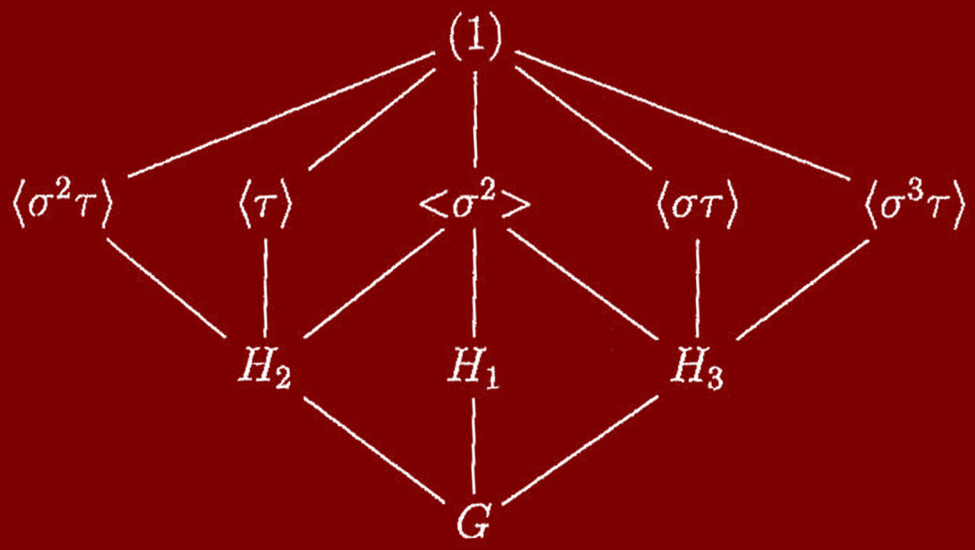
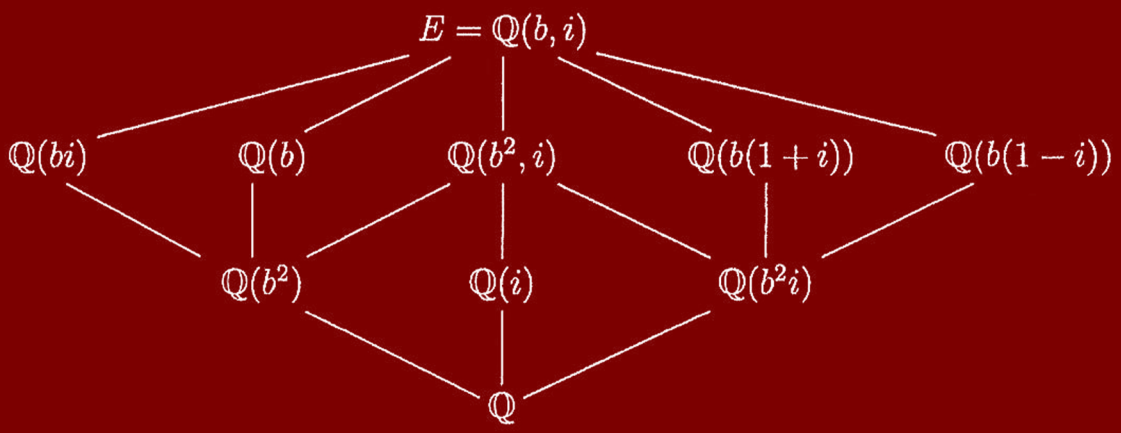
Θεοδώρα
Θεοχάρη - Αποστολίδη

Χαρά
Χαραλάμπους

ΘΕΩΡΙΑ GALOIS





Θεωρία Galois

Συγγραφή
Θεοδώρα Θεοχάρη-Αποστολίδη
Χαρά Χαραλάμπους

Κριτικός Αναγνώστης
Αριστείδης Κοντογεώργης

Συντελεστές Έκδοσης
ΓΛΩΣΣΙΚΗ ΕΠΙΜΕΛΕΙΑ : Θεοδώρα Θεοχάρη-Αποστολίδη
ΓΡΑΦΙΣΤΙΚΗ ΕΠΙΜΕΛΕΙΑ : Χαρά Χαραλάμπους
ΤΕΧΝΙΚΗ ΕΠΕΞΕΡΓΑΣΙΑ : Χαρά Χαραλάμπους
ΜΕΤΑΤΡΟΠΗ ΣΕ EPUB: Ιωάννης Καρύδης

ISBN: 978-960-603-208-0

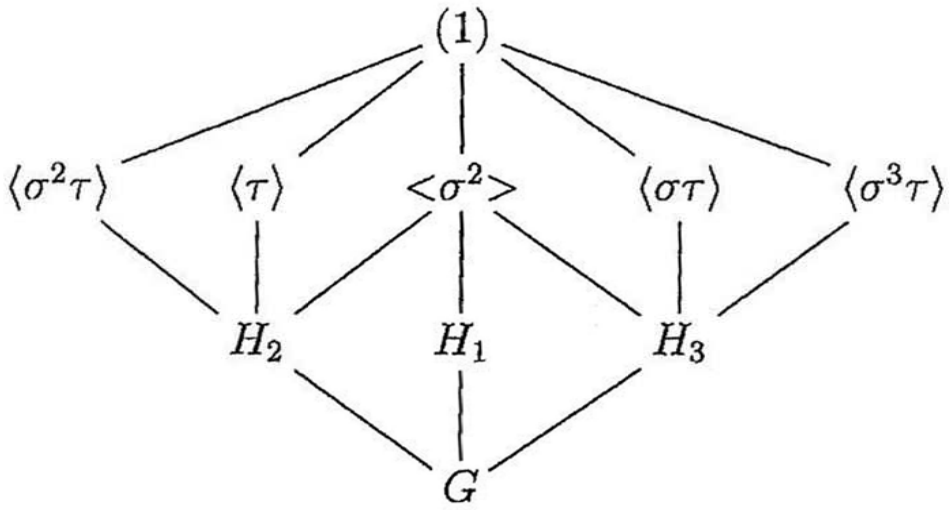
Σύνδεσμος Ελληνικών Ακαδημαϊκών Βιβλιοθηκών
Εθνικό Μετσόβιο Πολυτεχνείο
Ηρώων Πολυτεχνείου 9, 15780 Ζωγράφου

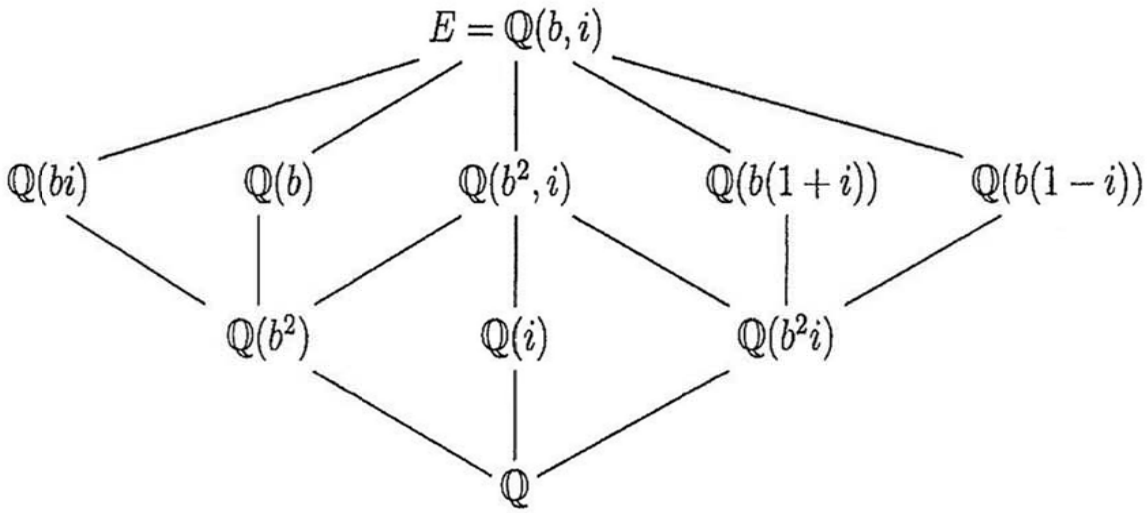
http://www.kallipos.gr

Θεοδώρα
Θεοχάρη - Αποστολίδη

Χαρά
Χαραλάμπους

ΘΕΩΡΙΑ GALOIS





Περιεχόμενα

Κατάλογος Ακρωνυμίων

ΑΠΘ	ΑΡΙΣΤΟΤΕΛΕΙΟ ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΕΣΣΑΛΟΝΙΚΗΣ
ΒΛ	ΒΛΕΠΕ
ΔΗΛ	ΔΗΛΑΔΗ
ΕΚΠ	ΕΛΑΧΙΣΤΟ ΚΟΙΝΟ ΠΟΛΛΑΠΛΑΣΙΟ
ΘΜΤ	ΘΕΩΡΗΜΑ ΜΕΣΗΣ ΤΙΜΗΣ
ΚΛΠ	ΚΑΙ ΛΟΙΠΑ
ΚΟΚ	ΚΑΙ ΟΥΤΩ ΚΑΘΕΞΗΣ
ΜΚΔ	ΜΕΓΙΣΤΟΣ ΚΟΙΝΟΣ ΔΙΑΙΡΕΤΗΣ
ΠΚΙ	ΠΕΡΙΟΧΗ ΚΥΡΙΩΝ ΙΔΕΩΔΩΝ
ΠΜΑ	ΠΕΡΙΟΧΗ ΜΟΝΟΣΗΜΑΝΤΗΣ ΑΝΑΛΥΣΗΣ
ΠΧ	ΠΑΡΑΔΕΙΓΜΑΤΟΣ ΧΑΡΙΝ

Κατάλογος Σχημάτων

Πρόλογος

Το βιβλίο αυτό απευθύνεται σε φοιτητές Μαθηματικών Τμημάτων και κατά κύριο μέρος στηρίζεται στις διαλέξεις μας στο προπτυχιακό μάθημα «Θεωρία Galois» που επί σειρά ετών διδάσκουμε στο Τμήμα Μαθηματικών της Σχολής Θετικών Επιστημών του Αριστοτελείου Πανεπιστημίου Θεσσαλονίκης.

Η Θεωρία Galois αρχικά αναφέρεται στην επίλυση αλγεβρικών, δηλ. πολυωνυμικών, εξισώσεων. Η επίλυση αλγεβρικών εξισώσεων απασχόλησε τους ανθρώπους περίπου από το 1700 π. Χ. σε διάφορες μορφές διατυπωμένες ανάλογα με το επίπεδο γνώσεων της εποχής. Φυσικά το πρώτο ερώτημα που διατυπώθηκε ήταν πώς μπορεί να λυθεί μία τέτοια εξίσωση και με την πάροδο των αιώνων οι μαθηματικοί αναρωτήθηκαν αν επιλύονται πάντα αυτές οι εξισώσεις. Την τελική απάντηση για την επιλυσιμότητα των αλγεβρικών εξισώσεων έδωσε ο Evariste Galois (1811-1832) στην ηλικία των 21 ετών στηριζόμενος στη μεγαλοφυφυΐα του και στο γιγάντιο σχετικό επιστημονικό έργο που είχε προηγηθεί της ζωής του.

Στο βιβλίο αναπτύσσουμε τη θεωρία που έλαβε το όνομά της από τον Galois. Σκοπός μας δεν είναι να δώσουμε τεχνικές επίλυσης διαφόρων συγκεκριμένων περιπτώσεων. Σκοπός μας είναι να αναπτύξουμε μία εξαιρετική μαθηματική θεωρία που αναπτύχθηκε από τον 17ο αιώνα και μετά και οδηγεί σε απαντήσεις ερωτημάτων που διατυπώθηκαν από τους Βαβυλώνιους και τους Αρχαίους Έλληνες και απαντήθηκαν τον 19ο αιώνα. Δεν θα μας απασχολήσει η ιστορική παρουσίαση των επιστημονικών γεγονότων κεντρικά, ούτε θα παρουσιάσουμε τη Θεωρία Galois όπως αυτή παρουσιάστηκε από τον Galois και αμέσως μετά όπως αυτή διατυπώθηκε από τους μαθηματικούς του 19ου αιώνα. Παρουσιάζουμε τη θεωρία αυτή με τη σύγχρονη θεώρηση της Άλγεβρας, ώστε ο αναγνώστης να εξοικειωθεί με τις εκπληκτικές ιδέες του νεαρού Galois, αλλά να μπορεί επίσης να παρακολουθήσει την εξέλιξη αυτής της θεωρίας και να κατευθύνει τους προβληματισμούς του σε σωστές διαδρομές σύγχρονων επιτευγμάτων.

Το βιβλίο αποτελείται από οκτώ κεφάλαια. Στο Κεφάλαιο 1 παρουσιάζονται τα κύρια θέματα που θα αναπτυχθούν στο κείμενο αυτό. Ακόμη, δίνονται οι απαιτούμενες έννοιες από τη θεωρία πολυωνύμων και τη θεωρία σωμάτων για τη μελέτη της θεωρίας Galois. Στο Κεφάλαιο 2 περιέχεται η θεωρία επεκτάσεων σωμάτων και ιδιαίτερα των αλγεβρικών επεκτάσεων. Επίσης δίνεται η έννοια της ομάδας Galois μίας επέκτασης. Στο Κεφάλαιο 3 μελετώνται οι επεκτάσεις Galois και αποδεικνύεται το θεμελιώδες θεώρημα της θεωρίας Galois. Η θεωρία που αναπτύχθηκε στο Κεφάλαιο 3 εφαρμόζεται στις επεκτάσεις πεπερασμένων σωμάτων και αυτό είναι το αντικείμενο του Κεφαλαίου 4. Στο Κεφάλαιο 5 συνεχίζεται η εφαρμογή της θεωρίας των επεκτάσεων Galois στη μελέτη των ριζών της μονάδας και των κυκλοτομικών επεκτάσεων. Στο Κεφάλαιο 6 αντιμετωπίζεται το ερώτημα πότε μπορεί να επιλυθεί μία αλγεβρική εξίσωση. Λέγοντας να επιλυθεί μία αλγεβρική εξίσωση εννοούμε να μπορούμε να βρούμε έναν τύπο που να παρέχει τις λύσεις της εξίσωσης, όπως αυτό συμβαίνει όταν το πολυώνυμο είναι δεύτερου βαθμού και έχουμε τον γνωστό τύπο από τις σχολικές μας γνώσεις. Στο κεφάλαιο αυτό αποδεικνύεται το Θεώρημα του Galois που δίνει μία ικανή και αναγκαία συνθήκη ώστε να είναι επιλύσιμη με ριζι-

κά μία αλγεβρική εξίσωση, απαντώντας σε ένα ερώτημα πολλών αιώνων και αποτελεί ένα από τα σημαντικότερα θεωρήματα των μαθηματικών. Ως εφαρμογή του θεωρήματος του Galois αντιμετωπίζονται τα τρία κλασικά προβλήματα κατασκευασιμότητας με κανόνα και διαβήτη που διατύπωσαν οι αρχαίοι έλληνες καθώς και προβλήματα κατασκευασιμότητας κανονικών πολυγώνων. Τέλος στο κεφάλαιο αυτό αποδεικνύεται το θεμελιώδες θεώρημα της Άλγεβρας κυρίως ως εφαρμογή του θεμελιώδους θεωρήματος της θεωρίας Galois. Στο Κεφάλαιο 7 εξετάζονται βαθύτερα οι αλγεβρικές επεκτάσεις και μελετώνται οι αλγεβρικά κλειστές επεκτάσεις. Η Θεωρία Galois είναι μία θεωρία που αναδεικνύει μία εξαιρετική σχέση μεταξύ της θεωρίας σωμάτων και της θεωρίας ομάδων. Βέβαια καθώς η μεγάλη επινόηση του Galois ήταν να εξετάσει τον ρόλο των μεταθέσεων των ριζών πολυωνύμων στην επιλυσιμότητα των πολυωνυμικών εξισώσεων, η ομάδα μεταθέσεων S_n των n αντικειμένων ήταν η μόνη ομάδα που απασχόλησε τους μαθηματικούς τον 19ο αιώνα. Στο Κεφάλαιο 8 αποδεικνύεται ότι υπάρχει πολυώνυμο του οποίου η ομάδα Galois είναι η S_n. Αυτό σημαίνει, ως συνέπεια του Θεμελιώδους Θεωρήματος της Θεωρίας Galois, ότι κάθε πεπερασμένη ομάδα είναι ομάδα Galois κάποιας επέκτασης σωμάτων. Στο υπόλοιπο του 8ου Κεφαλαίου σχολιάζουμε το καίριο ερώτημα που δημιουργείται: αν G είναι μία πεπερασμένη ομάδα υπάρχει επέκταση του σώματος των ρητών αριθμών με ομάδα Galois την G; Το ερώτημα αυτό δεν έχει απαντηθεί ακόμη και αποτελεί το λεγόμενο «Αντίστροφο Πρόβλημα της Θεωρίας Galois».

Κάθε κεφάλαιο του βιβλίου περιέχει πληθώρα παραδειγμάτων και στο τέλος κάθε κεφαλαίου υπάρχει ένα εδάφιο ασκήσεων. Μετά το 8ο κεφάλαιο παρατίθεται το Παράρτημα στο οποίο έχουν συμπεριληφθεί όλες οι προαπαιτούμενες γνώσεις της θεωρίας ομάδων, της θεωρίας δακτυλίων και της θεωρίας πολυωνύμων για την ανάπτυξη της μελέτης μας, ώστε το κείμενο να είναι πιο ολοκληρωμένο για το απρόσκοπτο διάβασμα. Δίνονται αναφορές που καθοδηγούν τον αναγνώστη σε άλλα συγγράμματα για τις προαπαιτούμενες γνώσεις, που συνήθως οι φοιτητές έχουν από άλλα μαθήματα άλγεβρας. Επίσης στο τέλος κάθε κεφαλαίου υπάρχει εκτενής βιβλιογραφία. Μέσα στο κείμενο οι αναφορές των θεωρημάτων, προτάσεων, ορισμάτων, παραδειγμάτων και ασκήσεων γίνεται με το αύξοντα αριθμό της θέσης του στο κείμενο. Π. χ. το Θεώρημα 3.5.3 είναι με αύξοντα αριθμό 3 στο Εδάφιο 5 του Κεφαλαίου 3. Το Παράδειγμα 1.2.7.1 είναι το παράδειγμα με αύξοντα αριθμό 1 στα Παραδείγματα με αριθμό 1.2.7. Ανάλογα αναφέρονται και οι ασκήσεις. Το Παράρτημα έχει πέντε εδάφια: I, II, III, IV, V έτσι το Θεώρημα I. 15 είναι το θεώρημα με αύξοντα αριθμό 15 στο Εδάφιο I του Παραρτήματος. Το τέλος κάθε απόδειξης επισημαίνεται με το σύμβολο □.

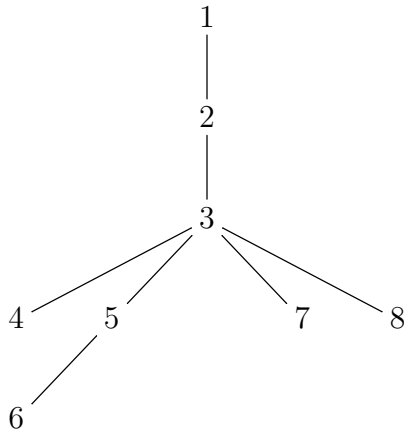
Όπως κάθε επιστημονικό αντικείμενο έτσι και αυτό κατακτάται με μελέτη και επιμονή. Η σελίδα-σελίδα κατανόηση του κειμένου είναι απαραίτητη για τη συνέχεια της μελέτης και ο έλεγχος της γνώσης γίνεται με την επίλυση των ασκήσεων. Αυτή η διαδικασία είναι εγγύηση για το αποτέλεσμα που επιδιώκει ο συνετός αναγνώστης. Τα παραδείγματα που παραθέτουμε καθώς και οι υποδείξεις των λύσεων έχουν στόχο να καταστήσουν τη διαδρομή μελέτης πι ο κατανοητή και, ελπίζουμε, απολαυστική. Θα είμαστε υπερήφανες αν καταφέρναμε συνεχώς και περισσότεροι αναγνώστες του βιβλίου αυτού να μπορέσουν να γευθούν την ηδονή της κατάκτησης και επεξεργασίας αυτής της καθόλου εύκολης αλλά σημαντικής γνώσης των μαθηματικών. Για μας η καθοδήγηση των δασκάλων μας σε όλη την πορεία μας φώτισε τις προσπάθειές μας. Οι φοιτητές μας, αγόρια και κορίτσια, με την αγάπη τους για τα μαθηματικά, την περιέργεια για την απάντηση στο ερώτημα, την έντονη προσπάθεια για την εύρεσή της, ο ενθουσιασμός και η υπερηφάνειά τους για την κατάκτηση της όλης γνώσης ήταν ο λόγος που αποφασίσαμε να συμπεριλάβουμε σε αυτό το κείμενο την εμπειρία μας από την μακρόχρονη διδασκαλία του αντικειμένου αυτού.

Μερικές συμβουλές για τον αναγνώστη αυτού του βιβλίου τις θεωρούμε απαραίτητες. Ο αναγνώστης που δεν είναι εξοικειωμένος με τη Θεωρία Ομάδων και τη Θεωρία Δακτυλίων οφείλει να ξεκινήσει τη μελέτη του από το Παράρτημα και να μελετήσει τα τέσσερα πρώτα εδάφια, δηλ. τα εδάφια I-IV. Στο εδάφιο V του Παραρτήματος, για πληρότητα, δίδονται οι ρίζες του γενικού πολυωνύμου τρίτου και η μελέτη του εδαφίου αυτού είναι ανεξάρτητη των υπολοίπων.

Στο εδάφιο με τίτλο «Υποδείξεις λύσεων επιλεγμένων ασκήσεων» δίνεται το αποτέλεσμα ή η υπόδειξη λύσης κάθε άσκησης που παρουσιάζει μεγαλύτερη δυσκολία.

Σε όλο το κείμενο μετά την εμφάνιση κάποιου επιστημονικού όρου για πρώτη φορά, η οποία επισημαίνεται με έντονους τυπογραφικούς χαρακτήρες, ακολουθεί ο ίδιος όρος στην αγγλική γλώσσα. Στο εδάφιο με τίτλο «Ευρετήρια» παραθέτουμε τα ευρετήρια των συμβολισμών και των μαθηματικών όρων και επώνυμων Θεωρημάτων και Λημμάτων που αναφέρονται στο κείμενο στην ελληνική και αγγλική γλώσσα και σημειώνουμε τη σελίδα στην οποία βρίσκονται. Με το ευρετήριο της αγγλικής ορολογίας ο αναγνώστης μπορεί εύκολα να αναζητήσει αντίστοιχα θέματα στην αγγλική βιβλιογραφία, εφόσον το επιθυμεί.

Το παρακάτω διάγραμμα δηλώνει τη σχέση εξάρτησης μεταξύ των κεφαλαίων του βιβλίου, εκτός του Παραρτήματος.



Για παράδειγμα το Κεφάλαιο 4 μπορεί να διαβαστεί ανεξάρτητα των Κεφαλαίων 5 και 6 κ.ο.κ. Το βιβλίο αυτό γράφτηκε στα πλαίσια του έργου Kallipos. Ευχαριστούμε θερμά τον κριτικό αναγνώστη του βιβλίου, Αναπληρωτή Καθηγητή του Τμήματος Μαθηματικών του Εθνικού Καποδιστριακού Πανεπιστημίου Αθηνών κ. Αριστείδη Κοντογεώργη για τις χρήσιμες παρατηρήσεις του, τον κ. Ιωάννη Καρύδη για τη μετατροπή του συγγράμματος σε μορφή HTML5 και την κ. Μαρία-Ιωάννα Χριστοφορίδου για την επιμέλεια του εξωφύλλου.

Σύντομη ιστορική ανασκόπηση

Η επίλυση πολυωνυμικών εξισώσεων, δηλαδή εξισώσεων της μορφής $f(x) = 0$, όπου $f(x)$ είναι ένα πολυώνυμο, απασχόλησε τους μαθηματικούς από την αρχαιότητα. Αρχαιολογικές έρευνες αναφέρουν ότι στη Μεσοποταμία βρέθηκαν ευρήματα περίπου 3300 χρόνια π. Χ., όπου σε κεραμικά εμφανίζονται σχέσεις που θυμίζουν τη σημερινή διαίρεση. Είναι γνωστό ότι, ανάμεσα στο 1900–1600 π.Χ., οι Βαβυλώνιοι ανέπτυξαν μεθόδους για την επίλυση δευτεροβάθμιων πολυωνυμικών εξισώσεων με συντελεστές θετικούς ακέραιους. Η εξαγωγή ριζικών είναι φανερή σε αυτές τις προσπάθειες.

Οι αρχαίοι Έλληνες κατέχουν μία περίοπτη θέση στην ιστορία των μαθηματικών, γιατί ανακάλυψαν την απόδειξη για την τεκμηρίωση της μαθηματικής αλήθειας. Το 430 π.Χ. με γεωμετρικές μεθόδους πρώτοι οι αρχαίοι Έλληνες της σχολής του Πυθαγόρα (570-495 π. Χ.) αποδεικνύουν ότι το $\sqrt{2}$ δεν είναι ρητός αριθμός. Το 300 π. Χ. ο Ευκλείδης έγραψε «Τα Στοιχεία» ένα έργο τεράστιας μαθηματικής αξίας. Αν και ο Ευκλείδης δεν ασχολήθηκε με την επίλυση τετραγωνικών εξισώσεων στη γενική τους μορφή, μπόρεσε να απαντήσει σε ερωτήσεις της μορφής: για ποια x, y, ισχύει $x - y = a$ και $xy = b$. Η επίλυση αλγεβρικών εξισώσεων δευτέρου βαθμού με χρήση γεωμετρικών μεθόδων απασχόλησε τους αρχαίους Έλληνες. Ο Πλούταρχος (46-120) αναφέρει ότι ο Πλάτωνας (427-347 π. Χ.) εισήγαγε τη μέθοδο γεωμετρικών κατασκευών με κανόνα και διαβήτη πιστεύοντας ότι ο διπλασιασμός του κύβου, ένα από τα κλασσικά προβλήματα της αρχαιότητας, έπρεπε να λυθεί με καθαρά γεωμετρικό τρόπο.

Πρώτος ο Άραβας Muhammad ibn Musa al-Khwarizmi (780-850) περίπου το 830 επισήμανε την ύπαρξη δευτεροβάθμιας εξίσωσης με δύο διακεκριμένες ρίζες θετικούς ακέραιους. Το 1074 ο Omar Khayyan (1048-1131), ο οποίος έζησε στο Ιράν, έδωσε λύσεις για κάποιες τριτοβάθμιες εξισώσεις με συντελεστές θετικούς ακέραιους χρησιμοποιώντας κωνικές τομές. Σημειώνουμε ότι οι αρνητικοί αριθμοί άρχισαν να χρησιμοποιούνται ευρέως τον 16ο αιώνα. Το 1515 ο Ιταλός Scipione del Ferro (1465-1526), καθηγητής στο πανεπιστήμιο της Bologna, υπολόγισε τις λύσεις της εξίσωσης $x^3 + mx = n$, για φυσικούς αριθμούς m και n. Το 1535 ο Niccolo Fontana (1500-1557), γνωστός ως Tartaglia, υπολόγισε τις ρίζες μερικών ειδικών περιπτώσεων τριτοβάθμιων αλγεβρικών εξισώσεων. Το 1539 ο Girolamo Cardano (1501-1576) δημοσίευσε στο βιβλίο του «Ars Magma» (Μέγα Έργο) τις λύσεις των εξισώσεων που έλυσε ο Tartaglia, χωρίς, όμως, την έγκριση του τελευταίου. Ο Cardano στο βιβλίο του αυτό δημοσίευσε την επίλυση 13 ακόμη περιπτώσεων τριτοβάθμιων εξισώσεων τις οποίες ο ίδιος υπολόγισε. Ο Cardano έδωσε μία πλήρη επίλυση των πολυωνυμικών εξισώσεων τρίτου βαθμού χρησιμοποιώντας και αρνητικούς αριθμούς. Στο έργο «Ars Magma» αναφέρεται επίσης μία μέθοδος επίλυσης πολυωνυμικών εξισώσεων τέταρτου βαθμού η οποία επινοήθηκε από τον Lodovico Ferrari (1522-1565), μαθητή του Cardano. Ο Rafaele Bombelli (1526-1572) στο βιβλίο του με τίτλο «Algebra» συγκέντρωσε τις μέχρι τότε γνώσεις και επηρεασμένος από το έργο το Διόφαντου (210-290) έγραψε αναλυτικά και με πιο σύγχρονο τρόπο την επίλυση των εξισώσεων 3ου και 4ου βαθμού δίνοντας την αριθμητική των αρνητικών αριθμών, αλλά και τις ιδιότητες των

μιγαδικών αριθμών. Το 1615 ο Γάλλος μαθηματικός Francois Viete (1540-1603) έδωσε μία ευκρινέστερη ανάπτυξη της μεθόδου του Ferrari και ήταν ο πρώτος που χρησιμοποίησε γράμματα για συντελεστές και αγνώστους σε μία εξίσωση χωρίς, όμως, να δώσει τη γενική λύση των εξισώσεων. Ο επίσης Γάλλος μαθηματικός Albert Girard (1595-1632) ήταν ο πρώτος ο οποίος ισχυρίστηκε ότι ένα πολυώνυμο βαθμού n έχει το πολύ n πλήθους πραγματικούς αριθμούς ως ρίζες και ακριβώς n αν συμπεριληφθούν και οι φανταστικοί αριθμοί ως ρίζες. Μετά από αυτά τα επιτεύγματα άρχισε η έντονη δραστηριότητα των μαθηματικών να συνεχιστεί η προσπάθεια εύρεσης των ριζών πολυωνυμικών εξισώσεων βαθμού μεγαλύτερου του 4 με ριζικά.

Το 1683 ο Γερμανός μαθηματικός Ehrenfried Walter von Tschirnhaus (1651-1708) παρουσίασε μία ενιαία μέθοδο επίλυσης μίας αλγεβρικής εξίσωσης οποιουδήποτε βαθμού. Η μέθοδος αυτή οδηγούσε στην επίλυση ενός γραμμικού συστήματος, που, όπως, επισήμανε ο Leibniz ήταν πολύ δύσκολο να λυθεί. Ο Γερμανός μαθηματικός Gottfried Wilhelm Leibniz (1646-1716), ένας από τους σημαντικούς ερευνητές στη μιγαδική ανάλυση, ασχολήθηκε ιδιαίτερα με την επίλυση πολυωνυμικών εξισώσεων 5ου βαθμού χωρίς, όμως, να φθάσει στον στόχο του. Στην εύρεση των λύσεων της εξίσωσης $x^n - 1 = 0$, δηλ. της εύρεσης των n-οστών ριζών της μονάδας, συνέτεινε ο Roger Cotes (1682-1716) χρησιμοποιώντας τριγωνομετρικές μεθόδους. Ο Γάλλος μαθηματικός Abraham de Moivre (1667-1754) εφαρμόζοντας και τελειοποιώντας τα αποτελέσματα της εργασίας του Cotes βρήκε τις ρίζες του πολυωνύμου $x^n - 1$ και έδωσε τους γνωστούς τύπους που φέρουν το όνομά του. Με την εργασία αυτή του de Moirve αποδείχθηκε ότι η εξαγωγή ριζών μιγαδικών αριθμών δεν παράγει νέους τύπους αριθμών, αλλά πάλι μιγαδικούς αριθμούς. Είναι αξιοσημείωτο ότι η εργασία του de Moirve ώθησε τους μαθηματικούς της εποχής σε μεθόδους προχωρημένων μαθηματικών για την επίλυση αλγεβρικών εξισώσεων. Η μέθοδος που πρότεινε το 1765 ο Γάλλος μαθηματικός Etienne Bezout (1730-1783) είχε ιδιαίτερο ενδιαφέρον γιατί χρησιμοποίησε την εξαγωγή ριζών της μονάδας για την επίλυση εξισώσεων μικρού βαθμού. Ο μέγας μαθηματικός Leonhard Euler (1707-1783), ο οποίος γεννήθηκε στην Ελβετία, ασχολήθηκε επίσης με την επίλυση αλγεβρικών εξισώσεων, αλλά και αυτός χωρίς να οδηγηθεί στον στόχο του παρά τις μεγάλες επιτεύξεις του σε μεγάλου εύρους μαθηματικές θεωρίες. Η πρώτη μεγάλη έκρηξη στην επίλυση αλγεβρικών εξισώσεων έγινε το 1770 με τη σχεδόν ταυτόχρονη δημοσίευση των συμπερασμάτων του Ιταλο-Γάλλου μαθηματικού Joseph-Louis Lagrange (1736-1813) και του Γάλλου μαθηματικού Alexandre-Theophile Vandermonde (1735-1796) οι οποίοι ανεξάρτητα ο ένας του άλλου έδωσαν έναν νέο τρόπο επίλυσης των αλγεβρικών εξισώσεων. Ο ίδιος ο Lagrange αναφέρει ότι η μελέτη του εξυπηρετεί δύο σκοπούς: ο πρώτος δίνει περισσότερο φως στις ήδη γνωστές λύσεις εξισώσεων 3ου και 4ου βαθμού και ο δεύτερος την εισήγηση μεθόδων που μπορούν να εφαρμοστούν σε λύσεις εξισώσεων μεγαλύτερου βαθμού. Ο Lagrange μελετώντας τις εργασίες των προγενεστέρων του ερευνητών και κυρίως των Euler, Bezout και Tschirnhaus διαπίστωσε ότι όλες οι μέθοδοι οδηγούν στην εύρεση κατάλληλων συναρτήσεων των ριζών της εξίσωσης που έχουν βαθμό μικρότερο από την αρχική εξίσωση και επιπλέον οι ρίζες μπορούν εύκολα να εξαχθούν από αυτές. Στο τέλος της εργασίας του ο Lagrange απέδειξε συμπεράσματα της Θεωρίας Ομάδων, με όρους μεταθέσεων, μεταξύ αυτών και το πολύ σημαντικό γνωστό σήμερα Θεώρημα του Lagrange. Πολύ ενδιαφέρον γεγονός είναι ότι σε αυτήν την εργασία του ο Lagrange μελετάει το ρόλο των μεταθέσεων των ριζών της αλγεβρικής εξίσωσης στην εύρεση των ριζών. Ο Vandermonde δεν υπήρξε ο μαθηματικός της κλάσης μεγέθους του Lagrange και του Euler, όμως είχε εξαιρετικές ιδέες για την επίλυση αλγεβρικών εξισώσεων. Ανάπτυξε πολλές από τις ιδέες του Lagrange πριν από τον Lagrange και μερικές σύγχρονα με αυτόν. Όμως, οι μέθοδοί του δεν ήσαν

διατυπωμένες με σαφήνεια και παρουσιάστηκαν δύο χρόνια μετά τις δημοσιεύσεις των εργασιών του Lagrange, ο οποίος ήταν πασίγνωστος. Ο μέγας Γερμανός μαθηματικός Carl Friedrich Gauss (1777-1855), ο αποκαλούμενος από όλους πλέον τους μαθηματικούς *πρίγκιπας των μαθηματικών*, είχε σημαντική συνεισφορά στην επίλυση αλγεβρικών εξισώσεων. Το 1799 απέδειξε το Θεμελιώδες Θεώρημα της Άλγεβρας με μεθόδους της μαθηματικής ανάλυσης. Η δεύτερη μεγάλη συνεισφορά του ήταν στην επίλυση των κυκλοτομικών εξισώσεων. Ο Gauss με τη μελέτη του στα κυκλοτομικά σώματα έδειξε πώς μπορούσε να εφαρμόσει και να τελειοποιήσει τα επιχειρήματα του Vandermonde για να βρει επαγωγικούς τύπους με ριζικά, προκειμένου να υπολογίσει τις n-ρίζες της μονάδας. Χωρίς να φθάσει στο επιδιωκόμενο αποτέλεσμα βρήκε τρόπους να αναγάγει την εύρεση των ριζών της μονάδας στην εύρεση ριζών κυκλοτομικών πολυωνύμων μικρότερων βαθμών. Ως εφαρμογή αυτών των συμπερασμάτων το 1796 κατασκεύασε με κανόνα και διαβήτη το κανονικό 17-γωνο σε ηλικία 19 ετών.

Οι μέθοδοι του Lagrange ενέπνευσαν τον Paolo Ruffini (1765- 1822), ο οποίος το 1799 δημοσίευσε ένα δίτομο έργο όπου αποδείκνυε ότι μία αλγεβρική εξίσωση βαθμού μεγαλύτερου του 5 δεν επιλύεται με ριζικά. Η εργασία του Ruffini ήταν ιδιαίτερα εκτενής και δυσνόητη. Κάποια συμπεράσματα του Ruffini γενικεύτηκαν από τον Γάλλο μαθηματικό Augustin Louis Cauchy (1789-1857), ο οποίος έδειξε ιδιαίτερο ενδιαφέρον για το έργο του Ruffini βρίσκοντας, όμως, ένα αποδεικτικό κενό. Το 1824 μία νέα σχετικά σύντομη απόδειξη του συμπεράσματος του Ruffini δόθηκε από τον νεαρό Νορβηγό μαθηματικό Niels-Henrik Abel (1802-1829). Η απόδειξη του Abel ήταν ανεξάρτητη από τη δουλειά του Ruffini και κάλυπτε το αποδεικτικό κενό της απόδειξης του Ruffini. Με τα σημαντικά συμπεράσματα των Gauss, Ruffini και Abel γνωρίζουμε μέχρι στιγμής ότι (εκτός από τα πολυώνυμα 3ου και 4ου βαθμού) κάποια από τα κυκλοτομικά πολυώνυμα βαθμού μεγαλύτερου του 5 είναι επιλύσιμα με ριζικά, καθώς και ότι υπάρχουν πολυώνυμα βαθμού μεγαλύτερου ή ίσου του 5 που δεν είναι επιλύσιμα με ριζικά. Το ερώτημα που πρέπει να απαντηθεί τώρα είναι πότε ένα πολυώνυμο είναι επιλύσιμο με ριζικά; Η τιμή της απάντησης στο κρίσιμο αυτό ερώτημα ανήκει στον ιδιοφυή νεαρό Evariste Galois (1811-1832). Ο Evariste Galois στα 21 χρόνια που έζησε είχε μία δραματική ζωή, που απασχολεί ακόμη τους ιστορικούς ώστε να φέρουν στο φως όλες τι πτυχές της, αλλά κατάφερε να κάνει σημαντικές μαθηματικές ανακαλύψεις από τη εποχή της δευτεροβάθμιας εκπαίδευσής του. Ο Galois μελέτησε το έργο του Lagrange και επηρεάστηκε από αυτό. Προσπάθησε από τον Μάιο του 1829 να δημοσιοποιήσει τα συμπεράσματά του. Δύο εργασίες του στάλθηκαν μέσω της Ακαδημίας Επιστημών του Παρισιού στον Cauchy για να τις κρίνει, ο οποίος τις έχασε. Το Φεβρουάριο του 1830 η εργασία του στάλθηκε πάλι από την Ακαδημία Επιστημών του Παρισιού για κρίση στον Joseph Fourier (1768-1830) ο οποίος πέθανε πριν τη διαβάσει και έτσι χάθηκε. Τον Ιανουάριο του 1831 ο Galois υπέβαλε την εργασία του στον Γάλλο μαθηματικό Simeon Denis Poisson (1781-1840) ο οποίος την απέρριψε ως ακατάληπτη. Οι ιστορικές αναφορές μας πληροφορούν ότι ο Galois την παραμονή μίας μονομαχίας, που του κόστισε τη ζωή, έγραψε μία επιστολή με ημερομηνία 29 Μαίου 1832 προς το φίλο του Auguste Chevallier στην οποία έδινε ένα σκίτσο των συμπερασμάτων του για την επίλυση αλγεβρικών εξισώσεων. Επιθυμία του Galois ήταν να μοιραστεί το περιεχόμενο της επιστολής σε επιφανή μέλη της μαθηματικής κοινότητας. Η επιθυμία του Galois εκτελέστηκε από τον Chevalier και τον αδελφό του Galois, έτσι ένα αντίγραφο έφθασε στον Joseph Liouville (1809-1882), ο οποίος ως μέλος της Ακαδημίας Επιστημών του Παρισιού, αναγνώρισε το κείμενο του Galois και διαβεβαίωσε την ορθότητά του με σχετική του ανακοίνωση στην Ακαδημία το 1843. Ο Liouville αποκωδικοποίησε το κείμενο του Galois και με τη φροντίδα του δημοσιεύθηκε το 1846. Η βασική ιδέα του

Galois ήταν να προσαρτήσει σε κάθε πολυώνυμο μία ομάδα μεταθέσεων των ριζών του και το βασικό του συμπέρασμα ήταν να αποδείξει μία ικανή και αναγκαία συνθήκη ώστε ένα πολυώνυμο να είναι επιλύσιμο με ριζικά. Απαντώντας σε ένα από τα πλέον σημαντικά ερωτήματα που απασχόλησαν τους πλέον επιφανείς μαθηματικούς τουλάχιστον μέχρι την εποχή του. Ο αναγνώστης μπορεί να βρει μία μετάφραση στα αγγλικά από τα γαλλικά της εργασίας του Galois, όπως γράφτηκε από τον ίδιο στην επιστολή του το 1832, στο [2] και [3].

Πρώτο μέλημα των μαθηματικών μετά την κοινοποίηση της θεωρίας του Galois ήταν να ετοιμαστεί το μαθηματικό υπόβαθρο ώστε αυτή να γίνει κατανοητή από όλους τους μαθηματικούς. Ο Γερμανός μαθηματικός Leopold Kronecker (1823- 1891) ανάπτυξε τη θεωρία σωμάτων κυρίως στο κατασκευαστικό της μέρος. Ο επίσης Γερμανός μαθηματικός Richard Dedekind (1831-1916) που θεμελίωσε τη θεωρία σωμάτων από τη συνολοθεωρητική της πλευρά, ήταν ο πρώτος ο οποίος ασχολήθηκε με την ομάδα αυτομορφισμών ενός σώματος στη θέση της ομάδας μεταθέσεων ριζών και όρισε την ομάδα Galois, όπως την εννοούμε σήμερα. Το 1854 ο Άγγλος μαθηματικός Arthur Cayley (1821-1895) όρισε την έννοια της ομάδας, όπως την εννοούμε σήμερα. Το ενδιαφέρον των μαθηματικών πλέον στράφηκε προς τη θεωρία ομάδων και δεν ασχολούνταν μόνο με τις ομάδες μεταθέσεων, λόγω της επιρροής της θεωρίας Galois . Ο Γερμανός μαθηματικός Emil Artin (1898-1962) ευθύνεται κατά ένα μεγάλο μέρος για τη σημερινή παρουσίαση της θεωρίας Galois, αυτός έδωσε τη μορφή στο Θεμελιώδες Θεώρημα της Θεωρίας Galois, όπως το διδάσκουμε σήμερα, και σε αυτόν οφείλονται πολλές από τις επί μέρους αποδείξεις, αφού από το κείμενο του Galois δεν ήταν σαφής η αντιστοιχία μεταξύ υποομάδων και υποσωμάτων. Το 1928 ο Γερμανός μαθηματικός Wolfgang Krull (1899-1971) επέκτεινε τη θεωρία Galois σε άπειρες επεκτάσεις σωμάτων όπου η τοπολογία παίζει σημαντικό ρόλο. Το 1968 οι S.U. Chase, D.K. Harrison και A. Rosenberg στο [1] επέκτειναν τη θεωρία Galois σε επεκτάσεις αντιμεταθετικών δακτυλίων. Η θεωρία Galois εξακολουθεί να δημιουργεί νέους προβληματισμούς και το επιστημονικό αυτό αντικείμενο είναι συνεχούς ενδιαφέροντος. Για περισσότερα ιστορικά στοιχεία παραπέμπουμε στα συγγράμματα που αναφέρονται στη βιβλιογραφία αυτού του εδαφίου και σε πολυμεσικές διαλέξεις του ψηφιακού μαθήματος (open courses) Ιστορία των Μαθηματικών του Τμήματος Μαθηματικών, Α.Π.Θ.

Βιβλιογραφία Ιστορικής Ανασκόπησης

[1] Chase, S.U., Harrison, D.K., Rosenberg, A. *Galois Theory and Galois homology of commutative rings*. Mem. Amer. Soc. **58**, 1965, 15-33.

[2] Edwards, H.M. *Galois Theory*. Springer, 1984.

[3] Escofier, J.P. *Galois Theory*. Springer, 2001.

[4] Katz, V. *Ιστορία των Μαθηματικών, Μία εισαγωγή*. Πανεπιστημιακές Εκδόσεις Κρήτης, 2013.

[5] Kleiner, I. *A History of Abstract Algebra*. Birhäuser, 2007.

[6] Stewart, I. *Galois Theory*. Champan and Hall, 1973.

[7] Tignol, J.P. *Galois Theory of Algebraic Equations*. World Scientific, 2011.

[8] van der Waerden, B.L. *A History of Algebra*. Springer, 1991.

[9] Zhmud, L. *The origin of the History of Science in Classical Antiquity*. Walker de Gruyter, 2006.

Κεφάλαιο 1

Βασικές Έννοιες

Στο Κεφάλαιο αυτό δίνουμε τις απαραίτητες προκαταρτικές γνώσεις από τη θεωρία πολυωνύμων και τη θεωρία σωμάτων που απαιτούνται για τα επόμενα κύρια κεφάλαια. Στο Εδάφιο 1.1 παρουσιάζουμε τα βασικά θέματα που πρόκειται να αναπτυχθούν εκτενώς στα κείμενο αυτό. Ο αναγνώστης μπορεί να συμβουλευτεί τα συγγράμματα της προτεινόμενης βιβλιογραφίας για αποδείξεις θεωρημάτων που παραλείπονται.

1.1 Εισαγωγικά

Στο εδάφιο αυτό θα περιγράψουμε τα τρία βασικά θέματα που θα μας απασχολήσουν σε αυτό το κείμενο:

- το Θεμελιώδες Θεώρημα της Άλγεβρας,
- την εύρεση ριζών πολυωνυμικών εξισώσεων και
- την κατασκευασιμότητα κανονικών πολυγώνων με κανόνα και διαβήτη.

1.1.1 Το Θεμελιώδες Θεώρημα της Άλγεβρας

Το Θεμελιώδες Θεώρημα της Άλγεβρας (Fundamental Theorem of Algebra) είναι από τα σημαντικότερα θεωρήματα στα μαθηματικά.

Θεμελιώδες Θεώρημα της Άλγεβρας *Αν $f(x) \in \mathbb{C}[x]$ και $\deg f(x) > 0$, τότε υπάρχει $a \in \mathbb{C}$ έτσι ώστε $f(a) = 0$. Δηλαδή κάθε μη σταθερό πολυώνυμο με συντελεστές από το σύνολο των μιγαδικών αριθμών έχει τουλάχιστον μία ρίζα στο $\mathbb{C}$.*

Είναι αξιοσημείωτο να τονίσουμε ότι το Θεμελιώδες Θεώρημα της Άλγεβρας βεβαιώνει την ύπαρξη ρίζας του $f(x)$, δεν κατασκευάζει, όμως, τη ρίζα αυτή. Παρατηρούμε ότι αν $f(x) \in \mathbb{C}[x]$ και $f(a) = 0$, τότε υπάρχει $q(x) \in \mathbb{C}[x]$ έτσι ώστε $f(x) = (x - a)q(x)$. Μπορεί λοιπόν να αποδειχθεί με απλή επαγωγή στον βαθμό του πολυωνύμου $f(x)$, ότι αν $f(x) \in \mathbb{C}[x]$ και $n = \deg f(x) > 0$, τότε το $f(x)$ έχει n ρίζες στο $\mathbb{C}$. Λέμε ότι το σώμα $\mathbb{C}$ είναι *αλγεβρικά κλειστό* εξαιτίας αυτής της ιδιότητας. Η ιδιότητα αυτή έχει ως συνέπεια ότι κάθε πολυώνυμο του $\mathbb{C}[x]$ αναλύεται σε γινόμενο γραμμικών παραγόντων στο $\mathbb{C}[x]$. Από το Θεμελιώδες Θεώρημα της Άλγεβρας προκύπτει ακόμα ότι τα μόνα ανάγωγα πολυώνυμα του $\mathbb{C}[x]$ είναι τα πολυώνυμα βαθμού 1. Αφού τα πολυώνυμα του $\mathbb{R}[x]$ ανήκουν και στον $\mathbb{C}[x]$, τα μη μηδενικά πολυώνυμα με πραγματικούς συντελεστές έχουν τόσες μιγαδικές ρίζες όσος είναι ο βαθμός τους, μετρώντας τις ρίζες σύμφωνα με την πολλαπλότητά τους.

Όμως σε αντίθεση με το $\mathbb{C}$, το σώμα $\mathbb{R}$ δεν είναι αλγεβρικά κλειστό. Για παράδειγμα το πολυώνυμο $x^2+1 \in \mathbb{R}[x]$ δεν έχει ούτε μία ρίζα στον $\mathbb{R}$.

Η πρώτη απόδειξη του Θεμελιώδους Θεωρήματος της Άλγεβρας αποδίδεται στον Gauss το 1799. Η απόδειξη αυτή χρησιμοποιεί ιδέες από τη τοπολογία και έχει κάποια κενά. Η πρώτη πλήρης απόδειξη οφείλεται στον Argand το 1814, ενώ στη συνέχεια ο Gauss έδωσε τουλάχιστον άλλες δύο πλήρεις διαφορετικές αποδείξεις. Έως σήμερα έχουν δοθεί πάνω από 200 αποδείξεις του Θεμελιώδους Θεωρήματος της Άλγεβρας που χρησιμοποιούν και σε κάποιες περιπτώσεις συνδυάζουν μεθόδους από τη Μαθηματική Ανάλυση, την Τοπολογία, την Άλγεβρα, τη Θεωρία Αριθμών, ακόμα και από τη Θεωρία Πιθανοτήτων.

Στο Κεφάλαιο 6 θα δώσουμε μία αλγεβρική απόδειξη του Θεμελιώδους Θεωρήματος της Άλγεβρας χρησιμοποιώντας τις βασικές ιδέες της Θεωρίας Galois. Για κάποια ιστορικά στοιχεία σχετικά με την απόδειξη του Θεμελιώδους Θεωρήματος της Άλγεβρας παραπέμπουμε σε πολυμεσικές διαλέξεις του ψηφιακού μαθήματος (open courses) Ιστορία των Μαθηματικών του Τμήματος Μαθηματικών, Α.Π.Θ. και συγκεκριμένα στη διάλεξη της Ενότητας 7.3. Για τον Gauss και την προσφορά του στα μαθηματικά παραπέμπουμε ειδικότερα στη διάλεξη της Ενότητας 8.2 καθώς και στον [5, Κεφ. 15].

1.1.2 Τύποι για τις ρίζες πολυωνύμων

Έως τον 19 αιώνα, ο όρος *Άλγεβρα* αναφερόταν στην επίλυση πολυωνυμικών εξισώσεων, δηλαδή εξισώσεων της μορφής $f(x)=0$, όπου $f(x)$ είναι ένα πολυώνυμο με συντελεστές από ένα σώμα. Όπως είδαμε προηγουμένως το Θεμελιώδες Θεώρημα της Άλγεβρας εγγυάται την ύπαρξη ριζών του $f(x)$, δεν δίνει όμως πληροφορίες για τον υπολογισμό αυτών των ριζών.

Τον 16ο αιώνα Ιταλοί Μαθηματικοί (dal Ferro, Cardano, Tartaglia, Ferrari) βρήκαν τύπους για την εύρεση ριζών πολυωνύμων βαθμού 3 και 4. Σημειώνουμε ότι στη διατύπωση αυτών των τύπων εμφανίζονται η πρόσθεση και αφαίρεση, ο πολλαπλασιασμός και η διαίρεση αριθμών, καθώς και η εξαγωγή ριζικών με χρήση των συντελεστών των πολυωνύμων. Για παράδειγμα ο τύπος για την εύρεση μίας ρίζας του πολυωνύμου x^3+mx-n, όπου m,n είναι ακέραιοι αριθμοί, είναι ο ακόλουθος:

$$\sqrt[3]{\frac{n}{2}+\sqrt{\left(\frac{n}{2}\right)^2+\left(\frac{m}{3}\right)^3}}-\sqrt[3]{-\frac{n}{2}+\sqrt{\left(\frac{n}{2}\right)^2+\left(\frac{m}{3}\right)^3}}. \tag{1.1.2.1}$$

Οι τύποι γίνονται πιο πολύπλοκοι για πολυώνυμα τέταρτου βαθμού. Η αναλυτική περιγραφή των ριζών πολυωνύμων τρίτου και τέταρτου βαθμού δίνεται στο Παράρτημα V. Εάν οι ρίζες ενός πολυωνύμου περιγράφονται με τύπους τέτοιας μορφής, λέμε ότι το πολυώνυμο *επιλύεται με ριζικά*.

Οι τύποι αυτοί ανάγκασαν τους μαθηματικούς της εποχής να αποδεχτούν το μυστήριο της άλγεβρας των φανταστικών αριθμών. Αν και οι τύποι των ριζών των τριτοβάθμιων και τεταρτοβάθμιων πολυωνύμων διατυπώθηκαν αρχικά για πολυώνυμα με ρητούς συντελεστές, οι τύποι αυτοί ισχύουν και για πολυώνυμα με συντελεστές από το $\mathbb{C}$. Μετά την επίλυση με ριζικά του τεταρτοβάθμιου πολυωνύμου η προσπάθεια επικεντρώθηκε στην εύρεση αντίστοιχου τύπου για τις ρίζες των πολυωνύμων πέμπτου βαθμού. Ο πρώτος, που ισχυρίστηκε γραπτά ότι δεν υπάρχει τέτοιος τύπος, ήταν ο Ιταλός μαθηματικός Ruffini σε μία εργασία του το 1799. Εκεί ο Ruffini εισήγαγε για πρώτη φορά την έννοια της *ομάδας* των μεταθέσεων. Ο Lagrange το 1771 είχε ορίσει τις μεταθέσεις στοιχείων, δεν είχε όμως αναγνωρίσει μία ιδιαίτερη δομή στο σύνολο των μεταθέσεων. Η εργασία του Ruffini είχε κάποια μικρά κενά και δεν αναγνωρίστηκε εκείνη την εποχή από τη

Μαθηματική κοινότητα, ούτε και οι μετέπειτα προσπάθειες του, όπου διόρθωνε ο ίδιος τα κενά, δημοσιεύοντας τις εργασίες του με δικά του έξοδα. Το 1824 ο Abel έδωσε μία ολοκληρωμένη απόδειξη της *μη επιλυσιμότητας* του γενικού πολυωνύμου πέμπτου βαθμού, χρησιμοποιώντας και αυτός τις μεταθέσεις των ριζών του πολυωνύμου. Σήμερα στο αντίστοιχο θεώρημα αποδίδουμε και τα δύο ονόματα κατά αλφαβητική σειρά των επιθέτων των συγγραφέων, όπως είθισται στις μαθηματικές εργασίες.

Θεώρημα των Abel-Ruffini. *Δεν υπάρχει τύπος με ριζικά που να επιλύει όλα τα πολυώνυμα βαθμού 5 με πραγματικούς συντελεστές.*

Σίγουρα, όμως, υπάρχουν πολυώνυμα βαθμού 5 που είναι επιλύσιμα με ριζικά. Για παράδειγμα ας θεωρήσουμε το πολυώνυμο $f(x) = x^5 - 2 \in \mathbb{C}[x]$. Μία ρίζα του $f(x)$ είναι ο πραγματικός αριθμός b, που δίνεται από τον τύπο $b = \sqrt[5]{2}$. Διαιρώντας το $f(x)$ με το $x - b$, προκύπτει ότι υπάρχει πολυώνυμο $q(x) \in \mathbb{R}[x]$ έτσι ώστε $f(x) = (x - b)q(x)$. Ο βαθμός του $q(x)$ είναι 4 και επομένως το πολυώνυμο $q(x)$ είναι επιλύσιμο με ριζικά (αφού όλα τα πολυώνυμα βαθμού τρία ή τέσσερα είναι επιλύσιμα με ριζικά). Οι ρίζες, όμως, του $q(x)$ είναι και ρίζες του $f(x)$. Έτσι το $f(x)$ είναι και αυτό επιλύσιμο με ριζικά όπως ισχυριστήκαμε. Τίθεται λοιπόν το εύλογο ερώτημα: ποια πολυώνυμα είναι τελικά επιλύσιμα με ριζικά;

Ο πρώτος που αντιλήφθηκε ότι η δυνατότητα προσδιορισμού των ριζών ενός πολυωνύμου $f(x)$ με τύπο συνδέεται με τη δομή της ομάδας των μεταθέσεων των ριζών του $f(x)$ είναι ο Galois, το 1831. Ο Galois χρησιμοποίησε μία υποομάδα της ομάδας των μεταθέσεων των ριζών του πολυωνύμου $f(x)$, η οποία σήμερα λέγεται ομάδα του Galois. Στο Κεφάλαιο 3 θα αποδείξουμε το ακόλουθο θεώρημα που αναφέρεται στην επιλυσιμότητα με ριζικά.

Θεώρημα του Galois. *Τα πολυώνυμα, των οποίων οι ρίζες εκφράζονται από κάποιον τύπο που εμπεριέχει πρόσθεση, αφαίρεση, πολλαπλασιασμό, διαίρεση και εξαγωγή ριζικών των συντελεστών, είναι ακριβώς εκείνα για τα οποία η αντίστοιχη ομάδα του Galois είναι επιλύσιμη.*

Η έννοια της *επιλυσιμότητας* μίας ομάδας προέρχεται, όπως θα δούμε στο Κεφάλαιο 6, από τη Θεωρία Ομάδων. Για να αποδείξουμε το παραπάνω θεώρημα θα χρειαστούμε το Θεμελιώδες Θεώρημα της Θεωρίας Galois, που περιγράφουμε εδώ χωρίς μαθηματική αυστηρότητα στη σύγχρονη εκδοσή του:

Θεμελιώδες Θεώρημα της Θεωρίας Galois *Έστω F σώμα και $f(x) \in F[x]$. Έστω E το μικρότερο σώμα που περιέχει το F και όλες τις ρίζες του $f(x)$. Υπάρχει μία πλήρης αντιστοιχία ανάμεσα στα υποσώματα του E που περιέχουν το F και στις υποομάδες της ομάδας Galois του $f(x)$.*

Παραλείψαμε σκόπιμα κάποιες συνθήκες στο παραπάνω θεώρημα για να κάνουμε κατανοητή τη βασική ιδέα. Για παράδειγμα, το θεώρημα ισχύει για τα *διαχωρίσιμα* πολυώνυμα. Ένα άλλο σημείο, όπου θα επιμείνουμε αργότερα, είναι η έννοια του *μικρότερου* σώματος που περιέχει το σώμα στο οποίο ανήκουν οι συντελεστές του πολυωνύμου, αλλά και οι ρίζες του, καθώς και η συνεπαγόμενη ερώτηση για το πόσα τέτοια διαφορετικά σώματα υπάρχουν. Θα χρειαστεί, λοιπόν, να μελετήσουμε ιδιότητες σωμάτων και να καταλάβουμε τις δομές τους. Θα τα μελετήσουμε όλα αυτά στα επόμενα εδάφια αυτού του κειμένου. Για την ιστορία που οδήγησε στην ανακάλυψη της θεωρημάτων των Abel-Ruffini και Galois παραπέμπουμε στο [5, Ενότητες 9.3, 15.2, 15.3] και στις πολυμεσικές διαλέξεις του ψηφιακού μαθήματος Ιστορία των Μαθηματικών του Τμήματος Μαθηματικών, Α.Π.Θ. και συγκεκριμένα στις διαλέξεις των Ενοτήτων 9.2 και 9.3.

1.1.3 Κατασκευές με κανόνα και διαβήτη.

Ως κατασκευές με κανόνα και διαβήτη εννοούμε τις γεωμετρικές κατασκευές για τις οποίες επιτρέπεται μόνο η χρήση του κανόνα και του διαβήτη. Ο κανόνας είναι ένα γεωμετρικό εργαλείο με μία πλευρά. Με τον κανόνα μπορούμε να χαράξουμε ένα ευθύγραμμο τμήμα με άκρα δύο προσδιορισμένα σημεία. Δεχόμαστε ότι μπορούμε να επεκτείνουμε το ευθύγραμμο τμήμα με τον κανόνα και προς τις δύο κατευθύνσεις απεριόριστα. Ο κανόνας, όμως, δεν φέρει υποδιαιρέσεις και δεν μπορεί από μόνος του να καθορίσει αποστάσεις. Ο διαβήτης είναι το γεωμετρικό εργαλείο με το οποίο μπορούμε να χαράξουμε την περιφέρεια ενός κύκλου του οποίου γνωρίζουμε το κέντρο και την ακτίνα. Στο κέντρο του κύκλου τοποθετούμε το άκρο του ενός σκέλους του διαβήτη, ενώ η ακτίνα προσδιορίζεται από το άνοιγμα των άκρων των σκελών του διαβήτη.

Για να μπορέσουμε να προχωρήσουμε σε μία γεωμετρική κατασκευή θα πρέπει να μπορούμε να κατασκευάσουμε σημεία, δηλ. να προσδιορίσουμε τη θέση τους πάντα και μόνο με κανόνα και διαβήτη και να συνδέουμε τα σημεία που μας ενδιαφέρουν με ευθείες γραμμές με τη χρήση του κανόνα. Θα εξετάσουμε πώς μπορούμε να κατασκευάσουμε σημεία στο επίπεδο. Όμως, πρώτα ας παρατηρήσουμε ότι αν ήδη έχουμε κατασκευάσει κάποια σημεία, τα νέα σημεία που μπορούμε να κατασευάσουμε από αυτά προκύπτουν με τον κανόνα και τον διαβήτη με έναν από τους ακόλουθους τρεις τρόπους:

- ως τομή δύο ευθύγραμμων τμημάτων,
- ως τομή ενός ευθύγραμμου τμήματος και της περιφέρειας ενός κύκλου,
- ως τομή των περιφερειών δύο κύκλων.

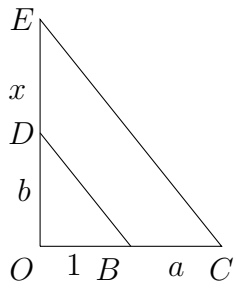
Θα ξεκινήσουμε με δύο αρχικά σημεία στο επίπεδο. Λέμε ότι μία απόσταση είναι ***κατασκευάσιμη*** (constructible) αν προκύπτει ως απόσταση ανάμεσα σε δύο κατασκευάσιμα σημεία. Συμφωνούμε η απόσταση ανάμεσα στα δύο αρχικά σημεία να είναι ίση με τη μονάδα μέτρησης, που συμβολίζουμε με 1, και χαράζουμε την ευθεία που διέρχεται από τα δύο αρχικά σημεία με τη χρήση του κανόνα. Στη συνέχεια ταυτίζουμε την ευθεία αυτή με την ευθεία των πραγματικών αριθμών και ορίζουμε τα αρχικά σημεία με 0 και 1, με το 1 στα δεξιά του 0. Θα προσπαθήσουμε να βρούμε όλα τα σημεία επί της πραγματικής ευθείας που είναι κατασκευάσιμα και τις αντίστοιχες κατασκευάσιμες αποστάσεις. Ξεκινούμε με την κατασκευή των ακέραιων αριθμών. Με κέντρο το σημείο 1 και ακτίνα το μήκος της μονάδας χαράσσουμε μία περιφέρεια κύκλου η οποία τέμνει την ευθεία σε ένα σημείο δεξιά του σημείου 1. Το σημείο αυτό είναι το 2. Συνεχίζοντας με αυτό το τρόπο, κατασκευάζουμε όλους τους φυσικούς αριθμούς. Επαναλαμβάνοντας τη διαδικασία αριστερά του σημείου 0 κατασκευάζουμε με κανόνα και διαβήτη τους αριθμούς $-1, -2$, κ.ο.κ. Έχουμε κατασκευάσει έτσι όλους τους ακέραιους αριθμούς. Παρατηρούμε επίσης ότι, αν a, b είναι κατασκευάσιμοι πραγματικοί αριθμοί επί της ευθείας που αρχικά χαράξαμε, μπορούμε με τον διαβήτη να κατασκευάσουμε τον αριθμό $a \pm b$.

Πριν προχωρήσουμε στην κατασκευή των ρητών αριθμών ας θυμηθούμε, ότι με κανόνα και διαβήτη είναι δυνατές οι επόμενες κατασκευές στο επίπεδο, (βλ. άσκηση 1.5.1):

- να χαράξουμε κάθετη ευθεία σε δοθείσα ευθεία που να περνάει από συγκεκριμένο σημείο επί της αρχικής ευθείας,
- να μεσοκάθετη σε δοθέν ευθύγραμμο τμήμα,
- να χαράξουμε ευθεία παράλληλη σε δοθείσα ευθεία που να περνάει από συγκεκριμένο σημείο εκτός της δοθείσης ευθείας,

- να χαράξουμε τη διχοτόμο δοθείσης γωνίας στο επίπεδο.

Για να κατασκευάσουμε τους αριθμούς a, b, a^{-1}, όπου a, b φυσικοί αριθμοί, χρησιμοποιούμε το Θεώρημα του Θαλή για τα όμοια τρίγωνα. Χαράσσουμε την κάθετη στο σημείο O της αρχικής ευθείας. Στην οριζόντια ευθεία με τον διαβήτη ορίζουμε το σημείο B έτσι ώστε το τμήμα OB να έχει μήκος ίσο με 1, το σημείο C έτσι ώστε το τμήμα OC να έχει μήκος a και στην κατακόρυφη ευθεία ορίζουμε το σημείο D έτσι ώστε το τμήμα OD να έχει μήκος b, (βλ. Σχήμα 1.1). Ενώνουμε τα σημεία BD με μία ευθεία χρησιμοποιώντας τον κανόνα και από το σημείο C φέρουμε παράλληλο προς την ευθεία που διέρχεται από τα σημεία B και D. Έστω E το σημείο τομής αυτής της παραλλήλου με την αρχική ευθεία.

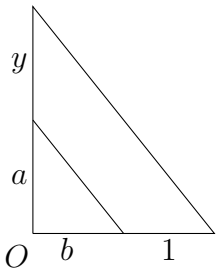


Σχήμα 1.1: $x = ab$

Αν x είναι το μήκος του τμήματος OE, τότε, από το Θεώρημα του Θαλή, προκύπτει ότι:

$$\frac{1}{b} = \frac{a}{x} \Rightarrow x = ab \ .$$

Όμοια, σύμφωνα με το Σχήμα 1.2, κατασκευάζουμε το κλάσμα $\frac{a}{b}$ από τους αριθμούς a, b, όταν $b \neq 0$.



Σχήμα 1.2: $y = \frac{a}{b}$

Η διαδικασία που ακολουθήσαμε μπορεί να εφαρμόζεται κάθε φορά που οι αριθμοί a, b είναι κατασκευάσιμοι θετικοί αριθμοί. Αφού ο αρνητικός αριθμός ενός κατασκευάσιμου αριθμού είναι κατασκευάσιμος, αντιλαμβανόμαστε ότι το σύνολο των κατασκευάσιμων αριθμών είναι σώμα: το άθροισμα, η διαφορά, το γινόμενο και το κλάσμα (όπου η διαίρεση επιτρέπεται) κατασκευάσιμων αριθμών είναι κατασκευάσιμος αριθμός. Έστω F το σώμα των κατασκευάσιμων αριθμών. Από τα παραπάνω έπεται ότι το F περιέχει τους ρητούς. Σύμφωνα με την άσκηση 1.5.2, αν ο $a \geq 0$ είναι κατασκευάσιμος αριθμός, τότε ο $\sqrt{a}$ είναι κατασκευάσιμος αριθμός. Αφού, λοιπόν, ο 2 είναι κατασκευάσιμος αριθμός, έπεται ότι ο

$\sqrt{2} \in F$. Ως γνωστό ο $\sqrt{2}$ δεν είναι ρητός. Έτσι βλέπουμε ότι το σώμα F εκτός από τους ρητούς περιέχει και άλλους πραγματικούς αριθμούς.

Παρατηρούμε, επίσης, ότι μπορούμε να κατασκευάσουμε στο επίπεδο ένα σύστημα καρτεσιανών συντεταγμένων: ο ένας άξονας είναι η αρχική ευθεία, ο δεύτερος άξονας είναι η κάθετος στο σημείο O, ενώ στο σημείο O δίνουμε τις συντεταγμένες $(0,0)$. Διαπιστώνουμε ότι μπορούμε να κατασκευάσουμε σημεία στο επίπεδο ανάγοντας αυτές τις κατασκευές στις συντεταγμένες των σημείων. Συμπεραίνουμε ότι όλα τα σημεία του συνόλου $\{(a,b) : \ a^2, b^2 \in \mathbb{Q}\}$ είναι κατασκευάσιμα.

Τα θέματα της κατασκευασιμότητας με κανόνα και διαβήτη απασχόλησαν τους αρχαίους Έλληνες που θρησκευτικές επιταγές και η αναζήτηση της *μαθηματικής καθαρότητας* απαιτούσαν τη χρήση μόνο κανόνα και διαβήτη. Έτσι γρήγορα οδηγήθηκαν στην ανάγκη επίλυσης των προβλημάτων:

- Μπορούμε να κατασκευάσουμε την τριχοτόμηση μίας γωνίας;
- Μπορούμε να κατασκευάσουμε κύβο με διπλάσιο όγκο ενός άλλου κύβου;
- Μπορούμε να τετραγωνίσουμε τον κύκλο;
- Ποια κανονικά πολύγωνα είναι κατασκευάσιμα;
- Ποιες αποστάσεις είναι κατασκευάσιμες;

Αυτά τα θέματα κατασκευασιμότητας με κανόνα και διαβήτη θα εξετάσουμε στο Κεφάλαιο 6 ως εφαρμογές της Θεωρίας Galois. Για ιστορικά στοιχεία σχετικά με τα άλυτα γεωμετρικά προβλήματα της αρχαιότητας παραπέμπουμε στην πολυμεσική διάλεξη 2.3 του ψηφιακού μαθήματος Ιστορία των Μαθηματικών του Τμήματος Μαθηματικών, Α.Π.Θ. Για τις μίνι-εφαρμογές (applets) των γεωμετρικών κατασκευών παραπέμπουμε στο [9].

1.2 Βασικές ιδιότητες των πολυωνύμων

Στο εδάφιο αυτό θα εξετάσουμε τις βασικές ιδιότητες των πολυωνύμων με συντελεστές από μία ακέραια περιοχή R ή από ένα σώμα F. Συχνά θα μας ενδιαφέρουν πολυώνυμα πάνω από τον $\mathbb{Z}$ και το $\mathbb{Q}$. Ο αναγνώστης καλείται να ανατρέξει στις Ενότητες II, III του Παραρτήματος για τους βασικούς ορισμούς. Εδώ θα αναφέρουμε τις έννοιες και τα συμπεράσματα που απαιτούνται για την ανάπτυξη της Θεωρίας Galois. Τις σχετικές αποδείξεις ο αναγνώστης μπορεί να τις αναζητήσει στα [3, Κεφάλαια 4, 6] και [2, Κεφάλαιο 9] καθώς και στο [7].

Έστω ότι F είναι σώμα και $F[x]$ ο δακτύλιος των πολυωνύμων με συντελεστές από το F. Ο δακτύλιος $F[x]$ είναι ένας F-διανυσματικός χώρος άπειρης διάστασης, αφού τα στοιχεία $\{x^i : \ i \in \mathbb{N}\}$ αποτελούν μία F-βάση του $F[x]$. Σημειώνουμε, λοιπόν, ότι $\dim_F F[x] = \infty$. Θυμίζουμε επίσης ότι ένα πολυώνυμο λέγεται *κανονικό ή μονικό* αν ο συντελεστής της μεγιστοβάθμιας δύναμης του x είναι ίσος με 1. Έτσι το πολυώνυμο $x^2 - 1 \in \mathbb{Q}[x]$ είναι κανονικό, ενώ το πολυώνυμο $2x - 1$ δεν είναι. Το επόμενο θεώρημα χαρακτηρίζει τον δακτύλιο πολυωνύμων $F[x]$ πάνω από σώμα F, βλ. Παράρτημα, Θεώρημα III.3.

Θεώρημα 1.2.1. *i. Έστω ότι F είναι σώμα και έστω $f(x), g(x) \in F[x]$, $g(x) \neq 0$. Τότε υπάρχουν μοναδικά πολυώνυμα $q(x), r(x) \in F[x]$ τέτοια ώστε $f(x) = g(x)q(x) + r(x)$ με $\deg r(x) < \deg g(x)$ ή $r(x) = 0$.*

ii. Έστω F ένα σώμα. Τότε ο δακτύλιος $F[x]$ είναι περιοχή κυρίων ιδεωδών (Π.Κ.Ι.).

Το πρώτο σκέλος του προηγουμένου θεωρήματος δηλώνει ότι ισχύει ο Ευκλείδειος αλγόριθμος στον $F[x]$. Από το δεύτερο σκέλος προκύπτει ότι αν I είναι ιδεώδες του $F[x]$, τότε υπάρχει ένα πολυώνυμο $f(x) \in F[x]$ ώστε:

$$I = \langle f(x) \rangle = \{f(x)g(x) : \ g(x) \in F[x]\}.$$

Το πολυώνυμο $f(x)$ καλείται γεννήτορας του ιδεώδους I και δεν ορίζεται μοναδικά για το I, αφού $\langle f(x) \rangle = \langle uf(x) \rangle$, για κάθε αντιστρέψιμο στοιχείο $u \in F[x]$, δηλ. για κάθε $u \in F^*$. Για αυτόν τον λόγο επιλέγουμε συνήθως ως γεννήτορα του I ένα κανονικό πολυώνυμο του $F[x]$, τον οποίο καλούμε ***κανονικό γεννήτορα*** του I. Πράγματι,

$$a_0 + \cdots + a_n x^n \neq 0 \ \Leftrightarrow \ a_n \neq 0$$

και σε αυτήν την περίπτωση

$$\langle a_0 + \cdots a_n x^n \rangle = \langle a_n^{-1}(a_0 + \cdots a_n x^n) \rangle = \langle a_0 a_n^{-1} + \cdots a_{n-1} a_n^{-1} x^{n-1} + x^n \rangle.$$

Έτσι προκύπτει ότι ο κανονικός γεννήτορας ενός μη μηδενικού ιδεώδους του $F[x]$ ορίζεται μοναδικά και προσδιορίζεται από την ιδιότητα ότι είναι το μοναδικό κανονικό πολυώνυμο ελάχιστου βαθμού που ανήκει στο ιδεώδες.

Ο δακτύλιος $F[x]$ ως Π.Κ.Ι. είναι περιοχή μονοσήμαντης ανάλυσης (Π.Μ.Α.). Έτσι τα ανάγωγα στοιχεία του $F[x]$ είναι τα πρώτα στοιχεία του. Αυτό σημαίνει ότι αν το $f(x)$ είναι *ανάγωγο*, τότε κάθε φορά που το $f(x)$ διαιρεί το γινόμενο δύο πολυωνύμων πρέπει να διαιρεί αναγκαστικά το ένα από τα δύο. Από τον ορισμό της Π.Μ.Α. προκύπτει ότι κάθε πολυώνυμο $f(x) \neq 0$ του $F[x]$ αναλύεται μοναδικά ως γινόμενο

$$f(x) = u p_1^{t_1}(x) \cdots p_s^{t_s}(x),$$

όπου $u \in F^*$ και τα $p_i(x)$, $1 \leq i \leq s$, είναι κανονικά ανάγωγα πολυώνυμα.

Όπως στην αριθμητική του $\mathbb{Z}$, έτσι και σε κάθε Π.Μ.Α. σημαντικό ρόλο παίζουν ο μέγιστος κοινός διαιρέτης (ΜΚΔ) και το ελάχιστο κοινό πολλαπλάσιο (ΕΚΠ) πεπερασμένου πλήθους στοιχείων του $F[x]$. Έστω $f_1(x), \ldots, f_s(x)$ στοιχεία (πολυώνυμα) του $F[x]$. Τότε υπάρχουν τα πολυώνυμα

$$\text{ΜΚΔ}\left(f_1(x), \ldots, f_s(x)\right), \ \text{ΕΚΠ}\left(f_1(x), \ldots, f_s(x)\right)$$

και αυτά ορίζονται μοναδικά με προσέγγιση ενός αντιστρέψιμου στοιχείου του $F[x]$. Αν $h(x) = \text{ΜΚΔ}\left(f_1(x), \ldots, f_s(x)\right)$, τότε από το Παράρτημα, Θεώρημα II.11, προκύπτει ότι υπάρχουν πολυώνυμα $q_1(x), \ldots, q_s(x)$ του $F[x]$, ώστε

$$h(x) = f_1(x)q_1(x) + \cdots + f_s(x)q_s(x)$$

και επομένως ισχύει η παρακάτω ισότητα για τα ιδεώδη:

$$\langle h(x) \rangle = \langle f_1(x), \ldots, f_s(x) \rangle,$$

δηλ. το κύριο ιδεώδες με γεννήτορα το $h(x)$ είναι το ιδεώδες του $F[x]$ που παράγεται από τα στοιχεία $f_1(x), \ldots, f_s(x)$.

Ιδιαίτερα, αν δύο πολυώνυμα $f_1(x)$ και $f_2(x)$ του $F[x]$ είναι πρώτα μεταξύ τους, δηλ. αν $\text{ΜΚΔ}(f_1(x), f_2(x)) = 1$, τότε

$$\langle f_1(x), f_2(x) \rangle = F[x] \ .$$

Το παραπάνω γενικεύεται για s πολυώνυμα $f_1(x), \ldots, f_s(x) \in F[x]$ όταν γνωρίζουμε ότι ΜΚΔ$(f_1(x), \ldots, f_s(x)) = 1$. Σε αυτήν την περίπτωση

$$\langle f_1(x), \ldots, f_s(x) \rangle = F[x] \ .$$

Λόγω της μοναδικής παραγοντοποίησης κάθε πολυωνύμου $f(x) \in F[x]$ σε γινόμενο αναγώγων πολυωνύμων καταλαβαίνουμε ότι τα ανάγωγα πολυώνυμα και, για πρακτικούς λόγους, τα κανονικά ανάγωγα πολυώνυμα παίζουν σημαντικό ρόλο στη μελέτη μας. Καταρχήν αν $p(x) \in F[x]$ είναι ανάγωγο, τότε το ιδεώδες $\langle p(x) \rangle$ είναι μέγιστο, βλ. Παράρτημα, Θεώρημα III.3, αλλά και αντίστροφα κάθε μέγιστο ιδεώδες του $F[x]$ έχει γεννήτορα ένα ανάγωγο πολυώνυμο του $F[x]$.

Ο έλεγχος για το αν ένα δοθέν πολυώνυμο είναι ανάγωγο δεν είναι εύκολη διαδικασία και δεν υπάρχει αλγόριθμος που να μας οδηγεί σε ένα τέτοιο συμπέρασμα. Υπάρχουν, όμως, κάποια κριτήρια με τα οποία θα ασχοληθούμε αργότερα για τον έλεγχο της αναγωγιμότητας ενός πολυωνύμου που δεν δίνουν, όμως, πάντα ικανές και αναγκαίες συνθήκες.

Οι ρίζες ενός πολυωνύμου συνδέονται με την παραγοντοποίησή του, όπως προκύπτει από το επόμενο συμπέρασμα με απλή εφαρμογή της Ευκλείδειας διαίρεσης.

Πρόταση 1.2.2. *Έστω $f(x) \in F[x]$. Το $a \in F$ είναι ρίζα του $f(x)$ αν και μόνο αν το $x - a$ διαιρεί το $f(x)$ στον $F[x]$.*

Απόδειξη. Σύμφωνα με τον Ευκλείδειο αλγόριθμο $f(x) = (x - a)q(x) + r(x)$, όπου $\deg r(x) < 1$, και συνεπώς $r(x) = r \in F$. Άρα το $x - a$ διαιρεί το $f(x)$ αν και μόνο αν το υπόλοιπο $r = 0$. Αυτό, όμως, συμβαίνει αν και μόνο αν $f(a) = 0$, δηλαδή αν a είναι ρίζα του $f(x)$. □

Εφαρμόζοντας διαδοχικά την προηγούμενη πρόταση προκύπτει το εξής πόρισμα.

Πόρισμα 1.2.3. *Αν $f(x) \in F[x]$ και $a_1, \ldots, a_n \in F$ είναι διακεκριμένες ρίζες του $f(x)$ τότε*

$$f(x) = (x - a_1) \cdots (x - a_n)p(x), \text{ όπου } p(x) \in F[x].$$

Ειδικότερα αν $n = \deg f(x)$ και $a_1, \ldots, a_n \in F$ είναι διακεκριμένες ρίζες του $f(x)$ τότε

$$f(x) = c(x - a_1) \cdots (x - a_n), \text{ όπου } c \in F.$$

Έστω ότι $\phi : \ F \to L$ είναι εμφύτευση σωμάτων και

$$\tilde{\phi} : \ F[x] \to L[x] : \ \sum c_i x^i \mapsto \sum \phi(c_i) x^i$$

είναι ο αντίστοιχος ομομορφισμός ανάμεσα στους δακτυλίους πολυωνύμων. Συμβολίζουμε με $\tilde{f}(x)$ την εικόνα του $f(x)$ στον $L[x]$. Είναι εύκολο να δούμε ότι αν a είναι ρίζα του $f(x)$ τότε $\phi(a)$ είναι ρίζα του $\tilde{f}(x)$. Πράγματι:

$$\tilde{f}(\phi(a)) = \sum \phi(c_i)\phi(a)^i = \sum \phi(c_i a^i) = \phi(\sum c_i a^i) = \phi(f(a)) = \phi(0) = 0.$$

Έτσι, από το Πόρισμα 1.2.3 προκύπτει το επόμενο συμπέρασμα με τον παραπάνω συμβολισμό.

