.15}$$

Εργαζόμενος όπως και προηγουμένως με τη βοήθεια του μετασχηματισμού $x' = y - \frac{n'}{3y}$ βρίσκει την ελαττωμένη εξίσωση $y^6 + p'y^3 - \frac{n'^3}{27} = 0$ και συμβολίζοντας με $r = \sqrt[3]{-\frac{p'}{2}} + \sqrt{\frac{p'^2}{4} + \frac{n'^3}{27}}$ βρίσκει τις τρεις τιμές του y, δηλαδή $y = r, y = \alpha r, y = \beta r$ οι οποίες μας δίνουν τις τρεις ρίζες για την (2.15):

$$x' = r - \frac{n'}{3r}, x' = \alpha r - \frac{n'}{3\alpha r}, x' = \beta r - \frac{n'}{3\beta r} \tag{2.16}$$

από τις οποίες αν αντιστρέψουμε τον αρχικό μετασχηματισμό $x = x' - \frac{m}{3}$ και συμβολίζοντας με $s = \frac{n'}{3r}$ οι τρεις ρίζες της αρχικής (2.14) είναι:

$$\begin{aligned} a &= -\tfrac{m}{3} + r - s \\ b &= -\tfrac{m}{3} + \alpha r - \tfrac{s}{\alpha} \\ c &= -\tfrac{m}{3} + \beta r - \tfrac{s}{\beta} \end{aligned} \tag{2.17}$$

Με διαδοχικές αφαιρέσεις της μιας από την άλλη σχέση, ο Lagrange καταλήγει στην

$$r = \frac{a}{(1-\alpha)(1-\beta)} + \frac{\alpha b}{(\alpha-1)(\alpha-\beta)} + \frac{\beta c}{(\beta-1)(\beta-\alpha)} \tag{2.18}$$

όπου α και β οι μη πραγματικές τρίτες ρίζες της μονάδας. Παραγωγίζοντας τώρα τη σχέση $x^3 - 1 = (x-1)(x-\alpha)(x-\beta)$ παίρνει $3x^2 = (x-\alpha)(x-\beta) + (x-1)(x-\beta) + (x-1)(x-\alpha)$ και αντικαθιστώντας με τη σειρά το x ίσο με 1, α, β βρίσκει τις ισότητες

$$\begin{aligned} 3 &= (1-\alpha)(1-\beta) \\ 3\alpha^2 &= (\alpha-1)(\alpha-\beta) \\ 3\beta^2 &= (\beta-1)(\beta-\alpha) \end{aligned} \tag{2.19}$$

τις οποίες αντικαθιστά στην 2.18 και έτσι παίρνει

$$r = \frac{a}{3} + \frac{b}{3\alpha} + \frac{c}{3\beta} \overset{\alpha\cdot\beta=1}{\Longrightarrow} r = \frac{a + \beta b + \alpha c}{3} \tag{2.20}$$

η οποία είναι και η τιμή του y, δηλαδή η λύση της εκτοβάθμιας, ή εναλλάσσοντας τα α και β παίρνουμε επίσης και $y = \frac{a+\alpha b+\beta c}{3}$, κάτι που είναι επιτρεπτό αφού η επιλογή για τα b και c ήταν τυχαία.

Από την προηγούμενη μελέτη ο Lagrange κάνει αντιληπτό τον λόγο για τον οποίο η ελαττωμένη μιας τριτοβάθμιας είναι έκτου βαθμού αφού, όπως λέει ο ίδιος, δεν εξαρτάται άμεσα από τις ρίζες a, b, c της τριτοβάθμιας αλλά μόνο από τους συντελεστές της στους οποίους οι ρίζες συνυπάρχουν ισότιμα, εννοώντας προφανώς τους τύπους του Viéte. Είναι επίσης ξεκάθαρο ότι στη σχέση που δίνει το y μπορούμε να εναλλάξουμε όπως θέλουμε τις ποσότητες a, b, c μεταξύ τους κι έτσι το y θα λάβει τόσες διαφορετικές τιμές όσες και οι μεταθέσεις των τριών ριζών. Κάνοντας λοιπόν όλους τους συνδυασμούς των τριών στοιχείων παίρνουμε $3! = 6$, που σημαίνει ότι το y παίρνει έξι τιμές, είναι δηλαδή λύση μιας εκτοβάθμιας.

Αξίζει να παρατηρήσουμε ότι στο σημείο αυτό ο Lagrange αναφέρει για πρώτη φορά τη φράση "μεταθέσεις ριζών" (*permutations*

des racines) μιας πολυωνυμικής εξίσωσης αναδεικνύοντας έτσι και τον σημαντικό ρόλο τους σε μια εξίσωση που λύνεται με ριζικά. Ίσως είναι και η πιο βασική συνεισφορά του στον αγώνα για για την επίλυση πολυωνυμικών εξισώσεων κάθε βαθμού, αφού σ' αυτή την έννοια στηρίζεται και η βάση της Θεωρίας Galois. Βέβαια ενώ ο Lagrange έβλεπε τις μεταθέσεις των ριζών μεμονωμένα, ο Galois είχε την ιδέα να τις δει ως σύνολο (ομάδα) και έτσι να προχωρήσει στη θεωρία του.

Συνεχίζοντας, από την ίδια σχέση για το y επιπλέον γίνεται αντιληπτός ο λόγος που η ελαττωμένη λύνεται σαν δευτεροβάθμια. Επειδή οι μόνες δυνάμεις που εμφανίζεται ο y είναι οι y^3 και y^6 δηλαδή πολλαπλάσια του 3 οπότε αν μια λύση είναι η $y = r$ τότε οι άλλες είναι οι $y = \alpha r$ και $y = \beta r$ αφού $\alpha^3 = 1$ και $\beta^3 = 1$. Η σχέση για το y μπορεί να γίνει και $y = \frac{a+\alpha b+\alpha^2 c}{3}$ εφόσον από τις σχέσεις $\alpha\beta = 1$ και $\alpha^3 = 1$ παίρνουμε ότι $\alpha\beta = \alpha^3 \leftrightarrow \beta = \alpha^2$ Κάνοντας όλες τις μεταθέσεις των ριζών a, b, c παίρνουμε για το y όλες τις ρίζες της ελαττωμένης:

$$\begin{array}{c} \frac{a+\alpha b+\alpha^2 c}{3}, \\ \frac{a+\alpha c+\alpha^2 b}{3}, \\ \frac{b+\alpha a+\alpha^2 c}{3}, \\ \frac{b+\alpha c+\alpha^2 a}{3}, \\ \frac{c+\alpha b+\alpha^2 a}{3}, \\ \frac{c+\alpha a+\alpha^2 b}{3} \end{array} \tag{2.21}$$

Ο Lagrange παρατηρεί, ισχυροποιώντας τα επιχειρήματά του, ότι πολλαπλασιάζοντας την πρώτη με α και με α^2 παίρνουμε την έκτη και τέταρτη σχέση αντίστοιχα. Ομοίως πολλαπλασιάζοντας την δεύτερη με α και με α^2 παίρνουμε την τρίτη και πέμπτη σχέση. Με τον ίδιο τρόπο για τις υπόλοιπες βρίσκουμε πάλι άλλα ζεύγη τα οποία όμως ανήκουν στις έξι αυτές λύσεις.

Αυτή η διαπίστωση, λέει ο Lagrange, μας οδηγεί σ' έναν τρόπο εύρεσης της ελαττωμένης από την οποία εξαρτάται η λύση της γενικής τριτοβάθμιας (2.14) με ρίζες a, b, c. Υποθέτει ότι οι ρίζες της ελαττωμένης παριστάνονται από μια πρωτοβάθμια συνάρτηση των ριζών a, b, c τέτοια ώστε

$$Aa + Bb + Cc \tag{2.22}$$

όπου A, B, C συντελεστές ανεξάρτητοι από τα a, b, c. Οι έξι ρίζες της ελαττωμένης λοιπόν προκύπτουν από τις μεταθέσεις των τριών

στοιχείων a, b, c στη σχέση που μόλις αναφέραμε, είναι δηλαδή οι:

$$\begin{array}{c} Aa+Bb+Cc, \\ Aa+Bc+Cb, \\ Ab+Ba+Cc, \\ Ab+Bc+Ca, \\ Ac+Bb+Ca, \\ Ac+Ba+Cb \end{array} \tag{2.23}$$

Για να έχει η ελαττωμένη δυνάμεις του αγνώστου μόνο πολλαπλάσια του 3 πρέπει, αν ονομάσουμε ως r μια ρίζα της, να είναι επίσης ρίζες και οι αr και $\beta r = \alpha^2 r$. Γι αυτό παίρνουμε την έκφραση $r = Aa+Bb+Cc$ και υπολογίζουμε την $\alpha r = \alpha Aa + \alpha Bb + \alpha Cc$ η οποία θα πρέπει να ισούται με μια από τις υπόλοιπες πέντε ρίζες της ελαττωμένης. Όπως παρατηρούμε θα είναι ίση με τη δεύτερη έκφραση ή με την τρίτη μόνο αν $\alpha = 1$ αφού τότε θα έχουμε $\alpha A = A$ και $\alpha C = C$. Αν την συγκρίνουμε με την τέταρτη έκφραση $Ab + Bc + Ca$ θα πρέπει να είναι $\alpha A = C$, $\alpha B = A$ και $\alpha C = B$ από όπου παίρνουμε $C = \alpha A$, $B = \alpha^2 A$ και $\alpha^3 A = A$ επιβεβαιώνοντας πάλι ότι $\alpha^3 = 1$ δηλαδή ότι το α είναι μια τρίτη ρίζα της μονάδας. Αν θέσουμε για απλότητα $A = 1$ θα βρούμε στις σχέσεις αυτές ότι $B = \alpha^2$ και $C = \alpha$ παίρνοντας τις ίδιες ρίζες που είχαμε υπολογίσει προηγούμενα αλλά χωρίς τον παρονομαστή 3.

Συμβολίζοντας με $r = a + \alpha b + \alpha^2 c$ και $s = a + \alpha c + \alpha^2 b$ θα έχουμε ως ρίζες της εκτοβάθμιας τις: $r, \alpha r, \alpha^2 r, s, \alpha s, \alpha^2 s$. Αν είναι y ο άγνωστος της εκτοβάθμιας τότε το γινόμενο

$$(y-r)(y-\alpha r)(y-\alpha^2 r)(y-s)(y-\alpha s)(y-\alpha^2 s) = (y^3-r^3)(y^3-s^3) \tag{2.24}$$

είναι η ελαττωμένη εξίσωση και κάνοντας τις πράξεις βρίσκουμε

$$y^6 - (r^3+s^3)y^3 + r^3 s^3 = 0 \tag{2.25}$$

η οποία έχει τη ζητούμενη μορφή. Υπολογίζουμε τώρα τους συντελεστές της παραπάνω εξίσωσης

$$\begin{array}{l} r^3 = a^3+b^3+c^3+6abc+3\alpha(a^2b+b^2c+c^2a)+3\alpha^2(ab^2+bc^2+ca^2) \\ s^3 = a^3+b^3+c^3+6abc+3\alpha(a^2c+c^2b+b^2a)+3\alpha^2(c^2a+b^2c+a^2b) \end{array} \tag{2.26}$$

συμβολίζοντας τώρα για απλότητα, όπως ακριβώς κάνει ο Lagrange,

$$\begin{array}{c} a^3+b^3+c^3+6abc = L, \\ a^2b+b^2c+c^2a = M, \\ a^2c+c^2b+b^2a = N \end{array} \tag{2.27}$$

βρίσκουμε τις εκφράσεις για το $r^3 + s^3 = 2L + 3(\alpha + \alpha^2)(M + N)$, όπου όμως επειδή οι $1, \alpha, \alpha 2$ είναι ρίζες της $x^3 - 1 = 0$ η οποία έχει τον συντελεστή του x^2 ίσο με 0, από τους τύπους του Viéte για τις ρίζες παίρνουμε $1 + \alpha + \alpha^2 = 0$. Έτσι καταλήγουμε ότι $r^3 + s^3 = 2L - 3(M + N)$ καθώς και ότι $r^3 s^3 = L[L - 3(M + N)] + 9[(M + N)^2 - 3MN]$. Στη συνέχεια θα δούμε ότι οι ποσότητες $L, M + N, MN$ μπορούν να εκφραστούν ως συνάρτηση των συντελεστών m, n, p της αρχικής εξίσωσης (2.14) χωρίς να είναι απαραίτητος ο υπολογισμός των ριζών a, b, c.

Από τους τύπους του Viéte για τις ρίζες παίρνουμε $-m = a + b + c, \quad n = ab + ac + bc, \quad -p = abc$ και από επίσης γνωστές σχέσεις για τις ρίζες έχουμε $a^2 + b^2 + c^2 = m^2 - 2n,$ και $a^3 + b^3 + c^3 = -m^3 + 3mn - 3p$ από τις οποίες τελικά βρίσκουμε ότι:

$$\begin{gathered} L = -m^3 + 3mn - 9p, \\ M + N = 3p = mn, \\ MN = n^3 + p(m^3 - 6mn) + 9p^2 \end{gathered} \tag{2.28}$$

Οπότε τελικά

$$\begin{gathered} r^3 + s^3 = -2m^3 + 9mn - 27p \text{ και} \\ r^3 s^3 = (m^2 - 3n)^3 \end{gathered} \tag{2.29}$$

Κι έτσι η ελαττωμένη εκφρασμένη ως συνάρτηση μόνο των συντελεστών m, n, p είναι η

$$y^6 + (2m^3 - 9mn + 27p)y^3 + (m^2 - 3n)^3 = 0 \tag{2.30}$$

Λύνοντας την τελευταία εξίσωση σαν δευτεροβάθμια αν θέσουμε $y^3 = z$ οπότε $z^2 + (2m^3 - 9mn + 27p)z + (m^2 - 3n)^3 = 0$ και ονομάζοντας z' και z'' τις ρίζες της παίρνουμε $y = \sqrt[3]{z'}$ ή $y = \sqrt[3]{z''}$. Επειδή υποθέσαμε ότι r και s είναι οι δύο τιμές του y μπορούμε να πάρουμε

$$\begin{gathered} r = a + \alpha b + \alpha^2 c = \sqrt[3]{z'} \quad \text{και} \\ s = a + \alpha c + \alpha^2 b = \sqrt[3]{z''} \end{gathered} \tag{2.31}$$

οι οποίες σε συνδυασμό με τη σχέση $a + b + c = -m$ σχηματίζουν ένα σύστημα τριών αγνώστων με τρεις εξισώσεις απ'όπου βρίσκουμε τις ρίζες a, b, c. Έτσι αφού $\alpha^3 = 1$ και $1 + \alpha + \alpha^2 = 0$ υπολογίζουμε

$$\begin{gathered} a = \frac{-m + \sqrt[3]{z'} + \sqrt[3]{z''}}{3} \\ b = \frac{-m + \alpha^2 \sqrt[3]{z'} + \alpha \sqrt[3]{z''}}{3} \\ c = \frac{-m + \alpha \sqrt[3]{z'} + \alpha^2 \sqrt[3]{z''}}{3} \end{gathered} \tag{2.32}$$

οι οποίες συμφωνούν με όσα έχουν υπολογιστεί και προηγουμένως.

Ο Lagrange παρατηρεί ότι οι ποσότητες M και N είναι τέτοιες ώστε η μία προκύπτει από την άλλη μετά από μια μετάθεση[5] των ριζών a, b, c. Οι ποσότητες αυτές λοιπόν μπορούν να είναι ρίζες μιας δευτεροβάθμιας με άγνωστο t όπως για παράδειγμα της:

$$t^2 - (M + N)t + MN = 0 \tag{2.33}$$

αντικαθιστώντας τα $M + N, MN$ με τις τιμές που έχουμε ήδη βρει στις ισότητες (2.28) παίρνουμε

$$t^2 - (3p - mn)t + n^3 + (m^3 - 6mn)p + 9p^2 = 0 \tag{2.34}$$

Με τη λύση της βρίσκουμε τα M και N και εφόσον έχουμε ήδη το L στις ισότητες (2.28) βρίσκουμε εύκολα τις τιμές των r^3, s^3 ή κατόπιν των z', z'' δηλαδή

$$\begin{aligned} z' &= L + 3\alpha M + 3\alpha^2 N \\ z'' &= L + 3\alpha N + 3\alpha^2 M \end{aligned} \tag{2.35}$$

και από αυτές παίρνουμε τις ρίζες a, b, c. Αυτή η ιδιότητα των M και N φανερώνει την αιτία που η ποσότητα $z = y^3 = (a + \alpha b + \alpha^2 c)^3$ εξαρτάται μόνο από μια δευτεροβάθμια με τρόπο τέτοιο ώστε η εξίσωση του y να περιλαμβάνει μόνο τις δυνάμεις y^3 και y^6.

Στη συνέχεια ο Lagrange εξετάζει τη μέθοδο επίλυσης του Tschirnhaus η οποία, όπως λέει, αν και πιο περίπλοκη από την προηγούμενη έχει το πλεονέκτημα να είναι πιο γενική και πιο ευθεία αφού μπορούμε να απαλείψουμε οποιουσδήποτε όρους θέλουμε από μια εξίσωση και επιπλέον μας οδηγεί απ' ευθείας σε μια ελαττωμένη δευτεροβάθμια και όχι μέσω μιας έκτου βαθμού. Σύμφωνα με αυτή τη μέθοδο χρειάζεται να βρούμε τους κατάλληλους συντελεστές a και b σε μια βοηθητική εξίσωση $x^2 = bx + a + y$ ώστε η πλήρης τριτοβάθμια (2.14) να πάρει τη μορφή $y^3 + C = 0$ και από αυτήν με εξαγωγή κυβικής ρίζας να φτάσουμε στις λύσεις

$$y = -\sqrt[3]{C}, y = -\alpha\sqrt[3]{C}, y = -\alpha^2\sqrt[3]{C} \tag{2.36}$$

όπου $\alpha, \alpha^2 s$ οι μη πραγματικές κυβικές ρίζες της μονάδας.

Ακολούθως μελετάει τη μέθοδο των Euler και Bezout σύμφωνα με την οποία οι ενδιάμεσοι όροι της πλήρους τριτοβάθμιας (2.14) απαλείφονται με την βοηθητική σχέση $x = a + by + cy^2$ όπου $y^3 + h = 0$.

Σχολιάζοντας και τις τρεις μεθόδους ο Lagrange αναφέρει ότι ο στόχος τους είναι να βρουν την ελαττωμένη εξίσωση της οποίας οι

[5]την κυκλική μετάθεση(abc)

λύσεις αναπαριστώνται με τη σχέση $x' + \alpha x'' + \alpha^2 x'''$ όταν η ελαττωμένη είναι έκτου βαθμού, που επιλύεται σαν δευτέρου βέβαια, ή με τη σχέση $(x' + \alpha x'' + \alpha^2 x''')^3$ όταν η ελαττωμένη είναι δευτέρου βαθμού.

Στο δεύτερο μέρος ο Lagrange μελετάει με την ίδια λεπτομέρεια όπως και στο πρώτο μέρος, τη μέθοδο του Louis Ferrari για την επίλυση της τεταρτοβάθμιας εξίσωσης, την οποία και χαρακτηρίζει ως την πιο εφυής (ingenieuse) από όλες και κατόπιν, με τη σειρά, τις αντίστοιχες μεθόδους του Descartes αλλά και τις πιο γενικές, δηλαδή του Tschirnaus και Euler-Bezout. Με την ανάλυσή του αυτή ο Lagrange δείχνει τη σχέση που έχουν αυτές μεταξύ τους και την αμοιβαία εξάρτησή τους. Δίνει επίσης την αιτία η οποία *"a priori"*, όπως λέει ο ίδιος, οδηγεί κάποιες σε ελαττωμένες τρίτου βαθμού και κάποιες άλλες σε ελαττωμένες έκτου βαθμού, οι οποίες όμως λύνονται σαν τριτοβάθμιες. Η αιτία είναι ότι οι ρίζες των ελαττωμένων αυτών είναι συναρτήσεις των ποσοτήτων x', x'', x''', x^{IV} τέτοιες ώστε κάνοντας όλες τις δυνατές μεταθέσεις ανάμεσα σ' αυτές τις ποσότητες καταλήγουμε σε τρεις μόνο διαφορετικές τιμές, όπως π.χ. η συνάρτηση $x'x' + x'''x^{IV}$, ή σε έξι διαφορετικές τιμές ανά δύο ίσες (με αντίθετα πρόσημα) όπως η συνάρτηση $x' + x'' - x''' + x^{IV}$, ή τέλος έξι διαφορετικές τιμές τέτοιες όμως ώστε αν τις πάρουμε ανά τρία ζεύγη το άθροισμα ή το γινόμενο των ζευγαριών θα είναι πάντοτε το ίδιο κάτω από οποιαδήποτε μετάθεση κάνουμε στις ποσότητες x', x'', x''', x^{IV}. Όπως παρατηρεί στο τέλος του δεύτερου μέρους ο ίδιος ο Lagrange:

> " Στην ύπαρξη αποκλειστικά τέτοιου είδους συναρτήσεων βασίζεται η γενική επίλυση των εξισώσεων τετάρτου βαθμού."

Στο τρίτο μέρος ο Lagrange αναγνωρίζει ότι δεν υπάρχει κάποια ολοκληρωμένη και σίγουρη γενική μέθοδος για την επίλυση εξισώσεων μεγαλύτερου του τετάρτου βαθμού, αλλά ούτε όμως και απόδειξη (μέχρι τότε που γράφτηκε η μελέτη) της μη ύπαρξης μιας τέτοιας μεθόδου. Οι μόνες έως τότε γνωστές μέθοδοι οι οποίες έδιναν κάποια ελπίδα επιτυχίας είναι αυτές που ήδη έχει παρουσιάσει στη μελέτη του για τις τριτοβάθμιες και τεταρτοβάθμιες, δηλαδή αυτές των Tschirnaus και Euler-Bezout. Οι μέθοδοι αυτές έχουν το πλεονέκτημα ότι είναι γενικές και μπορούν να εφαρμοστούν σε εξισώσεις οποιουδήποτε βαθμού, όμως οι υπολογισμοί που εμφανίζονται, στην περίπτωση της πεμπτοβάθμιας και πάνω, είναι τόσο πολύπλοκοι που τις καθιστούν μη πρακτικές. Για παράδειγμα αν εφαρμόσουμε τη μέθοδο του Tschirnaus στην πεμπτοβάθμια

εξίσωση θα οδηγηθούμε στη λύση τεσσάρων εξισώσεων με τέσσερις αγνώστους όπου η πρώτη εξίσωση είναι πρώτου βαθμού, η δέυτερη δευτέρου κ.ο.κ. Έτσι το σύστημα αυτών των εξισώσεων θα οδηγήσει στην επίλυση μιας εξίσωσης $1 \cdot 2 \cdot 3 \cdot 4 = 24^{ου}$ βαθμού, της οποίας η επίλυση αν είναι εφικτή θα χρειαστεί επίσης μακροσκελής και περίπλοκους υπολογισμούς. Τις ίδιες δυσκολίες αντιμετωπίζουμε ακολουθώντας και τη μέθοδο των Euler-Bezout, όπου εμφανίζεται μια εξίσωση $120^{ου}$ βαθμού με αγνώστους υψωμένους σε δυνάμεις που είναι πολλαπλάσια του 5 και επομένως μπορεί και αυτή να λυθεί, αν αυτό είναι βέβαια εφικτό, σαν εξίσωση $24^{ου}$ βαθμού. Παρά τις δυσκολίες των μεθόδων αυτών όμως, ο Lagrange προχωράει με τόλμη στην μελέτη της εφαρμογής τους για εξισώσεις μεγαλύτερου του 4ου βαθμού, εξαντλώντας όσα μπορούν να αναδειχθούν από αυτές και να αξιοποιηθούν κατάλληλα από άλλους μελετητές. Κάτι που όπως θα φανεί στη συνέχεια, όντως συνέβει από τους Abel, Ruffini και κυρίως τον Galois.

2.1.2 Ruffini

Ο πρώτος Μαθηματικός που ερεύνησε σε βάθος τις ιδέες του Lagrange για τις πολυωνυμικές εξισώσεις, ήταν ο Paolo Ruffini από τη Modena της Βόρειου Ιταλίας.[6] Το 1799 εξέδωσε το έργο του με τίτλο: *"Teoria generale delle equazioni"* όπου ισχυριζοταν ότι είχε αποδείξει την μη επιλυσιμότητα με ριζικά της πεμπτοβάθμιας εξίσωσης. Από την αρχή κατέστησε σαφές από ποιόν επηρεάστηκε αναφέροντας χαρακτηριστικά:

> Ο αθάνατος Lagrange με τους υπέροχους προβληματισμούς του για τις εξισώσεις, οι οποίες παρουσιάστηκαν στα Mémoires της Ακαδημίας του Βερολίνου, έχει δώσει το θεμέλιο της μελέτης μου.

Πράγματι, μεγάλο μέρος του πρώτου μέρους του *Teoria* είναι μια ανακεφαλαίωση των προβληματισμών του Lagrange, χρησιμοποιώντας μάλιστα και τον ίδιο συμβολισμό. Ο Ruffini πήγε για να αποδείξει, με τη ρητή καταγραφή και ανάλυση των 120 μεταθέσεων των πέντε μεταβλητών, ότι δεν είναι δυνατή για μια συνάρτηση με αυτές τις μεταβλητές να πάρει 3 ή 4 (ή 8) τιμές. Χρησιμοποίησε κατόπιν αυτά τα αποτελέσματα για να αποδείξει ότι δεν μπορεί να βρεθεί μια επιλύουσα εξίσωση για την πεμπτοβάθμια,

[6] αναφορές από το [33] και το [20]

η οποία είναι μικρότερη του πέμπτου βαθμού.[7] Ο Ruffini εφευρίσκει ένα εκτεταμένο σύστημα ταξινόμησης για τις διατάξεις, το οποίο δεν είναι εύκολο να μεταφραστεί στη σύγχρονη ορολογία, μπορούμε όμως να το προσεγγίσουμε με τη βοήθεια των ομάδων που παράγονται από τις μεταθέσεις των διατάξεων αυτών. Έτσι οι *"απλές"* μεταθέσεις των n στοιχείων παράγουν τις κυκλικές ομάδες, είτε αυτές παράγονται από n-κύκλους είτε από ένα στοιχείο που είναι το γινόμενο ξένων μεταξύ τους κύκλων. Οι *"σύνθετες"* μεταθέσεις παράγουν τρεις τύπους μη-κυκλικών ομάδων οι οποίες σήμερα ονομάζονται μη-μεταβατικές, μη-πρωταρχικές και πρωταρχικές.

Ο Lagrange είχε ήδη δείξει ότι το πλήθος των διακριτών τιμών που μπορεί να πάρει μια αλγεβρική παράσταση με n μεταβλητές είναι διαιρέτης του $n!$. Ο Ruffini είχε ως σκοπό να καθορίσει ποιοί διαιρέτες του $n!$ θα μπορούσαν να είναι αυτοί. Όρισε την "τάξη ισοδυναμίας" μιας αλγεβρικής παράστασης να είναι το πλήθος των μεταθέσεων που δεν μεταβάλλουν την παράσταση. Στη σύγχρονη ορολογία θα λέγαμε ότι αυτή είναι η τάξη της ομάδας αυτής της αλγεβρικής παράστασης. Έτσι αν p είναι η τάξη ισοδυναμίας μιας αλγεβρικής παράστασης f με n μεταβλητές, τότε σύμφωνα με το θεώρημα του Lagrange το πλήθος των τιμών που μπορεί να πάρει η f είναι $n!/p$. Ο Ruffini προχώρησε πέρα από αυτό ώστε να καθορίσει, εξετάζοντας κάθε περίπτωση μία προς μία τις πιθανές τιμές του p για κάθε μία από τις πέντε κατηγορίες στις οποίες είχε κατατάξει τις μεταθέσεις αυτές (όπως τις αναφέραμε παραπάνω). Ο στόχος του ήταν να δείξει ότι αν ο p δεν ήταν ούτε $n!$ ούτε $n!/2$, τότε το $n!/p$ είναι τουλάχιστον ίσο με 5.

