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"

Δ Ι Π Λ Ω Μ Α Τ Ι Κ Η Ε Ρ Γ Α Σ Ι Α

Θεωρία Galois: Διδακτικές και ιστορικές προσεγγίσεις

Ευάγγελος Παντελής
Δ201318

Επιβλέπων Συμβουλευτικής Επιτροπής

Ευάγγελος Ράπτης Καθηγητής

Αθήνα
Σεπτέμβριος 2015

Η παρούσα Διπλωματική Εργασία

εκπονήθηκε στα πλαίσια των σπουδών

για την απόκτηση του

Μεταπτυχιακού Διπλώματος Ειδίκευσης

που απονέμει το

Διαπανεπιστημιακό – Διατμηματικό Πρόγραμμα Μεταπτυχιακών Σπουδών στη

«Διδακτική και Μεθοδολογία των Μαθηματικών»

Εγκρίθηκε την 23η Οκτωβρίου 2015 από **Εξεταστική Επιτροπή** αποτελούμενη από τους :

Ονοματεπώνυμο	Βαθμίδα
▪ Ε. Ράπτη (Επιβλέπων)	Καθηγητής
▪ Δ. Λάππα	Αναπλ. Καθηγητής
▪ Γ. Ψυχάρη	Λέκτορας

Η εκπόνηση της παρούσας Διπλωματική Εργασία πραγματοποιήθηκε υπό την καθοδήγηση της **Συμβουλευτική Επιτροπής** αποτελούμενη από τους:

Ονοματεπώνυμο	Βαθμίδα
▪ Ε. Ράπτη (Επιβλέπων)	Ομοτ. Καθηγητή
▪ Δ. Βάρσο	Καθηγητή
▪ Δ. Λάππα	Αναπλ. Καθηγητή

Abstract

By the early 19th century no general solution of a general polynomial equation ‘by radicals’ was found despite considerable effort by many outstanding mathematicians. Eventually, the work of Abel and Galois led to a satisfactory framework for fully understanding this problem and the realization that the general polynomial equation of degree at least 5 could not always be solved by radicals.

This paper presents the progress and evolution of the concepts found in Galois theory, what people contributed and how they performed in the language of mathematics their innovative ideas.

Περίληψη

Από τις αρχές του 19ου αιώνα δεν είχε ανακαλυφτεί κάποια γενική λύση της γενικής πολυώνυμικης εξίσωσης «από ριζικά» παρά τις σημαντικές προσπάθειες από πολλούς διακεκριμένους μαθηματικούς. Τελικά, το έργο του Abel και Galois οδήγησε σε ένα ικανοποιητικό πλαίσιο για την πλήρη κατανόηση ότι η γενική πολυωνυμική εξίσωση μεγαλύτερη η ίση του $5^{ου}$ βαθμού δεν μπορούσε να λυθεί με ριζικά.

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.

Περιεχόμενα

Εισαγωγή

Η Θεωρία Γκαλουά είναι ο κλάδος της άλγεβρας που συνδέει τη θεωρία σωμάτων με τη θεωρία ομάδων. Πήρε το όνομά της από τον Γάλλο μαθηματικό Εβαρίστ Γκαλουά. Η Θεωρία Γκαλουά μας δίνει τρόπους για να πάρουμε πληροφορίες για επεκτάσεις σωμάτων μελετώντας συγκεκριμένες ομάδες που συνδέονται με αυτές τις επεκτάσεις.

Χρησιμοποιώντας τη θεωρία Γκαλουά, ορισμένα προβλήματα της θεωρίας σωμάτων μπορούν να αναχθούν σε προβλήματα της θεωρίας ομάδων, τα οποία είναι ευκολότερα και κατανοήσιμα.

Με την εκπόνηση της διπλωματικής αυτής εργασίας, θα μελετήσουμε διεξοδικά την ιστορία της Θεωρίας Galois. 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. Η γέννηση της θεωρίας Γκαλουά είχε σαν αρχικό κίνητρο το ακόλουθο ερώτημα, του οποίου η απάντηση είναι γνωστή σαν θεώρημα του Θεωρήματος Abel–Ruffini:

> *Γιατί δεν υπάρχει κανένας τύπος για την εύρεση των ριζών πολυωνύμου 5ου (και υψηλότερου) βαθμού με βάση τους συντελεστές του πολυωνύμου, χρησιμοποιώντας μόνο τις συνήθεις αλγεβρικές πράξεις (πρόσθεση, αφαίρεση, πολλαπλασιασμός, διαίρεση) και την βοήθεια των ριζών (τετραγωνικές ρίζες, κυβικές ρίζες κτλ.)*

Η θεωρία Γκαλουά δεν παρέχει μόνο μια όμορφη απάντηση στο ερώτημα αυτό, άλλα εξηγεί επίσης λεπτομερώς γιατί είναι δυνατών να λυθούν εξισώσεις (μέσω τύπων) 4ου το πολύ βαθμού και γιατί οι λύσεις τους λαμβάνουν μια συγκεκριμένη μορφή. Επιπλέον δίνει ένα σαφές εννοιολογικό περιεχόμενο, συχνά πρακτικό μέσω της αφήγησης, ποτέ μια εξίσωση υψηλότερου βαθμού μπορεί να λυθεί με αυτόν τον τρόπο (μέσω τύπων).

Σε αυτή την εργασία θα κάνουμε μια εκτενή αναφορά στην ιστορική διαδρομή της θεωρίας Γκαλουά. Πιο συγκεκριμένα στο $1^{ο}$ κεφάλαιο θα αναδείξουμε το πρόβλημα επίλυσης των πολυωνύμων μιας μεταβλητής και θα παρουσιάσουμε την πορεία επίλυσης των πολυωνύμων από την αρχαιότητα μέχρι την θεωρία του Galois.

Στο $2^{ο}$ κεφάλαιο θα ασχοληθούμε με τη Θεωρία ομάδων και τη Θεωρία σωμάτων, όπου μια σειρά από θεωρήματα, προτάσεις, λήμματα και παραδείγματα θα δοθούν προκειμένου να προσεγγίσουμε όσο δυνατόν καλύτερα το θέμα.

Στο 3ο κεφάλαιο θα δείξουμε ποια ήταν η θεωρία του Galois και η συμβολή της στην επίλυση πολυωνύμων με ριζικά. Τέλος θα βγάλουμε κάποια χρήσιμα συμπεράσματα.

Κεφάλαιο 1ο

Ιστορική εξέλιξη των μεθόδων επίλυσης πολυωνυμικών εξισώσεων

1.1 Πολυώνυμα

Η λέξη πολυώνυμο προέρχεται από το Ελληνικό πολύ, και το Λατινικό binomium, "binomial". Η λέξη εισήχθηκε στην λατινική γλώσσα από τον Franciscus Viete[1].

Στα μαθηματικά, τα πολυώνυμα είναι η απλούστερη τάξη μαθηματικών εκφράσεων (πέρα απ τους αριθμούς και τις εκφράσεις που αφορούν αριθμούς). Ένα πολυώνυμο είναι μια έκφραση κατασκευασμένη από μεταβλητές (που λέγονται επίσης άγνωστοι) και σταθερές (συνήθως αριθμοί άλλα όχι πάντα), χρησιμοποιώντας μόνο τις πράξεις της πρόσθεσης, αφαίρεσης, πολλαπλασιασμού, και μη αρνητικών ακεραίων δυνάμεων. Ωστόσο, επιτρέπεται η διαίρεση με σταθερά , επειδή η πολλαπλασιαστική αντιστροφή μιας μη μηδενικής σταθεράς είναι επίσης σταθερά.

Για παράδειγμα, $x^2 - \frac{x}{4} + 7$ είναι ένα πολυώνυμο, αλλά $x^2 - \frac{4}{x} + 7x^{\frac{3}{2}}$ είναι μια αλγεβρική έκφραση που δεν είναι πολυώνυμο, επειδή ο δεύτερος όρος περιέχει μια διαίρεση με την μεταβλητή x (ο όρος 4/x), και επίσης επειδή ο τρίτος όρος περιέχει έναν εκθέτη που δεν είναι μη αρνητικός ακέραιος (3/2).

Πολυώνυμο είναι αλγεβρική παράσταση σταθερών και μιας μεταβλητής που συνδέονται μεταξύ τους μόνο με τις πράξεις της πρόσθεσης και του πολλαπλασιασμού, ενώ η μεταβλητή μπορεί να εμφανίζεται υψωμένη σε διάφορες φυσικές δυνάμεις. Ουσιαστικά το πολυώνυμο είναι άθροισμα μονωνύμων της ίδιας μεταβλητής. Κάθε δύναμη εμφανίζεται μία φορά στο πολυώνυμο, δηλαδή στην τελική μορφή του αθροίσματος δεν εμφανίζονται δύο μονώνυμα με την ίδια δύναμη της μεταβλητής.

Συνήθως το πολυώνυμο της μεταβλητής x συμβολίζεται με P(x). Οι συντελεστές συμβολίζονται με ένα γράμμα με δείκτη συνήθως τη δύναμη της μεταβλητής που συνοδεύει. Ο σταθερός όρος έχει συνήθως δείκτη μηδέν. Έτσι, η γενική μορφή του πολυωνύμου είναι:

$$P(x)= \alpha_v x^v + \alpha_{v-1} x^{v-1} + ... + \alpha_1 x + \alpha_0$$

Σταθερό πολυώνυμο θεωρείται μια οποιαδήποτε σταθερά, ενώ αν η σταθερά είναι μηδέν, τότε το πολυώνυμο λέγεται μηδενικό πολυώνυμο. Βαθμός του πολυωνύμου ονομάζεται η μέγιστη δύναμη της μεταβλητής με μη μηδενικό συντελεστή. Σε σταθερό πολυώνυμο ορίζεται ως βαθμός του πολυωνύμου το μηδέν, ενώ σε μηδενικό πολυώνυμο δεν ορίζεται βαθμός.

[1] Ο Φρανσουά Βιέτ ήταν Γάλλος μαθηματικός, ο οποίος γεννήθηκε το 1540 και πέθανε το 1603.

Μία πολυωνυμική εξίσωση, καλείται επίσης αλγεβρική εξίσωση, είναι μία εξίσωση στην οποία ένα πολυώνυμο τίθεται ίσο με ένα άλλο πολυώνυμο. Στην περίπτωση μιας μεταβλητής πολυωνυμικής εξίσωσης, η μεταβλητή θεωρείται ως άγνωστη, και προσπαθούμε να βρούμε τις πιθανές τιμές για τις οποίες και τα δύο μέλη μιας εξίσωσης είναι ίσα για την ίδια τιμή (γενικά μπορεί να υπάρχουν περισσότερες από μία λύσεις). Μία πολυωνυμική εξίσωση έρχεται σε αντίθεση με μία πολυωνυμική ταυτότητα όπως $(x + y)(x – y) = x^2 – y^2$, όπου και τα δύο μέλη αντιπροσωπεύουν το ίδιο πολυώνυμο σε διαφορετικές μορφές, και σαν συνέπεια κάθε εκτίμηση και των δύο μελών δίνει σωστή ισότητα. Αυτό σημαίνει ότι μια πολυωνυμική ταυτότητα είναι μία πολυωνυμική εξίσωση για την οποία όλες οι πιθανές τιμές των αγνώστων είναι λύσεις.

Στην απλή άλγεβρα, δίνονται μέθοδοι για την λύση όλων των πρωτοβάθμιων και δευτεροβάθμιων πολυωνυμικών εξισώσεων μιας μεταβλητής. Υπάρχουν επίσης μέθοδοι για τριτοβάθμια και τεταρτοβάθμια. Για μεγαλύτερης τάξης, το θεώρημα Abel-Ruffini[2] βεβαιώνει ότι δεν μπορεί να υπάρξει μία γενική μέθοδος. Ωστόσο, μόνο η αριθμητική προσέγγιση των ριζών μπορεί να υπολογιστεί. Ο αριθμός των λύσεων μπορεί να μην υπερβαίνει τον βαθμό του πολυωνύμου, και είναι ίσος με τον βαθμό όταν οι μιγαδικές ρίζες υπολογίζονται με την δική τους πολλαπλότητα. Αυτό το γεγονός ονομάζεται Θεμελιώδες Θεώρημα της Άλγεβρας.

Η εκτίμηση των ριζών των πολυωνύμων, ή η "λύση αλγεβρικών εξισώσεων", είναι ανάμεσα στα παλαιότερα προβλήματα των μαθηματικών. Ωστόσο, η σημειογραφία που χρησιμοποιούμε σήμερα καθιερώθηκε μόλις τον 15ο αιώνα. Πριν από αυτό, οι εξισώσεις γράφονταν με λέξεις.

Κάθε πολυώνυμο P με μεταβλητή x αντιπροσωπεύει μία συνάρτηση, $f(x) = P$ (όπου οι λύσεις του x στο P αντιστοιχούν σε τιμές της f), ονομάζεται πολυωνυμική συνάρτηση του P, η εξίσωση του x που γίνεται $f(x) = 0$ είναι η πολυωνυμική εξίσωση που αντιστοιχεί στο P. Οι λύσεις αυτής της εξίσωσης, που ονομάζονται ρίζες του πολυωνύμου, είναι τα σημεία που μηδενίζεται η συνάρτηση f (είναι τα σημεία όπου το γράφημα της f τέμνει τον άξονα x). Ένας αριθμός a είναι μία λύση του P αν και μόνο αν το $x − a$ (βαθμού ένα ως προς x) διαιρεί το P. Αυτό μπορεί να σημαίνει ότι το $x − a$ διαιρεί το P περισσότερες από μία φορά: Εάν το $(x − a)^2$ διαιρεί το P τότε a καλείται πολλαπλή ρίζα του P, διαφορετικά a καλείται απλή ρίζα του P. Εάν P είναι ένα μη μηδενικό πολυώνυμο, υπάρχει η μεγαλύτερη δύναμη m όπως $(x − a)^m$ που διαιρεί το P, η οποία καλείται πολλαπλότητα της ρίζας a στο P. Όταν P είναι το μηδενικό πολυώνυμο, η αντίστοιχη πολυωνυμική εξίσωση είναι ασήμαντη, και σε αυτήν την περίπτωση είναι σύνηθες να παραλείπεται όταν με τους παραπάνω ορισμούς κάθε αριθμός μπορεί να είναι ρίζα ενός μηδενικού πολυωνύμου, με απροσδιόριστη (ή άπειρη) πολλαπλότητα. Με αυτήν

[2] Περισσότερα για το έργο του σε επόμενη ενότητα

την εξαίρεση, ο αριθμός των ριζών του P, ακόμη και να μετρηθεί με τις αντίστοιχες πολλαπλότητες, δεν μπορεί να υπερβαίνει τον βαθμό του P.

1.2 Ιστορική αναδρομή

1.2.1 $2^{ου}$ βαθμού εξίσωση

Στα μαθηματικά, δευτεροβάθμια εξίσωση ονομάζεται κάθε πολυωνυμική εξίσωση δευτέρου βαθμού. Η γενική μορφή μιας δευτεροβάθμιας εξίσωσης είναι:

$$ax^2 + \mathrm{bx} + \gamma = 0$$

όπου τα γράμματα α, β και γ παριστάνουν σταθερούς αριθμούς, με $\alpha \neq 0$

Οι σταθερές α, β και γ ονομάζονται συντελεστές, με το α να είναι ο συντελεστής του x^2, το β να είναι ο συντελεστής του x και γ ο σταθερός όρος. Οι συντελεστές μπορεί να είναι πραγματικοί ή μιγαδικοί αριθμοί.

Αιγύπτιοι, Κινέζοι και Βαβυλώνιοι μηχανικοί το 2000 π.χ. μπορούσαν να λύσουν προβλήματα, στα οποία συναρτούσαν τις πλευρές με τα εμβαδά ορθογωνίων. Το 1500 π.χ. Αιγύπτιοι μηχανικοί, παρότι δεν γνώριζαν μαθηματικά και εξισώσεις όπως στις μέρες μας, βρήκαν έναν τρόπο να υπολογίσουν μεγέθη. Πιο συγκεκριμένα, αντί να επινοήσουν έναν τύπο για τον υπολογισμό των πλευρών και των εμβαδών, έφτιαξαν έναν πίνακα ο οποίος περιείχε δείγματα εμβαδών από όλα τα πιθανά μεγέθη πλευρών ορθογωνίων και τετραγώνων, έτσι ώστε όταν οι μηχανικοί τις εποχής ήθελαν να φτιάξουν ένα σχέδιο με συγκεκριμένα μέτρα, συμβουλεύονταν τον πίνακα και εύρισκαν τα πιο ταιριαστά σχέδια.

Οι πρώτες προσπάθειες για την εύρεση μίας γενικότερης φόρμουλας για τον υπολογισμό των λύσεων των τετραγωνικών εξισώσεων ανέρχονται στην εποχή του Πυθαγόρα 500 π.χ. και του Ευκλείδη 300 π.χ. οι οποίοι χρησιμοποίησαν μία αυστηρή γεωμετρική προσέγγιση για να βρουν μια γενική διαδικασία για την επίλυση της εξίσωσης. Ο Πυθαγόρας παρατήρησε ότι οι αναλογίες ανάμεσα στο εμβαδόν ενός τετραγώνου και το αντίστοιχο μήκος της πλευράς του - η τετραγωνική ρίζα - δεν ήταν πάντα ακέραιος, αλλά αρνήθηκε να επιτρέψει αναλογίες πλην ρητών αριθμών. Ο Ευκλείδης προχώρησε ακόμη περισσότερο και διαπίστωσε ότι η αναλογία αυτή θα μπορούσε, επίσης, να μην είναι ρητός αριθμός. Κατέληξε στο συμπέρασμα ότι υπάρχουν άρρητοι αριθμοί.

Περίπου το 700 μ.χ. η γενική λύση για την εξίσωση δευτέρου βαθμού , αυτή τη φορά με τη χρήση αριθμών , επινοήθηκε από ένα ινδουιστή μαθηματικό, τον

Βραχμαγκούπτα. Ο Βραχμαγκούπτα ήταν ο πρώτος που επινόησε κανόνες για τον υπολογισμό με το μηδενικό ψηφίο. Έδωσε τη λύση της γενικής γραμμικής εξίσωσης στο κεφάλαιο δεκαοχτώ του Βραχμασφουτασιντάντα[3]. Σύμφωνα με το έργο του η εξίσωση $ax^2 + bx = \gamma$ έχει δύο λύσεις,

$$(\alpha)\ \chi = \frac{\sqrt{4\alpha\gamma+\beta^2}-\beta}{2\alpha}$$

$$(\beta)\ \chi = \frac{\sqrt{\alpha\gamma+\frac{\beta^2}{4}}-\frac{\beta}{2}}{\alpha}$$

Συνέχισε με την επίλυση ταυτόχρονων απροσδιόριστων εξισώσεων δηλώνοντας πως η επιθυμητή μεταβλητή πρέπει να απομονωθεί πρώτα, και κατόπιν η εξίσωση να διαιρεθεί με τον επιθυμητό συντελεστή της μεταβλητής. Συγκεκριμένα, πρότεινε να χρησιμοποιείται η μέθοδος της 'πολτοποίησης' για την λύση εξισώσεων με πολλαπλούς αγνώστους.

Η τελική, ολοκληρωμένη λύση όπως τη γνωρίζουμε σήμερα, ήρθε περίπου 1100 μ.χ., από έναν άλλο ινδουιστή μαθηματικό, τον Μπασκάρα (Baskhara). Ο Μπασκάρα ήταν ο πρώτος που αναγνώρισε ότι οποιοσδήποτε θετικός αριθμός έχει δύο τετραγωνικές ρίζες.

Η φόρμουλα του Μπασκάρα

Έστω η παρακάτω δευτέρου βαθμού εξίσωση

$$ax^2 + bx + c = 0$$

Με $\alpha \neq 0$ και πραγματικούς συντελεστές και δίνεται από τον παρακάτω τύπο:

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

Όπου Δ η διακρίνουσα : $\Delta = b^2-4ac$

Ανάλογα με το πρόσημο της Δ, έχουμε:

- $\Delta = 0$, τότε η εξίσωση έχει δύο ίσες ρίζες
- $\Delta > 0$, τότε η εξίσωση έχει δύο διαφορετικές ρίζες
- $\Delta < 0$, τότε η εξίσωση δεν έχει πραγματικές ρίζες.

Με την Αναγέννηση στην Ευρώπη, η ακαδημαϊκή προσοχή στράφηκε πίσω στα αρχικά μαθηματικά προβλήματα. Το 1.545 μ.χ. ο Τζιρόλαμο Καρντάνο, ο οποίος

[3] Μια θεωρητική μελέτη του 628 μ.χ. η οποία περιέχει τους πρώτους κανόνες για υπολογισμούς με το μηδέν

ήταν ένας τυπικός επιστήμονας της Αναγέννησης (δηλαδή, ενδιαφερόταν για την αλχημεία, τον αποκρυφισμό και άλλα παρόμοια), και ένας από τους καλύτερους αλγεβριστές της εποχής του, δημιούργησε έργα που σχετίζονται με τις τετραγωνικές εξισώσεις. Δεν ήταν ίσως η πρώτος ή μόνος που ασχολήθηκε, αλλά ήταν σίγουρα ο πιο διάσημος. Στα κείμενα του (κυρίως ρητορικά) επιτρέπει την ύπαρξη σύνθετων, ή φανταστικών αριθμών - δηλαδή, οι ρίζες των αρνητικών αριθμών. Στα τέλη του 16ου αιώνα η μαθηματική σημειογραφία και ο συμβολισμός εισήχθη από έναν ερασιτέχνη μαθηματικό τον François Viète, στη Γαλλία. Το 1637, όταν ο René Descartes δημοσίευσε το έργο La Géométrie, τα σύγχρονα μαθηματικά γεννήθηκαν, και η τετραγωνική εξίσωση πήρε τη μορφή που γνωρίζουμε σήμερα. (h2g2 2004)

1.2.2 Κυβική εξίσωση

Η εξισώσεις $3^{ου}$ βαθμού ήταν γνωστές από την αρχαιότητα, όπου οι αρχαίοι λαοί των Ελλήνων, των Βαβυλώνιων και των Αιγυπτίων αντιμετώπιζαν το πρόβλημα του διπλασιασμού του κύβου. Ο Διπλασιασμός του κύβου (επίσης γνωστός ως πρόβλημα της Δήλου - Δήλιον πρόβλημα) είναι ένα από τα τρία γνωστά προβλήματα της αρχαιότητας που δεν είναι δυνατόν να λυθούν μόνο με κανόνα και διαβήτη.