Πόρισμα 1.2.4. *Έστω ότι $a_1, \ldots, a_n \in F$ είναι διακεκριμένες ρίζες του $f(x)$, όπου $n = \deg f(x)$, $\phi : \ F \to L$ εμφύτευση σωμάτων και έστω ότι $\phi(a_1), \ldots, \phi(a_n)$ είναι ρίζες ενός πολυωνύμου $g(x) \in L[x]$. Τότε*

$$g(x) = \tilde{f}(x)p(x), \text{ όπου } p(x) \in L[x].$$

Παραθέτουμε αμέσως δύο παραδείγματα πολυωνύμων τα οποία αναλύουμε σε γινόμενο παραγόντων για να εφαρμόσουμε κάποιες γνωστές μεθόδους, αλλά και για να αντιληφθούμε τα ερωτήματα που ανακύπτουν από αυτές τις προσπάθειες.

Παράδειγμα 1.2.5. Θα αναλύσουμε το πολυώνυμο $f(x) = x^3 - 2$ σε γινόμενο αναγώγων παραγόντων ως πολυώνυμο του $\mathbb{Q}[x]$, του $\mathbb{R}[x]$ και του $\mathbb{C}[x]$. Ξεκινούμε βρίσκοντας τις ρίζες του $f(x)$ στο σώμα $\mathbb{C}$. Παρατηρούμε ότι το $b = \sqrt[3]{2}$ είναι μία ρίζα του $f(x)$ (είναι μάλιστα η ρίζα που προκύπτει από τον τύπο 1.1.2.1 αντικαθιστώντας $m = 0$, $n = 2$). Επομένως το πολυώνυμο $x - b \in \mathbb{R}[x]$ διαιρεί το πολυώνυμο $x^3 - 2$. Σύμφωνα με τον Ευκλείδειο αλγόριθμο διαίρεσης δύο πολυωνύμων βρίσκουμε ότι:

$$f(x) = x^3 - 2 = (x - \sqrt[3]{2})(x^2 + \sqrt[3]{2}\, x + \sqrt[3]{4}),$$

δηλαδή

$$f(x) = (x - b)(x^2 + b\, x + b^2).$$

Θέτουμε $p(x) = x^2 + b\ x + b^2$ και χρησιμοποιώντας τον τύπο που δίνει τις ρίζες ενός δευτεροβάθμιου πολυωνύμου, βρίσκουμε ότι οι άλλες δύο ρίζες του $x^3 - 2$ είναι:

$$\sqrt[3]{2}\left(-\frac{1}{2} \pm \frac{i\sqrt{3}}{2}\right).$$

Θέτουμε τώρα

$$\omega = -\frac{1}{2} + \frac{i\sqrt{3}}{2} = \cos\left(\frac{2\pi}{3}\right) + i \sin\left(\frac{2\pi}{3}\right).$$

Παρατηρούμε ότι

$$\omega = e^{2\pi i/3},\ \omega^2 = -\frac{1}{2} - \frac{i\sqrt{3}}{2}, \omega^3 = e^{2\pi i} = 1.$$

Άρα μπορούμε να γράψουμε τις 3 ρίζες του $x^3 - 2$ στο $\mathbb{C}$ ως εξής: b, ωb και $\omega^2 b$. Επίσης σημειώνουμε τα παρακάτω:

i. Καμία από τις ρίζες του $f(x)$ δεν ανήκει στο $\mathbb{Q}$. Αυτό σημαίνει ότι δεν υπάρχει πολυώνυμο βαθμού 1 στον $\mathbb{Q}[x]$ που να διαιρεί το $f(x)$. Κατά συνέπεια, το $f(x)$ δεν μπορεί να γραφεί ως γινόμενο δύο πολυωνύμων βαθμού (και των δύο) μικρότερου του 3. Άρα το $f(x)$ είναι ανάγωγο στον $\mathbb{Q}[x]$.

ii. Αφού το $b \in \mathbb{R}$ όπως και οι συντελεστές του $q(x)$, έπεται ότι $x - b, q(x) \in \mathbb{R}[x]$ και άρα στον $\mathbb{R}[x]$ ισχύει ότι $f(x) = (x - b)q(x)$. Επομένως το $f(x)$ δεν είναι ανάγωγο στον $\mathbb{R}[x]$. Το πολυώνυμο $q(x)$ έχει βαθμό 2, ενώ οι ρίζες του δεν ανήκουν στο σώμα $\mathbb{R}$. Όπως και προηγουμένως, από την ανάλυση των βαθμών προκύπτει ότι το $q(x)$ είναι ανάγωγο στον $\mathbb{R}[x]$. Έπεται επομένως ότι στον δακτύλιο $\mathbb{R}[x]$ η ανάλυση του $f(x)$ σε ανάγωγους παράγοντες είναι το γινόμενο $f(x) = (x - b)q(x)$.

iii. Κάθε πολυώνυμο βαθμού 1 είναι ανάγωγο. Έτσι η ανάλυση του $f(x)$ σε ανάγωγους παράγοντες στον $\mathbb{C}[x]$ είναι $f(x) = (x - b)(x - \omega b)(x - \omega^2 b)$.

Σημειώνουμε τα παρακάτω δύο συμπεράσματα. Το πρώτο προκύπτει από την ανάλυση των βαθμών. Το δεύτερο είναι επίσης άμεσο.

Πρόταση 1.2.6. *Έστω $f(x) \in F[x]$, όπου F σώμα.*

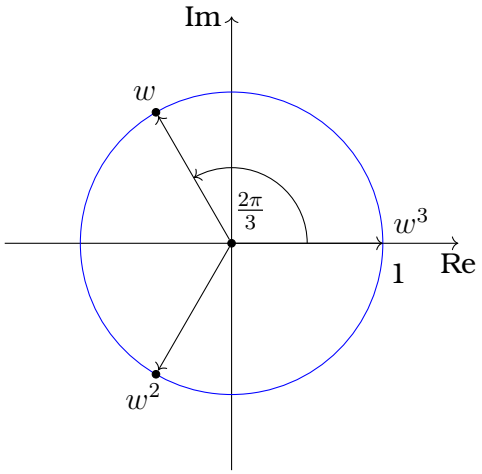
i. Αν $\deg f(x)$ είναι 2 ή 3, τότε το $f(x)$ είναι ανάγωγο αν και μόνο αν το $f(x)$ δεν έχει ρίζες στο F.

ii. Έστω ότι $F \subset E$, όπου E σώμα. Αν το $f(x)$ είναι ανάγωγο στον $E[x]$, τότε το $f(x)$ είναι ανάγωγο στον $F[x]$.

Παράδειγμα 1.2.7. Εξετάζουμε τώρα το πολυώνυμο $f(x) = x^3 - 1$. Το πολυώνυμο αυτό δεν είναι ανάγωγο στον $\mathbb{Q}[x]$, αφού $f(1) = 0$ και

$$x^3 - 1 = (x-1)(x^2 + x + 1). \tag{1.2.7.1}$$

Έστω $\Phi_3(x) = x^2 + x + 1$. Υπολογίσαμε τις ρίζες του $\Phi_3(x)$ στο προηγούμενο παράδειγμα: είναι οι συζυγείς μιγαδικοί αριθμοί ω και ω^2, όπου $\omega = e^{2\pi i/3}$. Στο Σχήμα 1.3 δίνεται η γραφική παράσταση των ριζών ω, ω^2 και $\omega^3 = 1$ του πολυωνύμου $x^3 - 1$ στο μιγαδικό επίπεδο.



Σχήμα 1.3: Οι ρίζες του $x^3 - 1$

Οι τρεις λοιπόν ρίζες της μονάδας, δηλαδή οι ρίζες του πολυωνύμου $x^3 - 1$, είναι οι ω, ω^2 και $\omega^3 = 1$, όπου $\omega = e^{2\pi i/3}$. Εύκολα επιβεβαιώνουμε ότι

$$(x - \omega)(x - \omega^2) = x^2 + x + 1.$$

Επομένως

1. $\omega^2 + \omega + 1 = 0$ και $(\omega^2)^2 + \omega^2 + 1 = 0$.
2. $\omega \cdot \omega^2 = 1$.

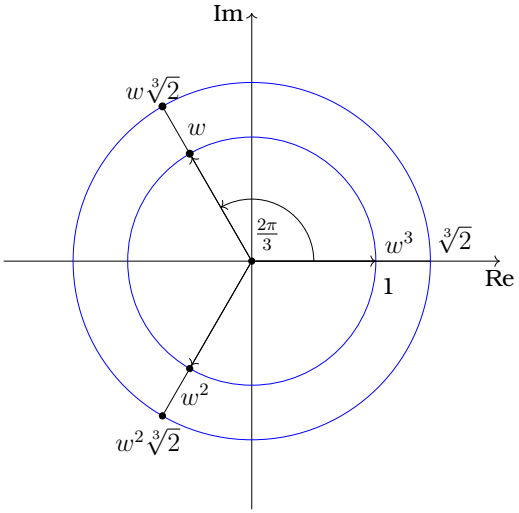
Από την Πρόταση 1.2.6 και αφού οι ρίζες του $\Phi_3(x)$ δεν είναι πραγματικοί αριθμοί, έπεται ότι το πολυώνυμο $\Phi_3(x)$ είναι ανάγωγο στον $\mathbb{R}[x]$ και στον $\mathbb{Q}[x]$. Βέβαια, το $\Phi_3(x)$ δεν είναι ανάγωγο στον $\mathbb{C}[x]$. Έτσι η ανάλυση του $x^3 - 1$ σε γινόμενο ανάγωγων πολυωνύμων στους δακτυλίους $\mathbb{R}[x]$ και $\mathbb{Q}[x]$ είναι η ανάλυση της σχέσης (1.2.7.1), δηλ.

$$x^3 - 1 = (x-1)(x^2 + x + 1),$$

ενώ η ανάλυση του $x^3 - 1$ σε γινόμενο ανάγωγων πολυωνύμων στον $\mathbb{C}[x]$ είναι

$$x^3 - 1 = (x-1)(x - \omega)(x - \omega^2).$$

Πριν προχωρήσουμε στο πολυώνυμο $x^n - 1$, σημειώνουμε τη θέση των ριζών του πολυωνύμου $x^3 - 2$ στο μιγαδικό επίπεδο, βλ. Παράδειγμα 1.2.5.



Σχήμα 1.4: Οι ρίζες του $x^3 - 2$

Οι επόμενες παρατηρήσεις αφορούν το πολυώνυμο $x^n - 1$ και τις ρίζες του στο σώμα $\mathbb{C}$. Θέτουμε

$$\omega = e^{2\pi i/n} = \cos\left(\frac{2\pi}{n}\right) + i\sin\left(\frac{2\pi}{n}\right).$$

Οι n-ρίζες της μονάδας, δηλ. οι ρίζες του $x^n - 1$ στο $\mathbb{C}$, είναι οι

$$1, \omega, \ldots, \omega^{n-1}.$$

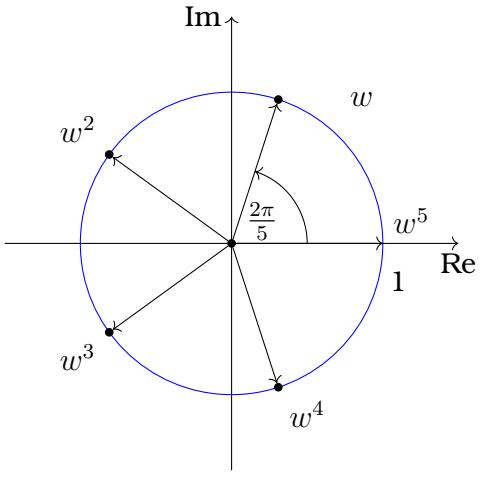
Ισχύουν τα εξής:

i) $x^n - 1 = (x-1)(x^{n-1} + x^{n-2} + \cdots + x + 1)$,

ii) οι ρίζες του $x^{n-1} + x^{n-2} + \cdots + x + 1$ στο $\mathbb{C}$ είναι οι ω, ω^2, $\ldots$, ω^{n-1}, και άρα

iii) $(\omega^k)^{n-1} + (\omega^k)^{n-2} \cdots + (\omega^k) + 1 = 0$, για $k = 1, \ldots, n-1$.

Οι n-ρίζες της μονάδας στο μιγαδικό επίπεδο, βρίσκονται επί του μοναδιαίου κύκλου σε γωνίες που αντιστοιχούν σε πολλαπλάσια του $2\pi/n$. Είδαμε, στο Σχήμα 1.3, τη γραφική αναπαράσταση των 3-ριζών της μονάδας. Ως δεύτερο παράδειγμα, οι 5-ρίζες της μονάδας απεικονίζονται στο Σχήμα 1.5.



Σχήμα 1.5: Οι 5-ρίζες της μονάδας

Στο επόμενο εδάφιο θα δούμε ότι όταν p είναι πρώτος φυσικός αριθμός, το πολυώνυμο $x^{p-1}+x^{p-2}+\cdots+x+1$ είναι ανάγωγο πολυώνυμο του δακτυλίου $\mathbb{Q}[x]$ και συμβολίζεται με $\Phi_p(x)$. Έτσι στον $\mathbb{Q}[x]$ ισχύει ότι

$$x^5-1=(x-1)\Phi_5(x)$$

είναι η ανάλυση του x^5-1 σε γινόμενο ανάγωγων παραγόντων. Εάν ο n δεν είναι πρώτος, τότε $x^{n-1}+x^{n-2}+\cdots+x+1$ δεν είναι ανάγωγο πολυώνυμο του $\mathbb{Q}[x]$. Για παράδειγμα όταν $n=4$, τότε $x^3+x^2+x+1=(x+1)(x^2+1)$ και

$$x^4-1=(x-1)(x+1)(x^2+1)$$

είναι η ανάλυση του x^4-1 σε γινόμενο ανάγωγων πολυωνύμων στον $\mathbb{R}[x]$ αλλά και στον $\mathbb{Q}[x]$. Παρατηρούμε ότι $\omega=e^{2\pi i/4}=e^{\pi i/2}=i$ είναι ρίζα του ανάγωγου πολυωνύμου x^2+1, που βέβαια είναι παράγοντας του x^3+x^2+x+1. Τονίζουμε ότι από τη γραφική παράσταση των ριζών της μονάδας, όταν ο n είναι περιττός φυσικός αριθμός, προκύπτει ότι το $x^{n-1}+x^{n-2}+\cdots+x+1$ δεν έχει πραγματικές ρίζες, άρα δεν έχει ανάγωγο παράγοντα βαθμού ένα στον $\mathbb{Q}[x]$ και στον $\mathbb{R}[x]$. Περισσότερα στοιχεία για αυτά τα πολυώνυμα θα δούμε στο Εδάφιο 5.

Ας θεωρήσουμε γενικότερα ένα ανάγωγο πολυώνυμο $p(x)\in F[x]$. Όπως είδαμε το ιδεώδες $\langle p(x)\rangle$ είναι μέγιστο και ο δακτύλιος $F[x]/\langle p(x)\rangle$ είναι σώμα. Αντίστροφα παρατηρούμε ότι τα πρώτα ιδεώδη I του $F[x]$ είναι ακριβώς εκείνα για τα οποία ο δακτύλιος πηλίκο $F[x]/I$ είναι ακέραια περιοχή. Κάθε πρώτο ιδεώδες $I\neq 0$ του $F[x]$ έχει γεννήτορα ένα πρώτο στοιχείο $p(x)$ του $F[x]$. Όμως, το $p(x)$ είναι ανάγωγο στον $F[x]$. Επομένως κάθε πρώτο μη μηδενικό ιδεώδες του $F[x]$ είναι μέγιστο και έχει γεννήτορα ένα ανάγωγο πολυώνυμο.

Για το ανάγωγο πολυώνυμο $p(x)$ του $F[x]$ η απεικόνιση

$$\phi:\ F\to F[x]/\langle p(x)\rangle,\ c\mapsto c+\langle p(x)\rangle \tag{1.2.7.2}$$

είναι ένας μονομορφισμός σωμάτων, (βλ. άσκηση 1.5.14). Επομένως το σώμα F εμφυτεύεται στο σώμα $F[x]/\langle p(x)\rangle$ και το $F[x]/\langle p(x)\rangle$ είναι επέκταση του F *μέσω* αυτής της εμφύτευσης. Με αυτό εννοούμε ότι το $F[x]/\langle p(x)\rangle$ είναι επέκταση του σώματος $\phi(F)$. Θα διευκρινίσουμε τα παραπάνω με δύο παραδείγματα.

Παραδείγματα 1.2.8.

1. Το ιδεώδες $I=\langle x^2+1\rangle$ είναι μέγιστο στον $\mathbb{R}[x]$. Το σώμα $\mathbb{R}[x]/I$ είναι επέκταση του $\mathbb{R}$ μέσω της εμφύτευσης:

   $$\phi:\ \mathbb{R}\to\mathbb{R}[x]/I,\ \phi(r)=r+I.$$

   Τα στοιχεία του $\mathbb{R}[x]/I$ είναι της μορφής $f(x)+I$. Σύμφωνα, όμως, με τον Ευκλείδειο αλγόριθμο διαίρεσης:

   $$f(x)=(x^2+1)q(x)+r(x),\ \text{όπου } r(x)\in\mathbb{R}[x], \deg r(x)\leq 1$$

   και επομένως $f(x)+I=r(x)+I$. Άρα τα στοιχεία του $\mathbb{R}[x]/I$ είναι της μορφής $a+bx+I$, $a,b\in\mathbb{R}$. Παρατηρούμε επίσης ότι το I είναι ο πυρήνας του επιμορφισμού δακτυλίων

   $$\mathbb{R}[x]\to\mathbb{C},\ f(x)\mapsto f(i).$$

Άρα η συνάρτηση

$$\psi:\ \mathbb{R}[x]/I \to \mathbb{C},\ f(x)+I \mapsto f(i)$$

είναι ισομορφισμός σωμάτων και μάλιστα παρατηρούμε ότι

$$\psi(a+bx+I) = a+bi.$$

Έτσι η συνάρτηση

$$\psi\circ\phi:\ \mathbb{R}\to\mathbb{C},\quad \psi\circ\phi\ (r) = \psi(r+I) = r$$

είναι εμφύτευση του $\mathbb{R}$ στο $\mathbb{C}$.

2. Έστω τώρα το ιδεώδες $I = \langle x^2-3\rangle$ του $\mathbb{Q}[x]$. Ο δακτύλιος $E = \mathbb{Q}[x]/I$ είναι σώμα, αφού το πολυώνυμο x^2-3 είναι ανάγωγο στον $\mathbb{Q}[x]$. Τα στοιχεία του E είναι της μορφής $f(x)+I$, όπου $f(x)\in\mathbb{Q}[x]$. Σύμφωνα με τον Ευκλείδειο αλγόριθμο διαίρεσης, ισχύει
$$f(x) = (x^2-3)q(x)+r(x),$$
όπου $r(x)\in\mathbb{Q}[x]$, $\deg r(x)\le 1$. Επομένως

$$E = \{ax+b+I:\ a,b\in\mathbb{Q}\}.$$

Το σώμα E είναι επέκταση του $\mathbb{Q}$ μέσω της εμφύτευσης $c\mapsto c+I$. Στη συνέχεια θα δούμε πώς υπολογίζουμε το αντίστροφο στοιχείου του E^*. Θα ξεκινήσουμε με το αντίστροφο του x^2+I στον E. Αφού $x^2+I = 3+I$ έπεται ότι

$$\frac{1}{3}(x^2+I) = \frac{1}{3}x^2+I = 1+I \Rightarrow (x^2+I)\left(\frac{1}{3}+I\right) = 1+I,$$

άρα

$$(x^2+I)^{-1} = \frac{1}{3}+I.$$

Στη γενική περίπτωση, παρατηρούμε ότι αν $r(x), f(x), g(x)\in\mathbb{Q}(x)$ έτσι ώστε

$$f(x)r(x)+g(x)(x^2-3) = 1,\ \text{τότε}\ f(x)r(x)+I = 1+I \tag{1.2.8.1}$$

και άρα

$$(r(x)+I)^{-1} = f(x)+I.$$

Αν για δοθέν $r(x)$ ισχύει ότι $r(x)+I\neq I$, τότε τα πολυώνυμα $f(x), g(x)\in\mathbb{Q}(x)$ της σχέσης (1.2.8.1) υπάρχουν, σύμφωνα με το Θεώρημα II.11 του Παραρτήματος. Θα εφαρμόσουμε τα παραπάνω για να υπολογίσουμε το $(r(x)+I)^{-1}$, όπου $r(x) = x+2$. Σύμφωνα με τον Ευκλείδειο αλγόριθμο διαίρεσης του x^2-3 με το $x-2$ βρίσκουμε ότι:

$$x^2-3 = (x-2)(x+2)+1\ \Rightarrow\ (2-x)(x+2)+(x^2-3) = 1$$

και άρα

$$(x+2+I)^{-1} = -x+2+I.$$

Τα πολυώνυμα στα δύο προηγούμενα παραδείγματα δεν είχαν ρίζες στο σώμα ορισμού τους. Η επόμενη πρόταση δείχνει ότι σε κάθε περίπτωση ο αριθμός ριζών ενός πολυωνύμου με συντελεστές από ένα σώμα δεν μπορεί να υπερβαίνει τον βαθμό του.

Πρόταση 1.2.9. *Έστω $f(x) \in F[x]$, όπου F σώμα και $\deg f(x) = n < \infty$. Τότε το $f(x)$ έχει το πολύ n ρίζες στο F.*

Απόδειξη. Αν $f(x)$ έχει s ρίζες, έστω $a_1, \ldots, a_s$, τότε εφαρμόζοντας διαδοχικά την Πρόταση 1.2.2 έπεται ότι $f(x) = (x - a_1) \cdots (x - a_s)g(x)$, για κάποιο πολυώνυμο $g(x) \in F[x]$. Συγκρίνοντας τους βαθμούς των πολυωνύμων των δύο μελών προκύπτει ότι $s \leq n$. □

Ο παρακάτω ορισμός αφορά την περίπτωση που το πολυώνυμο $f(x) \in F[x]$, βαθμού n, έχει ακριβώς n ρίζες (μετρημένες με τη πολλαπλότητά τους) στο F.

Ορισμός 1.2.10. *Λέμε ότι το $f(x) \in F[x]$, όπου F σώμα, με $\deg f(x) = n$* ***αναλύεται σε γινόμενο γραμμικών παραγόντων*** *(splits) στον $F[x]$ αν*

$$f(x) = c(x - a_1) \cdots (x - a_n),$$

όπου $c, a_1, \ldots, a_n \in F$.

1.3 Ανάγωγα πολυώνυμα

Έστω ότι F είναι σώμα. Στην Πρόταση 1.2.6 δώσαμε ένα κριτήριο για πολυώνυμα βαθμού ≤ 3 ώστε να είναι ανάγωγα. Παρακάτω θυμίζουμε κάποια χρήσιμα κριτήρια κυρίως για πολυώνυμα στον δακτύλιο $\mathbb{Q}[x]$ ώστε να είναι ανάγωγα. Για τις αποδείξεις που παραλείπουμε, ο αναγνώστης μπορεί να συμβουλευτεί τα [3, Ενότητες 4.6, 6.1] και [2, Ενότητες 9.4, 9.5]. Ξεκινάμε με το Κριτήριο του Gauss. Το θεώρημα αυτό αφορά ***πρωταρχικά*** (primitive) πολυώνυμα, δηλ. πολυώνυμα του $\mathbb{Z}[x]$ της μορφής $a_n x^n + \cdots + a_0$ με την ιδιότητα ΜΚΔ$(a_0, \ldots, a_n) = 1$.

Θεώρημα 1.3.1 (Κριτήριο του Gauss). *Έστω ότι $f(x) = a_n x^n + \cdots + a_0 \in \mathbb{Z}[x]$ είναι πρωταρχικό πολυώνυμο και έστω ότι $\deg f(x) > 0$. Τότε το $f(x)$ είναι ανάγωγο στον $\mathbb{Z}[x]$ αν και μόνο αν το $f(x)$ είναι ανάγωγο στον $\mathbb{Q}[x]$.*

Η επόμενη πρόταση είναι χρήσιμη για την εύρεση ριζών ενός πολυωνύμου με ακέραιους συντελεστές.

Πρόταση 1.3.2. *Έστω ότι $f(x) = a_n x^n + \cdots + a_0 \in \mathbb{Z}[x]$, $\deg f(x) = n$.*

$$\text{Αν } \frac{r}{s} \in \mathbb{Q},\ \text{ΜΚΔ}(r, s) = 1 \text{ και } f(\frac{r}{s}) = 0,\ \text{τότε } r | a_0 \text{ και } s | a_n.$$

Ιδιαίτερα, αν το $f(x)$ είναι κανονικό πολυώνυμο και $f(a) \neq 0$, για όλους τους ακέραιους a που διαιρούν το a_0, τότε το $f(x)$ δεν έχει ρίζες στο σώμα $\mathbb{Q}$.

Σημειώνουμε επίσης την παρακάτω πρόταση, συνέπεια του κριτηρίου του Gauss.

Πρόταση 1.3.3. *Έστω $f(x) \in \mathbb{Z}[x]$ κανονικό πολυώνυμο. Η ανάλυση*

$$f(x) = f_1(x) \cdots f_s(x)$$

σε γινόμενο αναγώγων παραγόντων στον $\mathbb{Z}[x]$ είναι επίσης η ανάλυση του $f(x)$ σε γινόμενο αναγώγων παραγόντων στον $\mathbb{Q}[x]$.

Παραδείγματα 1.3.4.

1. Έστω το κανονικό πολυώνυμο $f(x) = x^3 - 3x - 1$. Οι μόνοι ακέραιοι διαιρέτες του σταθερού όρου είναι οι ± 1. Αφού $f(\pm 1) \neq 0$, σύμφωνα με την Πρόταση 1.3.2, έπεται ότι το $f(x)$ δεν έχει ρίζες στο $\mathbb{Q}$. Αφού $\deg f(x) = 3$, έπεται ότι το $f(x)$ είναι ανάγωγο στον $\mathbb{Q}[x]$, σύμφωνα με την Πρόταση 1.2.6.
2. Έστω $n \in \mathbb{Z}$ έτσι ώστε $\sqrt{n} \notin \mathbb{Q}$. Για παράδειγμα έστω n πρώτος φυσικός αριθμός. Το πολυώνυμο $x^2 - n$ δεν έχει ρίζα στο $\mathbb{Q}$, σύμφωνα με την Πρόταση 1.3.2, και κατά συνέπεια είναι ανάγωγο στον δακτύλιο $\mathbb{Q}[x]$, σύμφωνα με την Πρόταση 1.2.6. Αντίστοιχα συμπεράσματα έχουμε για το πολυώνυμο $x^3 - n$ όταν $\sqrt[3]{n} \notin \mathbb{Q}$.

Το επόμενο θεώρημα είναι γνωστό ως Κριτήριο του Eisenstein.

Θεώρημα 1.3.5 (Κριτήριο του Eisenstein). *Έστω ότι το $f(x) = a_n x^n + \cdots + a_0 \in \mathbb{Z}[x]$ και $p \in \mathbb{Z}$ φυσικός πρώτος αριθμός. Αν ο p διαιρεί τους συντελεστές a_i, για $i = 0, \ldots, n-1$, δεν διαιρεί, όμως, τον a_n, ενώ ο p^2 δεν διαιρεί τον a_0, τότε το πολυώνυμο $f(x)$ είναι ανάγωγο στον δακτύλιο $\mathbb{Q}[x]$.*

Θα εφαρμόσουμε το Κριτήριο του Eisenstein στο επόμενο παράδειγμα:

Παράδειγμα 1.3.6. Έστω το πολυώνυμο

$$f(x) = \frac{2}{9}x^5 + \frac{5}{3}x^4 + x^3 + \frac{1}{3} \in \mathbb{Q}[x].$$

Παρατηρούμε ότι το $f(x)$ είναι ανάγωγο στον $\mathbb{Q}[x]$ αν και μόνο αν το

$$9f(x) = 2x^5 + 15x^4 + 9x^3 + 3$$

είναι ανάγωγο στον δακτύλιο $\mathbb{Q}[x]$. Το κριτήριο του Eisenstein (για $p = 3$) ισχύει για το πολυώνυμο $9f(x)$ και επομένως το $9f(x)$ είναι ανάγωγο στον $\mathbb{Q}[x]$. Κατά συνέπεια το πολυώνυμο $f(x)$ είναι ανάγωγο στον $\mathbb{Q}[x]$.

Σημειώνουμε επίσης την επόμενη πρόταση.

Πρόταση 1.3.7. *Έστω F σώμα και $f(x) \in F[x]$. Το πολυώνυμο $f(x)$ είναι ανάγωγο στον δακτύλιο $F[x]$ αν και μόνο αν $g(x) = f(ax + b)$ είναι ανάγωγο στον $F[x]$, όπου $a, b \in F$ και $a \neq 0$. Το πολυώνυμο $f(x)$ είναι ανάγωγο στον $F[x]$ αν και μόνο αν $cf(x)$ είναι ανάγωγο στον $F[x]$, όπου $c \in F^*$.*

Η πρόταση αυτή μπορεί να χρησιμοποιηθεί όταν το κριτήριο του Eisenstein δεν εφαρμόζεται άμεσα.

Παράδειγμα 1.3.8. Έστω p πρώτος φυσικός αριθμός. Θα δείξουμε ότι το πολυώνυμο $\Phi_p(x) = x^{p-1} + x^{p-2} + \cdots + x + 1 \in \mathbb{Q}[x]$ είναι ανάγωγο, εφαρμόζοντας το κριτήριο του Eisenstein στο $\Phi_p(x+1)$ για τον πρώτο p. Πράγματι

$$\Phi_p(x)(x-1) = x^p - 1,$$

άρα

$$\Phi_p(x+1)\big((x-1)+1\big) = (x+1)^p - 1 \Rightarrow \Phi_p(x+1)x = (x+1)^p - 1.$$

Επομένως

$$\Phi_p(x+1) = \frac{(x+1)^p - 1}{x} = \frac{x^p + \binom{p}{1}x^{p-1} + \binom{p}{2}x^{p-2} + \cdots + \binom{p}{p-1}x + 1 - 1}{x}$$

$$= x^{p-1} + \binom{p}{1}x^{p-2} + \cdots + \binom{p}{p-1} = x^{p-1} + px^{p-2} + \cdots + p.$$

Αφού ο p είναι πρώτος, έπεται ότι $p|\binom{p}{n}$, για $n = 1, \ldots, p-1$. Το κριτήριο του Eisenstein (για τον p) αποδεικνύει ότι το πολυώνυμο $\Phi_p(x+1)$ είναι ανάγωγο στον $\mathbb{Q}[x]$. Έτσι σύμφωνα με την Πρόταση 1.3.2 το πολυώνυμο $\Phi_p(x)$ είναι ανάγωγο στον $\mathbb{Q}[x]$.

Το επόμενο κριτήριο ανάγει το πρόβλημα της αναγωγιμότητας του $f(x) \in \mathbb{Z}[x]$ σε αντίστοιχο πρόβλημα στον δακτύλιο $\mathbb{Z}_p[x]$, όπου p πρώτος φυσικός αριθμός. Θεωρούμε τον φυσικό ομομορφισμό

$$\psi : \mathbb{Z} \to \mathbb{Z}_p,\ a \mapsto \bar{a} \equiv a \bmod p.$$

Ο ψ επεκτείνεται στον ομομορφισμό δακτυλίων

$$\Psi : \mathbb{Z}[x] \to \mathbb{Z}_p[x],\ a_0 + a_1x + \cdots + a_nx^n \mapsto \overline{a_0} + \overline{a_1}x + \cdots + \overline{a_n}x^n.$$

Παρατηρούμε ότι ο βαθμός του $\Psi(f(x))$ είναι ίσος με τον βαθμό του $f(x)$ αν και μόνο αν ο συντελεστής του μεγιστοβάθμιου όρου του $f(x)$ δε διαιρείται από το p.

Πρόταση 1.3.9. *Έστω $f(x) \in \mathbb{Z}[x]$, p πρώτος φυσικός αριθμός, έτσι ώστε $\deg f(x)$ να ισούται με τον $\deg \Psi(f(x))$. Αν το $\Psi(f(x))$ είναι ανάγωγο στον $\mathbb{Z}_p[x]$, τότε το $f(x)$ είναι ανάγωγο στον δακτύλιο $\mathbb{Q}[x]$.*

Το πλεονέκτημα αυτού του κριτηρίου βρίσκεται στο γεγονός ότι ο δακτύλιος $\mathbb{Z}_p$ είναι πεπερασμένο σώμα και επομένως η εύρεση παραγόντων αλλά και ριζών του $\Psi(f(x))$ είναι ευκολότερη εργασία. Για τα πολυώνυμα στο επόμενο παράδειγμα θα γράφουμε για λόγους απλότητας και συντομίας m για να εννοούμε τον ακέραιο m όταν είμαστε στον δακτύλιο $\mathbb{Q}[x]$ αλλά και το στοιχείο $\overline{m}$ όταν είμαστε στον δακτύλιο $\mathbb{Z}_p[x]$.

Παραδείγματα 1.3.10.

1. Σύμφωνα με την Πρόταση 1.2.6, τα πολυώνυμα x^2+x+1, x^3+x+1 και x^3+x^2+1 είναι ανάγωγα στον $\mathbb{Z}_2[x]$, αφού δεν έχουν ρίζες στο $\mathbb{Z}_2$. Σύμφωνα με το Παράδειγμα 1.3.8 τα πολυώνυμα x^2+x+1, x^3+x+1 και x^3+x^2+1 είναι ανάγωγα στον $\mathbb{Q}[x]$.
2. Το πολυώνυμο x^2+1 δεν είναι ανάγωγο στον $\mathbb{Z}_2[x]$, αφού $x^2+1 = (x+1)^2$ στον $\mathbb{Z}_2[x]$. Είναι, όμως, ανάγωγο στον $\mathbb{Z}[x]$. Το αντίστροφο, λοιπόν, της Πρότασης 1.3.9 δεν ισχύει.
3. Εξετάζοντας όλα τα πολυώνυμα βαθμού 2 και 3 στον $\mathbb{Z}_2[x]$ (υπάρχουν 12 τέτοια πολυώνυμα) και σύμφωνα με την Πρόταση 1.2.6, προκύπτει ότι τα ανάγωγα πολυώνυμα βαθμού ≤ 3 του $\mathbb{Z}_2[x]$ είναι τα

   $$x,\ x+1,\ x^2+x+1,\ x^3+x+1,\ x^3+x^2+1,$$

   εφόσον είναι τα μόνα πολυώνυμα βαθμού ≤ 3 που δεν έχουν ρίζες στον $\mathbb{Z}_2$.

   Υπάρχουν 2^4 πολυώνυμα βαθμού 4 στον $\mathbb{Z}_2[x]$. Θα δείξουμε ότι το x^4+x+1 είναι ανάγωγο στον $\mathbb{Z}_2[x]$. Αφού ο $\mathbb{Z}_2[x]$ είναι Π.Κ.Ι. συμπεραίνουμε ότι αν x^4+x+1 δεν ήταν ανάγωγο, τότε θα είχε έναν ανάγωγο παράγοντα βαθμού 1 ή 2. Αφού όμως x^4+x+1 δεν έχει ρίζες στο $\mathbb{Z}_2$ έπεται ότι x^4+x+1 δεν έχει ανάγωγο παράγοντα βαθμού 1. Μένει να εξετάσουμε αν το x^4+x+1 διαιρείται από το x^2+x+1 στον $\mathbb{Z}_2[x]$. Σύμφωνα με τον Ευκλείδειο Αλγόριθμο Διαίρεσης προκύπτει ότι:

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

και άρα το x^4+x+1 δεν έχει ανάγωγο παράγοντα στον $\mathbb{Z}_2[x]$ βαθμού 2. Από τα παραπάνω βλέπουμε ότι το x^4+x+1 είναι ανάγωγο στον $\mathbb{Z}_2[x]$. Σύμφωνα με την Πρόταση 1.3.9 το πολυώνυμο x^4+x+1 είναι ανάγωγο στον $\mathbb{Q}[x]$. Συμπεραίνουμε επίσης ότι το πολυώνυμο $x^4+11x-1$ είναι και αυτό ανάγωγο στον $\mathbb{Q}[x]$, αφού στον $\mathbb{Z}_2[x]$ μας δίνει και αυτό το ίδιο πολυώνυμο x^4+x+1.

4. Το πολυώνυμο $f(x)=x^4-10x+1\in\mathbb{Z}[x]$ δεν είναι ανάγωγο στον $\mathbb{Z}_p[x]$ για $p<17$, είναι, όμως, ανάγωγο στον $\mathbb{Z}_{17}[x]$ και άρα είναι ανάγωγο στον $\mathbb{Q}[x]$.

Απομονώνουμε μία παρατήρηση που χρησιμοποιήσαμε στο παραπάνω παράδειγμα.

Παρατήρηση 1.3.11. *Έστω F σώμα και $f(x)\in F[x]$. Αφού ο $F[x]$ είναι Π.Κ.Ι., το πολυώνυμο $f(x)$ είναι ανάγωγο στον $F[x]$ αν και μόνο αν το $f(x)$ δεν έχει ανάγωγο παράγοντα βαθμού μικρότερου ή ίσου του ημίσεως του* $\deg f(x)$.

Η παρατήρηση αυτή είναι ιδιαίτερα χρήσιμη, όταν το σώμα F είναι πεπερασμένο και το σύνολο των ανάγωγων πολυωνύμων σε κάθε βαθμό είναι πεπερασμένο.

1.4 Σώμα Ανάλυσης ενός πολυωνύμου

Έστω ότι το F είναι σώμα. Στο εδάφιο αυτό εξετάζουμε τις ρίζες ενός πολυωνύμου $f(x)\in F[x]$ σε σχέση με επεκτάσεις του σώματος F. Στόχος μας είναι να αναζητήσουμε μία επέκταση E του F έτσι ώστε το πολυώνυμο $f(x)$, όταν το θεωρούμε ως πολυώνυμο του $E[x]$, να έχει όλες του τις ρίζες στο E, δηλ. να αναλύεται σε γινόμενο γραμμικών παραγόντων στον $E[x]$. Το Θεμελιώδες Θεώρημα της Άλγεβρας διαβεβαιώνει ότι αν $F=\mathbb{Q}$, τότε το σώμα $\mathbb{C}$ περιέχει όλες τις ρίζες του $f(x)$. Τι συμβαίνει, όταν το F είναι τυχαίο σώμα; Σε κάθε περίπτωση, πώς μπορούμε να εντοπίσουμε το μικρότερο σώμα που περιέχει όλες τις ρίζες του $f(x)$; Αυτό θα επιτευχθεί στο επόμενο κεφάλαιο.

Παραδείγματα 1.4.1.

1. Το πολυώνυμο $x^2+1\in\mathbb{R}[x]$ αναλύεται σε γινόμενο γραμμικών παραγόντων στον $\mathbb{C}[x]$ ως $x^2+1=(x-i)(x+i)$. Είναι φανερό ότι δεν υπάρχει σώμα F έτσι ώστε $\mathbb{R}\subsetneqq F\subsetneqq\mathbb{C}$ που να περιέχει τις ρίζες $\pm i$. Πράγματι, αν $\mathbb{R}\subset F$ και $i\in F$, τότε $a+bi\in F$, για $a,b\in\mathbb{R}$, και άρα $F=\mathbb{C}$.
2. Έστω τώρα το σώμα $E=\mathbb{R}[y]/I$, όπου I το ιδεώδες $\langle y^2+1\rangle$ του $\mathbb{R}[y]$. Είδαμε στο Παράδειγμα 1.2.8.1 ότι $E\cong\mathbb{C}$. Θα θεωρήσουμε στη συνέχεια τον δακτύλιο $E[x]$. Θα δούμε ότι το πολυώνυμο $f(x)=x^2+1\in E[x]$ αναλύεται σε γινόμενο γραμμικών παραγόντων στον $E[x]$. Σημειώνουμε ότι το μοναδιαίο στοιχείο του E είναι το $1+I$. Όπου χρειάζεται, χρησιμοποιούμε δείκτες για να τονίσουμε το σώμα στο οποίο ανήκουν τα στοιχεία μας. Έτσι $1_E=1_{\mathbb{R}}+I$ και δίνοντας αυτήν την έμφαση γράφουμε $f(x)=x^2+1_E$. Έστω $a=y+I$. Αφού

$$-y^2+I=1_{\mathbb{R}}+I=1_E,$$

έχουμε ότι

$$(x-a)(x+a)=(x-(y+I))(x+(y+I))=(x-y+I)(x+y+I)=\\ =x^2-y^2+I=x^2+1_E=f(x).$$

Από τα παραπάνω έπεται ότι τα $\pm a$ είναι οι δύο ρίζες του $f(x)$ στο E, δηλ. το $f(x)$ αναλύεται σε γινόμενο γραμμικών παραγόντων στο $E[x]$.

3. Έστω $E = \mathbb{Q}[y]/I$, όπου $I = \langle y^2 - 3\rangle$. Αφού το $y^2 - 3$ είναι ανάγωγο στον $\mathbb{Q}[y]$, ο δακτύλιος E είναι σώμα. Έστω $b = y + I$. Όπως στο προηγούμενο παράδειγμα ο αναγνώστης καλείται να δείξει ότι στον $E[x]$ το πολυώνυμο $x^2 - 3 \in E[x]$ αναλύεται σε γινόμενο γραμμικών παραγόντων:

$$x^2 - 3 = (x - b)(x + b).$$

Σημειώνουμε ότι έχουμε ταυτίσει τα στοιχεία του $\mathbb{Q}$ με την εμφύτευσή τους στο E. Έτσι ο σταθερός όρος του $f(x)$ είναι, στην πραγματικότητα, το στοιχείο $3 + I$ του E.

Έστω F ένα σώμα, $p(y)$ ένα ανάγωγο πολυώνυμο του $F[y]$, $I = \langle p(y)\rangle$ και E το σώμα $F[y]/I$. Η εμφύτευση (1.2.7.2) $F \to E$, $c \mapsto c + I$, μετατρέπει το σώμα E σε F διανυσματικό χώρο, όπου

$$c \cdot (f(x) + I) := cf(x) + I.$$

Το Θεώρημα 1.4.2 γενικεύει τα προηγούμενα παραδείγματα.

Θεώρημα 1.4.2. *Έστω F ένα σώμα και $p(x)$ ένα ανάγωγο πολυώνυμο του $F[x]$. Τότε το $p(x)$ έχει μία ρίζα στο $F[y]/\langle p(y)\rangle$.*

Απόδειξη. Έστω ότι $I = \langle p(y)\rangle$ και $E = F[y]/I$. Παρατηρούμε ότι το $y + I \in E$ είναι ρίζα του $p(x)$. Πράγματι έστω ότι $p(x) = a_0 + a_1x + \cdots + a_nx^n \in F[x]$. Τότε

$$p(y + I) = a_0(1 + I) + a_1(y + I) + \cdots + a_n(y + I)^n$$

$$= (a_0 + I) + (a_1y + I) + \cdots + (a_ny^n + I) = p(y) + I = I.$$

□

Το επόμενο θεώρημα είναι γνωστό ως Θεώρημα του Kronecker.

Θεώρημα 1.4.3 (Kronecker). *Έστω $f(x) \in F[x]$, όπου το F είναι σώμα. Υπάρχει μία επέκταση σωμάτων L/F έτσι ώστε το $f(x)$ να αναλύεται σε γραμμικούς παράγοντες στο $L[x]$.*

Απόδειξη. Η απόδειξη γίνεται επαγωγικά ως προς τον βαθμό του $f(x)$. Αν $\deg f(x) = 1$ τότε $L = F$. Έστω ότι $\deg f(x) > 1$ και $f(x) = g(x)p(x)$, όπου τα $p(x), g(x) \in F[x]$ και το $p(x)$ είναι ανάγωγο πολυώνυμο. Αν το $p(x)$ είναι βαθμού 1, τότε το $f(x)$ αναλύεται σε γινόμενο γραμμικών παραγόντων σε ένα σώμα L, αρκεί το $g(x)$ να αναλύεται σε γινόμενο γραμμικών παραγόντων στον L. Όμως, τέτοιο σώμα υπάρχει από την υπόθεση της μαθηματικής επαγωγής, αφού $\deg g(x) = \deg f(x) - 1 < \deg f(x)$.

Τέλος αν $\deg p(x) > 1$, τότε, από το Θεώρημα 1.4.2, υπάρχει μία επέκταση M/F στην οποία το $p(x)$ έχει μία ρίζα, έστω $a \in M$. Άρα $p(x) = (x - a)h(x) \in M[x]$ και $f(x) = (x - a)h(x)g(x) \in M[x]$. Όμως, $\deg h(x)g(x) < \deg f(x)$. Επομένως υπάρχει ένα σώμα L επέκταση του M τέτοιο ώστε το $h(x)g(x)$ να αναλύεται σε γινόμενο γραμμικών παραγόντων. Κατά συνέπεια το $f(x)$ αναλύεται σε γινόμενο γραμμικών παραγόντων στο σώμα L που είναι επέκταση του F. □

Έστω $f(x) \in F[x]$, όπου F είναι ένα σώμα, και έστω L/F μία επέκταση του F τέτοια ώστε το $f(x)$ να αναλύεται σε γραμμικούς παράγοντες στο $L[x]$. Αν $\deg f(x) = n$, τότε στο σώμα L το $f(x)$ έχει την ανάλυση

$$f(x) = c(x - a_1)^{s_1} \cdots (x - a_t)^{s_t},$$

όπου $c \in F$, $a_i \in L$ και $a_i \neq a_J$, για $1 \leq i, j \leq t$. Οι ρίζες του $f(x)$ στο L είναι τα στοιχεία $a_1, \ldots, a_s$ του L. Είναι φανερό ότι το πλήθος των ριζών του $f(x)$ είναι ακριβώς n και $n = s_1 + \cdots + s_t$, συγκρίνοντας τους βαθμούς των πολυωνύμων των δύο μερών. Οι φυσικοί αριθμοί $s_1, \ldots, s_t$ είναι οι ***πολλαπλότητες*** (multiplicities) των ριζών $a_1, \ldots, a_t$ αντίστοιχα. Η Πρόταση 1.4.5 που ακολουθεί είναι χρήσιμη προκειμένου να δούμε αν το $f(x)$ έχει πολλαπλές ρίζες. Χρειαζόμαστε, όμως, πρώτα τον επόμενο ορισμό.

Ορισμός 1.4.4. *Έστω F ένα σώμα και $f(x) = c_n x^n + \cdots + c_1 x + c_o \in F[x]$. **Παράγωγος** (derivative) του $f(x)$ λέγεται το πολυώνυμο*

$$c_1 + 2c_2 + \cdots + nc_n x^{n-1}$$

και συμβολίζεται με $f'(x)$.

Δώσαμε παραπάνω τον ορισμό της παραγώγου ενός πολυωνύμου και δεν τον θεωρήσαμε δεδομένο από τη Μαθηματική Ανάλυση, διότι ένα πολυώνυμο είναι τυπική σειρά και όχι συνάρτηση, βλ. την Ενότητα III του Παραρτήματος. Είναι χρήσιμο να σημειώσουμε ότι το πολυώνυμο $f'(x)$ έχει τις ιδιότητες της παραγώγου από τη Μαθηματική Ανάλυση. Έτσι,

$$(f(x)g(x))' = f'(x)g(x) + f(x)g'(x).$$

Πρόταση 1.4.5. *Έστω $f(x) = c_0 + c_1 x + \cdots + c_n x^n \in F[x]$, όπου F είναι ένα σώμα, και έστω L/F μία επέκταση του F όπου το $f(x)$ αναλύεται σε γινόμενο γραμμικών παραγόντων. Το πολυώνυμο $f(x)$ έχει πολλαπλές ρίζες στο L αν και μόνο αν ΜΚΔ$(f(x), f'(x)) \neq 1$.*

Απόδειξη. Έστω ότι τα πολυώνυμα $q(x), r(x)$ του $F[x]$ είναι τέτοια ώστε, σύμφωνα με τον Ευκλείδειο αλγόριθμο στον $F[x]$, να ισχύει ότι

$$f(x) = f'(x)q(x) + r(x),\ \deg r(x) < \deg f'(x) \text{ ή } r(x) = 0. \tag{1.4.5.1}$$

Αφού $F[x] \subset L[x]$, έπεται ότι $q(x), r(x) \in L[x]$. Επομένως η σχέση 1.4.5.1 ισχύει στον δακτύλιο $L[x]$ και τα πολυώνυμα $q(x), r(x)$ είναι ακριβώς το πηλίκο και το υπόλοιπο που προβλέπει ο Ευκλείδειος αλγόριθμος από τη διαίρεση του $f(x)$ με το $f'(x)$ στον $L[x]$. Παρατηρούμε ότι ο υπολογισμός του ΜΚΔ $(f(x), f'(x))$ προκύπτει με τη χρήση του Ευκλείδειου αλγόριθμου. Έτσι οι ΜΚΔ $(f(x), f'(x))$ στα σώματα F και L ταυτίζονται. Έστω τώρα ότι

$$f(x) = c(x - a_1)^{s_1} \cdots (x - a_t)^{s_t} \in L[x].$$

Παρατηρούμε ότι αν $s_i > 1$, για κάποιο $i \in \{1, \ldots, t\}$, τότε το $x - a_i$ διαιρεί το $f(x)$ και το $f'(x)$ και επομένως,

$$\text{ΜΚΔ}\,(f(x), f'(x)) \neq 1.$$

Το αντίστροφο προκύπτει ανάλογα. □

Έστω ότι το $g(x) \in F[x]$ είναι ανάγωγο και έστω ότι το $g(x)$ αναλύεται σε γινόμενο γραμμικών παραγόντων στην επέκταση L/F. Λέμε ότι το $g(x)$ είναι ***διαχωρίσιμο*** όταν οι ρίζες του του $g(x)$ στο L είναι απλές. Γενικότερα, λέμε ότι το $g(x) \in F[x]$ είναι ***διαχωρίσιμο*** (separable), όταν κάθε ανάγωγος παράγοντας του $g(x)$ έχει απλές ρίζες. Έτσι για παράδειγμα, τα πολυώνυμα x^2+3, $(x-1)^2$ είναι διαχωρίσιμα στον $\mathbb{Q}[x]$. Όπως είδαμε παραπάνω, το ανάγωγο πολυώνυμο $g(x)$ είναι διαχωρίσιμο αν και μόνο αν ο ΜΚΔ $(g(x), g'(x)) = 1$. Όμως, αν οι ρίζες του $f(x)$ είναι απλές σε κάποια επέκταση του F παρατηρούμε ότι τότε θα είναι απλές πάνω από κάθε επέκταση του F.

Πόρισμα 1.4.6. *Έστω F ένα σώμα, $g(x) \in F[x]$ ένα ανάγωγο πολυώνυμο και έστω ότι το $g(x)$ αναλύεται σε γινόμενο γραμμικών παραγόντων στον $L[x]$, όπου L/F μία επέκταση του F. Αν το F έχει χαρακτηριστική 0, τότε το $g(x)$ είναι διαχωρίσιμο.*

Απόδειξη. Αφού η χαρακτηριστική του F είναι 0, έπεται ότι $g'(x) \neq 0$. Σύμφωνα με την υπόθεση, το πολυώνυμο $g(x)$ είναι ανάγωγο στον $F[x]$ και άρα οι μόνοι διαιρέτες του $g(x)$ στο $F[x]$ είναι τα σταθερά μη μηδενικά πολυώνυμα και το ίδιο το $g(x)$. Αφού ο ΜΚΔ $(g(x), g'(x))$ διαιρεί το πολυώνυμο $g(x)$ και $\deg g'(x) = \deg g(x) - 1$ έπεται ότι ΜΚΔ $(g(x), g'(x)) = 1$ Έτσι σύμφωνα με την Πρόταση 1.4.5, όλες οι ρίζες του $g(x)$ είναι απλές. □

Αν το F έχει χαρακτηριστική p, όπου p είναι πρώτος φυσικός αριθμός, τότε πρέπει να είμαστε πιο προσεκτικοί. Παρατηρούμε ότι $g'(x) = 0$ όταν ακριβώς το $g(x)$ είναι της μορφής

$$r_0 + r_1 x^p + \cdots + r_n x^{np},\ r_i \in F.$$

Στην περίπτωση αυτή έχουμε ότι ο ΜΚΔ $(g(x), g'(x)) = g(x)$. Έτσι καταλήγουμε στην παρακάτω πρόταση:

Πόρισμα 1.4.7. *Έστω F ένα σώμα τέτοιο ώστε* $\operatorname{char} F = p$, *$g(x) \in F[x]$ ένα ανάγωγο πολυώνυμο και έστω ότι το $g(x)$ αναλύεται σε γινόμενο γραμμικών παραγόντων στο $L[x]$, όπου L/F μία επέκταση του F. Το πολυώνυμο $g(x)$ δεν είναι διαχωρίσιμο αν και μόνο αν $g(x)$ είναι της μορφής*

$$g(x) = r_0 + r_1 x^p + \cdots + r_n x^{np}.$$

Στα επόμενα παραδείγματα θα αντιμετωπίσουμε τέτοιες περιπτώσεις.

Παραδείγματα 1.4.8.

1. Έστω $f(x) = x^2 + 1 \in \mathbb{Z}_2[x]$. Τότε $f'(x) = 0$ και $f(x) = (x+1)^2$ έχει ρίζα το 1 με πολλαπλότητα 2. Βέβαια, το πολυώνυμο $f(x)$ δεν είναι ανάγωγο στον $\mathbb{Z}_2[x]$.
2. Έστω $f(x) = x^p + x + a \in \mathbb{Z}_p[x]$, όπου p πρώτος, και έστω ότι το $f(x)$ αναλύεται σε γινόμενο γραμμικών παραγόντων στον $L[x]$, όπου L μία επέκταση του $\mathbb{Z}_p$. Αφού $f'(x) = 1$, έπεται ότι οι ρίζες του $f(x)$ στο L είναι απλές.
3. Έστω $F = \mathbb{Z}_2(t)$ το σώμα κλασμάτων του $\mathbb{Z}_2[x]$. Έτσι

$$\mathbb{Z}_2(t) = \left\{ \frac{a(t)}{b(t)} :\ a(t), b(t) \in \mathbb{Z}_2[t], b(t) \neq 0 \right\}.$$

   Το σώμα F έχει χαρακτηριστική 2. Αφού το πολυώνυμο $f(x) = x^2 - t$ δεν έχει ρίζες στο F, βλ. Άσκηση 1.5.15, έπεται ότι το $f(x)$ είναι ανάγωγο στο $F[x]$. Αφού $f'(x) = 0$, έπεται ότι ΜΚΔ $(f(x), f'(x)) = f(x)$ και άρα το $f(x)$ δεν είναι διαχωρίσιμο.

Έστω F ένα σώμα και $f(x) \in F[x]$. Μας ενδιαφέρουν οι *μικρότερες* επεκτάσεις $L/\ F$ με αυτήν την ιδιότητα για ένα συγκεκριμένο πολυώνυμο.

Ορισμός 1.4.9. *Έστω F ένα σώμα, $f(x) \in F[x]$ένα πολυώνυμο και έστω L/F μία επέκταση έτσι ώστε το $f(x)$ να αναλύεται σε γραμμικούς παράγοντες του $L[x]$. Εάν δεν υπάρχει ενδιάμεση επέκταση $F \subsetneqq E \subsetneqq L$ τέτοια ώστε το $f(x)$ να αναλύεται σε γραμμικούς παράγοντες στο $E[x]$, τότε το L λέγεται* ***σώμα ανάλυσης*** *(splitting field) του $f(x)$ πάνω από το F.*

Στο επόμενο κεφάλαιο θα δούμε πως κατασκευάζουμε σώματα ανάλυσης πολυωνύμων, βλ. Θεώρημα 2.2.10.

Παραδείγματα 1.4.10.

α') Το σώμα $\mathbb{C}$ δεν είναι σώμα ανάλυσης του $x^2 - 2$ πάνω από το $\mathbb{Q}$, αφού $x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2})$ αναλύεται σε γραμμικούς παράγοντες στο $\mathbb{R}[x]$.

β') Το σώμα $\mathbb{R}$ είναι σώμα ανάλυσης του $x^2 - 2$ πάνω από το $\mathbb{R}$, αφού $x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2})$ αναλύεται σε γραμμικούς παράγοντες στο $\mathbb{R}[x]$.

1.5 Ασκήσεις

1. Να δείξετε ότι με κανόνα και διαβήτη είναι δυνατές οι επόμενες κατασκευές στο επίπεδο:
   α) να χαράξουμε κάθετη ευθεία σε δοθείσα ευθεία που να περνάει από συγκεκριμένο σημείο επί της αρχικής ευθείας,
   β) να χαράξουμε μεσοκάθετη σε δοθέν ευθύγραμμο τμήμα,
   γ) να χαράξουμε ευθεία παράλληλη σε δοθείσα ευθεία που να περνάει από συγκεκριμένο σημείο εκτός της δοθείσης ευθείας,
   δ) να χαράξουμε τη διχοτόμο δοθείσης γωνίας στο επίπεδο.

2. Να αποδείξετε ότι αν a κατασκευάσιμος, τότε $\sqrt{a}$ είναι κατασκευάσιμος.

3. Να αποδείξετε ότι μία γωνία θ είναι κατασκευάσιμη αν και μόνο αν ο αριθμός $\cos(\theta)$ είναι κατασκευάσιμος. Στη συνέχεια να δείξετε ότι το το $\cos(\theta)$ είναι κατασκευάσιμος αριθμός αν και μόνο αν το $\sin(\theta)$ είναι κατασκευάσιμος αριθμός.

4. Έστω n φυσικός αριθμός. Να αποδείξετε ότι το κανονικό n-γωνο είναι κατασκευάσιμο αν και μόνο αν η γωνία $2\pi i/n$ είναι κατασκευάσιμη και ισοδύναμα αν και μόνο αν αν το σημείο $(\cos(2\pi i/p), \sin(2\pi i/p))$ είναι κατασκευάσιμο.

5. Να εξετάσετε αν τα παρακάτω πολυώνυμα του $\mathbb{Q}[x]$ είναι ανάγωγα:

   - $x^9 + 4x + 6$,
   - $x + 1$,
   - $x^4 + 4$,
   - $8x^3 - 6x - 1$,
   - $x^4 + 1$,
   - $x^7 + 7x + 14$,
   - $(4/3)x^5 + (6/5)x^2 + 2$,
   - $x^5 - 10x + 2$,

6. Να βρείτε όλα τα ανάγωγα πολυώνυμα βαθμού 4 στο $\mathbb{Z}_2[x]$.

7. Εξετάζοντας ανάγωγους παράγοντες βαθμού ένα, δύο και τρία να δείξετε ότι $x^6 + x^3 + 1$ είναι ανάγωγο στο $\mathbb{Z}_2[x]$. Να συμπεράνετε ότι $25x^6 - x^3 + 19$ είναι ανάγωγο στο $\mathbb{Q}[x]$.

8. Να εξετάσετε αν τα παρακάτω πολυώνυμα είναι ανάγωγα:

- $x^4+4 \in Z_3[x]$,
- $x^4+4 \in Z_{13}[x]$,
- $x^2+3 \in Z_7[x]$.

9. Να αποδείξετε ότι $\mathbb{Q}(\sqrt{2}) = \{a+b\sqrt{2} : a,b \in \mathbb{Q}\}$ είναι σώμα. Να δείξετε ότι το πολυώνυμο x^2-5 δεν έχει ρίζες στο $\mathbb{Q}(\sqrt{2})$ και άρα είναι ανάγωγο πολυώνυμο του $\mathbb{Q}(\sqrt{2})[x]$.

10. Να βρείτε ανάγωγο πολυώνυμο βαθμού 12 πάνω από το $\mathbb{Q}$.

11. Να βρείτε ανάγωγο πολυώνυμο βαθμού 12 πάνω από το $\mathbb{Z}_3$.

12. Να βρείτε τους ανάγωγους παράγοντες του $x^7+x^6+\cdots+x+1$ και του $x^8+x^7+\cdots+1$ στους $\mathbb{Q}[x]$, $\mathbb{R}[x]$ και $\mathbb{C}[x]$.

13. Να αποδείξετε ότι $\mathbb{Q}[x]/I$ είναι σώμα, όπου $I = \langle x^4+x^3+x^2+x+1\rangle$. Στη συνέχεια να βρείτε τον αντίστροφο του $2x^5+3+I$.

14. Έστω $p(x)$ ανάγωγο πολυώνυμο του $K[x]$. Να αποδείξετε ότι η απεικόνιση

$$\phi :\ K \to K[x]/\langle p(x)\rangle,\ c \mapsto c+\langle p(x)\rangle$$

είναι ένας μονομορφισμός σωμάτων.

15. Έστω $K = \mathbb{Z}_2(t)$. Να δείξετε ότι το πολυώνυμο $f(x) = x^2 - t \in K[x]$ είναι ανάγωγο. Να βρείτε ένα σώμα ανάλυσης L/K για το πολυώνυμο $f(x)$ και να δείξετε ότι το $f(x)$ έχει μία διπλή ρίζα.

16. Έστω E, F δύο σώματα και έστω $\sigma : E \to F$ ισομορφισμός σωμάτων. Να δείξετε ότι ο σ επεκτείνεται σε έναν ισομορφισμό $\widehat{\sigma}$ των δακτυλίων $E[x]$ και $F[x]$, ως εξής:

$$\widehat{\sigma} : E[x] \to F[x],\ \sum a_i x^i \mapsto \sum \sigma(a_i)x^i\ .$$

Στη συνέχεια να δείξετε ότι αν το E είναι σώμα ανάλυσης του $f(x) \in E[x]$, τότε το F είναι σώμα ανάλυσης του $\widehat{\sigma}(f(x)) \in F[x]$. Τέλος να δείξετε ότι αν το $g(x) \in E[x]$ είναι διαχωρίσιμο, τότε το $\widehat{\sigma}(g(x))$ είναι διαχωρίσιμο.

17. Έστω $p(x), g(x) \in F[x]$ έτσι ώστε το $p(x)$ να είναι ανάγωγο και το $g(x)$ να είναι διαχωρίσιμο. Αν τα $p(x)$ και $g(x)$ έχουν κοινές ρίζες σε ένα σώμα ανάλυσης του $p(x)$, να δείξετε ότι το $p(x)$ είναι διαχωρίσιμο και ότι το $p(x)|g(x)$.

18. Στον τύπο των Ιταλών μαθηματικών για τη ρίζα του τριτοβάθμιου πολυωνύμου, σε ορισμένες περιπτώσεις, εμφανίζεται η τετραγωνική ρίζα ενός αρνητικού ρητού αριθμού και γενικότερα η έκφραση

$$\sqrt[3]{a+bi}+\sqrt[3]{a-bi}\ , \tag{1.5.0.1}$$

όπου $a,b \in \mathbb{R}$. Με υπολογισμούς που έκανε ο Bombelli, σε κάποιες συγκεκριμένες περιπτώσεις, προκύπτει ότι η ρίζα του παραπάνω τύπου είναι πραγματικός αριθμός. Να εντοπίσετε γραφικά στο μιγαδικό επίπεδο τις τρεις ρίζες του μιγαδικού αριθμού $\sqrt[3]{a+bi}$ και στη συνέχεια τις τρεις ρίζες του $\sqrt[3]{a-bi}$. Να δείξετε ότι με κατάλληλη επιλογή ρίζας για κάθε έναν από τους δύο προσθετέους στην έκφραση 1.5.0.1, το άθροισμα είναι πραγματικός αριθμός.

Βιβλιογραφία Κεφαλαίου 1

[1] Βάρσος, Δ., Δεριζιώτης, Δ., Μαλιάκας, Μ., Ταλέλλη Ο., Εμμανουήλ, Ι., Μελάς, Α. *Μία Εισαγωγή στην Άλγεβρα*. ΕΚΠΑ, Εκδ. Σοφία, 2012.

[2] Dummit, D.S., Foote, R.M. *Abstract Algebra*. J. Wiley and Sons, INc, 2004.

[3] Fraleigh, J. *Εισαγωγή στην Άλγεβρα*. Πανεπιστημιακές εκδόσεις Κρήτης, 2011.

[4] Hungerford,T. *Algebra*. Springer, 1974.

[5] Katz, V. *Ιστορία των Μαθηματικών, Μία εισαγωγή*. Πανεπιστημιακές Εκδόσεις Κρήτης, 2013.

[6] Λάκκης, Κ. *Άλγεβρα*. Θεσσαλονίκη, 1980.

[7] Lang, S. *Algebra*. Springer, 2002.

[8] Menini, C. Van Oystaeyen, F. *Abstract Algebra*. Marcel Dekker, 2004.

[9] Page, John D. *Constructions* From Math Open Reference http://www.mathopenref.com/tocs/constructionstoc.html

[10] Πουλάκης, Δ. *Άλγεβρα*. Ζήτη, 2015.

[11] Stewart, I. *Galois Theory*. Champan and Hall, 1973.

Κεφάλαιο 2

Σώματα και βαθμοί επεκτάσεων

Στο κεφάλαιο αυτό μελετούμε τις επεκτάσεις σωμάτων. Ιδιαίτερα σημαντικό εργαλείο για τη μελέτη μας αυτή είναι τα πολυώνυμα, έτσι θα εφαρμόσουμε το περιεχόμενο του Κεφαλαίου 1. Έστω E/F μία επέκταση σωμάτων. Το σώμα E έχει την πρόσθετη δομή του F-διανυσματικού χώρου, με την πράξη του εξωτερικού πολλαπλασιασμού να είναι ο συνήθης πολλαπλασιασμός: $F \times E \to E$, $(c, a) \mapsto ca$. Θα χρησιμοποιήσουμε αυτή τη δομή για να καταλάβουμε καλύτερα το E.

2.1 Αλγεβρικά στοιχεία πάνω από ένα σώμα.

Όταν E/F είναι επέκταση σωμάτων και $f(x) \in F[x]$, τότε το $f(x)$ είναι στοιχείο και του δακτυλίου $E[x]$. Βέβαια, το πολυώνυμο $f(x) \in F[x]$ μπορεί να είναι ανάγωγο στο $F[x]$, αλλά να μην είναι ανάγωγο στο $E[x]$.

Ορισμός 2.1.1. *Έστω E/F επέκταση σωμάτων και $a \in E$. Το a λέγεται **αλγεβρικό** (algebraic) πάνω από το F αν υπάρχει $f(x) \in F[x]$, έτσι ώστε $f(x) \neq 0$ και $f(a) = 0$. Αν το a δεν είναι αλγεβρικό πάνω από το F, τότε το a λέγεται **υπερβατικό** (transcendental) πάνω από το F.*

Παραδείγματα 2.1.2.

1. Αν $a \in E$, τότε το a είναι αλγεβρικό πάνω από το E, αφού είναι ρίζα του $f(x) = x - a \in E[x]$.
2. Το $a = \sqrt{3} \in \mathbb{R}$ είναι αλγεβρικό πάνω από το $\mathbb{Q}$, αφού a είναι ρίζα του $f(x) = x^2 - 3 \in \mathbb{Q}[x]$.
3. Έστω I το ιδεώδες $(y^2 - 3)$ του $\mathbb{Q}[y]$, $E = \mathbb{Q}[y]/I$ και $b = y + i$. Τότε το b είναι ρίζα του πολυωνύμου $x^2 - 3 \in \mathbb{Q}[x]$, βλ. Παράδειγμα 1.4.1.3, και άρα το b είναι αλγεβρικό πάνω από το $\mathbb{Q}$.
4. Έστω $f(x) \in F[x]$ ένα ανάγωγο πολυώνυμο, $I = (f(x))$ και $E = F[x]/I$. Το στοιχείο $x + I \in E$ είναι αλγεβρικό πάνω από το F, βλ. Θεώρημα 1.4.2.
5. Έστω ότι E είναι ενδιάμεσο σώμα της επέκτασης L/F και ότι το $a \in L$ είναι αλγεβρικό πάνω από το F. Υπάρχει, λοιπόν, $0 \neq f(x) \in F[x]$ έτσι ώστε $f(a) = 0$. Αφού το $f(x) \in E[x]$, συμπεραίνουμε ότι το a είναι αλγεβρικό πάνω από το E.
6. Το στοιχείο $i \in \mathbb{C}$ είναι αλγεβρικό πάνω από τα σώματα $\mathbb{R}$ και $\mathbb{Q}$.

7. Έστω $z = a + bi \in \mathbb{C}$, $a, b \in \mathbb{R}$. Τότε $z - a = bi$ και $z^2 - 2az + a^2 = -b^2$. Άρα το z είναι ρίζα του πολυωνύμου $x^2 - 2ax + (a^2 + b^2) \in \mathbb{R}[x]$. Επομένως κάθε στοιχείο του $\mathbb{C}$ είναι αλγεβρικό πάνω από το $\mathbb{R}$. Παρατηρούμε ότι η άλλη ρίζα του πολυωνύμου $x^2 - 2ax + (a^2 + b^2)$ είναι ο συζυγής του z, δηλ. $\bar{z} = a - bi$. Επομένως όταν $z \notin \mathbb{R}$, τότε το πολυώνυμο $x^2 - 2ax + (a^2 + b^2) = x^2 - 2\mathrm{Re}\, z + z\bar{z}$ είναι ανάγωγο, βλ. Πρόταση 1.2.6.
8. Τα στοιχεία $a = \sqrt{2}$ και $b = \sqrt{3} \in \mathbb{R}$ είναι αλγεβρικά πάνω από το $\mathbb{Q}$, αφού είναι ρίζες αντίστοιχα των πολυωνύμων $x^2 - 2$ και $x^2 - 3 \in \mathbb{Q}[x]$. Το γινόμενο $a \cdot b = \sqrt{6}$ είναι αλγεβρικό πάνω από το $\mathbb{Q}$, αφού είναι ρίζα του πολυωνύμου $x^2 - 6 \in \mathbb{Q}[x]$.
9. Το άθροισμα $a + b = \sqrt{2} + \sqrt{3}$ είναι αλγεβρικό πάνω από το $\mathbb{Q}$. Πράγματι έστω $c = a + b = \sqrt{2} + \sqrt{3}$. Τότε $c^2 = 5 + 2\sqrt{6}$, οπότε $c^2 - 5 = 2\sqrt{6}$. Άρα $(c^2 - 5)^2 = 24$ και $c^4 - 10c + 1 = 0$. Επομένως το c είναι ρίζα του πολυωνύμου $f(x) = x^4 - 10x + 1$. Στην επόμενη ενότητα, Παράδειγμα 2.2.13, θα δούμε ότι το $f(x)$ είναι ανάγωγο στο $\mathbb{Q}[x]$ χρησιμοποιώντας τις διαστάσεις κατάλληλων διανυσματικών χώρων.
10. Το $\pi \in \mathbb{R}$ είναι υπερβατικό πάνω από το $\mathbb{Q}$. Η απόδειξη της υπερβατικότητας ενός στοιχείου συνήθως είναι ιδιαίτερα δύσκολη. Η απόδειξη για τον αριθμό π δόθηκε από τον Lindemann το 1882 και στηρίζεται στο ότι ο αριθμός e είναι επίσης υπερβατικός πάνω από το $\mathbb{Q}$, όπως έδειξε ο Hermite το 1873, ενώ $e^{i\pi} = -1$ (βλ. [3, Section1.7] και [5]).
11. Έστω $E = F(x)$ το σώμα κλασμάτων του δακτυλίου $F[x]$. Τότε το $x \in E$ είναι υπερβατικό πάνω από το F, (βλ. άσκηση 2.4.1).

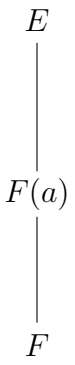
Έστω E/F μία επέκταση σωμάτων και $a \in E$. Για να καταλάβουμε αν το a είναι αλγεβρικό ή υπερβατικό πάνω από το F, θα μελετήσουμε τον μικρότερο δακτύλιο που περιέχει το F και το a.

Ορισμός 2.1.3. *Έστω E/F επέκταση σωμάτων και $a \in E$. Ορίζουμε $F[a]$ και $F(a)$ να είναι τα παρακάτω υποσύνολα του E:*

$$F[a] = \{f(a) : f(x) \in F[x]\},$$

$$F(a) = \left\{ \frac{f(a)}{g(a)} : g(a) \neq 0, f(x), g(x) \in F[x] \right\}.$$

Έστω E/F επέκταση σωμάτων και $a \in E$. Είναι εύκολο να αποδείξουμε ότι το σύνολο $F[a]$ είναι υποδακτύλιος του E, άρα το $F[a]$ είναι ακέραια περιοχή και το $F(a)$ είναι το σώμα κλασμάτων του $F[a]$. Το σώμα $F(a)$ λέγεται ***απλή*** (simple) επέκταση του F.



Σχήμα 2.1: Η απλή επέκταση $F(a)$.

Παρατηρούμε ότι το $F(a)$ είναι το ελάχιστο υπόσωμα του E που περιέχει το F και το a. Επομένως για να δείξουμε ότι η $E/F(a)$ είναι επέκταση σωμάτων, αρκεί να δείξουμε ότι η E/F είναι επέκταση σωμάτων και ότι το $a \in E$. Τέλος, παρατηρούμε ότι αν $F[a]$ είναι σώμα, τότε $F[a] = F(a)$.

Παραδείγματα 2.1.4.

1. Έστω F σώμα. Αν $a \in F$, τότε $F[a] = F(a) = F$.
2. Αφού $i^{2l} = \pm 1$ ενώ $i^{2l+1} = \pm i$, για $l \in \mathbb{N}$, έπεται ότι, για τυχαίο $f(x) \in \mathbb{R}[x]$, ισχύει $f(i) = a + bi$, όπου $a, b \in \mathbb{R}$. Άρα

$$\mathbb{R}[i] = \{a + bi : \ a, b \in \mathbb{R}\} = \mathbb{C} \text{ και επομένως } \mathbb{R}[i] = \mathbb{R}(i).$$

   Μία $\mathbb{R}$-βάση του $\mathbb{R}(i)$ είναι το σύνολο $\{1, i\}$ και $\dim_{\mathbb{R}} \mathbb{R}(i) = 2$.
3. Έστω ότι $\gamma \in \mathbb{C}$ και $\gamma \notin \mathbb{R}$. Τότε $\gamma = a + bi \in \mathbb{C}$, όπου $a, b \in \mathbb{R}$ και $b \neq 0$. Έστω $f(x) = (x - a)/b \in \mathbb{R}[x]$. Τότε

$$i = \frac{\gamma - a}{b} = f(\gamma) \text{ και επομένως } i \in \mathbb{R}[\gamma] \text{ και } \mathbb{R}[i] \subseteq \mathbb{R}[\gamma] \subseteq \mathbb{C}.$$

   Αφού $\mathbb{C} = \mathbb{R}[i]$, προκύπτει ότι $\mathbb{R}[\gamma] = \mathbb{R}[i] = \mathbb{C}$, άρα κάθε $\gamma \in \mathbb{C}$ είναι αλγεβρικό πάνω από το $\mathbb{R}$.
4. Αφού $\sqrt{3}^{2l} = 3^l$ και $\sqrt{3}^{2l+1} = 3^l\sqrt{3}$, για $l \in \mathbb{N}$, έπεται ότι

$$\mathbb{Q}[\sqrt{3}] = \{a + b\sqrt{3} : \ a, b \in \mathbb{Q}\}.$$

   Παρατηρούμε ότι αν κάποιο από τα $a, b \in \mathbb{Q}$ είναι διάφορο του μηδενός, τότε $0 \neq a^2 - 3b^2 \in \mathbb{Q}$ και θέτοντας $c = a^2 - 3b^2$ βλέπουμε ότι:

$$\frac{1}{a + b\sqrt{3}} = \frac{a - b\sqrt{3}}{a^2 - 3b^2} \ = \frac{a}{c} - \frac{b}{c}\sqrt{3} \ \in \mathbb{Q}[\sqrt{3}].$$

   Άρα $\mathbb{Q}(\sqrt{3}) \subset \mathbb{Q}[\sqrt{3}]$ και $\mathbb{Q}[\sqrt{3}] = \mathbb{Q}(\sqrt{3})$. Μία $\mathbb{Q}$-βάση του $\mathbb{Q}(\sqrt{3})$ είναι το σύνολο $\{1, \sqrt{3}\}$ και $\dim_{\mathbb{Q}} \mathbb{Q}(\sqrt{3}) = 2$.
5. Θα μελετήσουμε τον δακτύλιο $\mathbb{Q}[\sqrt[3]{2}]$. Έστω ότι $m \in \mathbb{N}$. Εκφράζουμε το $m = 3l + k$, όπου $k, l \in \mathbb{N}$ και $l \leq 2$. Αφού

$$(\sqrt[3]{2})^m = (\sqrt[3]{2})^{3l+k} = 2^l(\sqrt[3]{2})^k,$$

   έπεται ότι, για τυχαίο $f(x) = \sum c_i x^i \in \mathbb{Q}[x]$, ισχύει

$$f(\sqrt[3]{2}) = a_0 + a_1\sqrt[3]{2} + a_2\sqrt[3]{2}^2 : \quad a_i \in \mathbb{Q}.$$

   Άρα $\mathbb{Q}[\sqrt[3]{2}] = \left\{a_0 + a_1\sqrt[3]{2} + a_2\sqrt[3]{4} : \ a_i \in \mathbb{Q}\right\}$. Το σύνολο $\left\{1, \sqrt[3]{2}, \sqrt[3]{4}\right\}$ παράγει το $\mathbb{Q}[\sqrt[3]{2}]$ ως $\mathbb{Q}$-διανυσματικό χώρο και άρα $\dim_{\mathbb{Q}} \mathbb{Q}[\sqrt[3]{2}] \leq 3$. Στην επόμενη ενότητα θα δούμε ότι $\dim_{\mathbb{Q}} \mathbb{Q}[\sqrt[3]{2}] = 3$.
6. Έστω $E_1 = \mathbb{Q}[\sqrt{2}]$, $E_2 = \mathbb{Q}[\sqrt{2} + \sqrt{3}]$. Θα δείξουμε ότι $E_1 \subsetneqq E_2$. Πράγματι

$$-\sqrt{2} + \sqrt{3} = \frac{1}{\sqrt{2} + \sqrt{3}} \in E_2$$

και

$$\sqrt{2} = \frac{(\sqrt{2}+\sqrt{3}) - (-\sqrt{2}+\sqrt{3})}{2} \in E_2.$$

Άρα $E_1 \subset E_2$. Για να δείξουμε ότι $E_2 \neq E_1$, αρκεί να δείξουμε ότι $\sqrt{2}+\sqrt{3} \notin E_1$. Θα υποθέσουμε ότι $\sqrt{2}+\sqrt{3} \in E_1$ και θα καταλήξουμε σε άτοπο. Έστω, λοιπόν, ότι $\sqrt{2}+\sqrt{3} \in E_1$. Τότε

$$\sqrt{3} = (\sqrt{2}+\sqrt{3}) - (\sqrt{2}) \in E_1.$$

Αφού μία $\mathbb{Q}$-βάση του E_1 είναι το σύνολο $\{1, \sqrt{2}\}$ ενώ $\sqrt{3} \notin \mathbb{Q}$, έπεται ότι

$$\sqrt{3} = a + b\sqrt{2},\ a, b \in \mathbb{Q} \text{ και } b \neq 0. \tag{2.1.4.1}$$

Αν $a = 0$, τότε

$$\sqrt{3} = b\sqrt{2} \Rightarrow 3 = b^2 2,$$

άτοπο, αφού $2 \nmid 3$. Επομένως $ab \neq 0$ στην έκφραση (2.1.4.1) και υψώνοντας στο τετράγωνο

$$3 = a^2 + 2b^2 + 2ab\sqrt{2} \Rightarrow \sqrt{2} = \frac{3-(a^2+2b^2)}{2ab},$$

άτοπο, αφού $\sqrt{2} \notin \mathbb{Q}$.

7. Έστω p πρώτος, $\omega = e^{2\pi i/p}$ και $k \in \mathbb{N}$ έτσι, ώστε ΜΚΔ$(k,p) = 1$. Θα δείξουμε ότι $\mathbb{Q}[\omega] = \mathbb{Q}[\omega^k]$. Ο εγκλεισμός $\mathbb{Q}[\omega^k] \subset \mathbb{Q}[\omega]$ είναι εμφανής, αφού $\omega^k \in \mathbb{Q}[\omega]$. Για τον αντίστροφο εγκλεισμό παρατηρούμε ότι υπάρχουν $r, t \in \mathbb{Z}$ έτσι, ώστε $rp + tk = 1$. Επομένως

$$\omega = \omega^{rp+tk} = \omega^{rp}\,\omega^{tk} = (\omega^k)^t \in \mathbb{Q}[\omega^k] \text{ και } \mathbb{Q}[\omega] \subset \mathbb{Q}[\omega^k].$$

Έστω E/F επέκταση σωμάτων και $a \in E$. Εύκολα μπορεί να ελεγχθεί ότι η συνάρτηση

$$\phi : F[x] \to F[a], \quad \phi(h(x)) = h(a) \tag{2.1.4.2}$$

είναι επιμορφισμός δακτυλίων (βλ. Πρόταση III.5). Παρατηρούμε ότι $\phi(c) = c$, όταν $c \in F$, ενώ $\phi(x) = a$. Έχουμε ακόμα ότι $\ker\phi = \{f(x) \in F[x] :\ f(a) = 0\}$. Σύμφωνα με το Πρώτο Θεώρημα Ισομορφίας Δακτυλίων, προκύπτει ότι $F[x]/\ker\phi \cong \operatorname{Im}\phi = F[a]$. Εφόσον το $F[a]$ είναι ακεραία περιοχή, έπεται ότι $\ker\phi$ είναι πρώτο ιδεώδες.