Για τις δύο κατηγορίες των "απλών" μεταθέσεων, δηλαδή για τις περιπτώσεις που η ομάδα της f είναι κυκλική, ο Ruffini απέδειξε, με σύγχρονη ορολογία, ότι η τάξη της ομάδας είναι το ελάχιστο κοινό πολλαπλάσιο των τάξεων των γεννήτορων κύκλων. Για παράδειγμα η ομάδα που παράγεται από τη μετάθεση (12345) έχει τάξη 5, αυτή που παράγεται από την $(123)(45)$ έχει τάξη 6 και αυτή που παράγεται από την $(1234)(56)$ έχει τάξη 4. Στην πραγματικότητα για $n = 5$ οι πιθανές τιμές του p είναι 2, 3, 4 και 6.

[7] Εδώ, όμως, βρίσκεται και η αδυναμία στην επιχειρηματολογία του: ο Ruffini φαίνεται να έχει υποθέσει ότι αν δεν θα μπορούσε να βρεθεί μια επιλύουσα με ρητούς συντελεστές τότε η αρχική εξίσωση θα ήταν άλυτη, ενώ στην πραγματικότητα το μόνο που απέδειξε είναι ότι η εξίσωση ήταν άλυτη με τη βοήθεια μιας επιλύουσας εξίσωσης με ρητούς συντελεστές, χωρίς να αποκλείσει ότι δεν υπάρχει άλλη μέθοδος η οποία δίνει λύσεις με ριζικά.

Για μια "σύνθετη" μετάθεση της πρώτης μορφής, δηλαδή για την περίπτωση μιας μη-μεταβατικής ομάδας με κάποια ξένα μεταξύ τους σύνολα στα οποία είναι μεταβατική, το p είναι το γινόμενο των παραγοντικών του πλήθους κάθε συνόλου. Για παράδειγμα μια ομάδα μεταθετική στα σύνολα $\{1, 2, 3\}$ και $\{4, 5\}$ έχει τάξη ίση με $3! \times 2! = 12$. Για $n = 5$ οι πιθανές τιμές του p είναι 4 ή 12. Οι υπόλοιπες περιπτώσεις αποτελούνται από ένα πλήθος περιπτώσεων και ο Ruffini δεν τις εξετάζει πλήρως. Αρκεί για τους σκοπούς του για να δείξει, όπως και κάνει ύστερα από κοπιαστικές έρευνες αυτών των περιπτώσεων ότι η τιμή για το p δεν μπορεί να είναι κάποιο πολλαπλάσιο του 5. Έτσι το $n!/p$ για $n = 5$ περιέχει ένα παράγοντα ίσο με 5 εφόσον ο αριθμητής είναι πολλαπλάσιο του 5 ενώ ο παρονομαστής δεν είναι, ολοκληρώνοντας έτσι την απόδειξή του.

Κρίνοντας εκ των υστέρων το αποτέλεσμα, μπορεί να θεωρηθεί ότι παρουσιάζονται πολλά από τα βασικά βήματα της απόδειξης της μη-επιλυσιμότητας της συμμετρικής ομάδας των πέντε ή περισσότερων στοιχείων. Οι τιμές που υποθέτει ότι παίρνει η αλγεβρική παράσταση αντιστοιχούν σε εκείνα τα υποσύνολα της υποομάδας που αποτελούνται από τις μεταθέσεις της S_5 που δεν μεταβάλλουν την παράσταση. Αν αυτή η υποομάδα δεν είναι η εναλλάσουσα ομάδα τότε η τάξη της είναι τουλάχιστον 5.

Το έργο του Ruffini δεν έτυχε αποδοχής από τους σύγχρονούς του Μαθηματικούς. Ο χαρακτηρισμός που του αποδιδόταν συχνότερα ήταν "ασάφεια", ο οποίος είναι δικαιολογημένος δεδομένου ότι μέχρι εκείνη την εποχή το έργο των Μαθηματικών ήταν κυρίως υπολογιστικό και έτσι ήταν απροετοίμαστοι να αποδεχθούν και να κατανοήσουν μια νέα προσέγγιση θεωρητικών επιχειρημάτων και αποδείξεων ύπαρξης. Ο Ruffini στην προσπάθειά του να κάνει πιο κατανοητά τα επιχειρήματά του δημοσιευσε έξι παραλλαγές της απόδειξής του για την μη επιλυσιμότητα της πεμπτοβάθμιας, με την τελευταία να παρουσιάζεται το 1813. Ένας που αντιλήφθηκε το σημαντικό περιεχόμενο του έργου του Ruffini ήταν ο Cauchy, ο οποίος χρησιμοποίησε πολλά από τα αποτελέσματα στις εργασίες του σχετικά με τις μεταθέσεις που θα δούμε και παρακάτω. Το 1821 γράφει στον Ruffini εκφράζοντας την υποστήριξή του αναφέροντάς του ότι:

> Η εργασία σας για τη γενική λύση των εξισώσεων είναι ένα έργο που πάντα πίστευα πως θα πρέπει να λαμβάνεται υπόψη από μαθηματικούς και η οποία, κατά τη γνώμη μου, αποδεικνύει οριστικά τη μη επιλυσιμότητα με

> αλγεβρικές μεθόδους των γενικών εξισώσεων υψηλότερων του τέταρτου βαθμού.

Όμως και ο Abel για τον οποίο θα μιλήσουμε αμέσως μετά, αναφερόμενος στον Ruffini, έγραψε:

> Ο πρώτος και, αν δεν κάνω λάθος, ο μόνος που, πριν από μένα, προσπάθησε να αποδείξει την αδυναμία της αλγεβρικής λύσης των γενικών εξισώσεων είναι ο μαθηματικός Ruffini. Αλλά η εργασία του είναι τόσο περίπλοκη που είναι πολύ δύσκολο να προσδιοριστεί η εγκυρότητα της επιχειρηματολογίας του. Μου φαίνεται ότι η επιχειρηματολογία του δεν είναι πλήρως ικανοποιητική.

2.1.3 Abel

Ένας άλλος σημαντικός Μαθηματικός που αξιοποίησε στο έπακρο τις ιδέες του Lagrange σχετικά με τις πολυωνυμικές εξισώσεις ήταν ο Νορβηγός Niels Henrik Abel. Ξεκίνησε να ασχολείται με τις πολυωνυμικές εξισώσεις γύρω στο 1820, όντας ακόμη μαθητής 18 χρονών και προς στιγμή νόμισε ότι είχε βρει τη γενική λύση της γενικής πεμπτοβάθμιας πολυωνυμικής εξίσωσης. Βρίσκοντας όμως μόνος του το λάθος στη μέθοδο του, στράφηκε στην απόδειξη της μη επιλυσιμότητας της πεμπτοβάθμιας την οποία και δημοσίευσε το 1824 σε ένα φυλλάδιο με τίτλο *"Mémoire sur les équations algébriques ou on démontre l'impossibilité de la résolution de l'équation générale du cinquième degré"* το οποίο εκτύπωσε με δικά του έξοδα. Έχοντας μελετήσει μια εργασία του Cauchy γνώριζε ήδη το όνομα του Ruffini αλλά πιθανώς όχι το ακριβές περιεχόμενο του έργου του. Η απόδειξη του Abel όπως και αυτή του Ruffini βασιζόταν στην ιδέα των ριζών της εξίσωσης ως αθροίσματα ριζικών καθώς και στο πλήθος των τιμών που παίρνει μια συνάρτηση ύστερα από τις μεταθέσεις των μεταβλητών της.Όμως, αντίθετα με τον Ruffini, απέδειξε το βασικό θεώρημα ότι οι συντελεστές της επιλύουσας εξίσωσης θα είναι πάντοτε ρητοί, κάτι που δεν είχε απασχολήσει ούτε τον Lagrange αφού το θεωρούσε δεδομένο. Στην απόδειξη του, ο Abel χρησιμοποιεί τα θεωρήματα που έχουν αποδείξει οι Cauchy και Lagrange. Αλλά ενώ χρησιμοποιεί τα αποτελέσματά τους, αποφεύγει τη μεθοδολογία τους. Στο έργο του ο Abel χρησιμοποιεί ελάχιστα τις μεταθέσεις με σαφή τρόπο. Χρησιμοποιεί την ορολογία και τον συμβολισμό κατά την αναπαραγωγή των αποτελεσμάτων του Cauchy, σχετικά με το

πλήθος των τιμών που μπορεί να έχει μια αλγεβρική παράσταση, αλλά εκτός από αυτό το μέρος, μιλάει απλά και μόνο για "εναλλαγή" όρων.

Ο Abel δεν έπαψε να ασχολείται με τις πολυωνυμικές εξισώσεις, ακόμα και μετά την απόδειξη του θεωρήματος για το οποίο είναι γνωστός μέχρι και σήμερα. Αντιθέτως όπως γίνεται φανερό και από μια επιστολή του που έστειλε το 1826 στον φίλο του και δάσκαλό του Bernt Holmboe:

> Τώρα εργάζομαι πάνω στην θεωρία των εξισώσεων, που είναι το αγαπημένο μου θέμα, και μου φαίνεται ότι επιτέλους βρήκα τα μέσα να λύσω το γενικό πρόβλημα, που είναι να καθοριστεί η μορφή όλων των αλγεβρικών εξισώσεων που μπορούν να επιλυθούν με ριζικά.

Δύο μήνες πριν το θάνατό του το 1829, ο Abel δημοσίευσε στο Μαθηματικό περιοδικό του Crelle μία εργασία με τίτλο *Mémoire sur une classe particulière d'équations résolubles algébriquement* στην οποία αποδεικνύει ότι:

> Αν οι ρίζες μιας εξίσωσης σχετίζονται μεταξύ τους με τέτοιο τρόπο ώστε όλες αυτές οι ρίζες να μπορούν να εκφραστούν ως ρητή συνάρτηση της μίας εξ' αυτών, την οποία παριστάνουμε με x και αν επιπλέον, μετά τον καθορισμό οποιονδήποτε άλλων δύο ριζών με θx και $\theta_1 x$, έχουμε
>
> $$\theta\theta_1 x = \theta_1\theta x$$
>
> τότε η υπό μελέτη εξίσωση θα είναι πάντοτε αλγεβρικά επιλύσιμη.Επιπλέον αν υποθέσουμε ότι η εξισωση είναι ανάγωγη και ότι ο βαθμός της μπορεί να εκφραστεί ως
>
> $$\alpha_1^{\nu_1}\alpha_2^{\nu_2}\dots\alpha_\omega^{\nu_\omega}$$
>
> όπου $\alpha_1, \alpha_2, \dots \alpha_\omega$ είναι διαφορετικοί πρώτοι, τότε μπορούμε να ελαττώσουμε τη λύση αυτής της εξίσωσης στην επίλυση ν_1 εξισώσεων βαθμού α_1, ή ν_2 εξισώσεων βαθμού α_2 και λοιπά.

Στη σύγχρονη ορολογία η εργασία του αυτή κατοχυρώνει την μη επιλυσιμότητα με ριζικά των εξισώσεων εκείνων, των οποίων η Ομάδα Galois ειναι αβελιανή. Στην παραγματικότητα το όνομα του Abel συνδέθηκε με την αντιμεταθετικότητα μέσα από αυτή την εργασία του.

2.1.4 Cauchy

Στην ιστορία της εξέλιξης της Θεωρίας Galois, ο Augustin-Louis Cauchy κάνει ορισμένες εμφανίσεις. Αν και σε καμία από αυτές δεν ασχολείται με την επίλυση των αλγεβρικών εξισώσεων, η εργασία του πάνω στις μεταθέσεις πρόσφερε πολύτιμες ιδέες σε όσους μεταγενέστερα ασχολήθηκαν με την Θεωρία αυτή.[8]

Το πρώτο εγχείρημα του Cauchy έγινε στις 30 Νοεμβρίου του 1812 με μία εργασία που παρουσίασε στην Ακαδημία Επιστημών του Παρισιού με τίτλο *"Essai sur les Fonctions Symmétriques"* την οποία και εξέδωσε σε δύο μέρη το 1815 στο περιοδικό: *Journal de l'Ecole Polytechnique*. Η έκδοση αυτή ήταν διαθέσιμη στον Galois και οι ιδέες που περιείχε σχετικά με τις μεταθέσεις, αν και σε εμβρυακό στάδιο ακόμα, είναι εμφανείς στην περαιτέρω ανάπτυξη της Θεωρίας Ομάδων, όμως δεν υπάρχει πουθενά σαφής αναφορά ή άλλη ένδειξη ότι ο Galois πράγματι είχε μελετήσει την εργασία αυτή. Αν και πηγή έμπνευσης του Cauchy για την εργασία αυτή είναι η θεωρία των εξισώσεων, όπως μελετήθηκε από τους Lagrange, Vandermonde και Ruffini τους οποίους και αναφέρει ο ίδιος στην εισαγωγή του, παρ' όλα αυτά δεν αναφέρει τίποτα για την επιλυσιμότητα των εξισώσεων αφήνοντας να εννοηθεί ότι στόχος του είναι η καθαρή μελέτη των τιμών που μπορεί να πάρει μια συνάρτηση πολλών μεταβλητών κάτω από την επιρροή των μεταθέσεων χωρίς να ενδιαφέρεται για κάποια εφαρμογή τους.

Το ένα μέρος είχε τίτλο *'Mémoire sur le nombre des valeurs qu'une fonction peut acquérir, lorsqu'on y permute de toutes les manières possibles les quantités qu'elle renferme'*[5]. Σ' αυτό ο Cauchy αρχικά εισάγει, για πρώτη φορά, τον συμβολισμό των μεταθέσεων με δύο γραμμές ο οποίος διατηρείται ακόμα και σήμερα. Τέτοιος συμβολισμός δεν υπάρχει ούτε στο έργο του Lagrange ούτε στου Ruffini. Δίνει τους ακόλουθους ορισμούς: μία μετάθεση (*permutation*) είναι μία δεδομένη διάταξη n στοιχείων ή μεταβλητών, ενώ μια αντικατάσταση (*substitution*) είναι η μετάβαση από μια μετάθεση $A_1 = 1.2.4.3$ σε μία άλλη $A_2 = 2.4.3.1$ την οποία συμβολίζει με $\binom{1.2.4.3}{2.4.3.1}$ ή $\binom{A_1}{A_2}$. Αυτός ο νέος συμβολισμός επέτρεπε τον αλγεβρικό χειρισμό των πράξεων των μεταθέσεων χωρίς να αναφέρονται τα στοιχεία των διατάξεων. Έτσι ο Cauchy καταφέρνει να δώσει επίσης τον ορισμό του γινομένου δύο μεταθέσεων, της ταυτοτικής μετάθεσης, της τάξης μιας μετάθεσης, την κυκλική μετάθεση, καθώς και αυτόν μιας αντιμετάθεσης. Σκοπός

[8]πηγές από [33], [7], [25]

του ήταν η μελέτη συναρτήσεων που μπορούσαν να πάρουν μόνο τρεις τιμές. Έτσι όταν έχουμε τρεις μεταβλητές μπορούμε να βρούμε άπειρο πλήθος τέτοιων συναρτήσεων όπως οι: $a_1a_2 + a_3$, $a_1(a_2 + a_3)$, κ.α. Με όμοιο τρόπο μπορούμε να βρούμε συναρτήσεις με τη ζητούμενη ιδιότητα που να έχουν τέσσερις μεταβλητές όπως οι: $a_1a_2 + a_3a_4$ ή $(a_1 + a_2)(a_3 + a_4)$. Όμως για τις πέντε μεταβλητές δεν υπάρχουν συναρτήσεις που να παίρνουν μόνο τρεις ή τέσσερις τιμές, όπως είχε ήδη δείξει ο Ruffini στην εργασία του *'Teoria general delle equazioni'* του 1799 και την *'Risposta'* του 1805 τις οποίες αναφέρει και ο ίδιος ο Cauchy. Θέλοντας να επεκταθεί, επιχείρησε να αποδείξει ένα πιο γενικό θεώρημα: Το πλήθος των τιμών που παίρνει μια μη-συμμετρική συνάρτηση n μεταβλητών μπορεί να είναι 1 ή 2, αλλιώς δεν μπορεί να είναι λιγότερο από τον μεγαλύτερο πρώτο p που περιέχεται στον n (εννοώντας τον μεγαλύτερο πρώτο που είναι όμως μικρότερος ή ίσος του n). Η απόδειξη δόθηκε σε τρία στάδια:

i/ αν μια συνάρτηση παίρνει λιγότερες από p τιμές, τότε αυτές δεν μεταβάλλονται από καμία μετάθεση τάξης p

ii/ αν οι τιμές της δεν μεταβληθούν από οποιαδήποτε μετάθεση τάξης p, τότε δεν μεταβάλλονται από κανέναν 3-κύκλο

iii/ αν οι τιμές της δεν αλλάξουν από κανέναν 3-κύκλο, τότε η συνάρτηση μπορεί να πάρει μόνο 1 ή 2 τιμές.

Ο Cauchy καταλήγει με μια πιο ισχυρή εικασία: ότι για $n \geq 5$ το πλήθος των τιμών μπορεί να είναι 1 ή 2 αλλιώς όχι λιγότερο από το ίδιο το n.

Το 2ο μέρος που εμφανίστκε αμέσως μετά ονομαζόταν *'Mémoire sur les fonctions qui ne peuvent obtenir que deux valeurs inégales'*. Εκεί ο Cauchy μελετούσε συναρτήσεις της μορφης $(a_1 - a_2)(a_2 - a_3)\dots(a_{n-1} - a_n)$ οι οποίες παίρνουν δύο τιμές που διαφέρουν μόνο στο πρόσημο. Με αυτό τον τρόπο ουσιαστικά καθιέρωσε την θεωρία των διακρινουσών ως εναλλάσουσες συμμετρικές συναρτήσεις. Σ'αυτό το πλαίσιο επισήμανε την ταυτότητα:

$$a_2a_3^2 + a_3a_1^2 + a_1a_2^2 - a_3a_2^2 - a_2a_1^2 - a_1a_3^2 = (a_2 - a_1)(a_3 - a_1)(a_3 - a_2)$$

η οποία είχε ήδη δοθεί και από τον Vandermonde. Γι αυτόν τον λόγο το όνομά του συνδέθηκε με την ορίζουσα:

$$\begin{vmatrix} 1 & 1 & 1 \\ a_1 & a_2 & a_3 \\ a_1^2 & a_2^2 & a_3^2 \end{vmatrix}$$

Τα επόμενα 30 χρόνια, ο Cauchy δεν ξαναασχολήθηκε με το πλήθος των τιμών που μπορεί να πάρει μια συνάρτηση. Αυτό, μέχρι το 1845 όπου έλαβε προς επιμέλεια μία εργασία του Joseph Bertrand, ο οποίος εργάστηκε πάνω στην εικασία που είχε κάνει ο Cauchy το 1815, ότι η τάξη (όπως θα ονομάζαμε με τη σύγχρονη ορολογία) μιας μη τετριμμένης ομάδας n στοιχείων είναι τουλάχιστον ίση με n. Το ενδιαφέρον του Cauchy ανανεώθηκε, και πάλι, και από τις 15 Σεπτεμβρίου του 1845 μέχρι τις 11 Απριλίου του 1846 εξέδωσε 25 δικά του συγγράμματα σχετικά με το θέμα, συνολικά σχεδόν 300 σελίδων επεκτείνοντας τα προηγούμενα αποτελέσματά του. Το παράξενο είναι ότι δεν ανέφερε τίποτε σχετικά με τις παλιές του εργασίες αλλά ξεκίνησε εκ νέου τη μελέτη. Αυτές οι νέες έρευνες τον οδήγησαν, σχεδόν αμέσως, στη δημιουργία της έννοιας ενός "συστήματος συνδυασμένων μεταθέσεων" (*"système des substitutions conjuguées"*), το οποίο ανέφερε πρώτος ο Galois με το όνομα που είναι γνωστό έως σήμερα ως "ομάδα" μεταθέσεων.

2.2 Ομάδα Galois

2.2.1 Galois

Τι είχε μελετήσει ο Galois

Αν και ο Évariste Galois[9] έχει την ιδιότητα (ή τον τίτλο αν θέλει κάποιος) του Μαθηματικού, τόσο εκ των υστέρων όσο και κατά τη διάρκεια του βίου του, εν τούτοις δεν είχε ποτέ την αντίστοιχη ακαδημαϊκή μόρφωση (τουλάχιστον όχι ολοκληρωμένα) σε τυπικό επίπεδο.

Σύμφωνα με τον Dupuy[10][9] η πρώτη του επαφή με τα Μαθηματικά πρέπει να έγινε κατά τη διάρκεια του τρίτου έτους φοίτησής του στο Λύκειο: *Louis-le-Grand* όταν ήταν 15 χρονών. Λόγω διαρκούς ασθένειας υποχρώθηκε να επαναλάβει κάποια μαθήματα Ρητορικής του προηγούμενου έτους. Έτσι του δόθηκε η ευκαιρία να παρακολουθήσει ταυτόχρονα προπαρασκευαστικά μαθήματα Μαθηματικών που δίδασκε ο κ.Vernier και στη συνέχεια ο κ.Richard, ο οποίος αναγνωρίζοντας το ταλέντο και τις πραγματικές ικανότητες του μαθητή του, τον καθοδήγησε να ασχοληθεί με ανώτερα θέματα των Μαθηματικών. Από μαρτυρίες συμμαθητών του γνωρίζουμε ότι

[9] αναφορά από το [29]

[10] τον πρώτο βιογράφο του Galois.

διάβασε με μεγάλη ευκολία τα στοιχειώδη εγχειρίδια που διδάσκονταν. Ανάμεσά τους και την Γεωμετρία (*"Éléments de géométrie"*) του Legendre, έργο που αναπτύσει σε βάθος κάποια ζητήματα των ανώτερων Μαθηματικών, την οποία διάβασε εξαντλώντας την από άκρη σε άκρη. Επειδή τα εγχειρίδια την Άλγεβρας δεν τον ικανοποιούσαν, αφού δεν έβρισκε σ'αυτά ούτε την αυθεντία των συγγραφέων, ούτε τα βήματα που είχαν ακολουθήσει οι πραγματικοί εξερευνητές της, στράφηκε στη μελέτη κλασσικών συγγραμμάτων από καταξιωμένους Μαθηματικούς. Και σε αυτόν τον κλάδο επέλεξε πάλι, σύμφωνα με τις μαρτυρίες, τον Legendre και συγκεκριμένα τα έργα του: *"Résolution des équations numériques"*, *"Théorie des fonctions analytiques"*, καθώς και το έργο του *"Leçons sur le calcul des fonctions"* το οποίο αναφέρει και ο ίδιος ο Galois σε ένα χειρόγραφό του.

Δυστυχώς, επειδή Galois δεν είχε εκπαιδευτεί για να επικαλείται τις πηγές του και όπως φαίνεται από τα γραπτά του δεν είχε κανένα ένα έμφυτο ένστικτο να το πράξει, δεν μπορούμε να γνωρίζουμε τι ακριβώς είχε διαβάσει. Έτσι δεν υπάρχουν άλλες σαφείς αναφορές για άλλα συγγράμματα, όμως πρέπει να θεωρηθεί πολύ πιθανό ότι απέκτησε τις γνώσεις του πάνω στην αλγεβρική θεωρία των πολυωνυμικών εξισώσεων, μέσα από τα καθιερωμένα βιβλία της εποχής που διδάσκονταν στην φημισμένη *École polytechnique*, όπως τα *"Élémens d'algèbre"* και *"Complément des Élémens d'algèbre"*του Lacroix, ή άλλων, όπως το *"Cours de mathématiques"* του Bezout, το *"Élémens d'Algèbre"* του Clairaut και του Euler. Προφανώς διάβασε επίσης κάποια τεύχη των βασικών περιοδικών της εποχης, όπως το *"Annales de Mathématiques pures et appliquées"* του Gergonne και το *"Bulletin des Sciences Mathématiques, Physiques et Chimiques"* του Férussac στο οποίο δημοσιεύονταν παρουσιάσεις της Ακαδημίας Επιστημών.

Θα ήταν ενδιαφέρον να γνωρίζαμε με απόλυτη σιγουριά αν ο Galois είχε διαβάσει το έργο με τη μεγαλύτερη επιρροή σε όλους όσους ασχολήθηκαν με την αλγεβρική επίλυση των πολυωνυμικών εξισώσεων, το *"Réflexions sur la résolution algébrique des équations'"* του Lagrange.

Μπορούμε να είμαστε σίγουροι, ότι είχε γνώση του έργου του Gauss *"Disquisitiones arithmeticae"*, όχι επειδή αναφέρει ρητά το έργο, αλλά επειδή, για την πλειοψηφία των αναφορών του Galois στον Gauss, αυτό είναι το μόνο έργο που έχει σχέση με τα αναφερόμενα. Ίσως να του ήταν γνωστό βέβαια και επειδή κάποια αποτελέσματά του συμπεριλαμβάνονταν στα εγχειρίδια του Lacroix που προαναφέρθηκαν.

Μπορούμε επίσης να είμαστε βέβαιοι ότι είχε διαβάσει τα δύο άρθρα που εξέδωσε ο Cauchy το 1815 στο περιοδικό: *Journal de l'Ecole Polytechnique* για τις μεταθέσεις, τόσο γιατί αναφέρεται ρητά σε ένα σημείο της Πρότασης VII του *Premier Mémoire*, αλλά και επειδή συζητά θέματα μέσα από αυτά. Επίσης αν και δεν υιοθετεί το συμβολισμό του Cauchy, η γλώσσα που χρησιμοποιείται από το άρθρο για τις αντικαταστάσεις και τις μεταθέσεις είναι ταυτόσημη.

Τα γραπτά του Galois

Πέντε εργασίες των μαθηματικών του Galois δημοσιεύτηκαν κατά τη διάρκεια της ζωής του. Η πρώτη είχε τίτλο "Démonstration d'un Théorème sur les Fractions Continues Périodiques" και δημοσιεύτηκε τον Απρίλιο του 1829, όταν ήταν μόλις 17½χρονών, στο περιοδικό *"Annales de Mathématiques pures et appliquées"* του Gergonne. Οι επόμενες τρείς δημοσιεύτηκαν στο επίσης γνωστό για την εποχή περιοδικό *"Bulletin des Sciences Mathématiques, Physiques et Chimiques"* του Férussac, από τον Απρίλιο μέχρι τον Ιούνιο του 1830 και είχαν τους τίτλους: 'Analyse d'un Mémoire sur la résolution algébrique des équations', 'Note sur la résolution des équations numériques' και 'Sur la théorie des nombres'. Η τελευταία ήταν πάλι στο *"Annales"* του Gergonne το Δεκέμβριο του 1830 με θέμα από την Ανάλυση: 'Notes sur quelques points d'analyse'.