Το πρόβλημα συνίσταται στην κατασκευή ενός κύβου με διπλάσιο όγκο από ένα γνωστό κύβο πλευράς α. Ο απλός διπλασιασμός του μήκους της ακμής του κύβου οδηγεί σε οχταπλασιασμό του όγκου.

Αρκετοί αρχαίοι και νεώτεροι ασχολήθηκαν με το πρόβλημα όπως ο Αρχύτας ο Ταραντίνος, ο Εύδοξος ο Κνίδιος, ο Μέναιχμος, ο Νικομήδης, ο Απολλώνιος ο Περγαίος, ο Διοκλής, ο Ήρων ο Αλεξανδρεύς, ο Πάππος ο Αλεξανδρεύς, ο Καρτέσιος και άλλοι. Όλοι όμως έδιναν λύση που χρησιμοποιούσε και άλλες μεθόδους πλην της κλασσικής. Ο Ευτόκιος ο Ασκαλωνίτης δίνει στα έργα του πληροφορίες για 12 λύσεις του Δήλιου προβλήματος. Σήμερα σημαντικότερη θεωρείται η λύση του Αρχύτα καθώς κάνει χρήση τριών στερεών: κυλίνδρου, κώνου και σφαίρας. Πιο περίπλοκες μέθοδοι περιλαμβάνουν την Κισσοειδή του Διοκλή, την Κογχοειδή του Νικομήδη, ή τη γραμμή του Φίλωνα του Βυζαντινού. Ωστόσο, η ανυπαρξία μιας λύσης τελικά αποδεικνύεται από τον Pierre Wantzel το 1837, εφαρμόζοντας την πρόσφατη ανάπτυξη της αφηρημένης άλγεβρας από Galois (wiki)

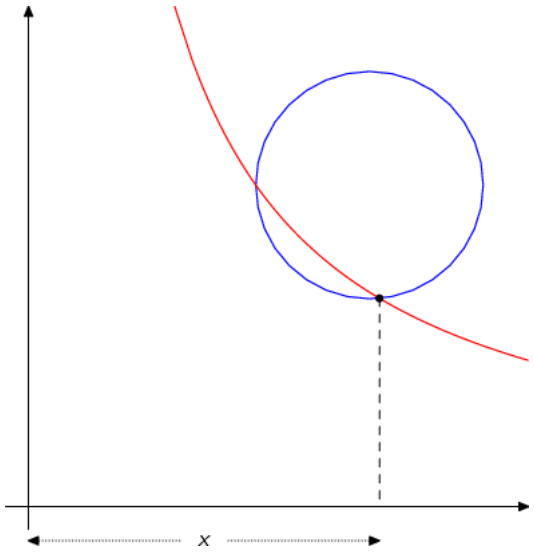
Βαβυλωνιακές σφηνοειδής επιγραφές έχουν βρεθεί μεταξύ του $20^{ου}$ και $16^{ου}$ αιώνα π.χ με πίνακες για τον υπολογισμό κύβων και κυβικών ριζών. Οι Βαβυλώνιοι μπορούσαν να χρησιμοποιήσουν τους πίνακες για να λύσουν τις κυβικές εξισώσεις, αλλά δεν υπάρχουν στοιχεία που να επιβεβαιώνουν ότι το έκαναν. Το πρόβλημα του διπλασιασμού του κύβου περιλαμβάνει την απλούστερη και πιο παλιά μελετημένη

κυβική εξίσωση, και αυτό για το οποίο οι αρχαίοι Αιγύπτιοι δεν πίστευαν ότι υπήρχε λύση.

Κατά τον 5ο αιώνα π.Χ., ο Ιπποκράτης μειώνει το πρόβλημα αυτό με εκείνο της εύρεσης δύο μέσων αναλογιών μεταξύ μίας γραμμής και μίας άλλης δύο φορές το μήκος της πρώτης, αλλά δεν μπορούσε να λύσει αυτό με κανόνα και διαβήτη, ένα έργο το οποίο είναι σήμερα γνωστό ότι είναι αδύνατο.

Τον 11ο αιώνα, ο διάσημος μαθηματικός Ομάρ Καγιάμ ανακάλυψε μια γεωμετρική μέθοδο για την επίλυση των κυβικών εξισώσεων που θα μπορούσε να χρησιμοποιηθεί για να πάρει αριθμητική απάντηση, τέμνοντας μια υπερβολή με έναν κύκλο, και χρησιμοποιώντας αυτή τη μέθοδο βρήκε ότι η κυβική εξίσωση μπορεί να έχει περισσότερες από μία λύσεις.

Σε ένα ατιτλοφόρητο κείμενο του Καγιάμ για τις κυβικές εξισώσεις, που ανακαλύφθηκε τον 20ό αιώνα, όπου εμφανίζεται το παραπάνω απόσπασμα, ο Καγιάμ ασχολείται με προβλήματα γεωμετρικής άλγεβρας. Πρώτο είναι το πρόβλημα της "εύρεσης ενός σημείου στο τεταρτημόριο ενός κύκλου, τέτοιου ώστε όταν άγεται μία κάθετος από το σημείο αυτό προς μία από τις ακτίνες που το ορίζουν ο λόγος του μήκους της καθέτου προς την ακτίνα να ισούται προς το λόγο των τμημάτων που ορίζονται από τον πόδα της καθέτου". Πάλι στην επίλυση αυτού του προβλήματος το μετατρέπει σε ένα άλλο γεωμετρικό πρόβλημα : "εύρεση ενός ορθογώνιο τρίγωνου με την ιδιότητα η υποτείνουσα του να ισούται με το άθροισμα της μιας κάθετης πλευράς του συν το ύψος επί την υποτείνουσα". Για να επιλύσει αυτό το γεωμετρικό πρόβλημα εισάγει μια παράμετρο και καταλήγει στην κυβική εξίσωση x^3 + 200x = $20\chi^2$ + 2000. Πράγματι βρίσκει μια θετική ρίζα για αυτή την εξίσωση τέμνοντας μια υπερβολή με ένα κύκλο.



x^3 + 200x = 20x^2 + 2000.

Δεν μπόρεσε να βρει έναν αλγεβρικό τρόπο για την γενικότερη επίλυση της κυβικής εξισώσεως όμως μπόρεσε να την λύσει γεωμετρικά. Επιπλέον προσκάλεσε και άλλους μαθηματικούς, προκειμένου να βρούνε μία φόρμουλα για την επίλυση των κυβικών εξισώσεων.

Το 12^{ο} αιώνα ένας άλλος πέρσης μαθηματικός, ο Sharaf al-Dīn al-Tūsī, έγραψε ένα έργο περί εξισώσεων όπου ασχολήθηκε με οκτώ τύπους κυβικών εξισώσεων με θετικές λύσεις και πέντε τύπους κυβικών εξισώσεων οι οποίες δεν μπορούν να έχουν θετικές λύσεις. Χρησιμοποιούσε μια μέθοδο η οποία αργότερα θα γίνονταν γνωστή ως "μέθοδος Ruffini-Horner" για να προσεγγίζει αριθμητικά τη ρίζα μιας κυβικής εξίσωσης. Ανέπτυξε επίσης τις έννοιες της παραγώγου συνάρτησης και τα μέγιστα και ελάχιστα των καμπυλών προκειμένου να λύσει κυβικές εξισώσεις οι οποίες δεν είχαν θετικές λύσεις. Κατάλαβε τη σημασία της διακρίνουσας στην κυβική εξίσωση προκειμένου να βρει αλγεβρικές λύσεις σε συγκεκριμένους τύπους κυβικών εξισώσεων.

Στις αρχές του 16ου αιώνα, ο Ιταλός μαθηματικός Scipione del Ferro (1465-1526) βρήκε μια μέθοδο για την επίλυση μίας κατηγορίας των κυβικών εξισώσεων, δηλαδή αυτά της μορφής x^3 + mx = n. Στην πραγματικότητα, όλες οι κυβικές εξισώσεις μπορούν να επαχθούν σε αυτή τη μορφή, αν επιτρέψουμε m και n να είναι αρνητικοί, αλλά οι αρνητικοί αριθμοί δεν ήταν γνωστοί σ 'αυτόν εκείνη την εποχή. Ο Del Ferro κράτησε τα επίτευγμα του μυστικά μέχρι λίγο πριν το θάνατό του, όταν τα αποκάλυψε στο μαθητή του Antonio Fiore.

Το 1535 ο Fiore συμμετείχε σε ένα διαγωνισμό με ένα μαθηματικό που ονομαζόταν Tartaglia, του οποίου το πραγματικό όνομα ήταν Nicalo Fontana. Κάθε διαγωνιζόμενος έπρεπε να θέσει ένα συγκεκριμένο ποσό χρημάτων και να προτείνει μια σειρά από προβλήματα για τον αντίπαλό του για να λύσει. Όποιος έλυνε τα

περισσότερα, μέσα σε 30 μέρες, θα ήταν και ο νικητής. Ο Tartaglia έλαβε εξισώσεις με τη μορφή $x^3 + mx = n$, για τις οποίες είχε εργαστεί σε μια γενική μέθοδο. Ο Fiore δέχτηκε εξισώσεις με τη μορφή $x^3 + mx^2 = n$, οι οποίες αποδείχθηκε ότι είναι πάρα πολύ δύσκολες γι 'αυτόν να λύσει, και ο Tartaglia κέρδισε το διαγωνισμό.

Η λύση του Tartaglia στην τριτοβάθμια εξίσωση (όπως απεικονίζεται στο Ars Magna):

Η γενική κυβική εξίσωση:

$$y^3 + Ay^2 + By + C = 0 \qquad (1)$$

Μπορεί να πάρει τη μορφή:

$$x^3 + cx = d \qquad (2)$$

Αντικαθιστώντας όπου y = $\chi - \frac{A}{3}$, οποιαδήποτε κυβική εξίσωση γίνεται της μορφής $x^3 + cx = d$.

Η εξίσωση (2) λύνεται ακολουθώντας τα παρακάτω βήματα:

1.Βρίσκουμε τα u και v, έτσι ώστε

$$(\alpha)\ u - v = d$$

$$(\beta)\ u \cdot v = \frac{c^3}{3}$$

2. Η λύση των εξισώσεων (α) και (β) για υ και ν δίνονται από:

$$(\alpha)\ u = \sqrt{(\frac{d}{2})^2 + (\frac{c}{3})^3} + \frac{d}{2}$$

$$(\beta)\ v = \sqrt{(\frac{d}{2})^2 + (\frac{c}{3})^3} - \frac{d}{2}$$

3. Η ρίζα στην εξίσωση (2) δίνεται από:

$$X = \sqrt[3]{u} - \sqrt[3]{v}$$

1.2.3 $4^{ου}$ βαθμού εξίσωση

Το 1545 ο Cardano δημοσίευσε το βιβλίο με τίτλο "Ars Magna[4]" το οποίο μπορεί να θεωρηθεί ως η αρχή της Άλγεβρας. Πέντε χρόνια πριν από αυτόν, ο Lodovico Ferrari ανακάλυψε τη φόρμουλα για να λύσει τις τεταρτοβάθμιες εξισώσεις, και περίπου την ίδια περίοδο ο Rene Descartes ανακάλυψε παρόμοια φόρμουλα για την επίλυση εξισώσεων $4^{ου}$ βαθμού.

Λύση του Ferrari στην τεταρτοβάθμια εξίσωση:

Η γενική μορφή της τεταρτοβάθμιας εξίσωσης,

$$y^4 + Ay^3 + By^2 + Cy + D = 0$$

μπορεί να επαχθεί σε πιο απλή μορφή

$$x^4 + ax^2 + bx + c = 0 \qquad (1)$$

αντικαθιστώντας όπου $y = x - \frac{A}{4}$. Επομένως, για την επίλυση οποιασδήποτε μορφής τεταρτοβάθμιας εξίσωσης, μπορούμε να λύσουμε την εξίσωση (1), (χωρίς τον κυβικό όρο).

Για την επίλυση της (1) πρώτα τη φέρνουμε στην ακόλουθη μορφή

$$x^4 + ax^2 = -bx - c$$

προσθέτουμε $ax^2 + a^2$ και στις δύο μεριές προκειμένου να δημιουργήσουμε ένα τέλειο τετράγωνο

$$x^4 + 2ax^2 + a^2 = -bx - c + ax^2 + a^2$$

οπότε έχουμε $(\chi^2 + a)^2 = -bx - c + ax^2 + a^2 \qquad (2).$

Φέρνουμε τη (2) στη μορφή

$$(\chi^2 + a + \zeta)^2 = (-bx - c + ax^2 + a^2) + 2x^2\zeta + 2\alpha\zeta + \zeta.$$

Αφού $(\chi^2 + a + \zeta)^2 = x^4 + 2\alpha x^2 + \alpha^4 + 2x^2\zeta + 2\alpha\zeta + \zeta$

Ομαδοποιούμε τους όρους στη δεξιά μεριά

$$(\chi^2 + a + \zeta)^2 = (2\zeta + \alpha)x^2 - bx + (\alpha^2 - c + 2\alpha\zeta + \zeta^2) \quad (3).$$

[4] Το Ars Magna (λατινικά: «Η Μεγάλη Τέχνη») είναι ένα σημαντικό βιβλίο για την άλγεβρα γραμμένο από τον Girolamo Cardano. Εκδόθηκε για πρώτη φορά το 1545

Στη συνέχεια επιλέγουμε ζ, τέτοιο ώστε η δεξιά μεριά της εξίσωσης (3) να είναι τέλειο τετράγωνο. Επομένως το δεξιό μέρος της (3) πρέπει να είναι της μορφής

$$((\sqrt{2\zeta+\alpha}\,)\chi \pm \sqrt{\alpha^2-c+2\alpha\zeta+\zeta^2}\,)^2 \quad (*)$$

εάν τετραγωνίσουμε το (*) τότε έχουμε

$$(a+2\zeta)\chi^2 \pm (2\sqrt{2\zeta+\alpha}\,\sqrt{\alpha^2-c+2\alpha\zeta+\zeta^2})\chi + (\alpha^2 - c + 2\alpha\zeta+\zeta^2\,)\ (**)$$

Εξισώνοντας την (3) με το (**) έχουμε

$$-b = \pm 2\sqrt{2\zeta+\alpha}\,\sqrt{\alpha^2-c+2\alpha\zeta+\zeta^2} \quad (4)$$

Τετραγωνίζουμε και τις δύο μεριές και έχουμε

$$b^2 = 4(2\zeta+\alpha)(\alpha^2-c+2\alpha\zeta+\zeta^2) \text{ ή}$$

$$4(2\zeta+\alpha)(\alpha^2-c+2\alpha\zeta+\zeta^2)\ -b^2 = 0 \quad (5)$$

Η (5) μπορεί να πάρει την παρακάτω μορφή

$$\zeta^3 + \frac{5}{2}\alpha\zeta^2 + (2\alpha^2 - c)\zeta + (\frac{\alpha^3}{2} - \frac{ac}{2} - \frac{\beta c}{2}) = 0 \ (5)$$

Όπου η μεταβλητή ζ μπορεί να υπολογιστεί από τις ήδη γνωστές φόρμουλες για την κυβική εξίσωση.

Όταν το ζ είναι ρίζα της (5) τότε το δεξιό μέρος της εξίσωσης (3) είναι ένα τέλειο τετράγωνο. Χρησιμοποιώντας μεθόδους από το Ars Magna για την επίλυση κυβικών εξισώσεων η (3) μπορεί να γραφτεί

$$(\chi^2+a+\zeta)^2 = (\sqrt{2\zeta+\alpha}\,)\chi \pm \sqrt{\alpha^2-c+2\alpha\zeta+\zeta^2})^2 \quad (6)$$

Παίρνοντας την τετραγωνική ρίζα της (6) έχουμε

$$\chi^2+\alpha+\zeta = \pm((\sqrt{2\zeta+\alpha}\,)\chi \pm \sqrt{\alpha^2-c+2\alpha\zeta+\zeta^2})) \quad (7)$$

Όπου στο τέλος χρησιμοποιούμε τη φόρμουλα για την τετραγωνική εξίσωση και βρίσκουμε τις λύσεις της εξίσωσης.

Η μέθοδος του Ferrari στη σύγχρονη σημειογραφία

Η γενική μορφή της τεταρτοβάθμιας εξίσωσης είναι (Hana Almoner Looka 2014)

$$\alpha x^4 + \beta x^3 + \gamma x^2 + \delta x + c = 0, \text{ όπου } \alpha \neq 0, \qquad (1)$$

- Αν α≠1, τότε διαιρούμε το β,γ,δ,c με το α και απλοποιούμε την εξίσωση (1). Η εξίσωση που προκείπτει είναι

$$x^4 + \frac{\beta}{\alpha}x^3 + \frac{\gamma}{\alpha}x^2 + \frac{\delta}{\alpha}x + \frac{c}{\alpha} = 0 \qquad (2)$$

- Τώρα ορίζουμε τις παρακάτω μεταβλητές προκειμένου να λύσουμε την εξίσωση (2)

  f= γ- $(\frac{3}{8}\beta^2)$

  g= δ+ $(\frac{1}{8}\beta^3)$- $(\frac{1}{2}\beta\gamma)$

  h= γ- $(\frac{3}{256}\beta^4)$ + $(\frac{1}{16}\beta^2\gamma)$- $(\frac{1}{4}\beta\gamma)$

- Βάζουμε τους αριθμούς f, g και h στην ακόλουθη κυβική εξίσωση

$$x^3 + (\frac{1}{2}f)x^2 + (\frac{f^2-4h}{16})x - (\frac{1}{64})g^2 = 0 \qquad (3)$$

- Εκτιμούμε τους α, β, γ και δ συντελεστές για την επίλυση εξίσωσης (3)

  $\beta = \frac{1}{2}f$

  $\gamma = \frac{f^2-4h}{16}$

  $\delta = \frac{-g^2}{64}$

- Μέτα βρίσκουμε τις ρίζες στην παρακάτω κυβική εξίσωση

$$x^3 + \beta x^2 + \gamma x + \delta = 0 \qquad (4)$$

- Για να πάρουμε τρεις ρίζες της εξίσωσης (4) μπορούμε να χρησιμοποιήσουμε τη μέθοδο του Tartaglia
  - Έστω p και q είναι οι τετραγωνικές ρίζες των δύο οποιωνδήποτε μη μηδενικών ριζών (χ_1,χ_2 και χ_3)
  - Έστω r= $\frac{-g}{pq}$ και s= $\frac{\beta}{4q}$
- Τώρα έχουμε ότι χρειαζόμαστε προκειμένου να λύσουμε την τεταρτοβάθμια εξίσωση και να βρούμε τις 4 λύσεις

  χ_1= p + q + r - s

  χ_2= p - q - r - s

$\chi_3 = -p + q - r - s$

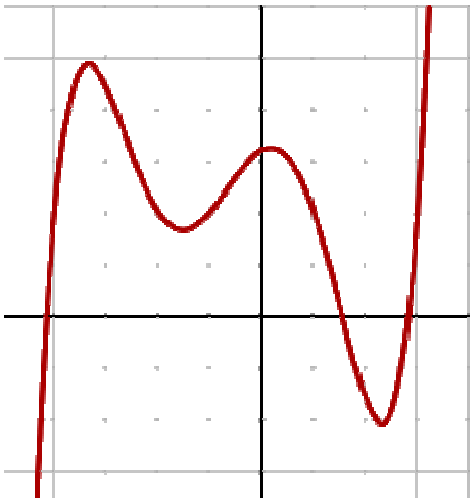
$\chi_4 = -p - q + r - s$

1.2.4 $5^{ου}$ βαθμού εξίσωση

Στα μαθηματικά, η συνάρτηση $5^{ου}$ βαθμού είναι μια συνάρτηση της μορφής

$g(x)=ax^5+bx^4+cx^3+dx^2+ex+f$

όπου a, b, c, d, e και f είναι μέλη ενός πεδίου, των ρητών, των πραγματικών και των μιγαδικών αριθμών, και το a είναι μη μηδενικός. Με άλλα λόγια, συνάρτηση $5^{ου}$ βαθμού ορίζεται από ένα πολυώνυμο $5^{ου}$ βαθμού .



Γραφική παράσταση ενός πολυωνύμου $5^{ου}$ βαθμού

Θέτοντας $g(x) = 0$ και υποθέτοντας ότι $\alpha \neq 0$ δημιουργούμε μια εξίσωση $5^{ου}$ βαθμού της μορφής:

$ax^5+bx^4+cx^3+dx^2+ex+f=0.$

Στις προηγούμενες ενότητες, είδαμε πως μπορούμε να λύσουμε τριτοβάθμιες και τεταρτοβάθμιες εξισώσεις χρησιμοποιώντας μόνο τις τέσσερις βασικές πράξεις (+, -, ×, ÷) και να βρίσκουμε τις ρίζες. Εξισώσεις που μπορούν να επιλυθούν με τη χρήση των λειτουργιών αυτών είναι επιλύσιμες με τις ρίζες.

Η επίλυση εξισώσεων $5^{ου}$ βαθμού ήταν ένα σημαντικό πρόβλημα στην άλγεβρα, από τον 16 αιώνα, όταν λύθηκαν κυβικές και τεταρτοβάθμιες εξισώσεις, μέχρι το πρώτο

μισό του 19ου αιώνα, όταν η αδυναμία μιας τέτοιας γενικής λύσης αποδείχθηκε (Abel-Ruffini θεώρημα[5]).