Πρόταση 2.1.5. *Έστω E/F μία επέκταση σωμάτων και έστω ότι $a \in E$. Το a είναι αλγεβρικό πάνω από το F αν και μόνο αν $F[a] = F(a)$. Όταν το a είναι υπερβατικό πάνω από το F, τότε $F[x] \cong F[a]$ και $\dim_F F[a] = \infty$.*

Απόδειξη. Θεωρούμε τον επιμορφισμό ϕ της σχέσης (2.1.4.2). Έστω ότι το a είναι αλγεβρικό πάνω από το F. Τότε υπάρχει $f(x) \in F[x]$ έτσι ώστε $f(a) = 0$ και $\ker\phi \neq 0$. Ο $\ker\phi$ όπως είδαμε παραπάνω είναι πρώτο ιδεώδες άρα μέγιστο, αφού ο $F[x]$ είναι Π.Κ.Ι. Άρα ο δακτύλιος $F[a] \cong F[x]/\ker\phi$ είναι σώμα. Αφού $F[a] \subset F(a)$ και $F(a)$ είναι το μικρότερο σώμα που περιέχει το F και το a, έπεται ότι $F[a] = F(a)$.

Αν το a είναι υπερβατικό πάνω από το F, τότε $\ker\phi = 0$ και $F[a] \cong F[x]$. Επομένως ο δακτύλιος $F[a]$ δεν είναι σώμα και $\dim_F F[a] = \infty$. □

Στην επόμενη ενότητα θα υπολογίσουμε τη διάσταση του F-διανυσματικού χώρου $F(a)$, όταν το a είναι αλγεβρικό. Θα κλείσουμε αυτήν την ενότητα με έναν ακόμη ορισμό.

Ορισμός 2.1.6. *Έστω E/F μία επέκταση σωμάτων. Ο **βαθμός** (degree) του E πάνω από το F συμβολίζεται με $[E : F]$ και ισούται με τη διάσταση του E ως F-διανυσματικού χώρου.*

Παραδείγματα 2.1.7.

1. Μία βάση του $\mathbb{C}$ ως $\mathbb{R}$-διανυσματικού χώρου είναι το σύνολο $\{1, i\}$ και $[\mathbb{C} : \mathbb{R}] = 2$.
2. Αφού ένα στοιχείο του $\mathbb{Q}[\sqrt{3}]$ γράφεται ως $a \cdot 1 + b \cdot \sqrt{3}$, όπου $a, b \in \mathbb{Q}\}$, έπεται ότι μία βάση του $\mathbb{Q}[\sqrt{3}]$ ως $\mathbb{Q}$-διανυσματικού χώρου είναι το σύνολο $\{1, \sqrt{3}\}$. Επομένως $[\mathbb{Q}[\sqrt{3}] : \mathbb{Q}] = 2$.
3. Παρατηρούμε ότι $\mathbb{R}[\sqrt{3}] = \mathbb{R}$ και επομένως $[\mathbb{R}[\sqrt{3}] : \mathbb{R}] = 1$.
4. $[\mathbb{Q}[\pi] : \mathbb{Q}] = \infty$.
5. Το άπειρο σύνολο $\{1, x, x^2, \ldots\}$ είναι F-βάση του $F[x]$. Αφού το σώμα $F(x)$ περιέχει ως F-υποχώρο τον δακτύλιο $F[x]$, έπεται ότι $\dim_F F(x) \geq \dim_F F[x]$ και άρα $[F(x) : F] = \infty$.

Απομονώνουμε τον συλλογισμό του τελευταίου παραδείγματος.

Πρόταση 2.1.8. *Αν E είναι ενδιάμεσο σώμα της επέκτασης L/F και $[E : F] = \infty$, τότε $[L : F] = \infty$.*

2.2 Αλγεβρικά στοιχεία και διάσταση

Έστω E/F μία επέκταση σωμάτων και $a \in E$ αλγεβρικό πάνω από το F. Στην προηγούμενη ενότητα είδαμε ότι $F[a] = F(a)$ και ότι το σύνολο

$$I = \{f(x) \in F[x] : \ f(a) = 0\}$$

είναι πρώτο ιδεώδες του $F[x]$. Επομένως το $I = \langle g(x) \rangle$, όπου το $g(x)$ είναι ανάγωγο πολυώνυμο του $F[x]$. Άρα, αν $h(x) \in I$, δηλαδή αν $h(a) = 0$, τότε $h(x) = q(x)g(x)$ και στην περίπτωση που $h(x) \neq 0$, τότε $\deg h(x) \geq \deg g(x)$. Επομένως αν $h(x) \in F[x]$ είναι ανάγωγο και $h(a) = 0$, τότε $h(x) = cg(x)$, όπου $c \in F[x]$. Οι παραπάνω παρατηρήσεις οδηγούν στον επόμενο ορισμό.

Ορισμός 2.2.1. *Έστω E/F μία επέκταση σωμάτων και $a \in E$ αλγεβρικό πάνω από το $F[x]$. Το μοναδικό κανονικό ανάγωγο πολυώνυμο του $F[x]$ που έχει το a ως ρίζα, ονομάζεται το **ανάγωγο πολυώνυμο** (irreducible polynomial) του a πάνω από το F και συμβολίζεται με $\mathrm{irr}_{(F,a)}(x)$. Οι ρίζες του $\mathrm{irr}_{(F,a)}(x)$ λέγονται **συζυγή στοιχεία** (conjugates) του a.*

Στα Παραδείγματα 2.2.2 υπολογίζουμε τα ανάγωγα πολυώνυμα σε κάποιες περιπτώσεις.

Παραδείγματα 2.2.2.

1. Έστω $a \in E$. Τότε $\mathrm{irr}_{(E,a)}(x) = x - a$. Αντίστροφα αν $\deg \mathrm{irr}_{(E,a)}(x) = 1$, τότε $a \in E$.
2. Θεωρούμε την επέκταση $\mathbb{R}/\mathbb{Q}$ και το στοιχείο $a = \sqrt{3}$. Αφού $a \notin \mathbb{Q}$, έπεται ότι $\mathrm{irr}_{(E,a)}(x) \geq 2$. Αφού $\sqrt{3}$ είναι ρίζα του $x^2 - 3$, έπεται ότι $\mathrm{irr}_{(\mathbb{Q},a)}(x) = x^2 - 3$.
3. Έστω p πρώτος φυσικός αριθμός και $\omega = e^{2\pi i/p} \in \mathbb{C}$. Όπως σημειώσαμε μετά το Παράδειγμα 1.2.7, το ω είναι ρίζα του $\Phi_p(x) = x^{p-1} + x^{p-2} + \cdots + 1$. Στο Παράδειγμα 1.3.8 αποδείξαμε ότι $\Phi_p(x)$ είναι ανάγωγο πολυώνυμο στο $\mathbb{Q}[x]$. Επομένως $\mathrm{irr}_{(\mathbb{Q},\omega)}(x) = \Phi_p(x) = x^{p-1} + x^{p-2} + \cdots + 1$.

4. Έστω $\omega = e^{2\pi i/8}$. Όπως και παραπάνω το ω είναι ρίζα του $x^7 + x^6 + \cdots + 1$, αλλά το πολυώνυμο αυτό δεν είναι ανάγωγο. Δεν είναι δύσκολο να δείξει κανείς ότι $\mathrm{irr}_{(\mathbb{Q},\omega)}(x) = x^4 + 1$, βλ. άσκηση 2.4.5.
5. Έστω $z = a + bi \in \mathbb{C}$, όπου $b \neq 0$. Τότε $\mathrm{irr}_{(\mathbb{R},z)}(x) = x^2 - 2\mathrm{Re}z + z\bar{z}$, βλ. Παράδειγμα 2.1.2.7.

Στη συνέχεια εξετάζουμε τη διάσταση του $F(a)$ ως F-διανυσματικού χώρου, όταν το a είναι αλγεβρικό πάνω από το F. Υπενθυμίζουμε ότι $F(a) = F[a]$, σύμφωνα με την Πρόταση 2.1.5.

Θεώρημα 2.2.3. *Έστω E/F μία επέκταση σωμάτων, $a \in E$ αλγεβρικό πάνω από το F και $\deg \mathrm{irr}_{(F,a)}(x) = n$. Το σύνολο $\{1, a, \ldots, a^{n-1}\}$ αποτελεί βάση του F-διανυσματικού χώρου $F(a)$ και $[F(a) : F] = n$.*

Απόδειξη. Θέτουμε $f(x) = \mathrm{irr}_{(F,a)}(x)$ και $B = \{1, a, \ldots, a^{n-1}\}$. Έστω $g(a)$ τυχαίο στοιχείο του $F[a]$, όπου $g(x) \in F[x]$. Σύμφωνα με τον Ευκλείδειο αλγόριθμο $g(x) = f(x)p(x) + r(x)$, όπου $p(x), r(x) \in F[x]$ και $t = \deg r(x) < n$. Δηλαδή

$$r(x) = c_t x^t + \cdots + c_1 x + c_0$$

και $c_i \in F$, για $i = 0, \ldots, t$. Παρατηρούμε ότι

$$g(a) = f(a)p(a) + r(a) = r(a) = c_t a^t + \cdots + c_1 a + c_0 \cdot 1$$

και ότι το $g(a)$ είναι F-γραμμικός συνδυασμός στοιχείων του συνόλου B. Θα δείξουμε ότι το σύνολο B είναι γραμμικά ανεξάρτητο. Έστω $d_0 \cdot 1 + \cdots + d_{n-1}a^{n-1} = 0$, $d_i \in F$, για $i = 0, \ldots, n-1$ μία σχέση γραμμικής εξάρτησης των $a^i : 0 \leq i \leq n-1$. Αν $h(x) = d_0 + d_1 x + \cdots + d_{n-1}x^{n-1}$, τότε $h(a) = 0$ και $h(x) \in (f(x))$. Αν $h(x) \neq 0$ οδηγούμαστε σε άτοπο, αφού $\deg h(x) < \deg f(x)$. Επομένως $h(x) = 0$ και άρα $d_i = 0$, για $i = 0, \ldots, n-1$. □

Η απόδειξη του παρακάτω πορίσματος είναι άμεση:

Πόρισμα 2.2.4. *Έστω E/F επέκταση σωμάτων, $a \in E$. Τότε το a είναι αλγεβρικό πάνω από το F αν και μόνο αν $[F(a) : F] < \infty$.*

Για το επόμενο πόρισμα, θεωρούμε γνωστό το Θεμελιώδες Θεώρημα της Άλγεβρας. Σημειώνουμε ότι η απόδειξη του Θεμελιώδους Θεωρήματος της Άλγεβρας, με τα εργαλεία της Θεωρίας Galois, δίνεται στην Ενότητα 6.3 και είναι ανεξάρτητη του Πορίσματος 2.2.5.

Πόρισμα 2.2.5. *Τα ανάγωγα πολυώνυμα του δακτυλίου $\mathbb{R}[x]$ έχουν βαθμό 1 ή 2. Αν $a \in \mathbb{C}$ είναι ρίζα του $f(x) \in \mathbb{R}[x]$, τότε $\bar{a}$ είναι ρίζα του $f(x)$.*

Απόδειξη. Έστω $f(x) \in \mathbb{R}[x]$ ανάγωγο. Σύμφωνα με το Θεμελιώδες Θεώρημα της Άλγεβρας υπάρχει $a \in \mathbb{C}$, τέτοιο ώστε $f(a) = 0$. Επίσης, αφού $f(x)$ είναι ανάγωγο, έπεται ότι $f(x) = c\,\mathrm{irr}_{(\mathbb{R},a)}(x)$, για κάποιο $0 \neq c \in \mathbb{R}$ και ότι

$$\deg f(x) = [\mathbb{R}(a) : \mathbb{R}].$$

Αν, λοιπόν, το a είναι πραγματικός αριθμός, τότε $\mathbb{R}(a) = \mathbb{R}$ και $\deg f(x) = 1$. Αν το $a \notin \mathbb{R}$ τότε, όπως είδαμε στο Παράδειγμα 2.1.4.2, $f(x) = (x-a)(x-\bar{a})$, $\mathbb{R}(a) = \mathbb{C}$ και $\deg f(x) = [\mathbb{C} : \mathbb{R}] = 2$. □

Ιδιαίτερη σημασία έχουν οι επεκτάσεις ενός σώματος F με την ιδιότητα όλα τα στοιχεία τους να είναι αλγεβρικά πάνω από το F.

Ορισμός 2.2.6. *Έστω E/F επέκταση σωμάτων. Το σώμα E λέγεται **αλγεβρικό** πάνω από το E αν κάθε στοιχείο του E είναι αλγεβρικό πάνω από το F και σε αυτήν την περίπτωση η επέκταση E/F λέγεται **αλγεβρική** (algebraic extension).*

Παράδειγμα 2.2.7. Το σώμα $\mathbb{C}$ είναι αλγεβρικό πάνω από το $\mathbb{R}$, βλ. Παράδειγμα 2.1.2.7. Το σώμα $\mathbb{R}$ δεν είναι αλγεβρικό πάνω από το $\mathbb{Q}$, βλ. Παράδειγμα 2.1.2. 10.

Η παρακάτω πρόταση δίνει ένα κριτήριο για να μπορούμε να αποφασίσουμε αν μία επέκταση E/F είναι αλγβερική.

Πρόταση 2.2.8. *Έστω E/F μία επέκταση σωμάτων έτσι ώστε $[E : F] < \infty$. Τότε η επέκταση E/F είναι αλγεβρική.*

Απόδειξη. Έστω ότι $[E : F] = n$ και ότι το a είναι τυχαίο στοιχείο του E. Το σύνολο $\{1, a, \ldots, a^n\}$ έχει $n + 1$ στοιχεία, επομένως είναι γραμμικά εξαρτημένο. Άρα υπάρχει μία σχέση γραμμικής εξάρτησης $d_0 \cdot 1 + \cdots + d_n a^n = 0$, όπου $d_i \in F$, για $i = 0, \ldots, n$ και τουλάχιστον ένα από αυτά δεν είναι μηδέν. Θεωρούμε το μη μηδενικό πολυώνυμο $g(x) = d_0 + d_1 x + \cdots + d_n x^n \in F[x]$. Το a είναι ρίζα του $g(x)$, άρα είναι αλγεβρικό πάνω από το F. □

Το αντίστροφο της Πρότασης 2.2.8 δεν ισχύει, βλ. άσκηση 2.4.14

Ορισμός 2.2.9. *Έστω E/F επέκταση σωμάτων, $a_1, \ldots, a_n \in E$. Ορίζουμε $F[a_1, \ldots, a_n]$ να είναι το σύνολο*

$$F[a_1, \ldots, a_n] = \{f(a_1, \ldots, a_n) : \ f(x_1, \ldots, x_n) \in F[x_1, \ldots, x_n]\}.$$

Αποδεικνύεται εύκολα ότι το $F[a_1, \ldots, a_n]$ είναι υποδακτύλιος του E και άρα ακέραια περιοχή. Συμβολίζουμε με $F(a_1, \ldots, a_n)$ το σώμα κλασμάτων του $F[a_1, \ldots, a_n]$. Είναι φανερό ότι το $F(a_1, \ldots, a_n)$ είναι το ελάχιστο υπόσωμα του E που περιέχει το F και τα στοιχεία $a_1, \ldots, a_n$. Αν $L = F(a_1, \ldots, a_n)$, τότε λέμε ότι τα $a_1, \ldots, a_n$ ***παράγουν την επέκταση*** (generate) E/F ή ότι το L προκύπτει από το F με *επισύναψη* των $a_1, \ldots, a_n$.

Σημειώνουμε ότι

$$F[a_1, \ldots, a_n] = F[a_1, \ldots, a_{n-1}][a_n] \text{ και } F(a_1, \ldots, a_n) = F(a_1, \ldots, a_{n-1})(a_n).$$

Θα δούμε, στο Πόρισμα 2.2.14 παρακάτω, ότι όταν τα $a_1, \ldots, a_n \in E$ είναι αλγεβρικά πάνω από το F , τότε $F[a_1, \ldots, a_n] = F(a_1, \ldots, a_n)$.

Θεώρημα 2.2.10. *Έστω F ένα σώμα και $f(x) \in F[x]$. Τότε υπάρχει επέκταση σωμάτων L/F, τέτοια ώστε $[L : F] < \infty$ και το L να είναι σώμα ανάλυσης του $f(x)$ πάνω από το F.*

Απόδειξη. Από το Θεώρημα 1.4.3, υπάρχει επέκταση E/F, τέτοια ώστε το $f(x)$ να αναλύεται σε γραμμικούς παράγοντες στο $E[x]$. Έστω ότι

$$f(x) = \prod_{i=1}^{n} (x - a_i), \quad a_i \in E$$

είναι η ανάλυση του $f(x)$ σε γινόμενο γραμμικών παραγόντων στο $E[x]$, όπου $n = \deg f(x)$. Θεωρούμε το σώμα $L := F(a_1, \ldots, a_n)$. Είναι φανερό, ότι το σώμα L είναι σώμα ανάλυσης του $f(x)$ πάνω από το F. □

Στο επόμενο κεφάλαιο θα δούμε ότι αν $f(x) \in F[x]$, τότε το σώμα ανάλυσης του $f(x)$ πάνω από το F είναι μοναδικό με προσέγγιση ισομορφίας, βλ. Πόρισμα 3.2.2.

Παράδειγμα 2.2.11. Θα αποδείξουμε ότι

$$\mathbb{Q}[\sqrt{2},\sqrt{3}] = \mathbb{Q}[\sqrt{2}+\sqrt{3}].$$

Στο Παράδειγμα 2.1.4.6 είδαμε ότι $\sqrt{2} \in \mathbb{Q}[\sqrt{2}+\sqrt{3}]$ και άρα $\mathbb{Q}[\sqrt{2}] \subset \mathbb{Q}[\sqrt{2}+\sqrt{3}]$. Με τον ίδιο τρόπο προκύπτει ότι $\sqrt{3} \in \mathbb{Q}[\sqrt{2}+\sqrt{3}]$ και άρα $\mathbb{Q}[\sqrt{2}][\sqrt{3}] = \mathbb{Q}[\sqrt{2},\sqrt{3}] \subset \mathbb{Q}[\sqrt{2}+\sqrt{3}]$. Για τον αντίστροφο εγκλεισμό παρατηρούμε ότι, αφού το στοιχείο $\sqrt{2}+\sqrt{3} \in \mathbb{Q}[\sqrt{2},\sqrt{3}]$, έπεται ότι $\mathbb{Q}[\sqrt{2}+\sqrt{3}] \subset \mathbb{Q}[\sqrt{2},\sqrt{3}]$.

Έστω E ένα ενδιάμεσο σώμα της επέκτασης L/F. Παρατηρούμε ότι το σώμα L έχει τη δομή ενός E-διανυσματικού χώρου όπως και τη δομή ενός F-διανυσματικού χώρου.

Θεώρημα 2.2.12. *Έστω E ένα ενδιάμεσο σώμα της επέκτασης L/F, $[E:F] < \infty$ και $[L:E] < \infty$. Τότε $[L:F] = [L:E]\,[E:F]$.*

Απόδειξη. Έστω $\{a_1,\ldots,a_n\}$ μία E-βάση του L και $\{b_1,\ldots,b_m\}$ μία F-βάση του E. Θα δείξουμε ότι το σύνολο $\{a_ib_j :\ i=1,\ldots,n, j=1,\ldots,m\}$ είναι μία F-βάση του L.

Ξεκινούμε με τη γραμμική ανεξαρτησία. Έστω:

$$\sum_{i,j} d_{ij}(a_ib_j) = 0,\ d_{ij} \in F, i=1,\ldots,n,\ j=1,\ldots,m.$$

Τότε

$$\sum_i (\sum_j d_{ij}b_j)a_i = 0, i=1,\ldots,n,\ j=1,\ldots,m.$$

Αφού $\sum_j d_{ij}b_j \in L$, η E-γραμμική ανεξαρτησία των $\{a_1,\ldots,a_n\}$ συνεπάγεται, για $i=1,\ldots,n$, ότι $\sum_j d_{ij}b_j = 0$. Για κάθε μία τέτοια εξίσωση, η F-γραμμική ανεξαρτησία των $\{b_1,\ldots,b_m\}$ συνεπάγεται ότι ο συντελεστής $d_{ij} = 0$, για $j=1,\ldots,m$.

Το τελευταίο κομμάτι της απόδειξης, δηλαδή το ότι τα στοιχεία παράγουν τον L ως F-διανυσματικό χώρο, αφήνεται ως άσκηση (βλ. άσκηση 2.4.9). □

Παρατηρούμε ότι αν E είναι ενδιάμεσο σώμα της επέκτασης L/F και $a \in L$ είναι αλγεβρικό πάνω από το F, τότε το $\mathrm{irr}_{(E,a)}(x)$ διαιρεί το πολυώνυμο $\mathrm{irr}_{(F,a)}(x)$ και $\deg \mathrm{irr}_{(E,a)}(x) \leq \deg \mathrm{irr}_{(F,a)}(x)$.

Παραδείγματα 2.2.13.

1. Έστω $E = \mathbb{Q}[\sqrt{2}+\sqrt{3}]$. Από το Παράδειγμα 2.2.11 ισχύει ότι $E = \mathbb{Q}(\sqrt{2},\sqrt{3})$. Μία $\mathbb{Q}$-βάση για το E προκύπτει από τις επεκτάσεις $\mathbb{Q} \subset \mathbb{Q}[\sqrt{2}] \subset E$ και είναι ίση με $\{1,\sqrt{2},\sqrt{3},\sqrt{6}\}$. Στο Παράδειγμα 2.1.2.9 είδαμε ότι το πολυώνυμο $f(x) = x^4-10x+1$ μηδενίζεται στο $\sqrt{2}+\sqrt{3}$. Μπορούμε τώρα να δείξουμε ότι το $f(x)$ είναι ανάγωγο στο $\mathbb{Q}[x]$. Πράγματι, αφού

$$4 = [\mathbb{Q}(\sqrt{2}+\sqrt{3}):\mathbb{Q}] = \deg \mathrm{irr}_{(\mathbb{Q},\sqrt{2}+\sqrt{3})}(x),$$

έπεται ότι $\mathrm{irr}_{(\mathbb{Q},\sqrt{2}+\sqrt{3})}(x) = f(x)$. Έτσι μία άλλη $\mathbb{Q}$-βάση για το E είναι το σύνολο $\{1,\sqrt{2}+\sqrt{3},(\sqrt{2}+\sqrt{3})^2,(\sqrt{2}+\sqrt{3})^3\}$.

2. Έστω $b = \sqrt[3]{2}$ και $\omega = e^{2\pi i/3}$, $L = \mathbb{Q}(b, \omega)$. Αφού $\mathrm{irr}_{(\mathbb{Q},b)}(x) = x^3 - 2$, έπεται ότι $[\mathbb{Q}(b) : \mathbb{Q}] = 3$ και ότι $\{1, b, b^2\}$ είναι μία $\mathbb{Q}$-βάση του $\mathbb{Q}(b)$. Γνωρίζουμε ότι $\mathrm{irr}_{(\mathbb{Q},\omega)}(x) = x^2 + x + 1$. Άρα $\mathrm{irr}_{(\mathbb{Q}(b),\omega)}(x)$ διαιρεί το πολυώνυμο $\mathrm{irr}_{(\mathbb{Q},\omega)}(x)$ και έχει βαθμό ≤ 2. Όμως, $\omega \notin \mathbb{Q}(b)$ και άρα $\deg \mathrm{irr}_{(\mathbb{Q}(b),\omega)} \geq 2$. Επομένως

$$\mathrm{irr}_{(\mathbb{Q}(b),\omega)}(x) = \mathrm{irr}_{(\mathbb{Q},\omega)}(x) = x^2 + x + 1$$

και $\{1, \omega\}$ είναι μία $\mathbb{Q}(b)$-βάση του E. Προκύπτει από την Πρόταση 2.2.12, ότι $[E : \mathbb{Q}] = 6$ και ότι μία $\mathbb{Q}$-βάση του E είναι το σύνολο $\{1, b, b^2, \omega, \omega b, \omega b^2\}$.

3. Έστω $b = \sqrt[5]{2}$, $\omega = e^{2\pi i/5}$, $L = \mathbb{Q}(b, \omega)$. Αφού

$$[L : \mathbb{Q}] = [L : \mathbb{Q}(b)][\mathbb{Q}(b) : \mathbb{Q}] \tag{2.2.13.1}$$

και $\deg \mathrm{irr}_{(\mathbb{Q},b)}(x) = 5$, έπεται ότι το 5 διαιρεί $[L : \mathbb{Q}]$. Αντίστοιχα, αφού

$$[L : \mathbb{Q}] = [L : Q(\omega)][\mathbb{Q}(\omega) : \mathbb{Q}]$$

και $\deg \mathrm{irr}_{(\mathbb{Q},\omega)}(x) = 4$, έπεται ότι το 4 διαιρεί τον βαθμό $[L : \mathbb{Q}]$. Άρα το 20 διαιρεί τον βαθμό $[L : \mathbb{Q}]$ και επομένως $[L : \mathbb{Q}] \geq 20$. Όμως $[L : \mathbb{Q}(b)] = \deg \mathrm{irr}_{(\mathbb{Q}(b),\omega)}(x)$ και

$$\deg \mathrm{irr}_{(\mathbb{Q}(b),\omega)}(x) \leq \deg \mathrm{irr}_{(\mathbb{Q},\omega)}(x) = 4.$$

Αντικαθιστώντας στη σχέση (2.2.13.1) προκύπτει ότι $[L : \mathbb{Q}] \leq 20$. Επομένως $[L : \mathbb{Q}] = 20$ και ότι

$$\mathrm{irr}_{(\mathbb{Q}(b),\omega)}(x) = x^4 + x^3 + x^2 + x + 1$$

ενώ

$$\mathrm{irr}_{(\mathbb{Q}(\omega),b)}(x) = x^5 - 2.$$

Το Θεώρημα 2.2.12 εφαρμόζεται στα παρακάτω πορίσματα:

Πόρισμα 2.2.14. *Έστω E/F επέκταση σωμάτων και έστω $a_1, \ldots, a_n \in F$ αλγεβρικά στοιχεία πάνω από το F. Τότε*

i) Ο βαθμός $[F(a_1, \ldots, a_n) : F] < \infty$.

ii) Ισχύει ότι $F(a_1, \ldots, a_n) = F[a_1, \ldots, a_n]$.

iii) Η επέκταση $F(a_1, \ldots, a_n)/F$ είναι αλγεβρική.

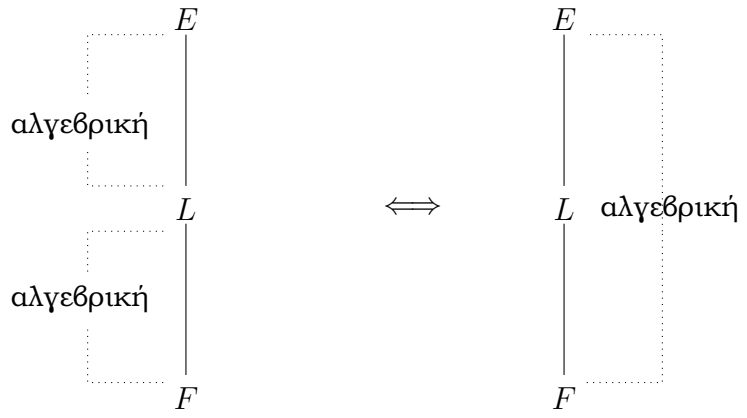
Απόδειξη. Για $n = 1$, η πρόταση είναι άμεση συνέπεια του Πορίσματος 2.2.4, της Πρότασης 2.1.5 και της Πρότασης 2.2.8. Υποθέτουμε, λοιπόν, ότι η πρόταση είναι αληθής όταν $n < k$ και θεωρούμε ότι τα στοιχεία $a_1, \ldots, a_k \in E$ είναι αλγεβρικά πάνω από το F. Έστω $L = F(a_1, \ldots, a_{k-1})$. Σύμφωνα με την υπόθεση της επαγωγής, η επέκταση L/F είναι αλγεβρική, $L = F[a_1, \ldots, a_{k-1}]$ και $[L : F] < \infty$. Αφού το a_k είναι αλγεβρικό πάνω από το F, έπεται ότι το a_k είναι αλγεβρικό και πάνω από το L. Επομένως, από το Πόρισμα 2.2.4, συμπεραίνουμε ότι $[L(a_k) : E] < \infty$. Συνεπώς, σύμφωνα με το Θεώρημα 2.2.12, προκύπτει ότι

$$[L(a_k) : F] = [L(a_k) : L][L : F] < \infty.$$

Τέλος, σύμφωνα με την παρατήρηση που ακολούθησε τον Ορισμό 2.2.9 και την υπόθεση της επαγωγής, ισχύει ότι

$$F(a_1, \ldots, a_k) = F(a_1, \ldots, a_{k-1})(a_k) = L(a_k) = L[a_k] = F[a_1, \ldots, a_k].$$

□



Σχήμα 2.2: Αλγεβρικές επεκτάσεις σωμάτων

Πρόταση 2.2.15. *Έστω ότι οι επεκτάσεις σωμάτων E/L και L/F είναι αλγεβρικές. Τότε η επέκταση E/F είναι αλγεβρική.*

Απόδειξη. Έστω $a \in E$. Τότε το a είναι αλγεβρικό πάνω από το L και έστω $f(x) = \mathrm{irr}_{(L,a)}(x) = x^n + c_{n-1}x^{n-1} + \cdots + c_0 \in L[x]$. Θεωρούμε το σώμα $A = F(c_0, \cdots, c_{n-1})$. Αφού το $f(x) \in A[x]$, το a είναι αλγεβρικό πάνω από το A. Σύμφωνα με το Πόρισμα 2.2.4, προκύπτει ότι $[A(a) : A] < \infty$. Επίσης, από το Πόρισμα 2.2.14 έπεται ότι $[A : F] < \infty$ και ότι η επέκταση A/F είναι αλγεβρική. Επομένως

$$[A(a) : F] = [A(a) : A]\,[A : F] < \infty.$$

Από το Πόρισμα 2.2.4 έπεται ότι το a είναι αλγεβρικό πάνω από το F. □

Το Σχήμα 2.2 περιγράφει το Πόρισμα 2.2.8 και την Πρόταση 2.2.15. Η περίπτωση που ο βαθμός της επέκτασης E/F είναι πρώτος φυσικός αριθμός αντιμετωπίζεται στο επόμενο Πόρισμα.

Πόρισμα 2.2.16. *Έστω E/F επέκταση σωμάτων έτσι ώστε $[E : F] = p$, p πρώτος. Τότε το E είναι απλή επέκταση του F και δεν υπάρχει ενδιάμεσο σώμα L έτσι ώστε $F \subsetneq L \subsetneq E$.*

Απόδειξη. Αφού $[E : F] = p$, έπεται ότι κάθε στοιχείο του E είναι αλγεβρικό πάνω από το F. Έστω $a \in E$, $a \notin F$. Τότε το $F \subsetneq F(a)$ και άρα $[F(a) : F] \neq 1$. Σύμφωνα με την Πρόταση 2.2.12, $[F(a) : F]$ διαιρεί το p, άρα $[F(a) : F] = p$ και κατά συνέπεια $[E : F(a)] = 1$. Επομένως $F(a) = E$. □

Παράδειγμα 2.2.17. Έστω $a = \sqrt[5]{2} \in \mathbb{R}$. Η επέκταση $\mathbb{Q}(a)/\mathbb{Q}$ έχει βαθμό 5 αφού $\mathrm{irr}_{(\mathbb{Q},a)}(x) = x^5 - 2$. Από το προηγούμενο Πόρισμα, συμπεραίνουμε ότι δεν υπάρχει ενδιάμεσο σώμα, ανάμεσα στο $\mathbb{Q}$ και στο $\mathbb{Q}(a)$.

2.3 Ομάδα Galois.

Έστω E/F μία επέκταση σωμάτων. Στην ενότητα αυτή θα μελετήσουμε τους F-αυτομορφισμούς του E, δηλ. τους ισομορφισμούς $\phi : E \to E$ έτσι ώστε $\phi(c) = c$, για κάθε $c \in F$, βλ. Ενότητα IV του Παραρτήματος.

Ορισμός 2.3.1. *Η* **ομάδα Galois** *(Galois group) του E πάνω από το F συμβολίζεται με* $\mathrm{Gal}(E/F)$ *ή* $\mathrm{Aut}_F(E)$ *και είναι το σύνολο των αυτομορφισμών του E που διατηρούν σταθερά τα στοιχεία του F:*

$$\mathrm{Gal}(E/F) := \{\phi \in \mathrm{Aut}(E) : \ \phi(c) = c, \ \forall c \in F\}.$$

Όπως υποννοεί το όνομα, το σύνολο $\mathrm{Gal}(E/K)$, με πράξη τη σύνθεση συναρτήσεων, είναι υποομάδα της ομάδας $\mathrm{Aut}(E)$, που αποτελείται από τους αυτομορφισμούς του E. Πράγματι, όπως θα δούμε αμέσως παρακάτω ισχύει ότι

- η σύνθεση δύο στοιχείων της $\mathrm{Gal}(E/F)$ διατηρεί τα στοιχεία του F σταθερά και επομένως ανήκει στη $\mathrm{Gal}(E/F)$ και
- το αντίστροφο ενός στοιχείου της $\mathrm{Gal}(E/F)$ διατηρεί τα στοιχεία του F σταθερά και επομένως και αυτό ανήκει στη $\mathrm{Gal}(E/F)$.

Έστω, λοιπόν, ότι $\phi, \psi \in \mathrm{Gal}(E/F), \ c \in F$. Τότε

i. $\phi \circ \psi \ (c) = \phi(\psi(c)) = \phi(c) = c$. Επομένως $\phi \circ \psi \in \mathrm{Gal}(E/F)$.
ii. $\phi^{-1}(c) = \phi^{-1}(\phi(c)) = (\phi^{-1} \circ \phi)(c) = \mathrm{id}_F(c) = c$.

Έστω τώρα ότι το $a \in E$ είναι αλγεβρικό πάνω από το F και έστω ότι $\sigma \in \mathrm{Gal}(E/F)$. Θα δούμε ότι το a και το $\sigma(a)$ έχουν το ίδιο ανάγωγο πολυώνυμο και έτσι αναγκαστικά το $\sigma(a)$ είναι μία από τις ρίζες του $\mathrm{irr}_{(F,a)}(x)$, δηλ. το $\sigma(a)$ είναι συζυγές στοιχείο του a.

Πρόταση 2.3.2. *Έστω E/F μία επέκταση σωμάτων, $a \in E$ αλγεβρικό πάνω από το F και $\sigma \in \mathrm{Gal}(E/F)$, Τότε* $\mathrm{irr}_{(F,a)}(x) = \mathrm{irr}_{(F,\sigma(a))}(x)$.

Απόδειξη. Έστω $q(x) = \mathrm{irr}_{(F,a)}(x) = \sum c_i x^i$. Αφού $q(a) = 0$, έπεται ότι $\sum c_i a^i = 0$. Επομένως

$$0 = \sigma(\sum c_i a^i) = \sum \sigma(c_i a^i) = \sum \sigma(c_i)\sigma(a^i) = \sum c_i \sigma(a)^i = \sum c_i b^i.$$

Άρα $q(x) = \mathrm{irr}_{(F,b)}(x)$. □

Για την αντίστροφη κατεύθυνση αυτής της πρότασης έχουμε το εξής θεώρημα:

Θεώρημα 2.3.3. *Έστω E/F μία επέκταση σωμάτων και $a, b \in E$ αλγεβρικά πάνω από το F τέτοια ώστε* $\mathrm{irr}_{(F,a)}(x) = \mathrm{irr}_{(F,b)}(x)$. *Τότε υπάρχει ένας ισομορφισμός σωμάτων $\phi : F(a) \longrightarrow F(b)$ έτσι ώστε $\phi|_F = \mathrm{id}_F$ και $\phi(a) = b$.*

Απόδειξη. Θεωρούμε το κύριο ιδεώδες I του $K[x]$ που παράγεται από το $\mathrm{irr}_{(F,a)}(x)$. Ο επιμορφισμός

$$\phi_1 : F[x] \longrightarrow F[a], \quad \phi_1(f(x)) = f(a)$$

δίνει τον ισομορφισμό

$$\bar{\phi_1} : F[x]/I \longrightarrow F(a), \ \bar{\phi_1}(f(x) + I) = f(a),$$

σύμφωνα με το Πρώτο Θεώρημα Ισομορφίας Δακτυλίων και την Πρόταση 2.1.5. Συγκεκριμένα $\bar{\phi_1}(x + I) = a$, ενώ $\bar{\phi_1}(c + I) = c$, για $c \in F$. Αντίστοιχα έχουμε τον ισομορφισμό

$$\bar{\phi_2} : F[x]/I \longrightarrow F(b), \quad \bar{\phi_1}(f(x) + I) = f(b).$$

Επομένως η σύνθεση

$$\bar{\phi_2} \circ \bar{\phi_1}^{-1} : \ F(a) \longrightarrow F(b)$$

έχει τις επιθυμητές ιδιότητες. □

Είναι εύκολο να δει κανείς ότι αν $\sigma : F \longrightarrow F'$ είναι ισομορφισμός σωμάτων, τότε η συνάρτηση

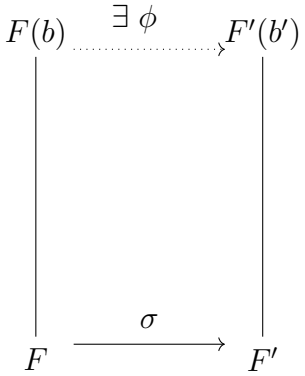
$$\widehat{\sigma} : F[x] \longrightarrow F'[x], \quad \sum a_i x^i \mapsto \sum \sigma(a_i) x^i$$

είναι ισομορφισμός, βλ. άσκηση 1.5.16. Σημειώνουμε έτσι την άμεση γενίκευση του Θεωρήματος 2.3.3 και αφήνουμε την απόδειξη ως άσκηση για τον αναγνώστη (άσκηση 2.4.15).

Θεώρημα 2.3.4. *Έστω E/F και E'/F' επεκτάσεις σωμάτων, $b \in E$, $b' \in E'$ αλγεβρικά πάνω από τα F, F' αντίστοιχα, και $\sigma : F \to F'$ ισομορφισμός έτσι ώστε*

$$\widehat{\sigma}(\mathrm{irr}_{(F,b)}(x)) = \mathrm{irr}_{(F',b')}(x).$$

Υπάρχει ένας ισομορφισμός σωμάτων $\phi : F(b) \longrightarrow F'(b')$ έτσι ώστε $\phi|_F = \sigma$ και $\phi(b) = b'$.



Σχήμα 2.3: Επέκταση του ισομορφισμού σ.

Στα επόμενα παραδείγματα θα υπολογίσουμε την ομάδα Galois σε διάφορες περιπτώσεις. Παρατηρούμε ότι id_E ανήκει στην ομάδα $G = \mathrm{Aut}_F E$, για κάθε επέκταση σωμάτων E/F.

Παραδείγματα 2.3.5.

1. $\mathrm{Gal}(\mathbb{Q}/\mathbb{Q}) = \mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}) = \{\mathrm{id}_{\mathbb{Q}}\}$.
2. Γενικότερα αν F είναι σώμα, τότε $\mathrm{Gal}(F/F) = \mathrm{Aut}_F(F) = \{\mathrm{id}_F\}$.
3. Έστω $G = \mathrm{Gal}(\mathbb{C}/\mathbb{R})$. Θα δείξουμε ότι $G \cong \mathbb{Z}_2$. Παρατηρούμε ότι $\mathbb{C} = \mathbb{R}(i)$ είναι το σώμα ανάλυσης του $f(x) = x^2 + 1$ πάνω από το $\mathbb{R}$. Τα στοιχεία της G στέλνουν τα στοιχεία του $\mathbb{R}$ στον εαυτό τους, ενώ σύμφωνα με την Πρόταση 2.3.2, η εικόνα του i μπορεί να πάρει ακριβώς δύο τιμές: $\pm i$. Η συνάρτηση $\sigma_1 : \mathbb{C} \to \mathbb{C}$, $\sigma_1(a + bi) = a - bi$, για $a, b \in \mathbb{R}$, ανήκει στην G. Επομένως $G = \{id_{\mathbb{C}}, \sigma_1\}$.
4. Έστω $E = \mathbb{Q}(\sqrt{2})$. Θα υπολογίσουμε την ομάδα $G = \mathrm{Gal}(E/\mathbb{Q})$. Πρώτα παρατηρούμε ότι

   $$\mathrm{irr}_{(\mathbb{Q},\sqrt{2})}(x) = x^2 - 2$$

   και ότι το E είναι σώμα ανάλυσης του $\mathrm{irr}_{(\mathbb{Q},\sqrt{2})}(x)$. Επομένως μία $\mathbb{Q}$-βάση του E είναι το σύνολο $\{1, \sqrt{2}\}$, ενώ $\mathbb{Q}(\sqrt{2}) = \mathbb{Q}(-\sqrt{2})$. Σύμφωνα με την Πρόταση 2.3.2, αν $\sigma \in G$ τότε $\sigma(\sqrt{2}) = \pm\sqrt{2}$.

Έστω, τώρα, $c + d\sqrt{2}$ τυχαίο στοιχείο του E, όπου $c, d \in \mathbb{Q}$. Υπάρχει μοναδικός αυτομορφισμός $\sigma \in G$ έτσι ώστε $\sigma(\sqrt{2}) = \sqrt{2}$, και είναι ο ταυτοτικός, $\sigma = \mathrm{id}_E$, αφού

$$\sigma(c + d\sqrt{2}) = \sigma(c) + \sigma(d\sqrt{2}) = c + d\sigma(\sqrt{2}) = c + d\sqrt{2}.$$

Επίσης, σύμφωνα με το Θεώρημα 2.3.3, υπάρχει ισομορφισμός $\tau \in G$ έτσι ώστε $\tau(\sqrt{2}) = -\sqrt{2}$, αφού $E = \mathbb{Q}(-\sqrt{2})$, και αυτή η ιδιότητα προσδιορίζει πλήρως τον ισομορφισμό τ, δηλ.

$$\tau(c + d\sqrt{2}) = c - d\sqrt{2}.$$

Άρα $G = \{\mathrm{id}_E, \tau\}$ και $G \cong \mathbb{Z}_2$.

5. Έστω $E = \mathbb{Q}(\omega)$, όπου $\omega = e^{2\pi i/3}$. Παρατηρούμε ότι $\mathrm{irr}_{(\mathbb{Q},\omega)}(x) = x^2 + x + 1$ και ότι

$$E = \mathbb{Q}(\omega^2).$$

Μία $\mathbb{Q}$-βάση του E είναι το σύνολο $\{1, \omega\}$. Έστω $\sigma \in \mathrm{Gal}(E/\mathbb{Q})$. Τότε $\sigma(c) = c,\ \forall c \in \mathbb{Q}$. Επίσης, σύμφωνα με την Πρόταση 2.3.2, το $\sigma(\omega)$ μπορεί να πάρει μία ακριβώς από τις δύο τιμές:

$$\sigma(\omega) = \begin{cases} \omega \\ \omega^2 = -\omega - 1. \end{cases}$$

Όπως και στο προηγούμενο παράδειγμα, σύμφωνα με το Θεώρημα 2.3.3, προκύπτει ότι $\mathrm{Gal}(E/\mathbb{Q}) = \{\sigma_0, \sigma_1\}$, όπου $\sigma_0 = id_{\mathbb{Q}}$ και

$$\sigma_1(c + d\omega) = c + d\omega^2 = (c - d) - d\omega, \text{ για } c, d \in \mathbb{Q}. \text{ Άρα } \mathrm{Gal}(E/\mathbb{Q}) \cong \mathbb{Z}_2.$$

6. Έστω $E = \mathbb{Q}(b)$, όπου $b = \sqrt[3]{2}$, και έστω $G = \mathrm{Gal}(\mathbb{Q}/E)$. Παρατηρούμε ότι $\mathrm{irr}_{(\mathbb{Q},b)}(x) = x^3 - 2$ και ότι μία $\mathbb{Q}$-βάση του E είναι το σύνολο $\{1, b, b^2\}$. Έστω $\sigma \in G$. Σύμφωνα με την Πρόταση 2.3.2, το $\sigma(b)$ πρέπει να είναι ρίζα του $\mathrm{irr}_{(\mathbb{Q},b)}(x)$. Θα πρέπει βέβαια $\sigma(b) \in E$. Αφού η μόνη ρίζα του $x^3 - 2$ στο E είναι το b, έπεται ότι $\sigma(b) = b$. Επομένως, για $c_0, c_1, c_2 \in \mathbb{Q}$,

$$\sigma(c_0 + c_1 b + c_2 b^2) = \sigma(c_0) + \sigma(c_1)\sigma(b) + \sigma(c_2)\sigma(b^2) = c_0 + c_1 b + c_2 b^2,$$

δηλ. $\sigma = \mathrm{id}_E$. Επομένως $G = \{\mathrm{id}_E\}$.

7. Έστω $E = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Θα υπολογίσουμε την ομάδα $G = \mathrm{Gal}(E/\mathbb{Q})$. Παρατηρούμε ότι μία $\mathbb{Q}$-βάση του E είναι το σύνολο $\{1, \sqrt{2}, \sqrt{3}, \sqrt{2} \cdot \sqrt{3}\}$. Έστω ότι $\sigma \in G$. Τότε

$$\sigma(1) = 1,\ \sigma(\sqrt{2} \cdot \sqrt{3}) = \sigma(\sqrt{2})\sigma(\sqrt{3}).$$

Επομένως ο αυτομορφισμός σ προσδιορίζεται από τις τιμές $\sigma(\sqrt{2})$ και $\sigma(\sqrt{3})$. Σύμφωνα με την Πρόταση 2.3.2,

$$\sigma(\sqrt{2}) = \begin{cases} \sqrt{2} \\ -\sqrt{2}, \end{cases} \qquad \sigma(\sqrt{3}) = \begin{cases} \sqrt{3} \\ -\sqrt{3}. \end{cases}$$

Επομένως $|G| \leq 4$. Παρατηρούμε ότι αν $\sigma(\sqrt{2}) = \sqrt{2}$ και $\sigma(\sqrt{3}) = \sqrt{3}$ τότε $\sigma = \mathrm{id}_E$. Έστω τώρα ότι $\sigma(\sqrt{2}) = \sqrt{2}$, δηλ. $\sigma|_{E_1} = \mathrm{id}_{E_1}$, όπου $E_1 = \mathbb{Q}(\sqrt{2})$. Παρατηρούμε ότι

$$E = E_1(\sqrt{3}) = E_1(-\sqrt{3}).$$

Αν $\sigma \neq \mathrm{id}_E$ τότε θα πρέπει να μετακινεί τη $\sqrt{3}$. Εφαρμόζοντας το Θεώρημα 2.3.3, προκύπτει ότι υπάρχει αυτομορφισμός σ_1 του σώματος E έτσι ώστε

$$\sigma_1(\sqrt{3}) = -\sqrt{3},\ \sigma_1|_{E_1} = \mathrm{id}_{E_1},$$

με άλλα λόγια υπάρχει $\sigma_1 \in G$, έτσι ώστε

$$\sigma_1(\sqrt{2}) = \sqrt{2},\ \ \sigma_1(\sqrt{3}) = -\sqrt{3}.$$

Ομοίως προκύπτει ότι υπάρχει $\sigma_2 \in G$ έτσι ώστε

$$\sigma_2(\sqrt{2}) = -\sqrt{2},\ \ \sigma_2(\sqrt{3}) = \sqrt{3}.$$

Επίσης, η σύνθεση $\sigma_3 = \sigma_1 \circ \sigma_2$ ανήκει στην G και

$$\sigma_3(\sqrt{2}) = \sigma_1 \circ \sigma_2(\sqrt{2}) = -\sqrt{2},\ \sigma_3(\sqrt{3}) = \sigma_1 \circ \sigma_2(\sqrt{3}) = -\sqrt{3}.$$

Υπολογίσαμε, ήδη, τέσσερις διαφορετικούς αυτομορφισμούς του E που ανήκουν στην G. Αφού $|G| \leq 4$, έπεται ότι $|G| = 4$. Υπάρχουν ακριβώς δύο ομάδες τεσσάρων στοιχείων με προσέγγιση ισομορφίας: η κυκλική ομάδα με 4 στοιχεία που είναι ισόμορφη με τη $\mathbb{Z}_4$ και η ομάδα του Klein που είναι ισόμορφη με τη $\mathbb{Z}_2 \times \mathbb{Z}_2$, βλ. Πρόταση Ι.23. Παρατηρούμε ότι ο ταυτοτικός αυτομομορφισμός έχει τάξη 1, ενώ όλα τα άλλα στοιχεία της G έχουν τάξη 2. Για παράδειγμα, επιβεβαιώνουμε ότι $\mathrm{ord}(\sigma_1) = 2$, ελέγχοντας ότι $\sigma_1^2 = \mathrm{id}_E$. Για να το δούμε αυτό, αρκεί να ελέγξουμε τις τιμές του σ_1 στα στοιχεία $\sqrt{2}$ και ω που παράγουν την επέκταση $E/\mathbb{Q}$. Πράγματι:

$$\sqrt{2} \overset{\sigma_1}{\mapsto} \sqrt{2} \overset{\sigma_1}{\mapsto} \sqrt{2}, \quad \sqrt{3} \overset{\sigma_1}{\mapsto} -\sqrt{3} \overset{\sigma_1}{\mapsto} -(-\sqrt{3}) = \sqrt{3},$$

Επομένως $\sigma_1^2 = \mathrm{id}_E$ και $\mathrm{ord}(\sigma_1) = 2$. Ομοίως μπορεί κανείς να δείξει ότι τα σ_2 και σ_3 έχουν τάξη 2. Εφόσον, λοιπόν, η G δεν έχει κάποιο στοιχείο που να έχει τάξη 4, έπεται ότι $G \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

Ολοκληρώνουμε αυτήν την ενότητα περιγράφοντας τη μέθοδο που έχουμε ακολουθήσει ως τώρα για την εύρεση της ομάδας $\mathrm{Gal}(E/F)$ στη περίπτωση που ο βαθμός του E πάνω από το F είναι πεπερασμένος. Τα βήματα είναι:

- Βρίσκουμε μία F-βάση B του E.
- Βρίσκουμε ένα σύνολο στοιχείων που παράγουν την επέκταση E/F, ξεκινώντας από τη B. Η προσπάθειά μας είναι να περιορίσουμε όσο μπορούμε το πλήθος των στοιχείων που παράγουν την επέκταση E/F.
- Βρίσκουμε τα ανάγωγα πολυώνυμα για τα στοιχεία που αναφέρονται στο προηγούμενο βήμα και τις ρίζες τους στο E.
- Χρησιμοποιώντας την Πρόταση 2.3.2 βρίσκουμε τις δυνατές εικόνες των στοιχείων που εντοπίσαμε στο δεύτερο βήμα.
- Βρίσκουμε τα στοιχεία της ομάδας $\mathrm{Gal}(E/F)$, χρησιμοποιώντας το Θεώρημα 2.3.3.

Στο επόμενο παράδειγμα θα μελετήσουμε το σώμα ανάλυσης του πολυωνύμου $x^3 - 2$ πάνω από το $\mathbb{Q}$.

Παράδειγμα 2.3.6. Έστω

$$b = \sqrt[3]{2},\ \omega = e^{2\pi i/3},\ E = \mathbb{Q}(b, \omega b, \omega^2 b).$$

Το σώμα E είναι υπόσωμα του $\mathbb{C}$ και είναι σώμα ανάλυσης του $x^3 - 2$ πάνω από το $\mathbb{Q}$. Αφού

$$\omega = \frac{\omega b}{b} \in E,$$

εύκολα προκύπτει ότι:

$$E = \mathbb{Q}(b, \omega b) = \mathbb{Q}(b, \omega^2 b) = \mathbb{Q}(\omega b, \omega^2 b) = \mathbb{Q}(b, \omega).$$

Χρησιμοποιούμε την τελευταία έκφραση $E = \mathbb{Q}(b, \omega)$, κυρίως, γιατί υπάρχουν δύο ανάγωγα (πάνω από το $\mathbb{Q}$) πολυώνυμα που θα διευκολύνουν τους υπολογισμούς μας, δηλ. τα πολυώνυμα

$$\mathrm{irr}_{(\mathbb{Q},b)}(x) = x^3 - 2,\ \mathrm{irr}_{(\mathbb{Q}),\omega}(x) = x^2 + x + 1.$$

Σύμφωνα με το Θεώρημα 2.2.12, εργαζόμαστε όπως στο Παράδειγμα 2.2.13. Έτσι, προκύπτει ότι μία $\mathbb{Q}$-βάση για το E είναι το σύνολο $\{1, b, b^2, \omega, \omega b, \omega b^2\}$ και ότι $[\ \mathbb{Q}(\omega) : \mathbb{Q}] = 6$.

Έστω $G = \mathrm{Gal}(E/\mathbb{Q})$ και έστω $\sigma \in G$. Ο αυτομορφισμός σ καθορίζεται πλήρως από τις εικόνες $\sigma(b)$ και $\sigma(\omega)$. Σύμφωνα με την Πρόταση 2.3.2, έχουμε τρεις δυνατές τιμές για την εικόνα $\sigma(b)$ και δύο δυνατές τιμές για τη $\sigma(\omega)$, όσες είναι οι ρίζες των αντίστοιχων ανάγωγων πολυωνύμων. Άρα η ομάδα G έχει τάξη το πολύ 6. Θα δείξουμε ότι η ομάδα G έχει τάξη ακριβώς 6.

Πράγματι,

$$E = \mathbb{Q}(\omega)(b)$$

και είναι εύκολο να συμπεράνει κανείς ότι

$$\mathrm{irr}_{(\mathbb{Q}(\omega),b)}(x) = \mathrm{irr}_{(\mathbb{Q},b)}(x) = x^3 - 2.$$

Σύμφωνα με το Θεώρημα 2.3.3 υπάρχουν τρία διαφορετικά στοιχεία της ομάδας αυτομορφισμών του E που διατηρούν σταθερά τα στοιχεία του $\mathbb{Q}(\omega)$, δηλ. απεικονίζουν $c \mapsto c$, για κάθε $c \in \mathbb{Q}(\omega)$, και έτσι ώστε το b να απεικονίζεται σε μία από τις τρεις ρίζες του $x^3 - 2$:

$$b \mapsto \begin{cases} b \\ \omega b \\ \omega^2 b \end{cases}.$$

Αντίστοιχα, αφού

$$E = \mathbb{Q}(b)(\omega)$$

και

$$\mathrm{irr}_{(\mathbb{Q}(b),\omega)}(x) = \mathrm{irr}_{(\mathbb{Q},\omega)}(x) = x^2 + x + 1,$$

υπάρχουν δύο αυτομορφισμοί στην G τέτοιοι ώστε $c \mapsto c$, $\forall\ c \in \mathbb{Q}(b)$, ενώ

$$\omega \mapsto \begin{cases} \omega \\ \omega^2. \end{cases}$$

Σημειώνουμε ότι όταν ένας αυτομορφισμός του E στέλνει $\omega \mapsto \omega$ και $b \mapsto b$, τότε $a \mapsto a$, $\forall\ a \in E$ και είναι ο ταυτοτικός αυτομορφισμός του E. Έτσι προς το παρόν έχουμε

βρει τέσσερα διαφορετικά στοιχεία της G. Οι συνθέσεις τους μας δίνουν άλλους δύο αυτομορφισμούς. Παρατηρούμε επίσης, ότι αν $\sigma \in G$ είναι ο αυτομορφισμός που στέλνει το b στο ωb και το ω στο ω, τότε ο ομομορφισμός σ^2 δρα ως εξής:

$$\begin{aligned} b &\mapsto \omega b \mapsto \omega(\omega b) = \omega^2 b \\ \omega &\mapsto \omega \mapsto \omega \end{aligned}$$

Επομένως η ομάδα G αποτελείται από 6 στοιχεία, όπως φαίνεται από τον παρακάτω πίνακα:

b	b	ωb	$\omega^2 b$	b	ωb	$\omega^2 b$
ω	ω	ω	ω	ω^2	ω^2	ω^2
	id_E	σ	σ^2	τ	$\sigma\tau$	$\tau\sigma$

(2.3.6.1)

Η ομάδα G δεν είναι αντιμεταθετική όπως φαίνεται από τον πίνακα (2.3.6.1), αφού $\sigma\tau \neq \tau\sigma$.

Είδαμε ότι $|G| = 6$. Γνωρίζουμε ότι με προσέγγιση ισομορφίας υπάρχει μόνο μία μη αντιμεταθετική ομάδα με έξι στοιχεία και ότι αυτή είναι η ομάδα S_3 των μεταθέσεων τριών στοιχείων, βλ. Πρόταση Ι.23. Άρα

$$\mathrm{Gal}(\mathbb{Q}(\omega, b)/\mathbb{Q} \cong S_3.$$

Έστω, τώρα, $a \in E$ και ας υπολογίσουμε την εικόνα $\sigma(a)$. Αφού

$$a = a_0 + a_1 b + a_2 b^2 + a_3\omega + a_4\omega b + a_5\omega b^2, \text{ για } a_i \in \mathbb{Q},\ 1 \leq i \leq 5$$

και $\sigma(a_i) = a_i$, $\sigma(b) = \omega b$, $\sigma(\omega) = \omega$, έπεται ότι $\sigma(b^2) = \omega^2 b^2$, $\sigma(\omega b) = \omega^2 b$ και $\sigma(\omega b^2) = \omega^3 b^2 = b^2$. Επίσης αφού ω είναι ρίζα του πολυωνύμου x^2+x+1, έπεται ότι $\omega^2+\omega+1 = 0$, δηλ. $\omega^2 = -1 - \omega$. Άρα

$$\sigma_1(a) = a_0 - a_4 b + (-a_2 + a_5)b^2 + a_4\omega + (a_1 - a_4)\omega b - a_2\omega b^2.$$

2.4 Ασκήσεις

1. Έστω $E = F(x)$ το σώμα κλασμάτων του δακτυλίου $F[x]$. Να αποδείξετε ότι το $x \in E$ είναι υπερβατικό πάνω από το F.
2. Να περιγραφούν τα σώματα: $\mathbb{Q}(\sqrt{5}, \sqrt{7})$, $\mathbb{Q}(i\sqrt{11})$.
3. Να βρεθεί το πολυώνυμο $\mathrm{irr}_{(\mathbb{Q},a)}(x)$ όταν
   - $a = \sqrt{7} + 1/2$,
   - $a = i\sqrt{3} - 1/2$.
4. Να γράψετε τον αντίστροφο του $\sqrt[3]{2}^{\,2} + 1$ ως γραμμικό συνδυασμό δυνάμεων του $\sqrt[3]{2}$ στο σώμα $\mathbb{Q}(\sqrt[3]{2})$.
5. Έστω $\omega = e^{2\pi i/8}$. Να τοποθετήσετε το ω στον μοναδιαίο κύκλο. Να δείξετε ότι $\mathrm{irr}_{(\mathbb{Q},\omega)}(x) = x^4 + 1$. Να βρείτε $\mathrm{irr}_{(\mathbb{Q},\omega^k)}(x)$ για $k = 0, \ldots, 7$.
6. Να βρεθούν οι βαθμοί των επεκτάσεων:
   - $\mathbb{C}/\ \mathbb{Q}$,
   - $\mathbb{Z}_5(x)/\ \mathbb{Z}_5$,

- $\mathbb{R}(\sqrt{5})/\ \mathbb{R}$,
- $\mathbb{Q}(\sqrt[7]{3})/\ \mathbb{Q}$.

7. Να ελέγξετε αν το σώμα $\mathbb{Q}[\sqrt{3}]$ είναι ισόμορφο με το σώμα $\mathbb{Q}[\sqrt{5}]$.
8. Έστω $E = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$. Να αποδείξετε ότι $[E : \mathbb{Q}] = 8$.
9. Έστω E/F, L/E επεκτάσεις σωμάτων και έστω ότι τα $a_1, \ldots, a_n$ παράγουν το σώμα L πάνω από το E, ενώ τα $b_1, \ldots, b_m$ παράγουν το E πάνω από το F. Να αποδείξετε ότι τα $a_i b_j :\ i = 1, \ldots, n, j = 1, \ldots, m$ παράγουν το L πάνω από το F.
10. Αν $[E : F] < \infty$, για σώματα $F \subset E$, να δείξετε ότι υπάρχουν $b_1, \ldots, b_n \in E$ έτσι ώστε $E = F(b_1, \ldots, b_n)$.
11. Έστω ότι τα $a, b \in E$ είναι αλγεβρικά πάνω από το F. Να αποδείξετε τα ακόλουθα

    - $[F(a + b) : F] < \infty$
    - Το στοιχείο $a + b$ είναι αλγεβρικό υπεράνω του F.

12. Έστω ότι E είναι ενδιάμεσο σώμα της επέκτασης L/F και έστω ότι $a \in L$. Να αποδείξετε ότι το πολυώνυμο $\mathrm{irr}_{(E,a)}(x)$ διαιρεί το πολυώνυμο $\mathrm{irr}_{(F,a)}(x)$. Να συμπεράνετε ότι αν $\deg \mathrm{irr}_{(F,a)}(x) = \deg \mathrm{irr}_{(E,a)}(x)$, τότε $\mathrm{irr}_{(F,a)}(x) = \mathrm{irr}_{(E,a)}(x)$.
13. Έστω ότι E είναι σώμα ανάλυσης ενός διαχωρίσιμου αναγώγου πολυωνύμου $f(x) \in K[x]$, βαθμού n, και έστω ότι $a_1, a_2, \ldots, a_n$ είναι οι ρίζες του $f(x)$ στο E. Αν $E_i = K(a_1, \ldots, a_i)$ να δείξετε ότι $\deg \mathrm{irr}_{(E_i,a_i)}(x) \leq n - i + 1$ και άρα $[E : E_i] \leq (n - i)!$. Να συμπεράνετε ότι $[E : K] \leq n!$.
14. Να θεωρήσετε $\overline{\mathbb{Q}} = \{r \in \mathbb{R} :\ a$ αλγεβρικό πάνω από το $\mathbb{Q}\}$. Να αποδείξετε ότι $\overline{\mathbb{Q}}$ είναι υπόσωμα το $\mathbb{R}$ και να βρείτε $[\overline{\mathbb{Q}} : \mathbb{Q}]$.
15. Έστω E/F και E'/F' επεκτάσεις σωμάτων, $b \in E$, $b' \in E'$ αλγεβρικά πάνω από τα F, F' αντίστοιχα και $\sigma :\ F \to F'$ ισομορφισμός έτσι ώστε

    $$\widehat{\sigma}(\mathrm{irr}_{(F,b)}(x)) = \mathrm{irr}_{(F',b')}(x).$$

    Να αποδείξετε ότι υπάρχει ένας ισομορφισμός σωμάτων $\phi : F[b] \longrightarrow F'[b']$ έτσι ώστε $\phi|_F = \sigma$ και $\phi(b) = b'$.
16. - Να αποδείξετε ότι $\mathbb{Q}(\sqrt{5} + \sqrt{2}) = \mathbb{Q}(\sqrt{5}, \sqrt{2})$.
    - Να βρείτε το ανάγωγο πολυώνυμο του $\sqrt{5} + \sqrt{2}$ πάνω από το $\mathbb{Q}(\sqrt{2})$.
    - Να βρείτε το ανάγωγο πολυώνυμο του $\sqrt{5} + \sqrt{2}$ πάνω από το $\mathbb{Q}(\sqrt{5}, \sqrt{2})$.
    - Να βρείτε το ανάγωγο πολυώνυμο του $\sqrt{5} + \sqrt{2}$ πάνω από το $\mathbb{Q}$.
17. Έστω $[L : K] < \infty$ μία πεπερασμένη επέκταση και $f(x) \in K[x]$ ανάγωγο. Να αποδείξετε ότι αν οι φυσικοί αριθμοί $\deg f(x) > 1$ και $[L : K]$ είναι πρώτοι μεταξύ τους, τότε το $f(x)$ δεν έχει ρίζες στο L.
18. Να υπολογισθεί η ομάδα Galois $\mathrm{Gal}(\mathbb{Q}(a)/\mathbb{Q})$ όταν

    - $a = \sqrt{5}$,
    - $a = 2i$,
    - $a = e^{2\pi i/5}$,
    - $a = \sqrt[3]{-2}$.

19. Έστω E/F επέκταση σωμάτων και έστω $e, \sigma_1, \ldots, \sigma_{n-1}$ διακεκριμένα στοιχεία της ομάδας $\mathrm{Gal}(E/F)$. Έστω $a \in E$. Αν τα στοιχεία $a, \sigma_1(a), \ldots, \sigma_{n-1}(a)$ είναι διακεκριμένα τότε να δείξετε ότι $\deg \mathrm{irr}_{(F,a)}(x) \geq n$.
20. Να βρείτε την τάξη των στοιχείων της ομάδας $\mathrm{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\ \mathbb{Q})$.
21. Να βρείτε την ομάδα $\mathrm{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\ \mathbb{Q}(\sqrt{2}))$.
22. Έστω $\omega = e^{2\pi i/3}$, $b = \sqrt{5}$, $E = \mathbb{Q}(\omega, b)$. Να βρείτε την ομάδα $\mathrm{Gal}(E/\mathbb{Q})$.
23. Έστω F σώμα και έστω K το πρώτο υπόσωμα του F. Να αποδείξετε ότι $\mathrm{Gal}(F/K)$ είναι υποομάδα της $\mathrm{Aut}(F)$, δηλ. της ομάδας των αυτομορφισμών του F.
24. Να αποδείξετε ότι η ομάδα $\mathrm{Gal}(\mathbb{R}/\mathbb{Q})$ είναι η τετριμμένη. (Σημειώστε και την εκφώνηση της άσκησης 7.3.6.)
25. Έστω $\omega = e^{2\pi i/11}$. Να αποδείξετε ότι η ομάδα $\mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q})$ είναι κυκλική και έχει τάξη 10.
26. Έστω $\omega = e^{2\pi i/12}$. Να αποδείξετε ότι η ομάδα $\mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q})$ έχει 4 στοιχεία και να ελέγξετε αν είναι κυκλική.
27. Για κάθε μία από τις παρακάτω προτάσεις να αποφασίσετε αν είναι αληθής ή όχι.

    (α΄) Πεπερασμένες επεκτάσεις σωμάτων ίσου βαθμού είναι ισόμορφες.

    (β΄) Οι άπειρες απλές επεκτάσεις ενός σώματος F είναι ισόμορφες.

    (γ΄) Κάθε αλγεβρική επέκταση πάνω από ένα σώμα είναι πεπερασμένη.

    (δ΄) Κάθε υπερβατική επέκταση σώματος δεν είναι πεπερασμένη.

    (ε΄) Κάθε στοιχείο του $\mathbb{C}$ είναι αλγεβρικό πάνω από το $\mathbb{R}$.

    (ϛ΄) Κάθε επέκταση του $\mathbb{R}$ είναι πεπερασμένη.

    (ζ΄) Κάθε επέκταση πεπερασμένου σώματος είναι πεπερασμένη.

    (η΄) Κάθε απλή αλγεβρική επέκταση σωμάτων είναι πεπερασμένη.

    (θ΄) Κάθε απλή επέκταση σωμάτων είναι πεπερασμένη.

    (ι΄) Κάθε σώμα έχει μη τετριμμένες επεκτάσεις.

    (ια΄) Κάθε σώμα έχει μη τετριμμένες αλγεβρικές επεκτάσεις.

    (ιβ΄) Κάθε απλή επέκταση σωμάτων είναι αλγεβρική.

    (ιγ΄) Κάθε επέκταση σωμάτων είναι απλή.

    (ιδ΄) Όλες οι απλές αλγεβρικές επεκτάσεις σωμάτων είναι ισόμορφες.

    (ιε΄) Όλες οι απλές υπερβατικές επεκτάσεις σώματος είναι ισόμορφες.

Βιβλιογραφία Κεφαλαίου 2

[1] Dummit, D.S., Foote, R.M. *Abstract Algebra*. J. Wiley and Sons, INc, 2004.

[2] Fraleigh, J. *Εισαγωγή στην Άλγεβρα*. Πανεπιστημιακές εκδόσεις Κρήτης, 2011.

[3] Hadlock, C. R *Field Theory and its Classical Problems*. 2000.

[4] Hungerford,T. *Algebra*. Springer, 1974.

[5] Lang, S. *Algebra*. Springer, 2002.

[6] Menini, C. Van Oystaeyen, F. *Abstract Algebra*. Marcel Dekker, 2004.

[7] Rotman, J. *Θεωρία Galois*. Leader Books, 2000.

[8] Stewart, I. *Galois Theory*. Champan and Hall, 1973.

Κεφάλαιο 3

Θεμελιώδες Θεώρημα της Θεωρίας Galois

Στο κεφάλαιο αυτό εξετάζουμε λεπτομερέστερα τις ομάδες Galois και μελετάμε τις επεκτάσεις ισομορφισμών σωμάτων. Στη συνέχεια ορίζουμε τις επεκτάσεις Galois σωμάτων και αποδεικνύουμε το θεμελιώδες θεώρημα της θεωρίας Galois.

3.1 Μεταθέσεις και ομάδα Galois

Στο Παράδειγμα 2.3.6 υπολογίσαμε την ομάδα Galois $\mathrm{Gal}(E/\mathbb{Q})$ του σώματος ανάλυσης E του πολυωνύμου $f(x) = x^3 - 2$ πάνω από το $\mathbb{Q}$ και είδαμε ότι είναι ισόμορφη με την S_3. Το βασικό θεώρημα αυτής της παραγράφου, συνδέει τα στοιχεία της $\mathrm{Gal}(E/F)$ και τις μεταθέσεις των ριζών του $f(x) \in F[x]$, όταν το E είναι το σώμα ανάλυσης του $f(x)$ πάνω από το F. Έτσι αντιλαμβανόμαστε την αξία αυτού του ισομορφισμού.

Θεώρημα 3.1.1. *Έστω $f(x) \in F[x]$ διαχωρίσιμο και ανάγωγο, $\deg f(x) = n$ και έστω E σώμα ανάλυσης του $f(x)$. Τότε η ομάδα $\mathrm{Gal}(E/F)$ εμφυτεύεται στην ομάδα των μεταθέσεων S_n.*

Απόδειξη. Έστω $X = \{b_1, \ldots, b_n\}$ το σύνολο των ριζών του $f(x)$. Τότε $E = F(b_1, \ldots, b_n)$. Τα στοιχεία του S_X είναι αμφιμονότιμες και επί συναρτήσεις του X στον εαυτό του και $S_X \cong S_n$. Αν $G = \mathrm{Gal}(E/F)$ και $\sigma \in G$, τότε θεωρούμε τη συνάρτηση $\theta_\sigma : X \to X$, $\theta_\sigma(b_i) = \sigma(b_i)$, όπου $i = 1, \ldots, n$. Είναι εύκολο να δείξει κανείς ότι $\theta_\sigma \in S_X$, δηλαδή ότι $\theta(b_i) = \theta(b_j) \Leftrightarrow b_i = b_j$. Έτσι οδηγούμαστε στον επόμενο ορισμό:

$$\phi_G : G \to S_X, \quad \sigma \mapsto \theta_\sigma.$$

Ο αναγνώστης μπορεί εύκολα να επιβεβαιώσει ότι

- $\phi_G(\sigma\,\tau) = \phi_G(\sigma)\,\phi_G(\tau)$, για $\sigma, \tau \in G$ και
- ϕ_G είναι αμφιμονότιμη, δηλ. $\phi_G(\sigma) = \phi_G(\tau) \Leftrightarrow \sigma = \tau$, για $\sigma, \tau \in G$.

Επομένως η συνάρτηση ϕ είναι μονομορφισμός ομάδων. □

Στα επόμενα παραδείγματα θα μελετήσουμε την εμφύτευση του Θεωρήματος 3.1.1.

Παραδείγματα 3.1.2.

1. Έστω $f(x) = x^3 - 2 \in \mathbb{Q}[x]$, $\omega = e^{2\pi i/3}$, $b = \sqrt[3]{2}$ και $E = \mathbb{Q}(b, \omega b)$. Όπως είδαμε στο παράδειγμα 2.3.6, το σώμα E είναι το σώμα ανάλυσης του $f(x)$ πάνω από το $\mathbb{Q}$ και η ομάδα $G = \mathrm{Gal}(E/\mathbb{Q})$ καθορίζεται από τον παρακάτω πίνακα:

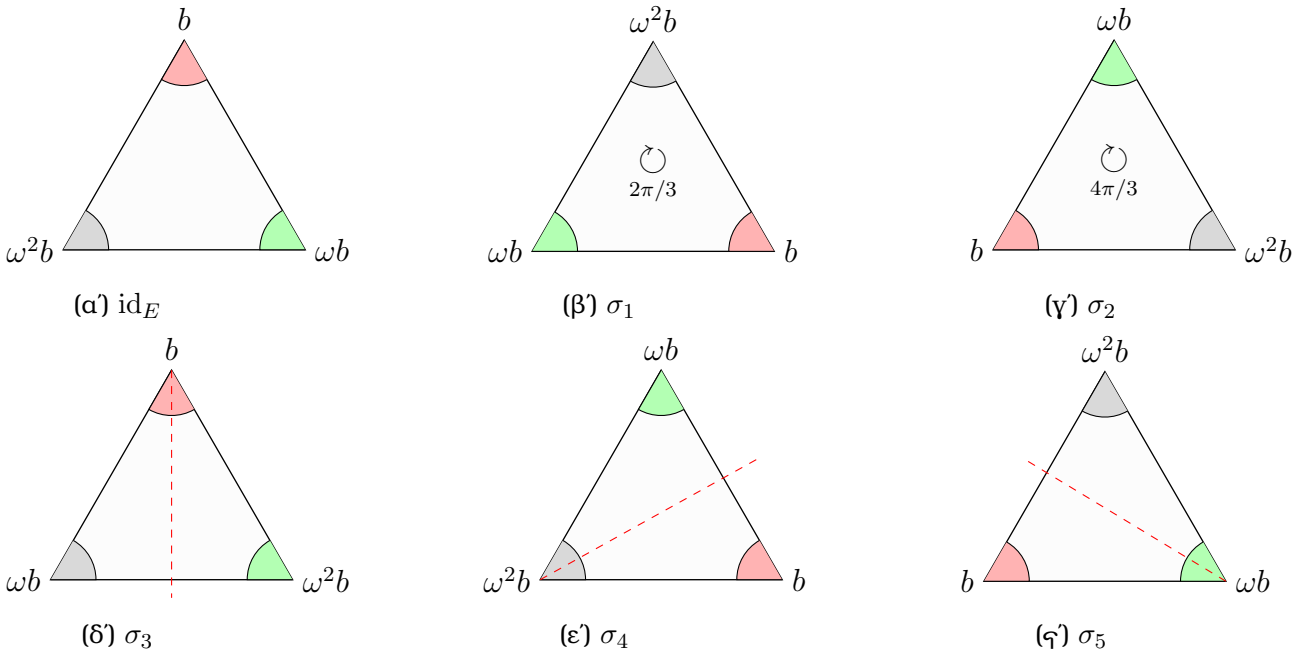
b	b	ωb	$\omega^2 b$	b	ωb	$\omega^2 b$
ω	ω	ω	ω	ω^2	ω^2	ω^2
	id_E	σ	σ^2	τ	$\sigma\tau$	$\tau\sigma$

Η ομάδα G είναι ισόμορφη με την S_3 και οι εικόνες των στοιχείων της G σύμφωνα με τον ισομορφισμό ϕ_G είναι:

$$\mathrm{id}_E \mapsto \begin{pmatrix} b & \omega b & \omega^2 b \\ b & \omega b & \omega^2 b \end{pmatrix}, \ \sigma \mapsto \begin{pmatrix} b & \omega b & \omega^2 b \\ \omega b & \omega^2 b & b \end{pmatrix}, \ \sigma^2 \mapsto \begin{pmatrix} b & \omega b & \omega^2 b \\ \omega^2 b & b & \omega b \end{pmatrix},$$

$$\tau \mapsto \begin{pmatrix} b & \omega b & \omega^2 b \\ b & \omega^2 b & \omega b \end{pmatrix}, \ \sigma\tau \mapsto \begin{pmatrix} b & \omega b & \omega^2 b \\ \omega b & b & \omega^2 b \end{pmatrix}, \ \tau\sigma \mapsto \begin{pmatrix} b & \omega b & \omega^2 b \\ \omega^2 b & \omega b & b \end{pmatrix}.$$

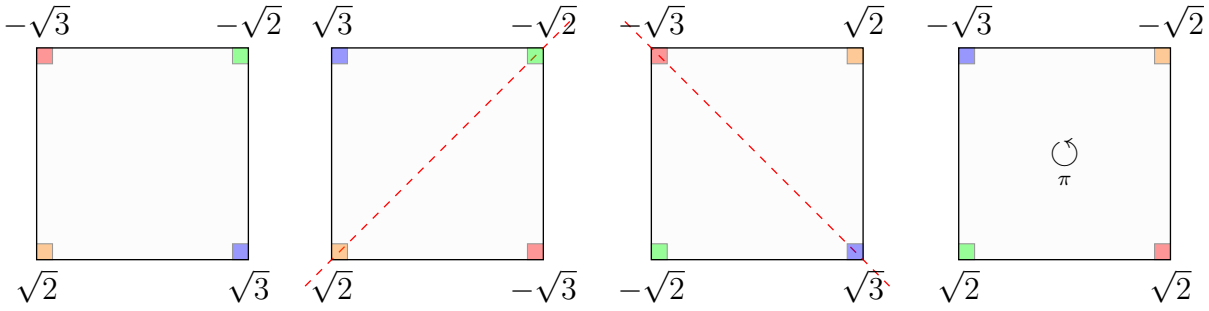
Το σχήμα 3.1, αντιστοιχεί την ομάδα G με τις συμμετρίες του ισόπλευρου τριγώνου.



Σχήμα 3.1: Συμμετρίες του ισόπλευρου τριγώνου και η ομάδα $\mathrm{Gal}(\mathbb{Q}(\omega, b)/\mathbb{Q})$

2. Έστω $f(x) = (x^2 - 2)(x^2 - 3) \in \mathbb{Q}[x]$. Το $E = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ είναι σώμα ανάλυσης του $f(x)$ πάνω από το $\mathbb{Q}$. Στο Παράδειγμα 2.3.5.7 είδαμε ότι $\mathrm{Gal}(E/\mathbb{Q}) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ και ότι τα στοιχεία της G καθορίζονται από τον παρακάτω πίνακα:

$\sqrt{2}$	$\sqrt{2}$	$\sqrt{2}$	$-\sqrt{2}$	$-\sqrt{2}$
$\sqrt{3}$	$\sqrt{3}$	$-\sqrt{3}$	$\sqrt{3}$	$-\sqrt{3}$
	id_E	σ_1	σ_2	$\sigma_1\sigma_2$



(α') id_E (β') σ_1 (γ') σ_2 (δ') $\sigma_1\sigma_2$

Σχήμα 3.2: Συμμετρίες και η ομάδα $\mathrm{Gal}(\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q})$

Αν διατάξουμε τις ρίζες του $f(x)$ ως το σύνολο $\{\sqrt{2},\sqrt{3},-\sqrt{2},-\sqrt{3}\}$, τότε οι εικόνες των σ_1, σ_2 και $\sigma_3=\sigma_1\sigma_2$ στην S_4 σύμφωνα με τον ισομορφισμό ϕ_G του Θεωρήματος 3.1.1 αντιστοιχούν στις μεταθέσεις $(2\ 4)$, $(1\ 3)$ και $(1\ 3)(2\ 4)$ αντίστοιχα. Το σχήμα 3.2, αντιστοιχεί την ομάδα G με κάποιες από τις γεωμετρικές συμμετρίες του τετραγώνου. Τοποθετώντας τις ρίζες του $f(x)$ ως κορυφές ενός τετραγώνου, παρατηρούμε ότι οι σ_1 και σ_2 αντιστοιχούν σε αντικατοπτρισμούς ως προς τις διαγωνίους, ενώ ο $\sigma_1\sigma_2$ αντιστοιχεί στην περιστροφή κατά γωνία π.