Τα πιο σημαντικά έργα, όμως, δημοσιεύτηκαν μετά το θάνατο του. Στις 29 Μαΐου 1832, την παραμονή της μοιραίας μονομαχίας, ο Galois έγραψε το διάσημο γράμμα-διαθήκη στον φίλο του Auguste Chevalier. Ένα γράμμα όπου συνοψίζονται τα μαθηματικά που ήταν αποθηκευμένα στο μυαλό του και που στην ουσία, ζητούσε από τον Chevalier να τα δημοσιοποιήσει. Η επιστολή αυτή έχει δημοσιευθεί, όπως Galois είχε ζητήσει, το Σεπτέμβριο του 1832 στην *"Revue Encyclopédique"*. Για να γίνουμε πιο συγκεκριμένοι του γράφει:

> Αγαπητέ μου φίλε,
> Έχω κάνει αρκετά νέα πράγματα στην ανάλυση.
> Μερικά αφορούν την θεωρία των εξισώσεων, άλλα τις ολοκληρωτικές συναρτήσεις.
> Στη θεωρία των εξισώσεων κοίταξα για τις συνθήκες υπό τις οποίες οι εξισώσεις είναι επιλύσιμες με ριζικά, αυτό μου έδωσε την ευκαιρία να εμβαθύνω αυτή τη θεωρία και να περιγράψω όλους τους δυνατούς μετασχηματισμούς μιας εξίσωσης, ακόμη και σε περίπτωση που δεν είναι επιλύσιμη

> με ριζικά.
> Θα μπορούσαν να γίνουν τρεις εργασίες από όλα αυτά.
> Η πρώτη είναι ήδη γραμμένη, και παρά τα όσα έχει πει γι αυτή ο Poisson, την κρατάω μαζί με τις διορθώσεις που της έχω κάνει.
> Η δεύτερη περιέχει μερικές αρκετά ενδιαφέρουσες εφαρμογές της θεωρίας εξισώσεων. Ιδού μια περίληψη από τα πιο σημαντικά από αυτά.
> ...
> Η τρίτη αφορά τα ολοκληρώματα.

Στη συνέχεια ο Joseph Liouville εξέδωσε το 1846 τα κύρια έργα του Galois, τα οποία του εμπιστεύτηκε ο Chevalier, στο περιοδικό *"Journal de Mathématiques pures et appliquées"* που είχε ιδρύσει ο ίδιος το 1835 με τον χαρακτηριστικό τίτλο Œuvres Mathématiques d'Évariste Galois'. Περιείχε τα έργα:

- 'Sur la théorie des nombres' που είχε ήδη εκδοθεί το 1830 και στο οποίο ο Galois παρουσίαζε αυτό που μετέπειτα θα ονομαζόταν Θεωρία των Πεπερασμένων Σωμάτων.

- 'Mémoire sur les conditions de résolubilité des équations par radicaux', πιο γνωστό στη βιβλιογραφία ως *Premier Mémoire*, είναι η εργασία που αναφέρει ως πρώτη εκ των τριών ο ίδιος ο Galois και την οποία απέρριψε η Ακαδημία των Επιστημών, επιστρέφοντάς την στον συγγραφέα της. Περιέχει βασικά μέρη της θεωρίας που σήμερα ονομάζουμε Θεωρία Galois.

- 'Des équations primitives qui sont solubles par radicaux' επίσης γνωστό στη βιβλιογραφία ως *Second Mémoire*, ειναι η εργασία που αναφέρει ως δεύτερη εκ των τριών και περιέχεται στο τελευταίο γράμμα του.

- την επιστολή της 29ης Μαΐου 1832 στον Auguste Chevalier γνωστή ως *Lettre testamentaire*.

Τα παραπάνω έργα του Galois όπως δημοσιεύθηκαν από τον Liouville, ανατυπώθηκαν και έχουν εκδοθεί σε μορφή βιβλίου από τον Picard το 1897 για λογαριασμό της Société de Mathématique de France.[40]

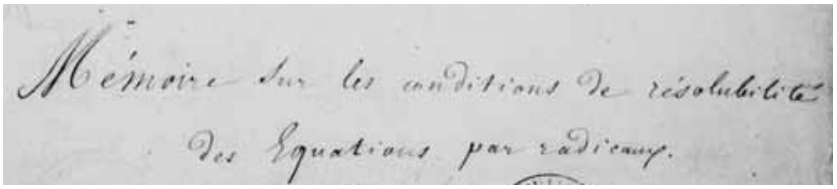
Από τα παραπάνω, θα εξετάσουμε αναλυτικότερα τα Premier και Second Mémoire, αφού σ'αυτά αναπτύσσει ο Galois το κύριο μέρος του έργου του.

Premier Mémoire

Το έτος 1829, στις 25 Μαΐου, ο Galois υπέβαλε την έρευνά του σχετικά με την αλγεβρική λύση των εξισώσεων στην Ακαδημία Επιστημών της Γαλλίας. Ο Cauchy, μέλος της Ακαδημίας και καθηγητής στην École Polytechnique, διορίστηκε να εξετάσει το έγγραφο. Έχασε όμως το χειρόγραφο, κι έτσι ένα δεύτερο έγγραφο υποβλήθηκε μια εβδομάδα αργότερα την 1 Ιουνίου. Αυτά τα χειρόγραφα δεν έχουν ποτέ βρεθεί.[11] Επειδή δεν λάμβανε καμία απάντηση, έστειλε μια νέα εκδοχή των ερευνών του τον Φεβρουάριο του 1830. Αυτή τη φορά η Ακαδημία εμπιστεύθηκε τον Fourier για να κρίνει την εργασία, όμως πέθανε λίγο αργότερα χωρίς να προλάβει να διαβάσει το χειρόγραφο, το οποίο επίσης δεν βρέθηκε ποτέ. Στις 17 Ιανουαρίου του 1831 υπέβαλε για τρίτη φορά την ίδια εργασία. Ύστερα από μήνες χωρίς απόκριση ο Galois παραπονέθηκε στον ίδιο τον Πρόεδρο της Ακαδημίας, λαβάνοντας ως απάντηση την απόρριψή της στις 4 Ιουλίου του 1831, όταν ο Galois ήταν στην φυλακή. Η κριτική της εργασίας του έγινε από τους Lacroix και Poisson οι οποίοι έγραψαν μεταξύ άλλων στην αναφορά τους:[12]

> Η προϋπόθεση για την επιλυσιμότητα, αν υπάρχει, θα έπρεπε να έχει έναν εξωτερικό χαρακτήρα που μπορεί να επαληθευθεί από την εξέταση των συντελεστών μιας συγκεκριμένης εξίσωσης ή, ακόμη καλύτερα, με την επίλυση άλλης εξίσωσης μικρότερου βαθμού από εκείνη την εξίσωση που πρέπει να επιλυθεί.

Τελικά όπως ήδη έχει αναφερθεί η εργασία αυτή εκδόθηκε, για πρώτη φορά το 1846, με τίτλο *'Mémoire sur les conditions de résolubilité des équations par radicaux'* από τον Liouville.[41] Όπως προλογίζει στην



Εικόνα 2.1: Ο τίτλος του Premier Mémoire από το χειρόγραφο του Galois

εργασία του και ο ίδιος ο Galois, αυτή αποτελείται από δύο μέρη: το

[11]σύμφωνα με το [20]

[12]αναφορά από [35], όπου υπάρχει η πλήρη αναφορά τους στις σελίδες 120-122.

πρώτο περιέχει τις γενικές αρχές της θεωρίας του και έχει τον τίτλο *"PRINCIPES"* και το δεύτερο έχει μία εφαρμογή μόνο της θεωρίας του και έχει τον τίτλο *"Application aux équations irréductibles de degré premier."*[13]

Η εργασία ξεκινάει με κάποιους ορισμούς τους οποίους ο Galois κρίνει απαραίτητο ότι πρέπει να δώσει. Αντιλαμβάνόμενος ότι η έννοια της αναγωγιμότητας ενός πολυωνύμου είναι καθοριστικής σημασίας αναφέρει:

Ορισμός 2.2.1. Μία εξίσωση ονομάζεται αναγώγιμη *(réductible)* όταν δέχεται ρητούς διαιρέτες. Σε αντίθετη περίπτωση ονομάζεται ανάγωγη *(irréductible)*.

Αμέσως μετά δίνει μια αναλυτική εξήγηση για τη λέξη "ρητός" που χρησιμοποιεί, αφού όπως παραδέχεται θα εμφανιστεί συχνά στην εργασία. Όσον αφορά τις εξισώσεις που έχουν ως συντελεστές ρητούς αριθμούς, αυτές απλά μπορούν να αναλυθούν σε παράγοντες με ρητούς επίσης συντελεστές. Όταν όμως η εξίσωση δεν έχει όλους τους συντελεστές ρητούς αριθμούς, τότε πρέπει να θεωρήσουμε ως ρητό διαιρέτη αυτόν που οι συντελεστές του μπορούν να παρασταθούν από μια ρητή συνάρτηση των αρχικών συντελεστών. Επεκτείνει την έννοια των ρητών διαιρετών κάνοντας την συμφωνία να δεχόμαστε ως ρητή κάθε συνάρτηση ενός συγκεκριμένου πλήθους ποσοτήτων, καθορισμένων εκ των προτέρων, μαζί με τους συντελεστές της εξίσωσης, όπως για παράδειγμα την ρίζα ενός αριθμού. Τότε θα λέμε ότι οι ποσότητες αυτές προσαρτώνται ή επισυνάπτονται *(adjoint)* στην εξίσωση. Δίνει έτσι, με τη δική του ορολογία βέβαια, αυτό που σήμερα γνωρίζουμε ως επέκταση του σώματος των συντελεστών ενός πολυωνύμου. Για να κάνει εμφανή τη χρησιμότητα της επισύναψης κάποιας ποσότητας σε μια εξίσωση δίνει ως παράδειγμα το κυκλοτομικό πολυώνυμο:

$$\frac{x^n - 1}{x - 1} = 0 \quad \text{,όπου n πρώτος} \tag{2.37}$$

το οποίο αν και είναι αρχικά ανάγωγο στο σώμα των συντελεστών, αν επισυνάψουμε μια πρωταρχική ν-στη ρίζα της μονάδας, όπως έχει δείξει ο Gauss, τότε παραγοντοποιείται στο νέο επεκτεταμένο σώμα.

Στη συνέχεια μιλάει για τις μεταθέσεις και τις αντικαταστάσεις χρησιμοποιώντας, χωρίς όμως να το αναφέρει ρητά, τους ορισμούς που δίνει ο Cauchy στα άρθρα του 1815[5].

[13]αναλυτική μελέτη της εργασίας με σύχγρονο συμβολισμό στο [30]

Ορισμός 2.2.2. Αν a,b,c,... ένα πλήθος n μεταβλητών, τότε:

- Μία διάταξη των μεταβλητών ονομάζεται μετάθεση *(permutation)*
- Η αλλαγή μιας μετάθεσης από μία άλλη ονομάζεται αντικατάσταση *(substitution)*

Το γεγονός ότι η λέξη "αντικατάσταση" του παραπάνω ορισμού είναι η μετάθεση με τη σύγχρονη ορολογία, ενώ η "μετάθεση" όπως δίνεται από τον παραπάνω ορισμό δεν χρησιμοποιείται πλέον, σε συνδυασμό με το ότι και η χρήση των λέξεων αυτών στο έργο του Galois δεν γίνεται με την πρέπουσα συνέπεια αφού ενίοτε χρησιμοποιεί τη λέξη "μετάθεση" αντί της "αντικατάστασης", προσδίδει μια επιπλέον δυσκολία στην κατανόηση του κειμένου τόσο στον σύγχρονο αναγνώστη όσο και στον αναγνώστη της εποχής του.

Ο τελευταίος ορισμός αρχίζει με τη φράση:

> *Quand nous voudrons **grouper** des substitutions, nous les ferons toutes provenir d'une même permutation.*
> ...
> *Donc, si dans un pareil **groupe** on a les substitutions S et T, on est sûr d'avoir la substitution ST.*

που σημαίνει:

> Όταν θέλουμε να **ομαδοποιήσουμε** τις αντικαταστάσεις, θα το κάνουμε ώστε όλες να προέρχονται από την ίδια μετάθεση.
> ...
> Έτσι, αν σε μία παρόμοια **ομάδα** έχουμε τις αντικαταστάσεις S και T, είμαστε σίγουροι ότι θα έχουμε και την αντικατάσταση ST.

Εδώ ο Galois χρησιμοποιεί για πρώτη φορά τη λέξη "ομάδα", δίνοντάς της την ιδιότητα της κλειστότητας, η οποία είναι από τότε, ακόμα σε χρήση, στη σύγχρονη γλώσσα των Μαθηματικών. Επειδή όμως δεν χρησιμοποιεί τον συμβολισμό του Cauchy για τις αντικαταστάσεις, δεν γράφει την ομάδα ως ένα σύνολο αντικαταστάσεων αλλά με τη μορφή ενός πίνακα μεταθέσεων[14]. Για παράδειγμα ο πίνακας

$$\begin{matrix} a & b & c & d \\ b & a & d & c \\ c & d & a & b \\ d & c & b & a \end{matrix}$$

[14]δηλαδή διατάξεων με την σύγχρονη έννοια.

περιγράφει, σύμφωνα με το Galois, την ομάδα των τεσσάρων στοιχείων του Klein (δηλαδή τη $V_4 = \{identity, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}$). Με άλλα λόγια ο Galois δίνει στην πραγματικότητα την τροχιά μιας δράσης της ομάδας σε μία μετάθεση[15].

Μετά τους ορισμούς, το πρώτο μέρος της εργασίας συνεχίζεται με την παρουσίαση και απόδειξη[16] τεσσάρων βοηθητικών Λημμάτων και πέντε Προτάσεων οι οποίες αποτελούν την καρδιά αυτού που σημερα ονομάζουμε "Θεωρία Galois".

Λήμμα 2.2.1. *Μια ανάγωγη εξίσωση δεν μπορεί να έχει καμία κοινή ρίζα με μια ρητή εξίσωση, χωρίς να την διαιρεί.*

Δηλαδή αν ένα ανάγωγο πολυώνυμο $P(x)$ έχει μία κοινή ρίζα με ένα πολυώνυμο $f(x)$, τότε μπορούμε να γράψουμε $f(x) = P(x) \times Q(x)$. Για παράδειγμα το πολυώνυμο $P(x) = x^2 + 1$ είναι ανάγωγο στο $\mathbb{R}$, αφού οι ρίζες του i και $-i$ ανήκουν στο σύνολο των Μιγαδικών αριθμών. Όμως το πολυώνυμο $f(x) = x^3 - x^2 + x - 1$ έχει επίσης τις ίδιες ρίζες στο $\mathbb{C}$ και παραγοντοποιείται στο $\mathbb{R}$ καθώς έχει ρίζα το 1, έτσι μπορούμε να γράψουμε: $f(x) = P(x)(x - 1)$.

Κατά τον Radloff[30] τα τρία επόμενα Λήμματα αποδεικνύουν το Θεώρημα του Πρωταρχικού Στοιχείου *(Primitive Element Theorem)* της σύγχρονης Θεωρίας Σωμάτων.

Η πρώτη πρόταση της "Θεωρίας" ορίζει την ομάδα μιας εξίσωσης ως ομάδα των μεταθέσεων των ριζών. Έτσι:

Προταση 2.2.1. *Έστω μια δεδομένη εξίσωση και a, b, c, ... οι m ρίζες της. Υπάρχει πάντοτε μία ομάδα μεταθέσεων των γραμμάτων a, b, c, ... που ικανοποιεί την ακόλουθη ιδιότητα:*

1. *Κάθε συνάρτηση των ριζών, αναλλοίωτη από τις αντικαταστάσεις της ομάδας αυτής, να είναι γνωστή.*

2. *Αντιστρόφως, κάθε συνάρτηση των ριζών, ρητά καθορισμένη, να είναι αναλλοίωτη από τις αντικαταστάσεις.*

Πριν από την απόδειξη της πρότασης, ο Galois, δίνει δύο παραδείγματα τέτοιων ομάδων μεταθέσεων. 1ο) Για τις αλγεβρικές εξισώσεις αναφέρει ότι η ομάδα αυτή δεν είναι τίποτε άλλο από το σύνολο των $m! = 1 \times 2 \times 3 \times \cdots \times m$ δυνατών μεταθέσεων[17] των m ριζών της, αφού σ'αυτήν την περίπτωση οι συμμετρικές συναρτήσεις

[15]δηλαδή σε μια διάταξη n στοιχείων
[16]όχι πάντοτε πολύ αυστηρή
[17]δηλαδή των διατάξεων

είναι οι μόνες που καθορίζονται ρητά. 2ο) Στην περίπτωση του κυκλοτομικού πολυωνύμου (2.37) αν θεωρήσουμε ως $a = r, b = r^g, c = r^{g^2}, \cdots$, όπου g μια πρωταρχική ρίζα, τοτε η ομάδα μεταθέσεων θα είναι η εξής:

$$\begin{array}{ccccccc} a & b & c & d & \cdots & \cdots & k \\ b & c & d & \cdots & \cdots & k & a \\ c & d & \cdots & \cdots & k & a & b \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ k & a & b & c & \cdots & \cdots & i \end{array}$$

σε αυτή την περίπτωση, το πλήθος των μεταθέσεων είναι ίσο με το βαθμό της εξίσωσης. Προσπαθώντας να εξηγήσει περισσότερο τι είναι η ομάδα των μεταθέσεων, γράφει στο *"Σχόλιο 1."* ότι δεν πρέπει να θεωρείται σημαντική η διάταξη των γραμμάτων, αλλά μόνο η αντικατάσταση[18] με την οποία περνάμε από τη μία μετάθεση στην άλλη.

Οι Προτάσεις ΙΙ και ΙΙΙ προσδιορίζουν τη σχέση μεταξύ της ομάδας μιας εξίσωση και των ποσοτήτων που επισυνάπτονται σ'αυτήν.

Προταση 2.2.2. *Αν επισυνάψουμε σε μια δεδομένη εξίσωση τη ρίζα r μιας βοηθητικής ανάγωγης εξίσωσης [βαθμού p πρώτου]*[19]*:*

1. *θα συμβούν ένα από τα δύο πράγματα: είτε η ομάδα της εξίσωσης δεν θα αλλάξει, είτε θα διαμερισθεί σε p ομάδες που ανήκουν στην δεδομένη εξίσωση αν της επισυνάψουμε κάθε μία ρίζα της βοηθητικής εξίσωσης.*

2. *αυτές οι ομάδες έχουν την αξιοσημείωτη ιδιότητα ότι μπορούμε να περάσουμε από τη μία στην άλλη εφαρμόζοντας την ίδια αντικατάσταση σε όλες τις μεταθέσεις της πρώτης.*

Στο χειρόγραφο και στην κανονική ροή του κειμένου βρίσκεται η επόμενη

Προταση 2.2.3. *Αν η εξίσωση του r είναι της μορφής $r^p = A$ και οι p-στες ρίζες της μονάδας βρισκονται ανάμεσα στις ήδη προσαρτημένες ποσότητες, οι p ομάδες που αναφέρονται στην Πρόταση ΙΙ έχουν την επιπλέον ιδιότητα, ότι οι αντικαταστάσεις των γραμμάτων με τις οποίες περνάμε από μία μετάθεση σε άλλη μέσα σε κάθε ομάδα θα είναι ίδιες για όλες τις ομάδες.*

[18]δηλαδη η μετάθεση με τη σύγχρονη έννοια

[19]ο Galois αργότερα διέγραψε τις λέξεις στα άγκιστρα

όμως την έχει διαγράψει με προσοχή και στο περιθώριο με ημερομηνία 1832 διατυπώνει ένα πιο γενικό θεώρημα με την ίδια αρίθμηση όπως η προηγούμενη

Προταση 2.2.3. *Αν επισυνάψουμε σε μια εξίσωση όλες τις ρίζες μιας βοηθητικής εξίσωσης, οι ομάδες που αναφέρονται στην Πρόταση ΙΙ θα ικανοποιούν επιπλέον κι αυτή την ιδιότητα, ότι οι αντικαταστάσεις θα είναι ίδιες σε κάθε ομάδα.*

Ακολούθως διατυπώνει την

Προταση 2.2.4. *Αν επισυνάψουμε σε μια εξίσωση την αριθμητική τιμή μιας ορισμένης συνάρτησης των ριζών της, τότε η ομάδα της εξίσωσης ελαττώνεται με τέτοιον τρόπο, ώστε να μην περιέχει άλλες μεταθέσεις εκτός από αυτές που αφήνουν αυτή τη συνάρτηση αναλλοίωτη.*

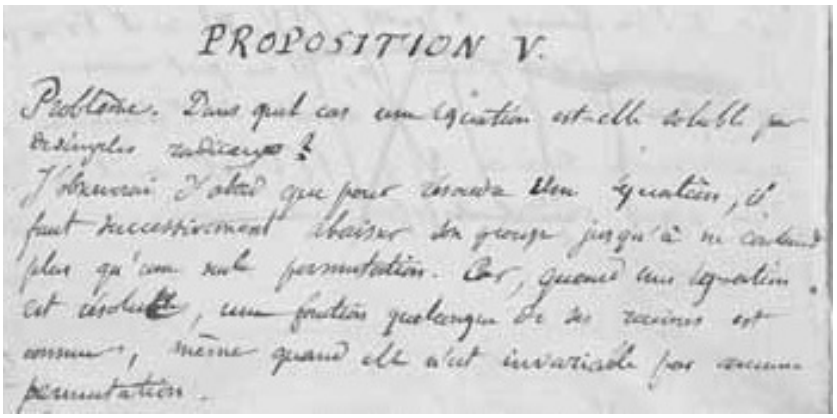
Στην πέμπτη και τελευταία πρόταση της θεωρίας του και πριν τις εφαρμογές της, δίνει την τελική απάντηση στο κεντρικό πρόβλημα της εργασίας του, δηλαδή πότε μια εξίσωση είναι επιλύσιμη με ριζικά.

Προταση 2.2.5. *Για να λύσουμε μια εξίσωση, πρέπει διαδοχικά να ελαττώσουμε την ομάδα της μέχρι να μην περιέχει παρά μία μετάθεση.*

Ωστόσο, αντί να αναφέρει το αποτέλεσμα αυτό ως ένα θεώρημα, ο Galois περιγράφει αλγοριθμικά τον μηχανισμό που συνδέει τη διαδικασία της επισύναψης μιας ποσότητας με εκείνη της ελάττωσης της ομάδας. Ο αφηγηματικός του τρόπος περιγραφής, παραλείποντας τα ενδιάμεσα αποτελέσματα, δίνει μια μη-υπολογιστική απόδειξη η οποία είναι ασυνήθιστη για τους Μαθηματικούς των αρχών του 19ου αιώνα[20]. Έτσι, αν η Πρόταση V παρέχει την κατανόηση του *γιατί* κάποιες εξισώσεις είναι επιλύσιμες και άλλες όχι, δεν λέει *πώς* ξεκινώντας από μια συγκεκριμένη εξίσωση, θα απαντήσουμε στο ερώτημα. Αμέσως μετά δίνει ένα, περιγραφικό πάλι, παράδειγμα για την τεταρτοβάθμια εξίσωση που αφορά φυσικά την επιλυσιμότητα της ομάδας S_4.

Το δεύτερο μέρος περιέχει, όπως λέει και ο ίδιος ο Galois, μια εφαρμογή μόνο της θεωρίας του, στις ανάγωγες εξισώσεις που έχουν βαθμό έναν πρώτο αριθμό. Την παρουσιάζει σε τρεις Προτάσεις, VI, VII και VIII, κάνοντας αντιληπτό ότι δεν χρειάζεται να γνωρίζουμε και να μελετούμε τις ρίζες μιας τέτοιας εξίσωσης, αλλά μόνο την ομάδα της. Τελειώνει γράφοντας ως παράδειγμα την ομάδα των μεταθέσεων που πρέπει να έχει μια εξίσωση πέμπτου βαθμού ώστε να είναι επιλύσιμη.

[20]δικαιολογώντας έτσι απολύτα το σχόλιο των Lacroix και Poisson, κριτών της εργασίας του. βλέπε σελ.75


PROPOSITION V.

Problème. Dans quel cas une équation est-elle soluble par radicaux?

J'observe d'abord que pour résoudre une équation, il faut successivement abaisser des groupes jusqu'à ne contenir plus qu'une seule permutation. Or, quand une équation est résoluble, une fonction quelconque de ses racines est connue, même quand elle n'est invariable par aucune permutation.

Εικόνα 2.2: Η Πρόταση V όπως φαίνεται στο χειρόγραφο του Galois

Second Mémoire

Είναι σχεδόν σίγουρο[21] ότι το Second Mémoire γράφτηκε τον Ιούνιο του 1830. Η πρώτη του δημοσίευση όμως ήταν αυτή του Liouville[41] το 1846. Η αρχική του μορφή είναι ένα ημιτελές προσχέδιο των ιδεών του συγγραφέα του στο οποίο ο ίδιος έδωσε τον τίτλο: *"Des équations primitives qui sont solubles par radicaux"*. Αν και δεν θεωρείται τόσο σημαντικό όσο το Premier Mémoire, το οποίο περιγράφει αυτό που γνωρίζουμε ως Θεωρία Galois, το Second Mémoire επικεντρώνεται κυρίως στην μελέτη των ομάδων και επηρέασε σε σημαντικό βαθμό, μέσω του έργου του Camille Jordan και άλλων, την Θεωρία Ομάδων όπως την μελετούμε σήμερα. Αποτελείται από δύο μέρη. Το πρώτο αφορά τις πεπερασμένες επιλύσιμες εξισώσεις και ομάδες, ενώ το δεύτερο τις ομάδες που σήμερα ονομάζουμε AGL (2, p) και PSL (2, p). Ο Galois χρησιμοποιεί μια ιδιαίτερα εξελιγμένη ορολογία για τη θεωρία ομάδων, πολύ διαφορετική από την ορολογία του πρώτου εγγράφου. Μιλά για τις ομάδες των μεταθέσεων - δηλαδή, των διατάξεων - των ριζών και τις αντικαταστάσεις τους κάνοντας μικρή αναφορά στις εξισώσεις από τις οποίες προήλθαν. Αναφέρεται επίσης, χωρίς ορισμό, σε έννοιες όπως οι πρωταρχικές ομάδες, συζυγείς και γραμμικές ομάδες, οι οποίες δείχνουν ένα επίπεδο εξέλιξης πολύ ανώτερο από εκείνο της πρώτης εργασίας. Δυστυχώς όμως δεν υπάρχει καμία ένδειξη για την προέλευση αυτών των όρων, ούτε ακόμη και της σημασίας τους, κάνοντας την κατανόηση του Second Mémoire πολύ δύσκολη.

Από τον τίτλο της εργασίας, αλλά και από την πρώτη παράγραφο,

[21]αναφορά από το [28]

ο Galois ξεκαθαρίζει το σκοπό του: να αναζητήσει κάτω από ποιές περιπτώσεις μια πρωταρχική εξίσωση *(équation primitive)* είναι επιλύσιμη με ριζικά. Στο μυαλό του Galois, το γραπτό αυτό, δεν αναπτύσσει περαιτέρω τη θεωρίας του, αλλά μάλλον είναι μια εφαρμογή της σε μια συγκεκριμένη κατηγορία εξισώσεων. Και συνεχίζει αναφέροντας ότι το κριτήριο σχετίζεται με το βαθμό της εξίσωσης, ειδικότερα αυτός πρέπει να είναι της μορφής p^ν, όπου p πρώτος. Το επιχείρημά του είναι ότι αν μια πρωταρχική εξίσωση είναι επιλύσιμη με ριζικά τότε, εκτός και εάν έχει βαθμό πρώτο αριθμό, η προσάρτηση απλών ριζικών, μία-μία, πρέπει να οδηγήσει τελικά σε ένα σημείο όπου η εξίσωση παύει να είναι πρωταρχική. Ο Galois χειριζόμενος αποκλειστικά τις ομάδες μεταθέσεων των ριζών και όχι τις εξισώσεις, αν και δεν είχε στη διάθεσή του έναν εύχρηστο συμβολισμό αλλά μόνο λεκτικές περιγραφές, αποδεικνύει, με κάποιες ατέλειες όμως, το αρχικό θεώρημά του. Ας μην ξεχνάμε βέβαια ότι δεν είναι μια δημοσιευμένη από τον ίδιο εργασία, αλλά ένα ημιτελές έργο που άφησε ως κληρονομιά στο τελευταίο του γράμμα, πριν από την μοιραία μονομαχία.