Υπάρχει μία διαφορά ανάμεσα στην εκτίμηση και τον υπολογισμό των ριζών. Μέθοδοι για τον υπολογισμό ριζών πολυωνύμου βαθμού 2, με συνθήκες τετραγώνου είναι γνωστές από την αρχαιότητα, και για πολυώνυμα βαθμού 3 η 4 παρόμοιες μέθοδοι (που χρησιμοποιούν κυβικές ρίζες όμως) έχουν βρεθεί τον 16ο αιώνα[6]. Αλλά μέθοδοι για 5ου βαθμού πολυώνυμα δεν έχουν βρεθεί ακόμη. Το 1824,ο Niels Henrik Abel απέδειξε το πολύ σημαντικό αποτέλεσμα ότι δεν μπορεί να υπάρξει γενικά μέθοδος, που να περιλαμβάνει μόνο αριθμητικές πράξεις, που να υπολογίζει τις ρίζες ενός πολυωνύμου βαθμού 5 η μεγαλύτερου βαθμού.

Σε αντίθεση με τις εξισώσεις βαθμού μικρότερου από πέντε, η $5^{ου}$ βαθμού εξίσωση δεν μπορεί να επιλυθεί με ρίζες. Το γεγονός αυτό δεν ήταν σαφές και δεν ήταν γνωστό μέχρι τις αρχές του 19ου αιώνα , όπου ο Νορβηγός μαθηματικός Niles Henrik Abel εισήγαγε ένα από τα πιο βαθιά θεωρήματα, όπου αναφέρει ότι δεν υπάρχει γενική αλγεβρική λύση των εξισώσεων βαθμού ≥ 5 σε ρίζες.

Το θεώρημα δεν ισχυρίζεται ότι ορισμένες πολυωνυμικές εξισώσεις υψηλότερου βαθμού δεν έχουν καμία λύση. Στην πραγματικότητα, το αντίθετο είναι αληθές: κάθε πολυώνυμο με μη σταθερή εξίσωση με ένα άγνωστο, με πραγματικούς ή μιγαδικούς συντελεστές, έχει τουλάχιστον έναν σύνθετο αριθμό ως λύση (και ως εκ τούτου, με την πολυωνυμική διαίρεση, έχει πολλές σύνθετες ρίζες όσες και ο βαθμός του, απαριθμώντας επαλαμβανόμενες ρίζες). Αυτό είναι το θεμελιώδες θεώρημα της άλγεβρας. Αυτές οι λύσεις μπορούν να υπολογιστούν με οποιοδήποτε επιθυμητό βαθμό ακριβείας με τη χρήση αριθμητικών μεθόδων όπως η μέθοδος Newton-Raphson ή μέθοδος Laguerre, και με αυτό τον τρόπο δεν είναι διαφορετικές από τις λύσεις για πολυωνυμικές εξισώσεις του δεύτερου, τρίτου και τέταρτου βαθμού. Το θεώρημα δείχνει μόνο ότι οι λύσεις μερικών από αυτών των εξισώσεων δεν μπορεί να εκφραστούν μέσω μιας γενικής έκφρασης σε ρίζες.

Επίσης, το θεώρημα δεν υποστηρίζει ότι ορισμένες πολυωνυμικές εξισώσεις υψηλότερου βαθμού έχουν λύσεις που δεν μπορούν να εκφράζονται σε όρους ριζών. Ενώ αυτό είναι πλέον γνωστό για να είναι αληθινό, είναι μια ισχυρότερη αξίωση, η οποία είχε μόλις αποδειχθεί λίγα χρόνια αργότερα από τον Galois. Το θεώρημα δείχνει μόνο ότι δεν υπάρχει γενική λύση από την άποψη των ριζών που δίνει τις ρίζες σε ένα γενικό πολυώνυμο με αυθαίρετους συντελεστές. Δεν απέκλεισε από μόνο του το ενδεχόμενο ότι κάθε πολυώνυμο μπορεί να λυθεί από την άποψη των ριζών για κάθε περίπτωση χωριστά.

Όταν ο Niles Henrik Abel άρχισε να εργάζεται στις εξισώσεις $5^{ου}$ βαθμού ήταν πολύ νέος, ηλικίας μόνο 19 (περίπου το 1821), αλλά αυτό το έργο ολοκληρώθηκε το 1824. Ωστόσο, δυστυχώς, πέθανε το 1829, όταν ήταν μόλις 26 ετών, εξαιτίας της

[5] Για μια πιο βαθειά προσέγγιση: Abel's impossibility theorem
[6] Αναφορά σε προηγούμενα υποκεφάλαια

φυματίωσης και του υποσιτισμού. Ωστόσο, μετά το θάνατό του το έργο του εκδόθηκε το 1830.

Ο Abel δεν ήταν ο μόνος μαθηματικός που ασχολήθηκε με τις εξισώσεις $5^{ου}$ βαθμού. Κατά την περίοδο αυτή, επίσης, ο Γάλλος μαθηματικός Everiste Galois, με την απαράμιλλη μεγαλοφυΐα του, ανακάλυψε μια μέθοδο για να προσδιοριστεί εάν η εξίσωση θα μπορούσε να λυθεί με ρίζες ή όχι, με τη χρήση εξελιγμένων τεχνικών οι οποίες οδήγησαν στην ίδρυση της θεωρίας των ομάδων και στη Θεωρία Galois[7].

Το 1830,ο Εβαρίστ Γκαλουά, μελέτησε την μεταλλαγή των ριζών ενός πολυωνύμου, επεκτείνοντας το θεώρημα Abel-Ruffini, δοθείσας μιας πολυωνυμικής εξίσωσης, κάποιος μπορεί να αποφασίσει αν είναι επιλύσιμο με πρωτογενή ανάλυση, και αν είναι, να το λύσει. Αυτό το αποτέλεσμα σημάδεψε την Θεωρία Galois και Θεωρία ομάδων, δύο σημαντικούς τομείς των σύγχρονων μαθηματικών. Ο Galois ο ίδιος παρατήρησε ότι οι υπολογισμοί με την μέθοδο του είναι ανέφικτοι. Παρόλα αυτά, μέθοδοι για επιλύσιμες εξισώσεις βαθμού 5 και 6 έχουν δημοσιευθεί.

[7] Περισσότερα για τη θεωρία του Galois στο κεφάλαιο 3

Κεφάλαιο 2

Θεωρία Ομάδων και Σωμάτων

2.1 θεωρία ομάδων

Η θεωρία ομάδων αποτελεί ένα βασικό κλάδο της άλγεβρας με σημαντικές εφαρμογές στην τοπολογία-γεωμετρία, μαθηματική φυσική αλλά και σε άλλους κλάδους εκτός των μαθηματικών. Έχει το πλεονέκτημα, έναντι άλλων κλάδων, να μην χρειάζεται κάποιο συγκεκριμένο υπόβαθρο. Στα μαθηματικά και την αφηρημένη άλγεβρα, η θεωρία ομάδων είναι το πεδίο που μελετά τις αλγεβρικές δομές γνωστές ως ομάδες. Η έννοια της ομάδας είναι θεμελιώδης στην αφηρημένη άλγεβρα: Άλλες γνωστές αλγεβρικές δομές, όπως **οι δακτύλιοι, τα σώματα, και οι διανυσματικοί χώροι,** μπορούν να αντιμετωπιστούν σαν ομάδες που έχουν εφοδιαστεί με επιπρόσθετες πράξεις και αξιώματα. Οι ομάδες συναντώνται επανειλημμένα σε όλο το φάσμα των μαθηματικών, και οι μέθοδοι της θεωρίας ομάδων έχουν επηρεάσει πολλούς τομείς της άλγεβρας. Οι Γραμμικές αλγεβρικές ομάδες και οι ομάδες Lie είναι δύο κλάδοι της θεωρίας ομάδων οι οποίοι έχουν εξελιχθεί αρκετά ώστε να αποτελούν ερευνητικά πεδία από μόνοι τους.

Η θεωρία ομάδων έχει τρεις κύριες ιστορικές καταβολές: τη θεωρία αριθμών, τη θεωρία αλγεβρικών εξισώσεων, και την γεωμετρία. Το αριθμο-θεωρητικό κομμάτι ξεκίνησε αρχικά από τον Λέοναρντ Όιλερ, και στη συνέχεια αναπτύχθηκε από τον Γκάους με την δουλειά του πάνω στους ισοϋπόλοιπους αριθμούς και στις προσθετικές και πολλαπλασιαστικές ομάδες που σχετίζονται με τα τετραγωνικά σώματα.

Τα πρώτα αποτελέσματα σχετικά με τις ομάδες μεταθέσεων βρέθηκαν από τους Λαγκράνζ, Ρουφίνι, και Άμπελ, στην προσπάθεια αναζήτησης γενικών λύσεων για τις πολυωνυμικές εξισώσεις μεγάλου βαθμού. Ο Évariste Galois όμως ήταν εκείνος που επινόησε τον όρο "ομάδα" και καθιέρωσε μία σύνδεση ανάμεσα στην τότε εκκολαπτόμενη θεωρία ομάδων και την θεωρία σωμάτων, αυτό που σήμερα ονομάζουμε Θεωρία Γκαλουά.

Ο Εβαρίστ Γκαλουά, τη δεκαετία του 1830, ήταν ο πρώτος που χρησιμοποίησε ομάδες για να προσδιορίσει την επιλυσημότητα των πολυουρικών εξισώσεων. Οι Άρθουρ Κέλεϋ και Ωγκυστέν-Λουί Κωσύ πήγαν την έρευνα ένα βήμα παραπέρα με τη δημιουργία της θεωρίας των ομάδων μεταθέσεων.

2.1.1 Ορισμός ομάδας

Στα μαθηματικά, η ομάδα ορίζεται ως εξής:

Ένα ζεύγος (G,*) με ένα σύνολο G και μια δυαδική πράξη *: G× G: G(a,b): a×b

ονομάζεται ομάδα, όταν ισχύουν οι εξής ιδιότητες:

- Προσεταιριστική: Για κάθε στοιχείο της ομάδας a, b και c ισχύει: (a*b)*c=a*(b*c)
- Ουδέτερο στοιχείο: Υπάρχει ουδέτερο στοιχείο $e \in G$, για το οποίο για κάθε στοιχείο a της ομάδας ισχύει: a*e=e*a=a.
- Αντίστροφο στοιχείο: Για κάθε στοιχείο a της ομάδας υπάρχει ένα στοιχείο $a^{-1} \in G$ έτσι ώστε να ισχύει $a*a^{-1}=a^{-1}*a=e$
- Μια ομάδα (G, *) καλείται αβελιανή ή μεταθετική αν :

  Η πράξη * είναι μεταθετική, δηλαδή ισχύει : □ α, b □ G : $x * y = y * x$

Η **τάξη** μιας ομάδας (G, *) ορίζεται να είναι το πλήθος |G| των στοιχείων του συνόλου G και από τώρα και στο εξής θα συμβολίζεται με o(G) := |G|. Η ομάδα (G, *) καλείται πεπερασμένη, αν $o(G) < \infty$. Διαφορετικά η (G, *) καλείται άπειρη ομάδα.

Οι ομάδες μπορούν να διαχωριστούν στις παρακάτω κατηγορίες:

- Ομάδες Μεταθέσεων
- Ομάδες Πινάκων
- Ομάδες Μετασχηματισμών
- Αφηρημένες ομάδες
- Τοπολογικές και αλγεβρικές ομάδες

Μία **υποομάδα S** μίας ομάδας G είναι ένα αυτοτελές υποσύνολο, που έχει τους ίδιους περιορισμούς με την ομάδα G. Ο συμβολισμός που χρησιμοποιούμε είναι S<G. (Roman S 1995)

Μία ομάδα G είναι **πεπερασμένη** εφόσον τα στοιχεία που περιέχει είναι πεπερασμένος αριθμός.

Σε αρκετές περιπτώσεις η δομή μίας ομάδας μεταθέσεων, μπορεί να μελετηθεί χρησιμοποιώντας τις ιδιότητες της δράσης της στο αντίστοιχο σύνολο. Για παράδειγμα με αυτόν τον τρόπο μπορεί κάποιος να δείξει ότι για $n \geq 5$ η εναλλάσσουσα ομάδα A_n είναι απλή, δηλαδή δεν περιέχει καμία γνήσια κανονική υποομάδα. Το γεγονός αυτό παίζει σημαντικότατο ρόλο στην απόδειξη της αδυναμίας επίλυσης με ριζικά των γενικών αλγεβρικών εξισώσεων με βαθμό $n \geq 5$

Έστω G μια πεπερασμένη ομάδα, και H μια υποομάδα της G. Είναι γνωστό ότι η ίδια η υποομάδα H είναι μια κλάση[8] της H. Για να βρούμε μια άλλη κλάση πρέπει να βρούμε ένα στοιχείο της G που δεν ανήκει στην κλάση H. Αν α_1 είναι ένα τέτοιο στοιχείο, τότε μπορούμε να σχηματίσουμε την κλάση α_1H. Αν α_2 είναι ένα στοιχείο της G που δεν ανήκει στις κλάσεις H και α_1H, τότε θα έχουμε μια νέα κλάση α_2H. Συνεχίζοντας με τον ίδιο τρόπο, κάποτε θα εξαντλήσουμε τα στοιχεία της G, εφόσον είναι μια πεπερασμένη ομάδα. Επειδή η ένωση όλων των κλάσεων μας δίνει το σύνολο G, το πλήθος των στοιχείων της ομάδας G γίνεται, τελικά πολλαπλάσιο του πλήθους των στοιχείων της H.

2.1.2 Θεώρημα Lagrange

Αν G είναι μια πεπερασμένη ομάδα, και H μια υποομάδα της G, τότε η τάξη

της H διαιρεί την τάξη της ομάδας G. Συγκεκριμένα ισχύει: [G:1]=[G:H][H:1].

Το Θεώρημα Lagrange είναι μια σημαντική βοήθεια, εφόσον συμπεράσματα από τη διαιρετότητα ακεραίων μπορούν να μας οδηγήσουν σε συμπεράσματα που αφορούν τις υποομάδες μιας ομάδας.

Παράδειγμα

Ας υποθέσουμε ότι θέλουμε να βρούμε όλες τις υποομάδες της προσθετικής ομάδας Z_{10} των ακεραίων mod10. Καταρχήν δύο υποομάδες είναι η τετριμμένη και η ίδια η ομάδα Z_{10}. Αν τώρα H είναι μια άλλη υποομάδα, τότε από το Θεώρημα Lagrange θα πρέπει να ισχύει

$$[Z_{10}:1]=[Z_{10}:H][H:1],$$

οπότε η τάξη της H πρέπει να είναι 2 ή 5. Επειδή κάθε υποομάδα της Z_{10} είναι κυκλική, θα πρέπει να βρούμε στοιχεία της Z_{10}, τα οποία έχουν τάξη 2 και 5 αντίστοιχα. Εύκολα διαπιστώνεται ότι ισχύουν

$$2\times\bar{2}=\bar{4}\neq\bar{0},3\times\bar{2}=\bar{6}\neq\bar{0},4\times\bar{2}=\bar{8}\neq\bar{0},5\times\bar{2}=\overline{10}=\bar{0},$$

και

$$2\times\bar{5}=\overline{10}=\bar{0}.$$

Αυτό σημαίνει ότι ord($\bar{2}$)=5 και ord($\bar{5}$)=2. Επομένως όλες οι υποομάδες της Z_{10} είναι οι

$$Z_{10},<\bar{0}>,<\bar{2}>,<\bar{5}>.$$

[8] Το πλήθος στοιχείων μίας πεπερασμένης ομάδας ονομάζεται κλάση της ομάδας και συμβολίζεται με IGI ή o(G)

Έστω G μια πεπερασμένη ομάδα, και a ένα στοιχείο της G. Είναι γνωστό ότι η τάξη του στοιχείου a είναι ίση με την τάξη της κυκλικής ομάδας που παράγεται από το στοιχείο αυτό, δηλαδή ισχύει

$$ord(a)=[<a>:1].$$

Επομένως από το Θεώρημα Lagrange προκύπτει ότι η τάξη του στοιχείου a πρέπει να

διαιρεί την τάξη της ομάδας G.

Παράδειγμα

Θεωρούμε την προσθετική ομάδα Z_{10} των ακεραίων mod10, και το στοιχείο $\bar{8}$ της ομάδας αυτής. Η τάξη του στοιχείου $\bar{8}$, πρέπει να διαιρεί την τάξη της ομάδας, άρα πρέπει να είναι 1 ή 2 ή 5 ή 10. Προφανώς δεν μπορεί να είναι 1, εφόσον$\bar{8}\neq\bar{0}$. Επίσης, από τη σχέση $2\times\bar{8}=\overline{16}=\bar{6}\neq\bar{0}$, προκύπτει ότι η τάξη του στοιχείου αυτού δεν είναι 2. Άρα η τάξη του $\bar{8}$, θα είναι 5 ή 10. Δηλαδή δεν χρειάζεται να εξετάσουμε αν ισχύει $3\times\bar{8}=\bar{0}$, διότι το Θεώρημα Lagrange δείχνει ότι δεν ισχύει. Είναι εύκολο να διαπιστώσει κανείς ότι η τάξη του $\bar{8}$ θα είναι 5.

Το παραπάνω παράδειγμα δείχνει ότι η παρουσία του Θεωρήματος Lagrange μπορεί να μειώσει τις πράξεις που απαιτούνται για τον υπολογισμό της τάξης ενός στοιχείου.

Ο Lagrange το 1971 με την εργασία του reflections on the algebraic solution of equations συνείσφερε σημαντικά στην επίλυση εξισώσεων με ριζικά. Στα δυο πρώτα μέρη της εργασίας ασχολείται με την ανάλυση των μέχρι τότε μεθόδων για την επίλυση των εξισώσεων $3^{ου}$ και $4^{ου}$ βαθμού και αποδεικνύει ότι καμία από αυτές δεν είναι κατάλληλη για την επίλυση εξισώσεων $5^{ου}$ βαθμού. Στο $3^{ο}$ μέρος αναλύει κάποιες περιπτώσεις εξισώσεων υψηλού βαθμού που μπορούν να λυθούν και ,τέλος, στο 4ο μέρος κάνει κάποιες γενικές παρατηρήσεις σχετικά με τη μετατροπή των εξισώσεων και τη μείωσή τους σε χαμηλότερο βαθμό.

2.2 R´eflexions sur la R´esolution Alg´ebrique des Equations

Έστω η παρακάτω εξίσωση 4ου βαθμου

$$\chi^4 + m\chi^3 + n\chi^2 + p\chi + q=0$$

Κάποιος μπορεί, επομένως, να συμπεράνει από αυτή την παρατήρηση έναν άμεσο τρόπο για να φτάσει στη μειωμένη εξίσωση [reduite] του τέταρτου βαθμού και από τη χρήση της σε μια γενική λύση για αυτό το βαθμό. Αφού ο συνδυασμός ab + cd των τεσσάρων ριζών a, b, c, d της εξίσωσης είναι τέτοιος ώστε μόνο τρείς παραλλαγές να είναι αποδεκτές

$$ad + cd \quad ac + bd \quad ad + cd$$

προκύπτει ότι αν θέσουμε

$$ab + cd = u$$

θα πάρουμε μια εξίσωση U του τρίτου βαθμού, η οποία θα έχει ρίζες

$$ab + cd\ ac + bd\ ad + bc$$

και θα είναι της μορφής

$$u^3 - Au^2 + B\,u - C = 0$$

Όπου θα έχει

$$A = ab + cd + ac + bd + ad + cb$$

$$B = (ab + cd)(ac + bd)+(ab + cd)(ad + cb)+(ac + bd)(ad + cb)$$

$$C = (ab + cd)(ac + bd)(ad + cb)$$

ή καλύτερα

$$A = ab + ac + ad + bc + bd + cd$$

$$B = \alpha^2(bc + bd + cd) + b^2\,(ac + ad + cd) + c^2\,(ab + ad + bd) + d^2\,(ab + ac + bc)$$

$$C = abcd(\alpha^2 + b^2 + c^2 + d^2) + a^2b^2c^2 + a^2b^2d^2 + a^2c^2d^2 + b^2c^2d^2$$

Οποιαδήποτε μετάθεση και να κάνει κανείς ανάμεσα στις ρίζες a, b, c, και d οι τιμές των A, B και C παραμένουν σταθερές.

Έτσι έχοντας

$$-m = a + b + c + d$$

$$n = ab + ac + ad + bc + bd + cd$$

$$-p = abc + abd + acd + bcd$$

$$q = abcd$$

βρίσκουμε ότι

$$A = n.$$

Για να βρούμε το B παρατηρούμε

$$a(bc + bd + cd) = -p - bcd$$

και με τον ίδιο τρόπο

$$b(ac + ad + cd) = -p - acd$$

οπότε

$$B = (a + b + c + d)(-p) - 4abcd$$

Άρα

$$B = mp - 4q$$

Τέλος για να βρούμε το C παρατηρούμε οτι

$$\alpha^2 + b^2 + c^2 + d^2 = m^2 - 2n$$

Έτσι ώστε το μέρος της εξίσωσης με τον όρο $abcd(\alpha^2 + b^2 + c^2 + d^2)$ να γίνει $(m^2 - 2n)q$. Για να υπολογίσουμε το άλλο μέρος , βρίσκουμε το τετράγωνο του p όπου επάγεται ότι

$$a^2b^2c^2 + a^2b^2d^2 + a^2c^2d^2 + b^2c^2d^2 =$$

$$p^2 - 2abcd\,(\,ab + ac + bc + ad + bd + cd\,) =$$

$$p^2 - 2nq,$$

Οπότε

$$C = (m^2 - 4n)q + p^2$$

Έτσι η μειωμένη εξίσωση γίνεται

$$u^3 - nu^2 + (mp - 4q)u - (m^2 - 4n)q - p^2 = 0$$

Θα δούμε τώρα πώς, γνωρίζοντας μία από τις τιμές των u, μπορεί κανείς να βρει τις τέσσερεις ρίζες a, b, c, d. Αφού

$$u = ab + cd \text{ και } abcd = q$$

είναι σαφές ότι οι δύο ποσότητες ab και cd θα είναι οι ρίζες αυτής της δεύτερου βαθμού εξίσωσης:

$$t^2 - ut + q = 0$$

έτσι ώστε ονομάζοντας κανείς αυτές τις ρίζες t' και t''θα μάθει κανείς τα δύο γινόμενα

$$ab = t' \text{ and } cd = t''$$

επιπλέον έχοντας

$$-p = ab(c + d) + cd(a + b) = t'(c + d) + t''(a + b)$$

Και επειδή

$$a + b + c + d = -m$$

θα έχει

$$a + b = \frac{p-mt'}{t'-t''}\ ,\ c + d = \frac{p-mt''}{t''-t'}$$

έτσι ώστε αφού

$$ab = t' \text{ and } cd = t''$$

είναι σαφές ότι η a και b θα είναι οι ρίζες της εξίσωσης

$$x^2 - \frac{p-mt'}{t'-t''}x + t' = 0$$

και c και d θα είναι οι ρίζες της

$$x^2 - \frac{p-mt''}{t''-t'}x + t'' = 0$$

Έτσι παρατηρούμε ότι αρκεί να γνωρίζουμε μια από τις ρίζες της μειωμένης εξίσωσης U προκειμένου να υπολογίσουμε τις 4 ρίζες a,b,c και d της αρχικής εξίσωσης. Επίσης, παρατηρούμε ότι κάθε μία από τις ρίζες αυτής της μειωμένης εξίσωσης θα δίνει πάντα τις ίδιες τέσσερις ρίζες a, b, c, d. Διότι, αν στη θέση της, λαμβάνοντας υ = ab + cd είχε πάρει ένα u = ac + bd ή u = ad + bc, δεν θα υπάρξει καμία άλλη αλλαγή στους τύπους μας, εκτός ότι ο b θα πρέπει να αλλάξει σε c ή d και ανάποδα.