3. Έστω $f(x)=x^4-2$. Αν $b=\sqrt[4]{2}$, οι ρίζες του $f(x)$ στο $\mathbb{C}$ είναι $\pm b$, $\pm bi$ και $E=\mathbb{Q}(2^{1/4},i)$ είναι σώμα ανάλυσης του $f(x)$ πάνω από το $\mathbb{Q}$. Θα δείξουμε ότι η ομάδα $G=\mathrm{Gal}(E/\mathbb{Q})$ είναι ισόμορφη με την ομάδα των συμμετριών του τετραγώνου. Πράγματι, η G έχει το πολύ 8 στοιχεία, αφού αν $\sigma\in G$, τότε

$$\sigma(b)=\begin{cases} b\\ -b\\ ib\\ -ib\end{cases},\ \sigma(i)=\begin{cases} i\\ -i\end{cases}.$$

Έστω $F=\mathbb{Q}(i)$. Από το Θεώρημα 2.3.3, αφού το ib είναι ρίζα του $\mathrm{irr}_{(F,b)}=x^4-2$ και $E=F(b)$, υπάρχει αυτομορφισμός $\sigma\in G$ έτσι ώστε

$$\sigma:\ b\mapsto ib, i\mapsto i.$$

Ομοίως βλέπουμε ότι υπάρχει $\tau\in G$ έτσι ώστε

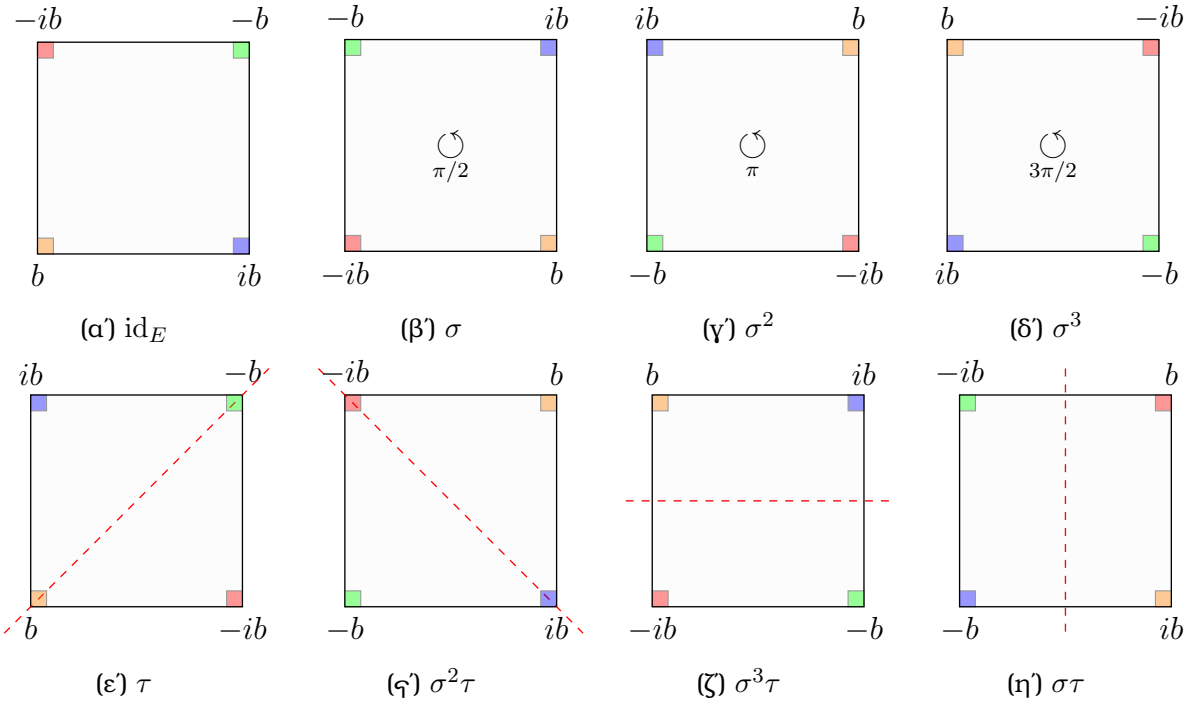
$$\tau:\ b\mapsto b, i\mapsto -i.$$

Οι συνθέσεις των σ και τ δίνουν έξι νέα στοιχεία της ομάδας G. Άρα η ομάδα G έχει όντως ακριβώς οκτώ στοιχεία. Αναλυτικά τα στοιχεία της G καθορίζονται από τον πίνακα:

b	b	$-b$	b	$-b$	ib	ib	$-ib$	$-ib$
i	i	i	$-i$	$-i$	i	$-i$	i	$-i$
	id_E	σ^2	τ	$\sigma^2\tau$	σ	$\sigma\tau$	σ^3	$\sigma^3\tau$

Οι αυτομορφισμοί σ και τ αντιστοιχούν στις μεταθέσεις

$$\begin{pmatrix} b & -b & ib & -ib\\ ib & -ib & -b & b\end{pmatrix}\ \text{και}\ \begin{pmatrix} b & -b & ib & -ib\\ b & -b & -ib & ib\end{pmatrix}.$$



(α′) id_E (β′) σ (γ′) σ^2 (δ′) σ^3

(ε′) τ (ϛ′) $\sigma^2\tau$ (ζ′) $\sigma^3\tau$ (η′) $\sigma\tau$

Σχήμα 3.3: Συμμετρίες του τετραγώνου και η ομάδα $\mathrm{Gal}(\mathbb{Q}(i,b)/\mathbb{Q})$

Τοποθετώντας τις ρίζες του $f(x)$ ως κορυφές ενός τετραγώνου όπως στο παραπάνω σχήμα, παρατηρούμε ότι ο σ αντιστοιχεί σε αριστερόστροφη περιστροφή με γωνία

$$\frac{2\pi}{4} = \frac{\pi}{2},$$

ενώ ο τ αντιστοιχεί στον αντικατοπτρισμό ως προς τη διαγώνιο που περνάει από τις κορυφές $b, -b$.

Από τα παραδείγματα που έχουμε δει ως τώρα αλλά και το Θεώρημα 3.1.1, δημιουργούνται εύλογα ερωτήματα:

- Ποιες ομάδες εμφανίζονται ως ομάδες Galois επεκτάσεων πάνω από σώματα;
- Αν E είναι το σώμα ανάλυσης του $f(x)$ πάνω από το K, πότε ισχύει ο ισομορφισμός $\mathrm{Gal}(E/K) \cong S_n$;

Θα απαντήσουμε σε αυτά τα ερωτήματα κατά τη διάρκεια του συγγράμματος. Παραπέμπουμε τον αναγνώστη στην Ενότητα 8.2 για μία τελική απάντηση.

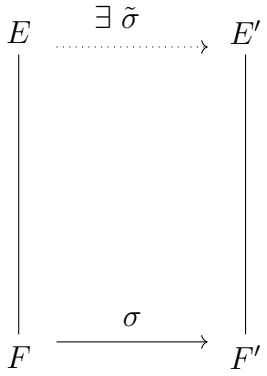
3.2 Τάξη της ομάδας Galois

Έστω E, F δύο σώματα και έστω $\sigma : E \to F$ ισομορφισμός σωμάτων. Σύμφωνα με την άσκηση 1.5.16, ο σ επεκτείνεται σε έναν ισομορφισμό $\widehat{\sigma}$ των δακτυλίων πολυωνύμων $E[x]$ και $F[x]$ ως εξής:

$$\widehat{\sigma} : E[x] \to F[x],\ \sum a_i x^i \mapsto \sum \sigma(a_i) x^i.$$

Αυτός ο ισομορφισμός θα χρησιμοποιηθεί στο επόμενο θεώρημα. Θυμίζουμε ότι ένα ανάγωγο πολυώνυμο $f(x)$ με συντελεστές από ένα σώμα F είναι διαχωρίσιμο αν και μόνο αν οι ρίζες του $f(x)$, σε κάποιο σώμα ανάλυσης του $f(x)$ πάνω από το F, είναι απλές ή ισοδύναμα αν και μόνο αν ΜΚΔ$(f(x), f'(x)) = 1$.

Θεώρημα 3.2.1. *Έστω $\sigma : F \longrightarrow F'$ ισομορφισμός σωμάτων και E/F και E'/F' επεκτάσεις σωμάτων έτσι ώστε το E να είναι ένα σώμα ανάλυσης του $f(x) \in F[x]$ πάνω από το F και E' να είναι το σώμα ανάλυσης του $\widehat{\sigma}(f(x))$ πάνω από το F'. Τότε υπάρχει $\tilde{\sigma} : E \longrightarrow E'$ έτσι ώστε $\tilde{\sigma}|_F = \sigma$. Αν το $f(x)$ είναι διαχωρίσιμο, τότε υπάρχουν ακριβώς $[E : F]$ τέτοιες επεκτάσεις.*



Σχήμα 3.4: Επέκταση του ισομορφισμού s σε σώματα ανάλυσης.

Απόδειξη. Η απόδειξη θα γίνει με επαγωγή στον βαθμό $[E : F]$. Έστω ότι $[E : F] = 1$. Επομένως $E = F$, δηλ. οι ρίζες του $f(x)$ ανήκουν στο F και το $f(x)$ αναλύεται σε γινόμενο γραμμικών παραγόντων στο $F[x]$. Επομένως, το $\tilde{\sigma}(f(x))$ αναλύεται σε γινόμενο γραμμικών παραγόντων στον $F'[x]$ (βλ. άσκηση 1.5.16) και άρα $F = F'$. Έτσι $\sigma = \tilde{\sigma}$.

Θα υποθέσουμε τώρα ότι η πρόταση ισχύει όταν ο βαθμός της επέκτασης $[E : F]$ είναι μικρότερος του n. Έστω ότι $[E : F] = n > 1$. Τότε $E \neq F$ και μία από τις ρίζες του $f(x)$, έστω b, δεν ανήκει στο F. Άρα $F(b) \neq F$ και επομένως $[F(b) : F] > 1$. Από τη σχέση

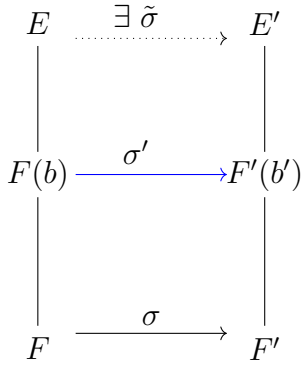
$$[E : F] = [E : F(b)][F(b) : F],$$

προκύπτει ότι $[E : F(b)] < n$. Θεωρούμε στη συνέχεια το πολυώνυμο $g(x) = \mathrm{irr}_{(F,b)}(x) \in F[x]$. Σημειώνουμε ότι το $g(x)$ διαιρεί το $f(x)$ (βλ. την παρατήρηση μετά το Θεώρημα 2.2.12) και αντίστοιχα το $\widehat{\sigma}(g(x))$ διαιρεί το $\widehat{\sigma}(f(x))$. Έστω b' τυχαία ρίζα του $\widehat{\sigma}(g(x))$ στο E'. Σύμφωνα με το Θεώρημα 2.3.4 υπάρχει ισομορφισμός

$$\sigma' : \ F(b) \to F'(b'), \quad \sigma'|_F = \sigma.$$

Σημειώνουμε ότι αφού το E είναι σώμα ανάλυσης του $f(x)$ πάνω από το F και το E περιέχει το $F(b)$, έπεται ότι το E είναι σώμα ανάλυσης του $f(x)$ πάνω από το $F(b)$. Αντίστοιχα, το E' είναι σώμα ανάλυσης του $\widehat{\sigma}(g(x))$ πάνω από το $F'(b')$. Από την υπόθεση της επαγωγής έπεται ότι υπάρχει $\tilde{\sigma} : \ E \longrightarrow E'$ που επεκτείνει τον σ', δηλ. $\tilde{\sigma}|_{F(b)} = \sigma'$. Επομένως

$$\tilde{\sigma}|_F = (\tilde{\sigma}|_{F(b)})|_F = \sigma'|_F = \sigma.$$



Σχήμα 3.5: Ενδιάμεσο βήμα στην απόδειξη της ύπαρξης $\tilde{\sigma}$.

Έστω, τώρα, ότι το $f(x)$ είναι διαχωρίσιμο. Αφού το πολυώνυμο $g(x) = \mathrm{irr}_{(F,b)}(x)$ διαιρεί το $f(x)$, έπεται ότι οι ρίζες του $g(x)$ στο E είναι απλές και ότι το $g(x)$ είναι και αυτό διαχωρίσιμο. Από την υπόθεση της επαγωγής για τον ισομορφισμό $\sigma' : F(b) \to F'(b')$ που προκύπτει για κάθε ρίζα b' του $\tilde{\sigma}(g(x))$, συμπεραίνουμε ότι υπάρχουν $[E : F(b)]$ ισομορφισμοί $\tilde{\sigma} : E \to E'$ έτσι ώστε $\tilde{\sigma}|_{F(b)} = \sigma'$. Μένει, λοιπόν, να μετρήσουμε τις διαφορετικές ρίζες b' του $\widehat{\sigma}(g(x))$. Σύμφωνα με την άσκηση 1.5.16, το ανάγωγο πολυώνυμο $\widehat{\sigma}(g(x))$ είναι διαχωρίσιμο. Επομένως ο αριθμός των διαφορετικών ριζών του $\widehat{\sigma}(g(x))$ είναι ίσος με τον βαθμό του πολυωνύμου $\widehat{\sigma}(g(x))$ και

$$\deg(\widehat{\sigma}(g(x))) = \deg(g(x)) = [F(b) : F].$$

Άρα συνολικά έχουμε

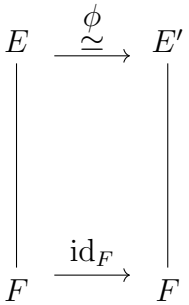
$$[E : F(b)]\ [F(b) : F]$$

πλήθους επιλογές, δηλ. υπάρχουν $[E : F]$ επεκτάσεις του σ. □

Ως άμεσο πόρισμα του Θεωρήματος 3.2.1 προκύπτει ότι το σώμα ανάλυσης ενός πολυωνύμου είναι μοναδικό με προσέγγιση ισομορφίας.

Πόρισμα 3.2.2. *Έστω F ένα σώμα, $f(x) \in F[x]$ και E, E' δύο σώματα ανάλυσης του $f(x)$ πάνω από το F. Τότε υπάρχει F-ισομορφισμός $\phi : E \longrightarrow E'$ και επομένως το σώμα ανάλυσης του $f(x) \in F[x]$ είναι μοναδικό με προσέγγιση F-ισομορφίας.*

Απόδειξη. Αφού $\widehat{\mathrm{id}}_F(f(x)) = f(x)$, οι υποθέσεις του Θεωρήματος 3.2.1 ικανοποιούνται, με $F' = F$ και $\sigma = \mathrm{id}_F$ και υπάρχει επέκταση $\phi : E \longrightarrow E'$ έτσι ώστε $\phi|_F = \mathrm{id}_F$, δηλ. ο ϕ είναι F-ισομορφισμός.



Σχήμα 3.6: Το σώμα ανάλυσης είναι μοναδικό με προσέγγιση ισομορφίας.

□

Αφού το σώμα ανάλυσης ενός πολυωνύμου είναι μοναδικό με προσέγγιση ισομορφίας μπορούμε να δώσουμε τον παρακάτω ορισμό.

Ορισμός 3.2.3. *Έστω F σώμα και $f(x) \in F[x]$. Η* **ομάδα Galois του** *$f(x)$ είναι η ομάδα $\mathrm{Gal}(E/F)$, όπου E είναι το σώμα ανάλυσης του $f(x)$ πάνω από το F.*

Η επόμενη πρόταση υπολογίζει την τάξη της ομάδας Galois.

Πόρισμα 3.2.4. *Έστω $f(x) \in F[x]$ διαχωρίσιμο πολυώνυμο και E ένα σώμα ανάλυσης του $f(x)$. Τότε $|\mathrm{Gal}(E/F)| = [E : F]$.*

Απόδειξη. Εφαρμόζουμε το Θεώρημα 3.2.1 στον ταυτοτικό ισομορφισμό $\mathrm{id}_F : F \longrightarrow F$ με $E = E'$. □

Παραδείγματα 3.2.5.

1. Έστω $E = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$. Τότε το E είναι σώμα ανάλυσης του διαχωρίσιμου πολυωνύμου $f(x) = (x^2-2)(x^2-3)(x^2-5)$ πάνω από το $\mathbb{Q}$. Αφού $[E : \mathbb{Q}] = 8$ (βλ. άσκηση 2.4.8) έπεται ότι $|\mathrm{Gal}(E/\mathbb{Q})| = 8$. Τα στοιχεία της $\mathrm{Gal}(E/\mathbb{Q})$ καθορίζονται από τις παρακάτω εικόνες:

   $$\sqrt{2} \mapsto \pm\sqrt{2},\ \sqrt{3} \mapsto \pm\sqrt{3},\ \sqrt{5} \mapsto \pm\sqrt{5}.$$

   Εύκολα ο αναγνώστης μπορεί να διαπιστώσει ότι η ομάδα $\mathrm{Gal}(E/\mathbb{Q})$ είναι αντιμεταθετική και ότι κάθε στοιχείο της έχει τάξη 2, άρα

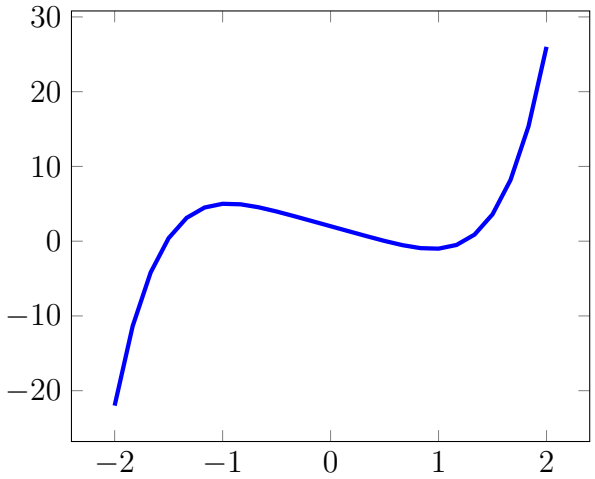
   $$\mathrm{Gal}(E/\mathbb{Q}) \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2.$$

2. Έστω $b = 2^{1/3}$, $\omega = e^{2\pi i/3}$ και E το σώμα ανάλυσης του $x^3 - b$ πάνω από το $\mathbb{Q}$. Η $\mathrm{Gal}(E/\mathbb{Q}) \cong S_3$, βλ. Παράδειγμα 2.3.6. Στη συνέχεια θα υπολογίσουμε την ομάδα $\mathrm{Gal}(E/F)$ όπου $F = \mathbb{Q}(\omega)$.

   Το σώμα E είναι σώμα ανάλυσης του διαχωρίσιμου πολυωνύμου $x^3 - 2$ πάνω από το F. Έτσι το σύνολο $\{1, b, b^2\}$ είναι μία F-βάση του E και $[E : F] = 3$. Σύμφωνα με το Πόρισμα 3.2.4, $|\mathrm{Gal}(E/F)| = 3$ και επομένως $\mathrm{Gal}(E/F) \cong \mathbb{Z}_3$. Αφού τα στοιχεία id_E, σ, σ^2 της $\mathrm{Gal}(E/\mathbb{Q})$ αφήνουν σταθερά τα στοιχεία του σώματος F (βλ. Παράδειγμα 2.3.6) ο αναγνώστης μπορεί να διαπιστώσει ότι $\mathrm{Gal}(E/F) = \{\mathrm{id}_E, \sigma, \sigma^2\} \cong \mathbb{Z}_3$. Παρατηρούμε ότι $\mathrm{Gal}(E/F)$ είναι υποομάδα της $\mathrm{Gal}(E/\mathbb{Q})$ και μάλιστα $\mathrm{Gal}(E/F) \lhd \mathrm{Gal}(E/\mathbb{Q})$, αφού $|\mathrm{Gal}(E/\mathbb{Q})| = 6$ και $|\mathrm{Gal}(E/F)| = 3$, βλ. Παρατήρηση Ι.13.

Στο επόμενο παράδειγμα δείχνουμε ότι υπάρχει $f(x) \in \mathbb{Q}[x]$ με σώμα ανάλυσης E πάνω από το $\mathbb{Q}$ έτσι ώστε $\mathrm{Gal}(E/\mathbb{Q}) \cong S_5$. Για την απόδειξη θα χρειαστούμε δύο θεωρήματα από τη Θεωρία Ομάδων, το Θεώρημα του Cauchy (Θεώρημα Ι.25) και το Θεώρημα Ι.35.

Παράδειγμα 3.2.6. Έστω $f(x) = x^5 - 4x + 2$, E το σώμα ανάλυσης του $f(x)$ πάνω από το $\mathbb{Q}$ και $G = \mathrm{Gal}(E/\mathbb{Q})$. Το πολυώνυμο $f(x)$ είναι ανάγωγο σύμφωνα με το κριτήριο του Eisenstein, για $p = 2$, και διαχωρίσιμο, αφού το $\mathbb{Q}$ έχει χαρακτηριστική 0. Επομένως το $f(x)$ έχει 5 διαφορετικές ρίζες. Σχεδιάζουμε το γράφημα του $f(x)$ στο πραγματικό επίπεδο με τη βοήθεια των παραγώγων $f'(x) = 5x^4 - 4$ και $f''(x) = 20x^3$.



Σχήμα 3.7: Το γράφημα του $x^5 - 4x + 2$.

Παρατηρούμε ότι το $f(x)$ συναντά τον άξονα των x ακριβώς 3 φορές. Άρα το $f(x)$ έχει τρεις πραγματικές ρίζες, έστω a_1, a_2, a_3, και δύο μιγαδικές, έστω a_4, a_5. Γνωρίζουμε ότι a_4, a_5 (Πόρισμα 2.2.5) είναι συζυγείς μιγαδικοί αριθμοί, δηλ. $a_4 = a + bi$ και $a_5 = a - bi$, για $a, b \in \mathbb{R}$.

Έτσι $E = \mathbb{Q}(a_1, \ldots, a_5)$. Αφού $\mathrm{irr}_{(Q,a_1)}(x) = f(x)$, συμπεραίνουμε ότι

$$|G| = [E : \mathbb{Q}] = [E : \mathbb{Q}(a_1)]\ [\mathbb{Q}(a_1) : Q] = 5\ [E : \mathbb{Q}(a_1)]$$

και σύμφωνα με το Θεώρημα του Cauchy (Θεώρημα I.25), η G περιέχει ένα στοιχείο που έχει τάξη 5.

Θα δείξουμε τώρα ότι η G περιέχει μία αντιμετάθεση. Πράγματι, έστω

$$\sigma :\ \mathbb{C} \longrightarrow \mathbb{C}, \quad c + di \mapsto c - di. \tag{3.2.6.1}$$

Ο σ είναι $\mathbb{Q}$-αυτομορφισμός του $\mathbb{C}$, δηλ. $\sigma|_{\mathbb{Q}} = \mathrm{id}_{\mathbb{Q}}$. Θα δείξουμε ότι $\sigma|_E$ ανήκει στην $\mathrm{Gal}(E/\mathbb{Q})$, δηλ. ότι $\sigma|_E$ είναι αυτομορφισμός του E. Πρέπει, λοιπόν, να δείξουμε ότι $\sigma|_E(E) \subset E$. Όμως, $E = \mathbb{Q}(a_1, \ldots, a_5)$ και $\sigma(a_i) = a_i$, για $i = 1, 2, 3$, ενώ $\sigma(a_4) = a_5$. Άρα $\sigma|_E \in \mathrm{Gal}(E/\mathbb{Q})$ και μάλιστα $\sigma|_E$ ως αντιμετάθεση δύο ριζών του $f(x)$ έχει τάξη 2.

Αφού, λοιπόν, η ομάδα G περιέχει ένα στοιχείο που έχει τάξη 5 και μία αντιμετάθεση, σύμφωνα με το Θεώρημα I.35, έπεται ότι η ομάδα G είναι ισόμορφη με την S_5.

Έστω $E_1 = \mathbb{Q}(a_1, a_2, a_3)$. Σύμφωνα με την άσκηση 2.4.13, το πολυώνυμο $\mathrm{irr}_{(E_1,a_4)}(x)$ έχει βαθμό δύο, όσος είναι ο βαθμός του $\mathrm{irr}_{(\mathbb{R},a_4)}(x)$. Επομένως $\mathrm{irr}_{(E_1,a_4)}(x) = \mathrm{irr}_{(\mathbb{R},a_4)}(x)$ (βλ. άσκηση 2.4.12). Άρα $|\mathrm{Gal}(E/E_1)| = 2$ και σύμφωνα με το Παράδειγμα 2.2.2.5

$$\mathrm{irr}_{(E_1,a_4)}(x) = x^2 - 2ax + (a^2 + b^2) \in E_1[x].$$

Επομένως $a, b^2 \in E_1$ και

$$E = E_1(a_4) = E_1(a + bi) = E_1(bi).$$

Σημειώνουμε ότι αφού οι δύο ρίζες του $x^2 + b^2 \in E_1[x]$ είναι οι $\pm bi$, σύμφωνα με το Θεώρημα 2.3.3, υπάρχει $\tau \in \mathrm{Gal}(E/E_1)$, έτσι ώστε $\tau(bi) = -bi$. Είναι εύκολο να δει κανείς ότι $\tau = \sigma|_E$, όπου σ είναι ο αυτομορφισμός της εξίσωσης (3.2.6.1).

3.3 Ενδιάμεσα σώματα και υποομάδες της ομάδας Galois

Στην ενότητα αυτή θα εξετάσουμε λεπτομερέστερα τη σχέση ανάμεσα στα ενδιάμεσα σώματα της επέκτασης E/F και στις υποοομάδες της $G = \mathrm{Gal}(E/F)$. Είναι εύκολο να δούμε ότι σε κάθε ενδιάμεσο σώμα της E/F αντιστοιχεί μία υποομάδα της G.

Πρόταση 3.3.1. *Έστω B ενδιάμεσο σώμα της επέκτασης E/F. Τότε $\mathrm{Gal}(E/B)$ είναι υποομάδα της $\mathrm{Gal}(E/F)$.*

Απόδειξη. Αν $\sigma \in \mathrm{Gal}(E/B)$, τότε $\sigma(b) = b$, για κάθε $b \in B$, και άρα $\sigma(c) = c$, για κάθε $c \in F$. Επομένως $\sigma \in \mathrm{Gal}(E/F)$. □

Το επόμενο θεώρημα εξετάζει πότε η υποομάδα $\mathrm{Gal}(E/B)$ της G είναι κανονική.

Θεώρημα 3.3.2. *Έστω E/F μία επέκταση του F. Αν το B είναι ενδιάμεσο σώμα της επέκτασης E/F και είναι σώμα ανάλυσης του $g(x) \in F[x]$ πάνω από το F, τότε η $\mathrm{Gal}(E/B)$ είναι κανονική υποομάδα της $\mathrm{Gal}(E/F)$ και υπάρχει εμφύτευση ομάδων:*

$$\mathrm{Gal}(E/F)/\mathrm{Gal}(E/B) \hookrightarrow \mathrm{Gal}(B/F).$$

Αν το E είναι σώμα ανάλυσης ενός πολυωνύμου $f(x) \in F[x]$, τότε

$$\mathrm{Gal}(E/F)/\mathrm{Gal}(E/B) \cong \mathrm{Gal}(B/F).$$

Απόδειξη. Αφού το B είναι το σώμα ανάλυσης του $g(x)$ πάνω από το F, έπεται ότι $B = F(b_1, \ldots, b_n)$, όπου b_i είναι οι ρίζες του $g(x)$, για $i = 1, \ldots, n$. Έστω $\sigma \in \mathrm{Gal}(E/F)$. Θα αποδείξουμε ότι

$$\phi : \mathrm{Gal}(E/F) \longrightarrow \mathrm{Gal}(B/F), \quad \sigma \mapsto \sigma|_B$$

είναι συνάρτηση, δηλ. ότι $\sigma|_B : B \longrightarrow B \in \mathrm{Gal}(B/F)$. Αφού ο σ είναι ομομορφισμός δακτυλίων, αρκεί να δείξουμε ότι $\sigma(B) \subset B$. Όμως, τα στοιχεία του B είναι πολυωνυμικοί συνδυασμοί των $b_1, \ldots, b_n$. Έτσι, αρκεί να δείξουμε ότι $\sigma(b_i) \in B$, για $1 \leq i, j \leq n$. Αυτό, όμως, προκύπτει εύκολα, αφού $\sigma(b_i) = b_j$, για $1 \leq i, j \leq n$, σύμφωνα με την Πρόταση 2.3.2. Είναι εύκολο να δει κανείς ότι η συνάρτηση ϕ είναι ομομορφισμός ομάδων:

$$\phi(\sigma_1\sigma_2) = (\sigma_1\sigma_2)|_B = (\sigma_1|_B)(\sigma_2|_B) = \phi(\sigma_1)\phi(s_2).$$

Σύμφωνα με το Πρώτο Θεώρημα Ισομορφίας Ομάδων, ο πυρήνας $\ker\phi$ είναι κανονική υποομάδα της $\mathrm{Gal}(E/F)$ και

$$\mathrm{Gal}(E/F)/\ker\phi \cong \mathrm{Im}\phi, \text{ άρα } \mathrm{Gal}(E/F)/\ker\phi \hookrightarrow \mathrm{Gal}(E/B). \tag{3.3.2.1}$$

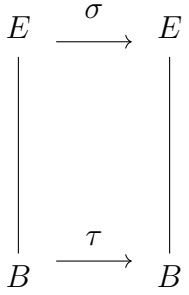
Στη συνέχεια θα δείξουμε ότι $\ker\phi = \mathrm{Gal}(E/B)$. Πράγματι,

$$\ker\phi = \{\sigma \in \mathrm{Gal}(E/F) : \ \phi(\sigma) = \mathrm{id}_B\} = \{\sigma \in \mathrm{Gal}(E/F) : \ \sigma|_B = \mathrm{id}_B\} = \mathrm{Gal}(E/B).$$

Από τη σχέση (3.3.2.1), συμπεραίνουμε ότι

$$\mathrm{Gal}(E/F)/\mathrm{Gal}(E/B) \hookrightarrow \mathrm{Gal}(B/F).$$

Τέλος, αν E είναι το σώμα ανάλυσης ενός πολυωνύμου $f(x) \in F[x]$, θα δείξουμε ότι ο ομομορφισμός ϕ είναι επιμορφισμός. Έστω ότι $\tau \in \mathrm{Gal}(B/F)$. Αφού το E είναι σώμα ανάλυσης του $f(x)$ πάνω από το F, έπεται ότι το E είναι σώμα ανάλυσης του $f(x)$ πάνω από το B. Εφαρμόζουμε το Θεώρημα 3.2.1 για τον ισομορφισμό $\tau : B \to B$. Επομένως, υπάρχει $\sigma : B \longrightarrow B$ έτσι ώστε $\sigma|_B = \tau$. Αφού $\tau \in \mathrm{Gal}(B/F)$, έπεται ότι $\tau(c) = c$, για κάθε $c \in F$. Επομένως, για $c \in F$, έχουμε ότι $\sigma(c) = \sigma|_B(c) = \tau(c) = c$ και $\sigma \in \mathrm{Gal}(E/F)$. □



Σχήμα 3.8: $\sigma \in \mathrm{Gal}(E/F)$, τέτοιο ώστε $\sigma|_B = \tau$.

Παράδειγμα 3.3.3. Έστω $G = \mathrm{Gal}(\mathbb{Q}(\omega, b)/\mathbb{Q})$, όπου $b = 2^{1/3}$, $\omega = e^{2\pi i/3}$, και έστω $F = \mathbb{Q}(\omega)$, όπως στο Παράδειγμα 3.2.5. Αφού το F είναι σώμα ανάλυσης του $x^3 - 1 \in \mathbb{Q}[x]$,

$$G/\,\mathrm{Gal}(E/F) \;\cong\; \mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q}) \;\cong\; \mathbb{Z}_2.$$

Έστω E/F μία επέκταση σωμάτων. Αν $H < \mathrm{Gal}(E/F)$, το **σώμα των σταθερών στοιχείων της** H (field of constants of H in E) συμβολίζεται ως E^H και είναι το σύνολο

$$E^H = \{a \in E :\ \sigma(a) = a,\ \forall \sigma \in H\}.$$

Ο αναγνώστης καλείται να διαπιστώσει ότι το E^H είναι πράγματι σώμα και να αποδείξει τη παρακάτω σημαντική πρόταση (βλ. άσκηση 3.7.1).

Πρόταση 3.3.4. *Έστω E/F επέκταση σωμάτων και $H_1, H_2 < \mathrm{Gal}(E/F)$. Αν $H_1 < H_2$, τότε $E^{H_2} \subset E^{H_1}$.*

Στα επόμενα παραδείγματα θα υπολογίσουμε κάποια ενδιάμεσα σώματα.

Παραδείγματα 3.3.5.

1. Έστω $E = \mathbb{Q}(i)$ και $G = \mathrm{Gal}(E/\mathbb{Q})$. Τότε $G = \{id_E, \sigma_1\}$, όπου $\sigma_1(a + bi) = a - bi$. Αν $a + bi \in E^G$ τότε $b = 0$. Επομένως $E^G \cong \mathbb{Q}$.
2. Έστω $E = \mathbb{Q}(2^{1/3})$, $G = \mathrm{Gal}(E/\mathbb{Q})$. Τότε $G = \{id_E\}$ (βλ. Παράδειγμα 2.3.5.6). Επομένως $E^G \cong E$.
3. Έστω $E = \mathbb{Q}(\omega, b)$, όπου $\omega = e^{2\pi i/3}$, $b = 2^{1/3}$ και έστω $G = \mathrm{Gal}(E/\mathbb{Q})$. Στο Παράδειγμα 2.3.6 υπολογίσαμε τα στοιχεία της G. Έστω $\sigma \in G$ ο αυτομορφισμός του E, ο οποίος καθορίζεται από τις εικόνες $\sigma(b) = \omega b$ και $\sigma(\omega) = \omega$ και $H = \langle\sigma\rangle < G$. Θα δείξουμε ότι $E^H = \mathbb{Q}(\omega)$. Πράγματι, είναι φανερό ότι $\mathbb{Q}(\omega) \subseteq E^H \subset E$. Αφού $[E : \mathbb{Q}(\omega)] = 3$, δεν υπάρχει ενδιάμεσο σώμα B έτσι ώστε $\mathbb{Q}(\omega) \subsetneq B \subsetneq E$ (βλ. Πόρισμα 2.2.16) και άρα $E^H = \mathbb{Q}(\omega)$. Θα επιβεβαιώσουμε αυτό το συμπέρασμα με αναλυτικούς υπολογισμούς. Για να το δείξουμε αυτό, θα χρησιμοποιήσουμε το ανάγωγο πολυώνυμο του ω πάνω από το $\mathbb{Q}$. Παρατηρούμε, λοιπόν, ότι $\omega^2 = -1 - \omega$, αφού $\mathrm{irr}_{\mathbb{Q},\omega} = x^2 + x + 1$. Στη συνέχεια, θεωρούμε τη $\mathbb{Q}$-βάση $\{1, \omega, b, b\omega, b^2, b^2\omega\}$ του E και υπολογίζουμε τις εικόνες των στοιχείων της, όπως φαίνεται στον παρακάτω πίνακα:

$$\begin{aligned}
\sigma(1) &= 1\\
\sigma(\omega) &= \omega\\
\sigma(b) &= b\omega\\
\sigma(b\omega) &= b\omega^2 = -b - b\omega\\
\sigma(b^2) &= b^2\omega^2 = -b^2 - b^2\omega\\
\sigma(b^2\omega) &= b^2\omega^3 = b^2
\end{aligned}$$

Έστω

$$a = a_0 + a_1\omega + a_2 b + a_3 b\omega + a_4 b^2 + a_5 b^2\omega \in E,\ a_i \in \mathbb{Q}\ .$$

Τότε

$$\sigma(a) = a_0 + a_1\omega - a_3 b + (a_2 - a_3)b\omega + (a_5 - a_4)b^2 - a_4 b^2.$$

Επομένως, το $a \in E^H$, δηλ. $a = \sigma(a)$ αν και μόνο αν $a_2 = -a_3$, $a_3 = a_2 - a_3$, $a_5 = a_5 - a_4$ και $a_5 = -a_4$. Λύνοντας αυτές τις εξισώσεις για $a_2, \ldots, a_5$, προκύπτει ότι η μόνη λύση είναι η μηδενική. Άρα

$$E^H = \{a_0 + a_1\omega :\ a_i \in \mathbb{Q}\} = \mathbb{Q}(\omega).$$

Έστω E/F μία επέκταση σωμάτων. Στην επόμενη ενότητα θα δούμε ότι $E^{\mathrm{Gal}(E/F)} = F$ αν και μόνο αν το E είναι σώμα ανάλυσης ενός διαχωρίσιμου πολυωνύμου $f(x) \in F[x]$.

3.4 Ιδιότητες της ομάδας Galois

Στο εδάφιο αυτό θα ορίσουμε τις επεκτάσεις Galois, θα εξετάσουμε βασικές ιδιότητές τους και θα αποδείξουμε ικανές και αναγκαίες συνθήκες για να είναι μία επέκταση σωμάτων επέκταση Galois. Έτσι θα ετοιμάσουμε το έδαφος για την απόδειξη του Θεμελιώδους Θεωρήματος της Θεωρίας Galois που είναι το αντικείμενο του επόμενου εδαφίου.

Ορισμός 3.4.1. *Η επέκταση E/F λέγεται **επέκταση του Galois** (Galois extension) αν το E είναι σώμα ανάλυσης ενός διαχωρίσιμου πολυωνύμου $f(x) \in F[x]$.*

Είναι φανερό ότι αν E/F είναι μία επέκταση του Galois και B είναι ενδιάμεσο σώμα τότε E/B είναι επέκταση του Galois. Η πράξη της ομάδας Galois είναι βέβαια η σύνθεση των F-αυτομορφισμών. Αν θεωρήσουμε γραμμικούς συνδυασμούς των F-αυτομορφισμών με συντελεστές από το E, το αποτέλεσμα δεν είναι πια κατανάγκην F-αυτομορφισμός. Παρόλα αυτά, δεν είναι δύσκολο να δει κανείς ότι ένας τέτοιος γραμμικός συνδυασμός δίνει έναν ομομορφισμό της προσθετικής ομάδας του E. Αναλυτικά, αν $\sigma_1, \ldots, \sigma_n \in \mathrm{Gal}(E/F)$ και $y_1, \ldots, y_n \in E$, τότε $\sum y_i\sigma_i$ ορίζεται ως εξής:

$$\sum y_i\sigma_i :\ E \longrightarrow E, \quad b \mapsto \sum y_i\sigma_i(b).$$

Είναι φανερό ότι το $\sum y_i\sigma_i$, για κατάλληλα y_i, έχει μη μηδενικό πυρήνα. Για ένα απλό παράδειγμα, ας θεωρήσουμε τους $\mathbb{Q}$-αυτομορφισμούς σ και σ^2 του Παραδείγματος 2.3.6. Τότε $(\sigma - \sigma^2)\ (\omega) = \sigma(\omega) - \sigma^2(\omega) = 0$ και είναι φανερό ότι $\sigma - \sigma^2$ δεν είναι η μηδενική συνάρτηση στο E, αφού $(\sigma - \sigma^2)\ (b) = (w - w^2)b \neq 0$. Είναι γενικά δυνατόν να βρούμε κάποιον (μη μηδενικό) γραμμικό συνδυασμό $\sum y_i\sigma_i$ των στοιχείων της G που να είναι η μηδενική συνάρτηση στο E; Σε αυτό το ερώτημα απαντά η επόμενη πρόταση.

Λήμμα 3.4.2. *Έστω E/F πεπερασμένη επέκταση, $\{\sigma_1, \ldots, \sigma_n\}$ διακεκριμένα στοιχεία της $\mathrm{Gal}(E/F)$ και $y_1, \ldots, y_n \in E$. Αν $y_1\sigma_1 + \cdots + y_n\sigma_n :\ E \longrightarrow E$ είναι η μηδενική συνάρτηση, δηλ. αν*

$$\sum_{i=1}^{n} y_i\sigma_i(b) = 0, \quad \forall\ b \in E,$$

τότε $y_i = 0,$ για $i = 1, \ldots, n$.

Απόδειξη. Έστω ότι υπάρχουν $y_1, \ldots, y_n \in E$ όχι όλα μηδέν έτσι ώστε

$$y_1\sigma_1(b) + \cdots + y_n\sigma_n(b) = 0, \quad \forall\, b \in E. \tag{3.4.2.1}$$

Χωρίς περιορισμό της γενικότητας μπορούμε να υποθέσουμε ότι $y_n \neq 0$. Αφού $\sigma_n \neq \sigma_1$, υπάρχει $c \in E$ έτσι ώστε $\sigma_n(c) \neq \sigma_1(c)$. Είναι φανερό ότι $c \in E \setminus E^G$ και ότι, αφού $c \neq 0$, $\sigma_1(c)\sigma_n(c) \neq 0$.

Αντικαθιστούμε στη σχέση (3.4.2.1) το στοιχείο bc στη θέση του b. Έστω ότι $\sigma_i(c) = c_i$. Επομένως,

$$y_1c_1\sigma_1(b) + \cdots + y_nc_n\sigma_n(b) = 0. \tag{3.4.2.2}$$

Πολλαπλασιάζοντας τη σχέση (3.4.2.1) με c_1 και αφαιρώντας από τη σχέση (3.4.2.2) βρίσκουμε ότι

$$y_2(c_2 - c_1)\sigma_2(b) + \cdots + y_n(c_n - c_1)\sigma_n(b) = 0. \tag{3.4.2.3}$$

Παρατηρούμε ότι ο συντελεστής του $\sigma_n(b)$ στη σχέση (3.4.2.3) είναι και πάλι διάφορος του μηδενός. Άρα υπάρχει $(z_2, \ldots, z_n)$, όπου $z_n \neq 0$, έτσι ώστε

$$\forall\, b \in E:\ z_2\sigma_2(b) + \cdots + z_n\sigma_n(b) = 0.$$

Επαναλαμβάνουμε αυτή τη διαδικασία άλλες $n-2$ φορές. Καταλήγουμε στο συμπέρασμα ότι υπάρχει μη μηδενικό $t \in E$ έτσι ώστε $t\sigma_n(b) = 0$, $\forall\, b \in E$. Άρα $\forall\, b \in E$, $\sigma_n(b) = 0$. Αυτό, όμως, είναι αδύνατον, αφού σ_n είναι αυτομορφισμός του E. Καταλήξαμε σε άτοπο, γιατί υποθέσαμε ότι υπάρχουν $y_1, \ldots, y_n \in E$, όχι όλα μηδέν, έτσι ώστε $y_1\sigma_1 + \cdots + y_n\sigma_n$ να είναι η μηδενική συνάρτηση στο E. Άρα αυτό είναι αδύνατον. □

Εξαιτίας της ιδιότητας του Λήμματος 3.4.2 λέμε ότι τα στοιχεία της $\mathrm{Gal}(E/F)$ είναι ***γραμμικά ανεξάρτητα*** (linearly indenpendent) πάνω από το σώμα E. Μία σημαντική συνέπεια είναι το παρακάτω Θεώρημα, γνωστό ως το Λήμμα του Artin.

Θεώρημα 3.4.3 (Artin). *Έστω E/F πεπερασμένη επέκταση. Τότε $[E : E^G] \geq n$, όπου $G = \mathrm{Gal}(E/F)$ και n είναι η τάξη της G.*

Απόδειξη. Έστω ότι $[E : E^G] = m < n$ και ότι $\{a_1, \ldots, a_m\}$ είναι μία E^G-βάση του E. Κάθε στοιχείο $b \in E$ γράφεται ως E^G-γραμμικός συνδυασμός:

$$b = c_1a_1 + \cdots + c_ma_m = \sum c_ia_i,\ c_i \in E^G.$$

Αν $\sigma \in G$, τότε $\sigma(c_i) = c_i$, για $i = 1, \ldots, m$, και άρα $\sigma \in G$ είναι μία E^G-γραμμική συνάρτηση:

$$\sigma(b) = \sigma(\sum c_ia_i) = \sum c_i\sigma(a_i).$$

Θεωρούμε το ομογενές σύστημα με m εξισώσεις και n αγνώστους στο E:

$$\begin{aligned} \sigma_1(a_1)x_1 + \cdots + \sigma_n(a_1)x_n &= 0 \\ &\vdots \\ \sigma_1(a_m)x_1 + \cdots + \sigma_n(a_m)x_n &= 0. \end{aligned}$$

Αφού $m < n$, το σύστημα έχει μία μη μηδενική λύση στο E, έστω $(y_1, \ldots, y_n) \neq 0$ μία τέτοια λύση. Δηλαδή, για $i = 1, \ldots, m$, ισχύει ότι

$$y_1\sigma_1(a_i) + \cdots + y_n\sigma_n(a_i) = 0. \tag{3.4.3.1}$$

Αφού η σχέση (3.4.3.1) ισχύει για κάθε στοιχείο της E^G-βάσης του E, είναι εύκολο να δείξουμε ότι ισχύει για κάθε $b \in E$. Πράγματι, έστω ότι $b = \sum c_i\, a_i$ με $c_i \in E^G$, για $i = 1, \ldots, m$. Θα δείξουμε ότι

$$y_1\sigma_1(b) + \cdots + y_n\sigma_n(b) = 0. \tag{3.4.3.2}$$

Παρατηρούμε ότι αν $c \in E^G$, τότε

$$c\,\sigma_j(a_i) = \sigma_j(c)\sigma_j(a_i) = \sigma_j(c\,a_i), \quad 1 \leq j \leq n.$$

Πολλαπλασιάζοντας την εξίσωση (3.4.3.1) με c_t, για $t = 1, \ldots, m$, προκύπτουν οι παρακάτω m ισότητες:

$$\begin{aligned} y_1\sigma_1(c_1a_i) + \cdots + y_n\sigma_n(c_1a_i) &= 0 \\ &\vdots \\ y_1\sigma_1(c_ma_i) + \cdots + y_n\sigma_n(c_ma_i) &= 0. \end{aligned}$$

Προσθέτοντας τις παραπάνω σχέσεις, έπεται ότι

$$y_1\sigma_1(c_1a_1 + \cdots + c_ma_m) + \cdots + y_n\sigma_n(c_1a_1 + \cdots + c_ma_m) = 0,$$

δηλ. η σχέση (3.4.3.2). Από το Λήμμα 3.4.2, αυτό είναι άτοπο. Καταλήξαμε σε άτοπο γιατί υποθέσαμε ότι $m < n$. Άρα $m \geq n$. □

Θα αποδείξουμε, τώρα, ότι το σταθερό σώμα της ομάδας $\mathrm{Gal}(E/F)$ είναι το F.

Θεώρημα 3.4.4. *Έστω E/F επέκταση του Galois. Τότε $E^{\mathrm{Gal}(E/F)} = F$.*

Απόδειξη. Σύμφωνα με το Πόρισμα 3.2.4, $|\mathrm{Gal}(E/F)| = [E : F]$. Έστω $G = \mathrm{Gal}(E/F)$ και $n = |\mathrm{Gal}(E/F)|$. Αφού

$$[E : F] = [E : E^G]\,[E^G : F],$$

για να δείξουμε ότι $E^G = F$, αρκεί να δείξουμε ότι $[E^G : F] = 1$ ή ισοδύναμα ότι $[E : E^G] = n$. Είναι προφανές ότι $[E : E^G] \leq n$. Σύμφωνα με το Θεώρημα 3.4.3 $[E : E^G] \geq n$. Επομένως $[E : E^G] = n$ και $E^G = F$. □

Σημειώνουμε μία εξαιρετικά σημαντική ιδιότητα εκείνων των πεπερασμένων επεκτάσεων E/F, για τις οποίες $E^{\mathrm{Gal}(E/F)} = F$.

Θεώρημα 3.4.5. *Έστω E/F μία πεπερασμένη επέκταση έτσι ώστε $E^{\mathrm{Gal}(E/F)} = F$. Κάθε ανάγωγο πολυώνυμο $p(x) \in F[x]$ που έχει μία ρίζα στο E είναι διαχωρίσιμο και έχει όλες τις ρίζες του στο E.*

Απόδειξη. Έστω $G = \mathrm{Gal}(E/F)$ και έστω $b \in E$ ρίζα του ανάγωγου πολυωνύμου $p(x) \in F[x]$. Θα δείξουμε ότι το $p(x)$ αναλύεται σε γινόμενο γραμμικών παραγόντων στο $E[x]$ και ότι οι ρίζες του $p(x)$ είναι απλές. Έστω ότι το σύνολο $X = \{\sigma(b) :\ \sigma \in G\}$ των συζυγών του b είναι $X = \{b_1, \ldots, b_n\}$, δηλ. $b_1, \ldots, b_n$ είναι οι διακεκριμένες εικόνες του b μέσω των στοιχείων της G. Σύμφωνα με την Πρόταση 2.3.2 τα στοιχεία του X είναι ρίζες του $p(x)$. Θεωρούμε το πολυώνυμο

$$\begin{aligned} g(x) = (x - b_1)\cdots(x - b_n) = x^n - (b_1 + \cdots + b_n)x^{n-1} + \\ (b_1b_2 + \cdots + b_{n-1}b_n)x^{n-2} + \cdots + (-1)^n b_1 \cdots b_n = \sum c_j x^j \in E[x] \end{aligned}$$

Θα δείξουμε ότι $g(x) = p(x)$. Πράγματι, για $j = 0, \ldots, n-1$, οι συντελεστές c_j του x^j είναι εκφράσεις συμμετρικές ως προς τα $b_1, \ldots, b_n$. Επομένως, αν $\sigma \in G$, τότε $\sigma(c_j) = c_j$. Άρα $c_j \in E^G$. Αφού $E^G = F$, έπεται ότι $g(x) \in F[x]$. Αφού όλες οι ρίζες του $g(x)$ είναι διακεκριμένες και είναι ρίζες του $p(x)$ έπεται ότι το $g(x)$ διαιρεί το $p(x)$ στον δακτύλιο $F[x]$, βλ. άσκηση 1.5.17. Επομένως $g(x) = p(x)$, δηλ. το $p(x)$ είναι διαχωρίσιμο και αναλύεται σε γινόμενο γραμμικών παραγόντων στο $E[x]$. □

Θα δείξουμε, τώρα, ότι ισχύει το αντίστροφο του Θεωρήματος 3.4.4.

Θεώρημα 3.4.6. *Έστω E/F μία πεπερασμένη επέκταση σωμάτων και $G = \mathrm{Gal}(E/F)$. Αν κάθε ανάγωγο πολυώνυμο $p(x) \in F[x]$ που έχει μία ρίζα στο E είναι διαχωρίσιμο και έχει όλες τις ρίζες του στο E, τότε η επέκταση E/F είναι επέκταση του Galois.*

Απόδειξη. Υποθέτουμε ότι $[E : F] > 1$ και επιλέγουμε ένα στοιχείο $a_1 \in E \setminus F$. Το a_1 είναι αλγεβρικό πάνω από το F, αφού η επέκταση E/F είναι πεπερασμένη. Έστω $p_1(x) = \mathrm{irr}_{(F,a_1)}(x)$. Από την υπόθεση, το $p_1(x)$ είναι διαχωρίσιμο και έχει όλες τις ρίζες του στο E. Επισυνάπτουμε στο F τις ρίζες του $p_1(x)$ και θεωρούμε E_1 το σώμα ανάλυσης του $p_1(x)$. Αν $E_1 = E$, τότε E/F είναι επέκταση του Galois. Διαφορετικά, υπάρχει $a_2 \in E \setminus E_1$. Έστω $p_2(x) = \mathrm{irr}_{(F,a_2)}(x)$. Επισυνάπτοντας στο E_1 τις ρίζες του $p_2(x)$ παίρνουμε το E_2, που είναι σώμα ανάλυσης του $p_1(x)p_2(x) \in F[x]$. Συνεχίζουμε με αυτόν τον τρόπο μέχρις ότου βρούμε ένα σώμα $E_m = E$. Αυτό θα συμβεί μετά από πεπερασμένου πλήθους βήματα, γιατί η επέκταση E/F είναι πεπερασμένη. □

Στο παρακάτω θεώρημα συγκεντρώνουμε τις ικανές και αναγκαίες συνθήκες ώστε μία επέκταση σωμάτων E/F να είναι επέκταση του Galois αξιοποιώντας τα προηγούμενα συμπεράσματα αυτού του εδαφίου.

Θεώρημα 3.4.7. *Έστω E/F μία πεπερασμένη επέκταση σωμάτων και $G = \mathrm{Gal}(E/F)$. Οι επόμενες συνθήκες είναι ισοδύναμες:*

i. Η επέκταση E/F είναι επέκταση του Galois.

ii. $F = E^G = \{a \in E : \sigma(a) = a, \forall\ \sigma \in G\}$.

iii. Κάθε ανάγωγο πολυώνυμο $p(x) \in F[x]$ που έχει μία ρίζα στο E είναι διαχωρίσιμο και έχει όλες τις ρίζες του στο E.

Απόδειξη. Η συνεπαγωγή (i ⇒ ii) είναι το Θεώρημα 3.4.4. Η συνεπαγωγή (ii ⇒ iii) είναι το Θεώρημα 3.4.5. Τέλος, η συνεπαγωγή (iii ⇒ i) είναι το Θεώρημα 3.4.6. □

Πριν ολοκληρώσουμε τα προκαταρτικά της απόδειξης του Θεμελιώδους Θεωρήματος της Θεωρίας Galois ας μελετήσουμε λίγο προσεκτικότερα την απόδειξη του Θεωρήματος 3.4.3. Πού ακριβώς χρησιμοποιήσαμε ότι το σύνολο $G = \mathrm{Gal}(E/F)$ έχει την αλγεβρική δομή ομάδας; Παρατηρούμε, λοιπόν, ότι η δομή της ομάδας δεν έπαιξε κανέναν ρόλο στην απόδειξη. Παρόλα αυτά, η εκφώνηση του θεωρήματος αναφερόταν στην G και στο σταθερό σώμα E^G. Είναι, όμως, αναγκαίο να περιοριστούμε σε σταθερά σώματα υποομάδων της ομάδας Galois; Μπορούμε να γενικεύσουμε τον ορισμό του σταθερού σώματος E^X, όπου X τυχαίο υποσύνολο της G; Πράγματι, παρατηρούμε ότι το σύνολο

$$E^X = \{a \in E :\ \sigma(a) = a,\ \forall \sigma \in X\}$$

είναι ενδιάμεσο σώμα της επέκτασης E/F για κάθε υποσύνολο X της G. Επομένως προκύπτει η παρακάτω γενική μορφή του Θεωρήματος του Artin (Θεώρημα 3.4.3).

Θεώρημα 3.4.8. *Έστω E/F πεπερασμένη επέκταση και $X \subset \mathrm{Gal}(E/F)$. Τότε $[E : E^X] \geq |X|$.*

Στην περίπτωση που το X είναι υποομάδα της $\mathrm{Gal}(E/F)$ μπορούμε να αποδείξουμε ότι ισχύει ισότητα στο παραπάνω θεώρημα.

Θεώρημα 3.4.9. *Έστω E/F πεπερασμένη επέκταση και $H \leq \mathrm{Gal}(E/F)$. Τότε $[E : E^H] = |H|$.*

Απόδειξη. Έστω ότι $H = \{\sigma_1, \ldots, \sigma_n\}$. Θα αποδείξουμε ότι οποιαδήποτε $n+1$ στοιχεία του E είναι γραμμικά εξαρτημένα πάνω από το σώμα E^H. Έστω $\{a_1, \ldots, a_{n+1}\}$ ένα E^H-γραμμικά ανεξάρτητο υποσύνολο του E. Θεωρούμε το ομογενές σύστημα με n εξισώσεις και $n+1$ αγνώστους στο E:

$$\begin{aligned} \sigma_1(a_1)x_1 + \cdots + \sigma_1(a_{n+1})x_{n+1} &= 0 \\ &\vdots \\ \sigma_n(a_1)x_1 + \cdots + \sigma_n(a_{n+1})x_{n+1} &= 0. \end{aligned} \tag{3.4.9.1}$$

Έστω $(c_1, \ldots, c_n, c_{n+1})$ μία μη μηδενική λύση. Χωρίς βλάβη της γενικότητας μπορούμε να θεωρήσουμε ότι $c_{n+1} \neq 0$ και κατά συνέπεια (διαιρώντας με το c_{n+1}) ότι $r = (r_1, \ldots, r_n, r_{n+1})$ είναι λύση του παραπάνω συστήματος, με $r_{n+1} = 1$. Επομένως

$$\sum_{j=1}^{n+1} \sigma_i(a_j) r_j = 0, \quad i = 1, \ldots, n. \tag{3.4.9.2}$$

Το 1 ανήκει, βέβαια, στο E^H. Όμως, υπάρχει κάποιο r_t, για $t = 1, \ldots, n$, έτσι ώστε $r_t \notin E^H$. Διαφορετικά, $\sigma_1(r_j) = r_j$, για $j = 1, \ldots, n+1$, και καταλήγουμε σε άτοπο εξαιτίας της γραμμικής ανεξαρτησίας του $\{a_1, \ldots, a_{n+1}\}$ πάνω από το E^H:

$$\sum_{i=1}^{n+1} \sigma_1(a_j) r_j = 0 \Rightarrow \sum_{i=1}^{n+1} \sigma_1(a_j)\sigma_1(r_j) = 0 \Rightarrow \sum_{i=1}^{n+1} \sigma_1(a_j r_j) = 0 \Rightarrow \sum_{i=1}^{n+1} a_j r_j = 0.$$

Έστω ότι το στοιχείο $\sigma \in H$ είναι αυτό που μετακινεί το r_t, δηλ. $\sigma(r_t) \neq r_t$. Από το σύστημα (3.4.9.2) προκύπτει, λοιπόν, ότι:

$$\sigma\left(\sum_{j=1}^{n+1} \sigma_i(a_j) r_j\right) = 0, \quad i = 1, \ldots, n,$$

δηλ.

$$\sum_{j=1}^{n+1} \sigma\sigma_i\,(a_j)\,\sigma(r_j) = 0, \quad i = 1, \ldots, n. \tag{3.4.9.3}$$

Όμως, η H είναι ομάδα και επομένως

$$\{\sigma\sigma_1, \ldots, \sigma\sigma_n\} = \{\sigma_1, \ldots, \sigma_n\}.$$

Άρα, σύμφωνα με τη σχέση (3.4.9.3), $r' = (\sigma(r_1), \ldots, \sigma(r_n), 1)$ είναι επίσης λύση του συστήματος (3.4.9.1). Επομένως και η διαφορά

$$r - r' = (r_1 - \sigma(r_1), \ldots, r_n - \sigma(r_n), 0)$$

είναι λύση του συστήματος (3.4.9.1) και μάλιστα μη μηδενική, αφού $r_t - \sigma(r_t) \neq 0$. Συνεχίζοντας καταυτόν τον τρόπο καταλήγουμε σε μία μη μηδενική λύση του συστήματος (3.4.9.1) με μία μόνο μη μηδενική συντεταγμένη. Αυτό όμως οδηγεί σε άτοπο, αφού αν $c \neq 0$ και $\sigma_i(a_t)c = 0$, τότε $a_t = 0$ και δεν μπορεί να είναι μέρος κανενός γραμμικά ανεξάρτητου συνόλου πάνω από το E^H. Αποδείξαμε λοιπόν ότι οποιαδήποτε $n+1$ στοιχεία του E είναι γραμμικά εξαρτημένα πάνω από το σώμα E^H. Άρα $[E : E^H] \leq n$ και από το Θεώρημα 3.4.8 προκύπτει ότι $[E : E^H] = n$, δηλ. $[E : E^H] = |H|$. □

3.5 Θεμελιώδες Θεώρημα Θεωρίας Galois

Στο εδάφιο αυτό όπως προαναγγείλαμε θα αποδείξουμε το Θεμελιώδες Θεώρημα της Θεωρίας Galois. Έστω E/F μία επέκταση Galois και έστω $\mathcal{A}$ το σύνολο των ενδιάμεσων σωμάτων της επέκτασης E/F και $\mathcal{D}$ το σύνολο των υποομάδων της $\mathrm{Gal}(E/F)$. Το Θεμελιώδες Θεώρημα της Θεωρίας Galois αφορά την αντιστοιχία ανάμεσα στα στοιχεία του $\mathcal{A}$ και του $\mathcal{D}$.

Θεώρημα 3.5.1 (Θεμελιώδες Θεώρημα της Θεωρίας Galois). *Έστω E/F μία επέκταση του Galois $G = \mathrm{Gal}(E/F)$. Τότε υπάρχει μία αμφιμονότιμη και επί συνάρτηση f μεταξύ των στοιχείων του συνόλου $\mathcal{A}$ των ενδιάμεσων σωμάτων της επέκτασης E/F και των στοιχείων του συνόλου $\mathcal{D}$ των υποομάδων της G:*

$$f : \mathcal{A} \longrightarrow \mathcal{D}, \qquad B \mapsto \mathrm{Gal}(E/B).$$

Αντίστροφα, αν H είναι υποομάδα της G τότε η αντιστοιχία

$$\phi : \mathcal{D} \longrightarrow \mathcal{A}, \qquad H \mapsto E^H$$

έχει τις εξής ιδιότητες:

i. $[B : F] = [G : \mathrm{Gal}(E/B)]$ *και* $[G : H] = [E^H : F]$

ii. $E^{\mathrm{Gal}(E/B)} = B$ *και* $\mathrm{Gal}(E/E^H) = H$

iii. B/F *είναι επέκταση Galois αν και μόνο αν* $\mathrm{Gal}(E/B) \trianglelefteq G$.

Απόδειξη. Είναι φανερό ότι οι f και ϕ είναι συναρτήσεις. Θα αποδείξουμε πρώτα το (ii). Η E/F είναι επέκταση του Galois, οπότε η E/B είναι επέκταση του Galois. Από το Θεώρημα 3.4.7, έπεται ότι $E^{\mathrm{Gal}(E/B)} = B$. Άρα

$$\mathrm{Gal}(E/B_1) = \mathrm{Gal}(E/B_2) \Rightarrow E^{\mathrm{Gal}(E/B_1)} = E^{\mathrm{Gal}(E/B_2)} \Rightarrow B_1 = B_2$$

και η f είναι αμφιμονότιμη.

Έστω τώρα $H \leq G$ και $H' = \mathrm{Gal}(E/E^H) = \{\sigma \in G : \ \sigma|_{E^H} = \mathrm{id}_{E^H}\}$. Είναι φανερό ότι $H \subseteq H'$ και άρα

$$|H| \leq |H'|. \tag{3.5.1.1}$$

Επίσης, αφού η E/E^H είναι επέκταση του Galois, από το Θεώρημα 3.4.4 , προκύπτει ότι

$$E^{\mathrm{Gal}(E/E^H)} = E^H.$$

Από το Πόρισμα 3.2.4, έπεται ότι

$$|H'| = [E : E^H]. \tag{3.5.1.2}$$

Σύμφωνα με το Θεώρημα 3.4.9,

$$[E : E^H] = |H|. \tag{3.5.1.3}$$

Άρα $|H| = |H'|$ και $\mathrm{Gal}(E/E^H) = H$. Επομένως

$$E^{H_1} = E^{H_2} \Rightarrow \mathrm{Gal}(E/E^{H_1}) = \mathrm{Gal}(E/E^{H_2}) \Rightarrow H_1 = H_2$$

και η ϕ είναι αμφιμονότιμη. Είναι φανερό ότι οι f και ϕ είναι αντίστροφες συναρτήσεις, άρα είναι επί.

Στη συνέχεια αποδεικνύουμε το (i). Αφού οι f και ϕ είναι αντίστροφες συναρτήσεις, αρκεί να αποδείξουμε τη μία από τις δύο ισότητες. Έστω B ενδιάμεσο σώμα και $H = \mathrm{Gal}(E/B)$. Αφού E/B είναι επέκταση του Galois, $[E : B] = |H|$ (Πόρισμα 3.2.4). Από τη σχέση

$$[E : F] = [E : B]\,[B : F]$$

προκύπτει ότι

$$|G| = |H|\,[B : F],$$

άρα, σύμφωνα με το Θεώρημα του Lagrange (Θεώρημα I.10)

$$[B : F] = [G : H] \;\Rightarrow\; [B : F] = [G : \mathrm{Gal}(E/B)].$$

Επομένως, για κάθε υποομάδα H της G ισχύει

$$[G : H] = [E^H : F].$$

Τέλος, για το (iii), παρατηρούμε ότι αν B/F είναι επέκταση του Galois τότε $\mathrm{Gal}(E/B) \trianglelefteq G$, από το Θεώρημα 3.3.2. Για την αντίστροφη κατεύθυνση, ας υποθέσουμε ότι $H \trianglelefteq G$, όπου $H = \mathrm{Gal}(E/B)$. Αυτό σημαίνει ότι αν $\sigma \in G$ και $\tau \in H$, τότε $\sigma\tau' = \tau\sigma$, για κάποιο $\tau' \in H$ (βλ. Ορισμό I.11). Για κάθε $a \in E$, έχουμε $\sigma\tau'(a) = \tau\sigma(a)$. Αν $a \in E^H$, δηλ. αν $a \in B$, τότε $\tau(a) = a$, άρα $\sigma(a) = \tau\sigma(a)$. Επομένως $\sigma(a) \in E^H$, για κάθε $\sigma \in G$ και για κάθε $a \in E^H$, δηλ. $\sigma(B) \subseteq B$. Θα αποδείξουμε ότι η επέκταση B/F είναι επέκταση του Galois εφαρμόζοντας το Θεώρημα 3.4.7. Έστω $p(x) \in F[x]$ ένα ανάγωγο πολυώνυμο που έχει μία ρίζα $b \in B$. Θα αποδείξουμε ότι όλες οι ρίζες του $p(x)$ ανήκουν στο B. Ας υποθέσουμε ότι υπάρχει μία ρίζα γ του $p(x)$ και $\gamma \notin B$. Βέβαια όλες οι ρίζες του $p(x)$ ανήκουν στο σώμα E, γιατί το $p(x)$ έχει μία ρίζα στο E (Θεώρημα 3.4.7). Θεωρούμε τον F-ισομορφισμό του Θεωρήματος 2.3.3:

$$F(b) \longrightarrow F(\gamma), \quad b \mapsto \gamma,$$

και ο οποίος επεκτείνεται σε έναν F-αυτομορφισμό σ του E, (Θεώρημα 3.2.1). Άρα $\sigma \in G$. Όμως $\sigma(B) \nsubseteq B$, αφού $\sigma(b) = \gamma \notin B$. Αυτό είναι άτοπο, γιατί όπως είδαμε $\sigma(B) \subseteq B$, για κάθε $\sigma \in G$. Άρα όλες οι ρίζες του $p(x)$ ανήκουν στο B και η επέκταση B/F είναι επέκταση του Galois σύμφωνα με το Θεώρημα 3.4.7. □

Σημειώνουμε το παρακάτω πόρισμα του Θεμελιώδους Θεωρήματος της Θεωρίας Galois.

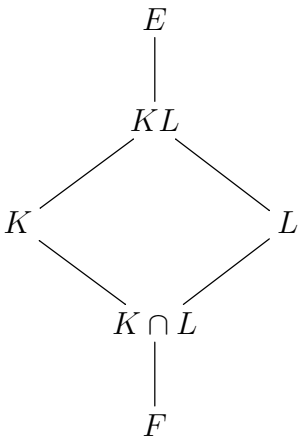
Πόρισμα 3.5.2. *Έστω E/F μία επέκταση Galois. Η επέκταση έχει πεπερασμένο αριθμό ενδιάμεσων σωμάτων.*

Απόδειξη. Η ομάδα $\mathrm{Gal}(E/F)$ είναι πεπερασμένη και έχει πεπερασμένο αριθμό υποομάδων. Επομένως, σύμφωνα με το Θεμελιώδες Θεώρημα της Θεωρίας Galois υπάρχουν πεπερασμένου πλήθους ενδιάμεσα σώματα. □

Αν K, L είναι σώματα, τότε με KL συμβολίζουμε το μικρότερο σώμα που περιέχει το K και το L. Το παρακάτω θεώρημα αναφέρεται και ως θεώρημα του παραλληλογράμμου για τις επεκτάσεις του Galois.

Θεώρημα 3.5.3. *Έστω ότι E/F είναι επέκταση σωμάτων, L, K ενδιάμεσα υποσώματα της επέκτασης τέτοια ώστε L/F να είναι επέκταση του Galois. Τότε οι KL/K και $L/\, L \cap K$ είναι επεκτάσεις του Galois και $\mathrm{Gal}(KL/K)$ είναι ισόμορφη με την $\mathrm{Gal}\,(L/(L \cap K))$.*

Σχηματικά, το θεώρημα συνδέει τις παράλληλες πλευρές του εσωτερικού παραλληλογράμμου του σχήματος 3.9.



Σχήμα 3.9: Θεώρημα του Παραλληλογράμμου

Απόδειξη. Αφού L/F είναι επέκταση του Galois και $F \subset L \cap K$, η επέκταση $L/(L \cap K)$ είναι επέκταση του Galois. Άρα το L είναι σώμα ανάλυσης ενός διαχωρίσιμου πολυωνύμου $g(x) \in (L \cap K)[x]$. Τότε, όμως, το $g(x) \in K[x]$ και το KL είναι σώμα ανάλυσης του $g(x)$. Άρα η KL/K είναι επίσης είναι επέκταση του Galois. Αν τώρα, ο $\sigma \in \mathrm{Gal}(KL/K)$ τότε, ο περιορισμός του σ στο σώμα L κρατά σταθερά τα στοιχεία του $(L \cap K) \subset K$ και επομένως, $\sigma|_L \in \mathrm{Gal}\,(L/(L \cap K))$. Έστω, λοιπόν, η συνάρτηση ϕ όπου

$$\phi :\ \mathrm{Gal}(KL/K) \to \mathrm{Gal}\,(L/(L \cap K))\,,\ \sigma \mapsto \sigma|_L.$$

Είναι φανερό ότι η ϕ είναι μονομορφισμός ομάδων. Θα αποδείξουμε ότι η ϕ είναι και επιμορφισμός. Για να το πετύχουμε αυτό, θέτουμε $H = \mathrm{Im}\phi$. Θα δείξουμε ότι $L^H = L \cap K$ και ο ισχυρισμός μας θα προκύψει από το Θεμελιώδες Θεώρημα της Θεωρίας Galois.

Ο εγκλεισμός $(L \cap K) \subset L^H$ είναι προφανής, αφού $(L \cap K) \subset K$ και τα στοιχεία της H είναι της μορφής $\sigma|_L$, όπου $\sigma \in \mathrm{Gal}(KL/K)$. Για την αντίστροφη κατεύθυνση, αν $a \in L^H$ τότε $a \in L$ και $\sigma|_L(a) = a$, για κάθε $\sigma \in \mathrm{Gal}(KL/K)$. Επομένως το $a \in KL$ και $\sigma(a) = a$, για κάθε $\sigma \in \mathrm{Gal}(KL/K)$, δηλ. $a \in (KL)^{\mathrm{Gal}(KL/K)}$. Όμως, σύμφωνα με το Θεμελιώδες Θεώρημα της Θεωρίας Galois, $(KL)^{\mathrm{Gal}(KL/K)} = K$ και άρα $a \in (L \cap K)$. Άρα $L^H \subset (L \cap K)$ και τελικά $H = \mathrm{Im}\phi = \mathrm{Gal}\,(L/(L \cap K))$. □

3.6 Υπολογισμοί και Παραδείγματα

Έστω $f(x) \in F[x]$ ένα κανονικό, ανάγωγο, διαχωρίσιμο πολυώνυμο βαθμού n, E το σώμα ανάλυσης του $f(x)$ πάνω από το F και $X = \{\alpha_1, \ldots, \alpha_n\} \subset E$ το σύνολο των ριζών του

$f(x)$. Με Δ συμβολίζουμε το στοιχείο

$$\Delta = \prod_{i<j}(\alpha_i - a_j) \in E.$$

Από το Θεώρημα 2.3.3 προκύπτει ότι αν $\sigma \in \mathrm{Gal}(E/F)$, τότε $\sigma(\Delta) = \pm\Delta$ και $\sigma(\Delta^2) = \Delta^2$. Επομένως $\Delta^2 \in E^G$. Αφού E/F είναι επέκταση του Galois, από το Θεώρημα 3.4.7 προκύπτει ότι

$$\Delta^2 \in F.$$

Είναι φανερό ότι το Δ^2 δεν εξαρτάται από την αρίθμηση των ριζών του $f(x)$. Η ***διακρίνουσα*** (discriminant) του $f(x)$, συμβολίζεται συνήθως με D και είναι το στοιχείο

$$D = \Delta^2.$$

Παρατηρούμε ότι όταν $\mathrm{char}\, F = 2$, τότε $-\Delta = \Delta$, συνεπώς $\sigma(\Delta) = \Delta$, για κάθε $\sigma \in \mathrm{Gal}(E/F)$, άρα $\Delta \in F$. Στη περίπτωση που $\mathrm{char}\, F \neq 2$ και $\Delta \notin F$, τότε προκύπτει ένα αξιοσημείωτο συμπέρασμα για την ομάδα $\mathrm{Gal}(E/F)$. Πράγματι, παρατηρούμε ότι

$$\mathrm{irr}_{(F,\Delta)}(x) = x^2 - D.$$

Επομένως, από το Θεώρημα 2.2.3 και το Θεμελιώδες Θεώρημα της Θεωρίας Galois (Θεώρημα 3.5.1), έπεται ότι

$$2 = [F(\Delta) : F] = [G : \mathrm{Gal}(E/F(\Delta))]. \tag{3.6.0.1}$$

Αποδείξαμε λοιπόν το εξής:

Πρόταση 3.6.1. *Έστω $f(x) \in F[x]$ ένα κανονικό, διαχωρίσιμο πολυώνυμο βαθμού n και E το σώμα ανάλυσης του $f(x)$ πάνω από το F. Αν $\Delta \notin F$, τότε η ομάδα Galois του $f(x)$ έχει μία κανονική υποομάδα με δείκτη 2.*

Θα εφαρμόσουμε τα παραπάνω όταν $\deg f(x) = 3$.

Πρόταση 3.6.2. *Έστω $f(x) \in F[x]$ ένα κανονικό, ανάγωγο, διαχωρίσιμο πολυώνυμο βαθμού 3 και E το σώμα ανάλυσης του $f(x)$. Αν $\Delta \notin F$ τότε $\mathrm{Gal}(E/F) \cong S_3$.*

Απόδειξη. Η ομάδα $\mathrm{Gal}(E/F)$ εμφυτεύεται στην S_3. Αφού $\deg f(x)$ διαιρεί την τάξη της $\mathrm{Gal}(E/F)$, έπεται ότι η τάξη της $\mathrm{Gal}(E/F)$ είναι τρία ή έξι. Αν $\Delta \notin F$ τότε, από την Πρόταση 3.6.1, το 2 διαιρεί την τάξη της ομάδας $|\mathrm{Gal}(E/F)|$ και άρα $\mathrm{Gal}(E/F) \cong S_3$. □

Στην άσκηση 3.7.5 ο αναγνώστης καλείται να διαπιστώσει ότι αν $\mathrm{char}\, F \neq 2$ και $\Delta \in F$ για ένα ανάγωγο και διαχωρίσιμο πολυώνυμο βαθμού 3, τότε $\mathrm{Gal}(E/F) \cong A_3$.

Παράδειγμα 3.6.3. Έστω $f(x) = x^3 - 3x - 1 \in \mathbb{Q}[x]$. Το $f(x)$ είναι ανάγωγο στο $\mathbb{Q}[x]$, αφού μπορεί να αποδειχθεί ότι δεν έχει ρίζες στο $\mathbb{Q}$ (βλ. Πρόταση 1.3.2). Έστω E το σώμα ανάλυσης του $f(x)$ πάνω από το $\mathbb{Q}$. Μπορεί να δείξει κανείς ότι $\Delta \in \mathbb{Q}$, βλ. τον τύπο στο Παράρτημα V. Επομένως $\mathrm{Gal}(E/\mathbb{Q}) \cong A_3$.

Στα επόμενα παραδείγματα θα υπολογίσουμε τις ομάδες Galois πάνω από το $\mathbb{Q}$, για πολυώνυμα βαθμού 4. Θα καταλήξουμε σε ενδιαφέροντα συμπεράσματα χρησιμοποιώντας τους τύπους της Ενότητας V του Παραρτήματος. Σημειώνουμε την επόμενη παρατήρηση.

Παρατηρήσεις 3.6.4.

i. Έστω $f(x) = x^4 + ax + b$. Τότε η διακρίνουσα του $f(x)$ είναι ίση με $-27a^4 + 256b^3$.

ii. Έστω $f(x) = x^4 + ax^2 + b$. Τότε η διακρίνουσα του $f(x)$ είναι ίση με $16(a^2 - 4b)^2$.

iii. Έστω $f(x) \in \mathbb{Q}[x]$, κανονικό πολυώνυμο και $\deg f(x) = 4$, E το σώμα ανάλυσης του $f(x)$ πάνω από το $\mathbb{Q}$ και $\alpha_1, \ldots, \alpha_4$ οι ρίζες του $f(x)$. Τότε οι ρίζες της κυβικής επιλύουσας (Παράρτημα V) είναι ίσες με

$$\alpha_1\alpha_2 + \alpha_3\alpha_4, \alpha_1\alpha_3 + \alpha_2\alpha_4, \alpha_1\alpha_4 + \alpha_2\alpha_3$$

και ανήκουν στο E. Άρα, το σώμα ανάλυσης της κυβικής επιλύουσας είναι ενδιάμεσο σώμα της επέκτασης $E/\mathbb{Q}$.

Όταν το $f(x)$ είναι ανάγωγο, τότε η ομάδα Galois G του $f(x)$ εμφυτεύεται στην S_4. Σύμφωνα με το Θεώρημα 3.2.1 η G έχει μία ενδιαφέρουσα ιδιότητα: για κάθε ζεύγος ριζών b, γ του $f(x)$, υπάρχει $\sigma \in G$ έτσι ώστε $\sigma(b) = \gamma$. Αυτό περιορίζει τις υποομάδες της S_4 που θα μπορούσαν να είναι ομάδες Galois ανάγωγων πολυωνύμων βαθμού 4.

Στην άσκηση 3.7.6 ο αναγνώστης καλείται να συμπληρώσει τις λεπτομέρειες του επόμενου παραδείγματος.

Παράδειγμα 3.6.5. Έστω $f(x) = x^4 + 2x + 2 \in \mathbb{Q}[x]$, E το σώμα ανάλυσης του $f(x)$ πάνω από το $\mathbb{Q}$ και $G = \mathrm{Gal}(E/\mathbb{Q})$. Το $f(x)$ είναι ανάγωγο, από το κριτήριο του Eisenstein. Η κυβική επιλύουσα του $f(x)$ είναι το πολυώνυμο $g(x) = x^3 - 8x - 4$, το οποίο είναι και αυτό ανάγωγο. Έστω B το σώμα ανάλυσης του $g(x)$. Αφού η διακρίνουσα D του $g(x)$ δεν είναι τετράγωνο ρητού αριθμού, έπεται ότι $\mathrm{Gal}(B/\mathbb{Q}) \cong S_3$ (Πρόταση 3.6.2) και επομένως το 6 διαιρεί την τάξη της G. Αφού η S_4 έχει τάξη 24 και η G εμφυτεύεται στην S_4, η G είναι ισόμορφη είτε με την A_4 είτε με την S_4. Όμως, η διακρίνουσα του $f(x)$ δεν είναι τετράγωνο ρητού αριθμού. Επομένως η G περιέχει μία μη άρτια αντιμετάθεση. Συνεπώς, η $G \cong S_4$.

Στο επόμενο παράδειγμα θα υπολογίσουμε αναλυτικά τα ενδιάμεσα σώματα της επέκτασης $E/\mathbb{Q}$, όπου E είναι το σώμα ανάλυσης του $f(x) = x^4 - 2$ πάνω από το $\mathbb{Q}$.