2.3 Επιλύσιμες ομάδες

Από τον θάνατο του Galois, το 1832, έως την έκδοση του έργου του από τον Liouville, το 1846, δεν σημειώνεται καμία εξέλιξη ή οποιαδήποτε άλλη αναφορά πάνω στη Θεωρία Galois. Ο Liouville διοργάνωσε μια σειρά διαλέξεων πάνω σε όσα είχε κατανοήσει από τις ιδέες του Galois, με προοπτική να εκδώσει έναν πλήρη σχολιασμό πάνω σ'αυτές. Ένας από τους λίγους που παρακολούθησαν αυτές τις διαλέξεις ήταν ο Joseph-Alfred Serret ο οποίος το 1849 εξέδωσε το γνωστό για την εποχή του εγχειρίδιο: *"Cours d'algebre supérieure"*. Το βιβλίο δεν περιείχε κάποια παρουσίαση της Θεωρίας Galois, όμως ανέφερε στην εισάγωγή του:

> Ο φίλος μου Liouville μου είπε ότι σχεδιάζει να δημοσιεύσει, κάποια μέρα, ένα σχόλιο πάνω στο σημαντικό αυτό έργο. Μόνο μέσω αυτών των σχολίων, μέρος των οποίων ο Liouville ειχε την καλοσύνη να συζητήσει με εμένα, κατάφερα να κατανοήσω ορισμένα σημεία των απομνημονευμάτων του Galois, τα οποία διαβάζονται μόνο από μαθηματικούς που ασχολούνται ιδιαίτερα με τη θεωρία των εξισώσεων. Μπορεί κανείς να αντιληφθεί το

> δέος το οποίο με εμποδίζει να παρουσιάσω τις ανακαλύψεις του Galois εδώ.

Στην επόμενη έκδοση του ίδιου έργου όμως, το 1849, ο Serret παρουσιάζει μια απόδειξη του 3ου Λήμματος του Galois. Τελικά τα πρώτα σχόλια που εκδόθηκαν σχετικά με το έργο του Galois ήταν το 1852 από τον Enrico Betti, έναν Ιταλό Μαθηματικό, ο οποίος όμως έγραψε στα Ιταλικά κι έτσι δεν είχε άμεση επιρροή στους σύγχρονούς του Γάλλους συναδέλφους.

2.3.1 Betti

Το πρώτο έργο που περιείχε μια εξέλιξη της Θεωρίας Galois είχε τίτλο: *"Sulla risoluzione delle equazioni algebriche"*[2] και εκδόθηκε στην Ιταλία το 1852 από τον Enrico Betti. Εκεί έδινε μια παρουσίαση των ιδεών του Galois, μαζί με μερικές δικές του προσθήκες. Στην εισαγωγή του έργου του ανέφερε χαρακτηριστικά:

> Οι συνθήκες για τη επιλυσιμότητα με ριζικά των εξισώσεων με βαθμό πρώτο αριθμό μπορούν να θεωρηθούν καθορισμένες και αποδεδειγμένες από τις διαδικασίες των δύο αυτών μαθηματικών. Απομένει να καθορισθούν οι συνθήκες για τις εξισώσεις με βαθμό μη πρώτο, αν και πολλές από αυτές προτείνονται από τον Galois και τον Abel με διαφορετικούς τρόπους, χωρίς όμως αποδείξεις, ανάμεσα στα μεταθανάτια χαρτιά τους. Η κάλυψη αυτών των κενών είναι ο κύριος σκοπός της δουλειάς μου.

Όπως είναι αναμενόμενο, το μεγαλύτερο μέρος της εργασίας του Betti αφιερώνεται στην θεωρία των μεταθέσεων, όπου ακολουθείται ο συμβολισμός και η ορολογία που περιέχεται στην εργασία του Cauchy το 1815. Χρησιμοποιεί το σύμβολο

$$\begin{pmatrix} x_i \\ x_{\phi(i)} \end{pmatrix}$$

για να σημειώσει την μετάθεση που σήμερα θα συμβολίζαμε με

$$\begin{pmatrix} x_1 & x_2 & x_3 & \cdots & x_n \\ x_{\phi(1)} & x_{\phi(2)} & x_{\phi(3)} & \cdots & x_{\phi(n)} \end{pmatrix}$$

όπου ϕ είναι μια συνάρτηση των δεικτών και η οποία μπορεί να θεωρηθεί και η ίδια μια μετάθεση των n στοιχείων.

Αναφέρεται φυσικά και σε ομάδες μεταθέσεων όπως ακριβώς τις κατανοούσε και ο Galois. Το γεγονός ότι οι ομάδες των μεταθέσεων ήταν τα κύρια στοιχεία της προσοχής του γίνεται αντιληπτό τόσο από τους ορισμούς που διατυπώνει όσο και από νέες λειτουργίες που επινοεί γι αυτές. Συγκεκριμένα ορίζει ότι δύο ομάδες θα είναι *ίσες* (*eguali*) όταν τα σύνολα των σχετικών μεταθέσεων είναι ίδια, ακόμα και αν τα σύνολα των διατάξεων είναι διαφορετικά, ενώ δύο ομάδες που περιέχουν το ίδιο πλήθος διατάξεων είναι *όμοιες* (*simili*) αν τα σύνολα των σχετικών μεταθέσεων, μολονότι διαφορετικά, περιέχουν το ίδιο πλήθος μεταθέσεων με ίδια τάξη. Επιπλέον επινοεί τον όρο "παράγωγο" (*"derivata"*) της μετάθεσης θ από την μετάθεση ψ, συμβολίζοντας και ορίζοντάς την ως $D_\psi\theta = \psi^{-1}\theta\psi$, μελετώντας στη συνέχεια τις ιδιότητες αυτού του συμβόλου. Το ίδιο σύμβολο το επεκτείνει και στις ομάδες ορίζοντας την ομάδα $D_\psi G = \psi^{-1}G\psi$ ως την ομάδα που "παράγεται από την G μέσω της ψ". Σημειώνει μάλιστα ότι αν μια μετάθεση ψ αντιστοιχεί μία διάταξη που ανήκει στην ομάδα G σε μία διάταξη που ανήκει στην παραγόμενη ομάδα K, τότε η ψ αντιστοιχεί κάθε διάταξη που ανήκει στην ομάδα G μέσα στην K. Έτσι όμοιες ομάδες διατάξεων επάγουν, με σύγχρονη ορολογία, συζυγής ομάδες μεταθέσεων, ενώ ίσες ομάδες διατάξεων επάγουν μια κανονική ομάδα.

Στο δεύτερο μέρος της εργασίας του, ο Betti εισάγει τον όρο *"επιλύουσα του Galois"* (*"risolvente di Galois"*) για την εξίσωση

$$F(V) = 0$$

της οποίας οι ρίζες $V_0, V_1, \cdots$ είναι οι $n!$ διακεκριμένες τιμές που προκύπτουν από τη σχέση $V(x_0, x_1, \cdots)$ κάτω από όλες τις μεταθέσεις των ριζών της εξίσωσης που ζητείται να επιλυθεί. Σχολιάζει επίσης ότι η "επιλύουσα Galois" είναι συνήθως ανάγωγο πολυώνυμο. Παρατηρεί ότι με την προσάρτηση των ριζών μιας κατάλληλα επιλεγμένης βοηθητικής εξίσωσης, δηλαδή της επιλύουσας Galois, η ομάδα της εξίσωσης χωρίζεται σε n όμοια παραγόμενες ομάδες, δηλαδή συζυγής ομάδες. Όταν ο Betti αναφέρει ότι η ομάδα χωρίζεται σε ομάδες δεν εννοεί ότι η ένωση αυτών των ομάδων θα είναι η αρχική, αφού τότε μόνο μία από αυτές θα πρέπει να περιέχει την ταυτοτική μετάθεση. Εννοεί, όπως άλλωστε και ο Galois, ότι το σύνολο των διατάξεων μπορεί να χωριστεί σε σύνολα ξένα μεταξύ τους, με τέτοιο τρόπο, ώστε το σύνολο των μεταθέσεων σε κάθε ένα από αυτά τα ξένα σύνολα να είναι μια ομάδα. Αντιλαμβάνεται στη συνέχεια ότι η επιλυσιμότητα απαιτεί η ομάδα της εξίσωσης να ελαττωθεί μέχρι το σημείο να περιέχει μόνο την ταυτοτική μετάθεση.

Είναι φανερό ότι η ανάπτυξη της θεωρίας Galois από τον Betti ειναι πολύ κοντά στην οπτική του ίδιου του Galois, γι αυτό μπορεί να θεωρηθεί απλά ως ένας σχολιασμός και επεξεργασία των αρχικών ιδεών, παρά μια πρωτότυπη εξέλιξή της. Ο Betti, όπως και ο συμπατριώτης του ο Ruffini, ήταν περιορισμένος μόνο στην επικράτειά του (για να μην πούμε καταδικασμένος) αφού εξέδιδε τις εργασίες του στην Ιταλική γλώσσα η οποία δεν είχε απήχηση στο ρεύμα της Μαθηματικής έρευνας του 19ου αιώνα. Έτσι δεν είναι σαφές ποιά επιρροή είχε η εργασία του Betti στις επόμενες παρουσιάσεις της Θεωρίας Galois. Αν τελικά άσκησε κάποια επιρροή, αυτή ήταν μόνο πάνω στον Jordan, αφού ήταν το μόνο εγχειρίδιο που υπήρχε μέχρι τότε.

2.3.2 Serret

Η πρώτη εμφάνιση της Θεωρίας Galois μέσα σε εγχειρίδιο Άλγεβρας στην Γαλλική γλώσσα έγινε στην τρίτη έκδοση, το 1866, του ήδη καθιερωμένου: *"Cours d'algebre supérieure"*[32] από τον Joseph Alfred Serret. Όπως και στο έργο του Betti, η προσέγγιση ακολουθεί πιστά τον Galois, πράγμα που ομολογεί και ο ίδιος ο Serret:

> Έχω ακολουθήσει τη σειρά των προτάσεων που υιοθέτησε ο Galois, αλλά πολύ συχνά έπρεπε να συμπληρώσω τις ανεπαρκείς αποδείξεις.

Υπάρχουν όμως και διαφορές στην παρουσίαση των στοιχειωδών εννοιών που οφείλονται στην εξέλιξή τους μετά από μια πεντηκονταετία. Για παράδειγμα ο Serret κάνει σαφή διαχωρισμό ανάμεσα στο πολυώνυμο $p(x)$ και την πολυωνυμική εξίσωση $p(x) = 0$. Έτσι σωστά σημειώνει ότι είναι το πολυώνυμο και όχι η εξίσωση που παραγοντοποιείται σε ανάγωγους παράγοντες.

Ο Serret υιοθετεί την ορολογία του Cauchy, "σύστημα συνδυασμένων μεταθέσεων" (*"système des substitutions conjuguées"*), για να δηλώσει τις ομάδες μεταθέσεων όπως είναι γνωστές σήμερα. Είναι το βασικό θέμα που αναπτύσσει και μάλιστα όπως σημειώνει και ο ίδιος:

> Ο Galois χρησιμοποίησε την έννοια των ομάδων των μεταθέσεων[22] .... αλλά φαίνεται καλύτερα για μας να

[22]με τη λέξη "μεταθέσεις", ο Serret όπως και ο Galois, εννοει τις διατάξεις, ενώ με τη λέξη "αντικαταστάσεις" εννοεί τις μεταθέσεις με τη σύγχρονη έννοια.

> κρατήσουμε τις αντικαταστάσεις. Εκτός αυτού, είναι μόνο μια απλή αλλαγή στη διατύπωση των θεωρημάτων, για έχουμε μόνο να εξετάζουμε τις μεταθέσεις από την μεριά των αντικαταστάσεων, με τις οποίες περνάμε από τη μία στην άλλη.

Η βασικότερη συνεισφορά του Serret βρίσκεται στον συμβολισμό. Στα γραπτά του εμφανίζεται για πρώτη φορά ο συμβολισμός που χρησιμοποιούμε σήμερα για τις ομάδες. Έτσι το

$$\Gamma = \{1, S_1, S_2, \cdots, S_{\mu-1}\}$$

είναι μία ομάδα μεταθέσεων. Ενώ η συζυγής της ομάδα[23] είναι η

$$\Gamma_1 = \{1, TS_1T^{-1}, TS_2T^{-1}, \cdots, TS_{\mu-1}T^{-1}\}$$

Ο Serret περιορίζει την μελέτη του, όπως και ο Galois, στην επίλυση ανάγωγων εξισώσεων με βαθμό πρώτο αριθμό. Στην ουσία δηλαδή ασχολείται μόνο με το Premier Mémoire του Galois. Όμως η μελέτη αυτή χαρακτηρίζεται από σωστή οργάνωση και σαφήνεια. Αυτό φαίνεται καθαρά στα δύο παρακάτω παραδείγματα. Το πρώτο αφορά τα Λήμματα II και III όπως τα ονομάζει ο Galois για τα οποία δίνει μια μικρή και πολύ συμπυκνωμένη απόδειξη. Αντιθέτως ο Serret εξηγεί και αποσαφηνίζει κάθε λεπτομέρεια.

Προταση 2.3.1 (Λήμματα II & III). [24] *Αν*

$$f(x) = 0 \tag{2.38}$$

είναι μια εξίσωση οποιουδήποτε βαθμού n, με διαφορετικές όμως ρίζες, και αν

$$V = \phi(x_0, x_1, \cdots, x_{n-1})$$

μία ρητή συνάρτηση των ριζών $x_0, x_1, \cdots, x_{n-1}$ της εξίσωσης (2.38), τέτοια ώστε, οι $n!$ τιμές που παίρνει από τις μεταθέσεις των ριζών να είναι όλες διαφορετικές, τότε μπορούμε να εκφράσουμε τις n ρίζες $x_0, x_1, \cdots, x_{n-1}$ ως ρητές συναρτήσεις της V.

Απόδειξη. Συμβολίζουμε με V_0 την δεδομένη τιμή της V και με

$$V_0, V_1, \cdots, V_{\mu-1}$$

[23] η "παράγουσα" ομάδα σύμφωνα με την ορολογία του Betti.
[24] βλέπε [32] §490, σελ.413

τις $\mu = 1 \cdot 2 \cdot 3 \cdots (n-1)$ τιμές που παίρνει η V από τις μεταθέσεις των n-1 ριζών

$$x_0, x_1, \cdots, x_{n-1}$$

Έχουμε λοιπόν μια εξίσωση ως προς V μ-στου βαθμού, την

$$(V - V_0)(V - V_1) \cdots (V - V_{\mu-1}) = 0 \tag{2.39}$$

της οποίας οι ρίζες $V_0, V_1, \cdots, V_{\mu-1}$ είναι όλες διαφορετικές και οι συντελεστές, που είναι συμμετρικές συναρτήσεις των ριζών $x_1, \cdots, x_{n-1}$ της εξίσωσης

$$\frac{f(x)}{x - x_0} = 0$$

είναι ρητές εκφράσεις των συντελεστών της αρχικής εξίσωσης (2.38). Εν συνεχεία, η εξίσωση (2.39) μπορεί να έρθει στη μορφή

$$F(V, x_0) = 0 \tag{2.40}$$

όπου η F είναι μία ρητή συνάρτηση των V και x_0. Επειδή οι εξισώσεις (2.39) και (2.40) επαληθεύονται για $V = V_0$ θα έχουμε ότι

$$F(V_0, x_0) = 0$$

δηλαδή ότι η εξίσωση

$$F(V_0, x) = 0 \tag{2.41}$$

επαληθεύεται για $x = x_0$. Συνεπώς οι εξισώσεις (2.38) και (2.41) έχουν μία κοινή ρίζα, την x_0. Επιπλέον δείχνουμε ότι δεν έχουν καμία άλλη κοινή ρίζα. Υποθέτουμε ότι η εξίσωση (2.41) επαληθεύεται και από την $x = x_1$, τότε θα έχουμε ομοίως

$$F(V_0, x_1) = 0$$

δηλαδή ότι η εξίσωση

$$F(V, x_1) = 0 \tag{2.42}$$

επαληθεύεται για $V = V_0$. Άρα η εξισωση (2.42) προκύπτει από τις εξισώσεις (2.40) ή (2.39) από την αντιμετάθεση των ριζών x_0 και x_1. Από αυτή την αντιμετάθεση οι ποσότητες $V_0, V_1, \cdots, V_{\mu-1}$ μετασχηματίζονται σε άλλες $V_0', V_1', \cdots, V_{\mu-1}'$ εντελώς διαφορετικές από αυτές της υπόθεσης, οπότε η εξίσωση (2.42) μετασχηματίζεται στην

$$(V - V_0')(V - V_1') \cdots (V - V_{\mu-1}') = 0$$

απ' όπου συμπεραίνουμε ότι δεν έχει ως ρίζα την V_0.

Οι εξισώσεις (2.38) και (2.41), έχοντας ως μοναδική κοινή ρίζα την x_0, είναι ευκολότερο να επιλυθούν καθορίζοντας την ρίζα αυτή. Αναζητούμε το μέγιστο κοινό διαιρέτη των $f(x) = 0$ και $F(V_0, x)$ και προχωρούμε την διαδικασία μέχρι να βρούμε ένα υπόλοιπο πρώτου βαθμού ως προς x. Εξισώνοντας το υπόλοιπο αυτό με το 0, θα προκύψει μια εξίσωση που θα κάνει γνωστή την τιμή της x_0,

$$x_0 = \psi(V_0) \quad \text{ή} \quad x_0 = \psi(V)$$

η οποία φυσικά είναι ρητή συνάρτηση της V αφού η διαδικασία εύρεσης του μέγιστου κοινού διαιρέτη δεν εισάγει ριζικά.

Ομοίως μπορούμε να βρούμε τις υπόλοιπες ρίζες, παίρνοντας έτσι τις ρητές εκφράσεις

$$x_0 = \psi_0(V), x_1 = \psi_1(V), \cdots, x_{n-1} = \psi_{n-1}(V)$$

□

Το δέυτερο παράδειγμα αφορά την παρουσίαση της τελικής Προτασης VIII του Premier Mémoire, όπου ενώ ο Galois δίνει την απόδειξή του, ημιτελή και σε μισή σελίδα, καταλήγοντας μάλιστα με τις λέξεις: *"Donc, etc."*, δηλαδή "Επομένως, κ.λ.π", ο Serret αφιερώνει πάνω από τέσσερις σελίδες λεπτομερούς απόδειξης.

Προταση 2.3.2 (Πρόταση VIII). [25] *Μία ανάγωγη εξίσωση με βαθμό έναν πρώτο αριθμό p είναι επιλύσιμη με ριζικά, αν και μόνο αν όλες οι ρίζες της μπορούν να εκφραστούν ως ρητές συναρτήσεις δύο οποιωνδήποτε εξ αυτών.*

Απόδειξη. [26] ($\Longrightarrow$) Αν μία εξίσωση είναι επιλύσιμη, τότε η ομάδα της θα περιέχει μόνο μεταθέσεις της μορφής

$$\begin{pmatrix} x_i \\ x_{ai+b} \end{pmatrix} \quad 0 < a < p, \quad 0 \leq b < p$$

Αλλά αν δεν είναι η ταυτοτική μετάθεση τότε υπάρχουν δύο περιπτώσεις:

1. αν $a = 1$ η μετάθεση αλλάζει όλες τις p ρίζες εφόσον $i \not\equiv i + b \pmod{p}$ για κάθε i, όταν $b \neq 0$

[25] βλέπε [32] §579-580, σελ.643

[26] θα παρουσιάσουμε μια σύνοψη μόνο της ολοκληρωμένης απόδειξης.

2. αν $a \neq 1$ τότε η εξίσωση $i \equiv ai + b \pmod p$ έχει μοναδική ακέραια λύση, δηλαδή μία μόνο ρίζα x_i απεικονίζεται στον εαυτό της.

Αλλά αν είναι γνωστές δύο ρίζες πρέπει κάθε μία να απεικονίζεται στον εαυτό της κάτω από όλες τις μεταθέσεις της ομάδας, το οποίο σημαίνει ότι η ομάδα περιέχει μόνο την ταυτοτική μετάθεση. Οπότε όλες οι ρίζες είναι γνωστές όταν δύο από αυτές είναι γνωστές.

($\Longleftarrow$) Έστω x_1 και x_2 δύο από τις ρίζες της εξίσωσης

$$f(x) = 0 \tag{2.43}$$

n-στου βαθμού. Αν G είναι η αρχική ομάδα[27] της εξίσωσης και Γ η ομάδα που προκύπτει μετά την προσάρτηση της ρίζας x_1, αλλά πρίν την προσάρτηση της x_2. Έστω επίσης

$$F(V) = 0 \tag{2.44}$$

η ανάγωγη εξίσωση που ονομάζουμε επιλύουσα και της οποίας ο βαθμός ισούται με την τάξη της G. Η ρίζα x_1 είναι μία ρητή συνάρτηση $x_1 = \phi(V_0)$ μιας από τις ρίζες της (2.44). Τότε ο Serret δείχνει ότι όταν προσαρτάται η x_1, η (2.44) παραγοντοποιείται σε n παράγοντες καθένας από τους οποίους έχει βαθμό ίσο με την τάξη της ομάδας Γ. Η ομάδα της εξίσωσης (2.43) είναι τώρα η Γ και η x_2 ειναι μία ρίζα της εξίσωσης

$$f_1(x, x_1) = 0 \tag{2.45}$$

όπου το πρώτο μέλος $f_1(x, x_1)$ είναι ίσο με $\frac{f(x)}{x-x_1}$ ή με κάποιο ρητό διαιρέτη του. Οπότε ο βαθμός της είναι ίσος, είτε με $n-1$, είτε με κάποιο διαιρέτη του έστω τον m και η τάξη της G είναι nm.

Στη συνέχεια ο Serret δείχνει ότι καμία μετάθεση στην G δεν μπορεί να κρατήσει δύο ρίζες της (2.43) σταθερές, εκτός αν είναι η ταυτοτική. Εκ κατασκευής η Γ αποτελείται από αυτές τις μεταθέσεις που κρατούν τον δείκτη 1 σταθερό, έτσι η G περιέχει, μαζί με την ταυτοτική, $m-1$ τέτοιες μεταθέσεις. Όμως εφόσον η υπόθεση ισχύει για κάθε μία από τις ρίζες x_1 και x_2, συνεπάγεται ότι η G περιέχει $(m-1)n + 1 = mn - (n-1)$ μεταθέσεις οι οποίες, όχι ταυτόχρονα, αλλάζουν όλους τους δείκτες. Αλλά η G περιέχει mn στοιχεία, οπότε θα έχει $n-1$ μεταθέσεις που αλλάζουν όλους τους δείκτες. Τελικά ο Serret δείχνει ότι αυτές οι μεταθέσεις είναι στην πραγματικότητα κυκλικές και μαζί με την ταυτοτική σχηματίζουν μία κυκλική ομάδα

[27] ο Serret χρησιμοποιεί τον όρο *"système conjugué propre"*

με τάξη n πρώτο αριθμό. Επομένως αυτές οι μεταθέσεις είναι της μορφής $T = \begin{pmatrix} i \\ i+1 \end{pmatrix}$ και των δυνάμεων της T. Από αυτό συμπεραίνουμε ότι οποιαδήποτε μετάθεση $U = \begin{pmatrix} i \\ F(i) \end{pmatrix}$ στην G συνεπάγεται $F(i) = ai + b$ και έτσι ολοκληρώνεται η απόδειξη. □

Το βιβλίο του Serret, *"Cours d'algebre supérieure"*, ήταν σημείο αναφοράς για περισσότερο από μισό αιώνα και ήταν αυτό που έδωσε την έμπνευση και την ώθηση στην περαιτέρω ανάπτυξη της Θεωρίας Galois, όπως ομολογεί και ο επόμενος που συνέβαλε σημαντικά σ'αυτήν, ο Camille Jordan.

2.3.3 Jordan

Οι έρευνες του Serret στην Άλγεβρα ενέπνευσαν τον πιο χαρισματικό μαθητή του, τον Camille Jordan. Ο ίδιος αναφέρει στη εισαγωγή του μνημειώδους έργου του *"Traité des substitutions et des équations algébriques"*[19]:

> Από τα έργα που συμβουλευτήκαμε, οφείλουμε να αναφέρουμε ειδικά, εκτός των ίδιων των έργων του Galois των οποίων αυτό εδώ το έργο είναι μόνο ένα σχόλιο, το *"Cours d'algebre supérieure"* του κ. J.-A.Serret. Η επιμελής ανάγνωση αυτού του βιβλίου μας εισήγαγε στην Άλγεβρα και μας ενέπνευσε την επιθυμία να συμβάλλουμε στην πρόοδό της.

Ο Jordan θεωρείται ο πρώτος από τους σύγχρονους Μαθηματικούς που μπορεί να χαρακτηρίζεται ως Αλγεβρίστας. Το πιο γνωστό έργο του *"Traité des substitutions et des équations algébriques"* εκδόθηκε το 1870 και περιείχε όλα όσα ήταν γνωστά για τη Θεωρία Ομάδων μέχρι τότε. Είχε προηγηθεί όμως μία δεκαετία που δημοσίευε συνεχώς άρθρα τα οποία εξέλισσαν την έννοια της ομάδας.

Από τις πρώτες κιόλας δημοσιεύσεις του, ο Jordan, παρουσιάζει μία έννοια άρρηκτα συνδεδεμένη με το όνομά του, τη συνθετική σειρά (*composition series*). Όπως αναφέρει και στο [19]§54,

> Μία ομάδα G είναι *απλή* αν δεν περιέχει καμία άλλη ομάδα της οποίας οι μεταθέσεις να αντιμεταθέτονται, ενώ ονομάζεται *σύνθετη* στην αντίθετη περίπτωση.

> Έστω G μια οποιαδήποτε σύνθετη ομάδα, μπορούμε να καθορίσουμε μία ακολουθία ομάδων
>
> $$G, H, H', \cdots, I, I', \cdots, K, \cdots, \mathtt{I}$$
>
> τέτοια ώστε:
>
> 1. καθεμία από τις ομάδες της ακολουθίας να περιέχεται στην προηγούμενη και να αντιμεταθέτονται από τις μεταθέσεις της,
> 2. να μην περιέχεται σε καμία πιο γενική ομάδα με την προϋπόθεση των δύο παραπάνω ιδιοτήτων,
> 3. η τελευταία ομάδα της σειράς να περιέχει μόνο την ταυτοτική μετάθεση.

Η σημασία της συνθετικής σειράς φαίνεται πολύ καθαρά στην απόδειξη του τελευταίου από μια σειρά θεωρημάτων που αφορούν τις επιλύσιμες με ριζικά εξισώσεις, για το οποίο ο ίδιος σχολιάζει:

> Με αυτήν την τελευταία μορφή [από τα θεωρήματα], ο Galois επισήμανε την ικανή και αναγκαία συνθήκη για την επίλυση με ριζικά.