2.3 Θώρημα του Abel-Ruffini

Μετά την εύρεση του τύπου των ριζών τεταροβάθμιων πολυωνύμων η προσπάθεια επικεντρώθηκε σε αντίστοιχο τύπο για πολυώνυμα πέμπτου βαθμού. Ο πρώτος που ισχυρίστηκε ότι δεν υπάρχει τέτοιος τύπος ήταν ο Ruffini το 1799 σε μία εργασία που εισήγαγε για πρώτη φορά την έννοια των μεταθέσεων. Ο Lagrange είχε ορίσει τις μεταθέσεις σαν μεμονωμένα στοιχεία. Το 1824 ο Abel έδωσε μια ολοκληρωμένη απόδειξη της μη επιλυσιμότητας πολυωνύμου πέμπτου βαθμού χρησιμοποιώντας τις μεταθέσεις των ριζών του πολυωνύμου. Το θεώρημα δείχνει ότι δεν υπάρχει τύπος με

ριζικά που να λύνει τα πολυώνυμα με βαθμό ίσο ή μεγαλύτερο του πέμπτου. (Χαραλάμπους Χ 2008)

Το θεώρημα του Abel-Ruffini λέει ότι υπάρχουν κάποιες εξισώσεις πέμπτου βαθμού των οποίων η λύση δεν μπορεί να εκφραστεί. Η εξίσωση χ^5- χ + 1 = 0 είναι ένα παράδειγμα. Ορισμένες άλλες πέμπτου βαθμού εξισώσεις μπορούν να λυθούν με ρίζες, για παράδειγμα $\chi^5 - \chi^4 - \chi + 1 = 0$, το οποίο μπορούμε να το παραγοντοποιήσουμε (χ-1)(χ-1)(χ+1)(χ+i)(χ-i) = 0. Το ακριβές κριτήριο που διακρίνει τις εξισώσεις που μπορούν να λυθούν με ριζικά και αυτές που δεν μπορούν, δόθηκε από τον Εβαρίστ Γκαλουά και είναι τώρα μέρος της θεωρίας Galois: μια πολυωνυμική εξίσωση μπορεί να λυθεί με ριζικά, αν και μόνο αν η ομάδα του Galois είναι επιλύσιμη ομάδα .

Απόδειξη θεωρήματος Abel-Ruffini

Ένα από τα θεμελιώδη θεωρήματα της θεωρίας Galois αναφέρει ότι ένα πολυώνυμο f(x) ∈ F[x] είναι επιλύσιμο με ριζικά στο F αν και μόνο αν το διασπασμένο κομμάτι K στο F έχει μία επιλύσιμη ομάδα Galois, έτσι ώστε η απόδειξη στο θεώρημα του Abel-Ruffini καθορίζει τον υπολογισμό της ομάδας Galois του γενικού πολυώνυμου πέμπτου βαθμού.

Έστω y_1 ένας πραγματικός υπερβατικός αριθμός, σε ένα πεδίο ρητών αριθμών Q, και έστω y_2 ένας πραγματικός υπερβατικός αριθμός στο $Q(y_1)$, μέχρι το y_5 οπου y πραγματικός υπερβατικός αριθμός στο $Q(y_1, y_2, y_3, y_4)$. Αυτοί οι αριθμοί ονομάζονται ανεξάρτητα υπερβατικά στοιχεία στο Q.

Έστω $E= Q(y_1, y_2, y_3, y_4, y_5)$

και $f(x)= (x-y_1)(x-y_2)(x-y_3)(x-y_4)(x-y_5) \in E(\chi)$.

επεκτείνοντας την f(x) παίρνουμε τις συμμετρικές συναρτήσεις της y_n :

$$s_1 = y_1 + y_2 + y_3 + y_4 + y_5$$

$$s_2 = y_1y_2 + y_1y_3 + y_1y_4 + y_1y_5 + y_2y_3 + y_2y_4 + y_2y_5 + y_3y_4 + y_3y_5 + y_4y_5$$

$$s_3 = y_1y_2y_3 + y_1y_2y_4 + y_1y_2y_5 + y_1y_3y_4 + y_1y_3y_5 + y_1y_4y_5 + y_2y_3y_4 + y_2y_3y_5 + y_2y_4y_5 + y_3y_4y_5$$

$$s_4 = y_1y_2y_3y_4 + y_1y_2y_3y_5 + y_1y_2y_4y_5 + y_1y_3y_4y_5 + y_2y_3y_4y_5$$

$$s_5 = y_1y_2y_3y_4y_5.$$

Ο συντελεστής του χ^n στην f(x) κατά συνέπεια είναι $(-1)^{5-n}s_{5-n}$. Έστω $F=Q(s_i)$ είναι το πεδίο το οποίο προκύπτει συνεφάπτοντας τις συμμετρικές συναρτήσεις με τους ρητούς (οι s_i είναι υπερβατικοί γιατί οιy_i είναι ανεξάρτητοι).

Επειδή οι ανεξάρτητοι υπερβατικοί y_n δρουν ως άγνωστοι στο Q, οποιαδήποτε μετάθεση σε μία συμμετρική ομάδα 5 στοιχείων S_5 προκαλεί ένα ξεχωριστό ισόμορφο σ' στο E, όπου αφήνει σταθερό το Q και μεταθετή τα y_n.

Δεδομένου ότι μια αυθαίρετη αναδιάταξη των ριζών ενός γινομένου εξακολουθεί να παράγει το ίδιο πολυώνυμο, π.χ.

$$(y - y_3)(y - y_1)(y - y_2)(y - y_5)(y - y_4)$$

εξακολουθεί να είναι το ίδιο όπως πολυώνυμο

$$(y - y_1)(y - y_2)(y - y_3)(y - y_4)(y - y_5).$$

Επίσης ο ισομορφισμός σ' αφήνει το f σταθερό, έτσι ώστε να είναι στοιχεία της ομάδας Galois G (E / F). Έτσι δείξαμε ότι $S_5 \subseteq G(E/F)$. Παρόλα αυτά είναι πιθανόν να υπάρξουν ισομορφισμοί που να μην ανήκουν στο S_5.

Δεδομένου ότι η σχετική ομάδα ισομορφισμών για το πεδίο του 5ου βαθμού πολυώνυμου έχει το πολύ 5! στοιχεία, προκύπτει ότι το G (E / F) είναι ισόμορφο με S_5. Γενικεύοντας το επιχείρημα αυτό δείχνει ότι η ομάδα Galois για κάθε βαθμού n πολυωνύμου είναι ισόμορφη με S_n.

Ισχύει ότι $S_5 \leq A_5 \leq e$ όπου A_5είναι μία εναλλασσόμενη ομάδα 5 στοιχείων. Επειδή το $\frac{A_5}{e}$ (ισόμορφο στο A_5) δεν αποτελεί αβελιανή ομάδα ,το S_5 δεν επιλύνεται , άρα η γενικότερη μορφή πολυωνύμου 5ου βαθμού δεν επιλύνεται με ριζικά. Επιπλέον, αφού η πρώτη μη τετριμμένη υποομάδα της συμμετρικής ομάδας n στοιχείων είναι πάντα η εναλλασσόμενη ομάδα n στοιχείων και αφού η εναλλασσόμενη ομάδα n στοιχείων για n≥ 5 είναι πάντα απλή και μη αβελιανή ομάδα, άρα και μη επιλύσιμη, σημαίνει επίσης ότι τα γενικά πολυώνυμα όλων των βαθμών υψηλότερα από ό, τι τον πέμπτο δεν έχουν επίσης καμία λύση σε ρίζες.

2.4 Θεωρία σωμάτων

Στα μαθηματικά, ένα αλγεβρικό σώμα αριθμών (ή απλά σώμα αριθμών) F είναι μια πεπερασμένη (και άρα αλγεβρική) επέκταση σώματος του σώματος των ρητών αριθμών Q. Έτσι το F είναι ένα σώμα που περιέχει το Q και έχει πεπερασμένη διάσταση όταν λογίζεται ως διανυσματικός χώρος πάνω από το Q.

Η ιδέα ενός αλγεβρικού σώματος βασίζεται στην έννοια ενός σώματος. Ένα σώμα αποτελείται από ένα σύνολο στοιχείων μαζί με δυο πράξεις, οι οποίες ονομάζονται πρόσθεση, και πολλαπλασιασμός, και μερικές υποθέσεις. Ένα έξοχο

παράδειγμα σώματος είναι το σώμα των ρητών αριθμών, συμβολιζόμενο συνήθως με Q, μαζί με τις συνήθεις πράξεις της πρόσθεσης κτλ.

Μια άλλη ιδέα που χρειάζεται για να προσδιορίσουμε αλγεβρικά σώματα είναι αυτή των διανυσματικών χώρων. Εδώ να προσθέσουμε ότι, μπορούμε να θεωρήσουμε πως οι διανυσματικοί χώροι αποτελούνται από ακολουθίες (x_1, x_2, ...) των οποίων οι όροι είναι στοιχεία ενός σταθερού σώματος, όπως το σώμα Q. Οποιεσδήποτε τέτοιες δυο ακολουθίες μπορούν να προστεθούν προσθέτοντας τους όρους έναν προς έναν. Επιπρόσθετα, κάθε ακολουθία μπορεί να πολλαπλασιαστεί από ένα συγκεκριμένο στοιχείο c του σταθερού σώματος. Οι δυο αυτές πράξεις γνωστές ως διανυσματική πρόθεση και βαθμωτός πολλαπλασιασμός ικανοποιούν ένα αριθμό ιδιοτήτων οι οποίες βοηθούν στο να ορίσουμε τους διανυσματικούς χώρους αφηρημένα. Οι διανυσματικοί χώροι μπορούν να είναι "πεπερασμένης διάστασης", δηλαδή οι ακολουθίες που τους απαρτίζουν να είναι πεπερασμένου μήκους. Αν, όμως, ο διανυσματικός χώρος αποτελείται από πεπερασμένες ακολουθίες (x_1, x_2, ..., x_n), ο διανυσματικός χώρος λέγεται πεπερασμένης διάστασης, n.

Ένα αλγεβρικό σώμα (ή απλά σώμα) είναι ένα πεπερασμένου βαθμού σώμα επέκτασης του σώματος των ρητών αριθμών. Εδώ η διάσταση του ως ένας διανυσματικός χώρος πάνω από το Q λέγεται απλά βαθμός.

2.4.1 Αλγεβρικότητα και δακτύλιος ακεραίων

Γενικά, στην αφηρημένη άλγεβρα, ένα σώμα επέκτασης F / E είναι αλγεβρικό αν κάθε στοιχείο f του μεγαλύτερου σώματος F είναι ρίζα ενός πολυωνύμου με συντελεστές e_0, ..., e_m από το E:

$p(f) = e_m f_m + e_m{-}1 f_m{-}1 + ... + e_1 f + e_0 = 0.$

Είναι γεγονός ότι κάθε πεπερασμένο σώμα επέκτασης είναι αλγεβρικό (απόδειξη: για x στο F απλά θεωρείστε x, x_2, x^3 ...παίρνουμε μια γραμμική εξάρτηση, π.χ. ένα πολυώνυμο x είναι μια ρίζα του!). Ειδικότερα αυτό εφαρμόζεται στα αλγεβρικά σώματα, έτσι ώστε κάθε στοιχείο f ενός αλγεβρικού σώματος F να μπορεί να γραφτεί σαν μια ρίζα ενός πολυωνύμου με ρητούς συντελεστές. Συνεπώς, τα στοιχεία του F αναφέρονται επίσης ως αλγεβρικοί αριθμοί. Δοθέντος ενός πολυωνύμου p τέτοιου ώστε p(f) = 0, μπορεί να εξασφαλιστεί ότι ο συντελεστής του μεγιστοβάθμιου όρου e_m είναι μονάδα, διαιρώντας όλους τους συντελεστές με αυτόν, αν είναι απαραίτητο. Ένα πολυώνυμο με αυτήν την ιδιότητα είναι γνωστό ως μονικό πολυώνυμο. Γενικά θα έχει ρητούς συντελεστές. Αν, όμως, οι συντελεστές του είναι όλοι ακέραιοι, το f καλείται ακέραιος αλγεβρικός. Κάθε (συνήθης) ακέραιος $z \in Z$ είναι αλγεβρικός ακέραιος, καθώς είναι ρίζα του γραμμικού μονικού πολυωνύμου:

$$p(t) = t - z.$$

Μπορεί να δειχθεί ότι κάθε ακέραιος αλγεβρικός που είναι επίσης ρητός αριθμός είναι στην πραγματικότητα ακέραιος, εξου και το όνομα "ακέραιος αλγεβρικός". Χρησιμοποιώντας ξανά αφηρημένη άλγεβρα, και συγκεκριμένα την ιδέα ενός πεπερασμένα παραγόμενου μοντέλου, μπορεί να δειχθεί ότι το άθροισμα και το γινόμενο οποιωνδήποτε δυο ακέραιων αλγεβρικών είναι επίσης ακέραιος αλγεβρικός, έπεται ότι οι ακέραιοι αλγεβρικοί του F σχηματίζουν έναν δακτύλιο που συμβολίζεται με Q_F και λέγεται δακτύλιος των ακεραίων του F. Είναι ένας υποδακτύλιος του (δηλαδή, ένας δακτύλιος που περιέχεται στο) F. Ένα σώμα δεν περιέχει διαιρέτες του μηδενός και η ιδιότητα αυτή κληρονομείται από κάθε υποδακτύλιο. Συνεπώς, ο δακτύλιος των ακεραίων του F είναι μια ακέραια περιοχή. Το σώμα F είναι το σώμα κλασμάτων της ακεραίας περιοχής O_F. Με τον τρόπο αυτό μπορεί κανείς να μεταβεί μπροστά και πίσω μεταξύ του αλγεβρικού σώματος F και του δακτυλίου του των ακεραίων O_F. Οι δακτύλιοι των ακεραίων αλγεβρικών έχουν τρεις χαρακτηριστικές ιδιότητες:

- Q_F είναι μια ακέραια περιοχή που είναι ολοκληρωτικά κλειστή στο σώμα κλασμάτων της F.
- Q_F είναι ένας Noetherian δακτύλιος.
- Τέλος, κάθε μη-μηδενικό πρώτο ιδεώδες του O_F είναι μέγιστο ή, ισοδύναμα, η Krull διάσταση του δακτυλίου αυτού είναι ένα. Ένας αντιμεταθετικός δακτύλιος με τις τρεις αυτές ιδιότητες λέγεται Dedekind δακτύλιος (ή Dedekind περιοχή), προς τιμήν του Richard Dedekind, ο οποίος ανέλαβε μια σε βάθος μελέτη των δακτυλίων των αλγεβρικών ακεραίων.

2.4.2 Βάσεις για σώματα αριθμών

Μια **ακέραια βάση** για ένα σώμα F βαθμού n είναι ένα σύνολο

$$B = \{b_1, \ldots, b_n\}$$

από n αλγεβρικούς ακεραίους του F έτσι ώστε κάθε στοιχείο του δακτυλίου των ακεραίων O_F του F να γράφεται μοναδικά ως ένας Z-γραμμικός συνδυασμός στοιχείων του B; έτσι, για κάθε x στο O_F έχουμε

$$x = m_1 b_1 + \ldots + m_n b_n,$$

όπου τα m_i είναι (συνηθισμένοι) ακέραιοι. Τότε ισχύει επίσης ότι κάθε στοιχείο του F μπορεί να γραφτεί μοναδικά ως

$$m_1 b_1 + \ldots + m_n b_n$$

όπου τώρα τα m_i είναι ρητοί αριθμοί. Οι αλγεβρικοί ακέραιοι του F είναι τότε ακριβώς εκείνα τα στοιχεία του F όπου τα m_i είναι όλα ακέραιοι.

Έστω F ένα σώμα βαθμού n. Μεταξύ όλων των πιθανών βάσεων του F (ως Q-διανυσματικός χώρος), υπάρχουν συγκεκριμένες βάσεις γνωστές ως βάσεις δύναμης, της μορφής

$$Bx = \{1, x, x^2, ..., x^{n-1}\}$$

για κάποια στοιχεία $x \in F$. Από το θεώρημα πρωτεύοντος στοιχείου, υπάρχει ένα τέτοιο x, που λέγεται πρωτεύον στοιχείο. Αν το x μπορεί να επιλεχθεί στο O_F και έτσι ώστε Bx να είναι βάση του O_F ως ένα ελεύθερο Z-module, τότε Bx λέγεται **βάση ακέραιας δύναμης**, και το σώμα F λέγεται μονογενικό σώμα. Ένα παράδειγμα σώματος που δεν είναι μονογενικό δόθηκε για πρώτη φορά από τον Dedekind. Το παράδειγμά του είναι το σώμα που προκύπτει επισυνάπτοντας μια ρίζα του πολυωνύμου $x^3 - x^2 - 2x - 8$.

2.4.3 Κατασκευές σωμάτων

Έστω k □ F, όπου k, F σώματα, και έστω $a \in$ F. Ορίζουμε k[a] = {f(a) : f(x) $\in$ R[x]}, ενώ k(a) = {f(a)/g(a) : g(a) $\neq$0, f(x), g(x) $\in$R[x]}.

Μπορούμε να δείξουμε ότι το σύνολο k[a] είναι ο μικρότερος δακτύλιος που περιέχει το k και το a, ενώ το σύνολο k(a) είναι το μικρότερο σώμα που περιέχει το k και το a. Αυτόματα k[a] □ k(a) □ F. Το k(a) είναι ισόμορφο με το σώμα κλασμάτων του k[a].

Παραδείγματα (Χαραλάμπους Χ. 2008)

- C = R[i] = {a + bi : a, b $\in$ R} και R[i] = R(i) = C
- $Q[\sqrt{3}] = Q(\sqrt{3}) = \{a + b\sqrt{3} : a, b \in Q\}$
- $Q[\sqrt[3]{2}] = \{\alpha_0 + \alpha_1 \sqrt[3]{2} + \alpha_2 \sqrt[3]{4} : a_i \in Q\} = Q(\sqrt[3]{2})$
- Μια βάση του $Q[\sqrt{3}]$ ως Q- διανυσματικός χώρος είναι το σύνολο $\{1, \sqrt{3}\}$.
- Μια βάση του $Q[\sqrt[3]{2}]$ ως Q- διανυσματικός χώρος είναι το σύνολο $\{1, \sqrt[3]{2}, \sqrt[3]{4}\}$.

Θυμίζουμε ότι αν το k είναι σώμα, τότε ο δακτύλιος k[x] είναι περιοχή κυρίων ιδεωδών για την οποία ισχύει ο Ευκλείδειος αλγόριθμος διαίρεσης πολυωνύμων.

Έπεται ότι εάν p(x) ∈ k[x] και a ∈ k είναι ρίζα του p(x) (δηλαδή p(a) = 0), τότε p(x) = (x − a)q(x). Συνεπάγεται ότι p(x) έχει το πολύ deg(p) ρίζες. Στον δακτύλιο k[x] κάθε πολυώνυμο μπορεί να παραγοντοποιηθεί μονοσήμαντα σε γινόμενο αναγώγων πολυωνύμων. Επίσης το μόνο ιδεώδες στο k[x] που είναι πρώτο αλλά όχι μέγιστο είναι το μηδενικό ιδεώδες. Το ιδεώδες I = (f(x)) είναι μέγιστο (και πρώτο) αν και μόνο αν το πολυώνυμο f(x) είναι ανάγωγο. Στην περίπτωση αυτή ο δακτύλιος πηλίκο k[x]/I είναι σώμα.