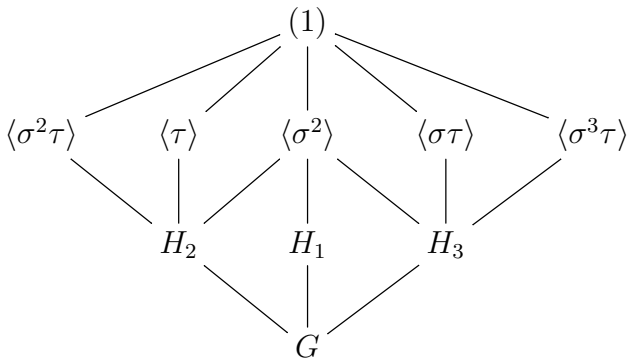
Παράδειγμα 3.6.6. Έστω $f(x) = x^4 - 2 \in \mathbb{Q}$, $E = \mathbb{Q}(b, i)$, όπου $b = 2^{1/4}$, και έστω $G = \mathrm{Gal}(E/\mathbb{Q})$. Στο Παράδειγμα 3.1.2, είδαμε ότι $G \cong D_8$ και ότι τα στοιχεία της G καθορίζονται από τον παρακάτω πίνακα, όπου η τελευταία γραμμή υπολογίζει την τάξη του ισομορφισμού, ως στοιχείου της G.

b	b	$-b$	b	$-b$	ib	ib	$-ib$	$-ib$
i	i	i	$-i$	$-i$	i	$-i$	i	$-i$
	id_E	σ^2	τ	$\sigma^2\tau$	σ	$\sigma\tau$	σ^3	$\sigma^3\tau$
τάξη	1	2	2	2	4	2	4	2

Οι γνήσιες μη τετριμμένες υποομάδες της G τάξης 4 είναι οι:

$$H_1 = \langle\sigma\rangle = \{\mathrm{id}_E, \sigma, \sigma^2, \sigma^3\}, \quad H_2 = \{\mathrm{id}_E, \sigma^2, \tau, \sigma^2\tau\} \quad H_3 = \{\mathrm{id}_E, \tau, \sigma\tau, \sigma^3\tau\},$$

ενώ κάθε ένα από τα στοιχεία της G με τάξη 2 παράγει μία αντίστοιχη υποομάδα τάξης 2. Έτσι το διάγραμμα των υποομάδων της G είναι:
Από τις υποομάδες της G που έχουν τάξη 2, μόνον η $\langle\tau\rangle$ είναι κανονική, όπως εύκολα ελέγχει κανείς. Σε αντιδιαστολή, κάθε μία από τις υποομάδες της G τάξης 4 είναι



Σχήμα 3.10: Υποομάδες της G

κανονική. Θα υπολογίσουμε τα ενδιάμεσα σώματα σύμφωνα με το Θεμελιώδες Θεώρημα της Θεωρίας Galois. Θα ξεκινήσουμε με την ομάδα $\langle\sigma\tau\rangle$. Μία βάση του E ως προς το $\mathbb{Q}$ είναι το σύνολο $\{1, b, b^2, b^3, i, ib, ib^2, ib^3\}$ και ένα τυχαίο στοιχείο y του E είναι ένας γραμμικός συνδυασμός

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

όπου $a_i \in \mathbb{Q}$. Επομένως,

$$\sigma\tau(y) = a_0 + a_1 ib - a_2 b^2 - ia_3 b^3 - a_4 i + a_5 b + a_6 ib^2 - a_7 b^3$$

Επομένως

$$\sigma\tau(y) = y \Leftrightarrow a_1 = a_5, a_2 = 0, a_3 = -a_7, a_4 = 0,$$

και

$$\sigma\tau(y) = y \Leftrightarrow y = a_0 + a_1 b(1+i) + a_3 b^3(1-i) + a_6 ib^2.$$

Άρα,

$$E^{\langle\sigma\tau\rangle} = \mathbb{Q}(b(1+i), b^3(1-i), ib^2).$$

Αφού $(b(1+i))^2 = 2ib^2$, $(b(1+i))^3 = -2b^3(1-i)$, έπεται ότι

$$E^{\langle\sigma\tau\rangle} = \mathbb{Q}(b(1+i)).$$

Στη συνέχεια θα βρούμε το σώμα $E^{\langle\sigma^2\rangle}$. Αφού $[G : \langle\sigma^2\rangle] = 4$, από το Θεμελιώδες Θεώρημα της Θεωρίας Galois συμπεραίνουμε ότι $[E^{\langle\sigma^2\rangle} : \mathbb{Q}] = 4$. Αφού

$$\sigma^2(i) = i \text{ και } \sigma^2(b^2) = \sigma^2(b)\sigma^2(b) = (-b)^2 = b^2,$$

έπεται ότι

$$\mathbb{Q}(b^2, i) \subset E^{\langle\sigma^2\rangle}.$$

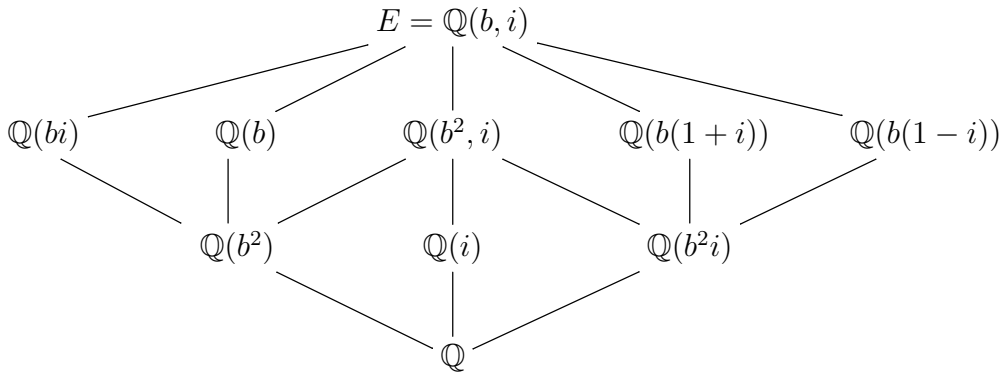
Αν $\mathbb{Q}(b^2, i) \neq E^{\langle\sigma^2\rangle}$, τότε

$$[\mathbb{Q}(b^2, i) : \mathbb{Q}] < 4 = [E^{\langle\sigma^2\rangle} : \mathbb{Q}].$$

Όμως, από τους εγκλεισμούς

$$\mathbb{Q} \subsetneq \mathbb{Q}(i) \subsetneq \mathbb{Q}(i, b^2) \subsetneq E,$$

έπεται ότι $[\mathbb{Q}(i, b^2) : \mathbb{Q}] = 4$. Άρα $E^{\langle\sigma^2\rangle} = \mathbb{Q}(i, b^2)$. Με αυτές τις τεχνικές βρίσκουμε και τα υπόλοιπα ενδιάμεσα σώματα του E.



Σχήμα 3.11: Ενδιάμεσα σώματα της $E/\mathbb{Q}$.

Έτσι στο διάγραμμα του σχήματος 3.10 αντιστοιχεί το παρακάτω διάγραμμα των ενδιάμεσων σωμάτων, αν στη θέση της υποομάδας H της G τοποθετήσουμε το σταθερό σώμα E^H. Σημειώνουμε ότι οι εγκλεισμοί αντιστρέφονται.
Τέλος παρατηρούμε ότι στις κανονικές υποοομάδες της G αντιστοιχούν τα παρακάτω ενδιάμεσα σώματα, όλα επεκτάσεις Galois πάνω από το $\mathbb{Q}$:

- $\mathbb{Q}(b^2)$ είναι το σώμα ανάλυσης του $x^2 - b$ πάνω από το $\mathbb{Q}$.
- $\mathbb{Q}(i)$ είναι το σώμα ανάλυσης του $x^2 + 1$ πάνω από το $\mathbb{Q}$.
- $\mathbb{Q}(b^2 i)$ είναι το σώμα ανάλυσης του $x^2 + 2$ πάνω από το $\mathbb{Q}$.
- $\mathbb{Q}(b^2, i)$ είναι το σώμα ανάλυσης του $(x^2 - b)(x^2 + 1)$ πάνω από το $\mathbb{Q}$.

3.7 Ασκήσεις

1. Έστω E/F επέκταση σωμάτων, $G = \mathrm{Gal}(E/F)$ και $H < G$. Να αποδείξετε ότι E^H είναι ενδιάμεσο σώμα της E/F, δηλ. $F \subset E^H \subset E$. Αν $H_1 < H_2 < G$, τότε να αποδείξετε ότι $E^{H_2} \subset E^{H_1}$.

2. Για κάθε μία από τις παρακάτω περιπτώσεις να δώσετε ένα παράδειγμα επεκτάσεων $\mathbb{Q} \subsetneqq B \subsetneqq E$ ή να εξηγήσετε γιατί είναι αδύνατον να συμβεί:

   - E/B επέκταση του Galois, $B/\mathbb{Q}$ επέκταση του Galois και $E/\mathbb{Q}$ δεν είναι επέκταση του Galois,
   - E/B δεν είναι επέκταση του Galois, $B/\mathbb{Q}$ επέκταση του Galois και $E/\mathbb{Q}$ επέκταση του Galois,
   - E/B επέκταση Galois, $B/\mathbb{Q}$ δεν είναι επέκταση Galois και $E/\mathbb{Q}$ είναι επέκταση του Galois.

3. Έστω $f(x)$ το πολυώνυμο $f(x) = x^4 - 4 \in \mathbb{Q}[x]$, E το σώμα ανάλυσης του $f(x)$ πάνω από το $\mathbb{Q}$ και $G = \mathrm{Gal}(E/\mathbb{Q})$.

   - Να υπολογίσετε το E.
   - Να γράψετε τα στοιχεία της G ως στοιχεία του S_4.
   - Να αποδείξετε ότι $G \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

- Για τα υποσώματα $B_1 = \mathbb{Q}(i\sqrt{2}),\ B_2 = \mathbb{Q}(i),\ B_3 = \mathbb{Q}(\sqrt{2})$ του E, να βρείτε τις υποομάδες $\mathrm{Gal}(E/B_1)$ $\mathrm{Gal}(E/B_2)$ $\mathrm{Gal}(E/B_3)$ της G.
- Έστω $a = \sqrt{2} + i$. Να υπολογίσετε την εικόνα του a για κάθε έναν από τους αυτομορφισμούς του E. Να αποδείξετε ότι $E = \mathbb{Q}(a)$.
- Να γράψετε το στοιχείο a^{-1} ως γραμμικό συνδυασμό δυνάμεων του a.

4. Έστω $E = \mathbb{Q}(\sqrt{3}, \sqrt{5})$.

   - Να αποδείξετε ότι $E/\mathbb{Q}$ είναι επέκταση του Galois, να υπολογίσετε τον βαθμό $[E : \mathbb{Q}]$ και να βρείτε μία $\mathbb{Q}$-βάση του E.
   - Να περιγράψετε τα στοιχεία της ομάδας $G = \mathrm{Gal}(E/\mathbb{Q})$.
   - Να βρείτε όλα τα ενδιάμεσα σώματα B του E πάνω από το $\mathbb{Q}$ και να υπολογίσετε τις ομάδες $\mathrm{Gal}(B/\mathbb{Q})$ και $\mathrm{Gal}(E/B)$.
   - Να βρείτε ανάγωγο πολυώνυμο $f(x)$ έτσι ώστε E να είναι σώμα ανάλυσης του $f(x)$ πάνω από το $\mathbb{Q}$.

5. Έστω $f(x) \in F[x]$ ανάγωγο, διαχωρίσιμο πολυώνυμο βαθμού 3, $\mathrm{char}\, F \neq 2$, και E το σώμα ανάλυσης του $f(x)$ πάνω από το F. Αν $\Delta \in F$, να αποδείξετε ότι $\mathrm{Gal}(E/F) \cong A_3$.

6. Να συμπληρώσετε τις λεπτομέρειες του Παραδείγματος 3.6.5 και να αποδείξετε ότι η ομάδα Galois του $f(x) = x^4 + 2x + 2 \in \mathbb{Q}[x]$ είναι ισόμορφη με την S_4. Να παρατηρήσετε κάτι ενδιαφέρον σχετικά με τις διακρίνουσες.

7. Να αποδείξετε ότι η ομάδα Galois του $f(x) = x^4 - 8x + 12 \in \mathbb{Q}[x]$ είναι ισόμορφη με την A_4.

8. Να αποδείξετε ότι η ομάδα Galois του $f(x) = x^4 + 5x + 5 \in \mathbb{Q}[x]$ είναι κυκλική τάξης 4.

9. Έστω $E = \mathbb{Q}(\omega, \sqrt[5]{3})$ και $G = \mathrm{Gal}(E/\mathbb{Q})$, όπου $\omega = e^{2\pi i/5}$.

   - Να βρείτε πολυώνυμο $f(x) \in \mathbb{Q}[x]$ έτσι ώστε E να είναι το σώμα ανάλυσης του $f(x)$ και να υπολογίσετε τον βαθμό $[E : \mathbb{Q}]$.
   - Να αποδείξετε ότι η G εμφυτεύεται στην S_5 και ότι $G \ncong S_5$.
   - Να βρείτε τα στοιχεία της $G_1 = \mathrm{Gal}(E/\mathbb{Q}(\sqrt[5]{3}))$. Να υπολογίσετε το $\sigma(a)$, όπου a τυχαίο στοιχείο της E και $\sigma \in G_1$, $\sigma \neq id_E$ (για ένα μόνο τέτοιο στοιχείο). Να δείξετε ότι η G_1 είναι κυκλική ομάδα.
   - Να βρείτε τα στοιχεία της $G_2 = \mathrm{Gal}(E/\mathbb{Q}(\omega))$. Να δείξετε ότι η G_2 είναι κυκλική ομάδα. Να υπολογίσετε το $\sigma(a)$, όπου a τυχαίο στοιχείο της E και $\sigma \in G_2$, $\sigma \neq id_E$ (για ένα μόνο τέτοιο στοιχείο).
   - Να βρείτε δύο στοιχεία της ομάδας $G = \mathrm{Gal}(E/\mathbb{Q})$ που δεν αντιμετατίθενται.

10. Έστω $E = \mathbb{Q}(\omega)$, όπου $\omega = e^{2\pi i/5}$.

    - Να δείξετε ότι $E/\mathbb{Q}$ είναι επέκταση Galois και να βρείτε τον βαθμό $[E : \mathbb{Q}]$.
    - Έστω $G = \mathrm{Gal}(E/\mathbb{Q})$. Να αποδείξετε ότι η G είναι κυκλική ομάδα.

- Να βρείτε όλα τα ενδιάμεσα σώματα του E.

11. Έστω E/F μία επέκταση Galois, $a \in E$, $G = \mathrm{Gal}(E/F)$. Να αποδείξετε ότι $N(a) \in F$, όπου
$$N(a) = \prod_{\sigma \in G} \sigma(a).$$

12. Έστω E/F μία επέκταση Galois και έστω $a \in E$. Να αποδείξετε ότι $\mathrm{irr}_{(F,a)}(x)$ αναλύεται σε γινόμενο γραμμικών παραγόντων στο $E[x]$.

13. Αν L/F επέκταση του Galois και $L \subset E$, να αποδείξετε ότι $L(a)/F(a)$ είναι επέκταση του Galois, όπου $a \in E$.

Βιβλιογραφία Κεφαλαίου 3

[1] Bastida, J. R. *Field Extensions and Galois Theory, Vol. 22*. Addison-Wesley, 2007.

[2] Bewersdorff, J. *Galois Theory for Beginners, A Historical Perspective*. AMS, 2006.

[3] Conrad, K. *Galois groups of cubics and quartics*. Expository Papers, `http://www.math.uconn.edu/~kconrad/blurbs/galoistheory/cubicquartic.pdf`.

[4] Dummit, D.S., Foote, R.M. *Abstract Algebra*. J. Wiley and Sons, INc, 2004.

[5] Edwards, H.M. *Galois Theory*. Springer, 1984.

[6] Escofier, J.P. *Galois Theory*. Springer, 2001.

[7] Fox, D. *Galois Theory*. John Wiley & Sons, 2012.

[8] Fraleigh, J. *Εισαγωγή στην Άλγεβρα*. Πανεπιστημιακές εκδόσεις Κρήτης, 2011.

[9] Gaal, L. *Classical Galois Theory with Examples*. Chelsea, 1988.

[10] Hadlock, C. R. *Field Theory and its Classical Problems*. MAA, 2000.

[11] Menini, C. Van Oystaeyen, F. *Abstract Algebra*. Marcel Dekker, 2004.

[12] Milne, J.S. *Fields and Galois Theory*. www.jmilne.org, 2014.

[13] Rotman, J. *Θεωρία Galois*. Leader Books, 2000.

[14] Stewart, I. *Galois Theory*. Champan and Hall, 1973.

[15] Swallow, J. *Exploratory Galois Theory*. Cambridge University Press, 2004.

[16] Tignol, J.P. *Galois Theory of Algebraic Equations*. World Scientific, 2011.

Κεφάλαιο 4

Πεπερασμένα σώματα

Στο κεφάλαιο αυτό εφαρμόζουμε τη Θεωρία Galois, όπως αυτή αναπτύχθηκε στα δύο προηγούμενα κεφάλαια, στην περίπτωση των πεπερασμένων σωμάτων.

4.1 Βασικές Έννοιες

Έστω F ένα πεπερασμένο σώμα, δηλ. $|F| < \infty$. Τότε η χαρακτηριστική του F είναι κάποιος πρώτος αριθμός p και έτσι το σώμα $\mathbb{Z}_p$ εμφυτεύεται στο F, βλ. Ενότητα IV του Παραρτήματος. Επομένως προκειμένου να εξετάσουμε τα πεπερασμένα σώματα αρκεί να εξετάσουμε πεπερασμένες επεκτάσεις σωμάτων $F/\mathbb{Z}_p$.

Έστω, λοιπόν, ότι $[F : \mathbb{Z}_p] = n$, για κάποιον φυσικό αριθμό n. Τότε το σώμα F είναι $\mathbb{Z}_p$-διανυσματικός χώρος διάστασης n, $|F| = p^n$, και $\operatorname{char} F = p$, βλ. Πρόταση IV.5. Η πολλαπλασιαστική ομάδα $(F^*, \cdot)$ του σώματος F, όπου $F^* = F - \{0\}$ έχει $p^n - 1$ στοιχεία. Ως συνέπεια του Θεωρήματος του Lagrange για τις πεπερασμένες ομάδες (βλ. Θεώρημα I.10), γνωρίζουμε ότι κάθε στοιχείο μίας ομάδας υψούμενο στην τάξη της ομάδας ισούται με το μοναδιαίο στοιχείο της ομάδας. Επομένως, για κάθε $a \in F^*$, ισχύει

$$a^{p^n-1} = 1 \Rightarrow a^{p^n} = a \Rightarrow a^{p^n} - a = 0,$$

δηλαδή το a είναι ρίζα του πολυωνύμου

$$f(x) = x^{p^n} - x \in \mathbb{Z}_p[x].$$

Το 0 είναι και αυτό ρίζα του $f(x)$. Ισχύει, λοιπόν, η παρακάτω πρόταση:

Πρόταση 4.1.1. *Έστω F πεπερασμένο σώμα και $|F| = p^n$ όπου p πρώτος φυσικός αριθμός. Κάθε στοιχείο του F είναι ρίζα του πολυωνύμου $f(x) = x^{p^n} - x$ και το F είναι σώμα ανάλυσης του $f(x)$, δηλ.*

$$x^{p^n} - x = \prod_{a \in F} (x - a).$$

Θα αποδείξουμε τώρα ότι, για κάθε φυσικό αριθμό $n > 1$ και για κάθε πρώτο φυσικό πρώτο αριθμό p, υπάρχει ένα σώμα F με p^n στοιχεία. Η χαρακτηριστική του F είναι βέβαια p. Έστω $f(x) = x^{p^n} - x \in \mathbb{Z}_p[x]$. Αφού $f'(x) = -1 \neq 0$, έπεται ότι το $f(x)$ είναι διαχωρίσιμο (Πρόταση 1.4.5). Από το Θεώρημα του Kronecker (Θεώρημα 1.4.3) υπάρχει μία επέκταση L του $\mathbb{Z}_p$ που είναι σώμα ανάλυσης του $f(x) = x^{p^n} - x$. Θεωρούμε, λοιπόν, το σύνολο των ριζών M του $f(x)$ στο L, δηλαδή

$$M = \{a \in L : a^{p^n} = a\}.$$

Θα δείξουμε ότι το M είναι υπόσωμα του L. Έστω $a, b \in M$. Αφού

$$p \mid \binom{p^n}{i} \text{ για } 1 \leq i \leq p^n - 1,$$

από την Πρόταση II.7 προκύπτει ότι

$$(a-b)^{p^n} = a^{p^n} - b^{p^n} = a - b \Rightarrow a - b \in M.$$

Ακόμη, αν $a, b \in M$, $b \neq 0$ τότε

$$(ab^{-1})^{p^n} = a^{p^n}(b^{p^n})^{-1} = ab^{-1} \Rightarrow ab^{-1} \in M.$$

Άρα όντως το M είναι υπόσωμα του L. Το πλήθος των στοιχείων του M είναι το πλήθος των διακεκριμένων ριζών του $f(x)$ που είναι ακριβώς p^n, αφού το $f(x)$ είναι διαχωρίσιμο. Άρα το M είναι το ζητούμενο σώμα. Το M ως σώμα ανάλυσης του διαχωρίσιμου πωλυωνύμου $f(x) \in \mathbb{Z}_p[x]$ είναι επέκταση του Galois πάνω από το $\mathbb{Z}_p$. Ακόμη το M είναι μοναδικό με προσέγγιση ισομορφίας, ως σώμα ανάλυσης του $f(x)$ (βλ. Πόρισμα 3.2.2). Τα παραπάνω, λοιπόν, αποδεικνύουν το επόμενο θεώρημα:

Θεώρημα 4.1.2. *Για κάθε πρώτο αριθμό p και για κάθε φυσικό αριθμό $n > 1$ υπάρχει μοναδικό πεπερασμένο σώμα F με p^n στοιχεία. Η επέκταση $F/\mathbb{Z}_p$ είναι επέκταση Galois βαθμού n.*

Το σώμα με p^n στοιχεία, όπως αναφέρεται στο Θεώρημα 4.1.2, λέγεται ***σώμα Galois με p^n στοιχεία*** (Galois field with p^n elements) και συνήθως συμβολίζεται ως $\mathrm{GF}(p^n)$. Ως συνήθως, η πολλαπλασιαστική ομάδα του $\mathrm{GF}(p^n)$ συμβολίζεται ως $\mathrm{GF}(p^n)^*$. Όταν $n = 1$, $\mathrm{GF}(p) \cong \mathbb{Z}_p$ και χρησιμοποιούμε ελεύθερα και τους δύο συμβολισμούς.

Παραδείγματα 4.1.3.

1. Θα κατασκευάσουμε ένα σώμα με 4 στοιχεία, δηλ. το $\mathrm{GF}(2^2)$. Είναι φανερό ότι η χαρακτηριστική του $\mathrm{GF}(2^2)$ είναι 2 και ότι το $\mathrm{GF}(2^2)$ είναι επέκταση του $\mathbb{Z}_2$ βαθμού 2. Έστω ακόμη ότι $\mathrm{GF}(2^2) = \{0, 1, a, b\}$. Παρατηρούμε ότι το στοιχείο $a + 1 \in \mathrm{GF}(2^2)$ και ότι $a + 1 = b$. Πράγματι αν $a + 1 = a$, τότε $1 = 0$, αδύνατον. Αν $a + 1 = 1$, τότε $a = 0$ αδύνατον. Αν $a + 1 = 0$, τότε $a = -1$, άρα $a = 1$, αδύνατον επίσης. Ο παρακάτω πίνακας αποτυπώνει τα αποτελέσματα των πράξεων στην προσθετική ομάδα $(\mathrm{GF}(2^2), +)$:

$+$	0	1	a	b
0	0	1	a	b
1	1	0	b	a
a	a	b	0	1
b	b	a	1	0.

   Η πολλαπλασιαστική ομάδα $(\mathrm{GF}(2^2)^*, \cdot)$ του $\mathrm{GF}(2^2)$ έχει τρία στοιχεία, άρα είναι κυκλική και παράγεται είτε από το a είτε από το b. Έτσι $\mathrm{GF}(2^2)^* = \{1, a, a^2 = b\}$. Έτσι, για τον πολλαπλασιασμό στην $(\mathrm{GF}(2^2)^*, \cdot)$ έχουμε τον παρακάτω πίνακα:

$\cdot$	1	a	$a^2 = b$
1	1	a	b
a	a	b	1
$b = a^2$	b	1	a.

Παρατηρούμε ακόμη ότι αφού $a^2 = b$ και $1 = -1$ στο $\mathbb{Z}_2$, τότε

$$a^2 = a + 1 \Rightarrow a^2 - a - 1 = 0 \Rightarrow a^2 + a + 1 = 0.$$

Δηλαδή το a είναι ρίζα του πολυωνύμου $x^2+x+1 \in \mathbb{Z}_2[x]$. Όμως, το x^2+x+1 είναι ανάγωγο, αφού δεν έχει ρίζα στο $\mathbb{Z}_2$. Άρα $\mathrm{GF}(2^2) = \mathbb{Z}_2(a)$ και $\mathrm{irr}_{(\mathbb{Z}_2,a)}(x) = x^2+x+1$. Οι ρίζες του $x^2 + x + 1$ στο $\mathrm{GF}(2^2)$ είναι a, $a^2 = a + 1$.

2. Έστω $\mathrm{GF}(2^3)$ το σώμα με 8 στοιχεία που κατασκευάζεται σύμφωνα με το Θεώρημα 4.1.2. Θα μελετήσουμε τη δομή του $\mathrm{GF}(2^3)$. Παρατηρούμε καταρχήν ότι η πολλαπλασιαστική ομάδα $(\mathrm{GF}(2^3)^*, \cdot)$ του $\mathrm{GF}(2^3)$ έχει 7 στοιχεία. Αφού το 7 είναι πρώτος, η ομάδα $\mathrm{GF}(2^3)^*$ είναι κυκλική (Θεώρημα Ι.14) και μάλιστα κάθε στοιχείο $1 \neq b \in \mathrm{GF}(2^3)^*$ παράγει την $\mathrm{GF}(2^3)^*$ (Πρόταση Ι.8). Επομένως αν $0, 1 \neq b \in \mathrm{GF}(2^3)$, τότε κάθε μη μηδενικό στοιχείο του $\mathrm{GF}(2^3)$ προκύπτει ως κάποια δύναμη του b και επομένως $\mathrm{GF}(2^3) = Z_2(b)$, $0, 1 \neq b \in \mathrm{GF}(2^3)$. Παρατηρούμε, επίσης, ότι $[\mathrm{GF}(2^3) : \mathbb{Z}_2] = 3$, βλ. Πρόταση IV.5. Σύμφωνα με το Θεώρημα 4.1.2, το $\mathrm{GF}(2^3)$ είναι το σώμα ανάλυσης του πολυωνύμου $x^8 - x$ πάνω από το $\mathbb{Z}_2$. Παρατηρούμε ότι x και $x + 1$ είναι δύο ανάγωγοι παράγοντες του $x^8 - x$. Με υπολογισμούς βρίσκουμε ότι το $x^2 + x + 1$ δεν διαιρεί το $x^8 - x$, ενώ τα πολυώνυμα $x^3 + x^2 + 1$, x^3+x+1 το διαιρούν. Έτσι η ανάλυση του x^8-x σε γινόμενο ανάγωγων πολυωνύμων στο $\mathbb{Z}_2[x]$ είναι:

$$x^8 - x = x^8 + x = x(x + 1)(x^3 + x^2 + 1)(x^3 + x + 1),$$

Έστω $a \in \mathrm{GF}(2^3)$ ρίζα του $x^3 + x^2 + 1$. Δηλαδή $\mathrm{irr}_{(\mathbb{Z}_2,a)}(x) = x^3 + x^2 + 1$. Αφού $[\mathbb{Z}_2(a) : \mathbb{Z}_2] = 3$, έπεται ότι $\mathbb{Z}_2(a) = \mathrm{GF}(2^3)$. Τα στοιχεία $1, a, a^2$ είναι μία $\mathbb{Z}_2$-βάση του $\mathrm{GF}(2^3)$. Αυτό σημαίνει ότι

$$\mathrm{GF}(2^3) = \{c_0 + c_1a + c_2a^2 : c_i \in \mathbb{Z}_2, 0 \leq i \leq 2\}$$

$$= \{0, 1, a, 1 + a, a^2, 1 + a^2, a + a^2, 1 + a + a^2\}.$$

Συγκεκριμένα αφού $\mathrm{irr}_{(\mathbb{Z}_2,a)}(x) = x^3 + x^2 + 1$ έπεται ότι

- $a^3 = a^2 + 1$,
- $a^4 = aa^3 = a^2 + a + 1$,
- $a^5 = a^2a^3 = a + 1$,
- $a^6 = aa^5 = a^2 + a$,
- $a^7 = 1$.

Οι ρίζες του x^3+x^2+1 είναι οι a, a^2, a^4, ενώ οι ρίζες του x^3+x+1 είναι οι a^3, a^5, a^6. Η αντίστοιχη ανάλυση μπορεί να γίνει και για $a \in \mathrm{GF}(2^3)$ που είναι ρίζα του x^3+x+1 και αφήνεται για τον αναγνώστη. Επίσης ο αναγνώστης μπορεί να υπολογίσει τους πίνακες για τις πράξεις στις ομάδες $(\mathrm{GF}(2^3), +)$ και $(\mathrm{GF}(2^3)^*, \cdot)$.

3. Έστω τώρα $\mathrm{GF}(2^4)$ το σώμα με 16 στοιχεία που κατασκευάζεται σύμφωνα με το Θεώρημα 4.1.2. Θα δείξουμε ότι υπάρχει $a \in \mathrm{GF}(2^4)$ έτσι ώστε $\mathrm{GF}(2^4) = \mathbb{Z}_2(a)$. Πράγματι, αρκεί να δείξουμε ότι υπάρχει ένα στοιχείο $a \in \mathrm{GF}(2^4)^*$ έτσι ώστε η τάξη του a στην πολλαπλασιαστική ομάδα $\mathrm{GF}(2^4)^*$ να είναι 15. Θα προσπαθήσουμε, λοιπόν, να μετρήσουμε το πλήθος των στοιχείων του $\mathrm{GF}(2^4)^*$ με τάξη μικρότερη του 15. Σύμφωνα με το Θεώρημα του Lagrange, τα στοιχεία αυτά του $\mathrm{GF}(2^4)^*$ θα έχουν τάξη 5, 3 ή 1. Αφού, όμως,

- τα στοιχεία με τάξη 5 είναι ρίζες του πολυωνύμου $x^5 - 1$,
- ένα πολυώνυμο βαθμού n πάνω από το σώμα F έχει το πολύ n ρίζες και
- το 1 είναι ρίζα του $x^5 - 1$ και 1 έχει τάξη 1,

έπεται ότι υπάρχουν το πολύ 4 στοιχεία με τάξη 5 στο $\mathrm{GF}(2^4)^*$. Αντίστοιχα υπάρχουν το πολύ 2 στοιχεία του F^* με τάξη 3. Υπάρχει βέβαια ακριβώς ένα στοιχείο με τάξη 1. Δηλαδή υπάρχουν το πολύ 7 στοιχεία στο $\mathrm{GF}(2^4)^*$ με τάξη μικρότερη του 15. Επομένως υπάρχουν τουλάχιστον $15-7=8$ στοιχεία στο $\mathrm{GF}(2^4)^*$ με τάξη 15. Έστω a ένα τέτοιο στοιχείο. Άρα $\mathrm{GF}(2^4)^* = \langle a\rangle$ και συνεπώς $\mathrm{GF}(2^4) = \mathbb{Z}_2(a)$.

Παρατηρούμε, επίσης, ότι γενικότερα για κάθε κυκλική ομάδα $G = \langle a\rangle$ με $|G| = 15$ ισχύουν τα εξής (βλ. Προτάσεις I.7 και I.8):

- $1 \le n \le 14$ και $(n, 15) = 1$, τότε το a^n έχει και αυτό τάξη 15. Δηλαδή υπάρχουν $\phi(15) = 8$ στοιχεία με τάξη 15 που προκύπτουν ως δυνάμεις του a, όπου ϕ είναι η συνάρτηση του Euler.
- αν $1 \le n \le 14$ και $(n, 15) = 3$, τότε a^n έχει τάξη 5. Υπάρχουν $\phi(5) = 4$ πλήθους τέτοιοι αριθμοί και $\langle a^3\rangle = \langle a^6\rangle = \langle a^9\rangle = \langle a^{12}\rangle$. Πράγματι, αφού $15 = 5 \cdot 3$, αν ξεκινήσουμε με $n = 3$, αρκεί στη συνέχεια να θεωρήσουμε τα πολλαπλάσια $3k$, όπου $1 \le k \le 5$, $(k, 5) = 1$.
- αν $1 \le n \le 14$ και $(n, 15) = 5$, τότε το a^n έχει τάξη 3. Υπάρχουν 2 τέτοιοι αριθμοί n: $n = 5$, $n = 10$. Δηλαδή $2 = \phi(3)$. Είναι επίσης φανερό ότι $\langle a^5\rangle = \langle a^{10}\rangle$.

Άρα ισχύει η παρακάτω σχέση:

$$15 = \phi(15) + \phi(5) + \phi(3) + \phi(1).$$

4.2 Πρωταρχικά στοιχεία

Στην ενότητα αυτή θα γενικεύσουμε τις παρατηρήσεις που έγιναν στα προηγούμενα παραδείγματα. Έστω $\phi : \mathbb{N} \to \mathbb{N}$, η γνωστή συνάρτηση του Euler (βλ. Παράδειγμα I.2.3), όπου $\phi(n) = |\mathbb{Z}_n^\sharp|$. Όταν C είναι μία κυκλική ομάδα, συμβολίζουμε με $g(C)$ το σύνολο των στοιχείων που παράγουν τη C. Έτσι, όταν $|C| = m$ τότε $|g(C)| = \phi(m)$ (βλ. Πρόταση I.8). Έστω G μία τυχαία ομάδα και C_1, C_2 δύο κυκλικές υποομάδες της G. Αν $C_1 \neq C_2$, τότε $g(C_1) \cap g(C_2) = \emptyset$. Είναι φανερό ότι ισχύει

$$G = \bigcup_C g(C), \tag{4.2.0.1}$$

όπου το C διατρέχει όλες τις κυκλικές υποομάδες της G.

Θα εφαρμόσουμε την παραπάνω σχέση στην περίπτωση που η ομάδα G είναι κυκλική τάξης n. Μετρώντας τα στοιχεία στα σύνολα που εμφανίζονται και στα δύο σκέλη της σχέση (4.2.0.1) βρίσκουμε ότι

$$n = \sum_C |g(C)|, \tag{4.2.0.2}$$

όπου το C διατρέχει όλες τις υποομάδες της G. Αφού, για κάθε d που διαιρεί το n, υπάρχει ακριβώς μία (κυκλική) ομάδα C έτσι ώστε $|C| = d$ (βλ. Θεώρημα I.14) και $|g(C)| = \phi(d)$ προκύπτει το εξής συμπέρασμα:

Πρόταση 4.2.1. *Έστω $n > 1$ φυσικός αριθμός. Τότε*

$$n = \sum_{d \mid n} \phi(d).$$

Παρατηρούμε ότι στη γενική περίπτωση μίας ομάδας G πληθυκότητας n είναι πιθανόν, να υπάρχουν παραπάνω από μία κυκλικές ομάδες τάξης d, όπου το d διαιρεί το n, ή και καμία. Παρακάτω αποδεικνύουμε το αντίστροφο του Θεωρήματος I.8.ii, χρησιμοποιώντας τις σχέσεις 4.2.0.1 και 4.2.1.

Θεώρημα 4.2.2. *Μία ομάδα G τάξης $n < \infty$ είναι κυκλική αν και μόνο αν, για κάθε διαιρέτη d του n, υπάρχει το πολύ μία κυκλική υποομάδα τάξης d.*

Απόδειξη. Αν η G είναι κυκλική, τότε το συμπέρασμα προκύπτει από το Θεώρημα I.8.ii. Υποθέτουμε αντίστροφα ότι, για κάθε διαιρέτη d του n, υπάρχει το πολύ μία κυκλική υποομάδα τάξης d. Άρα, όλα τα στοιχεία που έχουν τάξη d (αν υπάρχουν) παράγουν την ίδια υποομάδα και έτσι στη σχέση (4.2.0.2) μπορούμε ισοδύναμα να προσθέσουμε τους διαιρέτες του n. Επίσης, αν υπάρχει κυκλική υποομάδα C της G τάξης d, τότε όπως είδαμε $|g(C)| = \phi(d)$. Άρα,

$$n = \sum_{\substack{d|n, \\ |C|=d}} \phi(d),$$

όπου C είναι κυκλική ομάδα (αν υπάρχει). Εάν, λοιπόν, για κάποιο d δεν υπάρχει κάποια κυκλική υποομάδα τάξης d, ο όρος $\phi(d)$ δε θα εμφανίζεται στο παραπάνω άθροισμα. Όμως, από την Πρόταση 4.2.1, προκύπτει ότι αναγκαστικά, για κάθε d διαιρέτη του n, υπάρχει ακριβώς μία κυκλική υποομάδα της G τάξης d. Αυτό συμβαίνει και για $d = n$, δηλαδή η G είναι κυκλική. □

Οδηγούμαστε, λοιπόν, στο επόμενο θεώρημα.

Θεώρημα 4.2.3. *Κάθε πεπερασμένη υποομάδα της πολλαπλασιαστικής ομάδας ενός σώματος F είναι κυκλική.*

Απόδειξη. Έστω G μία υποομάδα της $(F^*, \cdot)$ τάξης n και $d|n$. Αν C είναι μία κυκλική υποομάδα της G τάξης d, τότε από το θεώρημα του Lagrange $c^d = 1, \forall\, c \in C$. Αν υπήρχε και δεύτερη κυκλική υποομάδα της G τάξης d, τότε θα υπήρχαν τουλάχιστον $d+1$ στοιχεία x της G που ικανοποιούν την εξίσωση $x^d = 1$. Όμως, το πολυώνυμο $x^d - 1$ έχει το πολύ d ρίζες σε ένα σώμα. Άρα υπάρχει το πολύ μία κυκλική υποομάδα της G τάξης d, για κάθε d διαιρέτη του n. Από το Θεώρημα 4.2.2 προκύπτει ότι η G είναι κυκλική. □

Πόρισμα 4.2.4. *Αν $\mathrm{GF}(p^n)$ είναι ένα πεπερασμένο σώμα τότε η $(\mathrm{GF}(p^n)^*, \cdot)$ είναι κυκλική ομάδα και $\mathrm{GF}(p^n) = \mathrm{GF}(p)(a)$, για κάποιον πρώτο p και για κάποιο στοιχείο a.*

Ειδικότερα, για p πρώτο φυσικό αριθμό, ισχύει η παρακάτω πρόταση.

Πρόταση 4.2.5. *Έστω p πρώτος. Η πολλαπλασιαστική ομάδα $\mathbb{Z}_p^\sharp$ είναι κυκλική.*

Παρατηρούμε ότι η Πρόταση 4.2.5 δεν είναι αληθής για τυχαίο n, όπως δείχνουν τα επόμενα παραδείγματα.

Παραδείγματα 4.2.6.

1. Η ομάδα $\mathbb{Z}_8^\sharp$ έχει $\phi(8) = 4$ πλήθους στοιχεία και $\mathbb{Z}_8^\sharp = \{\bar{1}, \bar{3}, \bar{5}, \bar{7}\}$. Αφού η τάξη των $\bar{3}$, $\bar{5}$, $\bar{7}$ είναι ίση με 2, η ομάδα $\mathbb{Z}_8^\sharp$ δεν είναι κυκλική. Επομένως, η $\mathbb{Z}_8^\sharp$ είναι ισόμορφη με την ομάδα του Klein.
2. Η ομάδα $\mathbb{Z}_9^\sharp$ έχει $\phi(9) = 6$ πλήθους στοιχεία και $\mathbb{Z}_8^\sharp = \{\bar{1}, \bar{2}, \bar{4}, \bar{5}, \bar{7}, \bar{8}\}$. Είναι εύκολο να υπολογίσουμε ότι η $\mathrm{ord}(\bar{2}) = 6$. Επομένως η $\mathbb{Z}_9^\sharp$ είναι κυκλική.

Ένα στοιχείο $a \in \mathrm{GF}(p^n)^*$ λέγεται ***πρωταρχικό*** (primitive) αν

$$(\mathrm{GF}(p^n)^*, \cdot) = \langle a \rangle.$$

Σημειώνουμε ότι αν $a \in \mathrm{GF}(p^n)^*$ είναι πρωταρχικό τότε

$$\mathrm{GF}(p^n) = \mathrm{GF}(p)(a).$$

Όπως θα δούμε στα επόμενα παραδείγματα, δεν ισχύει το αντίστροφο. Έτσι, είναι δυνατόν να ισχύει ότι $\mathrm{GF}(p^n) = \mathrm{GF}(p)(a)$ και a να μην είναι πρωταρχικό. Στη γενική περίπτωση δεν είναι γνωστή μία μέθοδος προσδιορισμού πρωταρχικών στοιχείων. Στα παρακάτω παραδείγματα ταυτίζουμε τον φυσικό αριθμό m με την εικόνα του $\bar{m}$ στο $\mathbb{Z}_p \cong \mathrm{GF}(p)$ και στην επέκταση $\mathrm{GF}(p^n)$ του $\mathrm{GF}(p)$.

Παραδείγματα 4.2.7.

1. Στο σώμα $\mathrm{GF}(11) \cong \mathbb{Z}_{11}$, το 2 είναι πρωταρχικό. Πράγματι, η τάξη του 2 στο $\mathbb{Z}_{11}^*$ πρέπει να διαιρεί το 10 σύμφωνα με το Θεώρημα του Lagrange. Απλοί υπολογισμοί, δείχνουν ότι
$$2^2 = 4 \neq 1, \text{ ενώ } 2^5 = 32 = -1 \neq 1.$$
Επομένως $\mathrm{ord}\,(2) = 10$ και $\mathbb{Z}_{11} = \langle 2 \rangle$.
2. Το πολυώνυμο $f(x) = x^2 - 2$ είναι ανάγωγο πάνω από το $\mathbb{Z}_5$, αφού δεν έχει ρίζες στο $\mathbb{Z}_5$. Έστω F το σώμα ανάλυσης του $f(x)$ πάνω από το $\mathbb{Z}_5$. Αν $a \in F$ είναι μία ρίζα του $f(x)$ τότε η άλλη ρίζα του $f(x)$ είναι το $-a$. Συνεπώς $F = \mathbb{Z}_5(a)$ και $|F| = 25$. Επομένως $F \cong \mathrm{GF}(5^2)$. Τα στοιχεία του F είναι της μορφής $k + la$, όπου $k, l \in \mathbb{Z}_5$. Παρατηρούμε ότι το a δεν είναι πρωταρχικό, αφού $a^2 = 2$. Υπολογίζοντας διαδοχικά τις δυνάμεις του $b = 2 + a$ διαπιστώνουμε ότι το b είναι πρωταρχικό. Πράγματι, οι δυνατές τάξεις του b είναι οι διαιρέτες του 24. Βλέπουμε ότι:

   - $b^2 = 2 + 4a + a^2 = 4 + 4a + 2 = 6 + 4a = 1 + 4a$.
   - $b^3 = (2 + a)(1 + 4a) = 2 + 9a + 4a^2 = 4a$.
   - $b^4 = 3 + 3a$.
   - $b^6 = (b^3)^2 = 2$.
   - $b^8 = 2 + 3a$.
   - $b^{12} = (b^6)^2 = 4$.

   Άρα, η τάξη του b στην $(F^*, \cdot)$ είναι 24, το b είναι πρωταρχικό και επομένως $F = \mathbb{Z}_5(b)$.

Σημειώνουμε την παρακάτω χρήσιμη πρόταση.

Πρόταση 4.2.8. *Έστω a πρωταρχικό στοιχείο του $\mathrm{GF}(p^n)$. Τότε το a είναι ρίζα ενός αναγώγου πολυωνύμου βαθμού n πάνω από το $\mathrm{GF}(p)$.*

Απόδειξη. Έστω $f(x) = \mathrm{irr}_{(\mathbb{Z}_p,a)}(x)$. Από το Πόρισμα 4.2.4 έπεται ότι $\mathrm{GF}(p^n) = \mathrm{GF}(p)(a)$. Αφού $[\mathrm{GF}(p^n) : \mathrm{GF}(p)] = n$, από το Θεώρημα 2.2.3 προκύπτει ότι $\deg f(x) = n$. □

Ως άμεση συνέπεια του Πορίσματος 4.2.4 και της Πρότασης 4.2.8, συμπεραίνουμε την ύπαρξη ανάγωγων πολυωνύμων στο $\mathrm{GF}(p)[x]$.

Πόρισμα 4.2.9. *Για κάθε φυσικό αριθμό $n > 1$, υπάρχει ανάγωγο πολυώνυμο $f(x) \in \mathrm{GF}(p)[x]$ βαθμού n.*

Στη συνέχεια εξετάζουμε την ομάδα Galois $\mathrm{Gal}\,(\mathrm{GF}(p^n)/\,\mathrm{GF}(p))$.

Θεώρημα 4.2.10. *Έστω $n > 1$ φυσικός αριθμός. Τότε*

$$\mathrm{Gal}\,(\mathrm{GF}(p^n)/\,\mathrm{GF}(p)) \cong \mathbb{Z}_n.$$

Απόδειξη. Σύμφωνα με το Πόρισμα 4.2.4, υπάρχει $a \in \mathrm{GF}(p^n)$ πρωταρχικό. Έστω $f(x) = \mathrm{irr}_{(\mathbb{Z}_p,a)}(x)$ και $G = \mathrm{Gal}\,(\mathrm{GF}(p^n)/\,\mathrm{GF}(p))$. Από το Θεώρημα 4.1.2, η επέκταση $\mathrm{GF}(p^n)/\,\mathrm{GF}(p)$ είναι επέκταση του Galois. Αφού το a είναι πρωταρχικό στοιχείο του $\mathrm{GF}(p^n)$, έπεται ότι $\mathrm{GF}(p^n) = \mathrm{GF}(p)(a)$. Κάθε ρίζα του $f(x)$ είναι επίσης ρίζα του διαχωρίσιμου πολυωνύμου $x^{p^n} - x \in \mathrm{GF}(p)[x]$, άρα το $f(x)$ είναι επίσης διαχωρίσιμο. Επομένως, από το Πόρισμα 3.2.4 έπεται ότι

$$|G| = [\mathrm{GF}(p^n) : \mathrm{GF}(p)] = n.$$

Στη συνέχεια θα δείξουμε ότι η ομάδα G είναι κυκλική προσδιορίζοντας έναν από τους γεννήτορες της G. Η συνάρτηση

$$\sigma :\ \mathrm{GF}(p^n) \to \mathrm{GF}(p^n), \quad b \mapsto b^p,\ b \in \mathrm{GF}(p^n),$$

είναι αυτομορφισμός του $\mathrm{GF}(p^n)$ (βλ. άσκηση 4.4.5) και διατηρεί τα στοιχεία του $\mathrm{GF}(p)$ σταθερά. Πράγματι, αφού η πολλαπλαστιακή ομάδα $(\mathrm{GF}(p)^*, \cdot)$ έχει $p-1$ στοιχεία, έπεται ότι $\forall c \in \mathrm{GF}(p)^*$, $c^{p-1} = 1$ και άρα $c^p = c$, $\forall c \in \mathrm{GF}(p)^*$. Άρα τα στοιχεία του $\mathrm{GF}(p)^*$ απεικονίζονται στον εαυτό τους. Εύκολα μπορεί να ελεγχθεί ότι η σ είναι ομομορφισμός δακτυλίων και ότι ο πυρήνας της είναι τετριμμένος. Αναγκαστικά αφού το σώμα $\mathrm{GF}(p)^*$ είναι πεπερασμένο, ο μονομορφισμός σ είναι και επιμορφισμός, δηλαδή αυτομορφισμός του $\mathrm{GF}(p)^*$. Συμπεραίνουμε, λοιπόν, ότι $\sigma \in G$. Ακόμα τα στοιχεία $\sigma, \sigma^2, \ldots, \sigma^n$ είναι διακεκριμένα στοιχεία της G. Διαφορετικά, για κάποιο $i < n$, θα είχαμε ότι $\sigma^i = \mathrm{id}_{\mathrm{GF}(p^n)}$ και ότι, για κάθε $b \in \mathrm{GF}(p^n)$, θα ίσχυε ότι

$$\sigma^i(b) = b \Rightarrow b^{p^i} = b \Rightarrow b^{p^i} - b = 0.$$

Δηλαδή, για κάθε $b \in \mathrm{GF}(p^n)$, το b θα ήταν ρίζα του πωλυωνύμου $x^{p^i} - x$. Όμως $|\,\mathrm{GF}(p^n)| = p^n$, ενώ $\deg(x^{p^i} - x) = p^i < p^n$ που είναι αδύνατον. Άρα

$$G = \langle \sigma \rangle.$$

Επομένως η G είναι κυκλική τάξης n, άρα είναι ισόμορφη με την $(\mathbb{Z}_n, +)$. □

Είδαμε ότι όταν p είναι πρώτος φυσικός αριθμός, τότε ο $\mathrm{GF}(p)$-αυτομορφισμός του $\mathrm{GF}(p^n)$

$$\sigma : \mathrm{GF}(p^n) \to \mathrm{GF}(p^n), \quad b \mapsto b^p,$$

παράγει την ομάδα $\mathrm{Gal}\,(\mathrm{GF}(p^n)/\,\mathrm{GF}(p))$. Ο αυτομορφισμός αυτός λέγεται ***αυτομορφισμός του Frobenius*** (Frobenius automorphism). Όταν $n = 1$, τότε ο αυτομορφισμός του Frobenius για το σώμα $\mathrm{GF}(p)$ είναι ακριβώς ο ταυτοτικός. Το σώμα $\mathrm{GF}(p^n)$ είναι *τέλειο*. Γενικότερα, ένα σώμα F λέγεται ***τέλειο*** (perfect) αν είναι χαρακτηριστικής μηδέν ή αν έχει χαρακτηριστική p και η συνάρτηση του Frobenius

$$f : F \to F, \quad a \mapsto a^p$$

είναι αυτομορφισμός. Η εικόνα της συνάρτησης του Frobenius συμβολίζεται με F^p, δηλ.

$$F^p = \{a^p : \ a \in F\}.$$

Είναι φανερό ότι το F^p είναι ένα υπόσωμα του F (βλ. άσκηση 4.4.6) και αποτελείται από τα στοιχεία $\beta \in F$ για τα οποία $\sqrt[p]{\beta} \in F$.

Παράδειγμα 4.2.11. Το σώμα κλασμάτων $F = \mathbb{Z}_p(x)$ του πολυωνυμικού δακτυλίου μίας μεταβλητής με συντελεστές από το σώμα $\mathbb{Z}_p$ είναι άπειρο και έχει χαρακτηριστική p. Το σώμα F δεν είναι τέλειο. Πράγματι, έστω f η συνάρτηση του Frobenius. Η f είναι μονομορφισμός. Όμως η f δεν είναι επιμορφισμός, αφού το στοιχείο $x \notin \mathrm{Im} f$, δηλ. δεν υπάρχουν πολυώνυμα $f(x)$, $g(x) \in \mathbb{Z}_p[x]$ έτσι ώστε

$$\left(\frac{f(x)}{g(x)}\right)^p = x$$

(ο αναγνώστης καλείται να συγκρίνει τους βαθμούς των πολυωνύμων $xg(x)^p$, $f(x)^p$, για να οδηγηθεί σε άτοπο).

4.3 Ενδιάμεσα υποσώματα

Στην ενότητα αυτή θα υπολογίσουμε τα ενδιάμεσα υποσώματα E του $\mathrm{GF}(p^n)$, για $n \geq 1$, όπου

$$\mathrm{GF}(p) \subset E \subset \mathrm{GF}(p^n).$$

Παρατηρούμε καταρχήν ότι ο βαθμός της επέκτασης $E/\,\mathrm{GF}(p)$, δηλ. ο $[E : \mathrm{GF}(p)]$ διαιρεί το n αφού

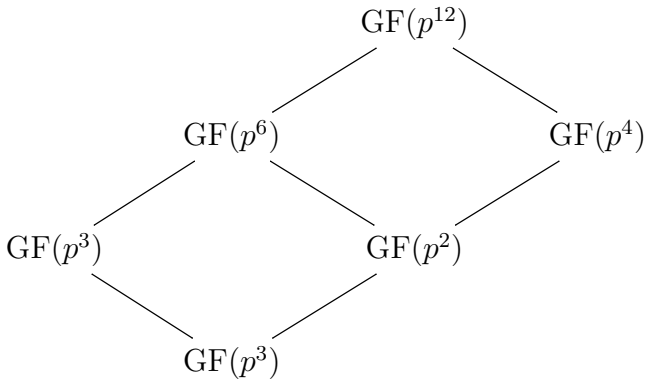
$$n = [\mathrm{GF}(p^n) : \mathrm{GF}(p)] = [\mathrm{GF}(p^n) : E]\,[E : \mathrm{GF}(p)].$$

Από το Θεμελιώδες Θεώρημα της Θεωρίας Galois γνωρίζουμε ότι σε κάθε υποομάδα της $\mathrm{Gal}\,(\mathrm{GF}(p^n)/\,\mathrm{GF}(p))$ αντιστοιχεί ακριβώς ένα ενδιάμεσο υποσώμα του $\mathrm{GF}(p^n)$. Από το Θεώρημα I.14 που περιγράφει όλες τις υποομάδες της κυκλικής ομάδας $\mathbb{Z}_n$, οδηγούμαστε στο παρακάτω συμπέρασμα.

Θεώρημα 4.3.1. *Έστω $n \geq 1$ ένας φυσικός αριθμός. Για κάθε $m|n$ υπάρχει μοναδικό υπόσωμα E του $\mathrm{GF}(p^n)$ τέτοιο ώστε $|E| = p^m$. Αντίστροφα κάθε υπόσωμα E του $\mathrm{GF}(p^n)$ έχει p^m στοιχεία, για κάποιο $m|n$.*

Στο παρακάτω παράδειγμα υπολογίζουμε τα υποσώματα του $\mathrm{GF}(p^{12})$.

Παράδειγμα 4.3.2. Το διάγραμμα των υποσωμάτων του $\mathrm{GF}(p^{12})$ φαίνεται στο Σχήμα 4.1:



Σχήμα 4.1: Τα υποσώματα του $\mathrm{GF}(p^{12})$

Έστω $\sigma \in \mathrm{Gal}\,(\mathrm{GF}(p^n)/\,\mathrm{GF}(p))$ ο αυτομορφισμός του Frobenius. Στο Θεώρημα 4.2.10 αποδείξαμε ότι το σ έχει τάξη n και ότι

$$\mathrm{Gal}\,(\mathrm{GF}(p^n)/\,\mathrm{GF}(p)) = \langle\sigma\rangle.$$

Έστω a πρωταρχικό στοιχείο του $\mathrm{GF}(p^n)$. Από την Πρόταση 2.3.2 προκύπτει ότι τα συζυγή στοιχεία του a στην $\mathrm{GF}(p^n)/\,\mathrm{GF}(p)$, δηλ. τα στοιχεία $\sigma^i(a)$, για $i = 0, \ldots, n-1$ είναι ρίζες του $\mathrm{irr}_{(\mathrm{GF}(p),a)}(x)$. Αφού

$$\deg \mathrm{irr}_{(\mathrm{GF}(p),a)}(x) = [\mathrm{GF}(p^n) : \mathrm{GF}(p)] = n,$$

από την άσκηση 2.4.19 προκύπτει ότι τα στοιχεία αυτά είναι διακεκριμένα. Απομονώνουμε, λοιπόν, τη χρήσιμη αυτή παρατήρηση.

Πρόταση 4.3.3. *Αν a είναι ένα πρωταρχικό στοιχείο του σώματος $\mathrm{GF}(p^n)$, τότε οι ρίζες του $\mathrm{irr}_{(\mathrm{GF}(p),a)}(x)$ είναι οι*

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

Θα γενικεύσουμε αυτήν την πρόταση παρακάτω. Πρώτα, όμως, έχουμε την επόμενη παρατήρηση.

Παρατήρηση 4.3.4. *Έστω $q = p^n$ και $f(x) \in \mathrm{GF}(q)[x]$. Τότε $f(x^q) = f(x)^q$. Έτσι αν a είναι ρίζα του $f(x)$, τότε το a^{q^t} είναι επίσης ρίζα του $f(x)$, για κάθε φυσικό αριθμό t.*

Απόδειξη. Έστω ότι

$$f(x) = \sum_{i=0}^{s} c_i x^i \in \mathrm{GF}(q)[x],\ \text{όπου } c_i \in \mathrm{GF}(q).$$

Θα αποδείξουμε ότι $f(x^q) = f(x)^q$. Καταρχήν, πριν υπολογίσουμε τη δύναμη $f(x)^q$, παρατηρούμε ότι $c^q = c$, για κάθε $c \in \mathrm{GF}(q)$. Πράγματι, αυτό είναι προφανές όταν $c = 0$, ενώ όταν $c \in \mathrm{GF}(q)^*$, τότε $c^{q-1} = 1$ από το Θεώρημα του Lagrange και άρα $c^q = c$. Στη συνέχεια, θα αποδείξουμε ότι

$$\left(\sum_{i=0}^{s} c_i x^i\right)^q = \sum_{i=0}^{s} c_i^q x^{iq}.$$

Με απλή μαθηματική επαγωγή αρκεί να αποδείξουμε αναλυτικά την παραπάνω πρόταση στην περίπτωση δύο προσθετέων. Αρκεί, λοιπόν, να αποδείξουμε ότι

$$(f_1 + f_2)^q = f_1^q + f_2^q, \text{ για } f_1, f_2 \in \mathrm{GF}(q)[x].$$

Αφού η ακέραια περιοχή $\mathrm{GF}(q)[x]$ έχει χαρακτηριστική τον πρώτο αριθμό p και ο p διαιρεί τον διωνυμικό συντελεστή $\binom{p}{i}$, για $i = 1, \ldots, p-1$, από την ανάπτυξη του διωνύμου, βλέπουμε ότι

$$(f_1 + f_2)^p = x_1^p + x_2^p, \text{ για } f_1, f_2 \in \mathrm{GF}(q)[x].$$

Έτσι

$$(f_1 + f_2)^{p^2} = ((f_1 + f_2)^p)^p = f_1^{p^2} + f_2^{p^2}.$$

Επαναλαμβάνοντας προκύπτει ότι

$$(f_1 + f_2)^q = f_1^q + f_2^q, \text{ για } f_1, f_2 \in \mathrm{GF}(q)[x].$$

Επομένως

$$f(x)^q = (\sum_{i=0}^{s} c_i x^i)^q = \sum_{i=0}^{s} c_i^q x^{iq} = \sum_{i=0}^{s} c_i (x^q)^i = f(x^q).$$

Έτσι, αν a είναι ρίζα του $f(x)$ και $f(a) = 0$, τότε

$$0 = f(a)^q = f(a^q),$$

δηλ. το a^q είναι επίσης ρίζα του $f(x)$. Επαναλαμβάνοντας, έχουμε ότι αν a είναι ρίζα του $f(x)$, τότε a^{q^t} είναι ρίζα του $f(x)$ για κάθε φυσικό αριθμό t. □

Όταν το πολυώνυμο $f(x) \in \mathrm{GF}(q)[x]$ είναι ανάγωγο, τότε μπορούμε να πούμε κάτι περισσότερο.

Πρόταση 4.3.5. *Έστω $n \geq 1$ φυσικός αριθμός, p ένας πρώτος φυσικός αριθμός, $q = p^n$ και $f(x) \in \mathrm{GF}(q)[x]$ ένα ανάγωγο πολυώνυμο βαθμού s.*

i) Για έναν φυσικό αριθμό t, ο s διαιρεί τον t αν και μόνο αν το $f(x)$ διαιρεί το πολυώνυμο $x^{q^t} - x$.

ii) Το $f(x)$ έχει μία ρίζα $a \in \mathrm{GF}(q^s)$ και όλες οι ρίζες του $f(x)$ στο $\mathrm{GF}(q^s)$ είναι οι: $a, a^q, \ldots, a^{q^{s-1}}$.

Απόδειξη. i) Έστω $a \in E$ μία ρίζα του $f(x)$, όπου E είναι το σώμα ανάλυσης του $f(x)$. Από το Θεώρημα 2.2.3, έχουμε την ισότητα

$$\deg f(x) = s = [\mathrm{GF}(q)(a) : \mathrm{GF}(q)]$$

και επομένως $\mathrm{GF}(q)(a)$ είναι πεπερασμένο σώμα με q^s στοιχεία. Σύμφωνα με το Θεώρημα 4.1.2 συμπεραίνουμε ότι το $\mathrm{GF}(q)(a)$ ταυτίζεται με το $\mathrm{GF}(q^s)$ με προσέγγιση ισομορφίας. Αν τώρα το $f(x)$ διαιρεί το πολυώνυμο $x^{q^t} - x$, τότε αφού το $\mathrm{GF}(q^t)$ είναι το σώμα ανάλυσης του $x^{q^t} - x$, ισχύει ο εγκλεισμός

$$\mathrm{GF}(q)(a) \subseteq E \subseteq \mathrm{GF}(q^t).$$

Έτσι,

$$\mathrm{GF}(q) \subseteq \mathrm{GF}(q)(a) \subseteq \mathrm{GF}(q^t)$$

και

$$[\mathrm{GF}(q^t) : \mathrm{GF}(q)] = [\mathrm{GF}(q^t) : \mathrm{GF}(q)(a)]\,[\mathrm{GF}(q)(a) : \mathrm{GF}(q)].$$

Επομένως

$$t = [\mathrm{GF}(q^t) : \mathrm{GF}(q)(a)]\,s$$

και $s|t$.

Αντίστροφα, αν $s|t$ τότε $\mathrm{GF}(q^s) \subseteq \mathrm{GF}(q^t)$ και επομένως κάθε ρίζα του $f(x)$ εμφυτεύεται στο $\mathrm{GF}(q^t)$. Αφού τα στοιχεία του $\mathrm{GF}(q^t)$ είναι οι ρίζες του $x^{q^t} - x$ (βλ. Πρόταση 4.1.1), συμπεραίνουμε ότι το $f(x)$ διαιρεί το $x^{q^t} - x$ (βλ.Πόρισμα 1.2.4).

ii) Έστω a μία ρίζα του $f(x)$ σε ένα σώμα ανάλυσης E. Όπως είδαμε στην απόδειξη του i), $\mathrm{GF}(q)(a) = \mathrm{GF}(q^s)$. Έστω $H = \mathrm{Gal}\,(\mathrm{GF}(q^s)/\,\mathrm{GF}(q))$ και $G = \mathrm{Gal}\,(\mathrm{GF}(q^s)/\,\mathrm{GF}(p))$. Αφού το $f(x)$ είναι ανάγωγο, από το Θεώρημα 2.2.3, έπεται ότι $|H| = s$. Από το Θεμελιώδες Θεώρημα της Θεωρίας Galois έχουμε ότι $H \leq G$. Επίσης, αφού $q^s = (p^n)^s = p^{ns}$, σύμφωνα με το Θεώρημα 4.2.10, η ομάδα G είναι κυκλική, τάξης ns και παράγεται από τον σ, τον αυτομορφισμό τους Frobenius. Έτσι, σύμφωνα με το Θεώρημα I.14, η υποομάδα H της G παράγεται από τον αυτομορφισμό $\sigma^{\frac{ns}{s}} = \sigma^n$. Παρατηρούμε ότι

$$\sigma^n :\ \mathrm{GF}(q^s) \to \mathrm{GF}(q^s), \quad a \mapsto a^q.$$

Σύμφωνα με την άσκηση 2.4.19, τα στοιχεία

$$a, a^q, \ldots, a^{q^{s-1}}$$

είναι διακεκριμένα. Από την Πρόταση 2.3.2 (ή την Παρατήρηση 4.3.4) τα στοιχεία αυτά είναι ρίζες του $f(x)$. □

Από την απόδειξη της Πρότασης 4.3.5 προκύπτει το παρακάτω συμπέρασμα.

Παρατήρηση 4.3.6. *Έστω $q = p^n$ και $f(x) \in \mathrm{GF}(q)[x]$ ανάγωγο. Τότε το $f(x)$ είναι διαχωρίσιμο.*

Απόδειξη. Έστω $\deg f(x) = s$. Τότε σύμφωνα με την Πρόταση 4.3.5

$$f(x) \mid (x^{q^s} - x).$$

Το $x^{q^s} - x \in \mathrm{GF}(q)[x]$ είναι διαχωρίσιμο, άρα και το $f(x)$. □

Σημειώνουμε ότι η ιδιότητα αυτή, δηλ. ότι κάθε ανάγωγο πολυώνυμο είναι και διαχωρίσιμο, χαρακτηρίζει τα τέλεια σώματα, βλ. άσκηση 4.4.8.

Παράδειγμα 4.3.7. Έστω F σώμα με χαρακτηριστική $p \neq 0$ και $a \in F$. Θα αποδείξουμε ότι το πολυώνυμο $x^{p^n} - a \in F[x]$, όπου $n > 1$ είναι ένας φυσικός αριθμός, είναι ανάγωγο αν και μόνο αν $a \notin F^p$. Πράγματι, αν $a \in F^p$, δηλ. $b^p = a$, για κάποιο $b \in F$, τότε

$$x^{p^n} - a = x^{p^n} - b^p = (x^{p^{n-1}})^{\,p} - b^p = (x^{p^{n-1}} - b)^{\,p}.$$

Αντίστροφα, έστω ότι $x^{p^n} - a$ δεν είναι ανάγωγο. Τότε υπάρχει $g(x) \in F[x]$ κανονικό, ανάγωγο και τέτοιο ώστε

$$g(x) \mid (x^{p^n} - a).$$

Από το Θεώρημα του Kronecker (Θεώρημα 1.4.3) υπάρχει μία επέκταση K/F, όπου το $g(x)$ έχει μία ρίζα, έστω β. Αυτό σημαίνει ότι

$$g(b) = 0 \Rightarrow b^{p^n} - a = 0 \Rightarrow \beta^{p^n} = a.$$

Άρα, στον δακτύλιο $K[x]$ ισχύει ότι

$$x^{p^n} - a = x^{p^n} - \beta^{p^n} = (x-\beta)^{p^n}$$

και

$$g(x) \mid (x-\beta)^{p^n}.$$

Αφού ο δακτύλιος $K[x]$ είναι Π.Μ.Α. έπεται ότι η ανάλυση του $g(x)$ σε ανάγωγους παράγοντες στον $K[x]$ είναι της μορφής

$$g(x) = (x-\beta)^s, \text{ όπου } s = \deg g(x).$$

Επομένως, στον $F[x]$ ισχύει ότι

$$g(x) = x^s - \beta x^{s-1} + \cdots + (-1)^s \beta^s.$$

Άρα $\beta^s \in F$ και μάλιστα $1 \leq s < p^n$. Έστω $p^t = \text{ΜΚΔ}(s, p^n)$. Τότε $t < n$ και

$$p^t = ks + lp^n \text{ για } k, l \in \mathbb{Z}.$$

Επομένως, για το $\beta^{p^t} \in F$ ισχύει:

$$\beta^{p^t} = \beta^{ks}\beta^{lp^n} = (b^s)^k (b^{p^n})^l = (b^s)^k a^l.$$

Συνεπώς

$$\beta^{p^{n-1}} = (\beta^{p^t})^{p^{n-1-t}} \in F.$$

Τότε, όμως,

$$a = \beta^{p^n} = (\beta^{p^{n-1}})^p \in F^p.$$

Αποδείξαμε, λοιπόν, το επόμενο συμπέρασμα:

Πρόταση 4.3.8. *$x^{p^n} - a \in F[x]$ είναι ανάγωγο αν και μόνο αν $a \notin F^p$.*

4.4 Ασκήσεις

1. Έστω $E = \mathrm{GF}(8)$.
   - Να υπολογίσετε τους πίνακες για τις πράξεις στις ομάδες $(E, +)$ και $(E^*, \cdot)$.
   - Να βρείτε ένα πρωταρχικό στοιχείο του E.
   - Να δείξετε ότι E είναι τέλειο, δείχνοντας αναλυτικά ότι $E = E^2$.
2. Έστω $f(x) = x^3 + x^2 + 2x \in \mathbb{Z}_5[x]$.
   - Να βρείτε ένα σώμα ανάλυσης E του $f(x)$.
   - Να περιγράψετε τα στοιχεία του E.
   - Να βρείτε ένα στοιχείο a έτσι ώστε $E = \mathbb{Z}_5(a)$.
3. Να δείξετε ότι υπάρχει ανάγωγο πολυώνυμο βαθμού 6 πάνω από το $\mathbb{Z}_5$.
4. Να υπολογίσετε τα υποσώματα $\mathrm{GF}(p) \subset E \subset \mathrm{GF}(p^{36})$.

5. Να αποδείξετε ότι αν F είναι σώμα χαρακτηριστικής $p \neq 0$, τότε η συνάρτηση του Frobenius, $f: F \to F$, $b \mapsto b^p$ είναι ομορφισμός του F.

6. Να αποδείξετε ότι αν F είναι σώμα χαρακτηριστικής $p \neq 0$, τότε F^p είναι υπόσωμα του F.

7. Έστω p ένας πρώτος φυσικός αριθμός και F ένα σώμα με $\mathrm{char}\, F = p$. Δίνεται το πολυώνυμο $f(x) = x^p - x - a \in F[x]$. Αν το $f(x)$ έχει μία ρίζα, έστω β, στο F, να αποδείξετε ότι οι ρίζες του $f(x)$ είναι οι $\beta, \beta+1, \ldots, \beta+(p-1) \in F$. Να αποδείξετε ότι το $f(x)$ είναι ανάγωγο στο $F[x]$ ή το $f(x)$ αναλύεται σε γινόμενο γραμμικών παραγόντων στο $F[x]$.

8. Να αποδείξετε ότι ένα σώμα F είναι τέλειο αν και μόνον αν κάθε ανάγωγο πολυώνυμο του $F[x]$ είναι διαχωρίσιμο.

Βιβλιογραφία Κεφαλαίου 4

[1] Bastida, J. R. *Field Extensions and Galois Theory, Vol. 22*. Addison-Wesley, 2007.

[2] Dummit, D.S., Foote, R.M. *Abstract Algebra*. J. Wiley and Sons, INc, 2004.

[3] Escofier, J.P. *Galois Theory*. Springer, 2001.

[4] Fox, D. *Galois Theory*. John Wiley & Sons, 2012.

[5] Lidl, R., Niederreiter, H. *Finite Fields*. Cambridge University Press, New York 1994.

[6] Milne, J.S. *Fields and Galois Theory*. www.jmilne.org, 2014.

[7] Rotman, J. *Θεωρία Galois*. Leader Books, 2000.

[8] Stewart, I. *Galois Theory*. Champan and Hall, 1973.

Κεφάλαιο 5

Κυκλοτομικά πολυώνυμα

Σε αυτό το κεφάλαιο εφαρμόζουμε τη θεωρία Galois, όπως αυτή αναπτύχθηκε στο Κεφάλαιο 3, για τα πολυώνυμα $x^n - 1$ και $x^n - a$. Επίσης εξετάζουμε τις κυκλοτομικές, τις κυκλικές και τις αβελιανές επεκτάσεις σωμάτων.

5.1 Ρίζες της μονάδας

Έστω F σώμα χαρακτηριστικής p, για κάποιον πρώτο αριθμό p. Αν $n = p^t k$, όπου $(k, p) = 1$, τότε

$$x^n - 1 = x^{kp^t} - 1 = (x^k)^{p^t} - 1 = (x^k - 1)^{p^t},$$

βλ. την απόδειξη της Παρατήρησης 4.3.4. Άρα, οι n-ρίζες της μονάδας είναι ακριβώς οι k-ρίζες της μονάδας. Έτσι, θα ασχοληθούμε με τις παρακάτω περιπτώσεις:

- η χαρακτηριστική του F είναι μηδέν, $\operatorname{char} F = 0$,
- $\operatorname{char} F = p$ και ο p δεν διαιρεί τον n.

Και στις δύο περιπτώσεις, το πολυώνυμο $x^n - 1$ είναι διαχωρίσιμο και μπορούμε να εφαρμόσουμε τα εργαλεία της Θεωρίας Galois.

Έστω, λοιπόν, E το σώμα ανάλυσης του πολωνύμου $f(x) = x^n - 1 \in F[x]$, όπου F και n είναι όπως θέσαμε παραπάνω. Το σύνολο των n-ριζών της μονάδας είναι υποομάδα της πολλαπλασιαστικής ομάδας του E^* και θα το καλούμε ***ομάδα των n-ριζών της μονάδας*** (group of the nth roots of unity) πάνω από το σώμα F. Σύμφωνα με το Θεώρημα 4.2.3, η υποομάδα αυτή είναι κυκλική. Ένα παράγον στοιχείο αυτής της ομάδας καλείται ***n-πρωταρχική ρίζα της μονάδας*** (nth primitive root of unity) πάνω από το F.

Παράδειγμα 5.1.1. Το στοιχείο $e^{2\pi i/n}$ είναι πρωταρχική n-ρίζα της μονάδας πάνω από το $\mathbb{Q}$.

Η επόμενη πρόταση συγκεντρώνει μερικές ιδιότητες των n-ριζών της μονάδας που μας είναι γνωστές από τις κυκλικές ομάδες.

Πρόταση 5.1.2. *Έστω F ένα σώμα και έστω ότι $\omega \in E$, όπου ω είναι μία πρωταρχική n-ρίζα της μονάδας πάνω από το F και n είναι φυσικός αριθμός. Τότε:*

i) Οι πρωταρχικές n-ρίζες της μονάδας πάνω από το F είναι πλήθους $\phi(n)$, όπου ϕ είναι η συνάρτηση του Euler.

ii) Έστω $d|n$. Τότε κάθε d-ρίζα της μονάδας είναι επίσης n-ρίζα της μονάδας. Η $\omega^{n/d}$ είναι μία d-πρωταρχική ρίζα της μονάδας πάνω από το F.

Απόδειξη. Η υπόθεση ότι το E περιέχει την ω σημαίνει ότι το E περιέχει όλες τις δυνάμεις της ω άρα και όλες τις ρίζες του $x^n-1 \in F[x]$. Το i) είναι άμεση συνέπεια του Θεωρήματος I.8. Για το ii), παρατηρούμε ότι σύμφωνα με την Πρόταση I.7.iv, έχουμε ότι $\operatorname{ord}\left(\omega^{n/d}\right) = d$ και άρα $\omega^{n/d}$ παράγει την κυκλική ομάδα των d-ριζών της μονάδας. □

Παραδείγματα 5.1.3.

1. Το -1 είναι 2-πρωταρχική ρίζα της μονάδας.
2. Έστω p πρώτος. Οι πρωταρχικές p-ρίζες της μονάδας πάνω από το $\mathbb{Q}$ είναι οι
$$e^{2\pi i/p},\ e^{4\pi i/p},\ \cdots, e^{2(p-1)\pi i/p}.$$
3. Θα υπολογίσουμε τις πρωταρχικές 8-ρίζες της μονάδας πάνω από το $\mathbb{Q}$. Αφού $\phi(8) = 4$, υπάρχουν 4 τέτοιες ρίζες. Είναι οι
$$e^{\pi i/4},\ e^{3\pi i/4},\ e^{5\pi i/4},\ e^{7\pi i/4}.$$
4. Έστω E πεπερασμένο σώμα, έτσι ώστε $|E| = 2^4$. Σύμφωνα με το Θεώρημα 4.2.6, το E^* είναι κυκλική ομάδα. Όπως είδαμε στο Παράδειγμα 4.1.3.3, υπάρχει $a \in E$ έτσι ώστε $\operatorname{ord}(a) = 15$. Άρα το $E = \mathbb{Z}_2(a)$ είναι σώμα ανάλυσης του $x^{15}-1$ πάνω από το $\mathbb{Z}_2$ και το a είναι πρωταρχική 15-ρίζα της μονάδας πάνω από το $\mathbb{Z}_2$. Υπάρχουν $\phi(15)$, δηλ. οκτώ, πρωταρχικές 15-ρίζες της μονάδας πάνω από το $\mathbb{Z}_2$. Είναι οι
$$a,\ a^2,\ a^4,\ a^7,\ a^8,\ a^{11},\ a^{13},\ a^{14}.$$
Σημειώνουμε ότι $\deg \operatorname{irr}_{(\mathbb{Z}_2,a)}(x) = 4$, αφού
$$4 = [E : \mathbb{Z}_2] = \deg \operatorname{irr}_{(\mathbb{Z}_2,a)}(x).$$
Σύμφωνα με την Πρόταση 5.1.2, το στοιχείο a^3 είναι μία 5-πρωταρχική ρίζα της μονάδας πάνω από το $\mathbb{Z}_2$. Επομένως, οι 5-ρίζες της μονάδας πάνω από το $\mathbb{Z}_2$ είναι οι
$$1,\ a^3,\ a^6,\ a^9,\ a^{12}.$$
Κατά συνέπεια, το υπόσωμα $L = \mathbb{Z}_2(a^3)$ του E είναι σώμα ανάλυσης του $x^5 - 1 \in \mathbb{Z}_2[x]$. Αφού $x-1$ και $x^4+x^3+x^2+x+1$ είναι ανάγωγα στο $\mathbb{Z}_2[x]$ και
$$x^5 - 1 = (x-1)(x^4+x^3+x^2+x+1),$$
έχουμε ότι $\operatorname{irr}_{(\mathbb{Z}_2,a^3)}(x) = x^4+x^3+x^2+x+1$ και άρα $[L : \mathbb{Z}_2] = 4$. Όμως $[E : \mathbb{Z}_2] = 4$ και επομένως $L = E$. Τέλος, σημειώνουμε ότι η ανάλυση του $x^{15} - 1 \in \mathbb{Z}_2[x]$ σε γινόμενο ανάγωγων πολυωνύμων έχει ως εξής:
$$x^{15} - 1 = (x-1)(x^2+x+1)(x^4+x+1)(x^4+x^3+1)(x^4+x^3+x^2+x+1).$$

Έστω E σώμα ανάλυσης του $x^n - 1$ πάνω από το σώμα F. Ένα πρώτο αποτέλεσμα για την ομάδα $\operatorname{Gal}(E/F)$ δίνεται στο Θεώρημα 5.1.4, στην περίπτωση που $\operatorname{char} F \nmid n$. Για την περίπτωση που το σώμα F είναι το σώμα των ρητών, τότε όπως θα δούμε, η απάντηση δίνεται από το Πόρισμα 5.1.5 και το Θεώρημα 5.2.9.

Θεώρημα 5.1.4. *Έστω F ένα σώμα έτσι ώστε $\operatorname{char} F \nmid n$, $f(x) = x^n - 1 \in F[x]$ και E το σώμα ανάλυσης του $f(x)$. Η ομάδα $\operatorname{Gal}(E/F)$ είναι ισόμορφη με μία υποομάδα της $\mathbb{Z}_n^\sharp$ και ο βαθμός της επέκτασης $[E : F]$ διαιρεί τον $\phi(n)$.*

Απόδειξη. Έστω $G = \mathrm{Gal}(E/F)$, ω μία πρωταρχική n-ρίζα της μονάδας στο E. Τότε το $E = F(\omega)$. Έστω $\sigma \in G$. Αφού το σύνολο των n-ριζών της μονάδας στο E είναι η κυκλική ομάδα $\langle\omega\rangle$, έπεται ότι $\sigma(\omega) = \omega^i$, για κάποιο $i \in \{1, \ldots, n\}$. Επομένως, ο περιορισμός του σ στην υποομάδα $\langle\omega\rangle$ του E^* είναι αυτομορφισμός της $\langle\omega\rangle$. Επίσης,

$$\tau = \sigma|_{\langle\omega\rangle} : \ \langle\omega\rangle \longrightarrow \langle\omega\rangle, \quad \omega \mapsto \omega^i$$

είναι ισομορφισμός ομάδων, αφού είναι μονομορφισμός πεπερασμένης ομάδας. Επομένως το ω^i είναι και αυτό παράγον στοιχείο της $\langle\omega\rangle$. Σύμφωνα με την Πρόταση Ι.7, ο μέγιστος κοινός διαιρέτης (i, n) είναι 1. Θεωρούμε τώρα την απεικόνιση

$$\psi : \ G \to \mathbb{Z}_n^\sharp, \quad \sigma \mapsto \bar{i}, \ \text{όπου } \sigma(\omega) = \omega^i.$$

Είναι εύκολο να αποδειχθεί ότι η ψ είναι ομομορφισμός ομάδων. Ακόμη

$$\ker\psi = \{\sigma \in G : \ \bar{i} = \bar{1}\} = \{\sigma \in G : \ \sigma(\omega) = \omega\} = \{\mathrm{id}_L\}$$

και η ψ είναι μονομορφισμός. □

Έστω τώρα p ένας περιττός πρώτος αριθμός. Το σώμα ανάλυσης του $x^p - 1$ πάνω από το $\mathbb{Q}$ είναι το $\mathbb{Q}(\omega)$, όπου $\omega = e^{2\pi i/p}$. Από το Θεώρημα 5.1.4 προκύπτει το παρακάτω Πόρισμα.

Πόρισμα 5.1.5. *Έστω $E = \mathbb{Q}(\omega)$, όπου $\omega = e^{2\pi i/p}$, για κάποιον περιττό πρώτο φυσικό αριθμό p. Τότε*

$$\mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q}) \cong \mathbb{Z}_p^*,$$

και

$$\mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q}) = \langle\sigma\rangle, \ \textit{όπου } \sigma : \omega \mapsto \omega^2.$$

Απόδειξη. Σύμφωνα με το Παράδειγμα 1.3.8 το πολυώνυμο

$$\Phi_p(x) = x^{p-1} + \cdots + x + 1$$

είναι ανάγωγο. Αφού $x^p - 1 = (x-1)\Phi_p(x)$ και $\omega^p - 1 = 0$, έπεται ότι το ω είναι ρίζα του $\Phi_p(x)$. Επομένως $\mathrm{irr}_{(\mathbb{Q},\omega)}(x) = \Phi_p(x)$ και $\deg \mathrm{irr}_{(\mathbb{Q},\omega)}(x) = p - 1$. Άρα

$$|\,\mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q})| = p - 1.$$

Σύμφωνα με το Θεώρημα 5.1.4, η ομάδα $\mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q})$ είναι ισόμορφη με υποομάδα της $\mathbb{Z}_p^*$. Επίσης, αφού $|\mathbb{Z}_p^*| = p - 1$, έπεται ότι

$$\mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q}) \cong \mathbb{Z}_p^* \,.$$

Τέλος, αφού η ομάδα $\mathbb{Z}_p^*$ είναι κυκλική, έπεται ότι και η ομάδα $\mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q})$ είναι κυκλική και

$$\mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q}) = \langle\sigma\rangle, \ \text{όπου } \sigma : \omega \mapsto \omega^2.$$

□

Παραδείγματα 5.1.6.

1. Έστω $\omega = e^{2\pi i/8} = e^{\pi i/4}$, η πρωταρχική 8-ρίζα της μονάδας. Τότε $\mathrm{irr}_{(\mathbb{Q},\omega)}(x) = x^4+1$ και
$$|\operatorname{Gal}(\mathbb{Q}(\omega)/\mathbb{Q})| = 4.$$
Σύμφωνα με το Θεώρημα 5.1.4 η ομάδα $\operatorname{Gal}(\mathbb{Q}(\omega)/\mathbb{Q})$ είναι ισόμορφη με υποομάδα της $\mathbb{Z}_8^\sharp$. Αφού $|\mathbb{Z}_8^\sharp| = 4$, έπεται ότι $\operatorname{Gal}(\mathbb{Q}(\omega)/\mathbb{Q}) \cong \mathbb{Z}_8^\sharp$, που δεν είναι κυκλική, βλ. Παράδειγμα 4.2.6.1. Άρα $\operatorname{Gal}(\mathbb{Q}(\omega)/\mathbb{Q})$ είναι ισόμορφη με την ομάδα του Klein.
2. Ο μονομορφισμός του Θεωρήματος 5.1.4 δεν είναι πάντα επιμορφισμός. Για παράδειγμα, έστω $E = \mathbb{Z}_2(a)$ το σώμα ανάλυσης του $x^{15}-1$ πάνω από το $\mathbb{Z}_2$, όπως στο Παράδειγμα 5.1.3.4. Η ομάδα $\mathbb{Z}_{15}^\sharp$ έχει 8 στοιχεία. Αφού $|E| = 16$ και $[E:\mathbb{Z}_2] = 4$, η ομάδα $\operatorname{Gal}(E/\mathbb{Z}_2)$ έχει τάξη 4 και μάλιστα $\operatorname{Gal}(E/\mathbb{Z}_2) \cong \mathbb{Z}_4$, σύμφωνα με το Θεώρημα 4.2.10.