Ο Jordan αρχικά ορίζει [19]§517, ως επιλύσιμες ομάδες αυτές που χαρακτηρίζουν τις επιλύσιμες με ριζικά εξισώσεις. Το εν λόγω θεώρημα [19]§524 αναφέρει:

Θεώρημα 2.3.1. *Για να είναι μια εξίσωση επιλύσιμη με ριζικά, πρέπει και αρκεί, η ομάδα της να μπορεί να θεωρηθεί ως παραγόμενη από μια κλίμακα (σκάλα) μεταθέσεων* $\mathtt{I}, a, b, \cdots, f, g$*, τέτοιων ώστε:*

1. *καθεμία από αυτές να αντιμεταθέτεται στην ομάδα που παράγεται από τις προηγούμενες,*
2. *η πρώτη από τις διαδοχικές τους δυνάμεις που περιέχονται στην εν λόγω ομάδα να είναι βαθμού πρώτου αριθμού.*

Απόδειξη. Έστω X μία εξίσωση επιλύσιμη με ριζικά. Έστω $N, \frac{N}{\lambda}, \frac{N}{\lambda\mu}, \cdots$ οι τάξεις αντίστοιχα της ομάδας της G και των ομάδων $H, I, \cdots$ στις οποίες ελαττώνεται μετά την προσάρτηση των ριζών των βοηθητικών αβελιανών εξισώσεων. Έστω $h_1, \cdots, h_\rho, \cdots$ οι μεταθέσεις της H, g μια μετάθεση της G η οποία δεν ανήκει στην H, g^q η πρώτη από τις συνάμεις που περιέχεται στην H. Η ομάδα G_1 που παράγεται από τη σύνθεση του g με την H, έχει προφανώς $q\frac{N}{\lambda}$ διαφορετικές μεταθέσεις

της μορφής $g^\alpha h_\rho$, όπου $0 \leq \alpha \leq q-1$ και $1 \leq \rho \leq \frac{N}{\lambda}$. Όμως η G_1 περιέχεται στην G, η οποία έχει τάξη N, έτσι το $q\frac{N}{\lambda}$ διαιρεί το N αλλά το $lambda$ είναι πρώτος οπότε θα έχουμε $q = \lambda$ και $G_1 = G$. Οπότε η G προκύπτει από το συνδυασμό της H με την g, με την οποία αντιμετατίθεται και της οποίας η δύναμη $lambda$ πρώτος αριθμός, είναι ο πρώτος ώστε να ανήκει στην H. Ομοίως βλέπουμε ότι η H προκύπτει από το συνδυασμό της I με μία μετάθεση f που αντιμετατίθεται στην I και τέτοια ώστε η πρώτη από τις δυνάμεις που την κάνουν να ανήκει στην I έχει ως βαθμό τον πρώτο αριθμό μ, κ.λ.π.

Αντιστρόφως, αν η G προκύπτει από το συνδυασμό των μεταθέσεων $\mathtt{I}, a, b, \cdots, f, g$ που ικανοποιούν τις συνθήκες της υπόθεσης του θεωρήματος, θα έχουμε μία ακολουθία ομάδων

$$G, H = (\mathtt{I}, a, b, \cdots, f), \cdots, (\mathtt{I}, a, b), (\mathtt{I}, a), \mathtt{I}$$

με τάξεις $N, \frac{N}{\lambda}, \frac{N}{\lambda\mu}, \cdots$, όπου οι $\lambda, \mu, \cdots$ είναι πρώτοι και τέτοιες ώστε καθεμία να περιέχεται στην προηγούμενη και να αντιμετατίθεται από τις μεταθέσεις της. Οπότε $\lambda, \mu, \cdots$ θα είναι οι παράγοντες σύνθεσης της G. Συνεπώς από προηγούμενο θεώρημα ([19]§520) η εξίσωση θα είναι επιλύσιμη με ριζικά. □

Μια πιο αναγνωρίσιμη μορφή, από τη σύγχρονη οπτική, του θεωρήματος είναι το παρακάτω [19]§531, το οποίο συνδέει άμεσα την επιλυσιμότητα με τη συνθετική σειρά.

Θεώρημα 2.3.2. *Για να είναι μια ομάδα L επιλύσιμη, πρέπει και αρκεί, να μπορούμε να φτιάξουμε μία ακολουθία ομάδων $\mathtt{I}, F, G, H, \cdots, L$ η οποία τελειώνει στην L και αυτές να έχουν τις ακόλουθες ιδιότητες:*

1. *καθεμία από αυτές τις ομάδες να περιέχεται στην επόμενη και να αντιμεταθέτεται με τις μεταθέσεις της L,*

2. *δύο οποιεσδήποτε από τις μεταθέσεις τους να είναι εναλλάξιμες μεταξύ τους, στις μεταθέσεις της προηγούμενης ομάδας.*

Ο Jordan αναζητώντας τον καθορισμό των διάφορων τύπων των επιλύσιμων εξισώσεων, λόγω αυτού του θεωρήματος (2.3.2) , οδηγείται στην ελαχιστοποίηση του αρχικού προβλήματος σε τρία μικρότερα προβλήματα, στα οποία αφιερώνει τις επόμενες 140 σελίδες του βιβλίου του:

Πρόβλημα Α Η σαφής κατασκευή για κάθε δεδομένο βαθμό των διάφορων ομάδων που είναι επιλύσιμες, μεταβατικές και γενικές[28].

Πρόβλημα Β Η κατασκευή των πιο γενικών επιλύσιμων και πρωταρχικών ομάδων που περιέχονται στη γραμμική ομάδα.

Πρόβλημα Γ Η κατασκευή των πιο γενικών επιλύσιμων και πρωταρχικών ομάδων που περιέχονται στις αβελιανές και υποαβελιανές ομάδες.

Αναφέρει χαρακτηριστικά ότι: "Αυτή η απλοποίηση δεν θα συνέβαινε αν λαμβάναμε ως σημείο εκκίνησης το θεώρημα (2.3.1), όπως έκανε ο Galois." Το έργο του Jordan σηματοδοτεί τη Θεωρία Ομάδων και μαζί της τη Θεωρία Galois ως θεμέλιο λίθο της σύγχρονης Άλγεβρας.

[28]ο Jordan χρησιμοποιεί τη λέξη *généraux* η οποία είναι συνώνυμη με τη λέξη *maximal* που χρησιμοποιούσε ο Betti και σημαίνει μία ομάδα η οποία δεν είναι κανονική σε καμία άλλη μεγαλύτερη ομάδα.

3

Σώματα

3.1 Επεκτάσεις σωμάτων

Ο Galois ήταν ο πρώτος που έδωσε σε ένα σύστημα μεταθέσεων το όνομα το οποίο χρησιμοποιούμε ακόμα και σήμερα, την *ομάδα*, καθώς και τον σημαντικό ρόλο που έχει στα Μαθηματικά. Δεν διατύπωσε όμως το ίδιο ρητά και αυτό που στη σύγχρονη ορολογία ονομάζουμε *σώμα*. Παρ' όλα αυτά, υπονόησε την ύπαρξη τους, αφού στο έργο του είναι φανερό ότι καταλάβαινε την έννοια αλλά και τις ιδιότητες των σωμάτων. Ήταν ο πρώτος που χρησιμοποίησε τον όρο *"adjoint"* ("προσάρτηση" ή "επισύναψη") με την τεχνική σύχρονη έννοια. Λέγοντας μάλιστα ότι σε μια εξίσωση προσαρτά μια ρίζα, έδινε στην ουσία την έννοια της επέκτασης ενός σώματος. Επιπλέον απέδειξε ένα θεμελιώδες θεώρημα για τη σύγχρονη Θεωρία Σωμάτων, το Θεώρημα του Πρωταρχικού Στοιχείου *(Primitive Element Theorem)*, το οποίο χρησιμοποίησε για να καθορίσει την ομάδα μιας εξίσωσης. Όμως και σε ένα από τα δημοσιευμένα άρθρα του, το *"Sur la théorie des nombres"* το 1830, αναπτύσσει την έννοια των πεπερασμένων σωμάτων με p^n στοιχεία.[1]

Αυτό που έκανε ο Galois για τις ομάδες, το έκανε ο Dedekind για τα σώματα, μελέτησε δηλαδή τη δομή τους και τους έδωσε την ονομασία που χρησιμοποιούμε σήμερα. Στην πραγματικότητα οι επόμενες έρευνες που επηρέασαν την ανάπτυξη της Θεωρίας Galois, έγιναν στη Γερμανία. Για την ακρίβεια, αυτές δεν είχαν ως κύρια αφετηρία την Θεωρία Galois όπως παρουσιαζόταν μέχρι τότε, αλλά ενσωματώθηκαν με τη θεωρία αυτή μόνο αφού είχαν αναπτυχθεί

[1] προς τιμήν του μάλιστα ονομάζονται Σώματα Galois.

καλά. Όπως η γαλλική σχολή των Μαθηματικών, τουλάχιστον στην Άλγεβρα, οφείλει τις απαρχές της στον Lagrange και το έργο του σχετικά με τις πολυωνυμικές εξισώσεις, έτσι και η γερμανική σχολή των Μαθηματικών, στον τομέα της Άλγεβρας, οφείλει την εξέλιξή της στο έργο του Gauss πάνω στη θεωρία αριθμών, η οποία οδήγησε τελικά στην ανάπτυξη της θεωρίας των σωμάτων. Όπως οι Μαθηματικοί, σαν τον Dirichlet και τον Dedekind, άρχιζαν να εξετάζουν, να επεκτείνουν και να γενικεύουν το έργο του Gauss σχετικά με τη θεωρία αριθμών, έγινε φανερό ότι έπρεπε να ληφθεί ιδιαίτερη προσοχή στη φύση και τα χαρακτηριστικά αυτών των αριθμητικών συστημάτων.

Κατά τον Kiernan[20], οι κύριοι μοχλοί ανάπτυξης των γερμανικών μαθηματικών, τον 19ο αιώνα, ήταν φιλοσοφικοί. Οι επικρατούσες τάσεις ήταν δύο. Η μία πίστευε ότι κάθε Μαθηματικό αποτέλεσμα ήταν αποδεκτό όταν μπορούσε να κατασκευασθεί και μάλιστα σε πεπερασμένο αριθμό βημάτων. Η τάση αυτή ονομάζεται *ιντουσιονισμός*[2]. Η άλλη υποστηρίζει ότι είναι αρκετός ένας σαφής ορισμός ενός αντικειμένου ή η αποδεδειγμένη ύπαρξή του, έστω κι αν δεν μπορούμε να το κατασκευάσουμε. Το όνομά της είναι γνωστό ως *φορμαλισμός*[3].

Σύμφωνα με τις παραπάνω φιλοσοφικές απόψεις, ο Galois μπορεί να θεωρηθεί ως φορμαλιστής(”existentialist”), αφού η απαιτησή του ήταν μόνο να γνωρίζει ότι η ομάδα μιας εξίσωσης υπάρχει και οι εκφράσεις, που όταν προσαρτούνται στην εξίσωση ελαττώνουν την ομάδα της, να είναι ρίζες επιλύσιμων εξισώσεων, χωρίς να προσπαθεί όμως να τις κατασκευάσει. Από την άλλη οι επόμενοι Γάλλοι Μαθηματικοί που ασχολήθηκαν με τη Θεωρία Galois μπορούν να θεωρηθούν ως ιντουσιονιστές (”constructionist”) αφού αναζητούσαν τη διαδικασία με την οποία η ομάδα μιας δεδομένης εξίσωσης να μπορεί να καθορίζεται ρητώς, καθώς και οι βοηθητικές εξισώσεις.

Η θεωρία των σωμάτων εξελίχθηκε σε καθεμία από τις δύο μαθηματικές παραδόσεις που επικράτησαν στη Γερμανία στο τελευταίο μέρος του19ου αιώνα από διαφορετικούς φυσικά ανθρώπους.

[2]ο Kiernan την αναφέρει ως ”constructionism”(κονστρουκτιβισμό).
[3]ο Kiernan την αναφέρει ως ”existentialism”(υπαρξισμό).

3.1.1 Kronecker

Από τις αρχές της δεκαετίας του 1850, ο Leopold Kronecker, προσπαθώντας να χαράξει μια γενική θεωρία στην οποία θα υπάγεται η Αλγεβρική Θεωρία Αριθμών και η Αλγεβρική Γεωμετρία ως ειδικές περιπτώσεις, ανάπτυσσε τις ιδέες του και δημοσίευε σχετικά, για αρκετές δεκαετίες.[4] Κατάληξη όλων αυτών των άρθρων ήταν η δημοσίευση, το 1882, μιας εκτενής παρουσίασης της έννοιας του για μια περιοχή ρητότητας *("domain of rationality")* η οποία ήδη προτεινόταν ως έννοια στα γραπτά του Galois. Η δημοσίευση είχε τον τίτλο *"Grundzüge einer arithmetischen theorie der algebraischen grössen"* και μάλιστα σ'αυτήν ο ίδιος ο Kronecker δηλώνει ότι είχε εργαστεί για το θέμα αυτό ήδη από το 1853, έτος κατά το οποίο ήρθε για πρώτη φορά σε επαφή με τη Θεωρία Galois, και είχε δώσει διαλέξεις σχετικά με αυτήν σε αρκετές περιπτώσεις. Μια από τις κεντρικές έννοιες που παρουσιάζει είναι το Σώμα, το οποίο όμως ονομάζει *"περιοχή ρητότητας" (Rationalitdtsbereich)* και για το οποίο δίνει τον ακόλουθο ορισμό:

Ορισμός 3.1.1. Η περιοχή ρητότητας $(R, R', R'', \cdots)$ περιέχει κάθε μία από αυτές τις ποσότητες οι οποίες είναι ρητές συναρτήσεις των ποσοτήτων $R, R', R'', \cdots$ με ακέραιους συντελεστές.

Πρόκειται για έναν καθαρά κατασκευαστικό ορισμό και όχι το είδος του ορισμού που θα ήταν αποδεκτό από εμάς σήμερα. Αλλά η διατύπωσή του, υπαγορεύτηκε από τις απόψεις του Kronecker σχετικά με τη φύση των μαθηματικών, ο οποίος ήταν από τους βασικούς υποστηρικτές της ιντουσιονιστικής θεώρησης. Για αυτόν τα Μαθηματικά έπρεπε να είναι κατασκευάσιμα και πεπερασμένα. Δεν βάζει κανέναν περιορισμό για τη φύση των ποσοτήτων $R, R', R'', \cdots$. Μπορεί να είναι είτε απροσδιόριστες ποσότητες είτε ρίζες αλγεβρικών εξισώσεων με ακέραιους συντελεστές. Όπου ο όρος "αλγεβρικός " χρησιμοποιείται από τον Kronecker με τη σύγχρονη έννοια, δηλαδή καθορίζει μια αλγεβρική συνάρτηση n-τού βαθμού των ποσοτήτων $R, R', R'', \cdots$ ως "κάθε ρίζα μιας ανάγωγης εξίσωσης n-τού βαθμού της οποίας οι συντελεστές βρίσκονται στην περιοχή ρητότητας $(R, R', R'', \cdots)$". Μία τέτοια αλγεβρική έκφραση μπορεί στη συνέχεια να είναι επισυναφθεί σε μια άλλη περιοχή για να σχηματίσουν μία νέα η οποία θα περιέχει αυτή την αλγεβρική έκφραση.

Ο Kronecker επινόησε μια διαδικασία για αυτή την επισύναψη η οποία εξαρτάται μόνο από την ύπαρξη των ακέραιων και των

[4] αναφορά από το [21] και [22]

απροσδιόριστων ποσοτήτων. Για παράδειγμα, με σύγχρονη ορολογία, το αλγεβρικό σώμα αριθμών $Q(\sqrt{2})$ ορίστηκε από τον Kronecker ως το σώμα πηλίκο του πολυωνυμικού δακτυλίου $Q[x]$ σε σχέση με το ιδεώδες που παράγεται από το $x^2 - 2$. Δηλαδή, αν δύο πολυώνυμα καλούνται ισοδύναμα όταν αφήνουν το ίδιο υπόλοιπο μετά τη διαίρεση με το πολυώνυμο $x^2 - 2$, τοτε το σύνολο των υπολοίπων είναι η περιοχή ρητότητας $Q(\sqrt{2})$, ή για να είμαστε πιο συνεπείς με την ορολογια του ίδιου του Kronecker, αυτά τα υπόλοιπα βρισκονται στην περιοχή ρητότητας $(1, \sqrt{2})$. Με αυτήν τη κατασκευή αποφεύγει την υπόθεση ύπαρξης των άρρητων αριθμών, αφού τους απέρριπτε, δεδομένου ότι για να οριστούν απαιτείται η χρήση του μαθηματικού απείρου. Αυτές οι ιδέες περιέχουν το φύτρο του θεωρήματος που έγινε γνωστό ως Θεώρημα Kronecker, δηλαδή ότι κάθε πολυώνυμο πάνω σε ένα σώμα έχει μια ρίζα σε κάποια επέκταση του σώματος αυτού.

Στο ίδιο άρθρο ο Kronecker εισάγει την έννοια του "γένους" *("Gattung")*, παρόμοια με την έννοια του στοιχείου που παράγει μια αλγεβρική επέκταση σωμάτων. Δείχνει ότι αν αυτό το στοιχείο είναι μια ρίζα εξίσωσης n-τού βαθμού, ανάγωγη στο σώμα των συντελεστών της, τότε κάθε στοιχείο της επέκτασης είναι μια ρίζα εξίσωσης βαθμού το πολύ n. Το γένος τότε θα λέγεται ότι είναι "τάξης n" πάνω στο σώμα.

Επιπλέον, ο Kronecker παρατηρεί ότι είναι δυνατό να επισυνάψει μια μεταβλητή ή απροσδιόριστη ποσότητα για να σχηματίσει μια νέα περιοχή ρητότητας και ότι το αποτέλεσμα θα είναι κατά μία έννοια το ίδιο χωρίς να έχει σημασία ποιά μη-αλγεβρική ποσότητα επισυνάφθηκε. Με σύγχρονους όρους θα μπορούσαμε να πούμε ότι, αν F είναι ένα σώμα, θ ένα στοιχείο υπερβατικό στο F και x μια μεταβλητή (απροσδιόριστη ποσότητα), τότε το $F(\theta)$ είναι ισόμορφο με το $F(x)$ μέσω ενός ισομορφισμού που αφήνει αναλλοίωτο το F. Αυτό το αποτέλεσμα εκφράζει απόλυτα τη φιλοσοφία του Kronecker: οι υπερβατικοί αριθμοί είναι απροσδιόριστοι. Αλλά το κρίσιμο σημείο είναι η αναγνώριση από τον Kronecker ότι και οι απροσδιόριστες ποσότητες μπορούν να επισυναφθούν ένα σώμα όπως μπορούν και οι αλγεβρικοί αριθμοί. Αυτό δεν σημαίνει ότι επεκτάσεις που προκύπτουν είναι και δομικά όμοιες. Για παράδειγμα το $Q(\sqrt{2})$ και το $Q(x)$ δεν είναι ισόμορφα, όπως αναγνωρίζει και ο ίδιος ο Kronecker.

Με αυτόν τον τρόπο, η έννοια του αριθμού επεκτάθηκε και όπως αναφέρει ο Kronecker:

> Αν $c_1, c_2, \cdots, c_n$ δηλώνουν *ακέραιες* ποσότητες της περιοχής ρητότητας των φυσικών $(R', R'', \cdots, R^{(n-1)})$ και

θέσουμε $F(x) = x^n - c_1x^{n-1} + c_2x^{n-2} - \cdots \pm c_n$, τότε ο $F(x)$ είναι μία ακέραιη ποσότητα στην περιοχή $(x, R', R'', \cdots, R^{(n-1)})$.

Ο Kronecker κάνει αναφορά, σε αυτό το άρθρο, σε πολλά σημεία του έργου του Galois. Κατά κύριο λόγο ασχολείται με την έννοια της επισύναψης και έτσι αυτό από μόνο του δεν είναι μια ανάπτυξη της θεωρίας Galois. Παρ' όλα αυτά, παρέχει την έννοια ενός συστήματος, την περιοχή ρητότητας των συντελεστών, στην οποία μπορούν να επισυναφθούν οι ρίζες των διαδοχικών βοηθητικών εξισώσεων. Μπορεί επίσης να αναγνωριστεί, σε πολύ πρώιμη μορφή, η σύνδεση μεταξύ της ομάδας της εξίσωσης και των αυτομορφισμών στο σώμα επέκτασης των συντελεστών. Φυσικά, ο Kronecker δεν θα μπορούσε να εκφράσει το αποτέλεσμα με αυτόν τον τρόπο, αφού δεν έβλεπε μια περιοχή ρητότητας ως μια ολοκληρωμένη οντότητα, αλλά απλώς ως μια περιοχή που περιείχε το αποτέλεσμα κάθε πεπερασμένου αριθμού αλγεβρικών πράξεων των στοιχείων του.

Ο Kronecker αναπτύσσει μια περίτεχνη ορολογία, που βασίζεται σε αυτό που αποκαλεί "επίδραση" (*"effect"*) της εξίσωσης που πρέπει να επιλυθεί, για την n-τού βαθμού εξίσωση $F(V) = 0$ που κατασκευάζεται στο πρώτο βήμα της θεωρίας Galois. Μια γενική εξίσωση δεν έχει καμία επίδραση αφού η εξίσωση $F(V) = 0$ είναι ανάγωγη. Αλλά μια ειδική εξίσωση έχει επίδραση στην $F(V) = 0$ αφού είναι αναγώγιμη και παραγοντοποιείται σε άλλους ανάγωγους παράγοντες που ονομάζονται, από την εποχή του Betti, επιλύουσες Galois. Η επέκταση του αρχικού σώματος των συντελεστών από τις ρίζες μιας από αυτές τις επιλύουσες ονομάζεται "επίδραση-γένους" (*"Affect-Gattung)"*) της εξίσωσης προς επίλυση. Η ομάδα των μεταθέσεων για την επίδραση-γένους, λέει ο Kronecker, είναι η Ομάδα Galois της εξίσωσης. Αν και η ορολογία αυτή του Kronecker δεν διατηρήθηκε στα Μαθηματικά κείμενα, η έννοια αυτή σηματοδοτεί το πρώτο βήμα για τη μετατόπιση της έμφασης της ομάδας της εξίσωσης, από μια ομάδα μεταθέσεων των ριζών σε μια ομάδα αυτομορφισμών, του σώματος επέκτασης του σώματος των συντελεστών.

3.1.2 Dedekind

Ο Julius Wilhelm Richard Dedekind είχε ακριβώς την αντίθετη θεώρηση από τον Kronecker για το πως πρέπει να δημιουργούνται τα Μαθηματικά. Αρκούσε η επινόηση ενός σαφούς ορισμού για να είναι

πλήρως αποδεκτή και κατανοητή η έννοια του αριθμητικού συνόλου που ο ίδιος ονόμασε ”σώμα”. Η βασική εργασία του Dedekind για την έννοια αυτή βρίσκεται στο συμπληρωματικό υλικό που επισυνάπτεται στο μεγάλο έργο του Dirichlet για την Θεωρία Αριθμών με τίτλο *”Vorlesungen über Zahlentheorie”*. Επεκτείνοντας το έργο του Gauss στη θεωρία αριθμών, ο Dirichlet και ο μαθητής του Dedekind τυποποίησαν τις ιδιότητες των ρητών αριθμών και στη συνέχεια να γενίκευσαν το αποτέλεσμα. Στο Συμπλήρωμα XI §160 ο Dedekind δίνει τον ορισμό του σώματος ως εξής[5]:

> Ένα σύστημα A πραγματικών ή μιγαδικών αριθμών a ονομάζεται *σώμα [Körper]* αν το άθροισμα, η διαφορά, το γινόμενο και το πηλίκο κάθε δύο τέτοιων αριθμών a βρίσκεται επίσης μέσα στο σύστημα A.

Στην υποσημείωση που κάνει για τη λέξη ”σώμα” αναφέρει τους λόγους που τον οδήγησαν να επιλέξει αυτή τη λέξη και να απορρίψει μιαν άλλη έκφραση που χρησιμοποιούσε για την ίδια έννοια. Συγκεκριμένα λέει:

> Αυτό το όνομα θα πρέπει, όπως και στις φυσικές επιστήμες, στη γεωμετρία και στη ζωή της ανθρώπινης κοινωνίας, να ορίσει επίσης εδώ ένα σύστημα το οποίο διαθέτει μια ορισμένη πληρότητα, τελειότητα και κλειστότητα, σύμφωνα με την οποία εμφανίζεται ως ένα οργανικό σύνολο, μια φυσική μονάδα. Αρχικά, στις διαλέξεις μου στο Gottingen (1857-1858), είχα χρησιμοποιήσει το όνομα *ρητή περιοχή [rationales Gebiet]* για την ίδια έννοια, αλλά αυτό είναι λιγότερο βολικό. Η έννοια ουσιαστικά ταυτίζεται με αυτό που Kronecker έχει ονομάσει *περιοχή ρητότητας [Rationalitätsbereich]*.

Στην ίδια υποσημείωση αναφέρει ότι χρησιμοποιούσε την έννοια του σώματος, από τον καιρό που έκανε διαλέξεις στο Göttingen το διάστημα 1857-1858, σχετικά με την Θεωρία Galois, μόνο που τότε του έδινε την ονομασία ”ρητή περιοχή” (*”rational Gebiet”*). Ο όρος ”σώμα” *(Körper)* αναφερόταν τότε μόνο σε σώματα που είχαν ως στοιχεία μιγαδικούς αριθμούς. Έτσι ο Dedekind, όπως και άλλοι μεταγενέστεροί του. διατυπώνει το εξής

Θεώρημα 3.1.1. *Κάθε σώμα*[6] *περιέχει το σώμα των ρητών αριθμών.*

[5]μετάφραση από [8]

[6]με τη σύγχρονη ορολογία εννοεί υπόσωμα του σώματος των μιγαδικών αριθμών.

Απόδειξη. Έστω F ένα υπόσωμα του σώματος $\mathbb{C}$ των μιγαδικών αριθμών. Επειδή είναι σώμα περιέχει το μοναδιαίο στοιχείο της πρόσθεσης καθώς και του πολλαπλασιασμού, δηλαδή $0, 1 \in F$. Είναι κλειστό όμως ως προς την πρόσθεση και έτσι $1 + 1 = 2 \in F, \quad 2 + 1 = 3 \in F, \quad \cdots$, δηλαδή κάθε φυσικός αριθμός ανήκει στο F. Ως σώμα είναι κλειστό και ως προς την αφαίρεση συνεπώς περιέχει και όλους τους αντίθετους των φυσικών, άρα όλους τους ακεραίους. Επίσης σ'αυτό ανήκουν και οι αντίστροφοι των ακεραίων ($\neq \ 0$) αφού το $F - \{0\}$ είναι κλειστό και ως προς τον πολλαπλασιασμό και ως προς την διαίρεση. Συνεπώς το F περιέχει όλους τους ρητούς αριθμούς. □

Αναφερόμενος στα πεπερασμένα σώματα, ήδη από το 1871, ο Dedekind χρησιμοποιεί τον όρο *"Endlich Körper"*. Σχολιάζει επίσης ότι το σώμα των μιγαδικών είναι "φυσικά" το μεγαλύτερο σώμα που μπορούμε να διανοηθούμε, αφού κάθε άλλο σώμα περιέχεται μέσα σ' αυτό.

Στην 4η και πιο ώριμη έκδοση του *"Zahlentheorie"*, το 1894, ο Dedekind αναπτύσσει μια θεωρία για τις επεκτάσεις των σωμάτων η οποία είναι από πολλές απόψεις παρόμοια με αυτή του Kronecker. Περιλαμβάνει σημαντικά αποτελέσματα τα οποία είναι πλέον καθιερωμένα στην Θεωρία Σωμάτων.