Παράδειγμα

Ο δακτύλιος E = Q[x]/(χ^2 −3) είναι σώμα. Έστω I το μέγιστο ιδεώδες (χ^2 −3). Έστω f(x)∈Q[x]. Τότε f(x) = (χ^2 −3)q(x)+r(x) όπου r(x) ∈ Q[x] και deg(r(x)) < 2. Επομένως στο E ισχύει ότι f(x) + I = r(x) + I. Ο αντίστροφος του x + I στο E είναι το στοιχείο $\frac{1}{3}$x + I , ενώ ο αντίστροφος του x + 2 + I είναι ίσο με −x + 2 + I. Μία βάση του E ως Q-διανυσματικου χώρου είναι το σύνολο $\{\bar{1}, \bar{\chi}\}$. Σύμφωνα με την προηγούμενη παρατήρηση ένα τυχαίο στοιχείο του E είναι της μορφής r(x)+I όπου r(x) = α_1x + α_0. Έπεται ότι r(x) + I = α_1 (x + I) + α_0 (1 + I) και άρα τα στοιχεία $\bar{1}$, $\bar{\chi}$ παράγουν το E. Για να δείξουμε τη γραμμική ανεξαρτησία των $\bar{1}$, $\bar{\chi}$,έστω ότι $c_0\bar{1}$ + $c_1\bar{\chi}$ = $\bar{0}$. Επομένως c_0(1 + I) + c_1(χ + I) = I και c_0 + c_1x □ (χ^2 − 3). Άρα c_0 + c_1x = g(x) (χ^2 − 3). Στη περίπτωση που g(x) ≠0 τότε deg(g(x)(χ^2 − 3)≥ 2, άτοπο. Άρα g(x) = 0 και c_0 = c_1 = 0 και επομένως $\bar{1}$, $\bar{\chi}$ είναι γραμμικά ανεξάρτητα. Επιπρόσθετα παρατηρούμε ότι αν εκτιμήσουμε το πολυώνυμο ($y^2 - \bar{3}$) στην τιμή $\bar{\chi}$ περνούμε 0 και άρα $\bar{\chi}$ είναι ρίζα του πολυωνύμου $y^2 - \bar{3}$: (x + I) ^{2} − (3 + I) = χ^2 − 3 + I = I.

Συμπεραίνουμε ότι

Έστω ότι F είναι σώμα και p(x) ∈F[x] είναι ανάγωγο. Ο δακτύλιος πηλίκο E = F[x]/I είναι σώμα. Τότε ισχύουν τα εξής :

- Το σώμα E μπορεί να θεωρηθεί σαν επέκταση του F, αφού υπάρχει μονομορφισμός F → E, c → c + I.
- Έστω ότι deg p(x) = n. Τότε ένα τυχαίο στοιχείο του E είναι της μορφής α_0 + α_1x + . . . + $\alpha_{n-1}x^{n-1}$ + I όπου α_i ∈F. Θέτοντας 1 = 1 + I και a = x + I έχουμε ότι

$$E = \{\alpha_0\ 1 + \alpha_1\alpha + \ldots + \alpha_n\alpha^{n-1}\ : \alpha_i \in F\}$$

- Το σώμα E είναι F-διανυσματικός χώρος. Μια βάση του υπεράνω του F είναι το σύνολο ο $\{1, a, \ldots, \alpha^{n-1}\}$. Η διάσταση του E ως F-διανυσματικός χώρος λέγεται βαθμός και συμβολίζεται με [E : F]. Ο βαθμός του E είναι ο βαθμός του πολυωνύμου p(x).
- Στο σώμα E, το στοιχείο a = x + I είναι ρίζα του πολυωνύμου p(y) ∈ E[y].
- Όταν το |F| = t τότε E = y^2 .

2.4.4 Αλγεβρικά στοιχεία πάνω από ένα σώμα K

Έστω F → E και a ∈E. Το a είναι αλγεβρικό πάνω από το F αν υπάρχει f(x) ∈F[x], έτσι ώστε f(x) ≠ 0 και f(a) = 0. Αν το a δεν είναι αλγεβρικό, τότε a είναι υπερβάτικο, υπεράνω του F.

Αν F→ E και a □ E τότε σύμφωνα με το πρώτο θεώρημα ισομορφίας των δακτυλίων

$$F[a] \sim= F[x]/\ker \varphi$$

Όπου φ : F[x]→F[a] είναι ο επιμορφισμός δακτυλίων που στέλνει το πολυώνυμο f(x) στο στοιχείο f(a) ∈F[a].

Παραδείγματα

- $\sqrt{3}$ αλγεβρικό υπεράνω του Q αφού είναι ρίζα του $\chi^2 - 3$.
- Έστω E = Q[x]/(x^2 − 3). Θεωρούμε το στοιχείο $\bar{\chi} \in$ E. Τοτε $\bar{\chi}$ είναι αλγεβρικό υπεράνω του Q αφού είναι ρίζα $y^2 - 3$.
- a ∈E είναι αλγεβρικό υπεράνω του E αφού είναι ρίζα του x − a.
- Αν k ⊆ F⊆ E και a ∈E είναι αλγεβρικό υπεράνω του K τότε a είναι αλγεβρικό υπεράνω του F

Έστω F → E και a ∈E. Αν το α είναι αλγεβρικό πάνω στο F τότε e F[a] = F(a).

Αν a ∈E είναι αλγεβρικό υπεράνω του F τότε dimF F[a] < ∞. Αν a □ E είναι υπερβατικό υπεράνω του F τότε dimF F[a] = ∞.

Αν a ∈E είναι αλγεβρικό υπεράνω του F τότε υπάρχει μοναδικό κανονικό ανάγωγο πολυώνυμο f(x) έτσι ώστε f(a) = 0. Αν g(x) ∈F[x] και g(a) = 0 τότε g(x) = q(x)f(x).

2.4.5 Πεπερασμένα σώματα

Στα μαθηματικά, ένα σώμα καλείται πεπερασμένο αν το πλήθος των στοιχείων του είναι πεπερασμένο. Ένα πεπερασμένο σώμα λέγεται αλλιώς και σώμα Γκαλουά προς τιμήν του Γάλλου μαθηματικού Γκαλουά (Évariste Galois). Τα πεπερασμένα σώματα είναι σημαντικά στην Θεωρία Αριθμών, την Αλγεβρική Γεωμετρία, την Κρυπτογραφία και τη Θεωρία Κωδικοποίησης.

Τα πεπερασμένα σώματα έχουν μελετηθεί πλήρως και κατηγοριοποιούνται ως εξής:

- Κάθε πεπερασμένο σώμα έχει pn στοιχεία, όπου p πρώτος αριθμός n ≥1 ακέραιος. (Το p ονομάζεται χαρακτηριστική του σώματος.)
- Για κάθε πρώτο p και κάθε ακέραιο n ≥ 1, υπάρχει ένα πεπερασμένο σώμα με pn στοιχεία.
- Όλα τα σώματα με pn στοιχεία είναι ισόμορφα μεταξύ τους. Μπορούμε να ταυτίσουμε όλα τα σώματα με τον ίδιο αριθμό στοιχείων. Συμβολισμός: GF(pn). όπου τα γράμματα "GF" προέρχονται από το αγγλικό "Galois field" (σώμα Γκαλουά).

Έστω A μια πεπερασμένη αβελιανή ομάδα. Τότε υπάρχουν πρώτοι αριθμοί, $p_1 \ldots, p_s$ *(όχι κατά ανάγκη διαφορετικοί) και φυσικοί αριθμοί* $n_1 \ldots, n_s$ *έτσι ώστε*

$$A = z_{p1}^{ni} \times \cdots \times z_{ps}^{ns}$$

Έστω f(x) $\in E[x]$ *και deg(f(x)) = n ≥ 1. Λέμε ότι το f(x) διασπάται πάνω από το E αν f(x) = b(x −* α_1*)· · ·(x −* α_n*) και* $\alpha_i \in E$.

Έστω f(x) $\in F[x]$. *Τότε υπάρχει ένα σώμα E, τέτοιο ώστε e* $F \subseteq$ *E και f(x) να διασπάται στο E.*

Υπάρχει σώμα με p^n *στοιχεία* (Χαραλάμπους 2008)

2.4.6 Κριτήρια για αναγωγιμότητα πολυωνύμων πάνω από σώμα

Κριτήριο Eisenstein: έστω ότι f(x) = $\alpha_n \chi^n + \cdots + \alpha_0$, $\alpha_i \in Z$, και ότι για κάποιον πρώτο αριθμό p ισχύει ότι p διαιρεί α_i για i = 0, . . . , n − 1, p δεν διαιρεί το α_n, ενώ p^2 δεν διαιρεί το α_0. Τότε το f(x) είναι ανάγωγο πάνω από το Q.

Έστω k σώμα , f(x) ∈ k[x]. Τότε f(x) είναι ανάγωγο στο K(x) αν και μόνο αν f(x + c) είναι ανάγωγο πάνω από το k για κάθε c ∈ k.

Έστω f(x) = $\alpha_n \chi^n + \cdots + \alpha_0$, $\alpha_i \in Z(\chi)$, πρωταρχικό. Έστω ότι για p ∈ Z, p πρώτο ισχύει ότι deg f(x) = deg $\overline{f(x)}$ όπου $\overline{f(x)} = \overline{\alpha_n}\, \chi^n + \cdots + \overline{\alpha_0}$. Αν $\overline{f(x)}$ είναι ανάγωγο στο $Z_P(\chi)$, τότε f(x) είναι ανάγωγο πάνω από το Z.

Κεφάλαιο 3ο

3.1 Θεωρία Γκαλουά

Η θεωρία Γκαλουά προέρχεται από την μελέτη των συμμετρικών συναρτήσεων. Οι συντελεστές του πολυωνύμου είναι τα στοιχειώδη συμμετρικά πολυώνυμα στις ρίζες. Για παράδειγμα το $(x-a)(x-b) = x^2 - (a+b)x + ab$, όπου 1, $a+b$ και ab είναι τα στοιχειώδη πολυώνημα βαθμού 0,1 και 2 σε δύο μεταβλητές.

Αυτό, πρώτη φορά επισημοποιήθηκε τον 16ο αιώνα από τον Γάλλο μαθηματικό Φρανσουά Βιέτα, στους τύπους Βιέτα, για την περίπτωση των θετικών πραγματικών ριζών. Κατά τη γνώμη του Βρετανού μαθηματικού Τσαρλς Χιούτον, τον 18ο αιώνα , η έκφραση των συντελεστών του πολυωνύμου σε σχέση με τις ρίζες (όχι μόνο για τις θετικές ρίζες) έγινε για πρώτη φορά κατανοητό από τον Γάλλο μαθηματικό Αλπέρ Ζιράρντ τον 17ο αιώνα.

Από τα νεανικά του ακόμα χρόνια, ήταν ικανός να προσδιορίσει μια ικανή και αναγκαία συνθήκη ώστε να γνωρίζει αν ένα πολυώνυμο είναι επιλύσιμο με ριζικά λύνοντας έτσι ένα πρόβλημα που βασάνιζε τους μαθηματικούς για αρκετούς αιώνες. Η προσφορά του για τα μαθηματικά ήταν στα θεμέλια της Θεωρίας Γκαλουά και Άλγεβρας. Ήταν ο πρώτος που χρησιμοποίησε τη λέξη ομάδα για να εκφράσει ένα σύνολο μεταθέσεων. Ήταν ριζοσπάστης Δημοκρατικός κατά τη διάρκεια της μοναρχίας του Λουδοβίκου Φίλιππου στη Γαλλία και πέθανε στην ηλικία των είκοσι ένα ετών σε μια μονομαχία. Τον Οκτώβριο του 1825, ο Γκαλουά εισέρχεται στο Βασιλικό Κολέγιο *Louis-Grand* όπου έχουν φοιτήσει ο Μολιέρος, ο Βίκτωρ Ουγκώ, ο Ροβεσπιέρος και ο Ντελακρουά. Ο Γκαλουά έλαβε υποτροφία και εισήχθη οικότροφος στο Κολέγιο. Τα πρώτα τρία χρόνια θεωρήθηκε ένας από τους καλύτερους σπουδαστές και τον Οκτώβριο του 1825 άρχισε να παρακολουθεί τον ανώτερο κύκλο σπουδών της σχολής – την τάξη ρητορικής. Αλλά οι ενδείξεις κόπωσης που παρουσίασε οδήγησαν τον διευθυντή να τον συμβουλεύσει να επαναλάβει το μάθημα τον Ιανουάριο του 1827. Χωρίς κάποια ιδιαίτερη προσπάθεια έγινε ξανά ένας από τους καλύτερους σπουδαστές και βραβεύθηκε για μεταφράσεις ελληνικών κειμένων καθώς έλαβε και επαίνους για άλλα τέσσερα θέματα. Τα χρόνια αυτή ήταν σημείο καμπής για τον Εβαρίστ που ανακάλυψε τα μαθηματικά και εισχώρησε στον κόσμο τους. ***(Wikimedia)***

Οι μαθηματικοί (αρχίζοντας από τους γραφείς της Βαβυλώνιας και φτάνοντας στους φυσικομαθηματικούς του 20ού αιώνα) έβρισκαν πρόβλημα στην έννοιας της συμμετρίας μέχρι την στιγμή που εμφανίστηκε ο Galois και έφερε μια νέα τροπή στην μαθηματική σκέψη.

Ήταν μια μαθηματική ιδιοφυία, που προσπάθησε από 15 ετών και τελικά απέδειξε ανεξάρτητα από τον Abel, με την περίφημη «θεωρία Galois» ότι εξισώσεις μεγαλύτερες του $4^{ου}$ βαθμού δεν λύνονται γενικά. Σκοτώθηκε σε στημένη μονομαχία σε ηλικία 21 ετών περίπου.

Ο Galois ανακάλυψε ότι η αδυναμία επίλυσης εξισώσεων πέμπτου βαθμού είναι απότοκο της συμμετρίας της εξίσωσης. Ήταν το πρόσωπο που άλλαξε την πορεία των μαθηματικών. Η λύση των αλγεβρικών εξισώσεων υπήρξε ένα από τα σπουδαιότερα πεδία έρευνας στην περιοχή της άλγεβρας και για πολλά χρόνια συγκέντρωσε το ενδιαφέρον κορυφαίων μαθηματικών όλων των εποχών. Μετά το πρώτο μισό του περασμένου αιώνα ο Γάλλος μαθηματικός **Evariste Galois** χρησιμοποιώντας την ομάδα μεταθέσεων των ριζών της εξίσωσης κατορθωσε να βρεί συνθήκες κάτω από τις οποίες λύνονται που έχουν βάθμο ανώτερο από τέταρτο (κάτι που αποτέλεσε σταθμό στην θεωρία ομάδων και τις εφαρμογες της).

3.2 Ιστορική ανασκόπηση πολυωνυμικών εξισώσεων

Al-jabr, al-Khwârizmi και ισλαμικά μαθηματικά

Το βιβλίο του al-Khwarizmi δεν χρησιμοποιεί τον σύγχρονο αλγεβρικό συμβολισμό ούτε και εξισώσεις. Το οτιδήποτε είναι γραμμένο με λέξεις. Διαπραγματεύεται κυρίως εξισώσεις. Μελετά έξι διαφορετικούς τύπους εξισώσεων. Ωστόσο τα ισλαμικά μαθηματικά δεν ασχολούνται με ΑΡΝΗΤΙΚΟΥΣ αριθμούς. Στη δευτεροβάθμια λόγου χάρη εξίσωση οι αρνητικές ρίζες αγνοούνται. Το ίδιο όμως βιβλίο περιέχει και κανόνες Αριθμητικής που διαμορφώθηκαν με τα ινδικά πρότυπα για την εκτέλεση πράξεων με ινδικά ψηφία . Αναφέρεται επίσης σε τετραγωνικές και κυβικές ρίζες, σε κλάσματα και στη μέθοδο των τριών.

Άλγεβρα των πολυωνύμων

Ο Abu Bakr al-Karaji συνέχισε την εργασία του al-Khwarizmi εστιάζοντας στο να εφαρμόσει τις τεχνικές της Αριθμητικής στην Άλγεβρα. Ανέπτυξε μια τεχνική κατά την οποία έδωσε όνομα στις νιοστές δυνάμεις x^n και στα αντίστροφά τους $1/x^n$. Μπορούσε έτσι να εργαστεί σε πράξεις – πρόσθεση, αφαίρεση, πολλαπλασιασμός, διαίρεση – στα πολυώνυμα.

Ο Ευκλείδης (πατέρας της γεωμετρίας) και η εξίσωση δευτέρου βαθμού

Μολονότι ο όρος Άλγεβρα δημιουργήθηκε κατά τον Μεσαίωνα πολλές «αλγεβρικές» έννοιες είχαν κάνει την εμφάνισή τους πολύ νωρίτερα. Το Βιβλίο 2 των Στοιχείων του Ευκλείδη ασχολείται με δευτεροβάθμιες αλγεβρικές εξισώσεις. Ο αλγεβρικός συμβολισμός δεν έχει επινοηθεί.

Ο **Ευκλείδης** από την Αλεξάνδρεια (~350 π.Χ. - 270 π.Χ.), ήταν Έλληνας μαθηματικός, που δίδαξε και πέθανε στην Αλεξάνδρεια της Αιγύπτου, περίπου κατά την διάρκεια της βασιλείας του Πτολεμαίου Α΄ (323 π.Χ. - 283 π.Χ.). Στις μέρες μας είναι γνωστός ως ο «πατέρας» της Γεωμετρίας. Ο Ευκλείδης κατέχει μια κρίσιμη θέση στην ιστορία της Λογικής και των Μαθηματικών, καθώς είναι ο πρώτος που παράγει ένα αυστηρά δομημένο και συνεκτικό σύστημα προτάσεων (θεωρημάτων και πορισμάτων) με βάση ένα σύνολο ορισμών και 5 μόνο αρχικές αναπόδεικτες προτάσεις (αιτήματα). Κατ' αυτό το τρόπο περιέλαβε στο σύστημα αυτό και προτάσεις ήδη διατυπωμένες παλαιότερων σημαντικών μαθηματικών, όπως ο Θαλής, ο Πυθαγόρας, ο Θεαίτητος, ο Λεωδάμαντας και ο Εύδοξος. Ο Ευκλείδης αναπαριστά τους αριθμούς με ευθύγραμμα τμήματα .

Οι αλγεβρικές ταυτότητες όπως η $(a+b)^2=a^2+2ab+b^2$ παρουσιάζονται πλεόν με μορφή γεωμετρική.

Οι πρωτοβάθμιες (γραμμικές) εξισώσεις λύνονται με γεωμετρικές κατασκευές.

Οι δευτεροβάθμιες εξισώσεις ανάγονταν σε γεωμετρικό ισοδύναμο μιας από τις μορφές η οποία στη συνέχεια λυνόταν με την εφαρμογή των ήδη θεμελιωμένων θεωρημάτων εμβαδού.

Αν και η μέθοδος δεν ήταν πολύ διαφορετική από εκείνη των Βαβυλωνίων, η «ελληνική» αυτή μέθοδος μπορούσε να οδηγήσει σε άρρητους αριθμούς. Η δευτεροβάθμια εξίσωση θεμελιώθηκε για τη λύση προβλημάτων και ειδικά εκείνων που εμπεριέχουν το πυθαγόρειο θεώρημα.

ο Διόφαντος

Αρκετούς αιώνες αργότερα στην Αλεξάνδρεια του 3ου μετά τον Χριστό αιώνα ο Διόφαντος με το βιβλίο του Αριθμητικά παρουσίασε μια όχι γεωμετρική Άλγεβρα στην οποία εντυπωσιάζει η απουσία γενικών μεθόδων και η επινόηση έξυπνων τεχνασμάτων για τη λύση 130 προβλημάτων. Το άλλο στοιχείο που χαρακτηρίζει το έργο του είναι τα πρώτα βήματα προς τον αλγεβρικό συμβολισμό. Δεν χρησιμοποιεί βέβαια γράμματα, χρησιμοποιεί όμως συντομογραφίες ενώ μέχρι την εποχή εκείνη η Άλγεβρα ήταν μόνο ρητορική. Το έργο του το ανακάλυψαν οι Ευρωπαίοι 1200 χρόνια μετά. Το 1570 ο Ιταλός μαθηματικός Ραφαήλ Μπομπέλι μετέφρασε στα λατινικά τα *Αριθμητικά* και χρησιμοποίησε τα προβλήματα που περιείχαν για τα δικά του συγγράμματα. Τον επόμενο αιώνα τα γραπτά του Διόφαντου επηρέασαν τον εξέχοντα μαθηματικό Πιέρ ντε Φερμά. Σήμερα **«διοφαντικές»** καλούνται οι εξισώσεις ακέραιων συντελεστών των οποίων ζητούνται οι ακέραιες λύσεις.

Στο μεταξύ το έργο των Ελλήνων φαίνεται ότι συνεχίστηκε από τους Άραβες

Οι Κινέζοι και τα εννέα κεφάλαια της Μαθηματικής Τέχνης

Τα «εννέα κεφάλαια της Μαθηματικής Τέχνης» ήταν μία καταγραφή των εξελίξεων στα πρώιμα κινεζικά μαθηματικά. Ο κύριος όμως στόχος τους είναι η παρουσίαση γνώσεων αστρονομίας και όχι ειδικά τα μαθηματικά. Πάντως παρουσιάζονται συστήματα πρωτοβάθμιων εξισώσεων στο κεφάλαιο 8. Η μέθοδος λέγεται «fang cheng » και οδηγεί στη λύση γραμμικών εξισώσεων. Η πρόσθεση και η αφαίρεση η οποία συμπεριλαμβάνει και αρνητικούς αριθμούς μνημονεύεται στο ίδιο αυτό βιβλίο στο οποίο γίνεται λόγος και για την «εξαγωγή» της τετραγωνικής και της κυβικής ρίζας με μέθοδο η οποία θυμίζει τη σύγχρονη

Οι Ιταλοί τον 14ο και 15ο αιώνα

Οι Ιταλοί δίδασκαν τους εμπόρους τις ινδοαραβικές τεχνικές για τη λύση προβλημάτων , και αναπτύσσοντες και προεκτείνοντες τις ισλαμικές μεθόδους - έγραφαν κείμενα τα οποία δημιούργησαν τη βάση για παραπέρα ανάπτυξη. Οι Ιταλοί εισήγαγαν τον ΑΛΓΕΒΡΙΚΟ ΣΥΜΒΟΛΙΣΜΟ ο οποίος δεν υπήρχε στην ισλαμική Άλγεβρα. Ωστόσο τα πράγματα άλλαζαν πολύ αργά και ο σύγχρονος αλγεβρικός συμβολισμός δεν καθιερώθηκα παρά μόνο κατά τον 17ο αιώνα .