5.2 Κυκλοτομικά πολυώνυμα

Σε αυτό το εδάφιο θα ασχοληθούμε με την ανάλυση του πολυωνύμου x^n-1 σε γινόμενο ανάγωγων παραγόντων στο $\mathbb{Q}[x]$. Ας συμβολίσουμε με U_n το σύνολο των πρωταρχικών n-ριζών της μονάδας. Από την Πρόταση 5.1.2 έχουμε ότι $|U_n| = \phi(n)$, όπου ϕ είναι η συνάρτηση του Euler. Το πολυώνυμο

$$\Phi_n(x) = \prod_{\omega\in U_n}(x-\omega) \in \mathbb{C}[x] \tag{5.2.0.1}$$

λέγεται ***n-κυκλοτομικό πολυώνυμο*** (n-cyclotomic polynomial).

Παράδειγμα 5.2.1. Οι 3-ρίζες της μονάδας είναι οι 1, ω, ω^2, όπου $\omega = e^{2\pi i/3}$. Από αυτές οι ω και ω^2 έχουν τάξη 3 και είναι πρωταρχικές 3-ρίζες της μονάδας. Άρα

$$\Phi_3(x) = (x-\omega)(x-\omega^2) = \frac{x^3-1}{x-1} = x^2+x+1.$$

Στο Παράδειγμα 5.2.3.2 βλέπουμε ότι, όταν ο n είναι πρώτος, τότε ο τύπος της (5.2.0.1) δίνει το κυκλοτομικό πολυώνυμο όπως το είδαμε στο Παράδειγμα 1.2.7. Η ορολογία κυκλοτομικό πολυώνυμο οφείλεται στην ιδιότητα που έχουν οι n-ρίζες της μονάδας να διαιρούν τον κύκλο σε n πλήθους ίσα τόξα όπως φαίνεται στο Σχήμα 5.1.

Πρόταση 5.2.2. *Έστω $n>0$ ένας φυσικός αριθμός. Τότε*

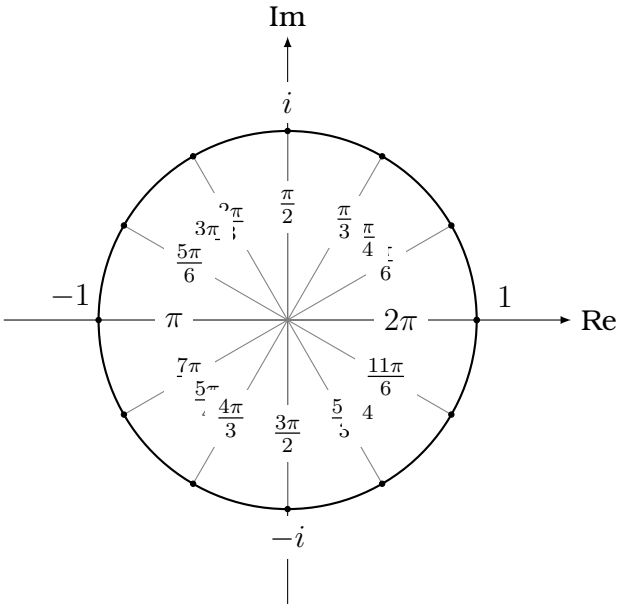
$$x^n-1 = \prod_{d\,|\,n}\Phi_d(x).$$

Απόδειξη. Έστω G η κυκλική ομάδα των n-ριζών της μονάδας στο σώμα των μιγαδικών αριθμών. Τα στοιχεία που παράγουν την υποομάδα της G τάξης d, όπου $d|n$, είναι οι πρωταρχικές d-ρίζες της μονάδας και αποτελούν το σύνολο U_d. Σύμφωνα με τον τύπο 4.2.0.1 έχουμε ότι

$$G = \bigcup_{d\,|\,n} U_d.$$

Αφού

$$x^n-1 = \prod_{a\in G}(x-a)$$



Σχήμα 5.1: Οι n-ρίζες της μονάδας

και

$$\Phi_d(x) = \prod_{a \in U_d} (x - a),$$

έπεται ότι

$$x^n - 1 = \prod_{d \mid n} \Phi_d(x).$$

□

Παραδείγματα 5.2.3.

1. Υπολογίζουμε το κυκλοτομικό πολυώνυμο $\Phi_n(x)$ για κάποιες μικρές τιμές του θετικού ακεραίου $n > 0$. Με ω συμβολίζουμε κάθε φορά μία πρωταρχική n-ρίζα της μονάδας.

   - $\Phi_1(x) = x - 1$.
   - $\Phi_2(x) = x + 1$. Πράγματι
   $$\Phi_2(x) = \frac{x^2 - 1}{x - 1} = x + 1.$$
   - Όπως είδαμε στο Παράδειγμα 5.2.1, $\Phi_3(x) = x^2 + x + 1$.
   - $\Phi_4(x) = x^2 + 1$. Πράγματι
   $$\Phi_4(x) = \prod_{(t,4)=1} (x - \omega^t) = (x - \omega)(x - \omega^3) = (x - i)(x + i).$$
   Παρατηρούμε επίσης ότι
   $$\Phi_1(x)\Phi_2(x)\Phi_4(x) = x^4 - 1.$$
   Εναλλακτικά, λοιπόν, θα μπορούσαμε να υπολογίσουμε το πολυώνυμο $\Phi_4(x)$ ως το πηλίκο
   $$\Phi_4(x) = \frac{x^4 - 1}{\Phi_1(x)\Phi_2(x)} = \frac{x^4 - 1}{x^2 - 1} = x^2 + 1.$$

- $\Phi_5(x) = x^4 + x^3 + x^2 + x + 1$.
- $\Phi_6(x) = x^2 - x + 1$.

2. Όταν p είναι πρώτος φυσικός αριθμός, τότε $U_p = \{\omega, \ldots, \omega^{p-1}\}$. Επομένως

$$x^p - 1 = (x-1)\Phi_p(x) \;\Rightarrow\; \Phi_p(x) = x^{p-1} + \cdots + x + 1.$$

Οι επόμενες προτάσεις δίνουν σημαντικές πληροφορίες για τα κυκλοτομικά πολυώνυμα.

Πρόταση 5.2.4. *$\Phi_n(x) \in \mathbb{Z}[x]$, για κάθε φυσικό αριθμό n.*

Απόδειξη. Θα αποδείξουμε την πρόταση επαγωγικά ως προς το n. Για $n = 1$, η πρόταση ισχύει αφού $\Phi_1(x) = x - 1$. Έστω ότι η πρόταση ισχύει για $1 \leq k < n$, δηλ. $\Phi_k(x) \in \mathbb{Z}[x]$, για $1 \leq k < n$. Θα αποδείξουμε ότι $\Phi_n(x) \in \mathbb{Z}[x]$. Παρατηρούμε ότι στον $\mathbb{C}[x]$, το $x^n - 1$ αναλύεται ως εξής:

$$x^n - 1 = \prod_{d \mid n} \Phi_d(x) = \Phi_n(x) \prod_{\substack{d \mid n \\ d<n}} \Phi_d(x). \tag{5.2.4.1}$$

Όμως, το πολυώνυμο $\prod_{\substack{d|n \\ d<n}} \Phi_d(x)$ έχει ακέραιους συντελεστές από την υπόθεση της μαθηματικής επαγωγής. Επομένως, από τη σχέση 5.2.4.1, συμπεραίνουμε ότι το $\prod_{\substack{d \mid n \\ d<n}} \Phi_d(x)$ διαιρεί το $x^n - 1$ στον $\mathbb{Z}[x]$ και επομένως $\Phi_n(x) \in \mathbb{Z}[x]$.

□

Έστω n ένας θετικός ακέραιος, ω μία πρωταρχική ρίζα της μονάδας και $f(x) = \mathrm{irr}_{(\mathbb{Q},\omega)}(x)$. Αφού ω είναι ρίζα του $x^n - 1$, έπεται ότι

$$x^n - 1 = f(x)g(x),$$

για κάποιο $g(x) \in \mathbb{Q}[x]$. Επομένως, σύμφωνα με την Πρόταση 1.3.3, το $f(x)$ ανήκει στους ανάγωγους παράγοντες του $x^n - 1$ στο $\mathbb{Z}[x]$ και κατά συνέπεια το $g(x) \in \mathbb{Z}[x]$.

Πρόταση 5.2.5. *Έστω n ένας θετικός ακέραιος, ω μία πρωταρχική n-ρίζα της μονάδας και $f(x) = \mathrm{irr}_{(\mathbb{Q},\omega)}(x)$. Τότε το ω^p είναι επίσης ρίζα του $f(x)$, για κάθε πρώτο $p \nmid n$.*

Απόδειξη. Σύμφωνα με τις παρατηρήσεις πριν από την πρόταση, βλέπουμε ότι

$$x^n - 1 = f(x)g(x),$$

για κάποιο πολυώνυμο $g(x) \in \mathbb{Z}[x]$. Ας υποθέσουμε ότι $f(\omega^p) \neq 0$, για κάποιο πρώτο $p \nmid n$. Σημειώνουμε ότι το $g(x)$ είναι κανονικό πολυώνυμο, αφού τα $x^n - 1$ και $f(x)$ είναι κανονικά πολυώνυμα στο $\mathbb{Z}[x]$. Επίσης, σημειώνουμε ότι το ω^p είναι και αυτό πρωταρχική n-ρίζα της μονάδας. Επομένως

$$f(\omega^p)g(\omega^p) = (\omega^p)^n - 1 = 0.$$

Αφού $f(\omega^p) \neq 0$, έπεται ότι $g(\omega^p) = 0$ και άρα το ω είναι ρίζα του $g(x^p)$. Όμως, $f(x) = \mathrm{irr}_{(\mathbb{Q},\omega)}(x)$ και άρα

$$g(x^p) = f(x)h(x),$$

για κάποιο $h(x) \in \mathbb{Q}[x]$. Παρατηρούμε ότι $h(x) \in \mathbb{Z}[x]$, σύμφωνα με την Πρόταση 1.3.3. Θεωρούμε τώρα τον ομομορφισμό δακτυλίων της Πρότασης 1.3.9:

$$\Psi : \mathbb{Z}[x] \to \mathbb{Z}_p[x],\ a_0 + a_1x + \cdots + a_nx^n \mapsto \bar{a}_0 + \bar{a}_1x + \cdots + \bar{a}_nx^n\ .$$

Στον $\mathbb{Z}_p[x]$ ισχύει ότι

$$x^n - 1 = \Psi\left(f(x)\right)\Psi\left(g(x)\right)$$

και

$$\Psi\left(g(x^p)\right) = \Psi\left(f(x)\right)\Psi\left(h(x)\right). \tag{5.2.5.1}$$

Όμως, σύμφωνα με την Πρόταση III.4,

$$\Psi\left(g(x^p)\right) = \Psi\left(g(x)\right)^p$$

και επομένως

$$\Psi\left(g(x)\right)^p = \Psi\left(f(x)\right)\Psi\left(h(x)\right).$$

Αφού $\Psi\left(f(x)\right)$ διαιρεί το $\Psi\left(g(x)\right)^p$, κάθε ανάγωγος παράγοντας του $\Psi\left(f(x)\right)$ διαιρεί το $\Psi\left(g(x)\right)$ και άρα

$$\text{ΜΚΔ}\left(\Psi\left(f(x)\right), \Psi\left(g(x)\right)\right) \neq 1.$$

Έστω, λοιπόν, $q(x) \in \mathbb{Z}_p[x]$ ο μέγιστος κοινός διαιρέτης των $\Psi\left(f(x)\right)$ και $\Psi\left(g(x)\right)$. Τότε $\deg q(x) \geq 1$ και από τη σχέση (5.2.5.1), το $q(x)^2$ διαιρεί το $x^n - 1$. Επομένως το πολυώνυμο $x^n - 1$ του $\mathbb{Z}_p[x]$ έχει πολλαπλές ρίζες. Αυτό, όμως, είναι άτοπο αφού η παράγωγος του $x^n - 1$ είναι $nx^{n-1} \neq 0$ ($p \nmid n$) και $\text{ΜΚΔ}(x^n - 1, nx^{n-1}) = 1$ (Πρόταση 1.4.5). Καταλήξαμε σε άτοπο γιατί υποθέσαμε ότι $f(\omega^p) \neq 0$. Επομένως $f(\omega^p) = 0$ για κάθε p πρώτο, $p \not| n$. □

Στα Παραδείγματα 5.2.3 είδαμε ότι, για $n \leq 6$ και όταν n είναι πρώτος, το πολυώνυμο $\Phi_n(x)$ είναι ανάγωγο. Το επόμενο θεώρημα δείχνει ότι αυτή είναι ιδιότητα του $\Phi_n(x)$, για κάθε φυσικό αριθμό n.

Θεώρημα 5.2.6. *Έστω n ένας θετικός ακέραιος. Το κυκλοτομικό πολυώνυμο $\Phi_n(x)$ είναι ανάγωγο στον $\mathbb{Q}[x]$.*

Απόδειξη. Έστω ω πρωταρχική n-ρίζα της μονάδας και $f(x) = \text{irr}_{(\mathbb{Q},\omega)}(x)$. Το σύνολο U_n περιγράφεται ως εξής:

$$U_n = \{\omega^s : (s, n) = 1\}.$$

Έστω λοιπόν ω^s άλλη πρωταρχική ρίζα. Τότε $s = p_1 \cdots p_t$, όπου p_i είναι πρώτοι φυσικοί αριθμοί με την ιδιότητα $p_i \nmid n$, για $1 \leq i \leq t$. Παρατηρούμε ότι

$$\{\omega^{p_1},\ \omega^{p_1p_2} = (\omega^{p_1})^{p_2},\ \ldots,\ \omega^{p_1\cdots p_{s-1}},\ \omega^s\} \subset U_n.$$

Εφαρμόζοντας διαδοχικά την Πρόταση 5.2.5 για τα στοιχεία

$$\omega^{p_1},\ \omega^{p_1p_2} = (\omega^{p_1})^{p_2},\ \ldots,\ \omega^s = (\omega^{p_1\cdots p_{s-1}})^{p_s}$$

προκύπτει ότι $f(\omega^s) = 0$. Επομένως όλες οι πρωταρχικές n-ρίζες της μονάδας έχουν το ίδιο ανάγωγο πολυώνυμο πάνω από τον $\mathbb{Q}[x]$ και επομένως το $f(x)$ διαιρεί το $\Phi_n(x)$. Όμως, τα δύο πολυώνυμα $f(x)$,$\Phi_n(x)$ έχουν τον ίδιο βαθμό. Τέλος, αφού τα $f(x), \Phi_n(x)$ είναι κανονικά πολυώνυμα έπεται ότι $f(x) = \Phi_n(x)$. Άρα το $\Phi_n(x)$ είναι ανάγωγο στον $\mathbb{Q}[x]$. □

Ως άμεση συνέπεια της Πρότασης 5.2.2 και του Θεωρήματος 5.2.6, έχουμε το παρακάτω πόρισμα.

Πόρισμα 5.2.7. *Η ανάλυση του $x^n - 1$ σε γινόμενο ανάγωγων πολυωνύμων στον $\mathbb{Q}[x]$ είναι:*

$$x^n - 1 = \prod_{d \mid n} \Phi_d(x).$$

Ένα σώμα ανάλυσης L του $x^n - 1 \in K[x]$, όπου K είναι ένα σώμα με $\operatorname{char} K = 0$ και n ένας θετικός ακέραιος, λέγεται ***κυκλοτομικό σώμα τάξης*** n (cyclotomic field of order n πάνω από το K. Από το Θεώρημα 5.1.4, η ομάδα $\operatorname{Gal}(L/K)$ είναι αβελιανή, ως υποομάδα της $\mathbb{Z}_n^\sharp$. Τέτοιες επεκτάσεις λέγονται ***αβελιανές επεκτάσεις*** (abelian extensions).

Στην Αλγεβρική Θεωρία Αριθμών, όπου μελετώνται πεπερασμένες επεκτάσεις πάνω από το $\mathbb{Q}$, οι αβελιανές επεκτάσεις παίζουν σημαντικό ρόλο. Έτσι είναι εξαιρετικά ενδιαφέρον το ερώτημα, σχετικά με το αντίστροφο του Θεωρήματος 5.1.4 πάνω από το $\mathbb{Q}$. Κάθε πεπερασμένη επέκταση του Galois $L/\mathbb{Q}$ για την οποία η $\operatorname{Gal}(L/\mathbb{Q})$ είναι αβελιανή, δηλ. η $L/\mathbb{Q}$ είναι αβελιανή επέκταση, περιέχεται σε ένα κυκλοτομικό σώμα πάνω από το $\mathbb{Q}$;

Το ερώτημα αυτό απαντήθηκε θετικά από τους Kronecker (1853) και Weber (1886). Το συμπέρασμά τους αποτελεί ένα από τα βαθύτερα θεωρήματα της Αλγεβρικής Θεωρίας Αριθμών (βλ. [5]).

Θεώρημα 5.2.8 (Kronecker - Weber). *Αν $L/\mathbb{Q}$ είναι μία πεπερασμένη αβελιανή επέκταση, τότε υπάρχει μία ρίζα της μονάδας ω, τέτοια ώστε $L \subset \mathbb{Q}(\omega)$.*

Η επόμενη πρόταση γενικεύει το Παράδειγμα 5.1.3.3 και το Πόρισμα 5.1.5.

Θεώρημα 5.2.9. *Έστω $n > 0$ ένας φυσικός αριθμός και έστω E ένα κυκλοτομικό σώμα τάξης n πάνω από το $\mathbb{Q}$. Τότε $[E : \mathbb{Q}] = \phi(n)$ και $\operatorname{Gal}(E/\mathbb{Q}) \cong \mathbb{Z}_n^\sharp$.*

Απόδειξη. Η επέκταση $E/\mathbb{Q}$ είναι σώμα ανάλυσης του $x^n - 1$ πάνω από το $\mathbb{Q}$ και είναι επέκταση του Galois, αφού το $x^n - 1 \in \mathbb{Q}[x]$ είναι διαχωρίσιμο. Από το Θεώρημα 5.1.4, η $\operatorname{Gal}(E/\mathbb{Q})$ εμφυτεύεται στη $\mathbb{Z}_n^\sharp$. Αν ω είναι μία πρωταρχική ρίζα της μονάδας, τότε $E = \mathbb{Q}(\omega)$ και

$$[\mathbb{Q}(\omega) : \mathbb{Q}] = \deg \Phi_n(x) = \phi(n),$$

όπου ϕ είναι η συνάρτηση του Euler, αφού $\Phi_n(x) = \operatorname{irr}_{(\mathbb{Q},\omega)}(x)$, (βλ. Θεώρημα 5.2.6). Αφού η τάξη της $\mathbb{Z}_n^\sharp$ είναι ίση με $\phi(n)$, συμπεραίνουμε ότι $\operatorname{Gal}(E/\mathbb{Q}) \cong \mathbb{Z}_n^\sharp$. □

5.3 Το πολυώνυμο $x^n - a$

Έστω n ένας φυσικός ακέραιος και F ένα σώμα, έτσι ώστε $\operatorname{char} F \nmid n$. Έστω επίσης ότι το F περιέχει το ω, μία πρωταρχική n-ρίζα της μονάδας, και έστω το a ένα στοιχείο του F. Στην ενότητα αυτή θα εξετάσουμε το πολυώνυμο $f(x) = x^n - a \in F[x]$ και την ομάδα $G = \operatorname{Gal}(L/F)$, όπου L ένα σώμα ανάλυσης του $f(x)$ πάνω από το F.

Παρατηρούμε ότι αν b είναι μία ρίζα του $f(x)$, τότε οι ρίζες του $f(x)$ είναι οι

$$b, b\omega, \cdots, b\omega^{n-1}.$$

Επομένως $L = F(b)$. Αν σ είναι ένα στοιχείο της G, τότε $\sigma(b) = b\omega^i$, για κάποιο i, αφού το $\sigma(b)$ πρέπει να είναι ρίζα του $f(x)$. Έτσι το σ προσδιορίζεται από τον εκθέτη i. Θεωρούμε την αντιστοιχία

$$\psi : G \to \mathbb{Z}_n, \quad \sigma \mapsto \bar{i}\ .$$

Παρατηρούμε ότι αν

$$\sigma, \tau \in G \; \psi(\sigma) = \psi(\tau) \Rightarrow \sigma(b) = \tau(b) \Rightarrow \sigma = \tau,$$

δηλαδή η ψ είναι αμφιμονότιμη συνάρτηση. Είναι δε φανερό ότι η ψ είναι ομομορφισμός ομάδων. Άρα η G εμφυτεύεται στη $\mathbb{Z}_n$.

Έστω, τώρα, ότι το $f(x)$ είναι ανάγωγο στο $F[x]$. Τότε το $f(x)$ είναι το $\mathrm{irr}_{(F,b)}(x)$ και είναι διαχωρίσιμο, άρα L/F είναι επέκταση του Galois. Επομένως $|G| = [L : F] = \deg f(x) = n$. Άρα η G είναι ισόμορφη με τη $\mathbb{Z}_n$. Αντίστροφα αν η G είναι ισόμορφη με τη $\mathbb{Z}_n$ και ψ είναι επιμορφισμός, τότε η πρώτη παρατήρηση που κάνουμε είναι ότι όλες οι ρίζες του $f(x)$ είναι διακεκριμένες. Θα δείξουμε ότι $f(x)$ είναι ανάγωγο. Έστω, λοιπόν, ότι

$$f(x) = g(x)h(x), \quad g(x), h(x) \in F[x], \quad (g(x), h(x)) = 1.$$

Χωρίς περιορισμό της γενικότητας έστω ότι $g(b) = 0$ και $h(b\omega^i) = 0$, για κάποιο i. Αφού η ψ είναι επιμορφισμός, έπεται ότι υπάρχει $\sigma \in G$ έτσι ώστε $\sigma(b) = b\omega^i$. Αφού $g(b) = 0$, έπεται ότι $\mathrm{irr}_{(F,b)}(x)$ διαιρεί το $g(x)$ ενώ αντίστοιχα $\mathrm{irr}_{(F,\sigma(b))}(x)$ διαιρεί το $h(x)$. Σύμφωνα με την Πρόταση 2.3.2 προκύπτει ότι

$$\mathrm{irr}_{(F,\sigma(b))}(x) = \mathrm{irr}_{(F,b)}(x).$$

Άρα το $\mathrm{irr}_{(F,b)}(x)$ διαιρεί τον μέγιστο κοινό διαιρέτη $(g(x), h(x))$, το οποίο είναι αδύνατον. Αποδείξαμε, λοιπόν, ότι:

Θεώρημα 5.3.1. *Αν το σώμα F περιέχει μία πρωταρχική n-ρίζα της μονάδας και E είναι σώμα ανάλυσης του $f(x) = x^n - a \in F[x]$ τότε η $\mathrm{Gal}(E/F)$ εμφυτεύεται στη $(\mathbb{Z}_n, +)$. Η $\mathrm{Gal}(E/F)$ είναι ισόμορφη με τη $\mathbb{Z}_n$ αν και μόνο αν το $f(x)$ είναι ανάγωγο, δηλ. αν και μόνο αν $[E : F] = n$.*

Το θεώρημα αυτό μας οδηγεί στο επόμενο συμπέρασμα:

Πόρισμα 5.3.2. *Έστω p πρώτος φυσικός αριθμός, F ένα σώμα που περιέχει μία p-ρίζα της μονάδας και $a \in F$. Αν το $x^p - a$ δεν είναι ανάγωγο στο $F[x]$, τότε το $x^p - a$ αναλύεται σε γινόμενο γραμμικών παραγόντων στο $F[x]$.*

Απόδειξη. Έστω L σώμα ανάλυσης του $x^p - a$. Είδαμε ότι η ομάδα $\mathrm{Gal}(L/F)$ εμφυτεύεται στο $\mathbb{Z}_p$. Άρα υπάρχουν ακριβώς δύο περιπτώσεις. Η πρώτη είναι $\mathrm{Gal}(L/F) \cong \{\mathrm{id}_L\}$ και η δεύτερη είναι $\mathrm{Gal}(L/F) \cong \mathbb{Z}_p$. Παρατηρούμε ότι στην πρώτη περίπτωση

$$L^{\mathrm{Gal}(L/F)} = L.$$

Όμως η $L/\mathbb{Z}_p$ είναι επέκταση του Galois και σύμφωνα με το Θεμελιώδες Θεώρημα της Θεωρίας Galois,

$$L^{\mathrm{Gal}(L/F)} = F.$$

Επομένως, αν $\mathrm{Gal}(L/F) \cong \{\mathrm{id}_L\}$ τότε $L = F$ και επομένως το $x^p - a$ δεν είναι ανάγωγο στο $F[x]$ και αναλύεται σε γινόμενο γραμμικών παραγόντων στο $F[x]$. Σύμφωνα με το Θώρημα 5.3.1 η δεύτερη περίπτωση ισχύει ακριβώς όταν το $x^p - a$ είναι ανάγωγο. □

Παράδειγμα 5.3.3. Έστω E, υπόσωμα του $\mathbb{C}$, έτσι ώστε E να είναι το σώμα ανάλυσης του $f(x) = x^p - 2 \in \mathbb{Q}[x]$, όπου p είναι πρώτος φυσικός αριθμός. Σημειώνουμε ότι $E/\mathbb{Q}$ είναι επέκταση του Galois. Το $f(x) \in \mathbb{Q}[x]$ είναι ανάγωγο σύμφωνα με το κριτήριο του

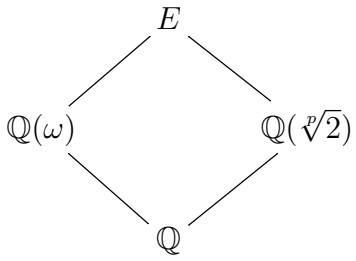
Eisenstein και $\mathrm{irr}_{(\mathbb{Q},\sqrt[p]{2})}(x) = x^p - 2$. Σημειώνουμε ότι $E/\mathbb{Q}$ είναι επέκταση του Galois. Οι ρίζες του $f(x)$ στο E είναι:

$$\sqrt[p]{2},\ \sqrt[p]{2}\omega, \dots\ , \sqrt[p]{2}\omega^{p-1},$$

όπου ω είναι μία πρωταρχική p-ρίζα της μονάδας. Άρα

$$E = \mathbb{Q}(\omega, \sqrt[p]{2}).$$

Από το ακόλουθο διάγραμμα των επεκτάσεων



Σχήμα 5.2: Σώμα ανάλυσης του $x^p - 2$ και υποσώματα.

παρατηρούμε ότι

$$[\mathbb{Q}(\omega) : \mathbb{Q}] = \deg \Phi(p) = \phi(p) = p - 1$$

και ότι

$$[\mathbb{Q}(\sqrt[p]{2}) : \mathbb{Q}] = \deg \mathrm{irr}_{(\mathbb{Q},\sqrt[p]{2})}(x) = p.$$

Άρα οι φυσικοί αριθμοί $p-1$ και p διαιρούν τον $[E : \mathbb{Q}]$ και αφού $(p, p-1) = 1$, έπεται ότι το γινόμενο $p(p-1)$ διαιρεί τον $[E : \mathbb{Q}]$ και επομένως $[E : \mathbb{Q}] \geq p(p-1)$. Επίσης,

$$[E : \mathbb{Q}] = [E : \mathbb{Q}(\omega)][\mathbb{Q}(\omega) : \mathbb{Q}]$$

και

$$[E : \mathbb{Q}(\omega)] = [\mathbb{Q}(\omega), \sqrt[p]{2}) : \mathbb{Q}(\omega)] \leq p,$$

αφού$\sqrt{2}$ είναι ρίζα του $x^p - 2 \in \mathbb{Q}[\omega]$. Από τις ανισότητες

$$p(p-1)\ \leq\ [E : \mathbb{Q}]\ \leq\ p\,[\mathbb{Q}(\omega) : \mathbb{Q}] = p(p-1),$$

έπεται ότι

$$[E : \mathbb{Q}] = p(p-1)$$

και ότι $[E : \mathbb{Q}(\omega)] = p$. Άρα το $f(x)$ είναι ανάγωγο πάνω από το $\mathbb{Q}(\omega)$. Από το Θεώρημα 5.3.1 προκύπτει ότι

$$\mathrm{Gal}\,(E/\mathbb{Q}(\omega)) \cong \mathbb{Z}_p,$$

ενώ από το Πόρισμα 5.1.5 προκύπτει ότι

$$\mathrm{Gal}\,(\mathbb{Q}(\omega) : \mathbb{Q}) \cong \mathbb{Z}_p^*.$$

Η επέκταση $\mathbb{Q}(\omega)/\mathbb{Q}$ είναι επέκταση του Galois και επομένως

$$\mathrm{Gal}\,(E/\mathbb{Q}(\omega)) \lhd \mathrm{Gal}(E/\mathbb{Q}).$$

Έστω σ, τ, τα στοιχεία της $\mathrm{Gal}(E/\mathbb{Q})$, όπως αυτά καθορίζονται από τη δράση τους στα στοιχεία $\sqrt[p]{2}$ και ω του E:

$$\begin{array}{lll} \sigma: & \sqrt[p]{2} \mapsto \sqrt[p]{2}\omega, & \omega \mapsto \omega \\ \tau: & \sqrt[p]{2} \mapsto \sqrt[p]{2}, & \omega \mapsto \omega^2. \end{array}$$

Εύκολα επιβεβαιώνει κανείς ότι $\sigma\tau \neq \tau\sigma$ και άρα η ομάδα $\mathrm{Gal}(E/\mathbb{Q})$ δεν είναι αβελιανή.

Ορισμός 5.3.4. *Μία επέκταση σωμάτων E/F λέγεται* ***κυκλική*** *(cyclic) αν E/F είναι επέκταση του Galois και αν η ομάδα $\mathrm{Gal}(E/F)$ είναι κυκλική.*

Παραδείγματα 5.3.5.

1. Έστω $E = \mathbb{Q}(\omega)$, όπου $\omega = e^{2\pi i/p}$, για κάποιον πρώτο φυσικό αριθμό p. Σύμφωνα με το Πόρισμα 5.1.5, η επέκταση $E/\mathbb{Q}$ είναι κυκλική.
2. Έστω $\omega = e^{\pi i/4}$ και $E = \mathbb{Q}(\omega)$. Η κυκλοτομική επέκταση $E/\mathbb{Q}$ δεν είναι κυκλική, βλ. Παράδειγμα 5.1.6.1.

Το επόμενο θεώρημα χαρακτηρίζει τις κυκλικές επεκτάσεις. Αν $a \in \mathbb{C}$, με $\sqrt[n]{a}$ συμβολίζουμε μία οποιαδήποτε ρίζα του πολυωνύμου $x^n - a$ στο $\mathbb{C}$.

Θεώρημα 5.3.6. *Έστω $F \subset \mathbb{C}$ ένα σώμα που περιέχει όλες τις n-ρίζες της μονάδας πάνω από το $\mathbb{Q}$. Μία επέκταση E/F είναι κυκλική βαθμού n αν και μόνο αν $E = F(\sqrt[n]{a})$, για κάποιο $a \in F$.*

Απόδειξη. Έστω ότι $E = F(\sqrt[n]{a})$, για κάποιο $a \in F$. Τότε η επέκταση E/F είναι κυκλική σύμφωνα με το Θεώρημα 5.3.1, αφού κάθε υποομάδα κυκλικής ομάδας είναι κυκλική.

Αντίστροφα, έστω ότι η επέκταση E/F είναι κυκλική βαθμού n και έστω ότι το σ παράγει την $\mathrm{Gal}(E/F)$, δηλ.

$$\mathrm{Gal}(E/F) = \langle\sigma\rangle = \{\mathrm{id}_E, \sigma, \ldots, \sigma^{n-1}\}.$$

Έστω ω μία πρωταρχική n-ρίζα της μονάδας. Τα στοιχεία της ομάδας $\mathrm{Gal}(E/F)$ είναι γραμμικά ανεξάρτητα πάνω από το σώμα E, βλ. Θεώρημα 3.4.2. Επομένως, ο γραμμικός συνδυασμός

$$h = \mathrm{id}_E + \omega\sigma + \cdots + \omega^{n-1}\sigma^{n-1}: \quad E \longrightarrow E$$

δεν είναι η μηδενική συνάρτηση στο E και υπάρχει ένα στοιχείο $b \in E$ τέτοιο ώστε $h(b) \neq 0$. Έστω $\gamma = h(b)$. Τότε

$$\gamma = b + \sigma(b)\omega + \cdots + \sigma^{n-1}(b)\omega^{n-1}. \tag{5.3.6.1}$$

και θεωρούμε την επέκταση $F(\gamma)/F$. Έτσι

$$F \subset F(\gamma) \subset E.$$

Παρατηρούμε ότι, αφού ο βαθμός της επέκτασης E/F είναι n, (δηλ. $[E : F] = n$), ο βαθμός της επέκτασης $F(\gamma)/F$ διαιρεί το n και άρα $[F(\gamma) : F] \leq n$. Θα αποδείξουμε ότι

$$[F(\gamma) : F] = n \text{ και } F(\gamma) = E.$$

Πράγματι,

$$\begin{aligned}\sigma(\gamma) &= \sigma(b) + \sigma^2(b)\omega + \cdots + \sigma^{n-1}(b)\omega^{n-2} + b\omega^{n-1} = \omega^{n-1}\gamma\\ \sigma^2(\gamma) &= \omega^{n-1}\sigma(\gamma) = \omega^{n-1}\omega^{n-1}\sigma(\gamma) = \omega^{n-2}\gamma\\ &\vdots\\ \sigma^{n-1}(\gamma) &= \omega\gamma.\end{aligned}$$

Άρα τα στοιχεία γ, $\sigma(\gamma), \ldots, \sigma^{n-1}(\gamma)$ είναι όλα διακεκριμένα. Σύμφωνα με την άσκηση 2.4.19, έπεται ότι $\deg \operatorname{irr}_{(F,\gamma)}(x) \geq n$ και επομένως $\deg \operatorname{irr}_{(F,\gamma)}(x) = n$. Άρα

$$n = \deg \operatorname{irr}_{(F,\gamma)}(x) = [F(\gamma) : F] \ \Rightarrow E = F(\gamma).$$

Μένει να δείξουμε ότι υπάρχει στοιχείο a στο F έτσι ώστε το γ να είναι ρίζα του πολυωνύμου $x^n - a \in F[x]$. Πράγματι, θέτουμε $a = \gamma^n$. Θα αποδείξουμε ότι $a \in F$. Παρατηρούμε ότι για $0 \leq i \leq n-1$,

$$\sigma^i(a) = \sigma^i(\gamma^n) = \big(\sigma^i(\gamma)\big)^n = \big(\omega^{n-i}\gamma\big)^n = \gamma^n = a.$$

Άρα $a \in E^{\mathrm{Gal}(E/F)}$. Όμως η E/F είναι επέκταση του Galois και σύμφωνα με το Θεμελιώδες Θεώρημα της Θεωρίας Galois, $E^{\mathrm{Gal}(E/F)} = F$. Άρα το $a \in F$ και το γ είναι ρίζες του $x^n - a \in F[x]$. Με άλλα λόγια, $E = F\,(\sqrt[n]{a})$ και αποδείχτηκε το αντίστροφο. □

Το στοιχείο γ λέγεται **επιλύουσα του Lagrange** (Lagrange's resolvent) για τα στοιχεία b, ω και σ.

5.4 Ασκήσεις

1. Να υπολογίσετε τα $\Phi_8(x)$ και $\Phi_9(x)$.

2. Να εξετάσετε αν το $x^{(p-1)p} + x^{(p-2)^p} + \cdots + x^{2p} + x^p + 1$ είναι ανάγωγο όταν ο p είναι πρώτος φυσικος αριθμός.

3. Έστω F ένα σώμα με $\operatorname{char} F = 0$, $a \in F$ και E το σώμα ανάλυσης του πολυωνύμου $x^n - a$, όπου n είναι φυσικός αριθμός. Αν ω είναι μία πρωταρχική n-ρίζα της μονάδας, να αποδείξετε ότι

   (α΄) η επέκταση $F(\omega)/F$ είναι επέκταση του Galois.
   (β΄) η σειρά $\mathrm{Gal}(E/E) \trianglelefteq \mathrm{Gal}(E/F(\omega)) \trianglelefteq \mathrm{Gal}(E/F)$ είναι επιλύσιμη.

4. Έστω E το σώμα ανάλυσης του $x^5 - 1$ πάνω από το $\mathbb{Z}_2$. Να βρείτε όλα τα ενδιάμεσα υποσώματα.

5. Έστω E το σώμα ανάλυσης του $x^5 - 1$ πάνω από το $\mathbb{Q}$. Να βρείτε όλα τα ενδιάμεσα υποσώματα.

6. Να αποδείξετε ότι για p πρώτο, $p > 2$,

$$\Phi_{2p}(x) = x^{p-1} - x^{p-2} + \cdots - x + 1.$$

7. Έστω E το κυκλοτομικό σώμα τάξης 12 πάνω από το $\mathbb{Q}$. Να βεθούν όλα τα ενδιάμεσα σώματα.

8. Έστω $n > 2$ ένας θετικός ακέραιος και ω μία πρωταρχική n-ρίζα της μονάδας πάνω από το $\mathbb{Q}$. Να αποδείξετε ότι

$$[\mathbb{Q}\left(\omega + \omega^{-1}\right) : \mathbb{Q}] = \frac{\phi(n)}{2}.$$

Βιβλιογραφία Κεφαλαίου 5

[1] Bastida, J. R. *Field Extensions and Galois Theory, Vol. 22*. Addison-Wesley, 2007.

[2] Gaal, L. *Classical Galois Theory with Examples*. Chelsea, 1988.

[3] Hadlock, C. R. *Field Theory and its Classical Problems*. MAA, 2000.

[4] Milne, J. S. *Fields and Galois Theory*. www.jmilne.org, 2014.

[5] Ribenhoim, P. *Algebraic Numbers*. Wiley-Interscience, New York, 1972.

[6] Rotman, J. *Θεωρία Galois*. Leader Books, 2000.

[7] Stewart, I. *Galois Theory*. Champan and Hall, 1973.

[8] Tignol, J. P. *Galois Theory of Algebraic Equations* . World Scientific, 2011.

Κεφάλαιο 6

Εφαρμογές

Στο Κεφάλαιο αυτό θα χρησιμοποιήσουμε τα εργαλεία της Θεωρίας Galois, για να απαντήσουμε σε ερωτήματα που θέσαμε στην αρχή του συγγράμματος. Έτσι, δοθέντος ενός πολυωνύμου, θα βρούμε ικανή και αναγκαία συνθήκη για να υπάρχει ακριβής τύπος για τις ρίζες του πολυωνύμου, δηλ. το Θεώρημα του Galois. Θα βρούμε επίσης ικανή και αναγκαία συνθήκη για να είναι κατασκευάσιμο κάποιο σημείο του πραγματικού επιπέδου. Τέλος, θα δώσουμε μία, κατά βάση αλγεβρική, απόδειξη του Θεμελιώδους Θεωρήματος της Άλγεβρας.

6.1 Επιλυσιμότητα με ριζικά

Στην Ενότητα 1.1.2 δώσαμε μία ιστορική αναφορά για την εύρεση των ριζών ενός πολυωνύμου με συντελεστές από το $\mathbb{Q}$. Είδαμε ότι υπάρχουν τύποι για την εύρεση ριζών όλων των πολυωνύμων του $\mathbb{Q}[x]$ με βαθμό ≤ 4. Είδαμε επίσης, ότι υπάρχουν πολυώνυμα βαθμού μεγαλύτερου του 4 που επιλύονται με ριζικά και οι ρίζες τους προκύπτουν από συνδυασμό πράξεων, όπως η πρόσθεση, ο πολλαπλασιασμός αλλά και εξαγωγή ριζικών στοιχείων του $\mathbb{Q}$. Στο εδάφιο αυτό θα αποδείξουμε το σημαντικό Θεώρημα του Galois, όπου δίνεται μία ικανή και αναγκαία συνθήκη για να είναι ένα πολυώνυμο επιλύσιμο με ριζικά.

Θα ξεκινήσουμε με τον ακριβή ορισμό της έκφρασης «*επιλύεται με ριζικά*», όπως προκύπτει από τη μελέτη των αλγεβρικών επεκτάσεων σωμάτων που έχουμε αναπτύξει.

Ορισμός 6.1.1. *Έστω $F \subset \mathbb{C}$ ένα σώμα και a ένα στοιχείο του $\mathbb{C}$ αλγεβρικό πάνω από το F. Θα λέμε ότι το στοιχείο a **εκφράζεται με ριζικά** (expressed with radicals) αν ανήκει σε ένα σώμα E τέτοιο ώστε να υπάρχει μία ακολουθία σωμάτων*

$$F = F_0 \subset F_1 \subset \cdots \subset F_i \subset F_{i+1} \subset \cdots \subset F_s = E, \tag{6.1.1.1}$$

για κάποιον φυσικό αριθμό s, όπου

$$F_{i+1} = F_i\left(\sqrt[n_i]{a_i}\right),$$

για κάποιο $a_i \in F_i$ και n_i φυσικό αριθμό, $0 \leq i \leq s-1$. Με $\sqrt[n_i]{a_i}$ συμβολίζουμε μία ρίζα του πολυωνύμου

$$x^{n_i} - a_i \in F_i[x].$$

Η ακολουθία (6.1.1.1) λέγεται ***ριζική ακολουθία*** (radical sequence) σωμάτων και η επέκταση E/F λέγεται ***ριζική επέκταση*** (radical extension). Ένα πολυώνυμο $f(x) \in$

$F[x]$ λέγεται ***επιλύσιμο με ριζικά*** (resolved by radicals) πάνω από το F, αν κάθε ρίζα του εκφράζεται με ριζικά, δηλ. αν υπάρχει μία ριζική επέκταση που περιέχει το σώμα ανάλυσης του $f(x)$ πάνω από το F.

Παραδείγματα 6.1.2.

1. Αν ω είναι μία n-ρίζα της μονάδας, τότε το ω εκφράζεται με ριζικά πάνω από το $\mathbb{Q}$, ως ρίζα του πολυωνύμου $x^n - 1 \in \mathbb{Q}[x]$, σύμφωνα με τη ριζική ακολουθία σωμάτων $\mathbb{Q} \subsetneq \mathbb{Q}(\omega)$.
2. Έστω $a = 1 + \sqrt{2} + \sqrt{1+\sqrt{2}}$ και $b = 1 + \sqrt{2}$. Θεωρούμε την ακολουθία

$$\mathbb{Q} \subsetneq \mathbb{Q}\left(\sqrt{2}\right) \subsetneq F_1(\sqrt{b}).$$

   Η ακολουθία αυτή είναι ριζική. Πράγματι, έστω $F_1 = \mathbb{Q}\left(\sqrt{2}\right)$ και $F_2 = F_1(\sqrt{b})$. Τότε

   - το $\sqrt{2}$ είναι ρίζα του $x^2 - 2 \in \mathbb{Q}[x]$,
   - το $\sqrt{b}$ είναι ρίζα του $x^2 - (1+\sqrt{2}) \in F_1[x]$,
   - το $a \in F_2$.

   Επομένως, το a εκφράζεται με ριζικά πάνω από το $\mathbb{Q}$. Ο αναγνώστης καλείται να αποδείξει ότι η F_2/F_1 είναι γνήσια επέκταση του F_1, (βλ. άσκηση 6.4.1).
3. Έστω $F \subset \mathbb{C}$ ένα σώμα που περιέχει όλες τις n-ρίζες της μονάδας, δηλ. τις ρίζες του $x^n - 1 \in F[x]$. Αν $a \in F$, τότε το πολυώνυμο $f(x) = x^n - a \in F[x]$ είναι επιλύσιμο με ριζικά, με ριζική ακολουθία την

$$F \subset F\left(\sqrt[n]{a}\right).$$

4. Η επέκταση $\mathbb{Q} \subset \mathbb{Q}\left(\sqrt[3]{2}\right)$ είναι ριζική, αλλά όχι επέκταση του Galois.
5. Έστω $f(x) = x^3 + q(x) + r \in \mathbb{Q}[x]$. Οι ρίζες του $f(x)$ δίνονται από τους τύπους $y+z, \omega y + \omega_3^2 z, \omega^2 y + \omega z$, όπου

$$\omega = e^{2\pi i/3},$$

$$y = \left(\frac{1}{2}\left(-r + \sqrt{r^2 + \frac{4q^3}{27}}\right)\right)^{\frac{1}{3}}$$

   και

$$z = \left(\frac{1}{2}\left(-r - \sqrt{r^2 + \frac{4q^3}{27}}\right)\right)^{\frac{1}{3}},$$

   βλ. Ενότητα V του Παραρτήματος. Παρατηρούμε ότι οι ρίζες του $f(x)$ εκφράζονται με τη βοήθεια των πράξεων της πρόσθεσης και του πολλαπλασιασμού και με την εξαγωγή ριζών δευτέρου και τρίτου βαθμού. Το σώμα $L = \mathbb{Q}(y+z, \omega y + \omega^2 z, \omega^2 y + \omega z)$ είναι σώμα ανάλυσης του $f(x)$. Θέτουμε $b = r^2 + 4q^3/27$ και θεωρούμε τα στοιχεία

$$\alpha_1 = e^{2\pi i/6},\ \alpha_2 = \sqrt{b},\ \alpha_3 = y,\ a_4 = z$$

και τα αντίστοιχα σώματα

$$B_1 = \mathbb{Q}(\alpha_1),\ B_2 = B_1(\alpha_2),\ B_3 = B_2(\alpha_3),\ B_4 = B_3(\alpha_4).$$

Είναι φανερό ότι $L \subset B_4$ αφού $w = \alpha_1^2 \in B_4$ και όλες οι ρίζες του $f(x)$ ανήκουν στο B_4. Η ακολουθία

$$\mathbb{Q} \subsetneq B_1 \subset B_2 \subset B_3 \subset B_4 \tag{6.1.2.1}$$

είναι ριζική αφού

$$b \in B_1,\ \ \alpha_3^3 = \frac{-r+\alpha_2}{2} \in B_2,\ \ \alpha_4^3 = \frac{-r-\alpha_2}{2} \in B_4$$

και

- α_1 είναι ρίζα του $x^{12} - 1 \in \mathbb{Q}[x]$,
- α_2 είναι ρίζα του $x^2 - b \in B_1[x]$,
- α_3 είναι ρίζα του $x^3 - \alpha_3^3 \in B_2[x]$,
- α_4 είναι ρίζα του $x^3 - \alpha_4^3 \in B_3[x]$.

Επομένως, το πολυώνυμο $f(x)$ επιλύεται με ριζικά. Σημειώνουμε ότι αφού $\omega \in B_1$, οι 3 ρίζες του $x^3 - \alpha_3^3$, δηλ. οι $a_3, \omega a_3$, $\omega^2 a_3$ ανήκουν στο B_3. Επομένως το B_3 είναι το σώμα ανάλυσης του πολυωνύμου $x^3 - \alpha_3^3 \in B_2[x]$.

Το επόμενο θεώρημα οφείλεται στον Galois και δίνει ικανή και αναγκαία συνθήκη για να είναι το πολυώνυμο $f(x)$ είναι επιλύσιμο με ριζικά. Παραπέμπουμε στο Παράρτημα Ι για τους σχετικούς ορισμούς και τα αναγκαία θεωρήματα από τη Θεωρία Ομάδων.

Θεώρημα 6.1.3 (Θεώρημα του Galois). *Έστω $F \subset \mathbb{C}$ ένα σώμα, $f(x) \in F[x]$ με σώμα ανάλυσης το L. Το πολυώνυμο $f(x)$ είναι επιλύσιμο με ριζικά πάνω από το $\mathbb{Q}$ αν και μόνο αν η ομάδα $\mathrm{Gal}(L/F)$ είναι επιλύσιμη.*

Απόδειξη. Έστω $G = \mathrm{Gal}(L/F)$ και έστω ότι το πολυώνυμο $f(x) \in F[x]$ είναι επιλύσιμο με ριζικά. Τότε υπάρχει μία ριζική επέκταση E/F, τέτοια ώστε το σώμα ανάλυσης L του $f(x)$ να περιέχεται στο E. Εφόσον η επέκταση E/F είναι ριζική, υπάρχει μία ριζική ακολουθία

$$F = F_0 \subset F_1 \subset \cdots \subset F_s = E, \tag{6.1.3.1}$$

για κάποιον φυσικό αριθμό s, όπου για $1 \leq i \leq s$, $F_i = F_{i-1}(\sqrt[n_i]{a_i})$, τα $a_i \in F_{i-1}$ και οι n_i είναι φυσικοί αριθμοί. Όμως, η επέκταση E/F μπορεί να μην είναι επέκταση του Galois. Για να εφαρμόσουμε τα εργαλεία της Θεωρίας Galois, θα θεωρήσουμε μία νέα ριζική ακολουθία (βλ. την ακολουθία (6.1.3.2)), που καταλήγει σε επέκταση του Galois. Έστω λοιπόν

$$n = \text{ΕΚΠ}(n_1, \ldots, n_s) \text{ και } \omega = e^{2\pi i/n}.$$

Επίσης, θέτουμε

$$F_i' = F_i(\omega),\ \text{για } 0 \leq i \leq s,$$

και θεωρούμε τη παρακάτω ακολουθία σωμάτων, με μήκος κατά ένα μεγαλύτερο της ακολουθίας (6.1.3.1):

$$F \subset F_0' \subset F_1' \cdots \subset F_s'. \tag{6.1.3.2}$$

Αφού,

- ω είναι ρίζα του $x^n - 1 \in F[x]$,
- $F'_i = F'_i(\sqrt[n_i]{a_i})$ και $a_i \in F'_{i-1}$, για $1 \leq i \leq s$,

έπεται ότι και η ακολουθία (6.1.3.2) είναι ριζική. Παρατηρούμε, τώρα, ότι F'_0/F είναι επέκταση του Galois ως σώμα ανάλυσης του διαχωρίσιμου πολυωνύμου $x^n - 1 \in F[x]$. Επίσης, η επέκταση F'_i/F'_{i-1} είναι επέκταση του Galois, για $0 \leq i \leq s$, ως σώμα ανάλυσης του πολυωνύμου

$$x^{n_i} - a_i \in F'_{i-1}[x].$$

Έστω, λοιπόν, $E' = F'_s$, $V = \mathrm{Gal}(E'/F)$ και $V_i = \mathrm{Gal}(E'/F'_i)$, για $0 \leq i \leq s$. Τότε $V_i \trianglerighteq V_{i+1}$ και $V_i/V_{i+1} \hookrightarrow \mathrm{Gal}(F'_{i+1}/F'_i)$, για $0 \leq i \leq s$. (βλ. Θεώρημα 3.3.2). Θεωρούμε την κανονική σειρά υποομάδων της V:

$$V \trianglerighteq V_0 \trianglerighteq \cdots \trianglerighteq V_{s-1} \trianglerighteq V_s = \{e\}. \tag{6.1.3.3}$$

Παρατηρούμε ότι για $0 \leq i \leq s$, η ομάδα πηλίκον V_i/V_{i+1} είναι αβελιανή, ως υποομάδα της κυκλικής ομάδας $\mathrm{Gal}\left(F'_i(\sqrt[n_i]{a_i})/F'_i\right)$ (βλ. Θεώρημα 5.3.6). Επίσης,

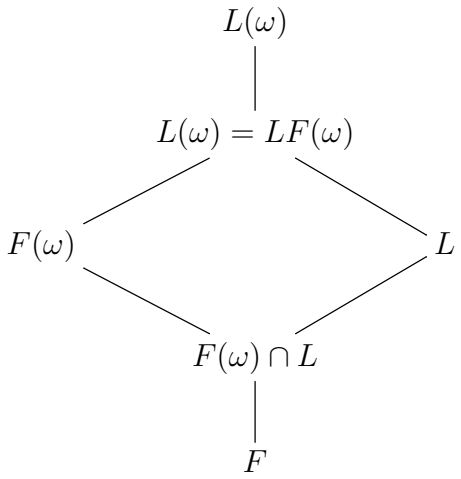
$$V/V_0 \cong \mathrm{Gal}(F'_0/F) = \mathrm{Gal}(F(\omega)/F)$$

είναι αβελιανή ομάδα, σύμφωνα με το Θεώρημα 5.1.4. Επομένως η κανονική σειρά (6.1.3.3) είναι επιλύσιμη και άρα η ομάδα V είναι επιλύσιμη. Αφού

$$G = \mathrm{Gal}(L/F) \cong \mathrm{Gal}(E'/F)/\mathrm{Gal}(E'/L),$$

έπεται ότι η G είναι επιλύσιμη ομάδα, σύμφωνα με το Θεώρημα Ι.29.

Αντίστροφα, ας υποθέσουμε ότι η $G = \mathrm{Gal}(L/F)$ είναι επιλύσιμη. Θεωρούμε μία πρωταρχική m-ρίζα της μονάδας ω, όπου $m = |G|$. Παρατηρούμε ότι, αφού $F \subset L$, το μικρότερο σώμα που περιέχει τα σώματα L και $F(\omega)$ ταυτόχρονα, δηλ. το $LF(\omega)$, είναι το σώμα $L(\omega)$. Έτσι, έχουμε το διάγραμμα σωμάτων που απεικονίζεται στο Σχήμα 6.1.



Σχήμα 6.1: Διάγραμμα υποσωμάτων του $L(\omega)$

Η επέκταση $L(\omega)/L$ είναι επέκταση του Galois, αφού είναι σώμα ανάλυσης του διαχωρισίμου πολυωνύμου $x^m - 1 \in L[x]$. Επίσης, $L(\omega)/F(\omega)$ είναι επέκταση του Galois, αφού είναι σώμα ανάλυσης του $f(x) \in F(\omega)$, βλ. άσκηση 3.7.13. Σύμφωνα με το Θεώρημα 3.5.3, έπεται ότι

$$\mathrm{Gal}\left(L(\omega)/F(\omega)\right) \cong \mathrm{Gal}\left(L/(F(\omega) \cap L)\right).$$

Έστω $H = \mathrm{Gal}\,(L(\omega)/F(\omega))$. Ο παραπάνω ισομορφισμός δείχνει ότι η H είναι ισόμορφη με υποομάδα της G. Επειδή η ομάδα G είναι επιλύσιμη, έπεται ότι και η H είναι επιλύσιμη και υπάρχει μία κανονική σειρά από υποομάδες της H, με κυκλικούς παράγοντες τάξης πρώτου αριθμού (Θεώρημα I.29):

$$H = H_0 \rhd H_1 \rhd \cdots \rhd H_r = \{e\},$$

όπου $|H_i/H_{i+1}| = p_i$, για κάποιον πρώτο φυσικό αριθμό p_i, $0 \leq i \leq r$. Παρατηρούμε ότι ο p_i διαιρεί την τάξη της H, για $0 \leq i \leq r$, όπως μπορεί εύκολα να αποδειχθεί με επαγωγή στο r και με το Θεώρημα του Lagrange. Επομένως, ο p_i διαιρεί την τάξη της G, δηλ. $p_i|m$, για $0 \leq i \leq r$. Στη συνέχεια, θεωρούμε το σώμα

$$E_i = L(\omega)^{H_i},\ 0 \leq i \leq r.$$

Αφού H_i είναι υποομάδα της $\mathrm{Gal}\,(L(\omega)/F(\omega))$, το σώμα E_i είναι ενδιάμεσο σώμα της επέκτασης $L(\omega)/F(\omega)$ και έτσι προκύπτει η παρακάτω ακολουθία σωμάτων

$$F(\omega) = E_0 \subset E_1 \subset \cdots \subset E_r = L(\omega). \tag{6.1.3.4}$$

Σύμφωνα με το Θεμελιώδες Θεώρημα της Θεωρίας Galois και χρησιμοποιώντας την ιδιότητα (ii), παρατηρούμε ότι

$$H_i = \mathrm{Gal}(L(\omega)/E_i), \quad \text{για } 0 \leq i \leq r.$$

Από το Θεμελιώδες Θεώρημα της Θεωρίας Galois και χρησιμοποιώντας την ιδιότητα (iii), συμπεραίνουμε ότι E_i/E_{i-1} είναι επέκταση Galois, αφού $H_i \rhd H_{i+1}$, για $1 \leq i \leq r$, ενώ

$$\mathrm{Gal}(E_i/E_{i-1}) \cong H_{i-1}/H_i \cong (\mathbb{Z}_{p_i}, +).$$

Αφού ω είναι πρωταρχική m-ρίζα της μονάδας και ανήκει σε κάθε E_i και $p_i \mid m$, για $0 \leq i \leq r$, είναι φανερό ότι το E_i περιέχει όλες τις p_i-ρίζες της μονάδας. Αφού E_i/E_{i-1} είναι κυκλική για $1 \leq i \leq r$, από το Θεώρημα 5.3.6 προκύπτει ότι υπάρχει $a_i \in E_{i-1}$, τέτοιο ώστε

$$E_i = E_{i-1}\,(\sqrt[p_i]{a_i})\,.$$

Άρα η ακολουθία σωμάτων

$$F \subset F(\omega) = E_0 \subset E_1 \subset \cdots \subset E_r = L(\omega)$$

είναι μία ριζική ακολουθία, δηλ. η $L(\omega)/F$ είναι μία ριζική επέκταση, η οποία περιέχει το σώμα ανάλυσης L του $f(x) \in F[x]$. Άρα το $f(x)$ είναι επιλύσιμο με ριζικά. □

Παράδειγμα 6.1.4. Έστω $f(x) = x^5 - 4x + 2 \in \mathbb{Q}[x]$ και έστω E το σώμα ανάλυσης του $f(x)$ πάνω από το $\mathbb{Q}$. Στο Παράδειγμα 3.2.6 αποδείξαμε ότι $\mathrm{Gal}(E/\mathbb{Q}) \cong S_5$. Αφού η G δεν είναι επιλύσιμη (βλ. Θεώρημα I.35) το $f(x)$ δεν είναι επιλύσιμο με ριζικά.

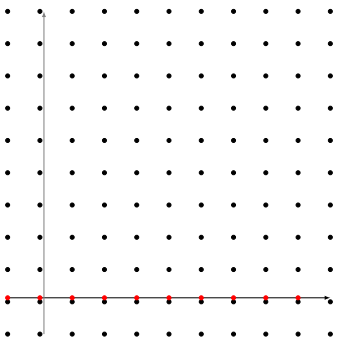
Στο [6, 4.5] αναφέρεται ένας αλγόριθμος επίλυσης ενός πολυωνύμου επιλύσιμου με ριζικά. Επίσης στο [6,4.9] δίνεται η μέθοδος του Lagrange για τον υπολογισμό της ομάδας του Galois ενός ανάγωγου πολυωνύμου χωρίς τον υπολογισμό των ριζών του πολυωνύμου και με τη χρήση της επιλύουσας του Lagrange.

6.2 Κατασκευάσιμοι αριθμοί και πολύγωνα

Στην Ενότητα 1.1.3, εισάγαμε το θέμα των κατασκευών με κανόνα και διαβήτη. Ένα σημείο του επιπέδου είναι ***κατασκευάσιμο*** (constructible) αν προκύπτει ως σημείο τομής κατασκευάσιμων ευθειών και κύκλων. Θυμίζουμε ότι για να είναι μία ευθεία κατασκευάσιμη, είναι αναγκαίο να έχουν προσδιοριστεί δύο κατασκευάσιμα σημεία επί της ευθείας, ενώ για να είναι ένας κύκλος κατασκευάσιμος, είναι αναγκαίο το κέντρο και η ακτίνα του κύκλου να είναι κατασκευάσιμα. Αν ταυτίσουμε την αρχική κατασκευάσιμη ευθεία με την ευθεία των πραγματικών αριθμών, το ζήτημα που τίθεται είναι ο προσδιορισμός των πραγματικών αριθμών που είναι κατασκευάσιμοι. Στην Ενότητα 1.1.3, είδαμε ότι αν F είναι το σύνολο των κατασκευάσιμων αριθμών, τότε το F είναι υπόσωμα του $\mathbb{R}$. Αυτόματα, λοιπόν, το F περιέχει ως πρώτο σώμα τους ρητούς. Είδαμε επίσης ότι αν $a \in \mathbb{R}$ και $a^2 \in \mathbb{Q}$, τότε $a \in F$. Έτσι είναι φανερό ότι

$$\mathbb{Q} \subsetneq F \subset \mathbb{R}$$

και ότι ο βαθμός $[F : \mathbb{Q}] = \infty$, βλ. άσκηση 6.4.4. Ποιοι πραγματικοί αριθμοί είναι, λοιπόν, κατασκευάσιμοι; Η κατασκευή κατασκευάσιμων σημείων γίνεται με τη χρήση εργαλείων με αναφορά στο επίπεδο (τον κανόνα και τον διαβήτη). Για να μπορέσουμε να απαντήσουμε στο παραπάνω ερώτημα, θα εισάγουμε την έννοια του ***πλέγματος του*** K (lattice of K), δηλ. το σύνολο $K \times K$, για κάθε ενδιάμεσο σώμα της επέκτασης $F/\mathbb{Q}$. Γεωμετρικά, για κάθε τέτοιο σώμα K, τοποθετούμε το πλέγμα του K εντός του $\mathbb{R}^2$. Έτσι, αν το $k \in K$, το στοιχείο $(k, 0)$ εμφανίζεται με κόκκινο στο σχήμα 6.2.



Σχήμα 6.2: Το πλέγμα του K στο $\mathbb{R}^2$.

Σημειώνουμε ότι τα στοιχεία του K είναι κατασκευάσιμοι αριθμοί. Είναι εύκολο να συμπεράνει κανείς ότι τα *σημεία* του πλέγματος του K είναι κατασκευάσιμα. Θα λέμε ότι μία ευθεία είναι κατασκευάσιμη εντός του K αν περνά από δύο σημεία του πλέγματος του K. Θα λέμε ότι ένας κύκλος είναι κατασκευάσιμος εντός του K αν το κέντρο του είναι στο πλέγμα του K και η ακτίνα του είναι στο K. Θα λέμε ότι ένα σημείο κατασκευάζεται από το K σε ένα βήμα, αν το σημείο προκύπτει ως σημείο τομής είτε δύο ευθειών κατασκευάσιμες εντός του K, είτε μίας ευθείας και ενός κύκλου κατασκευάσιμων εντός του K, είτε δύο κύκλων κατασκευάσιμων εντός του K. Αφήνουμε την απόδειξη των προτάσεων της επόμενης παρατήρησης ως εύκολη άσκηση για τον αναγνώστη, βλ. άσκηση 6.4.5.

Παρατήρηση 6.2.1. Έστω ότι K είναι ενδιάμεσο σώμα της επέκτασης $F/\mathbb{Q}$, όπου F το υπόσωμα των κατασκευάσιμων αριθμών στο $\mathbb{R}$.

i) Αν $c \in F$, τότε τα στοιχεία του $K(c)$ είναι και αυτά στο F.

ii) Αν l είναι μία κατασκευάσιμη ευθεία εντός του K, τότε η εξίσωση της ευθείας είναι της μορφής $ax + by + c = 0$, όπου $a, b, c \in K$.

iii) Αν C είναι ένας κύκλος κατασκευάσιμος εντός του K, τότε η εξίσωση του C είναι της μορφής $x^2 + y^2 + ax + by + c = 0$ όπου $a, b, c \in K$.

Έστω, λοιπόν, ότι K είναι ενδιάμεσο σώμα της επέκτασης $F/\mathbb{Q}$, όπου F το υπόσωμα των κατασκευάσιμων αριθμών στο $\mathbb{R}$. Είναι φανερό ότι η τομή δύο ευθειών με συντελεστές από το K θα δώσει σημείο που ήδη βρίσκεται στο πλέγμα του K. Επίσης είναι εύκολο να δει κανείς ότι το πρόβλημα εύρεσης σημείου τομής δύο κύκλων ανάγεται στο πρόβλημα εύρεσης τομής ενός κύκλου και μίας ευθείας, βλ. άσκηση 6.4.6. Έτσι, για να βρούμε σημεία κατασκευάσιμα από το K εκτός του πλέγματος του K αρκεί να επικεντρωθούμε σε σημεία τομής μίας ευθείας και ενός κύκλου με συντελεστές από το K.

Λήμμα 6.2.2. *Έστω K υπόσωμα του $\mathbb{R}$. Αν $l : \ ax + by + c = 0$ είναι μία ευθεία στο $\mathbb{R}^2$, όπου $a, b, c \in K$ και $C : \ x^2 + y^2 + dx + ey + f = 0$ είναι ένας κύκλος στο $\mathbb{R}^2$, όπου $d, e, f \in K$, έτσι ώστε l, C να έχουν σημεία τομής στο $\mathbb{R}^2$, τότε υπάρχει $q \in \mathbb{R}$ τέτοιος ώστε τα σημεία τομής των l και C να ανήκουν στο πλέγμα του $K(q)$.*

Απόδειξη. Έστω ότι $a \neq 0$. Λύνοντας την εξίσωση της l ως προς το a και αντικαθιστώντας στην εξίσωση του C προκύπτει μία εξίσωση δευτέρου βαθμού ως προς το y με συντελεστές από το K. Η τετραγωνική ρίζα της διακρίνουσας είναι το ζητούμενο q. Σημειώνουμε, ότι αφού l, C τέμνονται, η διακρίνουσα είναι θετική και $q \in \mathbb{R}$. Αν $a = 0$, κάνουμε το αντίστοιχο λύνοντας ως προς y. □

Είναι φανερό ότι αν ένα σημείο στο επίπεδο είναι κατασκευάσιμο, τότε το σημείο τομής της ευθείας που περνά από αυτό το σημείο και είναι κάθετη στην πραγματική ευθεία είναι κατασκευάσιμο, βλ. άσκηση 1.5.1. Διαδοχική, λοιπόν, εφαρμογή του παραπάνω Λήμματος οδηγεί στο εξής συμπέρασμα:

Θεώρημα 6.2.3. *Το $c \in \mathbb{R}$ είναι κατασκευάσιμο αν και μόνο αν υπάρχει μία ακολουθία σωμάτων*

$$\mathbb{Q} = K_0 \subset K_1 \cdots \subset K_t$$

έτσι ώστε $c \in K_t$ και $[K_{i+1} : K_i] = 2$, $i = 1, \ldots, t-1$.

Απόδειξη. Οι παρατηρήσεις πριν την εκφώνηση του Θεωρήματος 6.2.3, δείχνουν ότι η συνθήκη είναι αναγκαία. Για την αντίστροφη κατεύθυνση, θα δείξουμε ότι αν K είναι ενδιάμεσο σώμα της επέκτασης $F/\mathbb{Q}$, όπου F το υπόσωμα των κατασκευάσιμων αριθμών στο $\mathbb{R}$ και L/K είναι μία επέκταση με $[L : K] = 2$, τότε $L \subset F$. Πράγματι, έστω a ένα στοιχείο του L που δεν ανήκει στο K. Τότε $K(a) = L$ και $\deg \mathrm{irr}_{(K,a)}(x) = 2$. Έστω ότι

$$f(x) = \mathrm{irr}_{(K,a)}(x) = x^2 + bx + c.$$

Οι ρίζες του $f(x)$, και επομένως και το a, προκύπτουν από τον τύπο

$$\frac{-b \pm \sqrt{b^2 - 4ac}}{2}. \tag{6.2.3.1}$$

Αφού $b^2 - 4c \in K$, έπεται ότι $\sqrt{b^2 - 4c} \in F$ (βλ. άσκηση 1.5.2). Αφού το F είναι σώμα, από τον τύπο (6.2.3.1) συμπεραίνουμε ότι $a \in F$. Αποδείξαμε, λοιπόν, ότι αν K είναι ενδιάμεσο σώμα της επέκτασης $F/\mathbb{Q}$, όπου F το υπόσωμα των κατασκευάσιμων αριθμών

στο $\mathbb{R}$ και L/K είναι μία επέκταση με $[L : K] = 2$, τότε $L \subset F$. Έστω, λοιπόν, ότι υπάρχει μία ακολουθία σωμάτων

$$\mathbb{Q} = K_0 \subset K_1 \cdots \subset K_t$$

έτσι ώστε $c \in K_t$ και $[K_{i+1} : K_i] = 2$, $i = 1, \ldots, t-1$. Εφαρμόζοντας διαδοχικά το προηγούμενο βήμα προκύπτει ότι το c είναι κατασκευάσιμο. □

Το παρακάτω συμπέρασμα προκύπτει άμεσα από το Θεώρημα 6.2.3.

Πόρισμα 6.2.4. *Αν το $c \in \mathbb{R}$ είναι κατασκευάσιμο, τότε το c είναι αλγεβρικό στοιχείο πάνω από το $\mathbb{Q}$ και $\deg \operatorname{irr}_{(\mathbb{Q},c)}(x) = 2^n$, για $n \in \mathbb{N}_{\geq 0}$.*

Απόδειξη. Έστω ότι το c είναι κατασκευάσιμο και έστω $K_0, \ldots, K_t$, όπως στο Θεώρημα 6.2.3. Αφού $[K_t : \mathbb{Q}] = 2^t$, έπεται ότι ο βαθμός $[\mathbb{Q}(c) : \mathbb{Q}]$ διαιρεί το 2^t. Επομένως, αφού $\deg \operatorname{irr}_{\mathbb{Q},c}(x) = [\mathbb{Q}(c) : \mathbb{Q}]$, έπεται ότι ο βαθμός του ανάγωγου πολυωνύμου του c πάνω από το $\mathbb{Q}$ είναι μία δύναμη του 2. □

Παράδειγμα 6.2.5. Το $a = \sqrt[3]{5}$ δεν είναι κατασκευάσιμο, αφού $\operatorname{irr}_{(\mathbb{Q},a)}(x) = x^3 - 5$.

Σημειώνουμε, ότι η συνθήκη του Πορίσματος 6.2.4 είναι αναγκαία αλλά δεν είναι ικανή για να είναι το $c \in \mathbb{R}$ κατασκευάσιμο. Έτσι, το Πόρισμα 6.2.4 δεν είναι ισοδύναμο με το Θεώρημα 6.2.3. Σύμφωνα με την άσκηση 6.4.7, για να είναι το c κατασκευάσιμο, είναι απαραίτητο ο βαθμός της επέκτασης $L/\mathbb{Q}$ πάνω από το $\mathbb{Q}$ να είναι δύναμη του 2, όπου L το σώμα ανάλυσης του ανάγωγου πολυωνύμου του c πάνω από το $\mathbb{Q}$.

Παράδειγμα 6.2.6. Έστω $f(x) = x^4 + 2x - 2 \in \mathbb{Q}[x]$. Το $f(x)$ είναι ανάγωγο πάνω από το $\mathbb{Q}$ και δεν είναι δύσκολο να δει κανείς ότι το $f(x)$ έχει τουλάχιστον δύο πραγματικές ρίζες. Έστω b μία πραγματική ρίζα του $f(x)$ στο σώμα ανάλυσης L του $f(x)$ πάνω από το $\mathbb{Q}$. Μπορεί να δείξει κανείς, ότι το 3 διαιρεί την ομάδα $\operatorname{Gal}(L/Q)$ και επομένως, σύμφωνα με την άσκηση 6.4.7, το b δεν είναι κατασκευάσιμο (βλ. άσκηση 6.4.8).

Στη συνέχεια θα δώσουμε απαντήσεις στα άλυτα γεωμετρικά προβλήματα της αρχαιότητας.

Πόρισμα 6.2.7. *Μία γωνία 60° δεν μπορεί να τριχοτομηθεί με κανόνα και διαβήτη.*

Απόδειξη. Έστω ότι ήταν δυνατόν να τριχοτομηθεί η γωνία των 60°. Τότε θα ήταν δυνατόν να κατασκευασθεί ένα ορθογώνιο τρίγωνο με γωνίες 20° και 70°. Επομένως θα ήταν δυνατόν να κατασκευασθεί και ο πραγματικός αριθμός $\cos(20)$ ως πηλίκο δύο κατασκευάσιμων αριθμών, βλ. άσκηση 1.5.3. Έστω $a = \cos(20)$. Από τους τριγωνομετρικούς τύπους γνωρίζουμε ότι

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

Αφού $\cos(60^\circ) = 1/2$, συμπεραίνουμε ότι το a είναι ρίζα του πολυωνύμου $8x^3 - 6x - 1$. Το πολυώνυμο αυτό δεν έχει ρίζες στο $\mathbb{Q}$ και είναι ανάγωγο στο $\mathbb{Q}[x]$. Επομένως,

$$\operatorname{irr}_{(\mathbb{Q},a)}(x) = x^3 - \frac{3}{4}x - \frac{1}{8},$$

και $[\mathbb{Q}(a)) : \mathbb{Q}] = 3$. Επομένως το $\cos(20^\circ)$ δεν είναι κατασκευάσιμος αριθμός και ότι η γωνία 60° δεν μπορεί να τριχοτομηθεί με κανόνα και διαβήτη. □

Πόρισμα 6.2.8. *Δεν είναι δυνατόν να διπλασιασθεί ένας κύβος με κανόνα και διαβήτη.*

Απόδειξη. Έστω κύβος με πλευρά 1. Ο νέος κύβος (διπλάσιο σε όγκο) έχει πλευρά μήκους $a = \sqrt[3]{2}$. Το ανάγωγο πολυώνυμο του a είναι $x^3 - 2$ και $[\mathbb{Q}(a) : \mathbb{Q}] = 3$. Άρα το a δεν είναι κατασκευάσιμος αριθμός και ο κύβος δεν μπορεί να διπλασιαστεί με κανόνα και διαβήτη. □

Πόρισμα 6.2.9. *Δεν είναι δυνατόν να τετραγωνίσουμε τον κύκλο.*

Απόδειξη. Έστω κύκλος με ακτίνα 1. Εάν ήταν δυνατό να κατασκευάσουμε ένα τετράγωνο με εμβαδό π, τότε η ακμή του τετραγώνου θα είχε μήκος $\sqrt{\pi}$. Όμως, ο π και κατά συνέπεια και ο $\sqrt{\pi}$ δεν είναι αλγεβρικοί αριθμοί πάνω από το $\mathbb{Q}$. Επομένως ο $\sqrt{\pi}$ δεν είναι κατασκευάσιμος και είναι αδύνατον να τετραγωνίσουμε τον κύκλο με κανόνα και διαβήτη. □

Θα εξετάσουμε τώρα ποιά κανονικά p-γωνα είναι κατασκευάσιμα, όταν p είναι περιττός πρώτος αριθμός. Παρατηρούμε ότι ένα κανονικό n-γωνο είναι κατασκευάσιμο αν και μόνο αν η γωνία $2\pi i/n$ είναι κατασκευάσιμη (άσκηση 1.5.4). Έστω $\omega = 2^{\pi i/n}$. Το σώμα $L = \mathbb{Q}(\omega)$ είναι σώμα ανάλυσης του διαχωρίσιμου πολυωνύμου $x^n - 1$. Επομένως, από την άσκηση 6.4.10 προκύπτει το επόμενο συμπέρασμα.

Πρόταση 6.2.10. *Το κανονικό n-γωνο είναι κατασκευάσιμο αν και μόνο αν $[\mathbb{Q}(\omega) : \mathbb{Q}] = 2^s$, όπου $\omega = 2^{\pi i/n}$.*

Το επόμενο θεώρημα φέρει το όνομα του Gauss.

Θεώρημα 6.2.11 (Gauss). *Αν p είναι περιττός πρώτος, τότε το κανονικό p-γωνο είναι κατασκευάσιμο αν και μόνο αν*

$$p = 2^{2^m} + 1,\ m \in \mathbb{N}.$$

Απόδειξη. Έστω p περιττός πρώτος, $\omega = e^{2\pi i/p}$ και έστω ότι το κανονικό p-γωνο είναι κατασκευάσιμο. Τότε σύμφωνα με την Πρόταση 6.2.10, ο βαθμός $[\mathbb{Q}(\omega) : \mathbb{Q}]$ είναι δύναμη του 2. Αφού

$$\mathrm{irr}_{(\mathbb{Q},\omega)} = x^{p-1} + \cdots + x + 1,$$

έπεται ότι $p - 1 = 2^s$, για κάποιο $s \in \mathbb{N}_{\geq 0}$. Θα πρέπει τότε και το s να είναι δύναμη του 2. Πράγματι, αν υπάρχει περιττός αριθμός k τέτοιος ώστε $s = k\lambda$, τότε ο αριθμός

$$p = 2^s + 1 = (2^\lambda)^k + 1$$

έχει ως παράγοντα το $2^\lambda + 1$, αδύνατον αφού p πρώτος. Άρα $p - 1 = 2^{2^m}$, για κάποιο $m \geq 0$.

Για την αντίστροφη κατεύθυνση έστω ότι

$$p = 2^{2^m} + 1,\ m \in \mathbb{N}.$$

Επομένως

$$|\operatorname{Gal}(\mathbb{Q}(\omega)/\mathbb{Q})| = p - 1 = 2^{2^m},$$

και σύμφωνα με την Πρόταση 6.2.10, το κανονικό p-γωνο είναι κατασκευάσιμο. □

Οι πρώτοι αριθμοί της μορφής $2^{2^m} + 1$ λέγονται ***πρώτοι αριθμοί του Fermat*** (Fermat's prime). Αναφέρουμε χωρίς απόδειξη το θεώρημα που αφορά την περίπτωση του κανονικού n-γώνου. Για την απόδειξη παραπέμπουμε στο [5, Theorem 1.1.6].

Θεώρημα 6.2.12 (Θεώρημα των Gauss-Wentzel). *Ένα κανονικό n-γωνο είναι κατασκευάσιμο αν και μόνο αν*

$$n = 2^s p_1 \cdots p_r,$$

για κάποιον φυσικό s, όπου $p_1, \ldots, p_r$ είναι διακεκριμένοι πρώτοι αριθμοί του Fermat.

6.3 Θεμελιώδες Θεώρημα της Άλγεβρας

Στην Ενότητα 1.1.1 παρουσιάσαμε κάποια ιστορικά στοιχεία για το Θεμελιώδες Θεώρημα της Άλγεβρας. Το Θεμελιώδες Θεώρημα της Άλγεβας εγγυάται ότι κάθε πολυώνυμο με μιγαδικούς συντελεστές έχει μία ρίζα στο $\mathbb{C}$. Ειδικότερα, από το Θεμελιώδες Θεώρημα της Άλγεβας προκύπτει ότι αν $f(x) \in \mathbb{R}[x]$, τότε $f(x)$ έχει μία ρίζα στο $\mathbb{C}$ και κατά συνέπεια το σώμα ανάλυσης του πολυωνύμου εμφυτεύεται στο $\mathbb{C}$. Ισοδύναμα, όπως θα δούμε κατά τη διάρκεια της απόδειξης του Θεμελιώδους Θεωρήματος της Άλγεβρας, η ύπαρξη μιγαδικής ρίζας για πολυώνυμα με πραγματικούς συντελεστές, συνεπάγεται την ύπαρξη μιγαδικής ρίζας για πολυώνυμα με μιγαδικούς συντελεστές.

Η απόδειξη που δίνουμε σε αυτήν την ενότητα για το Θεμελιώδες Θεώρημα της Άλγεβρας έχει κυρίως αλγεβρικό χαρακτήρα. Βέβαια, ο μαθηματικός ορισμός του συνόλου των πραγματικών αριθμών χρησιμοποιεί τη γλώσσα της Μαθηματικής Ανάλυσης για την έννοια της πληρότητας. Έτσι ένα θεώρημα, που θεμελιωδώς αφορά το $\mathbb{R}$, είναι αδύνατον να μην χρησιμοποιεί με κάποιο τρόπο αναλυτικά εργαλεία. Η απόδειξη που δίνουμε χρησιμοποιεί από τη Μαθηματική Ανάλυση το Θεώρημα της Μέσης Τιμής (Θ.Μ.Τ) (Mean Value Theorem) για πολυώνυμα με πραγματικούς συντελεστές. Ο κύριος όμως κορμός της παρούσας σύντομης (σχετικά) απόδειξης του Θεμελιώδους Θεωρήματος της Άλγεβρας στηρίζεται στην αντιστοιχία, ανάμεσα στις υποομάδες μίας ομάδας Galois και τα ενδιάμεσα σώματα και χρειάζεται από τη Θεωρία Ομάδων, το Θεώρημα Ι.24. Για την πληρότητα της παρουσίασης, υπενθυμίζουμε το βασικό Θεώρημα της Μέσης Τιμής, που βασίζεται στην πληρότητα του συνόλου των πραγματικών αριθμών και στην έννοια της συνέχειας.