(i) Έστω $G = \{g', g'', \cdots\}$ ένα υποσύνολο του συνόλου $\mathbb{C}$ των μιγαδικών αριθμών με πληθικότητα *[Anzahl]*, πεπερασμένη ή άπειρη. Τότε η τομή όλων των σωμάτων που περιέχουν όλα τα στοιχεία του G είναι ένα σώμα M για το οποίο ισχύει $\mathbb{Q} \subset M \subset \mathbb{C}$. Ο Dedekind ονομάζει το M "ρητό ως προς G", χρησιμοποιεί μάλιστα τα παρακάτω λόγια[8]:

> Ακολουθώντας έναν τρόπο έκφρασης ο οποίος οφείλεται στον Galois θέλουμε επίσης να πούμε, το σώμα M προκύπτει από το σώμα $\mathbb{Q}$ των ρητών αριθμών με προσάρτηση *[Adjunktion]* του συστήματος G των αριθμών $g', g'', \cdots$

Συμβολίζει το σώμα αυτό με $\mathbb{Q}(G)$ ή $\mathbb{Q}(g', g'', \cdots)$ και αναφέρει ότι είναι το μικρότερο σώμα το οποίο εκτός από τα στοιχεία του $\mathbb{Q}$ περιέχει και τους αριθμούς $g', g'', \cdots$. Κάθε στοιχείο $m \in M$ μπορεί να παρασταθεί από ένα πεπερασμένο πλήθος ρητών πράξεων ανάμεσα σε πεπερασμένο πλήθος ρητών και πεπερασμένο πλήθος στοιχείων του G. Αν το G είναι

πεπερασμένο σύνολο τότε στην πραγματικότητα συμπίπτει με αυτό που ο Kronecker ονομάζει *περιοχή ρητότητας*.

(ii) Ορίζει τον ισομορφισμό σωμάτων, ονομάζοντάς τον *"μετάθεση [Permutation] του σώματος"*, ως μια απεικόνιση *[Abbildung]* ενός σώματος A σε ένα άλλο A'. Συμβολίζει αυτή την την μετάθεση με το γράμμα ϕ και την εικόνα $a' \in A'$, ενός στοιχείου $a \in A$, με $a' = a\phi$, καθώς και $A' = A\phi$ το οποίο ονομάζει *"σώμα παραγόμενο από την ϕ"*. Σημειώνει ότι μία απεικόνιση ϕ είναι *μετάθεση* αν για δύο στοιχεία $u, v \in A$ ικανοποιούνται οι παρακάτω *βασικοί κανόνες*:

$$\phi(u+v) = \phi(u) + \phi(v) \tag{3.1}$$

$$\phi(u-v) = \phi(u) - \phi(v) \tag{3.2}$$

$$\phi(uv) = \phi(u)\phi(v) \tag{3.3}$$

$$\phi(\frac{u}{v}) = \frac{\phi(u)}{\phi(v)} \tag{3.4}$$

δηλαδή να διατηρούνται και οι τέσσερις αριθμητικές πράξεις. Επισημαίνει ότι, η υπόθεση ότι το A' δεν είναι κενό σημαίνει πως, η αντιστοίχιση είναι ένα-προς-ένα, και πως είναι απαραίτητο μόνο να υποθέσουμε ότι διατηρούνται η πρόσθεση και ο πολλαπλασιασμός. Αναφέρει μάλιστα ότι και η αντίστροφη απεικόνιση ϕ^{-1} είναι κι αυτή μια μετάθεση και για αυτό το λόγο ονομάζει τα σώματα A και A' *συζυγή*. Αναγνωρίζει επιπλέον ότι το σώμα των ρητών αριθμών έχει μόνο την ταυτοτική μετάθεση, το οποίο σημαίνει ότι κάθε μετάθεση ϕ ενός σώματος A αφήνει αναλλοίωτο το σώμα $\mathbb{Q}$ ανεξάρτητα από το τι κάνει στα άλλα στοιχεία του A.

(iii) Ο Dedekind χρησιμοποιώντας την δική του ορολογία, κάνει περίπου τις ίδιες παρατηρήσεις που έκανε και ο Kronecker σχετικά με τη φύση των επισυναπτόμενων στοιχείων. Αρχικά δίνει τους ορισμούς:

Ορισμός 3.1.2. Ένα σύνολο T από m αριθμούς $\omega_1, \omega_2, \cdots, \omega_m$ ονομάζεται *αναγώγιμο [reduzibel]* πάνω στο σώμα A, αν υπάρχουν m αριθμοί $a_1, a_2, \cdots, a_m \in A$, όχι όλοι μηδέν, που ικανοποιούν την συνθήκη

$$a_1\omega_1 + a_2\omega_2 + \cdots + a_m\omega_m = 0$$

Στην αντίθετη περίπτωση το σύνολο T ονομάζεται *ανάγωγο* πάνω στο σώμα A. Σύμφωνα με το εάν συμβαίνει η πρώτη ή η τελευταία περίπτωση, θα λέμε ότι οι m αριθμοί $\omega_1, \omega_2, \cdots, \omega_m$ είναι *εξαρτημένοι [abhängig]*, ή *ανεξάρτητοι [unabhängen]*, μεταξύ τους (πάνω στο σώμα A).

Ορισμός 3.1.3. Λέμε ότι ένας αριθμός θ είναι *αλγεβρικός [algebraisch]* πάνω στο σώμα A, αν είναι ρίζα μιας πεπερασμένης αλγεβρικής εξίσωσης της μορφής

$$\theta^n + a_1\theta^{n-1} + \cdots + a_{n-1}\theta + a_n = 0$$

της οποίας οι συντελεστές $a_r \in A$. Ο ελάχιστος θετικός ακέραιος αριθμός n για τον οποίο ισχύει αυτό, ονομάζεται *βαθμός [Grad]* του θ πάνω στο σώμα A. Εάν $n = 1$ τότε είναι προφανές ότι ο θ περιέχεται στο A, αντιστρόφως κάθε αριθμός $\theta \in A$ είναι αλγεβρικός πρώτου βαθμού πάνω στο σώμα A.

Στη συνέχεια παρατηρεί ότι αν το παραπάνω σύνολο m αριθμών $\omega_1, \omega_2, \cdots, \omega_m$ είναι αναγώγιμο (εξαρτημένοι), τότε προφανώς ένα υποσύνολό του που μπορεί να αποτελείται από $n < m$ αριθμούς $\omega_1, \omega_2, \cdots, \omega_n$, είναι ανάγωγο (ανεξάρτητοι). Συμβολίζει με ω κάθε αριθμό που είναι εξαρτημένος από τους $\omega_1, \omega_2, \cdots, \omega_n$. Ονομάζει το σύνολο Ω όλων των αριθμών ω μία *οικογένεια [Schar]* πάνω στο σώμα A και το σύνολο των αριθμών $\omega_1, \omega_2, \cdots, \omega_n$ μία *βάση [Basis]* της οικογένειας Ω, τα δε στοιχεία του ω_r *μέλη ή στοιχεία* της βάσης. Οι χαρακτηριστικές ιδιότητες μιας τέτοιας οικογένειας Ω είναι:

I. Το Ω είναι κλειστό κάτω από τις πράξεις της πρόσθεσης και της αφαίρεσης.

II. Το Ω είναι κλειστό κάτω από τον πολλαπλασιασμό με στοιχεία του A.

III. Κάθε $n + 1$ στοιχεία του Ω είναι εξαρτημένα.

Αυτές οι συνθήκες καθορίζουν στη σύγχρονη Γραμμική Άλγεβρα ότι το Ω είναι ένας διανυσματικός χώρος πάνω στο A. Αν το Ω είναι ένα σώμα, τότε το A είναι ένα υπόσωμά του και το πλήθος των στοιχείων της βάσης n, ονομάζεται βαθμός του Ω πάνω στο A. Χρησιμοποιεί δε τον συμβολισμό $(\Omega, A) = n$.

Ο Dedekind αν και δίνει ιδιαίτερη βαρύτητα στο πεδίο της έρευνάς του λέγοντας ότι *"...ο πλήρης προσδιορισμός όλων αυτών των σωμάτων*

Κ και η διερεύνηση των μεταξύ τους σχέσεων , αποτελεί το πιο σημαντικό καθήκον της άλγεβρας", εν τούτοις αναγνωρίζει ότι τα τελικά συμπεράσματα της θεωρίας των εξισώσεων προκύπτουν, όπως βρήκε ο Galois, από τη συστηματική μελέτη της Θεωρίας των Ομάδων. Έτσι συνεχίζει ορίζοντας τις ομάδες "μεταθέσεων" των σωμάτων.

Ορισμός 3.1.4. Ένα σύνολο Π αποτελούμενο από n διαφορετικές μεταθέσεις π ονομάζεται *ομάδα [Gruppe]* αν κάθεμία μπορεί να συνδυαστεί με μια άλλη και το αποτέλεσμα να περιέχεται πάντοτε στο Π.

Από τον ορισμό κατανοούμε ότι οι μεταθέσεις π, οι οποίες για τον Dedekind είναι ισομορφισμοί, αναφέρονται όλες στο ίδιο σώμα, δηλαδή είναι αυτομορφισμοί του υπό μελέτη σώματος. Ένα από τα κύρια αποτελέσματά του σχετικά με τη σύνδεση, μεταξύ ενός σώματος και της ομάδας ισομορφισμών του, είναι το θεώρημα[8, σελ.39]:

Θεώρημα 3.1.2. *Αν μια ομάδα Π αποτελείται από n διαφορετικές μεταθέσεις π ενός σώματος και αν A είναι το σώμα του Π, τότε $(M, A) = n$, (και το υπόλοιπο του Π είναι η ταυτοτική μετάθεση του A).*

Απόδειξη. Για να το αποδείξουμε, επιλέγουμε ένα σύνολο n αριθμών $a_r \in M$ με τέτοιο τρόπο ώστε οι ορίζουσες που δημιουργούνται από τους n^2, στο πλήθος, αριθμούς της μορφής $a_r\pi$ να μην μηδενίζονται. Αν με ω συμβολίσουμει κάθε καθορισμένο αριθμό που ανήκει στο M υπάρχει ένα και μόνο ένα σύνολο n αριθμών x_r που πληρούν τις n στο πλήθος γραμμικές εξισώσεις

$$\omega\pi = x_1(a_1p) + x_2(a_2p) + \cdots + x_n(a_np) \tag{3.5}$$

Εφόσον όλοι οι αριθμοί $\omega\pi$, $a\pi$, που εμφανιζονται,ανήκουν στο M, το ίδιο συμβαίνει για τους n αριθμούς x_r και κατά συνέπεια, αν με π' παραστήσουμε μια ειδική μετάθεση στο Π τότε από το παραπάνω σύστημα εξισώσεων (3.5) προκύπτει η σχέση:

$$\omega\pi\pi' = (x_1\pi')(a_1\pi\pi') + (x_2\pi')(a_2\pi\ pi') + \cdots + (x_n\pi')(a_n\pi\ pi')$$

η οποία, επειδή η ποσότητα $\pi\pi'$ κυμαίνεται σε όλο το σύνολο Π όπως κάνει και το π, μπορεί να παρασταθεί στη μορφή

$$\omega\pi = (x_1\pi')(a_1\pi) + (x_2\pi')(a_2\pi) + \cdots + (x_n\pi')(a_n\pi)$$

Η τελευταία σχέση σε συνδυασμό με το σύστημα (3.5) δίνει ότι $x_r\pi' = x_r$ οπότε οι n αριθμοί x_r ανήκουν όλοι στο σώμα A το οποίο είναι μονότιμο στο Π. Αφού ανάμεσα στις μεταθέσεις π βρίσκεται και η ταυτοτική μετάθεση του M, από το σύστημα εξισώσεων (3.5) παίρνουμε ότι κάθε αριθμός $\omega \in M$ είναι της μορφής

$$\omega = x_1a_1 + x_2a_2 + \cdots + x_na_n$$

όπου $x_r \in A$. Δηλαδή το M είναι πεπερασμένο πάνω στο A, ή αλλιώς $(M, A) \leq n$. Αφού υπάρχουν n διαφορετικές μεταθέσεις π του M, που είναι πολλαπλάσια της ταυτοτικής μετάθεσης του A, συμπεραίνουμε ότι $(M, A) = n$ και ότι το σύνολο των n, στο πλήθος, αριθμών της μορφής a_r είναι ανάγωγο στο A. □

Ο Dedekind παρατηρεί, σχεδόν πρόχειρα, στη συνέχεια ότι αν Π′ είναι μια υποομάδα της Π, τότε υπάρχει ένα σώμα Α′, ώστε $A \subset A' \subset M$, το οποίο ανήκει στην Π′, δηλαδή, κάθε αυτομορφισμός του Μ στην Π′ διατηρεί το Α′ σταθερό. Επιπλέον, λέει πως οι βαθμοί τους σχετίζονται, με τη σχέση

$$(M, A')(A', A) = (M, A)$$

Το αποτέλεσμα αυτό όταν θα εφαρμοστεί από τον Artin στην Θεωρία Galois, θα είναι ένα από τα σημεία κλειδιά της ανάπτυξής της. Στην πραγματικότητα πολλά από τα αποτελέσματα του Dedekind χρησιμοποιήθηκαν από τον Artin για την εξέλιξη και τη νέα διατύπωση της Θεωρίας Galois.

3.2 Θεμελιώδες Θεώρημα της Θεωρίας Galois

Για τα επόμενα 40 περίπου χρόνια, δεν σημειώνεται κάποια σημαντική εξέλιξη στη Θεωρία Galois. Η έλλειψη των δημοσιεύσεων πάνω στη θεωρία αυτή, στις αρχές του 20ου αιώνα, δεν αντανακλά την έλλειψη ενδιαφέροντος για το θέμα, αλλά απλώς το γεγονός ότι, όσον αφορά την κλασική παρουσίαση της θεωρίας, υπήρχαν ήδη, όπως είδαμε, καθοριστικές μελέτες. Η ενεργός έρευνα είχε προχωρήσει και σε άλλες περιοχές, έτσι η Θεωρία Galois θεωρήθηκε ως ένα κλειστό ζήτημα.

Η μόνη εξαίρεση σ' αυτή τη στασιμότητα, ήταν η εμφάνιση από τον Heinrich Weber, του άρθρου *"Die allgemeinen Grundlagen der Galois'schen Gleichungstheorie"* το 1893, καθώς και η παρουσίαση της Θεωρίας, με καινούργιες ιδέες, μέσα στο βιβλίο του *"Lehrbuch der*

Algebra" που εκδόθηκε το 1895. Η ανάπτυξη του Weber δεν περιορίζεται στο σώμα των ρητών, αλλά σε οποιοδήποτε σώμα. Αναγνωρίζεται σαφώς ότι η θεωρία ενδιαφέρεται μόνο με τις επεκτάσεις του σώματος των συντελεστών και τις ομάδες των αυτομορφισμών του από αυτές τις επεκτάσεις. Σ' αυτό το πλαίσιο ακόμη και η εξέταση της διαδικασίας της λύσης έχει δευτερεύουσα σημασία σε σύγκριση με τη μελέτη της φύσης της λύσης. Με την ίδια άποψη παρουσιάζεται και το έργο που αναμόρφωσε τελικά την Θεωρία Galois και ανήκει στον Artin.

3.2.1 Artin

Από τις πρώτες έρευνές του, ο Emil Artin ενδιαφερόταν για την αφηρημένη έννοια του σώματος και τη θεωρία των επεκτάσεων των σωμάτων. Ο ίδιος παρατηρεί σε μια διάλεξη που έδωσε το 1950:

> Από την μαθηματική νεότητά μου είμαι υπό την επήρεια της κλασικής θεωρίας του Galois. Αυτή η γοητεία με έχει αναγκάσει να επανέλθω στο θέμα ξανά και ξανά, και να προσπαθήσω να βρω νέους τρόπους για να αποδείξω τα θεμελιώδη θεωρήματα του.

Για να κατανοήσουμε τη ριζική αλλαγή που έφερε το έργο του Artin στη Θεωρία Galois, υπενθυμίζουμε ότι, μέχρι τότε, κάθε διατύπωση της θεωρίας Galois απαιτούσε την επινόηση κάποιας έκφρασης των ριζών της εξίσωσης που έπρεπε να επιλυθεί. Σ' αυτό, κεντρικό ρόλο διαδραμάτιζε το θεώρημα για την ύπαρξη ενός *"πρωταρχικού στοιχείου" ("primitive element")*. Αρχικά, υπήρχε η ρητή έκφραση που υπέθετε $n!$ τιμές, τέτοιες ώστε αυτές να είναι ρίζες μιας εξίσωσης, της οποίας οι ανάγωγοι παράγοντες οδηγούν στην ομάδα της εξίσωσης. Επίσης, υπήρχε η έκφραση της οποίας οι συζυγείς ήταν ρίζες της βοηθητικής εξίσωσης, της οποίας η ομάδα ήταν μία ομάδα πηλίκο στη συνθετική σειρά της ομάδας της εξίσωσης που έπρεπε να επιλυθεί.

Αλλά ο Artin έδωσε μια νέα επαναστατική ματιά στην θεωρία, και ανέλαβε να παρουσιάσει την ιδέα η οποία αναφέρεται έμμεσα από τον Galois και η οποία ανακοινώθηκε αν και δεν ακούστηκε από τους Dedekind και Weber: Η θεωρία ασχολείται με τη σχέση μεταξύ των επεκτάσεων ενός σώματος και των ομάδων αυτομορφισμών τους. Η αλγεβρική λύση των εξισώσεων είναι μόνο μια εφαρμογή. Έτσι ο Artin προσπάθησε να διατυπώσει τη θεωρία, ανεξάρτητα από την εφαρμογή. Η εκδοχή της Θεωρίας Galois του Artin δημοσιεύτηκε σε

δύο σειρές εκπαιδευτικών σημειώσεων, η μία το 1938 με τίτλο *"Foundations of Galois Theory"* για τις διαλέξεις του στο New York University και η άλλη το 1942 με τίτλο *"Galois Theory"*[1] για τις διαλέξεις που έδωσε στο University of Notre Dame στην Indiana των Η.Π.Α. Η αναγνώριση και αποδοχή του έργου του Artin, σε σχέση με αυτό του Dedekind και του Weber από τους οποίους όμως η επιρροή είναι φανερή, οφείλεται κυρίως στο ότι η εποχή την οποία παρουσιάστηκε ήταν πιο δεκτική σε αφηρημένες προσεγγίσεις μαθηματικών εννοιών.

Είναι αλήθεια ότι έννοιες της Θεωρίας των Σωμάτων είχαν χρησιμοποιηθεί και πριν από τον Artin σε εκδοχές της Θεωρίας Galois, όμως υπήρχαν μόνο ούτως ώστε να παρέχουν την έννοια ενός συνόλου στο οποίο επισυνάπτονται ρίζες των βοηθητικών εξισώσεων. Η εξέταση των ιδιοτήτων των σωμάτων αυτών δεν είχε βασικό ρόλο. Όμως στις αρχές του 20ου αιώνα Γερμανοί Μαθηματικοί όπως η Emma Noether, εξέτασαν λεπτομερώς τα σώματα και τις γενικές ιδιότητές τους. Ο Artin εκμεταλεύτηκε στο έπακρο τους καρπούς αυτής της εξέλιξης στη νέα διατύπωση της Θεωρίας Galois. Το σκεπτικό του ήταν ότι, εφόσον θέλει να αφήσει απ' έξω τις πρακτικές εφαρμογές της Θεωρίας, δεν χρειάζεται να συμπεριλάβει σ' αυτήν την επίπονη διαδικασία της ανακάλυψης και επισύναψης των διαδοχικών βοηθητικών επιλυουσών εξισώσεων στο σώμα των συντελεστών. Κατευθυνόμενος από την οπτική του Dedekind για την επέκταση ενός σώματος ώς διανυσματικό χώρο πάνω στο σώμα των συντελεστών, ο Artin άρχισε να μιλάει για για το *"σώμα διασπάσεως" ("splitting field")* ενός πολυωνύμου.Δεν έθετε θέμα για το ποιό συγκεκριμένο σώμα ήταν αυτό, ή για το πώς, κατά την πρακτική έννοια, κατασκευάστηκε. Ο Kronecker είχε αποδείξει ότι υπήρχε, είτε η εξίσωση ήταν επιλύσιμη με ριζικά είτε όχι. Αυτή όμως η έννοια είναι και η ιδιαιτερότητα της άποψης του Artin για τη Θεωρία Galois.

Ο Artin αντιλήφθηκε ότι η Θεωρία Galois είχε στην πραγματικότητα ως αντικείμενο, τη σχέση μεταξύ της επέκτασης ενός σώματος και της ομάδας των αυτομορφισμών του πάνω σε κάποιο αρχικό σώμα. Έτσι η ιστορική εφαρμογή από την οποία ξεκίνησε ο Galois, συρρικνώνεται σε ένα μόνο ερώτημα: αν το σώμα διασπάσεως ανήκει σε μια επέκταση με ριζικά του σώματος των συντελεστών.

Θα δούμε τώρα πως ο Artin παρουσίασε τη Θεωρία Galois με τη νέα μορφή[1]. Ξεκινά με μια παρουσίαση στοιχείων της Γραμμικής Άλγεβρας και βασιζόμενος σ' αυτήν, αναπτύσσει την ιδέα της επέκτασης ενός σώματος ως διανυσματικό χώρο πάνω στο αρχικό σώμα. Στη συνέχεια μιλάει για την αλγεβρική επέκταση ενός

σώματος. Ορίζει ένα στοιχείο a της επέκτασης E ενός σώματος ως *"αλγεβρικό" ("algebraic"* αν υπάρχει πολυώνυμο με συνυελεστές από το F το οποίο έχει ως ρίζα το a. Αποδεικνύει ότι το πολυώνυμο αυτό είναι μοναδικό, ανάγωγο στο F, με τον ελάχιστο βαθμό και μονικό[7]. Λέει ότι το σύνολο $F(a) \subset E$ αποτελείται από όλα τα στοιχεία θ της μορφής

$$\theta = c_0 + c_1 a + c_2 a^2 + \cdots + c_{n-1} a^{n-1} \quad \text{, όπου} \quad c_0, c_1, c_2, \cdots, c_{n-1} \in F$$

και μάλιστα ο βαθμός επέκτασης είναι $[F(a) : F] = n$ αφού ο διανυσματικός χώρος $F(a)$ παράγεται από τα γραμμικώς ανεξάρτητα στοιχεία

$$1, a, a^2, \cdots, a^{n-1}$$

αποτέλεσμα στο οποίο είχε καταλήξει και ο Dedekind. Διατυπώνει ένα θεώρημα ύπαρξης, το οποίο το αποδίδει στον Kronecker

Θεώρημα 3.2.1 (Kronecker). *Αν $f(x)$ είναι ένα πολυώνυμο σε ένα σώμα F, τότε υπάρχει μια επέκταση E του F στην οποία το $f(x)$ έχει μια ρίζα.*

Συνεχίζει δίνοντας τον ακόλουθο

Ορισμός 3.2.1. Αν E είναι ένα σώμα επέκτασης ενός σώματος F στο οποίο ένα πολυώνυμο $p(x) \in F[x]$ παραγοντοποιείται σε πρωτοβάθμιους παράγοντες, και αν το $p(x)$ δεν μπορεί να παραγοντοποιηθεί με τέτοιο τρόπο σε κανένα άλλο ενδιάμεσο σώμα B, δηλαδή $F \subset B \subset E$, τότε ονομάζουμε το E *σώμα διασπάσεως (ή σώμα ριζών)* για το $p(x)$. Επιπλέον λέμε ότι αν το E είναι σώμα διασπάσεως για το $p(x)$, οι ρίζες του $p(x)$ παράγουν το E.

και κατόπιν αποδεικνύει το ακόλουθο βασικό

Θεώρημα 3.2.2. *Αν $p(x)$ είναι πολυώνυμο σε ένα σώμα F, τότε υπάρχει ένα σώμα διασπάσεως E του $p(x)$.*

Απόδειξη. Παραγοντοποιούμε το πολυώνυμο $p(x)$ μέσα στο σώμα F σε ανάγωγους παράγοντες $f_1(x) \cdots f_r(x) = p(x)$. Αν κάθε ένας από αυτούς είναι πρώτου βαθμού, τότε το σώμα διασπάσεως που ζητούμε είναι το ίδιο το F. Ας υποθέσουμε λοιπόν ότι ο παράγοντας $f_1(x)$ είναι βαθμού μεγαλύτερου του πρώτου. Από το θεώρημα του Kronecker (3.2.1) υπάρχει μια επέκταση F_1 του σώματος F, στην οποία ο $f_1(x)$ έχει μία ρίζα. Παραγοντοποιούμε κάθε παράγοντα $f_1(x) \cdots f_r(x)$ σε

[7] ο συντελεστής του μεγιστοβάθμιου όρου είναι 1.

ανάγωγους παράγοντες και συνεχίζουμε ομοίως. Θα καταλήξουμε τελικά σε ένα σώμα στο οποίο το $p(x)$ θα αναλύεται σε πρωτοβάθμιους παράγοντες. Το σώμα που παράγεται από F με την προσάρτηση των ριζών του $p(x)$ είναι το ζητούμενο σώμα διασπάσεως. □

Δείχνει επιλέον ότι αυτό το σώμα διασπάσεως είναι μοναδικό και πεπερασμένου βαθμού ως προς F. Ορίζει τους ισομορφισμούς και αυτομορφισμούς των σωμάτων και εξετάζει τις ιδιότητές τους, για να δείξει ότι αν E είναι ένα σώμα επέκτασης του F, τότε το σύνολο των αυτομορφισμών του E που αφήνει αναλλοίωτο το F είναι μια ομάδα. Φτάνει κατόπιν σε ένα σημαντικό αποτέλεσμα, το οποίο είχε βρει και ο Dedekind, ότι αν $\sigma_1, \sigma_2, \cdots, \sigma_n$ είναι μια ομάδα αυτομορφισμών ενός σώματος E και αν F το σώμα που μένει αναλλοίωτο από αυτούς, τότε ο βαθμός επέκτασης του σώματος ισούται με την τάξη της ομάδας, δηλαδή $[E : F] = n$.

Ο Artin ακολούθως ορίζει διάφορους όρους, όπως

Ορισμός 3.2.2. Μια επέκταση E ενός σώματος F ονομάζεται *κανονική (normal)* αν η ομάδα G των αυτομορφισμών του E που αφήνουν αναλλοίωτο το F, έχει ως σταθερό σώμα το F και ο βαθμός επέκτασης $[E : F]$ είναι πεπερασμένος.

Ορισμός 3.2.3. Ένα πολυώνυμο $f(x)$ ονομάζεται *διαχωρίσιμο (separable)* αν οι ανάγωγοι παράγοντές του δεν έχουν πολλαπλές ρίζες. Αν E είναι μια επέκταση ενός σώματος F, τότε το στοιχείο $a \in E$ ονομάζεται *διαχωρίσιμο* αν είναι ρίζα ενός διαχωρίσιμου πολυωνύμου $f(x)$ στο F και η E ονομάζεται *διαχωρίσιμη* επέκταση αν κάθε στοιχείο της E είναι διαχωρίσιμο.

Αποδεικνύει μάλιστα το θεώρημα που συνδέει όλες τις παραπάνω έννοιες.

Θεώρημα 3.2.3. *Η επέκταση E ενός σώματος F είναι κανονική αν και μόνο αν το E είναι το σώμα διάσπασης ενός διαχωρίσιμου πολυωνύμου $p(x)$ στο F.*

Ο Artin φτάνει τώρα στο σημείο να ορίσει την ομάδα (Galois) μιας εξίσωσης

Ορισμός 3.2.4. Αν $f(x)$ είναι πολυώνυμο στο σώμα F και E είναι το σώμα διάσπασής του, τότε ονομάζουμε *ομάδα της εξίσωσης* $f(x)$, την ομάδα αυτομορφισμών του E πάνω στο F.