Οι Ιταλοί ανέπτυξαν επίσης τη μελέτη της δευτεροβάθμιας εξίσωσης ενώ αναζητούσαν και τεχνικές για τη λύση τρίτου και τετάρτου βαθμού . Ο Maestro Dardi da Pisa εργάστηκε στις εξισώσεις τετάρτου βαθμού τις περισσότερες από τις οποίες τις ανήγαγε σε εξισώσεις δευτέρου βαθμού.

(Πηγή: Πολυωνυμικές εξισώσεις και Θεωρία του Galois του Θεόδωρου Εξαρχάκου)

3.3 Ομάδες Galois

Ένα αλγεβρικό πεδίο είναι, εξ ορισμού, ένα σύνολο στοιχείων (αριθμών) που είναι κλειστό υπό τις συνήθεις αριθμητικές πράξεις της πρόσθεσης, της αφαίρεσης, του πολλαπλασιασμού και της διαίρεσης (εκτός από διαίρεση με το μηδέν). Για παράδειγμα, το σύνολο των ρητών αριθμών είναι ένα πεδίο, ενώ οι ακέραιοι αριθμοί δεν είναι ένα πεδίο, επειδή δεν είναι κλειστοί κάτω από την πράξη της διαίρεσης (δηλαδή, το αποτέλεσμα της διαίρεσης ενός ακεραίου από μια άλλη, δεν είναι κατ 'ανάγκη ακέραιος αριθμός). Οι πραγματικοί αριθμοί αποτελούν επίσης ένα πεδίο, όπως και οι μιγαδικοί αριθμοί. Είναι δυνατόν να κατασκευάσουμε άλλα παραδείγματα πεδίων μέσω επεκτάσεων. Για παράδειγμα, δεδομένου του συνόλου Q των ρητών αριθμών, μπορούμε να αυξήσουμε το σύνολο Q κατά έναν συγκεκριμένο αριθμό ε ο οποίος δεν υπάρχει στο Q, και αυτό σημαίνει αυτομάτως ότι κάθε ορθολογική συνάρτηση του E είναι επίσης αποδεκτή σαν επέκταση του συνόλου

$$\frac{2+\frac{3}{2}\varepsilon+5\varepsilon^2+\frac{4}{7}\varepsilon^3}{7-\frac{2}{3}\varepsilon+8\varepsilon^2}$$

Το σύνολο των αριθμών που μπορούν να σχηματιστούν από τους ρητούς και το e μέσω απλών αριθμητικών πράξεων αποτελούν ένα νέο πεδίο E, το οποίο βέβαια αποτελεί επέκταση του αρχικού πεδίου Q.

Μια σημαντική ειδική περίπτωση συνάρτησης είναι όταν ο αριθμός e είναι αλγεβρικός αριθμός , δηλαδή, η ρίζα ενός πολυωνύμου με συντελεστές στο πεδίο βάσης. Σε αυτή την περίπτωση, η διαίρεση ενός πολυωνύμου σε e από οποιοδήποτε άλλο μπορεί πάντα να εκφράζεται ως ένα απλό πολυώνυμο με συντελεστές στο πεδίο βάσης. Για να αποδειχθεί αυτό, ας πούμε ότι το e είναι μια ρίζα της f δηλ. f(e) = 0 για κάποιο πολυώνυμο f βαθμού d, και ας υποθέσουμε ότι θέλουμε να αξιολογήσει την αναλογία g(e) / h(ε) για κάθε δύο πολυώνυμα g και h. Ο ισχυρισμός μας είναι ότι αυτή η αναλογία ισούται με ένα πολυώνυμο q (ε) βαθμού όχι μεγαλύτερου από του d. Αυτό ισχύει αν και μόνο αν g(ε) = h(ε)· q(ε) όπου το q είναι βαθμού που δεν είναι μεγαλύτερος από του d. Με την εφαρμογή της στη ταυτότητα f(e) = 0, μπορούμε να μειώσουμε και στις δύο πλευρές αυτής της εξίσωσης με υποτιθέμενο βαθμό όχι μεγαλύτερο από του d, και στη συνέχεια να εξισώσουμε τους συντελεστές όπως τις δυνάμεις για να καθορίσει d rational όρους σχετικά με τα d συντελεστές του q(ε), έτσι είμαστε σίγουροι για την εξεύρεση λύσης. Μια επέκταση στο πεδίο των ρητών Q βασίζεται σε ένα αλγεβρικό αριθμό επομένως συμβολίζεται ως Q[e], που σημαίνει ότι τα στοιχεία είναι όλα πολυώνυμα με rational συντελεστές.

Ένα σημαντικό και ενδιαφέρον χαρακτηριστικό του κάθε πεδίο που δίνεται είναι το σύνολο των αυτομορφισμών του πεδίου. Ένας αυτοματισμός είναι μια χαρτογράφηση

ένας-προς-έναν από τη σειρά προς τον εαυτό του τέτοιο ώστε οι πράξεις της πρόσθεσης και του πολλαπλασιασμού να διατηρούνται. Με άλλα λόγια, αν αφήσουμε M(x) να υποδηλώνει την εικόνα του x υπό την χαρτογράφηση M, αυτή η χαρτογράφηση είναι ένας αυτομορφισμός αν και μόνο αν είναι ένα-προς-ένα και ικανοποιεί τις σχέσεις M(x + y) = M(x) + M(y) και M(xy) = M(x)M(y). Είναι σαφές ότι η σύνθεση δύο ή περισσοτέρων αυτομορφισμών είναι επίσης ένας αυτομορφισμός και όλα αυτά αποτελούν μια ομάδα.

Για το πεδίο Q (δηλαδή, οι ρητοί αριθμοί) είναι εύκολο να δούμε ότι ο μόνος αυτομορφισμός είναι η χαρτογράφηση της ταυτότητας I(x) = x. Ωστόσο, για ορισμένους τομείς υπάρχουν και μη-τετριμμένοι αυτομορφισμοί. Ως παράδειγμα, εξετάστε το πεδίο $Q[\sqrt{2}]$, το οποίο αποτελείται από όλους τους αριθμούς της μορφής $p+q\sqrt{2}$ όπου p και q είναι ρητοί αριθμοί.

$$J\left(p+q\sqrt{2}\right) = p-q\sqrt{2}, J\left(p+q\sqrt{2}\right) = p-q\sqrt{2}$$

Για να αποδείξει κάποιος ότι αυτό είναι ένα αυτομορφισμός, οφείλουμε να παρατηρήσουμε ότι είναι ένα-προς-ένα συνάρτηση , και έχουμε τις σχέσεις:

$$\begin{aligned} J\left(\left[p+q\sqrt{2}\right]+\left[r+s\sqrt{2}\right]\right) &= (p+r)-(q+s)\sqrt{2} \\ &= J\left(p+q\sqrt{2}\right) + J\left(r+s\sqrt{2}\right) \end{aligned}$$

$$\begin{aligned} J\left(\left[p+q\sqrt{2}\right]\left[r+s\sqrt{2}\right]\right) &= (pr+2qs)-(ps+qr)\sqrt{2} \\ &= J\left(p+q\sqrt{2}\right)J\left(r+s\sqrt{2}\right) \end{aligned}$$

Προφανώς, η σύνθεση της J με τον ευατό της αποδίδει την ταυτότητα I, έτσι ώστε οι ομάδες των αυτομορφισμών για αυτό το πεδίο {I, J}, να δίνονται με τον πίνακα λειτουργία ομάδα

	I	J
I	I	J
J	J	I

http://www.mathpages.com/home/kmath290/kmath290.htm

Επίλυση πολυωνύμων με ριζικά

Εξίσωση 1ου βαθμού

Έστω $\alpha x+\beta=0$ (1) $\Leftrightarrow \alpha x=-\beta$

i) $\alpha \neq 0$ τότε (1) $\Leftrightarrow \alpha x=-\beta \Leftrightarrow x=-\frac{\beta}{\alpha}$ (Μοναδική λύση)

ii) α) $\alpha=0$ και $\beta \neq 0$ (1) $\Leftrightarrow 0x=-\beta$ Αδύνατη

β) $\alpha=0$ και $\beta=0$ (1) $\Leftrightarrow 0x=0$ Αόριστη (Άπειρες λύσεις)

Με $\alpha,\beta \in F$ όπου το F συμβολίζει κάποιο σώμα όπως □ ,□ ή το Q

Εξίσωση 2ου βαθμού

Ατελείς μορφές δευτεροβάθμιας εξίσωσης:

* Αν έχω την μορφή : $\alpha x^2 + \gamma = 0$ ($\alpha\neq0$) τότε θα είναι: $x=\pm\sqrt{-\frac{\gamma}{\alpha}}$, $-\frac{\gamma}{\alpha} \geq 0$ (αδύνατη αν $\alpha\gamma>0$)

* Αν έχω την μορφή : $\alpha x^2 + \beta x = 0$ ($\alpha\neq0$) τότε θα είναι : $x\cdot(\alpha x+\beta) = 0 \Leftrightarrow x= 0$ ή $x = -\frac{\beta}{\alpha}$

Επίλυση εξίσωσης β` Βαθμού

Έστω $\alpha x^2+\beta x+\gamma=0$, $\alpha\neq0$ (1)

i) Αν $\Delta= \beta^2-4\alpha\gamma>0$ τότε η (1) έχει δύο πραγματικές ρίζες άνισες τις : $x_1=\frac{-\beta+\sqrt{\Delta}}{2\alpha}$ και $x_2=\frac{-\beta-\sqrt{\Delta}}{2\alpha}$

Το δε τριώνυμο παραγοντοποιήται και γίνεται : $\alpha x^2+\beta x+\gamma=\alpha\cdot(x-x_1)\cdot(x-x_2)$

ii) Αν $\Delta= \beta^2 -4\alpha\gamma=0$ τότε η (1) έχει διπλή ρίζα την :

$x_0=\frac{-\beta}{2\alpha}$ και $\alpha x^2+\beta x+\gamma=\alpha\cdot(x-x_0)^2 = \alpha\cdot(x+\frac{\beta}{2\alpha})^2$

iii) Αν $\Delta= \beta^2 -4\alpha\gamma<0$ τότε η (1) δεν έχει πραγματικές ρίζες και το τριώνυμο $\alpha x^2+\beta x+\gamma$ δεν παραγοντοποιείται. $\alpha x^2+\beta x+\gamma= \alpha\cdot[(x+\frac{\beta}{2\alpha})^2 +\frac{-\Delta}{4\alpha}]$

Η κεντρική ιδέα της λύσης της δευτεροβάθμιας : $x_{1,2}=\frac{-\beta\pm\sqrt{\Delta}}{2\alpha}$ είναι το γεγονός ότι μια ρητή συμμετρική αλγεβρική παράσταση $P(\chi_1,\chi_2)$ μπορεί να εκφραστεί ως ρητή συνάρτηση στοιχειωδών συμμετρικών παραστάσεων.

<u>Τύποι Vieta</u> : $S=x_1+x_2=-\frac{\beta}{\alpha}$ και $P=x_1\cdot x_2=\frac{\gamma}{\alpha}$ $(x^2-sx+p=0)$

όπου **S** το άθροισμα των ριζών και **P** το γινόμενο των ριζών της εξίσωσης.

$$x_1^{\,3}+x_2^{\,3}=S-3SP$$

Επίσης, $\frac{1}{x_1}+\frac{1}{x_2}=\frac{S}{P}$

$$\frac{1}{x_1^{\,4}}+\frac{1}{x_2^{\,4}}=\frac{S^4-4S^2P+2P^2}{P^4}$$

<u>Εξίσωση 3^{ου} βαθμού</u>

Η γενική μορφή εξίσωσης 3ου βαθμού με έναν άγνωστο και πραγματικούς συντελεστές έναν άγνωστο και πραγματικούς συντελεστές είναι: $\chi^3+\kappa\chi^2+\lambda\chi+\mu=0$

Θέτωντας $\chi=\psi-\frac{\kappa}{3}$ η δοθείσα εξίσωση μετατρέπεται σε μια εξίσωση τρίτου βαθμού δίχως δευτεροβάθμιο όρο $\Leftrightarrow \chi^3+\alpha\chi+\beta=0$ (1)

Για να την λύσουμε θέτουμε $\chi=\psi+\zeta$ (2) οπότε θα έχουμε:

$\psi^3+\zeta^3+3\psi\zeta(\psi+\zeta)+\alpha(\psi+\zeta)+\beta=0$

Κατόπιν θέτουμε $3\psi\zeta=-\alpha \Leftrightarrow \psi\zeta=-\alpha/3$ (3)

Καταλήγουμε στο σύστημα: $\begin{cases}\psi\zeta=-\frac{\alpha}{3}\\ \psi^3+\zeta^3=-\beta\end{cases}\Rightarrow\begin{cases}\psi^3\zeta^3=-\frac{\alpha^3}{27}\\ \psi^3+\zeta^3=-\beta\end{cases}$ (4)

Εφόσον ξέρουμε το άθροισμα και το γινόμενο του ψ^3 και ζ^3 αυτές οι ποσότητες μπορούν να βρεθούν λύνοντας την δευτεροβάθμια εξίσωση: $t^2+\beta t-\frac{\alpha^3}{27}=0$ (5)

$$\text{Έχουμε}: \Delta=\beta^2+\frac{4\alpha^3}{27}=4[(\frac{\beta}{2})^2+(\frac{\alpha}{3})^3]$$

Επομένως,

$$\psi^3=\frac{-\beta-\sqrt{\Delta}}{2}=-\frac{\beta}{2}-\sqrt{(\frac{\beta}{2})^2+(\frac{\alpha}{3})^3}\ \Leftrightarrow \psi=\sqrt[3]{-\frac{\beta}{2}-\sqrt{(\frac{\beta}{2})^2+(\frac{\alpha}{3})^3}}$$

$$\zeta^3=\frac{-\beta+\sqrt{\Delta}}{2}=-\frac{\beta}{2}+\sqrt{(\frac{\beta}{2})^2+(\frac{\alpha}{3})^3}\ \Leftrightarrow \psi=\sqrt[3]{-\frac{\beta}{2}+\sqrt{(\frac{\beta}{2})^2+(\frac{\alpha}{3})^3}}$$

Καταλήγουμε έτσι στον τύπο που δίνει την λύση της σχέσης (1):

$$\chi=\sqrt[3]{-\frac{\beta}{2}-\sqrt{(\frac{\beta}{2})^2+(\frac{\alpha}{3})^3}}+\sqrt[3]{-\frac{\beta}{2}+\sqrt{(\frac{\beta}{2})^2+(\frac{\alpha}{3})^3}} \quad (6)$$

Ο παραπάνω τύπος αναφέρεται και ως τύπος του **Gardano** (Ιταλός μαθηματικός) και εκφράζει την λύση της τριτοβάθμιας εξίσωσης συναρτήσει των συντελεστών της.

Εξίσωση 4ου βαθμού

Η γενική μορφή μιας τεταρτοβάθμιας εξίσωσης είναι: $\chi^4 + \alpha_3 x^3 + \alpha_2 \chi^2 + \alpha_1 \chi + \alpha_0 = 0$

Σύμφωνα με τον Καρτέσιο αν θέσουμε $X = \chi - \frac{\alpha_3}{4}$ μετατρέπεται σε μορφή που δεν περιέχει τριτοβάθμιο όρο: $\chi^4 + \alpha\chi^2 + \beta\chi + \gamma = (\chi^2 + \kappa\chi + \lambda) \cdot (\chi^2 - \kappa\chi + \mu)$

Για να βρούμε τους αριθμούς κ,λ,μ πρέπει να λύσουμε το σύστημα :

$$\begin{cases} \mu - \kappa^2\lambda = \alpha \\ \kappa(\mu - \lambda) = \beta \\ \lambda\mu = \gamma \end{cases} \Rightarrow \begin{cases} 2\mu = \kappa^2 + \alpha + \frac{\beta}{\kappa} \\ \\ 2\lambda = \kappa^2 + \alpha - \frac{\beta}{\kappa} \end{cases}$$

Αντικαθιστώντας στην τρίτη εξίσωση θα έχουμε :

$$\lambda\mu = \gamma \Leftrightarrow 4\lambda\mu = 4\gamma \Leftrightarrow (\kappa^2 + \alpha + \frac{\beta}{\kappa}) \cdot (\kappa^2 + \alpha - \frac{\beta}{\kappa}) = 4\gamma$$

$$(\kappa^3 + \alpha\kappa + \beta) \cdot (\kappa^3 + \alpha\kappa - \beta) = 4\gamma\kappa^2 \Leftrightarrow (\kappa^3 + \alpha\kappa)^2 - \beta^2 = 4\gamma\kappa^2$$

$$\kappa^6 + 2\alpha\kappa^4 + (\alpha^2 - 4\gamma)\kappa^2 - \beta = 0$$

Η εξίσωση είναι κυβική ως προς κ^2 και λύνεται με αντίστοιχο τρόπο.

Επίλυση με ριζικά – Η ομάδα Galois

Μετά την επιτυχία στη λύση τριτοβάθμιων και τεταρτοβάθμιων εξισώσεων όπως ήταν φυσικό η έρευνα στράφηκε μοιραία σε εξισώσεις πέμπτου ή ανώτερου βαθμού. Αρχικά αναζητήθηκαν τύποι που να δίνουν τις λύσεις και τέτοιων εξισώσεων , τύπους που να εκφράζουν τις λύσεις των εξισώσεων μέσω εξαγωγών ν-οστών ριζών και πράξεων ανάμεσα στους αριθμούς που προκύπτουν συναρτήσει βεβαίως των συντελεστών των αντίστοιχων εξισώσεων (όλοι οι τύποι δηλαδή μέχρι τετάρτου βαθμού). Η απαίτηση για την λύση μιας πολυωνυμικής εξίσωσης αναφέρετε στην μαθηματική ορολογία ως **μέθοδος επίλυσης με ριζικά**.

Το 1750 ο Euler προσπάθησε να αναγάγει μια πεμπτοβάθμια εξίσωση προσπάθησε να αναγάγει την πεμπτοβάθμια εξίσωση στη λύση μιας εξίσωσης τετάρτου βαθμού όμως απέτυχε όπως επίσης απέτυχε και η προσπάθεια του μαθηματικού **Lagrange** 30 έτη μετά. Αργότερα ο ιταλός ιατρός **Πάολο Ρουφίνι** έδωσε μια μη ολοκλήρωμένη απόδειξη του γεγονότος ότι η γενική εξίσωση πέμπτου βαθμού δεν μπορεί να λυθεί με ριζικά. Μια ανεξάρτητη ελλιπής απόδειξη του ίδιου γεγονότος δώθηκε από τον Νορβηγό μαθημηματικό **Νίλς Χέντρικ Άμπελ**. Λίγο αργότερα ο Γάλλος μαθηματικός **Εβαρίστ Γκαλουά** που σκοτώθηκε σε μια μονομαχία με πιστολιά σε ηλικία 21 ετών άφησε μετά τον θανατό του μια επιστημονική διαθήκη η οποία όταν τελικά ερμηνεύτηκε αποδείχτηκε ότι πρόσφερε κριτήρια για την δυνατότητα επίλυσης μιας αλγεβρικής εξίσωσης με ριζικά.

Έστω $P(x) = a^{v}x_{v} + a^{v-1}x_{v-1} + ... + a_1 x + a_0 = 0$ μια τυχαία εξίσωση βαθμού ν με τους συντελεστές $a_i \in F$

Ήδη από τον 18^{ο}αιώνα ο Karl Friedrich Gauss είχε αποδείξει ότι μια πολυωνυμική εξίσωση βαθμού ν έχει ακριβώς ν μιγαδικές ρίζες $\chi_1,\chi_2,\ldots,\chi_v$.

Θα θέλαμε να μάθουμε αν υπάρχουν τύποι που εκφράζουν τις λύσεις $\chi_1,\chi_2,\ldots,\chi_v$ συναρτήσει των συντελεστών $\alpha_0,\alpha_1,\ldots\alpha_v$ με τη χρήση ριζικών και των τεσσάρων αριθμητικών πράξεων.

Αν στο αρχικό σώμα F που ανήκουν οι συντελεστές βάλουμε τις ρίζες της εξίσωσης P(x)=0 και διευρύνουμε την εκτέλεση των πράξεων ανάμεσα στα στοιχεία του νέου αυτού συνόλου τότε προκύπτει ένα σώμα που περιέχει το F συμβολίζεται $F(P)=F(\chi_1,\chi_2,\ldots,\chi_v)$ και γενικά είναι γνήσιο υποσύνολο του □ .

Το μικρότερο δυνατό σώμα που ικανοποιεί τις παραπάνω απαιτήσεις το ονομάζουμε **σώμα ριζών** του πολυωνύμου P(X).