Θεώρημα Μέσης Τιμής (Θ.Μ.Τ.) *Έστω $f(x) \in \mathbb{R}[x]$. Εάν υπάρχουν $a, b \in \mathbb{R}$ έτσι ώστε $f(a) > 0$ και $f(b) < 0$, τότε υπάρχει $c \in \mathbb{R}$ έτσι ώστε $f(c) = 0$.*

Σημειώνουμε τις παρακάτω συνέπειες του Θ.Μ.Τ.:

Πρόταση 6.3.1. *Έστω $a \in \mathbb{R}^+$. Τότε υπάρχει $r \in \mathbb{R}^+$ έτσι ώστε $r^2 = a$.*

Απόδειξη. Έστω $f(x) = x^2 - a \in \mathbb{R}[x]$. Τότε $f(1+a) = 1 + a^2 + a$, άρα $f(1+a) > 0$. Ακόμη $f(0) = -a < 0$. Από το Θ.Μ.Τ. έπεται ότι υπάρχει c έτσι ώστε $f(c) = 0$. Παρατηρούμε ότι οι ρίζες του $f(x)$ είναι οι $\pm c$. Έτσι επιλέγουμε για r τη θετική ρίζα του $f(x)$. □

Συμβολίζουμε τον θετικό πραγματικό αριθμό r της προηγούμενης πρότασης με $\sqrt{a}$. Στη συνέχεια θεωρούμε τους μιγαδικούς αριθμούς. Οι μόνες παραδοχές που κάνουμε για τα στοιχεία του $\mathbb{C}$ είναι ότι

$$\mathbb{C} = \{a + bi : \ a, b \in \mathbb{R}, \ i^2 = -1\}$$

και ότι κάθε μιγαδικός αριθμός $z \in \mathbb{C}$ μπορεί να γραφεί στη μορφή $re^{i\theta}$ όπου $r \in \mathbb{R}^+$. Δεν γνωρίζουμε a priori ότι ο μιγαδικός z έχει τετραγωνική ρίζα στο $\mathbb{C}$, δηλ. ότι υπάρχει κάποιο $w \in \mathbb{C}$, τέτοιο ώστε $w^2 = \mathbb{C}$. Αυτό, λοιπόν, διευκρινίζεται με την επόμενη πρόταση.

Πρόταση 6.3.2. *Έστω $z \in C$. Τότε υπάρχει $w \in \mathbb{C}$, τέτοιο ώστε $w^2 \in \mathbb{C}$.*

Απόδειξη. Έστω ότι $z = re^{i\theta}$, όπου $r \in \mathbb{R}^+$. Σύμφωνα με την Πρόταση 6.3.1, υπάρχει $\sqrt{r} \in \mathbb{R}^+$ και άρα $w = \sqrt{r}e^{i\theta/2} \in \mathbb{C}$ και $w^2 = z$. □

Συμβολίζουμε με $\sqrt{z}$ το w της προηγούμενης πρότασης. Το επόμενο αποτέλεσμα αφορά την ύπαρξη ριζών (στο $\mathbb{C}$) για πολυώνυμα του $\mathbb{C}[x]$ δεύτερου βαθμού.

Πρόταση 6.3.3. *Έστω $f(x) = z_1x^2 + z_2x + z_3 \in \mathbb{C}[x]$, $\deg f(x) = 2$. Υπάρχει $\alpha \in \mathbb{C}$, τέτοιο ώστε $f(\alpha) = 0$. Επομένως, δεν υπάρχει ανάγωγο πολυώνυμο στο $\mathbb{C}[x]$ βαθμού 2.*

Απόδειξη. Θα χρησιμοποιήσουμε τον γνωστό τύπο της δευτεροβάθμιας εξίσωσης. Από την Πρόταση 6.3.2 υπάρχει μιγαδικός αριθμός $\sqrt{z_2^2 - 4z_1z_3}$. Εύκολα επιβεβαιώνει κανείς ότι οι μιγαδικοί αριθμοί

$$\frac{-z_2 \pm \sqrt{z_2^2 - 4z_1z_3}}{2z_1},$$

είναι ρίζες του $f(x)$. □

Πρόταση 6.3.4. *Το σώμα $\mathbb{C}$ δεν έχει επέκταση βαθμού 2.*

Απόδειξη. Έστω $[E : \mathbb{C}] = 2$. Τότε υπάρχει $a \in E \setminus \mathbb{C}$ και αναγκαστικά $E = \mathbb{C}(a)$. Επομένως $\deg \mathrm{irr}_{\mathbb{C},a}(x) = 2$. Προκύπτει άτοπο από την Πρόταση 6.3.3. □

Πρόταση 6.3.5. *Έστω $f(x) \in \mathbb{R}[x]$ ανάγωγο κανονικό πολυώνυμο. Τότε $\deg f(x) = 2k$.*

Απόδειξη. Αρκεί να αποδείξουμε ότι αν $f(x) \in \mathbb{R}[x]$ και $\deg f(x)$ είναι περιττός ακέραιος, τότε το $f(x)$ έχει τουλάχιστον μία ρίζα στον $\mathbb{R}$. Έστω, λοιπόν, ότι

$$f(x) = a_0 + a_1x + \cdots + x^n \in \mathbb{R}[x], \text{ όπου } n = 2k + 1.$$

Θέτουμε

$$t = 1 + \sum_{i=0}^{i=n-1} |a_i| > 0.$$

Τότε

$$t - 1 = \sum_{i=0}^{i=n-1} |a_i|, \text{ άρα } |a_i| \leq t - 1, \text{ για } i = 0, \ldots, n-1.$$

Επομένως,

$$|a_0 + \cdots + a_{n-1}t^{n-1}| \leq |a_0| + \cdots + |a_{n-1}|\, t^{n-1} \leq (t-1) + \cdots + (t-1)t^{n-1} = \\ = (t-1)(1 + t + \cdots + t^{n-1}) = t^n - 1 < t^n.$$

Δηλαδή

$$\left|\sum_{i=0}^{n-1} a_it^i\right| < t^n, \text{ άρα } -t^n < a_0 + a_1t + \cdots + a_{n-1}t^{n-1} < t^n.$$

Επομένως,

$$0 < (a_0 + a_1t + \cdots + a_{n-1}t^{n-1}) + t^n = f(t).$$

Παρατηρούμε επίσης ότι

$$\left|\sum_{i=0}^{n-1} a_i(-t)^i\right| \leq |a_0|t + |a_1|t + \cdots + |a_{n-1}|t^{n-1}$$

και με τους ίδιους συλλογισμούς όπως προηγουμένως, οδηγούμαστε στις ανισότητες

$$-t^n \leq a_0 - a_1t + \cdots - a_{n-2}t^{n-2} + a_{n-1}t^{n-1} \leq t^n.$$

Αφού $n = 2k + 1$, έπεται ότι $(-t)^n = (-1)t^n$ και άρα

$$f(-t) = a_0 - a_1t + \cdots - a_{n-2}t^{n-2} + a_{n-1}t^{n-1} - t^n < 0.$$

Δείξαμε ότι αν $n = 2k + 1$, τότε $f(t) > 0$, ενώ $f(-t) < 0$. Σύμφωνα με το Θ.Μ.Τ. το $f(x)$ έχει μία πραγματική ρίζα. □

Πρόταση 6.3.6. *Έστω $L/\mathbb{R}$ μία πεπερασμένη επέκταση σωμάτων έτσι ώστε $\mathbb{R} \neq L$. Τότε $[L : \mathbb{R}] = 2n$*

Απόδειξη. Έστω $a \in L$, αλλά όχι στον $\mathbb{R}$. Από την Πρόταση 6.3.5, ο βαθμός του $\mathrm{irr}_{(\mathbb{R},a)}(x)$ πρέπει να είναι άρτιος. Επομένως

$$[L : \mathbb{R}] = [L : \mathbb{R}(a)][\mathbb{R}(a) : \mathbb{R}]$$

είναι άρτιος. □

Δίνουμε έμφαση στα συμπεράσματα των Προτάσεων 6.3.4, 6.3.6. Έχουμε δείξει ως τώρα ότι δεν υπάρχει επέκταση L του $\mathbb{C}$ έτσι ώστε $[L : \mathbb{C}] = 2$, ενώ έχουμε επίσης δείξει ότι κάθε πεπερασμένη επέκταση του $\mathbb{R}$ πρέπει να είναι άρτιου βαθμού. Είμαστε έτοιμοι για την απόδειξη του κύριου θεωρήματος αυτής της ενότητας.

Θεώρημα 6.3.7 (Θεμελιώδες Θεώρημα της Άλγεβρας). *Κάθε μη σταθερό πολυώνυμο του $\mathbb{C}[x]$ έχει μία μιγαδική ρίζα.*

Απόδειξη. Έστω $f(x) = \sum a_i x^i \in \mathbb{C}[x]$. Με $\overline{f(x)}$ συμβολίζουμε το πολυώνυμο $\sum \overline{a_i} x^i$, όπου $\overline{a}$ είναι ο συζυγής του $a \in \mathbb{C}$. Παρατηρούμε ότι

$$\overline{f(x)\overline{f(x)}} = f(x)\overline{f(x)}$$

και άρα $f(x)\overline{f(x)} \in \mathbb{R}[x]$. Ακόμη παρατηρούμε ότι

$$f(z) = 0 \Leftrightarrow \overline{f(\overline{z})} = 0 \ .$$

Άρα το $f(x)$ έχει μιγαδική ρίζα αν και μόνο αν $f(x)\overline{f(x)} \in \mathbb{R}[x]$ έχει μιγαδική ρίζα. Αρκεί, λοιπόν, να αποδείξουμε ότι το θεώρημα ισχύει για πολυώνυμα με πραγματικούς συντελεστές. Αφού κάθε πολυώνυμο γράφεται μοναδικά ως γινόμενο αναγώγων, αρκεί να αποδείξουμε το θεώρημα για ανάγωγα πολυώνυμα του $\mathbb{R}[x]$.

Έστω, λοιπόν, $p(x) \in \mathbb{R}[x]$ ανάγωγο πολυώνυμο. Θα θεωρήσουμε το πολυώνυμο

$$q(x) = (x^2 + 1)p(x) \in \mathbb{C}[x].$$

Έστω L το σώμα ανάλυσης του $q(x)$ πάνω από το $\mathbb{C}$ (Θεώρημα 2.2.10). Θα δείξουμε ότι $L = \mathbb{C}$ και άρα το πολυώνυμο $q(x)$ και κατά συνέπεια το $p(x)$ αναλύεται σε γινόμενο γραμμικών παραγόντων στο $\mathbb{C}[x]$. Για να επιτύχουμε το στόχο μας, θα μελετήσουμε το βαθμό της επέκτασης $[L : \mathbb{C}]$ επιζητώντας να δείξουμε ότι είναι ίσος με 1. Θα χρησιμοποιήσουμε το Θεμελιώδες Θεώρημα της Θεωρίας Galois, μελετώντας την ομάδα $\mathrm{Gal}(L/\mathbb{R})$ καθώς και την υποομάδα $\mathrm{Gal}(L/\mathbb{C})$. Πρώτα θα δείξουμε ότι η ομάδα $\mathrm{Gal}(L/\mathbb{R})$ έχει τάξη μία δύναμη του 2 και στη συνέχεια θα δείξουμε ότι $\mathrm{Gal}(L/\mathbb{C})$ είναι η τετριμμένη υποομάδα της $\mathrm{Gal}(L/\mathbb{R})$.

Αφού το L έχει χαρακτηριστική 0, το πολυώνυμο $q(x)$ είναι διαχωρίσιμο και το L είναι επέκταση Galois πάνω από το $\mathbb{C}$ και το $\mathbb{R}$. Έστω $G = \mathrm{Gal}(L/\mathbb{R})$ και έστω ότι $|G| = 2^m k$, όπου $(2, k) = 1$. Σύμφωνα με το Θεώρημα I.24 υπάρχει μία υποομάδα H της G έτσι ώστε $|H| = 2^m$ και άρα $[G : H] = k$. Σύμφωνα με το Θεμελιώδες Θεώρημα της Θεωρίας Galois έπεται ότι $[L^H : \mathbb{R}] = k$, ενώ $(2, k) = 1$. Αν το k δεν είναι 1, αν δηλ. $L^H \neq k$, τότε οδηγούμαστε σε άτοπο, από την Πρόταση 6.3.6. Επομένως $k = 1$, $L^H = \mathbb{R}$ και $G = H$, ενώ $|G| = 2^m$.

Κάθε υποομάδα της G, λοιπόν, έχει τάξη μία δύναμη του 2. Έστω

$$V = \mathrm{Gal}(L/\mathbb{C}) < G.$$

Τότε $|V| = 2^n$, για κάποιο $n \geq 0$. Αν $n > 0$, τότε από το Θεώρημα I.24 η ομάδα V έχει μία υποομάδα J έτσι ώστε $|J| = 2^{n-1}$. Επομένως $[V : J] = 2$. Σύμφωνα πάλι με το Θεμελιώδες Θεώρημα της Θεωρίας Galois, έπεται ότι $[L^J : \mathbb{C}] = 2$. Αυτό, όμως, είναι άτοπο από την Πρόταση 6.3.4. Άρα $n = 0$, δηλ. $|V| = |\mathrm{Gal}(L/\mathbb{C})| = 1$. Επομένως $[L : \mathbb{C}] = 1$, $L = \mathbb{C}$ και το σώμα ανάλυσης του $q(x)$ πάνω από το $\mathbb{C}$ είναι το $\mathbb{C}$. Άρα κάθε πολυώνυμο $f(x) \in \mathbb{C}[x]$ έχει μία ρίζα στο $\mathbb{C}$. □

6.4 Ασκήσεις

1. Έστω $b = 1 + \sqrt{2}$, $F_1 = \mathbb{Q}\left(\sqrt{2}\right)$ και $F_2 = F_1(\sqrt{b})$. Να εξετάσετε αν F_2/F_1 είναι γνήσια επέκταση του F_1 και να βρείτε τον βαθμό $[F_2 : F_1]$. Να εξετάσετε αν η $F_2/\mathbb{Q}$ είναι επέκταση του Galois. Στη συνέχεια να βρείτε τον βαθμό $[F_2 : \mathbb{Q}]$ και να περιγράψετε την ομάδα $\mathrm{Gal}(F_2/\mathbb{Q})$.

2. Να βρείτε μία ριζική επέκταση που να περιέχει το σώμα ανάλυσης του $x^4 - 2$.

3. Έστω $f(x) = x^4 + 2x^2 + 2x + 2$. Να βρείτε μία ριζική επέκταση που να περιέχει το σώμα ανάλυσης του $f(x)$.

4. Να αποδείξετε ότι αν F είναι το σώμα των κατασκευάσιμων αριθμών, τότε $F/\mathbb{Q}$ είναι άπειρη επέκταση.

5. Έστω ότι το K είναι ενδιάμεσο σώμα της επέκτασης $F/\mathbb{Q}$, όπου F το υπόσωμα των κατασκευάσιμων αριθμών στο $\mathbb{R}$. Να αποδείξετε ότι

   i) Αν $c \in F$, τότε τα στοιχεία του $K(c)$ είναι και αυτά στο F.
   ii) Αν l είναι μία κατασκευάσιμη ευθεία εντός του K, τότε η εξίσωση της ευθείας είναι της μορφής $ax + by + c = 0$, όπου $a, b, c \in K$.
   iii) Αν C είναι ένας κύκλος, κατασκευάσιμος εντός του K, τότε η εξίσωση του C είναι της μορφής $x^2 + y^2 + ax + by + c = 0$, όπου $a, b, c \in K$.

6. Να αποδείξετε ότι το πρόβλημα εύρεσης σημείου τομής δύο κύκλων ανάγεται στο πρόβλημα εύρεσης τομής ενός κύκλου και μίας ευθείας.

7. Έστω $c \in \mathbb{R}$ αλγεβρικό πάνω από το $\mathbb{Q}$, $f(x) = \mathrm{irr}_{(\mathbb{Q},c)}(x)$ και έστω L το σώμα ανάλυσης του $f(x)$ πάνω από το $\mathbb{Q}$. Να αποδείξετε ότι αν $[L : \mathbb{Q}] = 2^n$, για κάποιον φυσικό αριθμό n, τότε κάθε στοιχείο του L είναι κατασκευάσιμο.

8. Έστω $f(x) = x^4 + 2x - 2 \in \mathbb{Q}[x]$. Να αποδείξετε ότι το $f(x)$ είναι ανάγωγο και ότι έχει τουλάχιστον μία πραγματική ρίζα b. Στη συνέχεια, αν L είναι το σώμα ανάλυσης του $f(x)$ πάνω από το $\mathbb{Q}$ να δείξετε ότι το 3 διαιρεί την ομάδα $\mathrm{Gal}(L/Q)$. Να συμπεράνετε ότι το b δεν είναι κατασκευάσιμο.

9. Να αποδείξετε ότι το σημείο $(\cos(2\pi/5), \sin(2\pi/5))$ είναι κατασκευάσιμο.

10. Να αποδείξετε ότι το σημείο $(a, b) \in \mathbb{R}^2$ είναι κατασκευάσιμο αν και μόνο αν το $z = a + bi$ περιέχεται σε μία επέκταση Galois $L/\mathbb{Q}$ τέτοια ώστε η ομάδα $\mathrm{Gal}(L/\mathbb{Q})$ να έχει τάξη κάποια δύναμη του 2.

Βιβλιογραφία Κεφαλαίου 6

[1] Alekseev, V. B. *Abel's Theorem in Problems and Solutions, (based on the lectures of Prof. V.I. Arnold)*. Kluwer Academic Publishers, 2004.

[2] Bastida, J. R. *Field Extensions and Galois Theory, Vol. 22*. Addison-Wesley, 2007.

[3] Edwards, H. M. *Galois Theory*. Springer, 1984.

[4] Escofier, J. P. *Galois Theory*. Springer, 2001.

[5] Fox, D. *Galois Theory*. John Wiley & Sons, 2012.

[6] Gaal, L. *Classical Galois Theory with Examples*. Chelsea, 1988.

[7] Hadlock, C. R. *Field Theory and its Classical Problems*. MAA, 2000.

[8] Milne, J. S. *Fields and Galois Theory*. www.jmilne.org, 2014.

[9] Rotman, J. *Θεωρία Galois*. Leader Books, 2000.

[10] Stewart, I. *Galois Theory*. Champan and Hall, 1973.

[11] Swallow, J. *Exploratory Galois Theory*. Cambridge University Press, 2004.

[12] Tignol, J. P. *Galois Theory of Algebraic Equations*. World Scientific, 2011.

Κεφάλαιο 7

Απλές επεκτάσεις και Αλγεβρικές Θήκες

Στο κεφάλαιο αυτό εξετάζουμε τις απλές επεκτάσεις σωμάτων και τις συγκρίνουμε με τις επεκτάσεις Galois . Επίσης εξετάζουμε τις αλγεβρικά κλειστές επεκτάσεις και τις συγκρίνουμε με το σώμα των μιγαδικών αριθμών.

7.1 Απλές επεκτάσεις

Στην ενότητα αυτή θα εξετάσουμε ποιες επεκτάσεις σωμάτων είναι απλές. Έστω F ένα πεπερασμένο σώμα με $\operatorname{char} F = p$ και E/F μία επέκταση του Galois. Αφού $[E : F] < \infty$, έπεται ότι το E είναι πεπερασμένο σώμα. Σύμφωνα με το Πόρισμα 4.2.4 υπάρχει $a \in E$, τέτοιο ώστε $E = \mathrm{GF}(p)(a)$. Αφού

$$E = \mathrm{GF}(p)(a) \subseteq F(a) \subseteq E,$$

συμπεραίνουμε ότι $E = F(a)$. Δείξαμε λοιπόν ότι κάθε επέκταση του Galois E/F είναι απλή επέκταση, όταν $\operatorname{char} F = p$ και $|E| < \infty$. Θα δούμε ότι το αντίστοιχο ισχύει για επεκτάσεις Galois E/F, όταν η χαρακτηριστική του F είναι μηδέν.

Θεώρημα 7.1.1. *Έστω ότι E/F είναι επέκταση του Galois με $\operatorname{char} F = 0$. Τότε υπάρχει $a \in E$ έτσι ώστε $E = F(a)$.*

Απόδειξη. Αν το $E = F$, το συμπέρασμα είναι προφανές. Έστω, λοιπόν, ότι $E \neq F$. Αφού $[E : F] < \infty$, σύμφωνα με την άσκηση 2.4.10, υπάρχουν $b_1, \ldots, b_n$ έτσι ώστε $E = F(b_1, \ldots, b_n)$. Με απλή επαγωγή στο n, βλέπουμε ότι αρκεί να αποδείξουμε ότι E είναι απλή επέκταση του F στην περίπτωση που το $E = F(b, c)$ και το $c \notin F(b)$, δηλ. όταν

$$F(b) \subsetneqq F(b, c) = E. \tag{7.1.1.1}$$

Σύμφωνα με την άσκηση 3.7.12, τα πολυώνυμα $\operatorname{irr}_{(F,b)}(x)$ και $\operatorname{irr}_{(F,c)}(x)$ αναλύονται σε γινόμενα γραμμικών παραγόντων στο $E[x]$. Αφού $\operatorname{char} F = 0$, τα ανάγωγα πολυώνυμα του $F[x]$ είναι διαχωρίσιμα. Έστω $b_1, \ldots, b_n \in E$ οι ρίζες του $\operatorname{irr}_{(F,b)}(x)$ στο E, παίρνοντας ως b_1 το b, και όπου $n = \deg \operatorname{irr}_{(F,b)}(x)$. Αντίστοιχα, έστω και $c_1, \ldots, c_m \in E$ οι ρίζες του $\operatorname{irr}_{(F,c)}(x)$ στο E με $c_1 = c$, όπου $m = \deg \operatorname{irr}_{(F,c)}(x)$. Στη συνέχεια, θεωρούμε το παρακάτω (πεπερασμένο) υποσύνολο του E:

$$\left\{ \frac{b_i - b}{c - c_j} : \ 1 < i \leq n, 1 < j \leq m \right\} \subset E \ .$$

Αφού το F είναι άπειρο, υπάρχει κάποιο στοιχείο του F, διάφορο του μηδενός, που να μην ανήκει στο παραπάνω σύνολο, έστω d. Έτσι,

$$d \neq \frac{b_i - b}{c - c_j}, \text{ άρα } d(c - c_j) \neq b_i - b \text{ και επομένως } (b + dc) \neq (b_i + dc_j), \qquad (7.1.1.2)$$

όπου $1 < i \leq n$ και $1 < j \leq m$. Έστω τώρα το στοιχείο $a = b + dc$. Το a ανήκει βέβαια στο E. Αν $a \in F$ τότε

$$c = \frac{a - b}{d} \in F(b),$$

άτοπο, αφού είμαστε στην περίπτωση της (7.1.1.1). Επομένως $a \notin F$. Επίσης, από τη σχέση (7.1.1.2) προκύπτει ότι, για $1 < i \leq n$ και $1 < j \leq m$,

$$a \neq b_i + dc_j \ . \qquad (7.1.1.3)$$

Θα δείξουμε ότι $F(a) = E$. Έστω

$$h(x) = \mathrm{irr}_{(F,b)}(a - dx) \in F(a)[x].$$

Παρατηρούμε ότι το c είναι κοινή ρίζα των $h(x)$ και $\mathrm{irr}_{(F,c)}(x)$, ενώ δεν υπάρχει άλλη κοινή ρίζα αυτών των πολυωνύμων. Πράγματι,

$$h(c) = \mathrm{irr}_{(F,b)}(a - dc) = \mathrm{irr}_{(F,b)}(b) = 0.$$

Αν, τώρα, c_j ήταν ρίζα του $h(x)$, για κάποιο $j \neq 1$, τότε $\mathrm{irr}_{(F,b)}(a - dc_j) = 0$ και επομένως $a - dc_j$ πρέπει να είναι ένα από τα b_i, όπου $i = 1, \ldots, n$. Αν $a - dc_j = b_1$, τότε αφού $a = b_1 + dc_1$, έχουμε ότι

$$b_1 + dc_1 - dcj = b_1 \Rightarrow c = c_j,$$

άτοπο, αφού οι ρίζες $c_1, \ldots, c_m$ του $\mathrm{irr}_{(F,c)}(x)$ είναι διακεκριμένες και $j \neq 1$. Αν $a - dc_j = b_i$, για $i \neq 1$, οδηγούμαστε πάλι σε άτοπο, από τη σχέση (7.1.1.3). Άρα το c είναι η μόνη κοινή ρίζα των $h(x)$ και $\mathrm{irr}_{(F,c)}(x)$.

Έστω $q(x) \in F(a)[x]$ ο μέγιστος κοινός διαιρέτης των $h(x)$ και $\mathrm{irr}_{(F,c)}(x)$ στον δακτύλιο $F(a)[x]$. Ο μέγιστος κοινός διαιρέτης υπολογίζεται σύμφωνα με τον Ευκλείδειο αλγόριθμο. Έτσι, το $q(x)$ είναι μέγιστος κοινός διαιρέτης των $h(x)$ και $\mathrm{irr}_{(F,c)}(x)(x)$ στον δακτύλιο $E[x]$, βλ. Θεώρημα III.3. Αφού το c είναι η μόνη κοινή ρίζα στο E των $h(x)$ και $\mathrm{irr}_{(F,c)}(x)$ στον E και γνωρίζουμε πλήρως την ανάλυση των δύο αυτών πολυωνύμων σε γραμμικούς παράγοντες στον $E[x]$, συμπεραίνουμε ότι

$$q(x) = x - c.$$

Όμως, το $q(x) \in F(a)[x]$ και άρα $c \in F(a)$. Επίσης, αφού $b = a - dc$ συμπεραίνουμε ότι $b \in F(a)$ και επομένως

$$F(a) \subset F(b, c) \subset F(a).$$

δηλ. $F(a) = F(b, c)$ και η επέκταση $F(b, c)$ είναι απλή. □

Σημειώνουμε ότι αν $F = \mathrm{GF}(p)(x^p, y^p)$ και $E = \mathrm{GF}(p)(x, y)$ τότε η επέκταση E/F είναι πεπερασμένη. Όμως το E δεν είναι απλή επέκταση του F (βλ. άσκηση 7.3.3).

7.2 Αλγεβρικά κλειστές επεκτάσεις

Στην Ενότητα 6.3 αποδείξαμε ότι το $\mathbb{C}$ είναι αλγεβρικά κλειστό και ότι είναι το μικρότερο σώμα με αυτήν την ιδιότητα που περιέχει το $\mathbb{R}$. Σε αυτήν την ενότητα θα γενικεύσουμε τα παραπάνω για τυχαία σώματα.

Ορισμός 7.2.1. *Έστω E/F επέκταση σωμάτων. Η **αλγεβρική θήκη** (algebraic closure) του F στο E συμβολίζεται με $\overline{F}_E$ και είναι το σύνολο*

$$\overline{F}_E = \{a \in E : \ a \text{ είναι αλγεβρικό πάνω από το } F\}.$$

Πρόταση 7.2.2. *Έστω E/F επέκταση σωμάτων. Τότε η αλγεβρική θήκη $\overline{F}_E$ είναι σώμα.*

Απόδειξη. Αν $a, b \in \overline{F}_E$, τότε από το Πόρισμα 2.2.14 προκύπτει ότι $F(a,b)/F$ είναι αλγεβρική επέκταση. Επομένως κάθε στοιχείο του $F(a,b)$ ανήκει στην $\overline{F}_E$. Άρα $a-b$ και a/b ανήκουν στην $\overline{F}_E$ και επομένως $\overline{F}_E$ είναι σώμα. □

Παραδείγματα 7.2.3.

1. Έστω $E = \mathbb{Q}(\sqrt{2})$. Η αλγεβρική θήκη $\overline{\mathbb{Q}}_E$ είναι το το σώμα E, αφού κάθε στοιχείο του E είναι αλγεβρικό πάνω από το $\mathbb{Q}$, βλ. Πόρισμα 2.2.14.
2. Αν E/F είναι αλγεβρική επέκταση, τότε $\overline{F}_E = E$.
3. Η επέκταση $\overline{\mathbb{Q}}_{\mathbb{R}}/\mathbb{Q}$ είναι άπειρη και ***αριθμήσιμη*** (countable), δηλ. υπάρχει μία αριθμήσιμη βάση του σώματος $\overline{\mathbb{Q}}_{\mathbb{R}}$ πάνω από το $\mathbb{Q}$, βλ. άσκηση 7.3.5.

Ορισμός 7.2.4. *Ένα σώμα F λέγεται **αλγεβρικά κλειστό** (algebraic closure) αν $\overline{F}_E = F$, για κάθε σώμα E που περιέχει το F.*

Είναι φανερό ότι ένα σώμα F είναι αλγεβρικά κλειστό αν και μόνο αν κάθε μη σταθερό πολυώνυμο στο $F[x]$ έχει σώμα ανάλυσης το F. Βέβαια, για να δείξει κανείς ότι ένα σώμα είναι αλγεβρικά κλειστό, αρκεί να δείξει ότι κάθε μη σταθερό πολυώνυμο στο $F[x]$, έχει τουλάχιστον μία ρίζα στο F.

Παραδείγματα 7.2.5.

1. $\mathbb{Q}$ και $\mathbb{R}$ δεν είναι αλγεβρικά κλειστά σώματα.
2. Το Θεμελιώδες Θεώρημα της Άλγεβρας λέει ότι το $\mathbb{C}$ είναι αλγεβρικά κλειστό.
3. Έστω F ένα πεπερασμένο σώμα. Το F δεν είναι αλγεβρικά κλειστό, (άσκηση 7.3.5).

Το επόμενο συμπέρασμα γενικεύει το Θεώρημα 2.2.10.

Θεώρημα 7.2.6. *Έστω F σώμα και έστω $p_1(x), \ldots, p_n(x) \in F[x]$. Τότε υπάρχει επέκταση E/F, τέτοια ώστε $[E : F] < \infty$ και κάθε ένα από τα πολυώνυμα $p_1(x), \ldots, p_n(x)$ να αναλύεται σε γινόμενο γραμμικών παραγόντων στο E.*

Απόδειξη. Θα εφαρμόσουμε επαγωγή στο n. Αν $n = 1$ τότε, είμαστε στην περίπτωση του Θεωρήματος 2.2.10. Υποθέτουμε τώρα, ότι η πρόταση είναι αληθής για $n-1$ πολυώνυμα. Έστω, λοιπόν, E'/F μία επέκταση σωμάτων έτσι ώστε $[E' : F] < \infty$ και κάθε ένα από τα $p_2(x), \ldots, p_n(x)$ να αναλύεται σε γινόμενο γραμμικών παραγόντων στο E'. Αφού $F \subset E'$, θεωρούμε το $p_1(x)$ ως πολυώνυμο του $E'[x]$. Από το Θεώρημα 2.2.10, υπάρχει σώμα ανάλυσης E του $p_1(x)$ πάνω από το E' και $[E : E'] < \infty$. Επομένως, από την Πρόταση 2.2.12, έπεται ότι

$$[E : F] = [E : E'] \, [E' : F] < \infty$$

και το E έχει τις επιθυμητές ιδιότητες της πρότασης. □

Το επόμενο παράδειγμα θα βοηθήσει να γίνει κατανοητή η κατασκευή της απόδειξης του Θεωρήματος 7.2.8.

Παράδειγμα 7.2.7. Έστω $f_1(x) = x^2-2$ και $f_2(x) = x^3-5$ πολυώνυμα στον $\mathbb{Q}[x]$. Περνάμε τώρα στον δακτύλιο πολυωνύμων με τρεις ανεξάρτητες μεταβλητές, $R = \mathbb{Q}[X_1, X_2, X_3]$. Στη συνέχεια, θεωρούμε τα πολυώνυμα $f_1(X_1)$ και $f_2(X_2)$ του R. Έστω I το παρακάτω ιδεώδες του R

$$I = \langle X_1^2 + 2, X_2^3 - 5\rangle.$$

Για παράδειγμα, το πολυώνυμο

$$g(X_1, X_2, X_3) = (X_1X_3)f_1(X_1) + (X_1 + 2)f_2(X_2)$$

ανήκει στο I. Επίσης, το $g(\sqrt{2}, \sqrt[3]{5}, X_3)$ είναι το μηδενικό πολυώνυμο στο $\mathbb{Q}(\sqrt{2}, \sqrt[3]{5})[x]$, αφού

$$g(\sqrt{2}, \sqrt[3]{5}, X_3) = (\sqrt{2}X_3)f_1(\sqrt{2}) + (\sqrt{2} + 2)f_2(\sqrt[3]{5}) = (\sqrt{2}X_3)0 + (\sqrt{2} + 2)0 = 0.$$

Θεώρημα 7.2.8. *Έστω F σώμα. Υπάρχει επέκταση L/F, τέτοια ώστε κάθε μη σταθερό πολυώνυμο να έχει μία ρίζα στο L.*

Απόδειξη. Έστω

$$S = \{f : \ f \in F[x], \ \deg f \geq 1\}.$$

Σε κάθε στοιχείο f του S αντιστοιχούμε μία ανεξάρτητη μεταβλητή X_f. Θεωρούμε R, τον πολυωνυμικό δακτύλιο στις (άπειρες) μεταβλητές $\{X_f\}_{f\in S}$ και I το ιδεώδες που παράγεται από τα πολυώνυμα $f(X_f)$ στον R. Αν $g \in I$ τότε

$$g = r_1f_1(X_{f_1}) + \cdots + r_nf_n(X_{f_n}) \text{ για κάποιο } n \in \mathbb{N}, f_i \in S \text{ και } r_i \in R. \qquad (7.2.8.1)$$

Χρησιμοποιώντας το Θεώρημα 7.2.6, μπορεί να δείξει κανείς ότι το I είναι γνήσιο ιδεώδες του R. Πράγματι, θα υποθέσουμε ότι $I = R$ και θα καταλήξουμε σε άτοπο. Έστω, λοιπόν, ότι $I = R$, δηλ. ότι $1 \in I$. Τότε το 1 έχει μία έκφραση της μορφής (7.2.8.1). Άρα

$$1 = r_1f_1(X_{f_1}) + \cdots + r_nf_n(X_{f_n}) \text{ για κάποιο } n \in \mathbb{N}, f_i \in S \text{ και } r_i \in R. \qquad (7.2.8.2)$$

Από το Θεώρημα 7.2.6, υπάρχει μία επέκταση E του F τέτοια ώστε κάθε ένα από τα $f_i(x) \in F[x]$ να έχει από μία ρίζα, έστω $a_i \in E$, για $i = 1, \ldots, n$. Στην έκφραση (7.2.8.2), αντικαθιστούμε τις τιμές $a_1, \ldots, a_n$ για τις μεταβλητές $X_{f_1}, \ldots, X_{f_n}$ και 0 για κάθε μεταβλητή X_f, αν $f \neq f_1, \ldots, f_n$. Με την αντικατάσταση αυτή προκύπτει ότι $0 = 1$. Καταλήξαμε σε άτοπο, γιατί υποθέσαμε ότι $I = R$. Επομένως το I είναι γνήσιο ιδεώδες του R και σύμφωνα με την Πρόταση II.9, υπάρχει μέγιστο ιδεώδες M του R που να περιέχει το I. Έστω το σώμα $L = R/M$. Τότε

$$F : \to L, \quad c \mapsto c + M$$

είναι εμφύτευση του F στο L. Έστω τώρα $f(x)$ μη σταθερό πολυώνυμο στο $F[x]$. Τότε

$$f(X_f + M) = f(X_f) + M = M,$$

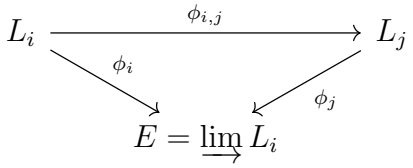
δηλ. 0, αφού το $f(X_f)$ ανήκει στο I και επομένως $X_f + M$ είναι ρίζα του $f(x)$ στο L.

□

Η κύρια ιδέα της απόδειξης του επόμενου Θεωρήματος είναι η διαδοχική εφαρμογή του Θεωρήματος 7.2.8. Με αυτόν τον τρόπο κατασκευάζεται μία αλυσίδα σωμάτων

$$F = L_0 \hookrightarrow L_1 \hookrightarrow L_2 \cdots \tag{7.2.8.3}$$

τέτοια ώστε, για κάθε $i \geq 0$, ο ομομορφισμός $\phi_{i,i+1} : L_i \to L_{i+1}$ να είναι εμφύτευση σωμάτων και κάθε πολυώνυμο του $L_i[x]$ να έχει μία ρίζα στο L_{i+1}. Παρατηρούμε ότι, παίρνοντας τις διαδοχικές συνθέσεις των εμφυτεύσεων, βρίσκουμε εμφυτεύσεις $\phi_{i,j} : L_i \to L_j$, για κάθε $i \leq j$, όπου βέβαια $\phi_{i,i} : L_i \to L_i$ είναι ο ταυτικός αυτομορφισμός του L_i. Η μαθηματική κατασκευή του ***ευθέως ορίου*** (direct limit) των L_i, $\varinjlim L_i$, δίνει ένα σώμα $E = \varinjlim L_i$ μαζί με ένα σύστημα εμφυτεύσεων $\phi_i : L_i \to E$, έτσι ώστε το διάγραμμα του σχήματος (7.1) να είναι ***αντιμεταθετικό*** (commutative), δηλ. $\phi_i = \phi_j \circ \phi_{i,j}$.



Σχήμα 7.1: Ευθύ όριο επεκτάσεων σωμάτων.

Χωρίς να μπούμε στις λεπτομέρειες της κατασκευής, σημειώνουμε ότι αν στην αλυσίδα (7.2.8.3), οι εμφυτεύσεις είναι εγκλεισμοί, αν δηλ. για $i \geq 0$, $L_i \subset L_{i+1}$, τότε

$$E = \varinjlim L_i = \bigcup_i L_i.$$

Γενικότερα, μπορούμε να σκεφτούμε το ευθύ όριο των L_i, ως την ένωση των L_i, όπου όμως για κάθε $j \geq i$, ταυτίζουμε τα στοιχεία των L_i με τις εικόνες τους στα L_j . Έτσι, αν για κάποιο λόγο, η διαδοχική εφαρμογή του Θεωρήματος 7.2.8, μας οδηγεί σε ένα σημείο σταθερότητας m, όπου για κάθε $i \geq m$, το $L_i = L_m$, όπως δείχνουμε στη παρακάτω αλυσίδα,

$$F = L_0 \hookrightarrow L_1 \hookrightarrow L_2 \cdots \hookrightarrow L_m \hookrightarrow L_m,$$

τότε $\varinjlim L_i = L_m$. Θα αγνοήσουμε, για τις ανάγκες αυτού του κειμένου, τις περαιτέρω τεχνικότητες της κατασκευής και θα εστιάσουμε στη παρακάτω παρατήρηση: κάθε στοιχείο του E, προκύπτει από κάποια εμφύτευση $\phi_i : L_i \to E$. Έτσι για οποιαδήποτε πεπερασμένη συλλογή στοιχείων του E μπορούμε να επιλέξουμε κατάλληλο μεγάλο δείκτη n και να θεωρήσουμε ότι όλα τα στοιχεία αυτής της συλλογής προέρχονται από εμφύτευση στοιχείων του L_n.

Θα δείξουμε τώρα ότι κάθε μη σταθερό πολυώνυμο στο E έχει μία ρίζα στο E. Έστω, λοιπόν, $p(x) = \sum a_i x^i \in E[x]$, $\deg p(x) \geq 1$ και n φυσικός αριθμός, έτσι ώστε $p(x) = \sum \phi_n(b_i)x^i$, όπου $b_i \in L_n$. Θεωρούμε το πολυώνυμο

$$q(x) = \sum b_i x^i \in L_n[x].$$

Παρατηρούμε ότι $\deg q(x) \geq 1$. Από το βήμα κατασκευής της αλυσίδας (7.2.8.3), το $q(x)$ έχει μία ρίζα, έστω a, στο $L_{n+1}[x]$. Επομένως,

$$\sum \phi_{n,n+1}(b_i)a^i = 0 \ .$$

Σύμφωνα με το αντιμεταθετικό διάγραμμα του Σχήματος (7.1), προκύπτει ότι:

$$\sum a_i \phi_{n+1}(a)^i = \sum \phi_{n+1}(\phi_{n,n+1}(b_i))\ \phi_{n+1}(a^i) = \phi_{n+1}(\sum \phi_{n,n+1}(b_i)a^i) = 0$$

και επομένως $\phi_{n+1}(a)$ είναι ρίζα του $p(x)$. Αποδείξαμε λοιπόν το παρακάτω συμπέρασμα:

Θεώρημα 7.2.9. *Έστω F σώμα. Υπάρχει αλγεβρικά κλειστό σώμα E, τέτοιο ώστε το F να εμφυτεύεται στο E.*

Αφού το $\mathbb{C}$ είναι αλγεβρικό πάνω από το $\mathbb{R}$ και το $\mathbb{C}$ είναι αλγεβρικά κλειστό, έχουμε ότι το $\mathbb{C} = \overline{\mathbb{R}}_{\mathbb{C}}$. Το $\mathbb{C}$ είναι το *μικρότερο* αλγεβρικά κλειστό σώμα που περιέχει το $\mathbb{R}$.

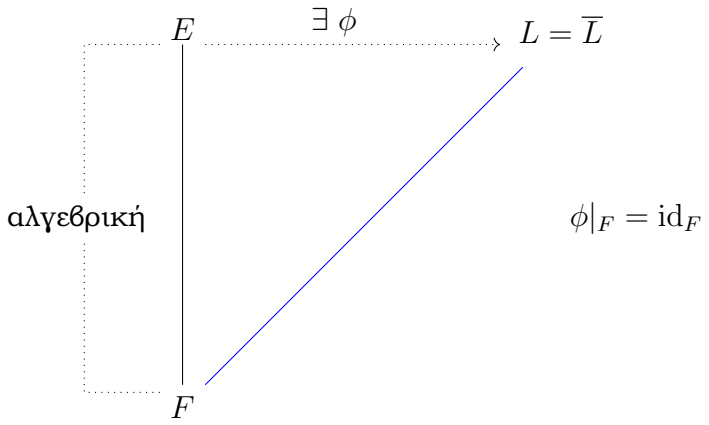
Ορισμός 7.2.10. *Έστω L/F επέκταση σωμάτων. Το E λέγεται **αλγεβρική θήκη** (algebraic cover) του F αν το L είναι αλγεβρικά κλειστό και εάν η επέκταση του L/F είναι αλγεβρική.*

Όπως είδαμε προηγουμένως, το $\mathbb{C}$ είναι η αλγεβρική θήκη του $\mathbb{R}$. Το επόμενο θεώρημα αφορά την ύπαρξη αλγεβρικών θηκών.

Θεώρημα 7.2.11. *Έστω F σώμα. Υπάρχει επέκταση E/F έτσι ώστε το E να είναι η αλγεβρική θήκη του F.*

Απόδειξη. Από το Θεώρημα 7.2.9, υπάρχει επέκταση E/F έτσι ώστε το E να είναι αλγεβρικά κλειστό. Θεωρούμε την αλγεβρική θήκη L του F στο E, δηλ. $L = \overline{F}_E$. Για να δείξουμε ότι $\overline{L} = L$, πρέπει να δείξουμε ότι το L είναι αλγεβρικά κλειστό σώμα. Έστω $p(x) \in L[x]$. Τότε το $p(x) \in E[x]$ και αφού το E είναι αλγεβρικά κλειστό, υπάρχει κάποια ρίζα a του $p(x)$ στο E. Επομένως η επέκταση $L(a)/L$ είναι αλγεβρική. Αφού η επέκταση L/F είναι επίσης αλγεβρική, συμπεραίνουμε ότι $L(a)/F$ είναι αλγεβρική, βλ. Πρόταση 2.2.15. Άρα a είναι αλγεβρικό πάνω από το F και επομένως ανήκει στην αλγεβρική θήκη του F στο E. Συνεπώς $a \in L$ και το L είναι αλγεβρικά κλειστό. □

Είναι η αλγεβρική θήκη μοναδική με προσέγγιση F-ισομορφίας; Η απάντηση είναι θετική, όπως μπορεί να δείξει κανείς χρησιμοποιώντας το Λήμμα του Zorn. Πρώτα, όμως, είναι χρήσιμο να δείξουμε ότι, αν η E/F είναι αλγεβρική επέκταση σωμάτων και L/F ένα μία επέκταση σωμάτων, όπου $L = \overline{L}$, τότε υπάρχει F-εμφύτευση $\phi : E \to L$, όπου $\phi(c) = c$, για κάθε $c \in F$.



Σχήμα 7.2: F-εμφύτευση αλγεβρικής επέκτασης σε αλγεβρικά κλειστό σώμα

Η συνήθης τεχνική, για την απόδειξη της F-εμφύτευσης, είναι να θεωρήσει κανείς το μη κενό μερικά διατεταγμένο σύνολο Ω, με στοιχεία ζεύγη (K, ψ), όπου K είναι ενδιάμεσο

σώμα της επέκτασης E/F και $\psi : K \to L$ μία F-εμφύτευση. Το σύνολο Ω είναι όντως μη κενό, αφού περιέχει το ζεύγος (F, i), όπου i είναι η εμφύτευση του F στο L. Η σχέση διάταξης στο Ω συγκρίνει ταυτόχρονα και τις δύο ενότητες του ζεύγους:

$$(K_1, \psi_1) \leq (K_2, \psi_2) \text{ αν } K_1 \subset K_2, \text{ και } \psi_2|_{K_1} = \psi_1.$$

Στη συνέχεια ελέγχουμε ότι κάθε αλυσίδα στο Ω έχει άνω φράγμα, και συμπεραίνουμε ότι το Ω έχει μέγιστο στοιχείο, από το Λήμμα του Zorn. Τέλος, δείχνουμε ότι το μέγιστο στοιχείο του Ω είναι της μορφής (E, ϕ). Εφαρμόζοντας τα παραπάνω, όταν το E και το L είναι αλγεβρικές θήκες του F, προκύπτουν F-ισομορφισμοί $\phi : E \to L$ και $\psi : L \to E$. Έτσι οδηγούμαστε στο συμπέρασμα της μοναδικότητας της αλγεβρικής θήκης. Ο αναγνώστης καλείται να συμπληρώσει τις λεπτομέρειες της απόδειξης.

Θεώρημα 7.2.12. *Η αλγεβρική θήκη ενός σώματος F είναι μοναδική με προσέγγιση F-ισομορφίας, δηλ. αν E_1 και E_2 είναι δύο αλγεβρικές θήκες του F, τότε υπάρχει $\phi : E_1 \to E_2$, τέτοια ώστε $\phi(c) = c$, για κάθε $c \in F$.*

Ως τελευταία παρατήρηση, ας αναφέρουμε έναν ακόμη συλλογισμό εξηγώντας το γιατί δεν τον χρησιμοποιήσαμε για να επιχειρηματολογήσουμε για την ύπαρξη της αλγεβρικής θήκης του F: έστω S η συλλογή

$$S = \{K : \ F/K \text{ αλγεβρική επέκταση του } F\},$$

με σχέση διάταξης τον εγκλεισμό συνόλων. Τότε, η S περιέχει το F και κάθε αλυσίδα στην S

$$K_1 \leq K_2 \leq \cdots$$

έχει άνω φράγμα στο S το σύνολο

$$\bigcup_i K_i.$$

Αποδεικνύεται ότι η K/F είναι αλγεβρική επέκταση σωμάτων. Από το Λήμμα του Zorn, προκύπτει ότι η S έχει μέγιστο στοιχείο E. Στη συνέχεια μπορεί να αποδειχθεί ότι το E είναι αλγεβρικά κλειστό και άρα είναι η αλγεβρική θήκη του F.

Είναι, όμως, η συλλογή S όπως έχει οριστεί (και για να μπορούμε να εφαρμόσουμε το Λήμμα του Zorn) σύνολο, ή υπεισέρχονται τα παράδοξα της Θεωρίας Συνόλων; Ξεφεύγει από τους στόχους του συγγράμματος αυτό το ερώτημα. Ο ενδιαφερόμενος αναγνώστης μπορεί να μελετήσει περαιτέρω το θέμα. Για μία σχετική ιδέα αναφέρουμε την άσκηση 7.3.4.

7.3 Ασκήσεις

1. Να αποδείξετε ότι κάθε αλγεβρικά κλειστό σώμα F είναι τέλειο.

2. Να δείξετε ότι $\mathbb{Q}(\sqrt[3]{2}, \sqrt{5}, \sqrt{7})$ είναι απλή επέκταση πάνω από το $\mathbb{Q}$.

3. Να δείξετε ότι αν $F = \mathrm{GF}(p)(x^p, y^p)$ και $E = \mathrm{GF}(p)(x, y)$ τότε η επέκταση E/F είναι πεπερασμένη. Όμως, το σώμα E δεν είναι απλή επέκταση του F.

4. Να αποδείξετε ότι η επέκταση $\overline{\mathbb{Q}}_{\mathbb{R}}/\mathbb{Q}$ είναι άπειρη και αριθμήσιμη, δηλ. υπάρχει μία αριθμήσιμη βάση του σώματος $\overline{\mathbb{Q}}_{\mathbb{R}}$ πάνω από το $\mathbb{Q}$.

5. Έστω F ένα πεπερασμένο σώμα. Να αποδείξετε ότι το F δεν είναι αλγεβρικά κλειστό.

6. Να αποδείξετε ότι η ομάδα $\mathrm{Gal}(\mathbb{C}/\mathbb{Q})$ είναι άπειρη. (Σημειώστε και την εκφώνηση της άσκησης 2.4.24.)

Βιβλιογραφία Κεφαλαίου 7

[1] Dummit, D.S., Foote, R.M. *Abstract Algebra*. J. Wiley and Sons, Inc, 2004.

[2] Lang, S. *Algebra*. Springer, 2002.

[3] Rotman, J. *Θεωρία Galois*. Leader Books, 2000.

Κεφάλαιο 8

Το γενικό πολυώνυμο και το αντίστροφο πρόβλημα

Σε αυτό το κεφάλαιο αρχικά αποδεικνύουμε ότι υπάρχει επέκταση σωμάτων με ομάδα Galois την S_n. Για το σκοπό αυτό εξετάζουμε τα συμμετρικά πολυώνυμα. Τέλος αναφερόμαστε στο αντίστροφο πρόβλημα της θεωρίας Galois.

8.1 Το γενικό πολυώνυμο

Ας θεωρήσουμε ένα πολυώνυμο $f(x) \in \mathbb{Q}[x]$ και L το σώμα ανάλυσης του $f(x)$ πάνω από το $\mathbb{Q}$. Επειδή $\operatorname{char}\mathbb{Q} = 0$, το $f(x)$ είναι διαχωρίσιμο και συνεπώς η επέκταση $L/\mathbb{Q}$ είναι επέκταση του Galois. Η ***ομάδα Galois του f(x)*** (Galois group of $f(x)$) είναι η ομάδα $G = \operatorname{Gal}(L/\mathbb{Q})$. Είδαμε ότι η ομάδα G εκφράζεται ως ομάδα μεταθέσεων των n αντικειμένων, όπου n είναι το πλήθος των διακεκριμένων ριζών του $f(x)$, δηλ. η ομάδα G εμφυτεύεται στην ομάδα S_n (βλ. Θεώρημα 3.1.1). Επομένως η τάξη της G διαιρεί το $n!$. Είναι λογικό να αναρωτηθούμε αν υπάρχει πολυώνυμο $f(x) \in \mathbb{Q}[x]$ τέτοιο ώστε η ομάδα Galois του $f(x)$ να είναι ισόμορφη με την S_n. Στην ενότητα αυτή θα ασχοληθούμε με αυτό το ερώτημα. Για την αντιμετώπισή του μας χρειάζεται η επόμενη έννοια.

Ορισμός 8.1.1. *Έστω E/F μία επέκταση σωμάτων και $a_1, \ldots, a_n \in E$. Τα στοιχεία $a_1, \ldots, a_n$ λέγονται **αλγεβρικά ανεξάρτητα πάνω από το** F (algebraically independent over F) αν δεν υπάρχει μη μηδενικό πολυώνυμο $f(x_1, \ldots, x_n) \in F[x_1, \ldots, x_n]$ έτσι ώστε $f(a_1, \ldots, a_n) = 0$.*

Με άλλα λόγια, τα στοιχεία $a_1, \ldots, a_n \in E$ είναι αλγεβρικά ανεξάρτητα πάνω από το F αν δεν υπάρχει μία (μη μηδενική) αλγεβρική σχέση με συντελεστές από το F, που να ικανοποιείται από τα στοιχεία $a_1, \ldots, a_n$. Για να κατανοήσουμε καλύτερα αυτήν την έννοια, θα ακολουθήσουμε τη διαδικασία ορισμού των αλγεβρικών και υπερβατικών στοιχείων πάνω από το σώμα F, με $\operatorname{char} F = 0$. Θεωρούμε τον πολυωνυμικό δακτύλιο $F[x_1, \ldots, x_n]$. Ο $F[x_1, \ldots, x_n]$ είναι μία ακέραια περιοχή με σώμα κλασμάτων το σώμα $F(x_1, \ldots, x_n)$ (βλ. III.4.1). Έστω η επέκταση E/F και $a_1, \ldots, a_n \in E$. Η συνάρτηση

$$h:\ F[x_1, \ldots, x_n] \to E, \quad f(x_1, \ldots, x_n) \mapsto f(a_1, \ldots, a_n)$$

είναι ένας ομομορφισμός δακτυλίων και

$$\ker h = \{f(x_1, \ldots, x_n):\ f(a_1, \ldots, a_n) = 0\}.$$

Φυσικά η συνάρτηση h εξαρτάται από τα στοιχεία $a_1, \ldots, a_n$ και ως γνωστόν ο $\ker h$ είναι ένα ιδεώδες του $F[x_1, \ldots, x_n]$. Αν ο $\ker h = \{0\}$, τότε τα στοιχεία $a_1, \ldots, a_n$ είναι αλγεβρικά ανεξάρτητα πάνω από το F. Αν ο $\ker h \neq \{0\}$, τότε τα στοιχεία $a_1, \ldots, a_n$ λέγονται ***αλγεβρικά εξαρτημένα*** (algebraically dependent). Από τα παραπάνω, προκύπτει το εξής:

Πρόταση 8.1.2. *Έστω E/F μία επέκταση σωμάτων και $a_1, \ldots, a_n \in E$ αλγεβρικά ανεξάρτητα πάνω από το F. Τότε $F[x_1, \ldots, x_n] \cong F[a_1, \ldots, a_n]$.*

Είναι φανερό ότι αν τα στοιχεία $a_1, \ldots, a_n$ είναι αλγεβρικά ανεξάρτητα πάνω από το F, τότε κανένα από τα a_i δεν είναι αλγεβρικό πάνω από το F, για $i = 1, \ldots, n$. Σημειώνουμε ότι η έννοια της αλγεβρικής ανεξαρτησίας είναι γενικότερη της έννοιας της γραμμικής ανεξαρτησίας. Η αλγεβρική ανεξαρτησία συνεπάγεται τη γραμμική ανεξαρτησία, χωρίς να ισχύει το αντίστροφο (βλ. άσκηση 7.3.1). Σημειώνουμε επίσης την παρακάτω γενίκευση της Πρότασης III.5.

Πρόταση 8.1.3. *Έστω E/F επέκταση σωμάτων και έστω $a_1, \ldots, a_n \in E$ γραμμικά ανεξάρτητα πάνω από το F. Αν $t : \{a_1, \ldots, a_n\} \to \{a_1, \ldots, a_n\}$ είναι μία συνάρτηση, τότε υπάρχουν μοναδικοί αυτομορφισμοί $\tilde{t}$ και $\tilde{\tilde{t}}$, όπου*

$$\tilde{t} : \ F[a_1, \ldots, a_n] \to F[a_1, \ldots, a_n], \ \text{με } f(a_1, \ldots, a_n) \mapsto f(t(a_1), \ldots, t(a_n))$$

και

$$\tilde{\tilde{t}} : \ F(a_1, \ldots, a_n) \to F(a_1, \ldots, a_n), \ \text{με } \frac{f_1(a_1, \ldots, a_n)}{f_2(a_1, \ldots, a_n)} \mapsto \frac{f_1(t(a_1), \ldots, t(a_n))}{f_2(t(a_1), \ldots, t(a_n))}.$$

Στη συνέχεια θα οδηγηθούμε σε ένα παράδειγμα αλγεβρικά ανεξάρτητων στοιχείων, που είναι χρήσιμο για το σκοπό μας.

Ορισμός 8.1.4. *Έστω n ένας θετικός ακέραιος και F ένα σώμα με $\operatorname{char} F = 0$. Ένα πολυώνυμο $f(x_1, \ldots, x_n) \in F[x_1, \ldots, x_n]$ λέγεται **συμμετρικό** (symmetric) αν*

$$f(x_1, \ldots, x_n) = f(x_{\sigma(1)}, \ldots, x_{\sigma(n)}), \ \text{για κάθε } \sigma \in S_n.$$

Τα πολυώνυμα

$$e_s(x_1, \ldots, x_n) = \sum_{\substack{T \subset \{1, \ldots, n\} \\ |T| = s}} \prod_{i \in T} x_i, \quad 0 \leq s \leq n$$

*λέγονται **στοιχειώδη συμμετρικά πολυώνυμα** (elementary symmetric polynomials).*

Έτσι τα στοιχειώδη συμμετρικά πολυώνυμα στον $F[x_1, \ldots, x_n]$ είναι τα:

$$\begin{aligned} e_0(x_1, \ldots, x_n) &= 1 \\ e_1(x_1, \ldots, x_n) &= x_1 + \cdots + x_n \\ e_2(x_1, \ldots, x_n) &= \sum_{1 \leq i < j \leq n} x_i x_j \\ &\vdots \\ e_n(x_1, \ldots, x_n) &= x_1 \cdots x_n \ . \end{aligned}$$

Οι επόμενες προτάσεις αναφέρονται στη δομή των συμμετρικών πολυωνύμων και δίνονται χωρίς απόδειξη, αφού ξεφεύγουν από τον κύριο σκοπό μας. Για την απόδειξη του Θεωρήματος 8.1.5 ο αναγνώστης μπορεί να συμβουλευθεί το [4, Theorem 3.1.2].

Θεώρημα 8.1.5 (Θεμελιώδες Θεώρημα των Συμμετρικών Πολυωνύμων).

i) Τα μη σταθερά στοιχειώδη συμμετρικά πολυώνυμα $e_1(x_1,\dots,x_n),\ \dots,e_n(x_1,\dots,x_n)$ *του* $F[x_1,\dots,x_n]$ *είναι αλγεβρικά ανεξάρτητα πάνω από το σώμα* F*.*

ii) Το σύνολο των συμμετρικών πολυωνύμων του $F[x_1,\dots,x_n]$ *αποτελεί έναν υποδακτύλιο του* $F[x_1,\dots,x_n]$*, που παράγεται ακριβώς από τα* $e_1(x_1,\dots,x_n),\dots,e_n(x_1,\dots,x_n)$*.*

Η απόδειξη της επόμενης πρότασης γίνεται επαγωγικά ως προς το n και αφήνεται για τον αναγνώστη (βλ.άσκηση 7.3.2).

Πρόταση 8.1.6. *Έστω* $a_1,\dots,a_n\in E$*. Τότε*

$$\prod_{i=1}^{n}(x-a_i)=\sum_{k=0}^{n}(-1)^{n-k}e_{n-k}(a_1,\dots,a_n)x^k,$$

όπου $e_s(x_1,\dots,x_n)\in E[x_1,\dots,x_n]$*,* $0\le s\le n$*, τα στοιχειώδη συμμετρικά πολυώνυμα του* $E[x_1,\dots,x_n]$*.*

Έστω τώρα n ένας θετικός ακέραιος και $a_1,\dots,a_n\in E$ αλγεβρικά ανεξάρτητα στοιχεία πάνω από το F, όπου E/F επέκταση σωμάτων με $\operatorname{char}F=0$. Τότε το πολυώνυμο

$$f(x)=\prod_{i=1}^{n}(x-a_i)\in E[x_1,\dots,x_n] \tag{8.1.6.1}$$

γράφεται ως

$$f(x)=x^n+\sum_{k=0}^{n-1}c_kx^k, \tag{8.1.6.2}$$

όπου $c_i=e_{n-i}(a_1,\dots,a_n)$ για $i=0,\dots,n-1$, σύμφωνα με την Πρόταση 8.1.6. Το πολυώνυμο που αναφέρεται στις σχέσεις (8.1.6.1) και (8.1.6.2) λέγεται ***γενικό πολυώνυμο βαθμού n*** (general polynomial of degree n) και η εξίσωση $f(x)=0$ λέγεται ***γενική εξίσωση βαθμού n*** (general equation of degree n). Η παρακάτω παρατήρηση είναι σημαντική.

Παρατήρηση 8.1.7. *Με τους παραπάνω συμβολισμούς, αν* $a_1,\dots,a_n$ *είναι αλγεβρικά ανεξάρτητα στοιχεία πάνω από το* F*, τότε τα στοιχεία* $c_0,c_1,\dots,c_{n-1}$ *είναι αλγεβρικά ανεξάρτητα πάνω από το* F*.*

Απόδειξη. Έστω ότι τα $c_0,c_1,\dots,c_{n-1}$ είναι αλγεβρικά εξαρτημένα πάνω από το F. Τότε υπάρχει $h(y_0,\dots,y_{n-1})\in F[y_0,\dots,y_{n-1}]$ έτσι ώστε $h(c_0,\dots,c_{n-1})=0$. Τότε, όμως,

$$g(x_1,\dots,x_n):=h\left(e_n(x_1,\dots,x_n),\dots,e_1(x_1,\dots,x_n)\right)\in F[x_1,\dots,x_n]$$

και $g(a_1,\dots,a_n)=0$. Αυτό αντιφάσκει με την υπόθεση ότι τα $a_1,\dots,a_n$ είναι αλγεβρικά ανεξάρτητα πάνω από το F. □

Θεωρούμε, τώρα, το σώμα $L=F(a_1,\dots,a_n)$ και το σώμα $K=F(c_0,\dots,c_{n-1})$ για τα αλγεβρικά ανεξάρτητα στοιχεία $a_1,\dots,a_n\in E$, όπου $c_i=e_{n-i}(a_1,\dots,a_n)$, για $i=0,\dots,n-1$. Σημειώνουμε ότι $f(x)\in K[x]$ και ότι $K\subset L$. Αφού $a_1,\dots,a_n$ είναι ρίζες του $f(x)$, συμπεραίνουμε επίσης ότι το L είναι σώμα ανάλυσης του $f(x)$ πάνω από το K. Ακόμη το πολυώνυμο $f(x)$ είναι διαχωρίσιμο, αφού τα $a_1,\dots,a_n$ είναι αλγεβρικά ανεξάρτητα και συνεπώς διακεκριμένα στοιχεία του E. Έτσι καταλήγουμε στην επόμενη πρόταση.

Πρόταση 8.1.8. *Αν τα $a_1, \ldots, a_n$ είναι αλγεβρικά ανεξάρτητα στοιχεία πάνω από το F, τότε η $L = F(a_1, \ldots, a_n)$ είναι επέκταση του Galois πάνω από $K = F(c_0, \ldots, c_{n-1})$, όπου $c_i = e_{n-i}(a_1, \ldots, a_n)$ για $i = 0, \ldots, n-1$.*

Ερχόμαστε, τώρα, στο κύριο συμπέρασμα αυτού του εδαφίου, που απαντά στο ερώτημα που τέθηκε στην αρχή του.

Θεώρημα 8.1.9. *Έστω $a_1, \ldots, a_n$ αλγεβρικά ανεξάρτητα στοιχεία πάνω από το σώμα $\mathbb{Q}$ για έναν θετικό ακέραιο n και*

$$f(x) = x^n + \sum_{k=0}^{n-1} c_k x^k$$

το γενικό πολυώνυμο βαθμού n, όπου $c_i = e_{n-i}(a_1, \ldots, a_n)$ για $i = 0, \ldots, n-1$. Η ομάδα Galois της επέκτασης

$$\mathbb{Q}(a_1, \ldots, a_n)/\mathbb{Q}(c_0, \ldots, c_{n-1})$$

είναι ισόμορφη με την S_n.

Απόδειξη. Αφού $\deg f(x) = n$ και $\mathbb{Q}(a_1, \ldots, a_n)/\mathbb{Q}(c_0, \ldots, c_{n-1})$ είναι επέκταση του Galois, συμπεραίνουμε ότι $G = \mathrm{Gal}\left(\mathbb{Q}(a_1, \ldots, a_n)/\mathbb{Q}(c_0, \ldots, c_{n-1})\right)$ εμφυτεύεται στην S_n (βλ. Θεώρημα 3.1.1). Έστω $\sigma \in S_n$. Θεωρούμε την αντιστοιχία

$$g_\sigma : \mathbb{Q}(a_1, \ldots, a_n) \to \mathbb{Q}(a_1, \ldots, a_n), \quad \frac{f_1(a_1, \ldots, a_n)}{f_2(a_1, \ldots, a_n)} \mapsto \frac{f_1(a_{\sigma(1)}, \ldots, a_{\sigma(n)})}{f_2(a_{\sigma(1)}, \ldots, a_{\sigma(n)})}.$$

Είναι φανερό ότι η g_σ είναι αυτομορφισμός του $\mathbb{Q}(a_1, \ldots, a_n)$ (βλ. Πρόταση 8.1.3) που κρατά σταθερά τα στοιχεία του $\mathbb{Q}(c_0, \ldots, c_{n-1})$. Επομένως

$$H = \{g_\sigma : \sigma \in S_n\} \leq G \hookrightarrow S_n.$$

Όμως $|H| = n!$ και άρα $H \cong S_n$, με $g_\sigma \mapsto \sigma$. Επομένως

$$S_n \cong \mathrm{Gal}\left(\mathbb{Q}(a_1, \ldots, a_n)/\mathbb{Q}(c_0, \ldots, c_{n-1})\right).$$

Αποδείξαμε λοιπόν ότι η ομάδα Galois της επέκτασης $\mathbb{Q}(a_1, \ldots, a_n)/\mathbb{Q}(c_0, \ldots, c_{n-1})$ είναι ισόμορφη με την S_n. □

8.2 Το αντίστροφο πρόβλημα

Όπως είδαμε στην προηγούμενη ενότητα, για κάθε φυσικό αριθμό n, υπάρχουν κατάλληλες επεκτάσεις σωμάτων L/K, όπου K επέκταση του $\mathbb{Q}$, έτσι ώστε $\mathrm{Gal}(L/K) \cong S_n$, (βλ. Θεώρημα 8.1.9). Από το Θεώρημα του Cayley (βλ. Θεώρημα I.17) κάθε πεπερασμένη ομάδα τάξης n εμφυτεύεται στην S_n. Επομένως, σύμφωνα με το Θεμελιώδες Θεώρημα της Θεωρίας Galois, αν G είναι υποομάδα της S_n, τότε υπάρχει ενδιάμεσο υπόσωμα M του L ώστε $\mathrm{Gal}(L/M) \cong G$. Αφού M/K είναι επέκταση του $\mathbb{Q}$, έπεται ότι το M είναι επίσης επέκταση του $\mathbb{Q}$. Καταλήγουμε έτσι στο συμπέρασμα:

Πρόταση 8.2.1. *Αν G είναι μία πεπερασμένη ομάδα, τότε υπάρχει επέκταση L/M, όπου το M είναι επέκταση του $\mathbb{Q}$, τέτοια ώστε $\mathrm{Gal}(L/M) \cong G$.*

Με χρήση του σημαντικού Θεωρήματος Αναγωγιμότητας του Hilbert αποδεικνύεται το επόμενο θεώρημα, που παρουσιάζουμε χωρίς απόδειξη.

Θεώρημα 8.2.2. *Για κάθε θετικό ακέραιο n υπάρχει επέκταση $L/\mathbb{Q}$ έτσι ώστε* $\mathrm{Gal}(L/\mathbb{Q}) \cong S_n$.

Για την απόδειξη και την εκφώνηση του Θεωρήματος του Hilbert παραπέμπουμε στο [4, Chapter 3] και [3, Theorem 4.3]. Ακόμη και μετά τα Θεωρήματα 8.2.1 και 8.2.2 παραμένει το ερώτημα, αν ισχύει το αντίστοιχο με το Θεώρημα 8.2.2, με G στη θέση της S_n, όπου G είναι μία πεπερασμένη ομάδα. Το ερώτημα αυτό είναι γνωστό, ως το Αντίστροφο Πρόβλημα της Θεωρίας Galois (Inverse Problem of Galois Theory).

Ερώτημα 8.2.3 (Αντίστροφο πρόβλημα της Θεωρίας Galois). *Έστω G μία πεπερασμένη ομάδα. Υπάρχει επέκταση $L/\mathbb{Q}$, έτσι ώστε* $\mathrm{Gal}(L/\mathbb{Q}) \cong G$*;*

Όπως είδαμε στην Ενότητα 5.2, από το Θεώρημα των Kronecker-Weber προκύπτει ότι αν $K/\mathbb{Q}$ είναι μία πεπερασμένη επέκταση του Galois έτσι ώστε η $\mathrm{Gal}(K/\mathbb{Q})$ να είναι αβελιανή, τότε υπάρχει μία ρίζα της μονάδας ω ώστε $K \subset \mathbb{Q}(\omega)$ (βλ. Θεώρημα 5.2.8). Από το Θεώρημα των Kronecker-Weber, το Θεμελιώδες Θεώρημα της Θεωρίας Galois και τη Θεωρία των κυκλοτομικών σωμάτων που αναπτύξαμε στην Ενότητα 5.2, προκύπτει ότι αν δοθεί μία πεπερασμένη αβελιανή ομάδα G, τότε υπάρχει επέκταση $M/\mathbb{Q}$, ώστε $\mathrm{Gal}(M/\mathbb{Q}) \cong G$ (βλ. άσκηση 7.3.3).

Έχουμε επομένως μία μερική απάντηση του ερωτήματος 8.2.3. Η πλήρης όμως απάντηση στο Αντίστροφο Πρόβλημα της Θεωρίας Galois δεν έχει δοθεί ακόμη και το ερώτημα 8.2.3 παραμένει αναπάντητο. Αξίζει να επισημάνουμε το ακόλουθο σημαντικό σχετικό συμπέρασμα που αποδείχθηκε από τον I. Shafarevich το 1954 στην εργασία: *Construction of fields of algebraic numbers with given solvable Galois groups*, Izv. Akad. Nauk SSSR Ser. Mat. (525 - 578).

Θεώρημα 8.2.4 (Shafarevich). *Για κάθε πεπερασμένη επιλύσιμη ομάδα G, υπάρχει επέκταση $L/\mathbb{Q}$ έτσι ώστε* $\mathrm{Gal}(L/\mathbb{Q}) \cong G$.

8.3 Ασκήσεις

1. Να δώσετε ένα παράδειγμα γραμμικά ανεξάρτητων στοιχείων πάνω από το $\mathbb{Q}$ που δεν είναι αλγεβρικά ανεξάρτητα.

2. Έστω $a_1, \ldots, a_n \in E$ και $e_s(x_1, \ldots, x_n) \in E[x_1, \ldots, x_n]$, $0 \leq s \leq n$ τα στοιχειώδη συμμετρικά πολυώνυμα του $E[x_1, \ldots, x_n]$. Να αποδείξετε ότι

$$\prod_{i=1}^{n}(x - a_i) = \sum_{k=0}^{n}(-1)^{n-k} e_{n-k}(a_1, \ldots, a_n)x^k.$$

3. Να αποδείξετε ότι αν δοθεί μία πεπερασμένη αβελιανή ομάδα G, τότε υπάρχει επέκταση $M/\mathbb{Q}$, ώστε $\mathrm{Gal}(M/\mathbb{Q}) \cong G$.

Βιβλιογραφία Κεφαλαίου 8

[1] Bastida, J. R. *Field Extensions and Galois Theory, Vol. 22.* Addison-Wesley, 2007.

[2] Escofier, J.P. *Galois Theory.* Springer, 2001.

[3] Hadlock, C. R *Field Theory and its Classical Problems*. MAA, 2000.

[4] Prasolov, V. *Polynomials*. Springer, 2012.

[5] Ribenhoim, P. *Algebraic Numbers*. Wiley-Interscience, New York, 1972.

[6] Rotman, J. *Θεωρία Galois*. Leader Books, 2000.

[7] Serre, J. P. *Topics in Galois Theory*. Jones and Bartlett Boston, 1992.

[8] Volklein, H. *Groups as Galois Groups: An Introduction*. Cambridge Studies in Advnaced Mathematics 53, 1996.

Παράρτημα

I Στοιχεία από τη Θεωρία Ομάδων

Ορισμός Ι.1. *Ένα μη κενό σύνολο G λέγεται* ***ομάδα*** *(group) αν σε αυτό ορίζεται μία πράξη*

$$\cdot : G \times G \longrightarrow G, \quad (a, b) \mapsto ab$$

με τις ακόλουθες ιδιότητες:

α. Η πράξη είναι προσεταιριστική, δηλ. $a(bc) = (ab)c$*, για* $a, b, c \in G$*,*

β. υπάρχει ένα στοιχείο $e \in G$ *τέτοιο ώστε* $ea = a = ae$*, για* $a \in G$*,*

γ. για κάθε $a \in G$*, υπάρχει ένα στοιχείο* $a^{-1} \in G$ *τέτοιο ώστε* $a^{-1}a = e = aa^{-1}$*.*

Το στοιχείο e λέγεται ουδέτερο ή μοναδιαίο στοιχείο της ομάδας. Η ομάδα G συμβολίζεται ως $(G, \cdot)$ όταν χρειάζεται να δοθεί έμφαση στην πράξη της. Αν η πράξη είναι αντιμεταθετική, δηλ.

$$ab = ba, \text{ για } a, b \in G \ ,$$

τότε η ομάδα G λέγεται αντιμεταθετική ή αβελιανή. Ιδιαίτερα όταν η πράξη συμβολίζεται με $+$ και ονομάζεται πρόσθεση, τότε το ουδέτερο στοιχείο e λέγεται μηδενικό στοιχείο και συμβολίζεται με 0. Αν το G είναι ένα αριθμητικό σύνολο, π.χ. υποσύνολο του συνόλου $\mathbb{C}$ των μιγαδικών αριθμών και η πράξη είναι ο πολλαπλασιασμός των αριθμών, τότε το e συμβολίζεται με 1. Το στοιχείο a^{-1} λέγεται αντίστροφο του a. Ιδιαίτερα όταν η πράξη συμβολίζεται με $+$, τότε το a^{-1} λέγεται αντίθετο του a και συμβολίζεται με $-a$. Το πλήθος των στοιχείων $|G|$ του συνόλου G λέγεται ***τάξη*** (order) της G. Αν $|G| < \infty$, τότε η G λέγεται ομάδα πεπερασμένης τάξης ή πεπερασμένη ομάδα. Αν $|G| = \infty$, τότε η G λέγεται άπειρης τάξης ομάδα ή άπειρη ομάδα.

Παραδείγματα Ι.2.

1. Οι $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$, $(\mathbb{Q}^*, \cdot)$, $(\mathbb{R}^*, \cdot)$, $(\mathbb{C}^*, \cdot)$ είναι παραδείγματα άπειρων αβελιανών ομάδων, όπου $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$, και ανάλογα ορίζονται τα $\mathbb{R}^*$, $\mathbb{C}^*$.

2. Έστω $n > 1$ φυσικός αριθμός. Με $\mathbb{Z}_n$ συμβολίζουμε το σύνολο των κλάσεων υπολοίπων $\bmod n$, δηλ.

   $$\mathbb{Z}_n = \{\bar{a} : \ 0 \leq a \leq n-1\},$$

   όπου

   $$\bar{a} = \{a + kn : \ k \in \mathbb{Z}\}.$$

   Στο σύνολο $\mathbb{Z}_n$ ορίζουμε τις πράξεις $+$ και $\cdot$ ως εξής:

   $$\bar{a} + \bar{b} = \overline{a+b} \quad \text{και} \quad \bar{a} \cdot \bar{b} = \overline{ab}.$$

   Η $(\mathbb{Z}_n, +)$ είναι αβελιανή ομάδα με n στοιχεία. Η $(\mathbb{Z}_n, \cdot)$ δεν είναι ομάδα, αφού δεν υπάρχει αντίστροφο για το $\bar{0}$.

3. Συμβολίζουμε με
$$\mathbb{Z}_n^\sharp = \{\bar{a} \in \mathbb{Z}_n : \ (a,n) = 1\} \ .$$
Η $(\mathbb{Z}_n^\sharp, \cdot)$ είναι αβελιανή ομάδα. Πράγματι, θα αποδείξουμε την ύπαρξη αντίστροφου στοιχείου. Έστω $\bar{a} \in \mathbb{Z}_n^\sharp$. Επειδή $(a,n) = 1$, έπεται ότι υπάρχουν κ και $\lambda \in \mathbb{Z}$, τέτοια ώστε $a\kappa + n\lambda = 1$. Επομένως
$$\overline{a\kappa + n\lambda} = \bar{1} \text{ και } \overline{a\kappa} = \bar{1}, \text{ δηλ. } \bar{a}\,\bar{\kappa} = \bar{1}.$$
Συμπεραίνουμε ότι η $\bar{k}$ είναι η αντίστροφη κλάση της $\bar{a}$ στο $\mathbb{Z}_n^\sharp$. Από τις ιδιότητες του πολλαπλασιασμού έπεται ότι η $(\mathbb{Z}_n^\sharp, \cdot)$ είναι αβελιανή ομάδα.

Η ***συνάρτηση του Euler*** (Euler's ϕ function) ορίζεται ως η συνάρτηση
$$\phi : \ \mathbb{N} \longrightarrow \mathbb{Z}, \ n \mapsto |\mathbb{Z}_n^\sharp|.$$
Όταν $n = p$ είναι πρώτος φυσικός αριθμός, τότε $\mathbb{Z}_p^\sharp = \mathbb{Z}_p \setminus \{\bar{0}\}$ και $\phi(p) = p - 1$.

4. Έστω F ένα σώμα, π.χ. $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ ή $\mathbb{Z}_p$, όπου p είναι πρώτος φυσικός αριθμός. Έστω $\mathcal{M}_n(K)$ το σύνολο των $n \times n$ πινάκων με συντελεστές από το σώμα F. Τότε $(\mathcal{M}_n(K), +)$ είναι μία αντιμεταθετική ομάδα.

5. Έστω F ένα σώμα. Τότε το σύνολο
$$\mathrm{GL}_n(K) = \{A \in \mathcal{M}_n(K) : \ \det(A) \neq 0\},$$
όπου $\det(A)$ είναι η ορίζουσα του πίνακα A, αποτελεί ομάδα με πράξη τον πολλαπλασιασμό πινάκων. Η ομάδα $\mathrm{GL}_n(K)$ λέγεται ***γενική γραμμική ομάδα*** (general linear group) και είναι αβελιανή αν και μόνο αν $n = 1$.

6. Έστω X ένα μη κενό σύνολο και S_X το σύνολο όλων των αμφιμονότιμων και επί συναρτήσεων $f : X \to X$. Το S_X λέγεται σύνολο των μετασχηματισμών του συνόλου X και αποτελεί ομάδα με πράξη τη σύνθεση συναρτήσεων. Η ομάδα S_X είναι εν γένει μη αβελιανή. Ιδιαίτερα, αν $X = \{x_1, \ldots, x_n\}$ τότε η ομάδα S_X συμβολίζεται S_n και λέγεται ***ομάδα των μεταθέσεων των n αντικειμένων*** (permutaion group of n elements). Η S_n είναι αβελιανή αν και μόνο αν $n \leq 2$.

7. Έστω G_1, G_2 δύο ομάδες. Το καρτεσιανό γινόμενο
$$G_1 \times G_2 = \{(g_1, g_2) : \ g_i \in G_i, \ i = 1, 2\}$$
γίνεται ομάδα με πράξη την
$$(g_1, g_2)(g_1', g_2') = (g_1 g_2, g_1' g_2').$$
Μοναδιαίο στοιχείο αυτής της ομάδας είναι το (e_1, e_2), όπου e_i είναι το μοναδιαίο στοιχείο των G_i, $i = 1, 2$ και
$$(g_1, g_2)^{-1} = (g_1^{-1}, g_2^{-1}).$$
Ανάλογα ορίζεται και η ομάδα $G_1 \times G_2 \times \cdots \times G_n$, όπου G_i είναι ομάδα, για $i = 1, \ldots, n$, και ο πολλαπλασιασμός ορίζεται κατά τις συντεταγμένες των στοιχείων. Η ομάδα $G_1 \times G_2 \times \cdots \times G_n$ λέγεται ***ευθύ εξωτερικό γινόμενο*** (external direct product) των ομάδων $G_1, \ldots, G_n$, για $n \geq 2$.

Είναι σημαντικό να γνωρίζουμε ποια υποσύνολα μίας ομάδας G αποτελούν ομάδα ως προς την ίδια πράξη. Ένα τέτοιο υποσύνολο λέγεται ***υποομάδα*** (subgroup) της G. Μία υποομάδα H της G συμβολίζεται με $H \leq G$ ή με $H < G$ όταν πρόκειται για ***γνήσια υποομάδα*** της G, δηλ. όταν $H \neq G$. Ακολουθεί ένα χρήσιμο για τις εφαρμογές κριτήριο.

Θεώρημα Ι.3. *Έστω $(G, \cdot)$ μία ομάδα και $H \subset G$.*

i. $H \leq G$ αν και μόνο αν $h_1 h_2^{-1} \in H$, για όλα τα $h_1, h_2 \in H$. Ισοδύναμα, $H \leq G$ αν και μόνο αν $h_1^{-1} h_2 \in H$, για όλα τα $h_1, h_2 \in H$.

ii. Ιδιαίτερα αν $|H| < \infty$, τότε $H \leq G$ αν και μόνο αν $h_1 h_2 \in H$, για όλα τα $h_1, h_2 \in H$.

Παραδείγματα Ι.4.