και στη συνέχεια να αποδείξει ένα θεώρημα το οποίο, κατά τον ίδιο, είναι το σημαντικότερο από όλα τα άλλα της Θεωρίας αυτής, αφού εξετάζει τη σχέση μεταξύ του σώματος διάσπασης και της ομάδας των αυτομορφισμών του. Γι αυτό του δίνει ένα όνομα με το οποίο είναι γνωστό ως σήμερα:

Θεώρημα 3.2.4 (Θεμελιώδες Θεώρημα της Θεωρίας Galois)**.** *Αν $p(x)$ είναι ένα διαχωρίσιμο πολυώνυμο σε ένα σώμα F, και G η ομάδα της εξίσωσης $p(x) = 0$ όπου E είναι το σώμα διάσπασης του $p(x)$ τότε:*

1. *κάθε ενδιάμεσο σώμα B, είναι το σταθερό σώμα μιας υποομάδας της G και διαφορετικές υποομάδες έχουν διαφορετικά σταθερά σώματα. Λέμε ότι τα B και G_B, "ανήκουν" ("belong") το ένα στο άλλο,*

2. *το ενδιάμεσο σώμα B είναι μια κανονική επέκταση του F, αν και μόνο αν, η υποομάδα G_B είναι μια κανονική υποομάδα της G. Σε αυτήν την περίπτωση η ομάδα των αυτομορφισμών του B οι οποίες αφήνουν το F αναλλοίωτο ειναι ισόμορφη με την ομάδα πηλίκο G/G_B,*

3. *για κάθε ενδιάμεσο σώμα B έχουμε $[B : F] =$ δείκτης της G_B και $[E : B] =$ τάξη της G_B.*

Με τον τρόπο αυτό, ο Artin συγκεντρώνει σε ένα θεώρημα τα κυριότερα συμπεράσματα της Θεωρίας Galois μεταμορφώνοντάς την όμως σε μια θεωρία σχετικά με τα σώματα και όχι σχετικά με τα πολυώνυμα.

Ο Artin συνδύασε όλες τις προηγούμενες προσεγγίσεις και έδωσε μια πολύ συνεκτική, ακριβή και σύγχρονη παρουσίαση της Θεωρίας Galois, σε μια εποχή που η μαθηματική κοινότητα ήταν τελικά σε θέση να την αναγνωρίσει ως αναπόσπαστο μέρος της αφηρημένης άλγεβρας. Από αυτό το σημείο, Θεωρία Galois δεν είχε πλέον καμία σχέση με την πρακτική κατασκευή των ριζών μιας εξίσωσης.

Μέρος ΙΙ

Θεωρία Galois

4

Θεωρία Galois

Στο δεύτερο μέρος της παρούσας εργασίας θα παρουσιάσουμε (εν συντομία) το περιεχόμενο της Θεωρίας Galois.[1]

Η Θεωρία Galois είναι ένας κλάδος της Αφηρημένης Άλγεβρας που συνδέει την θεωρία Σωμάτων με την θεωρία Ομάδων. Με τη χρήση της Θεωρίας Galois επιτυγχάνεται η απλοποίηση προβλημάτων της θεωρίας Σωμάτων αντιστοιχίζοντάς τα σε προβλήματα Ομάδων. Αρχικά ο Galois χρησιμοποίησε τις ομάδες μεταθέσεων για να περιγράψει το πώς οι διάφορες ρίζες μιας δεδομένης πολυωνυμικής εξίσωσης σχετίζονται μεταξύ τους. Η σύγχρονη προσέγγιση της θεωρίας Galois, που αναπτύχθηκε από τον Richard Dedekind, Leopold Kronecker και Emil Artin, μεταξύ άλλων, περιλαμβάνει τη μελέτη των αυτομορφισμών των επεκτάσεων των σωμάτων.

4.1 Στοιχειώδης προσέγγιση

Η στοιχειώδης (elementary) προσέγγιση της θεωρίας Galois γίνεται μέσω της ομάδας μεταθέσεων των ριζών ενός πολυωνύμου. Η κεντρική ιδέα είναι να εξετάσει τις μεταθέσεις των ριζών που έχουν την ιδιότητα ότι κάθε αλγεβρική εξίσωση που ικανοποιείται από τις ρίζες εξακολουθεί να ικανοποιείται και μετά από τη μετάθεση των ριζών. Στην παράγραφο αυτή §4.1 ο στόχος θα είναι να διαπιστωθεί ο λόγος που λειτουργεί η παραπάνω ιδέα και όχι η παρουσιασή της με αυστηρά Μαθηματικό τρόπο. Στην επόμενη παράγραφο §4.2, όπου θα δούμε τη σύγχρονη άποψη της Θεωρίας Galois, θα διατηρήσουμε μια πιο αυστηρή, από Μαθηματικης πλευράς, παρουσίαση.

[1] αναφορές από [3], [6], [34], [12], [31], [39]

Θεωρούμε την πολυωνυμική εξίσωση

$$x^n + \alpha_{n-1}x^{n-1} + \alpha_{n-2}x^{n-2} + \cdots + \alpha_1 x + \alpha_0 = 0$$

με ρητούς συντελεστές και ρίζες πολλαπλότητας 1. [2] Η εξίσωση μπορεί να αναπαρασταθεί καλύτερα από τη γενική της μορφή αν υπάρχουν πολυωνυμικές εκφράσεις ανάμεσα στις ρίζες $x_1, x_2, \cdots, x_n$. Κάθε τέτοια έκφραση αντιστοιχεί σε ένα πολυώνυμο που παίρνει τιμή 0 για τις ρίζες $x_1, \cdots, x_n$. Για παράδειγμα η σχέση $x_1^2 = x_2 + 2$ αντιστοιχεί στο πολυώνυμο $h(X_1, \cdots, X_n) = X_1^2 - X_2 - 2$ για το οποίο έχουμε $h(x_1, x_2) = 0$. Συμβολίζουμε με B_K το σύνολο αυτών των πολυωνύμων με συντελεστές από το σώμα K. Η καταγραφή όλων των στοιχείων του B_K είναι φυσικά πολύ δύσκολη (αν όχι αδύνατη). Το σύνολο αυτό είναι όλο και μεγαλύτερο όσο πιο απλή είναι η αρχική εξίσωση, αφού υπάρχουν όλο και πιο πολλές σχέσεις μεταξύ των ριζών. Έτσι αποτελεί ένα μέτρο "πολυπλοκότητας" της εξίσωσης. Στην προσέγγιση αυτής της "πολυπλοκότητας" θα φανεί χρήσιμη η μελέτη της Ομάδας Galois.

Ορισμός 4.1.1. Για μια πολυωνυμική εξίσωση χωρίς πολλαπλές ρίζες και με συντελεστές από ένα σώμα K, ονομάζουμε Ομάδα Galois το σύνολο όλων των μεταθέσεων σ της συμμετρικής ομάδας S_n οι οποίες μεταθέτουν τους δείκτες $1, \cdots, n$ των λύσεων $x_1, x_2, \cdots, x_n$ με τέτοιο τρόπο ώστε για κάθε πολυώνυμο $h(X_1, \cdots, X_n)$ με συντελεστές από το K και $h(x_1, \cdots, x_n) = 0$ να ισχύει $h(x_{\sigma(1)}, \cdots, x_{\sigma(n)}) = 0$.

Ο παραπάνω ορισμός δηλαδή εννοεί ότι οι μεταθέσεις των ριζών πρέπει να μετασχηματίζουν τα πολυώνυμα του B_K σε άλλα τα οποία ανήκουν πάλι στο B_K. Μία συνέπεια του ορισμού είναι πως όταν υπάρχουν στο B_K μόνο τα συμμετρικά πολυώνυμα (όπως π.χ. αυτά που προέρχονται από τους τύπους του Viete) τότε η Ομάδα Galois περιέχει όλες τις μεταθέσεις, έχει δηλαδή $n!$ στοιχεία.

Θα δούμε ένα παράδειγμα για να κατανοήσουμε πως η Ομάδα Galois δείχνει το βαθμό "πολυπλοκότητας" μιας εξίσωσης. Παίρνουμε την εξίσωση

$$x^4 - 4x^3 - 4x^2 + 8x - 2 = 0 \tag{4.1}$$

η οποία έχει λύσεις

$$x_{1,3} = 1 + \sqrt{2} \pm \sqrt{3 + \sqrt{2}}$$

[2] αν οι ρίζες x_i έχουν πολλαπλότητα k_i αντίστοιχα, τότε διαιρούμε το αρχικό πολυώνυμο με το $\prod(x - x_i)^{k_i - 1}$ ώστε να προκύψει ένα πολυώνυμο με απλές ρίζες.

Εμφύτευση ποσοτήτων	Σώματα επέκτασης	Ομάδα Galois
συντελεστές της εξίσωσης	$\mathbb{Q}$	$\sigma_0, \sigma_1, \sigma_2, \sigma_3,$ $\sigma_4, \sigma_5, \sigma_6, \sigma_7$
$\sqrt{2}$	$\mathbb{Q}(\sqrt{2})$	$\sigma_0, \sigma_1, \sigma_2, \sigma_3$
$\sqrt{3+\sqrt{2}}$	$\mathbb{Q}(\sqrt{2}, \sqrt{3+\sqrt{2}})$	σ_0, σ_2
$\sqrt{3-\sqrt{2}}$	$\mathbb{Q}(\sqrt{2}, \sqrt{3+\sqrt{2}}, \sqrt{3-\sqrt{2}})$	σ_0

Πίνακας 4.1: Στάδια προσδιορισμού της ομάδας Galois.

και

$$x_{2,4} = 1 - \sqrt{2} \pm \sqrt{3-\sqrt{2}}$$

Μπορούμε με πράξεις ανάμεσα στις ρίζες να διαπιστώσουμε ότι ισχύει η σχέση $x_1x_3 + x_2x_4 = 0$, ενώ $x_1x_4 + x_2x_3 \neq 0$ και $x_1x_2 + x_3x_4 \neq 0$. Αυτό σημαίνει ότι μόνο το πολυώνυμο $X_1X_3 + X_2X_4 \in B_{\mathbb{Q}}$ οπότε από τις $4! = 24$ μεταθέσεις των τεσσάρων στοιχείων μόνο οι 8 που αφήνουν το πολυώνυμο αυτό ανεπηρέαστο ανήκουν στην ομάδα Galois της εξίσωσης (4.1). Ας συμβολίσουμε τις μεταθέσεις αυτές:

$$\sigma_0 = (1234) \quad \sigma_1 = (3214) \quad \sigma_2 = (1432) \quad \sigma_3 = (3412)$$

$$\sigma_4 = (2143) \quad \sigma_5 = (4123) \quad \sigma_6 = (2341) \quad \sigma_7 = (4321)$$

Ξεκινώντας με το σώμα των ρητών $\mathbb{Q}$ ως σώμα των συντελεστών προσαρτούμε πρώτα την $\sqrt{2}$. Η προσάρτηση αυτή οδηγεί για παράδειγμα στο αποτέλεσμα ότι το πολυώνυμο

$$h_1(X_1 - X_2 + X_3 - X_4 - 4\sqrt{2}) \in B_{\mathbb{Q}(\sqrt{2})}$$

εφ' όσον, αν εκτελέσουμε τις πράξεις, διαπιστώνουμε ότι ισχύει

$$x_1 - x_2 + x_3 - x_4 = 4\sqrt{2}$$

Όμως οι τέσσερις μεταθέσεις $\sigma = \sigma_4, \sigma_5, \sigma_6, \sigma_7$ ικανοποιούν τη σχέση

$$x_{\sigma(1)} - x_{\sigma(2)} + x_{\sigma(3)} - x_{\sigma(4)} = -4\sqrt{2}$$

οπότε δεν ανήκουν πλέον στην ομάδα Galois (δηλαδή παραμένουν μόνο οι μεταθέσεις $\sigma_0, \sigma_1, \sigma_2, \sigma_3$) Έτσι μετά την επέκταση του σώματος $\mathbb{Q}$ στο $\mathbb{Q}(\sqrt{2})$ η ομάδα Galois μειώθηκε στο μισό. Επισυνάπτουμε τώρα τη δεύτερη ενδιάμεση ποσότητα $\sqrt{3+\sqrt{2}}$. Τώρα επειδή για παράδειγμα ισχύει $x_1 - x_3 = 2\sqrt{3+\sqrt{2}}$ έχουμε ότι το πολυώνυμο

$$h_2(X_1 - X_3 - 2\sqrt{3+\sqrt{2}}) \in B_{\mathbb{Q}(\sqrt{2}, \sqrt{3+\sqrt{2}})}$$

	σ_0	σ_2	σ_1	σ_3	σ_4	σ_5	σ_6	σ_7
σ_0	σ_0	σ_2	σ_1	σ_3	σ_4	σ_5	σ_6	σ_7
σ_2	σ_2	σ_0	σ_3	σ_1	σ_5	σ_4	σ_7	σ_6
σ_1	σ_1	σ_3	σ_0	σ_2	σ_6	σ_7	σ_4	σ_5
σ_3	σ_3	σ_1	σ_2	σ_0	σ_7	σ_6	σ_5	σ_4
σ_4	σ_4	σ_6	σ_5	σ_7	σ_0	σ_1	σ_2	σ_3
σ_5	σ_5	σ_7	σ_4	σ_6	σ_2	σ_3	σ_0	σ_1
σ_6	σ_6	σ_4	σ_7	σ_5	σ_1	σ_0	σ_3	σ_2
σ_7	σ_7	σ_5	σ_6	σ_4	σ_3	σ_2	σ_1	σ_0

Πίνακας 4.2: Πίνακας πολλαπλασιασμού της Ομάδας Galois.

Όμως για τις μεταθέσεις $\sigma = \sigma_1, \sigma_3$ ισχύει η εξίσωση

$$x_{\sigma(1)} - x_{\sigma(3)} = -2\sqrt{3+\sqrt{2}}$$

κι έτσι οι μεταθέσεις αυτές δεν ανήκουν πλέον στην Ομάδα Galois, οπότε πάλι μειώνεται στο μισό. (ενώ παραμένουν οι μεταθέσεις σ_0, σ_2) Τέλος προσαρτώντας την ποσότητα $\sqrt{3-\sqrt{2}}$ και οι τέσσερις λύσεις μπορούν να εκφραστούν ως συναρτήσεις στο $\mathbb{Q}(\sqrt{2}, \sqrt{3+\sqrt{2}}, \sqrt{3-\sqrt{2}})$. Μπορούμε συνεπώς να πάρουμε τα πολυώνυμα $X_i - x_i,\ i = 1, \cdots, 4$ και τότε η Ομάδα Galois θα περιέχει μόνο την ταυτοτική μετάθεση σ_0. Ο πίνακας 4.1 συνοψίζει τις μεταβολές που περιγράψαμε.

Από αυτά καταλαβαίνουμε ότι αρκεί η αρχική Ομάδα Galois του πολυωνύμου να έχει μια σταδιακή "μείωση" μέχρι την ταυτοτική μετάθεση σ_0 για να μπορεί η αρχική εξίσωση να είναι επιλύσιμη με ριζικά. Μπορούμε να δούμε αυτή τη "μείωση" και στον πίνακα πολλαπλασιασμού 4.2 της Ομάδας Galois, όπου ο πίνακας ελαττώνεται προς τα πάνω και αριστερά (με τις μεταθέσεις κατάλληλα διατεταγμένες). Να λοιπόν πως η Ομάδα Galois περιέχει τις πληροφορίες που χρειαζόμαστε για να αποφανθούμε αν μια εξίσωση είναι επιλύσιμη με ριζικά. Προκύπτει λοιπόν το θεώρημα

Θεώρημα 4.1.1. *Μία ανάγωγη εξίσωση είναι επιλύσιμη με ριζικά όταν η Ομάδα Galois μπορεί σταδιακά να ελαττωθεί σε ομάδα του ενός στοιχείου: της ταυτοτικής μετάθεσης, όπου κάθε βήμα αντιστοιχεί στην ελάττωση του (κατάλληλα ταξινομημένου) πίνακα πολλαπλασιασμού σε $\nu \times \nu$ τετράγωνα.*

Η ερώτηση βέβαια που προκύπτει είναι πως θα βρούμε την ομάδα Galois αν δεν γνωρίζουμε τις ρίζες της εξίσωσης. Ο ίδιος ο Galois

επινόησε μια τεχνική για να αντιμετωπίσει αυτό ακριβώς το προβλημα, χρησιμοποιώντας τη λεγόμενη "επιλύουσα" του Galois *(Galois resolvent)* η οποία όμως περιέχει δυσκολίες στο χειρισμό της και δεν κρίνεται σκόπιμο να αναφερθεί στην παρούσα εργασία. Γι αυτό το λόγο έχει επικρατήσει η "σύγχρονη" άποψη της Θεωρίας Galois η οποία βασίζεται στις Αλγεβρικές Δομές και θα εξετασθεί στην αμέσως επόμενη ενότητα.

4.2 Σύγχρονη προσέγγιση

Στη στοιχειώδη προσέγγιση που είδαμε, ο Galois μιλάει για πολυώνυμα με συντελεστές από ένα σώμα $K \subseteq \mathbb{C}$, όπου οι ρίζες του πολυωνύμου ορίζουν μαζί με το K ένα άλλο σώμα L ίσως μεγαλύτερο. Στη σύγχρονη (modern) προσέγγιση χρησιμοποιούμε τις αφηρημένες αλγεβρικές δομές, έτσι ξεκινάμε με μια επέκταση L/K (διαβάζεται: L πάνω στο K) του σώματος K, και εξετάζουμε την ομάδα των αυτομορφισμών της L/K (αυτές είναι απεικονίσεις της μορφής $\alpha : L \mapsto L,\ \alpha(x) = x$ για όλα τα $x \in$ K).

Η σύνδεση μεταξύ των δύο προσεγγίσεων είναι η εξής. Οι συντελεστές του πολυωνύμου που μελετάμε πρέπει να επιλεχθούν από το βασικό σώμα K. Το σώμα επέκτασης L θα πρέπει να είναι το σώμα που προκύπτει από την προσάρτηση των ριζών του εν λόγω πολυωνύμου στο αρχικό σώμα. Κάθε μετάθεση των ριζών που διατηρεί την αλγεβρική εξίσωση, οδηγεί σε έναν αυτομορφισμό του L/K και αντιστρόφως. Στην πραγματικότητα η ομάδα αυτομορφισμών και η ομάδα μεταθέσεων είναι μεταξύ τους ισόμορφες.[3]

Για να δούμε τη σύγχρονη προσέγγιση, θα αναφέρουμε τους απαραίτητους ορισμούς και τα θεωρήματα που χρειαζόμαστε.[4] Θεωρούμε πάλι την πολυωνυμική εξίσωση

$$x^n + \alpha_{n-1}x^{n-1} + \alpha_{n-2}x^{n-2} + \cdots + \alpha_1 x + \alpha_0 = 0$$

με ρητούς συντελεστές και ρίζες πολλαπλότητας 1. Ο στόχος είναι να εξετάσουμε αν η εξίσωση μπορεί να λυθεί με ριζικά, δηλαδή μόνο με χρήση των τεσσάρων βασικών πράξεων και την εξαγωγή ριζών στο σώμα των συντελεστών.

[3]μια απόδειξη του ισομορφισμού αυτού βρίσκεται στο [6, ΚΕΦ. 6]

[4]Ορισμοί και θεωρήματα που πρέπει να γνωρίζουμε από την βασική Άλγεβρα δίνονται στο παράρτημα

Ορισμός 4.2.1. Έστω στοιχείο α που ανήκει σε ένα σώμα επέκτασης $L \subset F$. Ονομάζουμε ελάχιστο πολυώνυμο του α ένα μη σταθερό πολυώνυμο $p(x)$ τέτοιο ώστε να ισχύουν:

- $p(\alpha) = 0$
- αν οποιοδήποτε άλλο πολυώνυμο $f \in F[x]$ έχει ρίζα το α, αυτό να είναι πολλαπλάσιο του $p(x)$.

Αξίζει να αναφέρουμε το βασικό θεώρημα των συμμετρικών πολυωνύμων το οποίο παίζει σημαντικό ρόλο στη Θεωρία Galois. Πρώτα δίνουμε δυο ορισμούς:

Ορισμός 4.2.2. Ονομάζουμε στοιχειώδη συμμετρικά πολυώνυμα των μεταβλητών t_i τα πολυώνυμα

$$\sigma_1 = \sum_i t_i \ , \quad \sigma_2 = \sum_{i<j} t_i t_j \ , \quad \sigma_3 = \sum_{i<j<k} t_i t_j t_k \ , \cdots , \sigma_n = \prod_{i=1}^{n} t_i$$

Ορισμός 4.2.3. Ένα πολυώνυμο $p(t_1, \cdots, t_n)$ ονομάζεται συμμετρικό όταν παραμένει αναλλοίωτο ύστερα από μιά μετάθεση των μεταβλητών του t_i. Δηλαδη όταν

$$p(t_{\sigma(1)}, \cdots, t_{\sigma(n)}) = p(t_1, \cdots, t_n)$$

για κάθε μετάθεση σ των $\{1, \cdots, n\}$ στοιχείων.

Θεώρημα 4.2.1 (Θεώρημα Newton για τα συμμετρικά πολυώνυμα)**.** *Κάθε συμμετρικό πολυώνυμο με μεταβλητές $t_1, \cdots, t_n$ μπορεί να γραφεί με μοναδικό τρόπο ως πολυώνυμο των στοιχειωδών συμμετρικών πολυωνύμων $\sigma_1, \cdots, \sigma_n$.*

Η σημασία του παραπάνω θεωρήματος για τη Θεωρία Galois βρίσκεται στο γεγονός ότι ένα πολυώνυμο $p(x)$ με ρίζες $t_1, \cdots, t_n$ μπορεί να γραφεί συναρτήσει των στοιχειωδών συμμετρικών πολυωνύμων $\sigma_1, \cdots, \sigma_n$ ως εξής:

$$p(x) = x^n - \sigma_1 x^{x-1} + \cdots + (-1)^n \sigma_n$$

Δηλαδή οι συντελεστές του μπορούν να εκφράσουν τα στοιχειώδη συμμετρικά πολυώνυμα άρα και κάθε άλλο συμμετρικό πολυώνυμο.

Ορισμός 4.2.4. Έστω μια επέκταση σωμάτων $L \subset F$. Ονομάζουμε βαθμό επέκτασης και συμβολίζουμε με $[L : F]$ τη διάσταση του L αν αυτό ληφθεί ως διανυσματικός χώρος του F.

Για τους βαθμούς επέκτασης ισχύει το παρακάτω

Θεώρημα 4.2.2. *Αν για υποσώματα του $\mathbb{C}$ ισχύει $K_0 \subseteq K_1 \subseteq \cdots \subseteq K_n$ τότε*

$$[K_n : K_0] = [K_n : K_{n-1}][K_{n-1} : K_{n-2}] \cdots [K_1 : K_0]$$

Ορισμός 4.2.5. Ένα στοιχείο α του L είναι αλγεβρικό στο F, αν υπάρχει μη σταθερό πολυώνυμο με συντελεστές από το F για το οποίο το α είναι ρίζα. Αν δεν υπάρχει τέτοιο πολυώνυμο, τότε το α ονομάζεται υπερβατικο στο F.

Ορισμός 4.2.6. Μια επέκταση σωμάτων ονομάζεται πεπερασμένη αν ο βαθμός επέκτασής της είναι πεπερασμένος αριθμός

Ορισμός 4.2.7. Μια επέκταση σωμάτων $L \subset F$ ονομάζεται αλγεβρική αν κάθε στοιχείο του L είναι αλγεβρικό στο F.

Ορισμός 4.2.8. Μια επέκταση σωμάτων $L \subset F$ ονομάζεται σώμα αναλυσεως ενός πολυωνύμου $f \in F[x]$ βαθμού n πάνω στο σώμα F αν:

- $f = c(x - a_1) \cdots (x - a_n)$, όπου $c \in F$ και $a_i \in L$
- $L = F(a_1, \cdots, a_n)$

Ορισμός 4.2.9. Μια επέκταση σωμάτων $L \subset F$ ονομάζεται κανονική αν κάθε ανάγωγο πολυώνυμο $f \in F[x]$ που έχει μία ρίζα στο L, τότε αναλύεται εξ'ολοκλήρου στο L.

Ορισμός 4.2.10. Μια επέκταση σωμάτων $L \subset F$ ονομάζεται διαχωρίσιμη αν για κάθε στοιχείο $a \in L$ το ελάχιστο πολυώνυμό του αναλύεται (σε πρωτοβάθμιους παράγοντες) εξ'ολοκλήρου στο L.

Ορισμός 4.2.11. Έστω μια επέκταση σωμάτων $L \subset F$, όπου L το σώμα αναλύσεως ενός πολυωνύμου $f \in F[x]$. Ονομάζουμε Ομάδα Galois του πολυωνύμου το σύνολο των αυτομορφισμών του L οι οποίοι είναι ταυτοτικοί στο F. Δηλαδή:

$$Gal(L/F) = \{\sigma : L \mapsto L |\ \sigma \text{ είναι αυτομορφισμός }, \sigma(a) = a \quad \forall a \in F\}$$

Σχετικά με την Ομάδα Galois ισχύει το παρακάτω

Θεώρημα 4.2.3. *Αν L είναι το σώμα αναλύσεως ενός διαχωρίσιμου πολυωνύμου $f \in F[x]$, τότε η τάξη της Ομάδας Galois είναι $|Gal(L/F)| = [L : F]$*

Ορισμός 4.2.12. Μια πεπερασμένη επέκταση σωμάτων $L \subset F$ ονομάζεται επέκταση Galois αν ικανοποιείται ένα από τα παρακάτω:

- το L είναι το σώμα αναλύσεως ενός διαχωρίσιμου πολυωνύμου $f \in F[x]$
- το F είναι το σώμα σταθερών στοιχείων της Ομάδας Galois $Gal(L/F)$ όταν δρα πάνω στο L
- η επέκταση είναι διαχωρίσιμη και κανονική.

Ορισμός 4.2.13. Μια επέκταση σωμάτων $L \subset F$ ονομάζεται επέκταση με ριζικά αν υπάρχει μια ακολουθία σωμάτων

$$F = F_0 \subset F_1 \subset \cdots \subset F_{n-1} \subset F_n = L$$

ώστε για κάθε δείκτη $i = 1, 2, \cdots, n$ να υπάρχει $\gamma_i \in F_i$ με $F_i = F_{i-1}(\gamma_i)$, όπου $\gamma_i^{m_i} \in F_{i-1}$, $m_i > 0$

Ορισμός 4.2.14. Μία ομάδα ονομάζεται επιλύσιμη αν υπάρχει μια ακολουθία κανονικών υποομάδων της μορφής

$$\{e\} = H_n \lhd H_{n-1} \cdots \lhd H_2 \lhd H_1 \lhd G$$

όπου όλα τα πηλίκα H_{i-1}/H_i είναι αβελιανές ομάδες.