Επιλυσιμότητα ομαδων και επιλυσιμότητα με ριζικά

Όπως είδαμε στην προηγούμενη παράγραφο, μια εξίσωση επιλύεται με ριζικά αν και μόνο αν η ομάδα Galois της εξίσωσης είναι επιλύσιμη. Επειδή τώρα οι ομάδες Galois είναι υποομάδες των ομάδων μεταθέσεων S_n το εύλογο ερώτημα που τίθεται είναι κατά πόσο οι συμμετρικές ομάδες S_n είναι επιλύσιμες. Η ομάδα S_2 αποτελείται από τις μεταθέσεις $\sigma_1 = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}$ και $\sigma_2 = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$ και είναι προφανώς επιλύσιμη αφού $I \triangleleft S_2$. Το γεγονός ότι $[S_2 : I] = 2$ σημαίνει πως η δευτεροβάθμια εξίσωση λύνεται γενικά με χρήση τετραγωνικής ρίζας. Είδαμε επίσης στα προηγούμενα ότι και η ομάδα S_3 είναι επιλύσιμη αφού $\{I\} \triangleleft A_3 \triangleleft S_3$ και $[A_3: \{I\}] = 3$ $[S_3: A_3] = 2$. Αυτό σημαίνει πως η τριτοβάθμια εξίσωση λύνεται γενικά με χρήση τετραγωνικών και

κυβικών ριζών. Στην τέταρτη παράγραφο δείξαμε ότι και η τριτοβάθμια εξίσωση λύνεται με ριζικά. Ας δούμε τώρα το ίδιο πρόβλημα με έναν διαφορετικό τρόπο, μελετώντας την ομάδα S_4. Η ομάδα αυτή περιέχει τις 4! = 24 μεταθέσεις του συνόλου $I_4 = \{1, 2, 3, 4\}$. Αν σ είναι μια τέτοια μετάθεση τότε αυτή μπορεί να παρασταθεί όπως είδαμε με τον πίνακα: $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ \sigma(1) & \sigma(2) & \sigma(3) & \sigma(4) \end{pmatrix}$. Ορίζουμε ως πρόσημο ε(σ) της μετάθεσης τον αριθμό $\varepsilon(\sigma) = \prod_{i<j} \frac{i-j}{\sigma(i)-\sigma(j)}$ (6.1). Για παράδειγμα αν θεωρήσουμε τις μεταθέσεις $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$ και $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$ τότε θα έχουμε $\varepsilon(\sigma) = \frac{1-2}{4-3} \cdot \frac{1-3}{4-2} \cdot \frac{1-4}{4-1} \cdot \frac{2-3}{3-2} \cdot \frac{2-4}{3-1} \cdot \frac{3-4}{2-1} = +1$, ενώ $\varepsilon(\tau) = \frac{1-2}{4-1} \cdot \frac{1-3}{4-2} \cdot \frac{1-4}{4-3} \cdot \frac{2-3}{1-2} \cdot \frac{2-4}{1-3} \cdot \frac{3-4}{2-3} = -1$. Δεδομένου ότι τα σ(i) και σ(j) δεν είναι παρά κάποια από τα στοιχεία του I_4 γραμμένα με διαφορετική σειρά είναι σχεδόν φανερό ότι για τυχούσα μετάθεση σ θα είναι ε(σ) = ±1. Τις μεταθέσεις που έχουν πρόσημο +1 τις ονομάζουμε άρτιες μεταθέσεις, ενώ τις μεταθέσεις που έχουν πρόσημο -1 τις ονομάζουμε περιττές μεταθέσεις. Επειδή για μια μετάθεση σ μπορούμε να γράψουμε $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ \sigma(1) & \sigma(2) & \sigma(3) & \sigma(4) \end{pmatrix} = \begin{pmatrix} \tau(1) & \tau(2) & \tau(3) & \tau(4) \\ \sigma\tau(1) & \sigma\tau(2) & \sigma\tau(3) & \sigma\tau(4) \end{pmatrix}$ θα έχουμε $\varepsilon(\sigma)\varepsilon(\tau) = \prod_{i<j} \frac{i-j}{\sigma(i)-\sigma(j)} \prod_{i<j} \frac{i-j}{\tau(i)-\tau(j)} = \varepsilon(\sigma\tau)$. Αποδείξαμε δηλαδή ότι ε(στ) = ε(σ)ε(τ) (6.2). Επειδή η ταυτοτική μετάθεση είναι προφανώς άρτια από τον τύπο (6.2) θα έχουμε $+1 = \varepsilon(I) = \varepsilon(\sigma\sigma^{-1}) = \varepsilon(\sigma)\varepsilon(\sigma^{-1})$, πράγμα που σημαίνει ότι η αντίστροφη μιας άρτιας μετάθεσης είναι επίσης άρτια και η αντίστροφη μιας περιττής μετάθεσης είναι επίσης περιττή. Αν συμβολίσουμε με A_n το σύνολο των άρτιων μεταθέσεων και με Π_n το σύνολο των περιττών μεταθέσεων τότε $Sn = An \cup \Pi n$. (Αν και μιλούσαμε για την S_4, τα παραπάνω ισχύουν για κάθε ομάδα S_n). Αφού το γινόμενο δύο άρτιων είναι επίσης άρτια μετάθεση, και η αντίστροφη μιας άρτιας είναι επίσης άρτια είναι φανερό ότι το σύνολο A_n των άρτιων μεταθέσεων αποτελεί υποομάδα της S_n.

Μπορούμε να αποδείξουμε τώρα ότι οι άρτιες μεταθέσεις είναι όσες και οι περιττές:

Αν ρ είναι μια συγκεκριμένη περιττή μετάθεση και σ διατρέχει τις άρτιες μεταθέσεις, η ρσ διατρέχει τις περιττές μεταθέσεις. Είναι $\rho\sigma_1 \neq \rho\sigma_2$ όταν $\sigma_1 \neq \sigma_2$ γιατί αν $\rho\sigma_1 = \rho\sigma_2$ πολλαπλασιάζοντας τα δύο μέλη της ισότητας με ρ^{-1} προκύπτει $\rho^{-1}(\rho\sigma_1) = \rho^{-1}(\rho\sigma_2) \leftrightarrow \sigma_1 = \sigma_2$. Επίσης αν π είναι τυχούσα περιττή μετάθεση, τότε αυτή γράφεται στη μορφή $\pi = \rho(\rho^{-1}\pi)$ και η $\rho^{-1}\pi$ είναι άρτια αφού $\varepsilon(\rho^{-1}\pi) = \varepsilon(\rho^{-1})\varepsilon(\pi) = (-1)(+1) = +1$. Τα προηγούμενα λοιπόν δείχνουν ότι η απεικόνιση $f: A_n \to \Pi_n$ είναι ένα προς ένα και επί. Άρα το πλήθος των άρτιων μεταθέσεων θα είναι ίσο με το πλήθος των περιττών μεταθέσεων και μάλιστα ισχύει $|A_n| = n!/2$.

Ανακεφαλαιώνοντας, είδαμε ότι η ομάδα A_n των άρτιων μεταθέσεων είναι πάντοτε υποομάδα της συμμετρικής ομάδας S_n. Ο δείκτης της A_n στην S_n είναι $[Sn: An] = \frac{n!}{\frac{n!}{2}} = 2$. Αποδεικνύεται ότι η A_n είναι κανονική υποομάδα της S_n ώστε για κάθε φυσικό $n \geq 2$ ισχύει I $A_n \lhd S_n$, $[Sn: An] = 2$. (6.3)

Ας είναι α, β, γ…..ω r ≤ n στοιχεία του συνόλου I_n = {1,2,3…..n}. Τότε (α β γ ….. ω) θα συμβολίζει τη μετάθεση που απεικονίζει α → β, β → γ, …. , ω → α και κάθε άλλο στοιχείο του I_n στον εαυτό του. Η μετάθεση (α, β, γ…., ω) θα καλείται κύκλος μήκους r ή απλά r-κύκλος. Ειδικότερα ένας 2-κύκλος θα λέγεται αντιμετάθεση ή μετάβαση.

Παράδειγμα: η μετάθεση $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} = (1\ \ 2\ \ 3\ \ 4)$ είναι ένας 4-κύκλος. Το στοιχείο $r = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix} = (1\ 2\ \ 4)$ είναι ένας 3-κύκλος. Μπορούμε να διαπιστώσουμε ότι ένας ν-κύκλος είναι ένα στοιχείο της ομάδας μεταθέσεων με τάξη ν, δηλαδή σ^v = I. Έτσι για τους σ, τ θα έχουμε σ^4 = I και σ^3 = I. Μπορούμε να διαπιστώσουμε ότι κάθε μετάθεση σ, μπορεί να αναλυθεί σε γινόμενο αντιμεταθέσεων. Αν και η ανάλυση αυτή δεν είναι μοναδική το πλήθος των αντιμεταθέσεων στις οποίες μπορεί να αναλυθεί μια άρτια μετάθεση είναι πάντα άρτιος αριθμός, ενώ το πλήθος των αντιμεταθέσεων στις οποίες μπορεί να αναλυθεί μια περιττή μετάθεση είναι πάντοτε περιττός αριθμός. Έτσι π.χ. θα έχουμε $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix} = (1\ \ 2)(1\ \ 3)(1\ \ 4)(2\ \ 3) = (1\ \ 3)(1\ \ 4)$ και η σ είναι σίγουρα άρτια μετάθεση. Είναι εύκολο να δούμε ότι το σύνολο K = {I, (1 2)(3 4), (1 3)(2 4), (1 4)(2 3)} είναι μια κανονική υποομάδα του A_4. (Ομάδα τεσσάρων στοιχείων του Klein). Προφανώς και το σύνολο H = {I, (1 2)(3 4)} αποτελεί κανονική υποομάδα της K. Για την ομάδα S_4 συνεπώς παρατηρούμε ότι υπάρχει η εξής σειρά κανονικών υποομάδων της: S_4 ◁ K ◁ H ◁ I και [S_4 : K= 2, [K:H] = 12:4 = 3, [HÏ] = 2 (6.4). Άρα η ομάδα S_4 είναι επιλύσιμη και επομένως η γενική εξίσωση τετάρτου βαθμού είναι επιλύσιμη με ριζικά.

Ας δούμε τώρα πώς οι σχέσεις (6.4) μπορούν να μας οδηγήσουν στη λύση της εξίσωσης $\chi^4 + \alpha_1\chi^3 + \alpha_2\chi^2 + \alpha_3\chi + \alpha_4 = 0$ με $\alpha_1, \alpha_2, \alpha_3, \alpha_4 \in F$ (6.5)

Αν $\chi_1, \chi_2, \chi_3, \chi_4$ είναι οι ρίζες της (6.5) μέσα σε ένα σώμα διάσπασης της E, από τους τύπους του Vieta θα έχουμε:

$$\left.\begin{aligned} &\chi_1 + \chi_2 + \chi_3 + \chi_4 = -\alpha_1 \\ &\chi_1\chi_2 + \chi_1\chi_3 + \chi_1\chi_4 + \chi_2\chi_3 + \chi_2\chi_4 + \chi_3\chi_4 = \alpha_2 \\ &\chi_1\chi_2\chi_3 + \chi_1\chi_3\chi_4 + \chi_1\chi_2\chi_4 + \chi_2\chi_3\chi_4 = -\alpha_3 \\ &\chi_1\,\chi_2\,\chi_3\,\chi_4 = \alpha_4 \end{aligned}\right\} \quad (6.6)$$

Αν G είναι μια ομάδα θα συμβολίζουμε με [G] το σύνολο όλων των αλγεβρικών παραστάσεων P ($\chi_1, \chi_2, \chi_3, \chi_4$) που μένουν αναλλοίωτες όταν δράσουν πάνω τους τα

στοιχεία της ομάδας G (παραστάσεις συμμετρικές ως προς την G). Είναι φανερό ότι $\chi_1, \chi_2, \chi_3, \chi_4 \in [I]$. θα προσπαθήσουμε να εκφράσουμε τα $\chi_1, \chi_2, \chi_3, \chi_4$ συναρτήσει στοιχείων του [H]. Η συνθήκη $I \triangleleft H$ $[H:I] = 2$ μας βεβαιώνει ότι αυτό είναι πάντοτε εφικτό στη χειρότερη περίπτωση με χρήση τετραγωνικών ριζών. Από τις παραστάσεις

$$\chi_1 + \chi_2 - \chi_3 - \chi_4 = \beta_1$$

$$\chi_1 - \chi_2 + \chi_3 - \chi_4 = \beta_2$$

$$\chi_1 - \chi_2 - \chi_3 + \chi_4 = \beta_3$$

μόνο η β_1 ανήκει στο [H] όμως τα τετράγωνά τους προφανώς ανήκουν στο [H]. θεωρούμε το σύστημα:

$$\left.\begin{aligned} \chi_1 + \chi_2 - \chi_3 - \chi_4 &= \beta_1 \\ \chi_1 - \chi_2 + \chi_3 - \chi_4 &= \beta_2 \\ \chi_1 - \chi_2 - \chi_3 + \chi_4 &= \beta_3 \\ \chi_1 + \chi_2 + \chi_3 + \chi_4 &= -\alpha_1. \end{aligned}\right\} \qquad (6.7)$$

Με πρόσθεση κατά μέλη των εξισώσεών του προκύπτει $\chi_1 = \frac{1}{4}(\beta_1+\beta_2+\beta_3+\alpha_1) = \frac{1}{4}\sqrt{\beta_1^2}+\sqrt{\beta_2^2}+\sqrt{\beta_3^2}-\alpha_1)$ (6.8).

Όπως βλέπουμε το χ_1 και παρόμοια και οι υπόλοιπες ρίζες εκφράζονται όντως από τα στοιχεία του [H] με χρήση τετραγωνικών ριζών.

Το επόμενο βήμα είναι να εκφράσουμε τα στοιχεία του [H] από τα στοιχεία του K. Υπολογίζοντας τα $\beta_1^2, \beta_2^2, \beta_3^2$ με βάση τους τύπους (6.6) και (6.7) βρίσκουμε:

$$\left.\begin{aligned} \beta_1^2 &= \alpha_1^2 - 4\alpha_2 + 4\eta_1, \text{ όπου } \eta_1 = \chi_1\chi_2 + \chi_3\chi_4 \\ \beta_2^2 &= \alpha_1^2 - 4\alpha_2 + 4^{\eta}{}_2, \text{ όπου } \eta_2 = \chi_1\chi_3 + \chi_2\chi_4 \\ \beta_3^2 &= \alpha_1^2 - 4\alpha_2 + 4^{\eta}{}_3, \text{ όπου } \eta_3 = \chi_1\chi_4 + \chi_3\chi_2 \end{aligned}\right\} (6.8)$$

Δεδομένου τώρα ότι οι παραστάσεις η_1, η_2, η_3 ανήκουν στο K βρίσκουμε π.χ. ότι: $\chi_1 = \frac{1}{4}(\sqrt{\alpha_1^2 - 4\alpha_2 + 4\eta_1} + \sqrt{\alpha_1^2 - 4\alpha_2 + 4\eta_2} + \sqrt{\alpha_1^2 - 4\alpha_2 + 4\eta_3} - \alpha_1)$.

Πρέπει στη συνέχεια να εκφράσουμε τα η_1, η_2, η_3 συναρτήσει των στοιχείων του $[A_1]$. Παρατηρούμε ότι:

$$\begin{cases} \eta_1 + \eta_2 + \eta_3 = \alpha_2 \\ \eta_1\eta_2 + \eta_1\eta_3 + \eta_2\eta_3 = \alpha_1\alpha_3 - 4\alpha_4 \\ \eta_1\eta_2\eta_3 = \alpha_4\alpha_1^2 + \alpha_3^2 - 4\alpha_4\alpha_2 \end{cases}$$

Επομένως οι αριθμοί η_1, η_2, η_3 μπορούν να υπολογιστούν ως ρίζες της κυβικής εξίσωσης: $\psi^3 - \alpha_2\psi^2 + (\alpha_1\alpha_3 - 4\alpha_4)\psi - (\alpha_4\alpha_1^2 + \alpha_3^2 - 4\alpha_4\alpha_2) = 0$ (6.9)

Ακολουθώντας βήματα προηγούμενης παραγράφου διαπιστώνουμε πως τα η_1,η_2,η_3 εκφράζονται τελικά από τα στοιχεία του $[S_4]$ συναρτήσει των $\alpha_1,\alpha_2,\alpha_3,\alpha_4$ και χρήση τετραγωνικών και κυβικών ριζών.

Μέχρι στιγμής δείξαμε ότι οι ομάδες S_2,S_3,S_4 είναι επιλύσιμες δυστυχώς όμως για $n\geq 5$ δεν είναι επιλύσιμες δηλ. δεν μπορούν να λυθούν με ριζικά βέβαια αυτό δεν σημαίνει ότι όλες ανώτερου του πέμπτου βαθμού δεν επιλύονται με ριζικά ενδεχομένως μια εξίσωση να έχει ομάδα Galois κάποια υποομάδα της S_n η οποία να είναι επιλύσιμη.

Αν επιθυμούμε να δώσουμε μια απόδειξη για τη μη επιλυσιμότητα της S_n , $n\geq 5$ θα πρέπει να δούμε κάποια επιπλέον στοιχεία από την θεωρία ομάδων. Αν G είναι μια ομάδα με πεπερασμένο πλήθος στοιχείων ν, ο αριθμός ν καλείται **τάξη της ομάδας** και συμβολίζεται $|G| = \nu$. Αν $\alpha \in G$ τότε οι δυνάμεις $\alpha^0,\alpha^1,\alpha^2,....,\alpha^\nu,\alpha^{\nu+1},.....$ δεν μπορεί να είναι όλες διαφορετικές μεταξύ τους όταν η ομάδα έχει τάξη ν. Έτσι θα υπάρχουν στοιχεία κ,μ με κ<μ έτσι ώστε $\alpha^\mu=\alpha^\kappa$

Πολλαπλασιάζοντας την τελευταία ισότητα επί α^{-1} , κ φορές διαδοχικά βρίσκουμε ότι $\alpha^{\mu-\kappa}=I$, όπου I το ουδέτερο στοιχείο της G. Επομένως, υπάρχει φυσικός αριθμός $n\geq 1$ ώστε $\alpha n=I$. Τον ελάχιστο τέτοιο φυσικό αριθμό n τον ονομάζουμε τάξη του στοιχείου α (Αν δεν υπάρχει τότε λέμε ότι το στοιχείο α είναι μηδενικής τάξεως).

Αν α είναι στοιχείο μιας ομάδας G τότε το σύνολο $\{\alpha^\kappa/\kappa=0,1,2,3,\ldots\}$ που αποτελείται από τις δυνάμεις του α αποτελεί ουσιαστικά μια υποομάδα της G. Αυτή την ομάδα την λέμε κυκλική παραγόμενη από το στοιχείο α και την συμβολίζουμε ως (α). δηλ. είναι $(\alpha)=\{\alpha^\kappa/\kappa=0,1,2,3,\ldots\}$. Κάθε κυκλική ομάδα είναι πάντοντε αντιμεταθετική.

Έστω H μια υποομάδα της G, μέσα στην G μπορούμε να ορίσουμε μια σχέση ισοδυναμίας ως εξής: $\alpha \square \beta \Leftrightarrow \alpha^{-1}\beta \in H \Leftrightarrow \beta \in \alpha H$. Η σχέση αυτή είναι μια σχέση ισοδυναμίας στο G,

δηλ. είναι ανακλαστική $\alpha \square \alpha$

συμμετρική $\alpha \square \beta \Leftrightarrow \beta \square \alpha$

και μεταβατική $\alpha \square \beta$ και $\beta \square \gamma \Rightarrow \alpha \square \gamma$

Η βασική λειτουργία μιας σχέσης ισοδυναμίας στο G είναι ότι διαμερίζει το σύνολο αυτό σε υποσύνολα που καλούνται κλάσεις ισοδυναμίας τα οποία είναι ανα δύο ξένα μεταξύ τους και η ενωσή τους ισούται με G. Αν συμβολίσουμε με <α> την κλάση ισοδυναμίας του α δηλ. το σύνολο όλων των στοιχείων της G που είναι ισοδύναμα με το α είναι φανερό τότε ότι <α>=αH. Το δε σύνολο όλων των κλάσεων ισοδυναμίας καλείται σύνολο πηλίκο της σχέσης και θα το συμβολίσουμε με G/H. Τα στοιχεία του G/H τα ονομάζουμε αριστερές κλάσεις της H στη G.

Έχουμε λοιπόν $G/H=\{\alpha H/\ \alpha \in G\ \}$ με

$$G = \bigcup_{<\alpha>\in G/H} <\alpha>$$

$$<\alpha> \cap <b> = \varnothing \quad \forall\ <\alpha>,<b> \in G/H \quad \text{με} \ <\alpha> \neq <b>$$

Είναι πολύ δύσκολο να δούμε ότι όλες οι αριστερές κλάσεις έχουν το ίδιο πλήθος στοιχείων με την υποομάδα H. Από τις παραπάνω σχέσεις εξάγεται πως :

$$|G| = \sum_{\alpha\in G/H} |<\alpha>| = \sum_{\alpha\in G/H} |H| = |G/H|\cdot|H|$$

δηλ. $|G| = |G/H|\cdot|H|$ **(θεώρημα Lagrange)**

Ο τύπος αυτός μας δείχνει επίσης πως η τάξη μιας υποομάδας H της ομάδας G διαιρεί την τάξη της ομάδας. Τώρα αφού η τάξη ενός στοιχείου α ισούται με την τάξη της κυκλικής ομάδας (α) που παράγεται από το α θα ισχύει ότι και η τάξη ενός στοιχείου πάντοτε διαιρεί την τάξη της ομάδας. Έτσι αν η τάξη του α είναι ν και η τάξη της ομάδας είναι μ θα έχουμε μ=νκ για κάποιο θετικό ακέραιο κ. Τότε όμως $\alpha^{\mu}=\alpha^{\nu\kappa}=(\alpha^{\nu})^{\kappa}=I^{\kappa}=I$ που σημαίνει ότι κάθε στοιχείο μιας ομάδας υψωμένος στην τάξη της ομάδας θα μου δίνει πάντοτε το ουδέτερο στοιχείο της ομάδας.

Αν η τάξη μιας ομάδας G είναι ο πρώτος αριθμός ρ τότε η ομάδα είναι κυκλική. Όντως, αν ν η τάξη ενός στοιχείου α της $G \neq I$ τότε θα πρέπει το ν να διαιρεί τον ρ. Αφού όμως ο ρ είναι πρώτος θα πρέπει $\nu=\rho \Rightarrow G=(\alpha)$.

Αν $A, B \subseteq G$ το γινόμενο τους ορίζεται ως $AB=\{\ \alpha\beta\ /\ \alpha \in A \ \text{ και } \ \beta \in B\ \}$. Βεβαίως πάντα ισχύει $AB \subset G$.