Βασικό αποτέλεσμα της Θεωρίας Galois είναι το παρακάτω

Θεώρημα 4.2.4. *Έστω $F \subset L$ μία επέκταση Galois. Η επέκταση $F \subset L$ είναι επιλύσιμη αν και μόνο αν η Ομάδα Galois είναι επιλύσιμη ομάδα.*

4.3 Παραδείγματα

Παράδειγμα 1. Θεωρούμε το πολυώνυμο

$$f(x) = x^4 - 10x^2 + 1 \tag{4.2}$$

το οποίο έχει ρίζες

$$x_1 = \sqrt{2} + \sqrt{3}, \quad x_2 = \sqrt{2} - \sqrt{3}, \quad x_3 = -\sqrt{2} + \sqrt{3}, \quad x_4 = -\sqrt{2} - \sqrt{3}$$

Άρα οι ρίζες του πολυωνύμου (4.2) βρίσκονται στο σώμα $\mathbb{Q}(\sqrt{2}, \sqrt{3})$. Από το κριτήριο του Eisenstein, το $x^2 - 2$ είναι το ελάχιστο πολυώνυμο του $\sqrt{2}$ στο $\mathbb{Q}$. Έτσι $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$, οπότε $\mathbb{Q}(\sqrt{2}) = \{\alpha + \beta\sqrt{2}/\alpha, \beta \in \mathbb{Q}\}$

Επίσης από το ίδιο κριτήριο και επειδή $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$ έχουμε ότι το $x^2 - 3$ είναι το ελάχιστο πολυώνυμο του $\sqrt{3}$ στο $\mathbb{Q}(\sqrt{2})$, έτσι βρίσκουμε ότι

$$[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})] \cdot [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2 \cdot 2 = 4$$

Μπορούμε να δείξουμε ότι το σώμα επέκτασης $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ μπορεί να γραφεί και ως $\mathbb{Q}(\sqrt{2}+\sqrt{3})$. Αρχικά παρατηρούμε ότι $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}+\sqrt{3}) \subset \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Επίσης το πολυώνυμο (4.2) είναι το ελάχιστο πολυώνυμο του $\sqrt{2} + \sqrt{3}$ στο $\mathbb{Q}$, άρα $[\mathbb{Q}(\sqrt{2} + \sqrt{3}) : \mathbb{Q}] = 4$. Έτσι από τους βαθμούς επέκτασης των σωμάτων παίρνουμε ότι:

$$[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2}+\sqrt{3})] \cdot [\mathbb{Q}(\sqrt{2}+\sqrt{3}) : \mathbb{Q}] \Leftrightarrow 4 = x \cdot 4 \Leftrightarrow$$

$$\Leftrightarrow x = 1 \Longleftrightarrow [\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2}+\sqrt{3})] = 1 \Longleftrightarrow \mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2}+\sqrt{3})$$

Θα ερευνήσουμε τώρα την Ομάδα Galois του σώματος επέκτασης. Η Ομάδα Galois μεταθέτει τις ποσότητες $\sqrt{2}$ και $\sqrt{3}$ στις $\pm\sqrt{2}$ και $\pm\sqrt{3}$ αντίστοιχα. Επειδή $\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$ συμπεραίνουμε ότι η Ομάδα Galois έχει 4 στοιχεία και συγκεκριμένα είναι η υποομάδα

$$V = \{e, (12), (34), (12)(34)\} \subset \mathbb{S}_4$$

δηλαδή η λεγόμενη ομάδα του Klein. Η ομάδα αυτή είναι επιλύσιμη εφόσον υπάρχει η συνθετική σειρά $\{e\} \triangleleft V$ με την ομάδα πηλίκο $V/\{e\}$ αβελιανή ώς ομάδα τάξης 4.

Παράδειγμα 2. Θεωρούμε το πολυώνυμο

$$f(x) = x^3 - 2 \tag{4.3}$$

το οποίο έχει ρίζες

$$x_1 = \sqrt[3]{2}, \quad x_2 = \omega\sqrt[3]{2}, \quad x_3 = \omega^2\sqrt[3]{2}\text{ , όπου } \quad \omega = e^{\frac{2\pi i}{3}}$$

Άρα οι ρίζες του πολυωνύμου (4.3) βρίσκονται στο σώμα $\mathbb{Q}(\omega, \sqrt[3]{2})$.
Από το κριτήριο του Eisenstein, το $x^3 - 2$ είναι ανάγωγο πολυώνυμο κι έτσι είναι το ελάχιστο πολυώνυμο του $\sqrt[3]{2}$ στο $\mathbb{Q}$. Άρα $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$. Το πολυώνυμο $x^2 + x + 1$ έχει ρίζες ω και ω^2, αλλά από το κριτήριο του Eisenstein έχουμε ότι είναι ανάγωγο άρα είναι το ελάχιστο πολυώνυμο του ω στο $\mathbb{R}$ και επομένως και στο σώμα $\mathbb{Q}(\sqrt[3]{2}) \subset \mathbb{R}$, οπότε $[\mathbb{Q}(\omega, \sqrt[3]{2}) : \mathbb{Q}(\sqrt[3]{2})] = 2$. Έτσι βρίσκουμε ότι

$$[\mathbb{Q}(\omega, \sqrt[3]{2}) : \mathbb{Q}] = [\mathbb{Q}(\omega, \sqrt[3]{2}) : \mathbb{Q}(\sqrt[3]{2})] \cdot [\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 2 \cdot 3 = 6$$

Θα ερευνήσουμε τώρα την Ομάδα Galois του σώματος επέκτασης. Η Ομάδα Galois μεταθέτει τις τρεις ρίζες του πολυωνύμου εφόσον αυτό είναι ανάγωγο, δηλαδή ειναι ισόμορφη με την $\mathbb{S}_3$ και έχει 6 στοιχεία. Η ομάδα αυτή είναι επιλύσιμη εφόσον υπάρχει η συνθετική σειρά $\{e\} \triangleleft \mathbb{A}_3 \triangleleft \mathbb{S}_3$ με τις ομάδες πηλίκο $\mathbb{A}_3/\{e\}$ και $\mathbb{S}_3/\mathbb{A}_3$ να είναι αβελιανές αφού $[\mathbb{A}_3 : \{e\}] = 3$ και $[\mathbb{S}_3 : \mathbb{A}_3] = 2$ αντίστοιχα.

Παράδειγμα 3. Θα εξετάσουμε την περίπτωση του γενικού πολυωνύμου πέμπτου βαθμού

$$f(x) = x^5 + \alpha_4 x^4 + \alpha_3 x^3 + \alpha_2 x^2 + \alpha_1 x + \alpha_0 \tag{4.4}$$

Σύμφωνα με το Θεμελιώδες Θεώρημα της Άλγεβρας, έχει πέντε ρίζες στο σώμα $\mathbb{C}$ των μιγαδικών αριθμών. Έτσι η Ομάδα Galois είναι ισόμορφη με την ομάδα μεταθέσεων των πέντε στοιχείων $\mathbb{S}_5$. Θα προχωρήσουμε αναλύοντας την απόδειξη σε διακεκριμένα μέρη.

$\rightsquigarrow$ Η $\mathbb{A}_5$ είναι απλή ομάδα

Ορισμός 4.3.1. Μία ομάδα ονομάζεται απλή όταν οι μόνες κανονικές υποομάδες της είναι η τετριμμένη (δηλαδή αυτή που περιέχει μόνο το μοναδιαίο στοιχείο) και ο εαυτός της.

Λήμμα 4.3.1. *Κάθε άρτια μετάθεση παράγεται από 3-κύκλους.*

Απόδειξη. Οι άρτιες μεταθέσεις αποτελούνται από ζεύγη αντιμεταθέσεων για τα οποία υπάρχουν δύο περιπτώσεις:

1. $(ab)(bc)$ δηλαδή να έχουν ένα κοινό στοιχείο
2. $(ab)(cd)$ δηλαδή να μην έχουν κοινά στοιχεία

Στην πρώτη περίπτωση θα έχουμε $(ab)(bc) = (abc)$ αφού:

$$(ab)(bc) = \begin{pmatrix} a & b & c \\ b & a & c \end{pmatrix} \begin{pmatrix} a & b & c \\ a & c & b \end{pmatrix} = \begin{pmatrix} a & b & c \\ b & c & a \end{pmatrix} = (abc)$$

Στη δεύτερη περίπτωση θα ισχύει:

$$(ab)(cd) = (ab)(bc)(bc)(cd) = (abc)(bcd)$$

□

Λήμμα 4.3.2. *Μία κανονική υποομάδα H της $\mathbb{A}_5$ περιέχει τουλάχιστον έναν 3-κύκλο.*

Απόδειξη. Αφού η Η είναι υποσύνολο της $\mathbb{A}_5$ θα περιέχει στοιχεία τάξης 5, 3 ή 2, δηλαδή αν $\sigma \in H$ τότε είναι άρτια μετάθεση της μορφής:

1. $\sigma = (abcde)$ ή
2. $\sigma = (ab)(cd)$ ή
3. $\sigma = (abc)$

Εξετάζουμε τώρα κάθε περίπτωση ξεχωριστά.

1. Αν $\sigma = (abcde)$ τότε ονομάζουμε $\tau = (ab)(cd) \in \mathbb{A}_5$, οπότε βρίσκουμε

$$\tau\sigma\tau^{-1} = (ab)(cd)(abcde)(ab)(cd) = (adceb) = \sigma'$$

   Όμως η Η είναι κανονική στην $\mathbb{A}_5$ άρα $\sigma' = \tau\sigma\tau^{-1} \in H$ και επειδή η Η είναι ομάδα θα ισχύει $\sigma\sigma' \in H$ δηλαδή το στοιχείο $(abcde)(adceb) = (aec)$ το οποίο είναι ένας 3-κύκλος περιέχεται στην Η.

2. Αν $\sigma = (ab)(cd)$ τότε ονομάζουμε $\tau = (abe) \in \mathbb{A}_5$, οπότε βρίσκουμε

$$\tau\sigma\tau^{-1} = (abe)(ab)(cd)(aeb) = (be)(cd) = \sigma'$$

   Όμως η Η είναι κανονική στην $\mathbb{A}_5$ άρα $\sigma' = \tau\sigma\tau^{-1} \in H$ και επειδή η Η είναι ομάδα θα ισχύει $\sigma\sigma' \in H$ δηλαδή το στοιχείο $(ab)(cd)(be)(cd) = (abe)$ το οποίο είναι ένας 3-κύκλος περιέχεται στην Η.

3. Αν $\sigma = (abc)$ τότε η Η περιέχει τουλάχιστον έναν 3-κύκλο, τον σ.

Δείξαμε λοιπόν ότι αν $H \neq \{e\}$ με $H \triangleleft \mathbb{A}_5$, τότε περιέχει τουλάχιστον έναν 3-κύκλο, έστω τον $(abc) \in H$. □

Λήμμα 4.3.3. *Αν μία κανονική υποομάδα Η της $\mathbb{A}_5$ περιέχει τουλάχιστον έναν 3-κύκλο, τότε περιέχει και όλους τους κύκλους του ίδιου μήκους.*

Απόδειξη. Έστω $(abc) \in H$. Θεωρούμε τις μετατάξεις:

$$s = \begin{pmatrix} a & b & c & d & e \\ x & y & z & s & t \end{pmatrix} \in \mathbb{A}_5 \quad \text{και} \quad s' = \begin{pmatrix} a & b & c & d & e \\ x & y & z & t & s \end{pmatrix} \in \mathbb{A}_5$$

τότε

$$s(abc)s^{-1} = \begin{pmatrix} a & b & c & d & e \\ x & y & z & s & t \end{pmatrix} \begin{pmatrix} a & b & c & d & e \\ b & c & a & d & e \end{pmatrix} \begin{pmatrix} x & y & z & s & t \\ a & b & c & d & e \end{pmatrix} =$$

$$= \begin{pmatrix} x & y & z & s & t \\ y & z & x & s & t \end{pmatrix} = (xyz)$$

και

$$s'(abc)s'^{-1} = \begin{pmatrix} a & b & c & d & e \\ x & y & z & t & s \end{pmatrix} \begin{pmatrix} a & b & c & d & e \\ b & c & a & d & e \end{pmatrix} \begin{pmatrix} x & y & z & t & s \\ a & b & c & d & e \end{pmatrix} =$$

$$= \begin{pmatrix} x & y & z & s & t \\ y & z & x & s & t \end{pmatrix} = (xyz)$$

Αφού όμως οι s και s' διαφέρουν κατά μία αντιμετάθεση, θα ισχύει ότι μια από τις δύο είναι άρτια , δηλαδή ανήκει στην $\mathbb{A}_5$, οπότε αφού η Η είναι κανονική θα έχουμε $(xyz) \in H$. Επειδή όμως η (xyz) είναι τυχαία συμπεραίνουμε ότι η Η περιέχει όλους τους 3-κύκλους □

Προταση 4.3.1. *Η ομάδα $\mathbb{A}_5$ είναι απλή.*

Απόδειξη. Έστω $H \triangleleft \mathbb{A}_5$, με $H \neq \{e\}$. Εφόσον κάθε άρτια μετάθεση παράγεται σύμφωνα με το Λήμμα 4.3.1 από 3-κύκλους, αλλά η Η περιέχει σύμφωνα με το Λήμμα 4.3.2 τουλάχιστον έναν 3-κύκλο, άρα και όλους τους 3-κύκλους σύμφωνα με το Λήμμα 4.3.3, τότε είναι όλη η $\mathbb{A}_5$. Άρα μια κανονική υποομάδα της είναι είτε η τετριμμένη είτε η $\mathbb{A}_5$, συνεπώς η $\mathbb{A}_5$ είναι απλή. □

$\rightsquigarrow$ Η $\mathbb{S}_5$ είναι μη επιλύσιμη ομάδα

Η ομάδα $\mathbb{S}_5$ έχει προφανώς μια κανονική υποομάδα, την $\mathbb{A}_5$ αφού $[\mathbb{S}_5 : \mathbb{A}_5] = 2$. Έστω ότι Η είναι μία άλλη κανονική υποομάδα της $\mathbb{S}_5$. Θα δείξουμε ότι τότε ισχύει μία μόνο από τις περιπτώσεις:

1. $H = \{e\}$ ή
2. $H = \mathbb{A}_5$ ή
3. $H = \mathbb{S}_5$

Πρώτα θα χρειαστούμε τα παρακάτω

Λήμμα 4.3.4 (Τύπος γινομένου)**.** *Αν A και B δύο πεπερασμένες υποομάδες μιας ομάδας G, τότε*

$$|AB| = \frac{|A||B|}{|A \cap B|}$$

Απόδειξη. Έστω

$$x_1(A \cap B), x_2(A \cap B), \cdots, x_k(A \cap B)$$

τα αριστερά σύμπλοκα της τομής $A \cap B$ στην ομάδα A, δηλαδή $|A/A \cap B| = k$. Έχουμε ότι αν $i \neq j$ τότε το $x_j^{-1}x_i$ δεν είναι στοιχείο της τομής, αφού σε αντίθετη περίπτωση για κάθε $h_1 \in A \cap B$ θα υπάρχει κάποιο $h_2 \in A \cap B$ τέτοιο ώστε $x_j^{-1}x_ih_1 = h_2 \Leftrightarrow x_ih_1 = h_2x_j$, άτοπο αφού το $x_ih_1 \in x_i(A \cap B)$ και το $x_jh_2 \in x_j(A \cap B)$ ενώ όπως γνωρίζουμε τα σύμπλοκα μιας ομάδας είναι διακεκριμένα, δηλαδή δεν έχουν κοινά στοιχεία. Έστω τώρα ab ένα τυχαίο στοιχείο της ομάδας AB. Τότε επειδή κάθε στοιχείο της A ανήκει στην $x_i(A \cap B)$ για κάποιο $1 \leq i \leq k$, μπορούμε να γράψουμε το a στη μορφή x_ig όπου g στοιχείο της τομής, έχουμε δηλαδή $ab = (x_ig)b = x_i(gb)$. Αφού τα g και b ανήκουν στην B, αυτό σημαίνει ότι το ab είναι στοιχείο του συνόλου x_iB. Επιπλέον τα σύνολα $x_iB(i = 1, \cdots, k)$ είναι επίσης διακεκριμένα, ειδάλλως αν ίσχυε $x_iB = x_jB$ για κάποια i και j τότε το $x_j^{-1}x_i$ θα ήταν και στοιχείο του B. Εφόσον όμως τα στοιχεία x_i και x_j ανήκουν και στην υποομάδα A, συμπεραίνουμε ότι το $x_j^{-1}x_i$ ανήκει στην τομή $A \cap B$, άτοπο όπως δείξαμε στην αρχή. Δείξαμε λοιπόν ότι η B διαμερίζει την AB σε σύμπλοκα της μορφής x_iB όπου $1 \leq i \leq k$ και άρα $|AB/B| = k$. Συμπεράινουμε επομένως ότι $|\frac{A}{A \cap B}| = k = |\frac{AB}{B}| \Rightarrow \frac{|A|}{|A \cap B|} = \frac{|AB|}{|B|}$ το οποίο συνεπάγεται τη ζητούμενη σχέση $|AB| = \frac{|A||B|}{|A \cap B|}$ □

Λήμμα 4.3.5. *Αν H κανονική υποομάδα της $\mathbb{S}_5$ τότε η $H \cap \mathbb{A}_5$ είναι μια κανονική υποομάδα της $\mathbb{A}_5$.*

Απόδειξη. Για κάθε στοιχείο $a \in H \cap \mathbb{A}_5$ θα έχουμε ότι:

- $a \in H \cap \mathbb{A}_5$ άρα και $a \in \mathbb{A}_5$ οπότε για ένα στοιχείο $\gamma \in \mathbb{A}_5$, αφού η $\mathbb{A}_5$ είναι ομάδα, θα ισχύει ότι $\gamma a \gamma^{-1} \in \mathbb{A}_5$
- $a \in H \cap \mathbb{A}_5$ άρα και $a \in H$ οπότε για ένα στοιχείο $\gamma \in \mathbb{A}_5 \Rightarrow \gamma \in G$ (εφόσον η $\mathbb{A}_5$ είναι υποομάδα της G), αφού η H είναι κανονική υποοομάδα της G, θα ισχύει ότι $\gamma a \gamma^{-1} \in H$

Συνεπώς $\forall a \in H \cap \mathbb{A}_5, \gamma \in \mathbb{A}_5 \Rightarrow \gamma a \gamma^{-1} \in H \cap \mathbb{A}_5$ δηλαδή $\gamma(H \cap \mathbb{A}_5)\gamma^{-1} = H \cap \mathbb{A}_5$, οπότε η υποομάδα $H \cap \mathbb{A}_5$ είναι μια κανονική υποομάδα της $\mathbb{A}_5$. □

Τώρα είμαστε σε θέση να αποδείξουμε την τελική πρόταση.

Προταση 4.3.2. *Αν H κανονική υποομάδα της $\mathbb{S}_5$ τότε είτε $H = \{e\}$, είτε $H = \mathbb{A}_5$, είτε $H = \mathbb{S}_5$.*

Απόδειξη. Το προηγούμενο Λήμμα 4.3.5 σε συνδυασμό με την Πρόταση 4.3.1, μας οδηγεί στο συμπέρασμα ότι είτε $H \cap \mathbb{A}_5 = \{e\}$, είτε $H \cap \mathbb{A}_5 = \mathbb{A}_5$. Θα εξετάσουμε την κάθε περίπτωση.

- αν $H \cap \mathbb{A}_5 = \{e\}$, από το Λήμμα 4.3.4 και επειδή το σύνολο $H\mathbb{A}_5$ περιέχει το πολύ όλα τα στοιχεία της $\mathbb{S}_5$ βλέπουμε ότι: $\frac{|H||\mathbb{A}_5|}{|H \cap \mathbb{A}_5|} = |H\mathbb{A}_5| \Rightarrow \frac{|H|60}{1} \leq 120$. Εφόσον όμως $|H| \in \mathbb{N}^*$ θα έχουμε ότι $|H| = 1 \Rightarrow H = \{e\}$ οπότε αποδείχθηκε, είτε $|H| = 2$. Σ'αυτή την περίπτωση το Η εκτός του μοναδιαίου θα περιέχει και ένα στοιχείο τάξης 2, δηλαδή της μορφής (ab) ή $(ab)(cd)$. Επειδή όμως είμαστε στην περίπτωση που $H \cap \mathbb{A}_5 = \{e\}$, το στοιχείο αυτό δεν θα είναι άρτια μετάθεση, συνεπώς η κανονική υποομάδα είναι η $H = \{e, (ab)\}$. Σύμφωνα όμως με προηγούμενο Λήμμα, περίπτωση του Λήμματος 4.3.3 για κύκλους μήκους 2, θα πρέπει να περιέχει και όλα τα στοιχεία της μορφής $(ab) \in \mathbb{S}_5$, το οποίο είναι άτοπο αφού η Η περιέχει μόνο δύο στοιχεία.

- αν $H \cap \mathbb{A}_5 = \mathbb{A}_5$ τότε εφόσον δεν υπάρχει υποομάδα Κ της $\mathbb{S}_5$ τέτοια ώστε $60 < |K| < 120$ αφού δεν θα διαιρούσε την τάξη της $\mathbb{S}_5$, συμπεραίνουμε ότι $H = \mathbb{A}_5$ ή $H = \mathbb{S}_5$.

□

Συνεπώς από την Πρόταση 4.3.2 συμπεράινουμε ότι η μοναδική κανονική γνήσια και μη τετριμμένη υποομάδα της $\mathbb{S}_5$ είναι η $\mathbb{A}_5$ η οποία είναι απλή. Αυτό σημαίνει πως η μόνη συνθετική σειρά για την $\mathbb{S}_5$ είναι η

$$\{e\} \triangleleft \mathbb{A}_5 \triangleleft \mathbb{S}_5$$

Όμως, ενώ $|\mathbb{S}_5/\mathbb{A}_5| = 2$ οπότε το πηλίκο είναι αβελιανό, η $\mathbb{A}_5$ δεν είναι αβελιανή και έτσι το πηλίκο $\mathbb{A}_5/\{e\} \cong \mathbb{A}_5$ δεν είναι αβελιανό, συνεπώς η ομάδα $\mathbb{S}_5$ δεν είναι επιλύσιμη και άρα το γενικό πολυώνυμο πέμπτου βαθμού δεν είναι επιλύσιμο με ριζικά.

Βιβλιογραφία

[1] Emil Artin. *Galois Theory*. The University of Notre Dame Press, 1942.

[2] Enrico Betti. Sulla risoluzione delle equazioni algebriche. *Annali di scienze matematiche e fisiche*, vol.3:p.49–115, 1852.

[3] Jörg Bewersdorff. *Galois Theory for Beginners: A Historical Perspective*. American Mathematical Society, 2006.

[4] Girolamo Cardano. *Ars Magna, or the Rules of Algebra*. Dover Publications, 1993.

[5] Augustin-Louis Cauchy. Mémoire sur le nombre des valeurs qu'une fonction peut acquérir, lorsqu'on y permute de toutes les manières possibles les quantités qu'elles renferment. *Journal de l'École polytechnique*, no10:p.1–28, 1815.

[6] David A. Cox. *Galois Theory*. Wiley-Interscience, 2004.

[7] Amy Dahan. Les Travaux de Cauchy sur les Substitutions. Étude de son approche du concept de groupe. *Archive for History of Exact Sciences*, 23:279–319, 1980. 10.1007/BF00327913.

[8] Edward T. Dean. Dedekind's Treatment of Galois Theory in the Vorlesungen. Technical Report Paper 106, Department of Philosophy - Carnegie Mellon University, December 2009.

[9] Paul Dupuy. La vie d'Évariste Galois. *Annales scientifiques de l'École Normale Supérieure*, Sér.3, vol.13:p. 197–266, 1896.

[10] Heinz-Dieter Ebbinghaus, Hans Hermes, Friedrich Hirzebruch, Max Koecher, Klaus Mainzer, Jürgen Neukirch, Alexander Prestel, and

Reinhold Remmert. *Numbers*. Graduate texts in mathematics. Springer, 1991.

[11] Harold M. Edwards. *Galois Theory*. Springer, 1984.

[12] Jean-Pierre Escofier. *Théorie de Galois : Cours et exercices corrigés*. Dunod, 2nd edition, 2003.

[13] Benjamin Fine and Gerhard Rosenberger. *The Fundamental Theorem of Algebra*. Springer, 1997.

[14] H. Gray Funkhouser. A Short Account of the History of Symmetric Functions of Roots of Equations. *The American Mathematical Monthly*, Vol. 37(No. 7):pp. 357–365, Aug. - Sep. 1930.

[15] Christian Gilain. Sur l'histoire du théorème fondamental de l'algèbre. *Archive for history of exact sciences*, Vol. 42(No. 2):pp. 91–136, 1991.

[16] Albert Girard. *Invention nouvelle en l'Algèbre*. Blauew, 1629.

[17] Robin Rider Hamburg. The theory of equations in the 18th century: The work of Joseph Lagrange. *Archive for History of Exact Sciences*, Vol. 16(No. 1):pp. 17–36, 1976.

[18] Thomas L. Heath. *Diophantus Of Alexandria - A Study In The History Of Greek Algebra*. Cambridge University Press, 1910.

[19] Camille Jordan. *Traité des substitutions et des équations algébriques*. Gauthier-Villars, 1870.

[20] B. Melvin Kiernan. The Development of Galois Theory from Lagrange to Artin. *Archive for History of Exact Sciences*, Vol. 8(No. 1-2):pp.40–154, January 1971.

[21] Israel Kleiner. Field Theory: From Equations to Axiomatization. *The American Mathematical Monthly*, Vol. 106(No. 7):pp. 677–684, 1999.

[22] Israel Kleiner. *A History of Abstract Algebra*. Birkhäuser Boston, 2007.

[23] Arthur Knoebel, Reinhard Laubenbacher, Jerry Lodder, and David Pengelley. *Mathematical Masterpieces: Further Chronicles by the Explorers*. Springer, 2007.

[24] Joseph Louis Lagrange. Réflexions sur la résolution algébrique des équations. *Nouveaux mémoires de l'Académie royale des sciences et belles-lettres de Berlin (reprinted in Oeuvres de Lagrange)*, pages pp. 205–422, 1770 & 1771.

[25] Michael Meo. The mathematical life of Cauchy's group theorem. *Historia Mathematica*, vol. 31(Number 2):p. 196–211, May 2004.

[26] Olaf Neumann. *Cyclotomy From Euler through Vandermonde to Gauss*, pages 323–362. Elsevier, 2007.

[27] Olaf Neumann. *The Shaping of Arithmetic after C.F. Gauss's Disquisitiones Arithmeticae*, chapter II.1 The Disquisitiones Arithmeticae and the Theory of Equations, pages 107–127. Springer-Verlag Berlin Heidelberg, 2007.

[28] Peter M. Neumann. The Concept of Primitivity in Group Theory and the Second Memoir of Galois. *Archive for History of Exact Sciences*, vol.60:p.379–429, 2006.

[29] Peter M. Neumann. *The Mathematical Writings of Évariste Galois*. Heritage of European Mathematics, 2011.

[30] Ivo Radloff. Évariste Galois: Principles and Applications. *Historia Mathematica*, vol.29(2):p.114–137, May 2002.

[31] Joseph Rotman. *Galois Theory*. Springer, 2nd edition, 1998.

[32] Joseph Serret. *Cours d'algebre supérieure*. Gauthier Villars, 3ème edition, 1866.

[33] Jacqueline Stedall. *From Cardano's Great Art to Lagrange's Reflections: Filling a Gap in the History of Algebra*. Heritage of European Mathematics). European Mathematical Society, 15 March 2011.

[34] Ian Stewart. *Galois Theory*. Chapman and Hall/CRC, 3rd edition, 2003.

[35] René Taton. Les relations d'Évariste Galois avec les mathématiciens de son temps. *Revue d'histoire des sciences et de leurs applications*, vol.1(1-2):pp. 114–130, 1947.

[36] Jean-Pierre Tignol. *Galois' Theory of Algebraic Equations*. World Scientific Publishing Company, 2001.

[37] Bartel L. Van Der Waerden. *A History of Algebra From al-Khwarizmi to Emmy Noether*. Springer, 1985.

[38] Bartel L. Van Der Waerden. *Η Αφύπνιση της Επιστήμης*. Πανεπιστημιακές Εκδόσεις Κρήτης, 2000.

[39] Wikipedia. Galois Theory. `http://en.wikipedia.org/wiki/Galois_theory`.

[40] Émile Picard. *OEuvres Mathématiques d'Évariste Galois*. Gauthiers-Villars, 1897.

[41] Évariste Galois. *Œuvres mathématiques publiées en 1846 dans le Journal de Liouville*. Jacques Gabay, 1989.