Αν η ομάδα δεν είναι αντιμεταθετική τότε AB≠BA. Αν τα A, B είναι υποομάδες της G τότε το γινόμενο AB δεν είναι υποομάδα της.
Είχαμε δει ότι το σύνολο πηλίκο $G/H=\{\alpha H/\alpha \in G\}$. Κάθε κλάση αH είναι υποσύνολο της G και έτσι μπορεί να οριστεί το γινόμενο μεταξύ δύο κλάσεων (αH), (βH). Αυτό το γινόμενο είναι μεν υποσύνολο της G αλλά δεν ανήκει στο G/H. Παρατηρούμε όμως ότι να ισχύει αH=Hα για κάθε $\alpha \in G$ τότε για το γινόμενο των δύο κλάσεων θα έχουμε :

(αH)(βH)=α(Hβ)H=α(βH)H=(αβH)H=αβH δηλ. το γινόμενο των κλάσεων αH ,βH είναι επίσης η κλάση αβH με πιο απλά λόγια το G/H είναι κλειστό ως προς τον

πολλαπλασιασμό των πράξεων. Το στοιχείο αυτό είναι μείζονος σημασίας διότι ο πολλαπλασιαμός των κλάσεων ικανοποιεί και τα υπόλοιπα αξιώματα του ορισμού μιας ομάδας. (Στα μαθηματικά, **ομάδα** είναι ένα σύνολο στοιχείων μαζί με μία πράξη, η οποία συνδυάζει δύο στοιχεία του συνόλου για να σχηματίσουν ένα τρίτο στοιχείο που ανήκει επίσης στο σύνολο, ικανοποιώντας ταυτόχρονα τέσσερις συνθήκες που ονομάζονται αξιώματα της ομάδας και αναφορικά είναι η κλειστότητα, η προσεταιριστική ιδιότητα, η ταυτότητα και η αντιστρεψιμότητα).

Συγκεκριμένα είναι προσεταιριστικός: $(\alpha H)[(\beta H)(\gamma H)]=[(\alpha H)(\beta H)](\gamma H)=\alpha\beta\gamma H$

Έχει ουδέτερο στοιχείο που είναι η κλάση H: $(\alpha H)H=\alpha H=H(\alpha H)$

Υπάρχει αντίστροφο στοιχείο: $(\alpha H)^{-1}=\alpha^{-1}H$

Το ζήτημα είναι ότι δεν ισχύει πάντα η ισότητα $\alpha H=H\alpha \ \forall \alpha \in G$. Στην περίπτωση που η συνθήκη αυτή ικανοποιείται η ομάδα H λέμε ότι είναι κανονική υποομάδα της G και το γεγονός αυτό το συμβολίζουμε $H \lhd G$.

(Πηγή: Εισαγωγή στην θεωρία Galois , Κασσαπίδης Γεώργιος)

3.4 Θεμελιώδες θεώρημα θεωρίας Galois

Έστω η επέκταση E/F , G =Gal{ E/F } , το σύνολο των υποομάδων της G. Λέμε ότι η επέκταση E/F είναι επέκταση Galois πάνω από το F αν E σώμα ανάλυσης ενός διαχωρίσιμου πολυωνύμου $f(x) \subset F[x]$. Συμβολίζουμε με P το σύνολο των επεκτάσεων του F που είναι υποσώματα του E.

Θεώρημα: Έστω E επέκταση Galois πάνω από το F , G =Gal{ E/F } . Υπάρχει μια αμφιμονοσήμαντη αντιστοιχία ανάμεσα στα στοιχεία του συνόλου P των υποσωμάτων του E που είναι επεκτάσεις του F και στα στοιχεία του συνόλου G των υποομάδων G.

Συγκεκριμένα , η συνάρτηση Gal{ E/F }: P→G , B⇔ Gal{ E/B }

Είναι ένα προς ένα με αντίστροφη

E^{-}: G→P , H⇔E^{H}

Ισχύουν οι ιδιότητες:

- $|B:F|$ = |G:Gal (E/B) | και |G:H| =|E^{H}:F|
- $E^{\text{Gal (E/B)}}$ – B & Gal (E/E^{H}) – H
- B είναι επέκταση Galois πάνω από το F αν και μόνο αν Gal (E/B) $\triangleleft$ G

Το πολυώνυμο $x^3 - 2$

Αρχικά μελετάμε το κανονικό πολυώνυμο f(x)=x^3-2 και βρίσκουμε τους ανάγωγους παράγοντες του στο Q(x),R(x),C(x).

Βρίσκουμε τις ρίζες στο και παρατηρούμε ότι το b= $\sqrt[3]{2}$ είναι μια ρίζα της f(x) οπότε το πολυώνυμο $x - \sqrt[3]{2}$ διαιρεί το πολυώνυμο f(x)=x^3-2 και έτσι σύμφωνα με τον ευκλείδειο αλγόριθμο διαίρεσης πολυωνύμων βρίσκουμε ότι $f(x)=x^3 - 2 = (x - \sqrt[3]{2}) \cdot (x^2 + \sqrt[3]{2}x + \sqrt[3]{4})$

Δηλαδή

$f(x) = (x-b)(x^2 + bx + b^2)$ όπου $x^2 + bx + b^2 = p(x)$

Χρησιμοποιώντας τον τύπο για την εύρεση ριζών μιας δευτεροβάθμιας εξίσωσης βρίσκουμε ότι οι άλλες δύο ρίζες του πολυωνύμου είναι : $\sqrt[3]{2}(-\frac{1}{2}\pm\frac{i\sqrt{3}}{2})$

Θέτουμε τώρα $\omega=-\frac{1}{2}+\frac{i\sqrt{3}}{2}$

και παρατηρούμε πως $\begin{cases}\omega^0-\omega^3-e^{2\pi i}-1\\ \omega-e^{2\pi i/3}-\cos(\frac{2\pi}{3})+i\sin(\frac{2\pi}{3})\\ \omega^2-\frac{1}{2}-\frac{i\sqrt{3}}{2}\end{cases}$

Συνεπώς , μπορούμε να γράψουμε τις 3 ρίζες της εξίσωσης x^3-2 στο σύνολο των μιγαδικών αριθμών ως εξής:

(α) Καμία από τις ρίζες του f(x) δεν ανήκει στο Q πράγμα που σημαίνει πως υπάρχει πολυώνυμο A βαθμού στο Q(x) που να διαιρεί το f(x) οπότε f(x) ανάγωγο του Q(x).

(β) Εφόσον το b και οι συντελεστές του q(x) ανήκουν στο R ισχύει τότε ότι f(x)=(x-b)·q(x) στον R(x). Οι ρίζες του Q(x) δεν ανήκουν στον R και επομένως q(x) είναι ανάγωγο στον R(x). Στον δακτύλιο R(x) η ανάλυση του f(x) σε ανάγωγους παράγοντες θα είναι το γινόμενο f(x)=(x-b)·q(x)

(γ) Η ανάλυση του f(x) σε ανάγωγους παράγοντες στο □(x) είναι το γινόμενο f(x)=(x-b)·(x-ωb)·(x-ω^2 b)

Οπότε , συμπεραίνουμε τα εξής:

1) Υπάρχει $b\in K$ έτσι ώστε f(b)=0 αν και μόνο αν f(x)=(x-b)·q(x) όπου $q(x)b\in K[x]$

2) Αν deg f(x)=1 ⇔ τότε f(x) ανάγωγο

3) Αν deg f(x)=2,3 ⇔ τότε f(x) ανάγωγο αν και μόνο αν f(x) δεν έχει ρίζες στο K

4) Αν $K\subset F$ όπου το F είναι σώμα και f(x) ανάγωγο στο F(x) τότε f(x) ανάγωγο στο K(x)

Πηγή: Σημείωσεις μαθήματος «Θεωρία Galois» των Θεοδώρα Θεοχάρη Αποστολίδη και Χαρά Χαραλάμπους Νοέμβριος 2014

Δεύτερο παράδειγμα

Έστω $f(x)=x^4-2\in Q$

E=Q(b,i) όπου $b=\sqrt[4]{2}$

Οι ρίζες του f(x) είναι $\{\pm b, \pm ib\}$ και E επέκταση Galois πάνω από το Q. Παρατηρούμε ότι μια βάση του E ως προς το Q είναι το σύνολο $\{1, b, b^2, b^3, i, ib, ib^2, ib^3\}$

Έστω G=Gal(E/Q) όπου ισχύει $G \approx D_s$ και τα στοιχεία της G καθορίζονται από τις απεικονίσεις b, i όπως φαίνεται από τον παρακάτω πίνακα:

b	b	b	-b	-b	ib	ib	-ib	-ib
i	i	-i	i	-i	i	-i	i	-i
	σ_o	σ_1	σ_2	σ_3	σ_4	σ_5	σ_6	σ_7

Υπάρχουν 5 ακριβώς στοιχεία στην G με τάξη 2 και 5 υποομάδες επίσης με τάξη 2. Επιπλέον, το σ_4 έχει τάξη 4 άρα η κυκλική ομάδα $< \sigma_4 >$ έχει και αυτή τάξη 4. Η G Έχει άλλες δύο υποομάδες με τάξη 4 και πιο συγκεκριμένα οι γνήσιες μη τετριμμένες υποομάδες της G είναι:

I. $H_1 = < \sigma_4 > = \{ \sigma_0, \sigma_4, \sigma_2 = (\sigma_4)^2, \sigma_6 = (\sigma_4)^3 \}$

II. $H_2 = \{ \sigma_0, \sigma_2, \sigma_1, \sigma_3 \}$

III. $H_3 = \{ \sigma_0, \sigma_2, \sigma_5, \sigma_7 \}$

IV. $< \sigma_3 > = \{ id_E, \sigma_3 \}$

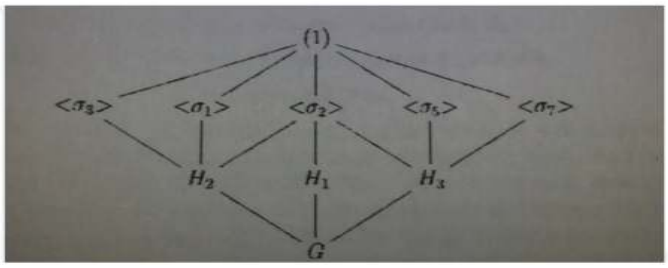
V. $< \sigma_1 > = \{ id_E, \sigma_1 \}$

VI. $< \sigma_2 > = \{ id_E, \sigma_2 \}$

VII. $< \sigma_5 > = \{ id_E, \sigma_5 \}$

VIII. $< \sigma_7 > = \{ id_E, \sigma_7 \}$

Διάγραμμα υποομάδων



Η μόνη κανονική υποομάδα τάξης 2 είναι η $< \sigma_2>$. Οι 3 υποομάδες τάξης 4 είναι κανονικές. Για κάθε υποομάδα της G θα υπολογίσουμε τα αντίστοιχα ενδιάμεσα σώματα. Θα ξεκινήσουμε με την ομαδα $< \sigma_3>$. Έστω ότι ανήκει στο Ε όπου:

$y = a_0 + a_1 b + a_2 b^2 + a_3 b^3 + a_4 i + a_5 ib - a_6 ib^2 + a_7 ib^3$

επειδή $\alpha_i \in Q$ έπεται ότι:

$<\sigma_3(y) >= a_0 + a_1 b - a_2 b^2 - a_3 b^3 - a_4 i + a_5 ib + a_6 ib^2 - a_7 ib^3$

θα ισχύει $\sigma_3(y) - y$ αν και μόνο αν

$y=a_0 + a_1 b(1+i) - a_3 b^3(1-i) + a_6 ib^2$

Άρα $E^{<\sigma 3>}=Q(b(1-i),b^3(1-i),ib^2)$

Και εφόσον:

$(b(1+i))^2=2ib^2$

$(b(1+i))^3=-2b^3(1-i)$

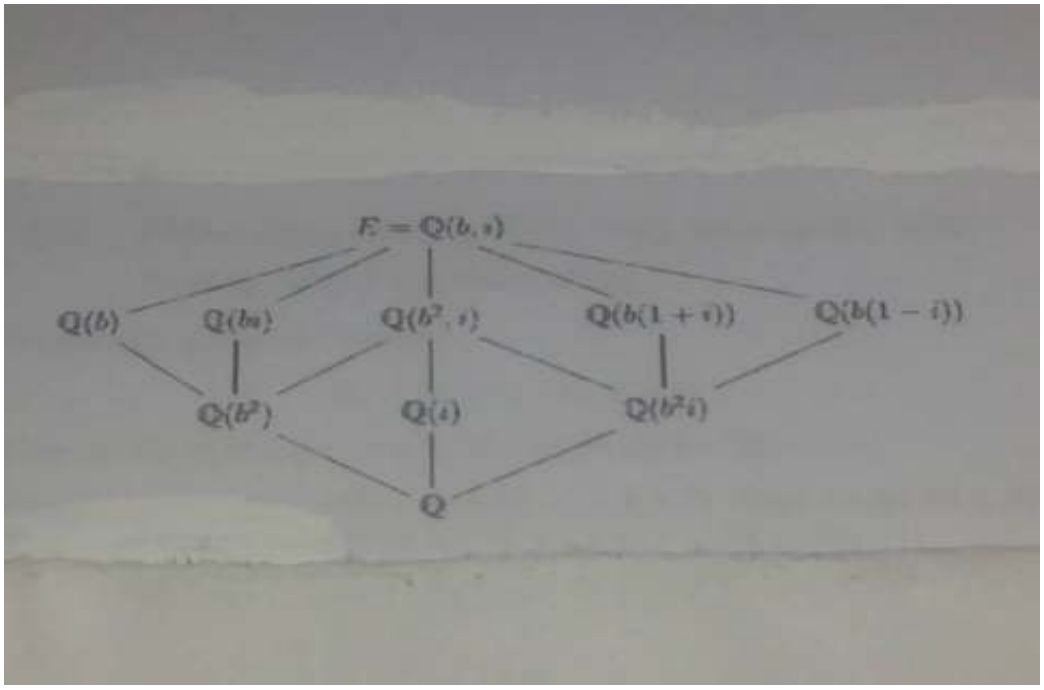
Θα έχουμε ότι : $E^{<\sigma_3>} = Q(b(1+i))$

Στην συνέχεια θα βρούμε το σώμα του $E^{<\sigma_2>}$. Στην περίπτωση αυτή παρατηρούμε ότι $[G: < \sigma_2>]=4$

Αφού $\sigma_2(i)=i$ & $\sigma_2(b^2)=\sigma_2(b)^2=(-b)^2=b^2$ έπεται ότι $Q(b^2,i) \subset E^{<\sigma_2>}$

Αφού $Q \subseteq Q(i) \subseteq Q(i,b^2) \subseteq E$ έπεται ότι $[Q(I,b^2):Q]=4$

Επομένως $E^{<\sigma_2>} = Q(i,b^2)$. Με τον ίδιο τρόπο βρίσκουμε και τα άλλα ενδιάμεσα σώματα του Ε και έτσι προκύπτει το παρακάτω διάγραμμα για ενδιάμεσα σώματα:



Τέλος παρατηρούμε ότι:

- $B_2=Q(b^2)$ είναι σώμα ανάλυσης του x^2-2 πάνω από το Q & $Gal(E/B_2)\approx H_2$
- $B_1=Q(i)$ είναι σώμα ανάλυσης του x^2+1 πάνω από το Q & $Gal(E/B_1)\approx H_1$
- $B_3=Q(b^2i)$ είναι σώμα ανάλυσης του x^2+2 πάνω από το Q & $Gal(E/B_3)\approx H_3$
- $B_4=Q(b^2,i)$ είναι σώμα ανάλυσης του $(x^2-b)\cdot(x^2-1)$ πάνω από το Q & $Gal(E/B_4)\approx <\sigma_2>$.

Τρίτο παράδειγμα

Έστω η εξίσωση έκτου βαθμού $f(x)=(x^2-x+1)^3-\alpha(x^2-x)=0$. Την εξίσωση τη γράφουμε με δυο διαφορετικούς τρόπους

$$(x+\frac{1}{x}-1)^3-\alpha(x+\frac{1}{x}-2)=0 \quad (\alpha)$$

$$[x(1-x)+1]^3-\alpha[x(1-x)]^2=0 \quad (\beta)$$

Από την (α) βλέπουμε ότι αν x ρίζα της εξίσωσης τότε και η 1/x είναι ρίζα και από τη (β) προκύπτει ότι και η 1-x είναι επίσης ρίζα. Συνεπώς αν θ ρίζα της εξίσωσης τότε και οι $\frac{1}{\theta}, 1-\theta, \frac{1}{1-\theta}, 1-\frac{1}{\theta}=\frac{\theta-1}{\theta}, \frac{\theta}{\theta-1}$

είναι επίσης ρίζες. Μπορούμε να επιλέξουμε τον αριθμό α ώστε όλες οι παραπάνω λύσεις να είναι διαφορετικές μεταξύ τους.

Το σώμα ριζών του πολυωνύμου f(x) είναι το $E = Q(\alpha,\theta,1/\theta,1-\theta,\frac{1}{1-\theta},\frac{\theta-1}{\theta},\frac{\theta}{\theta-1})$

Η ομάδα Galois G(f) του f(x) αποτελείται από τους αυτομορφισμούς του E που αφήνουν σημειακά αναλλοίωτο το σώμα Q(α) και επειδή ο περιορισμός ενός τέτοιου αυτομορφισμού πάνω στο σύνολο $A = \{\alpha,\theta,1/\theta,1-\theta,\frac{1}{1-\theta},\frac{\theta-1}{\theta},\frac{\theta}{\theta-1}\}$ των ριζών του πολυωνύμου f(x) αποτελεί ουσιαστικά μια μετάθεση του A. Αν $\sigma \in G(f)$ τότε η τιμή σ(θ) καθορίζει πλήρως τον σ και υπάρχουν έξι διαφορετικοί τρόποι για να οριστεί το σ(θ).

Πιο συγκεκριμένα : $\sigma(\theta) = \begin{pmatrix} \theta \\ \frac{1}{\theta} \\ 1-\theta \\ \frac{1}{1-\theta} \\ \frac{\theta-1}{\theta} \\ \frac{\theta}{\theta-1} \end{pmatrix}$

Δεν είναι δύσκολο να διαπιστώσουμε πως $G(f)=S_3$. Όπως βλέπουμε η συγκεκριμένη ομάδα Galois είναι γνήσια υποομάδα της S_6 . Το αξιοσημείωτο είναι πως ενώ δεν γνωρίζουμε τις ρίζες του f(x) η ομάδα Γκαλουά μας είναι απολύτως γνωστή.

Η αναγκαία και ικανή συνθήκη που βρήκε ο Γκαλουά για να είναι μια πολυωνυμική εξίσωση επιλύσιμη με ριζικά είναι η συνθήκη η αντίστοιχη ομάδα Galois να είναι επιλύσιμη.

Επομένως, μπορούμε να πούμε πως μια ομάδα G είναι επιλύσιμη αν υπάρχει μια ακολουθία υποομάδων της τέτοια ώστε $G>G_1>G_2>\ldots>G_r=\{I\}$ όπου {I} η τετριμμένη υποομάδα της G που αποτελείται μόνο από το ουδέτερο στοιχείο και στην οποία ακολουθία κάθε ομάδα είναι κανονική υποομάδα της προηγούμενης με δείκτη πρώτο αριθμό.

Η ομάδα Galois

Παρακάτω θα εκθέσουμε μια αναλογία που συσχετίζει τις συμμετρίες των πολυγώνων του επιπέδου με κάποιες αντίστοιχες αλγεβρικές έννοιες, παρόλο που ορισμένες από αυτές δεν έχουν ακόμα ορισθεί

πολύγωνο P	πολυώνυμο $f(x) \in F[x]$
επίπεδο	σώμα διάσπασης E του f(x)
$vert(P)=\{u_1,...,u_v\}$	θέσεις μηδενισμού $\{\alpha_1,...,\alpha_v\}$
γραμμικός μετασχηματισμός	αυτομορφισμός του E
ορθογώνιος μετασχηματισμός	αυτομορφισμός του E που διατηρεί το σώμα F
Σ(P)	ομάδα Galois Gal(f)=Gal(E/F)
κανονικό πολύγωνο	ανάγωγο πολυώνυμο

ΒΙΒΛΙΟΓΡΑΦΙΑ

Ελληνόγλωσση

Στυλιανός Ανδρεαδάκης (1993) *Θεωρία Galois.* Εκδόσεις Συμμετρία.

John B. Fraleigh (1996) *Εισαγωγή στην Άλγεβρα*. Δεύτερη έκδοση. Ηράκλειο: Πανεπιστημιακές Εκδόσεις Κρήτης.

Joseph Rotman (2000) *Θεωρία Galois*. Leader Books.

Ξενόγλωσση

Emil Artin (1998). *Galois Theory.* Dover Publications. (Reprinting of second revised edition of 1944, The University of Notre Dame Press).

Girolamo Cardano. Ars Magna, or the Rules of Algebra. Dover Publications, 1993.

Harold M. Edwards (1984). *Galois Theory.* Springer-Verlag. (Galois' original paper, with extensive background and commentary.)

Ian Stewart (2004) *Galois Theory.* 3rd Edition. Εκδόσεις Τραύλος

Janelidze G., Borceux Francis (2001). *Galois theories.* Cambridge University Press.

Jörg Bewersdorff (2006). *Galois Theory for Beginners: A Historical Perspective.* American Mathematical Society.

Joseph Rotman (1998). *Galois Theory* (2nd edition). Springer.

Lang Serge (1994). *Algebraic Number Theory.* Berlin, New York: Springer-Verlag.

Marcus du Sautoy (2004). *Θεωρία Ομάδων.* Εκδόσεις Τραύλος

Michael Artin (1991) *Algebra.* Prentice Hall.

Patrick Morandi (1996). *Field and Galois Theory.* [online] Graduate Texts in Mathematics, 167. Springer

Pop Florian (2001). *(Some) New Trends in Galois Theory and Arithmetic.*

Steven Roman (2005) *Field Theory.* [online] Graduate Texts in Mathematics, 158. 2nd Edition. Springer.

Völklein Helmut (1996). *Groups as Galois groups: an introduction.* Cambridge University Press.

Ιντερνετική

https://el.wikipedia.org/wiki/%CE%95%CE%B2%CE%B1%CF%81%CE%AF%CF%83%CF%84_%CE%93%CE%BA%CE%B1%CE%BB%CE%BF%CF%85%CE%AC

http://www-history.mcs.st-andrews.ac.uk/Biographies/Galois.html

https://galois.com/