1. Έχουμε τις παρακάτω αλυσίδες υποομάδων της $(\mathbb{C}, +)$:

$$(\mathbb{Z}, +) < (\mathbb{Q}, +) < (\mathbb{R}, +) < (\mathbb{C}, +) \,,$$

$$(\mathbb{Q}^*, \cdot) < (\mathbb{R}^*, \cdot) < (\mathbb{C}^*, \cdot).$$

2. Έστω F ένα σώμα. Το σύνολο

$$\mathrm{SL}_n(K) = \{A \in \mathrm{GL}_n(K) : \ \det A = 1\}$$

είναι υποομάδα της $\mathrm{GL}_n(K)$.

3. Έστω $X \neq \emptyset$ ένα σύνολο και $Y \subset X$. Τότε $S_Y \leq S_X$.

Ιδιαίτερα, αν X είναι ο Ευκλείδειος χώρος $\mathbb{R}^2$ και V είναι το σύνολο των σημείων ενός γεωμετρικού σχήματος στο επίπεδο, η ομάδα S_Y λέγεται ***ομάδα συμμετρίας*** (symmetry group) του V. Έτσι για παράδειγμα έχουμε την ομάδα συμμετρίας του ισόπλευρου τριγώνου, του τετραγώνου, του κανονικού πολυγώνου, κ. λ. π.

Ορίζουμε τις ακέραιες δυνάμεις του τυχαίου στοιχείου μίας ομάδας G ως εξής:

$$a^n = \begin{cases} \overbrace{a \cdot a \cdots a}^{n \text{ φορές}} & \text{εάν } n \geq 1 \\ e & \text{εάν } n = 0 \\ (a^{-1})^{-n} & \text{εάν } n < 0. \end{cases}$$

Ιδιαίτερα, όταν η ομάδα $(G, +)$ είναι προσθετική, τότε οι δυνάμεις είναι τα πολλαπλάσια:

$$na = \begin{cases} \overbrace{a + a \cdots + a}^{n \text{ φορές}} & \text{εάν } n \geq 1 \\ 0 & \text{εάν } n = 0 \\ (-n)(-a) & \text{εάν } n < 0. \end{cases}$$

Οι βασικές ιδιότητες των δυνάμεων δίνονται στην επόμενη πρόταση.

Πρόταση Ι.5. *Έστω $(G, \cdot)$ μία ομάδα και $a \in G$. Τότε:*

i. $(a^{-1})^{-n} = (a^n)^{-1}$, $n \in \mathbb{Z}$.

ii. $a^n a^m = a^{n+m}$, $n, m \in \mathbb{Z}$.

iii. $(a^n)^m = a^{nm}$, $n, m \in \mathbb{Z}$.

Έστω $(G, \cdot)$ μία ομάδα και $g \in G$. Είναι εύκολο να διαπιστώσουμε ότι το σύνολο

$$\langle \mathbf{g} \rangle := \{g^s : \ s \in \mathbb{Z}\}$$

είναι υποομάδα της G. Η υποομάδα αυτή λέγεται ***κυκλική ομάδα*** (cyclic group) παραγόμενη από το $g \in G$. Βεβαίως είναι δυνατόν η ίδια η G να είναι κυκλική. Για παράδειγμα είναι εύκολο να διαπιστώσουμε ότι

$$(\mathbb{Z}, +) = \langle 1 \rangle = \langle -1 \rangle$$

και

$$(\mathbb{Z}_n, +) = \langle \bar{1} \rangle \ .$$

Ένα υποσύνολο X της πολλαπλασιαστικής ομάδας G λέγεται ***παράγον σύνολο*** (generating set) της G και συμβολίζουμε $G = \langle X \rangle$ ή $G = \langle x : \ x \in X \rangle$, αν

$$G = \{x_1^{\epsilon_1} \cdots x_s^{\epsilon_s} : \ x_i \in X, \ \epsilon_i = \pm 1, \ s \in \mathbb{N}\}.$$

Από το Θεμελιώδες Θεώρημα της Αριθμητικής διαπιστώνουμε ότι

$$(\mathbb{Q}, +) = \langle \frac{1}{n} : \ n \in \mathbb{N} \rangle,$$

ενώ

$$(\mathbb{Q}^*, \cdot) = \langle p : \ p \text{ είναι πρώτος φυσικός αριθμός} \rangle \ .$$

Έστω G μία ομάδα και $g \in G$. Είναι δυνατόν όλες οι ακέραιες δυνάμεις του στοιχείου g να είναι διακεκριμένες, οπότε $|\langle g \rangle| = \infty$. Αυτό συμβαίνει με το 1 της ομάδας $(\mathbb{Z}, +)$. Είναι δυνατόν όμως $|\langle g \rangle| < \infty$. Για παράδειγμα στην ομάδα $(\mathbb{C}^*, \cdot)$, η κυκλική υποομάδα που παράγεται από το i έχει τέσσερα στοιχεία:

$$\langle i \rangle = \{1, i, -1, -i\} \leq (\mathbb{C}^*, \cdot).$$

Είναι εύκολο να αποδείξει κανείς, ότι όταν οι δυνάμεις του g δεν είναι διακεκριμένες, τότε υπάρχει ακέραιος s τέτοιος ώστε $g^s = e$. Έτσι έχει νόημα ο επόμενος ορισμός.

Ορισμός Ι.6. *Έστω G μία ομάδα και $g \in G$. Αν $|\langle g \rangle| = \infty$, τότε λέμε ότι η **τάξη** (order) του g είναι άπειρη και γράφουμε $\mathrm{ord}(g) = \infty$. Αν $|\langle g \rangle| < \infty$ καλούμε **τάξη** (order) του g τον ελάχιστο φυσικό αριθμό $n \neq 0$ για τον οποίο $g^n = e$ και γράφουμε $\mathrm{ord}(g)$.*

Έτσι $\mathrm{ord}(i) = 4$ στην ομάδα $(\mathbb{C}^*, \cdot)$, ενώ $\mathrm{ord}(\bar{1}) = n$ στην ομάδα $(\mathbb{Z}_n, +)$. Η επόμενη πρόταση συγκεντρώνει τις κυριότερες ιδιότητες των τάξεων των στοιχείων μίας ομάδας.

Πρόταση Ι.7. *Έστω G μία ομάδα και $g \in G$. Τότε:*

i. $\mathrm{ord}(g) = |\langle g \rangle|$.

ii. *Έστω* $\mathrm{ord}(g) = n < \infty$. *Τότε, για* $\kappa, \lambda \in \mathbb{Z}$, $g^\kappa = g^\lambda \Leftrightarrow \kappa \equiv \lambda \bmod n$. *Ιδιαίτερα* $g^\kappa = e \Leftrightarrow \kappa \equiv 0 \bmod n$

iii. *Έστω* $\mathrm{ord}(g) = \infty$. *Τότε, για* $\kappa, \lambda \in \mathbb{Z}$, $g^\kappa = g^\lambda \Leftrightarrow \kappa = \lambda$.

iv. Για $\kappa \in \mathbb{Z}$, ισχύει

$$\operatorname{ord}(g^\kappa) = \frac{n}{(n,\kappa)},$$

όπου $(n,k) = ΜΚΔ(n,\kappa)$.

v. Έστω $\operatorname{ord}(g) = n < \infty$. Τότε $\langle g\rangle = \langle g^\kappa\rangle$, αν και μόνο αν $(n,\kappa) = 1$.

vi. Έστω $g, h \in G$. Τότε

$$\operatorname{ord}(g) = \operatorname{ord}(g^{-1}),\ \ \operatorname{ord}(gh) = \operatorname{ord}(hg) \text{ και } \operatorname{ord}(ghg^{-1}) = \operatorname{ord}(h).$$

vii. Έστω $g, h \in G$ έτσι ώστε $gh = hg$ και $(\operatorname{ord}(g), \operatorname{ord}(h)) = 1$. Τότε

$$\operatorname{ord}(gh) = \operatorname{ord}(g)\operatorname{ord}(h).$$

Ιδιαίτερα, όταν η ομάδα G είναι κυκλική, συμπεραίνουμε τα εξής:

Πρόταση Ι.8. *Έστω $G = \langle g\rangle$ μία κυκλική ομάδα.*

i. Έστω $\operatorname{ord}(g) = \infty$. Τότε $G = \langle g\rangle = \langle g^k\rangle \Leftrightarrow k = \pm 1$.

ii. Έστω $\operatorname{ord}(g) = n < \infty$. Τότε $G = \langle g\rangle = \langle g^k\rangle \Leftrightarrow (n,k) = 1$, δηλ. η G έχει $\phi(n)$ πλήθους στοιχεία που την παράγουν, όπου ϕ είναι η συνάρτηση του Euler.

Παράδειγμα Ι.9. $\mathbb{Z}_8^\sharp = \{\bar{1}, \bar{3}, \bar{5}, \bar{7}\}$ και $\phi(8) = 4$. Αφού η τάξη των $\bar{3}$, $\bar{5}$, $\bar{7}$ είναι ίση με 2, η ομάδα $\mathbb{Z}_8^\sharp$ δεν είναι κυκλική.

Ένα από τα σημαντικότερα θεωρήματα της Θεωρίας Ομάδων είναι το Θεώρημα του Lagrange. Το θεώρημα αυτό παρέχει για τις πεπερασμένες ομάδες την εξαιρετική πληροφορία ότι η τάξη κάθε υποομάδας διαιρεί την τάξη της ομάδας.

Θεώρημα Ι.10 (Lagrange). *Έστω G μία ομάδα και $H \leq G$.*

i. Η σχέση $a \sim b \Leftrightarrow a^{-1}b \in H$, για $a, b \in G$, είναι σχέση ισοδυναμίας στο σύνολο G. Η κλάση ισοδυναμίας που περιέχει το $a \in G$ είναι το σύνολο $\bar{a} = aH = \{ah :\ h \in H\}$. Ισχύει ότι

$$G = \bigcup_{a\in X} aH,$$

όπου X είναι ένα πλήρες σύστημα αντιπροσώπων της σχέσης αυτής. Ακόμη $|H| = |aH|$, για $a \in G$.

ii. Η σχέση $a \sim b \Leftrightarrow ba^{-1} \in H$, $a, b \in G$, είναι σχέση ισοδυναμίας στο σύνολο G. Η κλάση ισοδυναμίας που περιέχει το $a \in G$ είναι το σύνολο $\bar{a} = Ha$ και

$$G = \bigcup_{a\in Y} Ha,$$

όπου Y είναι ένα πλήρες σύστημα αντιπροσώπων της σχέσης αυτής. Ακόμη $|H| = |Ha|$, $a \in G$.

iii. Τα σύνολα X και Y που εμφανίζονται παραπάνω έχουν την ίδια πληθυκότητα την οποία συμβολίζουμε με $[G : H]$. Ισχύει η ισότητα

$$|G| = [G : H]|H|\ .$$

iv. Αν η ομάδα G είναι πεπερασμένη, τότε η τάξη κάθε υποομάδας της H διαιρεί την τάξη της G.

Το σύνολο aH (αντίστοιχα Ha), $a \in G$, λέγεται ***αριστερή κλάση*** (αντίστοιχα ***δεξιά κλάση***) (right and left cosets) της H στη G και η πληθυκότητα $[G : H]$ λέγεται ***δείκτης*** (index) της H στην G. Παρατηρούμε ότι ο δείκτης $[G : H]$ μπορεί να είναι πεπερασμένος αριθμός, μπορεί και όχι, π.χ. $[\mathbb{Z} : \mathbb{Z}_n] = n < \infty$, ενώ $[\mathbb{Q} : \mathbb{Z}] = \infty$. Αν η ομάδα G είναι αβελιανή είναι φανερό ότι $aH = Ha$, για κάθε $a \in G$ και για κάθε $H \leq G$. Αυτό, όμως, δεν συμβαίνει πάντα. Έτσι έχει νόημα ο παρακάτω ορισμός.

Ορισμός Ι.11. *Μία υποομάδα H της G λέγεται **κανονική** (normal) και συμβολίζουμε $H \trianglelefteq G$, αν*

$$aH = Ha \ , \ \textit{για κάθε } a \in G.$$

Ισοδύναμα, μία υποομάδα H είναι κανονική αν και μόνο αν $aHa^{-1} = H$, για κάθε $a \in G$. Γράφουμε $H \lhd G$, αν η H είναι γνήσια κανονική υποομάδα της G.

Η σημαντικότητα της κανονικής υποομάδας φαίνεται από το επόμενο θεώρημα.

Θεώρημα Ι.12. *Έστω G μία ομάδα και $H \leq G$. Η υποομάδα H είναι κανονική αν και μόνο αν το σύνολο*

$$G/H := \{aH : \ a \in G\}$$

αποτελεί ομάδα, με πράξη

$$(a_1H) \cdot (a_2H) = (a_1a_2)H.$$

Το μοναδιαίο στοιχείο της G/H είναι το H, ενώ $(aH)^{-1} = a^{-1}H$, για $a \in G$.

Όταν $H \trianglelefteq G$, η ομάδα G/H λέγεται ***ομάδα πηλίκο*** (quotient group) της H στην G. Το αποτέλεσμα της πράξης $(a_1H) \cdot (a_2H)$ είναι ανεξάρτητο της επιλογής των αντιπροσώπων a_1, a_2. Έτσι αν $b_1 \in a_1H$ και $b_2 \in b_2H$, τότε

$$(a_1H) \cdot (a_2H) = (a_1a_2)H = (b_1b_2)H \ .$$

Οι υποομάδες της G/H είναι της μορφής N/H, όπου N υποομάδα της G που περιέχει την H. Είναι εύκολο να δούμε ότι:

(i) $n\mathbb{Z} \lhd \mathbb{Z}$ και $\mathbb{Z}/n\mathbb{Z} = \{a + n\mathbb{Z} : \ a \in \mathbb{Z}\} = \mathbb{Z}_n$

(ii) $\mathrm{SL}_n(\mathbb{Q}) \lhd \mathrm{GL}_n(\mathbb{Q})$.

Σημειώνουμε την επόμενη παρατήρηση.

Παρατήρηση Ι.13.

i. Κάθε υποομάδα αβελιανής ομάδας είναι αβελιανή.

ii. Έστω G μία ομάδα και $H \leq G$ με $[G : H] = 2$. Τότε $H \trianglelefteq G$.

Από το Θεώρημα του Lagrange (Θεώρημα Ι.10) και τις ιδιότητες των κυκλικών ομάδων έχουμε το παρακάτω θεώρημα.

Θεώρημα Ι.14.

i. Κάθε υποομάδα κυκλικής ομάδας είναι κυκλική.

ii. *Έστω $G = \langle a \rangle$ μία πεπερασμένη κυκλική ομάδα με τάξη n. Για κάθε φυσικό αριθμό m που διαιρεί το n, υπάρχει μοναδική υποομάδα H της G με τάξη m και $H = \langle a^{n/m} \rangle$.*

iii. *Κάθε ομάδα τάξης p, όπου p είναι πρώτος φυσικός αριθμός, είναι κυκλική.*

iv. **(Fermat)** *Αν p είναι πρώτος φυσικός αριθμός, τότε $a^{p-1} \equiv 1 \bmod p$, για κάθε $a \in \mathbb{Z}$.*

Στη συνέχεια εξετάζουμε τις συναρτήσεις μεταξύ ομάδων. Έστω $(G, \cdot)$ και $(H, *)$ ομάδες και $f : G \to H$ μία συνάρτηση. Η f λέγεται ***ομομορφισμός*** (homomorphism) αν

$$f(a \cdot b) = f(a) * f(b).$$

Ιδιαίτερα αν $G = H$, τότε ο f λέγεται ***ενδομορφισμός*** Ο ομομορφισμός $f : G \to H$ λέγεται ***επιμορφισμός*** (epimorphism) αν η f είναι επί συνάρτηση. Ο ομομορφισμός $f : G \to H$ λέγεται ***μονομορφισμός*** (monomorphism) αν η f είναι αμφιμονότιμη συνάρτηση. Σε αυτήν την περίπτωση, η f λέγεται επίσης ***εμφύτευση*** (embedding) και λέμε ότι η G εμφυτεύεται στην H. Συχνά, η εμφύτευση συμβολίζεται ως $\hookrightarrow$. Ο ομομορφισμός $f : G \to H$ λέγεται ***ισομορφισμός*** (isomorphism) αν η f είναι αμφιμονότιμη και επί συνάρτηση. Σε αυτήν την περίπτωση, λέμε ότι οι ομάδες G, H είναι ***ισόμορφες*** (isomorphic) και συμβολίζουμε $G \cong H$. Ιδιαίτερα, αν $G = H$, τότε ο f λέγεται ***αυτομορφισμός*** (automorphism). (endomorphism).

Το σύνολο

$$\ker f := \{a \in G : \ f(a) = e\} \subset G$$

λέγεται ***πυρήνας*** (kernel) του f. Το σύνολο

$$\operatorname{Im} f := \{f(a) : \ a \in G\} \subset H$$

λέγεται ***εικόνα*** (image) του f. Η επόμενη πρόταση συγκεντρώνει τις βασικότερες ιδιότητες των ομομορφισμών ομάδων.

Πρόταση Ι.15. *Έστω $f : G \to H$ ομομορφισμός ομάδων.*

i. *$f(e) = e$ και $f(a^{-1}) = f(a)^{-1}$, για κάθε $a \in G$.*

ii. *$\ker f \trianglelefteq G$, $\operatorname{Im} f \leq H$.*

iii. *$\ker f = \{e\}$ αν και μόνο αν f είναι μονομορφισμός.*

iv. *Η G εμφυτεύεται στην H αν και μόνον αν η G είναι ισόμορφη με υποομάδα της H.*

v. *Αν $a \in G$ και $\operatorname{ord}(f(a)) = \infty$, τότε $\operatorname{ord}(a) = \infty$.*

vi. *Αν $a \in G$ και $\operatorname{ord}(f(a)) < \infty$, τότε $\operatorname{ord}(f(a)) | \operatorname{ord}(a)$.*

vii. *Αν ο f είναι μονομορφισμός και $a \in G$, τότε $\operatorname{ord}(f(a)) = \operatorname{ord}(a)$.*

Ο ομομορφισμός ομάδων δίνει σημαντικά εργαλεία για τη σύγκριση ομάδων και η ταξινόμηση όλων των ομάδων με προσέγγιση ισομορφίας είναι ο κύριος στόχος της Θεωρίας Ομάδων. Τα επόμενα θεωρήματα δίνουν πληροφορίες προς αυτήν την κατεύθυνση της οποίας η τελική διαδρομή είναι ακόμη άγνωστη.

Θεώρημα Ι.16. *Το σύνολο των αυτομορφισμών μίας ομάδας G, με πράξη τη σύνθεση συναρτήσεων, αποτελεί ομάδα που συμβολίζεται με $\operatorname{Aut}(G)$.*

Αναφέραμε νωρίτερα την ομάδα μετασχηματισμών ενός συνόλου. Το επόμενο θεώρημα δείχνει ότι η μελέτη της είναι ιδιαίτερου ενδιαφέροντος.

Θεώρημα Ι.17 (Cayley). *Κάθε ομάδα G εμφυτεύεται στην ομάδα S_G των μετασχηματισμών του συνόλου της. Ιδιαίτερα, αν η ομάδα G είναι πεπερασμένη και $|G| = n$, τότε $G \hookrightarrow S_n$.*

Για τις κυκλικές ομάδες έχουμε το παρακάτω θεώρημα.

Θεώρημα Ι.18. *i. Κάθε κυκλική ομάδα άπειρης τάξης είναι ισόμορφη με την $(\mathbb{Z}, +)$.*

ii. Κάθε κυκλική ομάδα πεπερασμένης τάξης $n < \infty$ είναι ισόμορφη με την $(\mathbb{Z}_n, +)$.

iii. Η $\mathrm{Aut}(\mathbb{Z})$ είναι κυκλική ομάδα τάξης 2.

iv. Η $\mathrm{Aut}(\mathbb{Z}_n)$ είναι αβελιανή ομάδα τάξης $\phi(n)$ και είναι ισόμορφη με την $(\mathbb{Z}_n^\sharp, \cdot)$.

v. Έστω $m, n \in \mathbb{N}$. Τότε

$$(\mathbb{Z}_m \times \mathbb{Z}_n, +) \cong (\mathbb{Z}_{mn}, +) \Leftrightarrow (m, n) = 1 \ .$$

Στη συνέχεια αναφέρουμε τα Θεωρήματα Ισομορφίας ομάδων. Αν K, N είναι υποομάδες της ομάδας G, με KN εννοούμε το σύνολο $KN = \{kn : \ k \in K, n \in N\}$.

Θεώρημα Ι.19 (Πρώτο Θεώρημα Ισομορφίας Ομάδων)**.** *Έστω $f : \ G \to H$ ένας ομομορφισμός ομάδων. Τότε*

$$G/\ker f \cong \mathrm{Im}\, f \ , \text{όπου } g \ker f \mapsto f(g) \ .$$

Θεώρημα Ι.20 (Δεύτερο Θεώρημα Ισομορφίας Ομάδων)**.** *Έστω G μία ομάδα, $N, K \leq G$ και $N \trianglelefteq G$. Τότε*

i. $KN \leq G$ και $K \cap N \trianglelefteq K$.

ii. $KN/N \ \cong \ K/K \cap N$.

Θεώρημα Ι.21 (Τρίτο Θεώρημα Ισομορφίας Ομάδων)**.** *Έστω G μία ομάδα, $N, H \trianglelefteq G$ και $N \leq H \leq G$. Τότε*

i. $H/N \trianglelefteq G/N$.

ii. $(G/N)\big/(H/N) \ \cong \ G/H$.

Το επόμενο θεώρημα χαρακτηρίζει τις ομάδες που είναι ισόμορφες με το ευθύ εξωτερικό γινόμενο υποομάδων τους.

Θεώρημα Ι.22. *Έστω G μία ομάδα και $H, K \leq G$. Η G είναι ισόμορφη με την ομάδα $H \times K$ αν και μόνο αν ισχύουν οι παρακάτω τρεις συνθήκες:*

i. $H \trianglelefteq G$, $K \trianglelefteq G$,

ii. $H \cap K = \{e\}$,

iii. $G = HK$.

Ισοδύναμα, $G \cong H \times K$ αν και μόνον αν

i. τα στοιχεία της H αντιμεταθέτονται με τα στοιχεία της F και

ii. κάθε στοιχείο της G γράφεται μοναδικά ως γινόμενο hk, για κάποια $h \in H$ και $k \in K$.

Δεν είναι δύσκολο να αποδείξει κανείς το επόμενο συμπέρασμα.

Πρόταση Ι.23. *i) Με προσέγγιση ισομορφίας, υπάρχουν ακριβώς δύο ομάδες τάξης 4:*

- *η $(\mathbb{Z}_4, +)$,*
- *η $(\mathbb{Z}_2 \times \mathbb{Z}_2, +)$, η οποία λέγεται **ομάδα του Klein**.*

ii) Με προσέγγιση ισομορφίας, υπάρχουν ακριβώς δύο ομάδες τάξης 6:

- *η $(\mathbb{Z}_6, +)$,*
- *η $(S_3, \circ)$.*

Τα Θεωρήματα του Sylow

Ένα εύλογο ερώτημα αφορά την ισχύ του αντίστροφου του Θεωρήματος του Lagrange. Αν μία ομάδα έχει τάξη $n < \infty$ και $m|n$, υπάρχει υποομάδα της τάξης m; Τα θεωρήματα του Sylow προσφέρουν μία ικανοποιητική απάντηση σε αυτό το ερώτημα. Συγκεντρώνουμε τα θεωρήματα αυτά παρακάτω:

Θεώρημα I.24 (Sylow). *Έστω G μία ομάδα τάξης $n < \infty$ και $n = p^s m$, όπου p πρώτος και $p \nmid m$. Με $N_p(t)$ συμβολίζουμε το πλήθος των υποομάδων της G που έχουν τάξη p^t.*

i. Υπάρχουν υποομάδες της G με τάξη p^t, $0 \leq t \leq s$, και $N_p(t) \equiv 1 \bmod p$.

*ii. Οι υποομάδες τάξης p^s της G είναι **συζυγείς**, δηλ. αν H_1, H_2 είναι δύο τέτοιες υποομάδες, τότε υπάρχει $g \in G$ τέτοιο ώστε $H_1 = gHg^{-1}$. (Οι υποομάδες τάξης p^s της G λέγονται* **Sylow p-υποομάδες***).*

iii. $N_p(s)|m$.

Για $t = 1$, από το Θεώρημα I.24,(i), προκύπτει ότι αν p διαιρεί την τάξη της G, όπου p πρώτος, τότε υπάρχει υποομάδα της G με τάξη p. Έτσι σύμφωνα με το Θεώρημα I.14, η υποομάδα αυτή είναι κυκλική και, επομένως, η G έχει ένα στοιχεία τάξης p. Έτσι προκύπτει το επόμενο Θεώρημα του Cauchy.

Θεώρημα I.25 (Cauchy). *Έστω G πεπερασμένη ομάδα, p πρώτος έτσι ώστε p διαιρεί $|G|$. Υπάρχει στοιχείο $g \in G$ τάξης p, δηλ. $\mathrm{ord}(g) = p$.*

Παραδείγματα I.26.

1. Έστω G μία ομάδα τάξης 15. Θα αποδείξουμε ότι η G είναι κυκλική και συνεπώς $G \cong \mathbb{Z}_{15}$. Από το Θεώρημα I.24,(i), υπάρχει τουλάχιστον μία υποομάδα, έστω G_3 της G, τάξης 3 και μία υποομάδα, έστω G_5, της G, τάξης 5. Τότε $N_3(1) \equiv 1 \bmod 3$ και $N_3(1) \mid 5$, άρα $N_3(1) = 1$. Ομοίως, $N_5(1) = 1$. Επομένως, οι G_3 και G_5, ως μοναδικές 3-Sylow και 5-Sylow αντίστοιχα υποομάδες, είναι κανονικές, αφού ταυτίζονται με τις συζυγείς τους, Θεώρημα I.24,(ii). Σύμφωνα με το Θεώρημα I.18, οι G_3 και G_5 είναι κυκλικές. Επίσης $G_3 \cap G_5 = \{e\}$, αφού ως υποομάδα της G_3 και της G_5 η τάξη της διαιρεί το 3 και το 5, (Θεώρημα I.14). Συνεπώς, σύμφωνα με τα Θεωρήματα I.22 και I.18, προκύπτει ότι

   $$G \cong G_3 \times G_5 \cong \mathbb{Z}_3 \times \mathbb{Z}_5 \cong \mathbb{Z}_{15} \ ,$$

   δηλ. η G είναι κυκλική.

2. Μία ομάδα G λέγεται ***απλή*** (simple) αν δεν έχει κανονική υποομάδα διάφορη των $\{e\}$ και G. Θα αποδείξουμε ότι οι μόνες απλές αβελιανές ομάδες είναι οι ομάδες τάξης πρώτου αριθμού.

   Πράγματι, έστω G μία αβελιανή ομάδα τάξης p, όπου p είναι πρώτος φυσικός αριθμός. Από το Θεώρημα I.10, δεν υπάρχει υποομάδα της G διάφορη των $\{e\}$ και G. Αντίστροφα, αν η G είναι αβελιανή ομάδα τάξης $n < \infty$ και ο n δεν είναι πρώτος αριθμός, τότε υπάρχει πρώτος $p < n$ τέτοιος ώστε $p|n$. Από το Θεώρημα I.24 υπάρχει υποομάδα $H < G$ με $|H| = p$. Επίσης, $H \lhd G$, αφού η G είναι αβελιανή. Επομένως η G δεν είναι απλή.

Επιλύσιμες Ομάδες

Έστω G μία πεπερασμένα ομάδα. ***Κανονική σειρά*** (normal series) της G λέγεται μία ακολουθία υποομάδων G_i, $0 \leq i \leq s$, της G ως εξής:

$$G = G_0 \rhd G_1 \cdots \rhd G_{s-1} \rhd G_s = \{e\}.$$

Ο φυσικός αριθμός s λέγεται ***μήκος της σειράς*** (length) και οι ομάδες G_i/G_{i+1}, $0 \leq i \leq s-1$, λέγονται ***παράγοντες της σειράς*** (factors). Ιδιαίτερα, αν οι παράγοντες της κανονικής σειράς είναι αβελιανές ομάδες, τότε η σειρά λέγεται ***επιλύσιμη*** (solvable). Μία πεπερασμένη ομάδα G που έχει μία επιλύσιμη σειρά λέγεται ***επιλύσιμη*** (solvable).

Παραδείγματα I.27.

1. Η ομάδα G τάξης 15 με τους συμβολισμούς του Παραδείγματος I.26,1 είναι επιλύσιμη, αφού η σειρά της G
$$G \rhd G_3 \rhd \{e\}$$
έχει τις ιδιότητες:
$$G/G_3 \cong \mathbb{Z}_5 \text{ και } G_3 \cong \mathbb{Z}_3.$$

2. Κάθε πεπερασμένη αβελιανή ομάδα είναι επιλύσιμη. Πράγματι, η
$$G \lhd \{e\}$$
είναι μία επιλύσιμη σειρά.

Με χρήση των Θεωρημάτων του Sylow και της μαθηματικής επαγωγής, αποδεικνύεται το παρακάτω χρήσιμο θεώρημα.

Θεώρημα I.28. *Έστω G μία πεπερασμένη p-ομάδα, δηλ. μία ομάδα με $|G| = p^n$, για κάποιον πρώτο φυσικό αριθμό p και κάποιον φυσικό αριθμό n. Τότε υπάρχει μία κανονική σειρά υποομάδων G_i, $0 \leq i \leq s$, της G*

$$G = G_0 \rhd G_1 \cdots \rhd G_{s-1} \rhd G_s = \{e\}$$

έτσι ώστε $|G_i/G_{i+1}| = p$.

Το επόμενο θεώρημα συγκεντρώνει τις κυριότερες ιδιότητες των επιλύσιμων ομάδων.

Θεώρημα I.29. *i. Μία πεπερασμένη ομάδα G είναι επιλύσιμη αν και μόνο αν έχει μία κανονική σειρά τέτοια ώστε κάθε παράγοντας της σειράς να είναι ομάδα τάξης πρώτου αριθμού.*

ii. Κάθε υποομάδα επιλύσιμης ομάδας είναι επιλύσιμη.

iii. Κάθε ομάδα πηλίκο επιλύσιμης ομάδας είναι επιλύσιμη.

iv. Το ευθύ γινόμενο πεπερασμένου πλήθους πεπερασμένων επιλύσιμων ομάδων είναι επιλύσιμη ομάδα.

v. Η ομομορφική εικόνα επιλύσιμης ομάδας είναι επιλύσιμη ομάδα.

Η ομάδα S_n

Στο εδάφιο αυτό εξετάζουμε την ομάδα S_n. Από τον ορισμό της η S_n, ως σύνολο των μεταθέσεων n αντικειμένων, έχει $n!$ στοιχεία. Για ευκολία συμβολίζουμε τα αντικείμενα αυτά ως $1, 2, \ldots, n$. Έστω $\sigma \in S_n$. Ένα στοιχείο $\sigma \in S_n$ μπορούμε να το συμβολίσουμε ως

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix},$$

όπου αν $\sigma(n) = n$, τότε το σ μπορεί να θεωρηθεί ως στοιχείο της S_{n-1}, παραλείποντας την πληροφορία $\sigma(n) = n$. Έτσι μπορούμε να θεωρήσουμε τις διαδοχικές εμφυτεύσεις

$$S_1 \hookrightarrow S_2 \hookrightarrow \cdots \hookrightarrow S_{n-1} \hookrightarrow S_n$$

και επομένως να θεωρούμε ότι

$$S_1 < S_2 < \cdots < S_{n-1} < S_n.$$

Επίσης στην παράσταση του στοιχείου σ μπορούμε να παραλείπουμε τα στοιχεία του συνόλου $\{1, 2, \ldots, n\}$ που μένουν σταθερά από τη σ, αν βέβαια αυτό δεν δημιουργεί παρανοήσεις. ***Κυκλική μετάθεση*** ή ***κύκλος*** (cycle) λέγεται ένα στοιχείο της S_n της μορφής

$$\tau := \begin{pmatrix} i_1 & i_2 & \cdots & i_{s-1} & i_s \\ i_2 & i_3 & \cdots & i_s & i_1 \end{pmatrix},$$

όπου $\{i_1, i_2, \ldots, i_s\} \subseteq \{1, 2, \ldots, n\}$. Η κυκλική μετάθεση τ συμβολίζεται ως $(i_1 i_2 \cdots i_s)$ και ο αριθμός s λέγεται ***μήκος*** (length) της σ. Ένας κύκλος μήκους 2 λέγεται ***αντιμετάθεση*** (transposition). Η ομάδα S_n είναι μη αντιμεταθετική για $n \geq 2$. Όμως, εύκολα διαπιστώνουμε ότι αν

$$\sigma := \begin{pmatrix} i_1 & i_2 & \cdots & & i_t \\ \sigma(i_1) & \sigma(i_2) & \cdots & \sigma(i_t) & \end{pmatrix}, \quad \tau := \begin{pmatrix} j_1 & j_2 & \cdots & j_s \\ \sigma(j_1) & \sigma(j_2) & \cdots & \sigma(j_s) \end{pmatrix},$$

όπου $\{i_1, \ldots, i_t\}$, $\{j_1, \ldots, j_s\}$ είναι ξένα μεταξύ τους υποσύνολα του $\{1, 2, \ldots, n\}$, τότε $\sigma\tau = \tau\sigma$. Τότε οι μεταθέσεις σ, τ λέγονται ***μεταθέσεις ξένες μεταξύ τους*** (disjoint permutions). Η επόμενη πρόταση είναι σημαντική για την περιγραφή στοιχείων της S_n.

Πρόταση Ι.30. *i. Κάθε στοιχείο $\sigma \in S_n$ αναλύεται σε γινόμενο κυκλικών μεταθέσεων ξένων μεταξύ τους ανά δύο. Η ανάλυση αυτή είναι μοναδική με προσέγγιση αντιμετάθεσης των παραγόντων της.*

ii. Η τάξη μίας κυκλικής μετάθεσης ισούται με το μήκος της.

iii. Έστω $\sigma = \sigma_1\sigma_2 \cdots \sigma_k$ η ανάλυση μίας μετάθεσης σε γινόμενο κύκλων ξένων μεταξύ τους ανά δύο. Τότε

$$\mathrm{ord}(\sigma) = \mathit{ΕΚΠ}(\mathrm{ord}(\sigma), \ldots, \mathrm{ord}(\sigma_k)).$$

*iv. Δύο στοιχεία σ, τ της S_n είναι **συζυγή** (conjugate), δηλ. $\sigma = f\tau f^{-1}$, για κάποιο $f \in S_n$, αν και μόνο αν τα σ, τ έχουν την ίδια δομή ως γινόμενα κυκλικών μεταθέσεων ξένων μεταξύ τους ανά δύο.*

Παράδειγμα Ι.31. Έστω $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 2 & 5 & 4 \end{pmatrix}$, τότε $\sigma = (132)(45) = (45)(132)$. Αν $\tau = (15) \in S_5$ τότε

$$\tau\sigma\tau^{-1} = (532)(41).$$

Έστω $\sigma \in S_n$. Θεωρούμε το πολυώνυμο

$$f(x_1, x_2, \ldots, x_n) = \prod_{\substack{i>j \\ 1\le i,j\le n}} (x_i - x_j)$$

με n ανεξάρτητες μεταβλητές και συμβολίζουμε

$$\sigma f(x_1 \ldots, x_n) = \prod_{\substack{i>j \\ 1\le i,j\le n}} (x_{\sigma(i)} - x_{\sigma(j)}) = \pm f(x_1, \ldots, x_n).$$

Αν $\sigma f(x_1, \ldots, x_n) = f(x_1, \ldots, x_n)$, τότε η σ λέγεται ***άρτια*** (even) μετάθεση, διαφορετικά λέγεται ***περιττή*** (odd). Το σύνολο των άρτιων μεταθέσεων συμβολίζεται με A_n. Η επόμενη πρόταση είναι ιδιαίτερα χρήσιμη.

Πρόταση Ι.32. *i.* $A_n \lhd S_n$ *και* $S_n/A_n \cong \mathbb{Z}_2$.

ii. Για έναν κύκλο $(i_1 \cdots i_s)$, *ισχύει* $(i_1 i_2 \cdots i_s) = (i_1 i_s)(i_2 i_s) \cdots (i_{s-1} i_s)$.

iii. Κάθε $\sigma \in S_n$ *αναλύεται σε γινόμενο αντιμεταθέσεων. Η ανάλυση αυτή δεν είναι μοναδική. Ακόμη, ένα στοιχείο της* S_n *είναι άρτια μετάθεση αν και μόνο αν είναι γινόμενο άρτιου πλήθους αντιμεταθέσεων.*

iv. $S_n = \langle\, (ij) :\ 1 \le i, j \le n \,\rangle = \langle\, (12), (13), \ldots, (1n) \,\rangle$.

v. $S_n = \langle\, (12), (12 \cdots n) \,\rangle$.

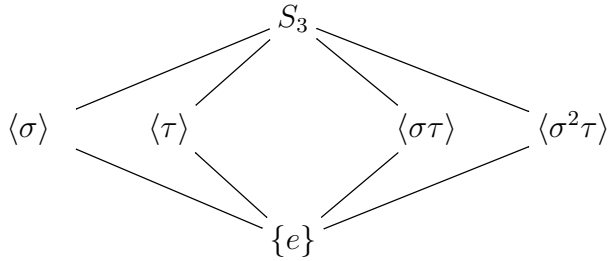
vi. $A_n = \langle\, (abc) :\ a, b, c \in \{1, 2, \ldots, n\} \,\rangle = \langle\, (123), (124), \ldots, (12n) \,\rangle$.

Στη συνέχεια εξετάζουμε λεπτομερέστερα την ομάδα S_3.

Παράδειγμα Ι.33. Παρατηρούμε ότι αν $\sigma := (123)$ και $\tau := (12)$, τότε

$$S_3 = \{e, \sigma, \sigma^2, \tau, \sigma\tau, \sigma^2\tau\}\ ,\ \text{δηλ.}\ S_3 = \langle \sigma, \tau \rangle.$$

Το διάγραμμα των υποομάδων της S_3 είναι



Η μόνη γνήσια κανονική υποομάδα της S_3, διάφορη της $\{e\}$, είναι η $\langle\sigma\rangle$. Η S_3 είναι επιλύσιμη με επιλύσιμη σειρά

$$S_3 \rhd \langle\sigma\rangle \rhd \{e\}\ .$$

Ας έλθουμε τώρα στην S_4.

Παράδειγμα Ι.34. Έστω

$$K = \{\, e, (12)(34), (13)(24), (14)(23) \,\} \subset S_4.$$

Είναι εύκολο να διαπιστώσουμε ότι $K < A_4$. Επίσης, $K \lhd S_4$, αφού σύμφωνα με την Πρόταση Ι.30, όλα τα συζυγή των στοιχείων της K είναι της ίδιας μορφής όπως τα στοιχεία

της K και άρα ανήκουν στη K. Άρα $K \lhd A_4$. Αφού $|K| = 4$, έπεται ότι K είναι αβελιανή ομάδα και επομένως όλες οι υποομάδες της K είναι κανονικές. Έτσι, αν $\sigma = (12)(34)$ τότε $\langle\sigma\rangle \lhd K$. Επομένως, έχουμε την κανονική σειρά

$$S_4 \rhd A_4 \rhd K \rhd \langle\sigma\rangle \rhd \{e\},$$

η οποία είναι επιλύσιμη γιατί

$$S_4/A_4 \cong \mathbb{Z}_2 \ , \ A_4/K \cong \mathbb{Z}_3 \ , \ K/\langle\sigma\rangle \cong \mathbb{Z}_2 \ , \ \langle\sigma\rangle \cong \mathbb{Z}_2.$$

Άρα η S_4 είναι επιλύσιμη ομάδα. Τέλος παρατηρούμε ότι $S_4 = \langle\, (12), (1234)\,\rangle$.

Για $n \geq 5$, συγκεντρώνουμε κάποιες από τις ιδιότητες της S_n στο παρακάτω θεώρημα.

Θεώρημα Ι.35. *i. Η S_5 παράγεται από μία τυχαία αντιμετάθεση και έναν τυχαίο κύκλο μήκους 5.*

ii. Η ομάδα S_n δεν είναι επιλύσιμη για $n \geq 5$.

iii. Η ομάδα A_n των άρτιων μεταθέσεων της S_n είναι απλή για $n \geq 5$.

ΙΙ Αντιμεταθετικοί Δακτύλιοι

Ένα μη κενό σύνολο R εφοδιασμένο με δύο πράξεις, την πρόσθεση $(+)$ και τον πολλαπλασιασμό $(\cdot)$, λέγεται ***αντιμεταθετικός δακτύλιος*** (commutative ring) με μοναδιαίο στοιχείο, αν ικανοποιούνται τα επόμενα:

α. $(R, +)$ είναι μία αβελιανή ομάδα (με 0 συμβολίζουμε το μηδενικό της στοιχείο).

β. $a(bc) = (ab)c$, για όλα τα $a, b, c \in R$.

γ. Υπάρχει $1 \in R$, έτσι ώστε $1 \neq 0$ και $a \cdot 1 = a = 1 \cdot a$, για όλα τα $a \in R$.

δ. $ab = ba$, για όλα τα $a, b \in R$.

ε. $a(b + c) = ab + ac$ και $(a + b)c = ac + bc$, για ολα τα $a, b, c \in R$.

Εάν επιπλέον η $(R \setminus \{0\}, \cdot)$ είναι πολλαπλασιαστική ομάδα, τότε ο R λέγεται ***σώμα*** (field). Με a^{-1} συμβολίζουμε το αντίστροφο του στοιχείου $a \in R \setminus 0$, αν αυτό υπάρχει. Συμβολίζουμε με $U(R)$ το σύνολο των αντρέψιμων στοιχείων του R, δηλ.

$$U(R) := \{a \in R : \ \exists\, b \in R, ab = 1\}.$$

Το σύνολο $(U(R), \cdot)$ είναι ομάδα, ενώ ο R είναι σώμα αν και μόνο αν $U(R) = R \setminus \{0\}$. Συμβολίζουμε με R^* το σύνολο $R \setminus \{0\}$.

Οι δακτύλιοι $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ είναι σώματα. Ο αντιμεταθετικός δακτύλιος $\mathbb{Z}$ δεν είναι σώμα και $U(\mathbb{Z}) = \{\pm 1\}$. Ο αντιμεταθετικός δακτύλιος $\mathbb{Z}_n$ είναι σώμα αν και μόνο αν n είναι πρώτος φυσικός αριθμός, αφού

$$U(\mathbb{Z}_n) = \{\overline{m} : \ (m, n) = 1\} = \mathbb{Z}_n^* \text{ αν και μόνο αν } n \text{ είναι πρώτος.}$$

Ένα μη κενό υποσύνολο S του αντιμεταθετικού δακτυλίου R λέγεται ***υποδακτύλιος*** (subring) του R και γράφουμε $S \leq R$, αν το S αποτελεί δακτύλιο ως προς τις πράξεις του R. Ένα μη κενό υποσύνολο A του σώματος K λέγεται ***υπόσωμα*** (subfield) του K και γράφουμε $A \leq K$, αν το A ως προς τις πράξεις του F είναι σώμα. Παραθέτουμε ένα κριτήριο που ελαχιστοποιεί τον σχετικό έλεγχο για τους υποδακτυλίους και τα υποσώματα.

Πρόταση ΙΙ.1. *Ένα υποσύνολο $S \neq \emptyset$ του R είναι υποδακτύλιος του R αν και μόνο αν*

$$s_1 - s_2,\ s_1 \cdot s_2 \in S,\ \textit{για όλα τα}\ s_1, s_2 \in S.$$

Ένα υποσύνολο $A \neq \emptyset$ του σώματος K είναι υπόσωμα του K αν και μόνο αν

$$a_1 - a_2 \in A\ \textit{για όλα τα}\ a_1, a_2 \in A\ \textit{και}\ a_1 a_2^{-1} \in A,\ \textit{για όλα τα}\ a_1 \in A\ \textit{και}\ a_2 \in A \setminus \{0\}.$$

Ένα υποσύνολο $I \neq \emptyset$ του δακτυλίου R λέγεται ***ιδεώδες*** (ideal) αν $(I, +)$ είναι υποομάδα του $(R, +)$ και για κάθε $r \in R$ και για κάθε $a \in I$ ισχύει $ra \in I$. Συμβολίζουμε με $I \trianglelefteq R$ για να δηλώσουμε ότι το I είναι ιδεώδες του R. Αν $I \trianglelefteq R$ και $a \in U(R)$ είναι τέτοιο ώστε $a \in I$, τότε $I = R$. Αν $I \trianglelefteq R$ και $I \neq R$, τότε λέμε ότι το I είναι ***γνήσιο ιδεώδες*** (proper ideal) του R και γράφουμε $I \triangleleft R$. Σημειώνουμε την παρακάτω πρόταση για ένα σώμα K.

Πρόταση ΙΙ.2. *Τα μόνα ιδεώδη ενός σώματος K είναι τα (0) και F.*

Αν $I, J \trianglelefteq R$, ορίζουμε $I + J := \{a + b :\ a \in I, b \in J\}$ και το IJ να είναι το σύνολο που αποτελείται από όλα τα στοιχεία που γράφονται ως πεπερασμένα αθροίσματα στοιχείων της μορφής hk, όπου $h \in I$ και $k \in J$. Είναι εύκολο να δει κανείς ότι τα σύνολα $I + J$, $I \cap J$ και IJ είναι ιδεώδη του R και ότι

$$IJ \subset I \cap J \subset I, J \subset I + J.$$

Έστω $I \triangleleft R$. Ο ***δακτύλιος πηλίκο*** (quotient ring) R/I του R ως προς το I έχει ως στοιχεία τα σύνολα $r + I$, όπου $r \in R$, δηλ. $R/I := \{r + I :\ r \in R\}$ και πράξεις

$$(r_1 + I) + (r_2 + I) = (r_1 + r_2) + I,\ (r_1 + I) \cdot (r_2 + I) = (r_1 r_2) + I.$$

Τα αποτελέσματα των πράξεων $(r_1 + I) + (r_2 + I)$ και $(r_1 + I) \cdot (r_2 + I)$ είναι ανεξάρτητα της επιλογής των αντιπροσώπων r_1, r_2. Έτσι αν $r_1' \in r_1 + I$ και $r_2' \in r_2 + I$, τότε

$$(r_1 + I) + (r_2 + I) = (r_1 + r_2) + I = (r_1' + r_2') + I \ \text{ και}$$

$$(r_1 + I) \cdot (r_2 + I) = (r_1 r_2) + I = (r_1' r_2') + I.$$

Το μηδενικό στοιχείο του δακτυλίου R/I είναι το $I = 0 + I$, ενώ το μοναδιαίο στοιχείο του δακτυλίου R/I είναι το $1 + I$. Τα ιδεώδη του R/I έχουν τη μορφή

$$J/I := \{j + I :\ j \in J,\ J \trianglelefteq R,\ I \subset J\}\ .$$

Μία συνάρτηση $f : R \to S$, όπου R και S είναι δακτύλιοι, λέγεται ***ομομορφισμός δακτυλίων*** (ring homomorphism) αν η f σέβεται την αλγεβρική δομή των δακτυλίων, δηλ.

$$f(r_1 + r_2) = f(r_1) + f(r_2),\ f(r_1 r_2 = f(r_1) f(r_2),$$

για κάθε $r_1, r_2 \in R$. Ο ***πυρήνας*** (kernel) του ομομορφισμού $f :\ R \to S$ είναι το σύνολο

$$\ker f := \{r \in R :\ f(r) = 0\},$$

το οποίο είναι ιδεώδες του R, δηλ. $\ker f \trianglelefteq R$. Ακολουθούν τα Θεωρήματα Ισομορφίας για τους δακτυλίους.

Θεώρημα II.3 (Πρώτο Θεώρημα Ισομορφίας Δακτυλίων)**.** *Έστω $f : R \to S$ ένας ομομορφισμός δακτυλίων. Τότε*

$$R/\ker f \to \operatorname{Im} f,\ r + \ker f \mapsto f(r)$$

είναι ισομορφισμός και $R/\ker f \cong \operatorname{Im} f$.

Θεώρημα II.4 (Δεύτερο Θεώρημα Ισομορφίας Δακτυλίων)**.** *Έστω $I \neq J$ γνήσια ιδεώδη του R. Τότε έχουμε ισομορφισμό δακτυλίων*

$$(I + J)/I \cong J/(I \cap J).$$

Θεώρημα II.5 (Τρίτο Θεώρημα Ισομορφίας Δακτυλίων)**.** *Έστω I και J ιδεώδη του R και $I \subset J$. Τότε έχουμε ισομορφισμό δακτυλίων*

$$(R/I)/(J/I) \cong R/J.$$

Αφού τα μόνα ιδεώδη ενός σώματος είναι τα (0) και το ίδιο το σώμα προκύπτει η επόμενη πρόταση ως άμεση συνέπεια του Πρώτου Θεωρήματος Ισομορφίας Δακτυλίων:

Πρόταση II.6. *Έστω K, K' σώματα. Αν $f : K \to K'$ είναι ομομορφισμός δακτυλίων, τότε είτε ο f είναι η μηδενική συνάρτηση είτε ο f είναι μονομορφισμός.*

Έστω F σώμα. Ένας ισομορφισμός $\phi : F \to F$ λέγεται ***αυτομορφισμός*** (automorphism) του F. Το σύνολο των αυτομορφισμών του F συμβολίζεται με $\operatorname{Aut}(F)$ και εύκολα αποδεικνύεται ότι είναι ομάδα με πράξη τη σύνθεση συναρτήσεων.

Ένας δακτύλιος R λέγεται ***ακέραια περιοχή*** (integral domain) αν δεν έχει *διαιρέτες του μηδενός*, δηλ. δεν υπάρχουν στοιχεία $r, s \in R^*$ ώστε $rs = 0$. Ο $\mathbb{Z}$ είναι ένα χαρακτηριστικό παράδειγμα ακέραιας περιοχής.

Για κάθε ακέραια περιοχή R ορίζεται το ***σώμα κλασμάτων*** (ή πηλίκων) (field of fractions) $K(R)$, όπου

$$K(R) := \left\{ \frac{r}{s} :\ r \in R, s \in R^* \right\}$$

με πράξεις

$$\frac{r_1}{s_1} + \frac{r_2}{s_2} = \frac{r_1 s_2 + s_1 r_2}{s_1 s_2},\quad \frac{r_1}{s_1}\frac{r_2}{s_2} = \frac{r_1 r_2}{s_1 s_2}.$$

Τα στοιχεία του $K(R)$ είναι στην πραγματικότητα κλάσεις ισοδυναμίας του $R \times R^*$ ως προς τη σχέση $(r, s) \sim (r', s') \Leftrightarrow rs' = r's$. Για λεπτομέρειες για την κατασκευή του σώματος κλασμάτων μίας ακέραιας περιοχής και την μοναδικότητά του με προσέγγιση ισομορφίας ο αναγνώστης παραπέμπεται στο [4, Ενότητα 4.4].

Έστω R αντιμεταθετικός δακτύλιος. Σημειώνουμε την παρακάτω χρήσιμη πρόταση:

Πρόταση II.7. *Έστω R αντιμεταθετικός δακτύλιος, $a, b \in R$. Αν n είναι φυσικός αριθμός, τότε*

$$(a+b)^n = \sum_{i=0}^{n} a^{n-i} b^i = a^n + \binom{n}{1} a b^{n-1} + \cdots + \binom{n}{n-1} a^{n-1} b + b^n.$$

Ένα γνήσιο ιδεώδες P του δακτυλίου R λέγεται ***πρώτο*** (prime) αν

$$ab \in P \text{ για } a, b \in R \Rightarrow a \in P \text{ ή } b \in P.$$

Ένα γνήσιο ιδεώδες M του δακτυλίου R λέγεται ***μέγιστο*** (maximal), αν δεν υπάρχει γνήσιο δεώδες I του R έτσι ώστε $M \subsetneq I$.

Το επόμενο θεώρημα δίνει σημαντικές πληροφορίες για τα πρώτα και μέγιστα ιδεώδη, αφού οι ιδότητες αυτές αντανακλούν ιδιότητες σε δακτυλίους πηλίκα.

Θεώρημα II.8. *Έστω R ένας δακτύλιος και $I \lhd R$. Τα επόμενα ισχύουν:*

i. Το I είναι πρώτο ιδεώδες αν και μόνο αν ο δακτύλιος R/I είναι ακέραια περιοχή.

ii. Το I είναι μέγιστο ιδεώδες αν και μόνο αν ο δακτύλιος R/I είναι σώμα.

Είναι φανερό ότι κάθε μέγιστο ιδεώδες είναι πρώτο ιδεώδες, αφού το σώμα είναι ακέραια περιοχή. Έστω P ένα μερικά διατεταγμένο σύνολο με διάταξη $\leq$. Μία ***αλυσίδα*** (chain) του P είναι μία ακολουθία στοιχείων $A_i \in P$, για $i = 1, \ldots$, τέτοια ώστε

$$A_1 \leq A_2 \leq \cdots$$

Το Λήμμα του Zorn (Zorn's Lemma) είναι βασικό αξίωμα της Θεωρίας Συνόλων.

Λήμμα του Zorn. *Έστω P ένα (μη κενό) διατεταγμένο σύνολο τέτοιο ώστε κάθε αλυσίδα στοιχείων του P να έχει άνω φράγμα. Τότε το P έχει μέγιστο στοιχείο.*

Με χρήση του Λήμματος του Zorn αποδεικνύεται ότι σε κάθε δακτύλιο υπάρχουν μέγιστα ιδεώδη, άρα και πρώτα.

Πρόταση II.9. *Έστω R ένας δακτύλιος και I γνήσιο ιδεώδες του R. Υπάρχει μέγιστο ιδεώδες M του R τέτοιο ώστε $I \subset M$.*

Πράγματι, έστω $(P, \leq)$ το σύνολο των γνήσιων ιδεωδών του R που περιέχουν το I, με σχέση διάταξης $\leq$ τη συνήθη σχέση εγκλεισμού $\subseteq$. Έτσι,

$$P = \{J : \ I \subset J \text{ και } J \ \lhd \ R\} \text{ και } I_1 \leq I_2 \text{ αν } I_1 \subseteq I_2, \text{ για } I_1, I_2 \in P.$$

Είναι εύκολο να δει κανείς, ότι τα μέγιστα στοιχεία του P ως προς τη διάταξη $\leq$ είναι μέγιστα ιδεώδη του R και περιέχουν το I. Όμως, μία αλυσίδα στο P έχει τη μορφή:

$$J_1 \leq J_2 \leq \cdots \tag{II.9.1}$$

και εύκολα αποδεικνύεται (εξαιτίας των εγκλεισμών) ότι το σύνολο

$$J = \bigcup_{i=1} J_i$$

είναι γνήσιο ιδεώδες του R και ότι είναι άνω φράγμα της αλυσίδας (II.9.1). Σύμφωνα, λοιπόν, με το Λήμμα του Zorn, το P έχει μέγιστο στοιχείο. Το μέγιστο στοιχείο του P είναι ένα μέγιστο ιδεώδες του R που περιέχει το I.

Ιδιαίτερη σημασία έχουν στο κείμενο αυτό οι ***περιοχές κυρίων ιδεωδών*** (Principal Ideal Domains), για συντομία Π.Κ.Ι. Μία Π.Κ.Ι. είναι μία ακέραια περιοχή στην οποία κάθε ιδεώδες είναι ***κύριο*** (principal), δηλ. παράγεται από ένα μόνον στοιχείο. Έτσι αν R είναι Π.Κ.Ι. και $I \trianglelefteq R$, τότε υπάρχει $a \in R$ ώστε $I = \langle a \rangle := aR = \{ar : \ r \in R\}$ και το a λέγεται ***γεννήτορας*** (generator) του I. Το ιδεώδες I του R που ***παράγεται*** (generated) από το υποσύνολο X του R, συμβολίζεται $I = \langle X \rangle$ και είναι το σύνολο

$$I := \left\{ \sum_{i=1}^{s} r_i x_i : \ r_i \in R, x_i \in X, s \in \mathbb{N} \right\}.$$

Για δύο στοιχεία $a, b \in R$ λέμε ότι το a ***διαιρεί*** (divides) το b και γράφουμε $a|b$ αν υπάρχει στοιχείο $r \in R$ ώστε $b = ra$. Ένα στοιχείο $p \in R$ λέγεται***πρώτο*** (prime) αν $p \notin U(R)$ και

$$p|ab, \text{ για } a, b \in R \Rightarrow p|a \text{ ή } p|b.$$

Ένα στοιχείο $u \in R$ λέγεται ***ανάγωγο*** (irreducible) αν $u \notin U(R)$ και

$$u = ab, \text{ για } a, b \in R \Rightarrow a \in U(R) \text{ ή } b \in U(R).$$

Ένας δακτύλιος λέγεται ***περιοχή μονοσήμαντης ανάλυσης*** (Unique Factorization Domain), για συντομία Π.Μ.Α., αν είναι ακέραια περιοχή και κάθε στοιχείο $a \in R^*$ αναλύεται *μοναδικά*

$$a = uq_1q_2 \cdots q_s \ ,$$

όπου $u \in U(R)$ και $q_1, \ldots, q_s$ είναι ανάγωγα στοιχεία. Όταν λέμε μοναδικά εννοούμε ότι αν υπάρχει και άλλη τέτοια ανάλυση για το στοιχείο a, δηλ.

$$a = u'w_1w_2 \cdots w_t \ ,$$

τότε $s = t$ και $w_i = e_iq_i'$, όπου $e_i \in U(R)$ και η ακολουθία $(q_1', \ldots, q_s')$ είναι μία μετάθεση της ακολουθίας $(q_1, \ldots, q_s)$. Το επόμενο θεώρημα συνδέει τις προηγούμενες έννοιες.

Θεώρημα Π.10. *i. Κάθε πρώτο στοιχείο ενός δακτυλίου R είναι ανάγωγο χωρίς να ισχύει το αντίστροφο.*

ii. Σε μία Π.Μ.Α. οι έννοιες ανάγωγο και πρώτο στοιχείο ταυτίζονται.

iii. Κάθε Π.Κ.Ι. είναι Π.Μ.Α. χωρίς να ισχύει το αντίστροφο.

iv. Έστω R μία Π.Κ.Ι. Ένα ιδεώδες $I = (r) \trianglelefteq R$ είναι μέγιστο αν και μόνο αν το r είναι ανάγωγο.

Έστω R μία Π.Μ.Α. Θα ορίσουμε την έννοια του μέγιστου κοινού διαιρέτη και του ελαχίστου κοινού πολλαπλασίου στοιχείων του δακτυλίου R. Έστω $a_1, \ldots, a_s$ στοιχεία του R. Τότε το στοιχείο $d \in R$ λέγεται ο ***μέγιστος κοινός διαιρέτης*** (greatest common divisor) τους και γράφουμε $d = \text{ΜΚΔ}(a_1, \ldots, a_s)$ αν

α. $d|a_i, \text{ για } 1 \leq i \leq s$, και

β. όποτε $d' \,|a_i, \text{ για } 1 \leq i \leq s$ και για κάποιο $d' \in R$, τότε $d' \,|d$.

Αντίστοιχα, το στοιχείο $e \in R$ λέγεται το ***ελάχιστο κοινό πολλαπλάσιο*** (least common multiple) των $a_1, \ldots, a_s$ και γράφουμε $e = \text{ΕΚΠ}(a_1, \ldots, a_s)$ αν

α. $a_i|e, \text{ για } 1 \leq i \leq s$, και

β. όποτε $a_i|e', \text{ για } 1 \leq i \leq s$ και για κάποιο $e' \in R$, τότε $e|e'$.

Θεώρημα Π.11. *Σε μία Π.Μ.Α. υπάρχει ο ΜΚΔ$(a_1, \ldots, a_s)$ και ο ΕΚΠ$(a_1, \ldots, a_s)$, για οποιαδήποτε στοιχεία $a_1, \ldots, a_s$ του R. Ιδιαίτερα, αν $d = \text{ΜΚΔ}(a_1, \ldots, a_s)$, τότε υπάρχουν στοιχεία $r_1, \ldots, r_s \in R$, τέτοια ώστε $d = r_1a_1 + \cdots + r_sa_s$.*

Έστω $n > 1$ φυσικός αριθμός. Από το Πρώτο Θεώρημα Ισομορφίας Δακτυλίων προκύπτει ότι η συνάρτηση

$$\mathbb{Z} \to \mathbb{Z}_n, \ s \mapsto s \bmod n$$

είναι επιμορφισμός δακτυλίων με πυρήνα το ιδεώδες $n\mathbb{Z} = \langle n \rangle$. Άρα $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$. Εφαρμόζοντας τα προηγούμενα συμπεράσματα στον δακτύλιο $\mathbb{Z}$, που είναι Π.Κ.Ι., παρατηρούμε ότι το ιδεώδες $\langle n \rangle$ είναι μέγιστο αν και μόνο αν τοn είναι πρώτος φυσικός αριθμός. Έτσι, ο δακτύλιος $\mathbb{Z}/\langle n \rangle \cong \mathbb{Z}_n$ είναι σώμα αν και μόνο αν ο n είναι πρώτος φυσικός αριθμός.

III Δακτύλιοι Πολυωνύμων

Έστω R ένας δακτύλιος. Μία άπειρη ακολουθία $f := (a_0, a_1, \ldots, a_n, \ldots)$ με $a_i \in R$, $i \in \mathbb{N}$, λέγεται ***τυπική σειρά*** (formal series) πάνω από τον R. Συμβολίζουμε με $R[[x]]$ το σύνολο όλων των τυπικών σειρών πάνω από το R. Το $R[[x]]$ γίνεται δακτύλιος με τις ακόλουθες πράξεις: αν $f := (a_0, a_1, \ldots, a_n, \ldots)$ και $g := (b_0, b_1, \ldots, b_n, \ldots)$ είναι στοιχεία του $R[[x]]$ τότε

$$f + g = (a_0 + b_0, a_1 + b_1, \ldots)$$

και

$$fg = (a_0b_0, a_0b_1 + a_1b_0, \ldots, a_0b_n + a_1b_{n-1} + \cdots + a_nb_0, \ldots).$$

Το μηδενικό στοιχείο του $R[[x]]$ είναι η τυπική σειρά $(0, 0, \ldots)$, ενώ το μοναδιαίο στοιχείο του R είναι η τυπική σειρά $(1, 0, \ldots)$. Είναι φανερό ότι η αντιστοιχία

$$R \to R[[x]], \quad a \mapsto (a, 0, \cdots, 0, \cdots)$$

είναι μονομορφισμός δακτυλίων και ότι ο R εμφυτεύεται με αυτόν τον τρόπο στον $R[[x]]$. Θα ταυτίσουμε τον R με την εικόνα του στον $R[[x]]$ και χωρίς να δημιουργείται σύγχυση θα συμβολίζουμε με a το στοιχείο $(a, 0, \ldots)$. Συμβολίζουμε επίσης με x το στοιχείο $(0, 1, 0, \ldots)$. Έτσι $x^2 = (0, 0, 1, 0 \ldots)$, $x^3 = (0, 0, 0, 1, \ldots)$ κ.ο.κ., ακόμη

$$a_0 + a_1x + a_2x^2 + \cdots = (a_0, a_1, \ldots, a_n, \ldots).$$

Θεώρημα III.1. *Ένα στοιχείο $f = (a_0, a_1, \ldots, a_n, \ldots) \in R[[x]]$ είναι αντιστρέψιμο αν και μόνο αν το a_0 είναι αντιστρέψιμο στον δακτύλιο R, δηλ. αν το $a_0 \in U(R)$. Αν F είναι σώμα, τότε το f είναι αντιστρέψιμο αν και μόνο αν το $a_0 \neq 0$.*

Για παράδειγμα το $1 + x \in U(F[[x]])$ και παρατηρούμε ότι

$$(1 + x)^{-1} = 1 - x + x^2 - x^3 + \cdots .$$

Ο ***δακτύλιος πολυωνύμων με συντελεστές από τον*** R (polynomial ring with coefficients from R), συμβολίζεται με $R[x]$, και είναι ο υποδακτύλιος του $R[[x]]$, που αποτελείται από όλες τις τυπικές σειρές με πεπερασμένο πλήθος μη μηδενικών συντελεστών, δηλ.

$$R[x] = \{a_0 + a_1x + \cdots + a_nx^n : \ \text{όπου} \ \ n \geq 0 \ \text{και} \ \alpha_k \in R, \ \text{για} \ 0 \leq k \leq n\}.$$

Από τον ορισμό του $R[x]$, είναι φανερό ότι τα στοιχεία του $R[x]$ δεν είναι συναρτήσεις. Μπορούμε, όμως, εύκολα να αποδείξουμε ότι η αντιστοιχία

$$R[x] \to R, \quad a_0 + a_1x + \cdots + a_nx^n \mapsto a_0 + a_1a + \cdots + a_na^n,$$

όπου a είναι τυχαίο στοιχείο του R, είναι ένας ομομορφισμός δακτυλίων. Αν $f(x) = a_0 + a_1x + \cdots + a_nx^n \in R[x]$, γράφουμε $f(a) = a_0 + a_1a + \cdots + a_na^n \in R$. Σύμφωνα λοιπόν με τα παραπάνω, η συνάρτηση

$$\phi_a : \ R[x] \to R, \quad f(x) \mapsto f(a), \ \text{για} \ a \in R,$$

είναι ομομορφισμός δακτυλίων. Μπορούμε επίσης να ορίσουμε μία ***πολυωνυμική συνάρτηση*** (polynomial function) F_f, για κάθε $f(x) \in R[x]$, ως εξής:

$$F_f : \ R \to R, \quad a \mapsto f(a).$$

Έστω $f(x) = a_0 + a_1x + \cdots + a_nx^n \in R[x]$ ένα μη μηδενικό στοιχείο του $R[x]$, με $a_n \neq 0$. Αν $a_n = 1$, τότε το $f(x)$ λέγεται ***κανονικό*** ή *μονικό* (monic) πολυώνυμο. Ο φυσικός αριθμός n λέγεται ***βαθμός*** (degree) του πολυωνύμου $f(x)$ και συμβολίζεται $\deg f(x)$. Τα πολυώνυμα βαθμού μηδέν είναι ακριβώς τα μη μηδενικά στοιχεία του R. Το επόμενο θεώρημα δίνει τις ιδιότητες του βαθμού των μη μηδενικών πολυωνύμων.

Θεώρημα III.2. *Έστω $f(x)$ και $g(x)$ δύο μη μηδενικά στοιχεία του $R[x]$. Τότε*

i. Αν $f(x)g(x) \neq 0$, τότε $\deg f(x)g(x) \leq \deg f(x) + \deg g(x)$. Ιδιαίτερα αν ο R είναι μία ακέραια περιοχή, τότε $\deg f(x)g(x) = \deg f(x) + \deg g(x)$.

ii. Αν $f(x) + g(x) \neq 0$, τότε $\deg f(x) + \deg g(x) \leq \max(\deg f(x), \deg g(x))$.

iii. Αν R είναι ακέραια περιοχή, τότε ο $R[x]$ είναι ακέραια περιοχή επίσης.

Σημειώνουμε ότι το πολυώνυμο 0 δεν έχει βαθμό. Πρέπει να παρατηρήσουμε ότι ο δακτύλιος $R[x]$ δεν είναι σώμα σε καμία περίπτωση, ακόμη και αν ο R είναι σώμα. Για παράδειγμα, το πολυώνυμο x δεν είναι αντιστρέψιμο. Όταν ο R είναι ακέραια περιοχή, τότε τα αντιστρέψιμα στοιχεία του $R[x]$ είναι ακριβώς τα στοιχεία του $U(R)$. Πράγματι, αν $f(x)g(x) = 1$ τότε $0 = \deg f(x)g(x) = \deg f(x) + \deg g(x)$ και άρα $\deg f(x) = \deg g(x) = 0$, δηλ. $f(x), g(x) \in R$ και είναι αντιστρέψιμα.

Έστω F ένα σώμα. Όπως είδαμε παραπάνω, ο δακτύλιος $F[x]$ είναι ακέραια περιοχή. Το παρακάτω θεώρημα περιγράφει τις ιδιότητες του $F[x]$.

Θεώρημα III.3. *Έστω F ένα σώμα.*

i. **(Θεώρημα Διαίρεσης)** *Αν $f(x), g(x) \in F[x]$, τότε υπάρχουν μοναδικά $q(x), r(x) \in F[x]$ έτσι ώστε $f(x) = g(x)q(x) + r(x)$, με $\deg r(x) < \deg q(x)$ ή $r(x) = 0$.*

ii. Ο δακτύλιος $F[x]$ είναι Π.Κ.Ι. και κατά συνέπεια Π.Μ.Α.

iii. Το $f(x) \in F[x]$ είναι ανάγωγο αν και μόνο αν δεν υπάρχουν πολυώνυμα $f_1(x)$, $f_2(x)$ τέτοια ώστε $f(x) = f_1(x)f_2(x)$ και $\deg f_1(x), \deg f_2(x) < \deg f(x)$. Το $f(x)$ είναι πρώτο αν και μόνο αν το $f(x)$ είναι ανάγωγο.

iv. Το ιδεώδες $\langle f(x) \rangle$ του $F[x]$ είναι μέγιστο αν και μόνο αν το $f(x)$ είναι ανάγωγο στο $F[x]$.

v. **(Ευκλείδειος Αλγόριθμος)** *Αν $f(x)$, $g(x) \in F[x]$, τότε υπάρχουν $q(x)$, $h(x) \in F[x]$ τέτοια ώστε ΜΚΔ$(f(x), g(x)) = q(x)f(x) + h(x)g(x)$.*

vi. Έστω E ένα σώμα, έτσι ώστε $F \subset E$. Αν $f(x)$, $g(x) \in F[x]$, τότε οι μέγιστοι κοινοί διαιρέτες των $f(x)$, $g(x)$ στους δακτυλίους $F[x]$ και $E[x]$ ταυτίζονται.

Σημειώνουμε ότι όταν p είναι πρώτος φυσικός αριθμός και $a \in \mathbb{Z}_p$, τότε $a^p = a$ (βλ. Θεώρημα I.14.iv). Το επόμενο συμπέρασμα προκύπτει εύκολα από την Πρόταση II.7 και την παρατήρηση ότι ο p διαιρεί τον $\binom{p}{i}$ για $i = 1, \ldots, p-1$.

Πρόταση III.4. *Έστω $f(x) \in \mathbb{Z}_p[x]$. Τότε $f(x^p) = f(x)^p$.*

Το σώμα κλασμάτων της ακέραιας περιοχής $F[x]$ συμβολίζεται με $F(x)$, δηλ.

$$F(x) := \left\{ \frac{f(x)}{g(x)} : \ f(x), g(x) \in F[x], g(x) \neq 0 \right\} .$$

Η θεωρία για τον δακτύλιο πολυωνύμων με μία μεταβλητή μπορεί να επεκταθεί για δακτυλίους πολυωνύμων με περισσότερες της μίας μεταβλητής. Σημειώνουμε, για τον συμβολισμό, ότι

$$R[x_1, x_2] := (R[x_1])\ [x_2]$$

και επαγωγικά

$$R[x_1, \ldots, x_n] := (R[x_1, \ldots, x_{n-1}])\,[x_n].$$

Αν F είναι σώμα, τότε ο δακτύλιος $F[x_1, \ldots, x_n]$ είναι ακέραια περιοχή και το σώμα κλασμάτων του $F[x_1, \ldots, x_n]$ συμβολίζεται με $F(x_1, \ldots, x_n)$, δηλ.

$$F(x_1, \ldots, x_n) := \left\{ \frac{f}{g} :\ f, g \in F[x_1, \ldots, x_n], g \neq 0 \right\}. \tag{III.4.1}$$

Σημειώνουμε την παρακάτω πρόταση:

Πρόταση III.5. *Έστω F σώμα, S δακτύλιος και $t : \{x_1, \ldots, x_n\} \to S$ μία συνάρτηση. Τότε υπάρχει μοναδικός ομομορφισμός δακτυλίων*

$$\tilde{t} :\ F[x_1, \ldots, x_n] \to S,\ \textit{όπου}\ f(x_1, \ldots, x_n) \mapsto f(t(x_1), \ldots, t(x_n))\ .$$

Τέλος στην ενότητα 7.2, θα χρειαστούμε την έννοια του δακτυλίου πολυωνύμων με μεταβλητές από ένα σύνολο ανεξάρτητων μεταβλητών (μη πεπερασμένο). Αναφέρουμε, λοιπόν, ότι η κατασκευή του δακτυλίων πολυωνύμων, γενικεύεται για αυτήν την περίπτωση. Έστω S ένα σύνολο ανεξάρτητων μεταβλητών, δηλ. $S = \{X_\alpha :\ a \in A\}$, όπου A είναι κάποιο σύνολο δεικτών, και έστω F ένα σώμα. Θεωρούμε τον πολυωνυμικό δακτύλιο $R = F[S]$ με συντελεστές από το F και με σύνολο μεταβλητών το S. Ένα τυχαίο στοιχείο του R εκφράζεται ως πολυώνυμο με πεπερασμένο αριθμό μεταβλητών από το σύνολο S. Οι πράξεις ανάμεσα στα στοιχεία του R ικανοποιούν τους ίδιους κανόνες όπως στους συνήθεις πολυωνυμικούς δακτύλιους.

IV Χαρακτηριστική σώματος και πρώτα σώματα

Η ***χαρακτηριστική*** (characteristic) ενός αντιμεταθετικού δακτυλίου R με μοναδιαίο στοιχείο συμβολίζεται με $\operatorname{char} R$ και είναι ο μικρότερος θετικός ακέραιος n, αν υπάρχει, έτσι ώστε

$$n \cdot 1 := \underbrace{1 + \cdots + 1}_{n\text{-φορές}} = 0.$$

Αν δεν υπάρχει τέτοιο n, τότε η χαρακτηριστική του R ορίζεται να είναι μηδέν. Οι δακτύλιοι $\mathbb{Z}$, $\mathbb{Z}[x]$ και τα σώματα $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ με τις γνωστές πράξεις της πρόσθεσης και του πολλαπλασιασμού έχουν χαρακτηριστική 0. Οι δακτύλιοι $\mathbb{Z}_n$ και $\mathbb{Z}_n[x]$ έχουν χαρακτηριστική n. Αφού

$$(mn) \cdot 1 = \underbrace{1 + \cdots + 1}_{mn\text{-φορές}} = (\underbrace{1 + \cdots + 1}_{m\text{-φορές}})(\underbrace{1 + \cdots + 1}_{n\text{-φορές}}) = (m \cdot 1)(n \cdot 1),$$

για τη χαρακτηριστική μίας ακέραιας περιοχή ισχύει η επόμενη πρόταση.

Πρόταση IV.1. *Έστω R ακέραια περιοχή. Η χαρακτηριστική του R είναι είτε 0 είτε κάποιος πρώτος φυσικός αριθμός p. Αν $|R| < \infty$, τότε $\operatorname{char} R = p$, όπου p πρώτος φυσικός αριθμός.*

Υπάρχουν και άπειρες ακέραιες περιοχές με χαρακτηριστική p, όπως για παράδειγμα ο δακτύλιος πολυωνύμων $\mathbb{Z}_p[x]$ και το σώμα κλασμάτων $\mathbb{Z}_p(x)$. Παρακάτω θα δούμε ότι η χαρακτηριστική ενός σώματος F καθορίζει το μικρότερο σώμα που περιέχεται στο F. Αν ο δακτύλιος R περιέχει ως υποδακτύλιο ένα σώμα F, τότε ο δακτύλιος R έχει τη δομή διανυσματικού χώρου πάνω από το F. Σε αυτήν την περίπτωση είναι φανερό ότι $\operatorname{char} R = \operatorname{char} F$.

Ορισμός IV.2. ***Πρώτο υπόσωμα*** *(prime subfield) ενός σώματος F είναι η τομή όλων των υποσωμάτων του.*

Κάθε υπόσωμα ενός σώματος περιέχει τα στοιχεία 0 και 1. Ακόμη παρατηρούμε ότι τα σώματα $\mathbb{Q}$ και $\mathbb{Z}_p$ δεν έχουν γνήσια υποσώματα και επομένως είναι ίσα με τα πρώτα υποσώματά τους. Το επόμενο θεώρημα αποδεικνύει ότι το $\mathbb{Q}$ και το $\mathbb{Z}_p$, όπου p πρώτος φυσικός αριθμός, είναι τα μόνα πρώτα υποσώματα με προσέγγιση ισομορφίας.

Θεώρημα IV.3. *Κάθε πρώτο υπόσωμα είναι ισόμορφο είτε με το σώμα $\mathbb{Q}$ είτε με το σώμα $\mathbb{Z}_p$, όπου p πρώτος φυσικός αριθμός.*

Πράγματι, έστω F ένα σώμα. Τότε η συνάρτηση

$$\phi:\ \mathbb{Z} \to F,\ n \mapsto n \cdot 1$$

είναι ομορφισμός δακτυλίων. Αν $\operatorname{char} F = 0$, τότε ο ϕ είναι μονομορφισμός και

$$\psi:\ \mathbb{Q} \to F,\ \psi\left(\frac{n}{s}\right) \mapsto (n \cdot 1)(s \cdot 1)^{-1}$$

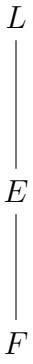
είναι μονομορφισμός σωμάτων. Έτσι το σώμα $\mathbb{Q}$ εμφυτεύεται στο F. Αν, όμως, $\operatorname{char} F = p$, τότε ο πυρήνας του ομομορφισμού ϕ είναι ίσος με $p\mathbb{Z}$. Σύμφωνα με το Πρώτο Θεώρημα Ισομορφίας Δακτυλίων έπεται ότι

$$\mathbb{Z}_p \cong \mathbb{Z}/p\mathbb{Z} \cong \operatorname{Im}\phi$$

δηλ. το $\mathbb{Z}_p$ είναι ισόμορφο με το υπόσωμα $\{0, 1, 2\cdot 1, \ldots, (p-1)\cdot 1\}$ του F. Με άλλα λόγια το $\mathbb{Z}_p$ εμφυτεύεται στο F. Σημειώνουμε επίσης ότι αν F, E είναι δύο σώματα και $i:\ F \to E$ είναι μη μηδενικός ομομορφισμός δακτυλίων, τότε ο i είναι εμφύτευση του F στο E και το F είναι ισόμορφο με το υπόσωμα $i(F)$ του E. Το σώμα E γίνεται F-διανυσματικός χώρος πάνω από το F μέσω αυτής της εμφύτευσης: $c \cdot e = i(c)e$, για $c \in F, e \in E$.

Ορισμός IV.4. *Το σώμα E λέγεται* ***επέκταση*** *(extension) του σώματος F και γράφουμε E/F, αν υπάρχει εμφύτευση $i:\ F \hookrightarrow E$. Το σώμα E λέγεται* ***πεπερασμένη επέκταση*** *(finite extension) του F όταν $\dim_F E = n < \infty$. Διαφορετικά λέμε ότι το E είναι* ***άπειρη επέκταση*** *(infinite extension) του F.*

Όταν $i : F \hookrightarrow E$ και $j : E \hookrightarrow L$ είναι εμφυτεύσεις σωμάτων, τότε η σύνθεση των i και j είναι μία εμφύτευση σωμάτων $F \hookrightarrow L$ και λέμε ότι το σώμα E είναι ***ενδιάμεσο σώμα*** (intermediate field) της επέκτασης L/F. Εφεξής, όταν E/F είναι μία επέκταση, ταυτίζουμε το F με την ισομορφική του εικόνα στο E. Αν E_1/F, E_2/F είναι δύο επεκτάσεις του F, τότε ο ομομορφισμός δακτυλίων $\phi :\ E_1 \to E_2$ λέγεται F-***ομομορφισμός*** (F-homomorphism) αν $\phi(c) = c$, για κάθε $c \in F$.



Σχήμα IV.1: Το E είναι ενδιάμεσο σώμα της επέκτασης L/F.

Έστω ότι L είναι μία πεπερασμένη επέκταση του $\mathbb{Z}_p$, έτσι ώστε $\dim_{\mathbb{Z}_p} L = n$. Από αυτό έπεται ότι το σώμα L ως διανυσματικός χώρος είναι ισόμορφος με τον διανυσματικό χώρο

$$\underbrace{\mathbb{Z}_p \times \cdots \times \mathbb{Z}_p}_{n\text{-φορές}}.$$

Επομένως το L έχει πληθυκότητα p^n. Συμπεραίνουμε έτσι την ακόλουθη πρόταση.

Πρόταση IV.5. *Έστω F ένα πεπερασμένο σώμα, δηλ. $|F| < \infty$. Τότε, η χαρακτηριστική του F είναι κάποιος πρώτος αριθμός p και το πρώτο σώμα του F είναι ισόμορφο με το $\mathbb{Z}_p$. Αντίστροφα, κάθε πεπερασμένη επέκταση L ενός σώματος $\mathbb{Z}_p$ έχει πεπερασμένου πλήθους στοιχεία και το πλήθος των στοιχείων της είναι μία δύναμη του p. Η πληθυκότητα του L είναι p^n αν και μόνο αν $\dim_{\mathbb{Z}_p} L = n$.*

Παρατηρούμε ότι η επέκταση $F(x)$ του σώματος F είναι άπειρη επέκταση, αφού τα στοιχεία $1, x, x^2, \ldots, x^n, \ldots$ είναι F-γραμμικά ανεξάρτητα. Έτσι οι επεκτάσεις

$$\mathbb{Q}(x)/\mathbb{Q}, \;\; \mathbb{R}(x)/\mathbb{R}, \;\; \mathbb{C}(x)/C, \;\; \mathbb{Z}_p(x)/\mathbb{Z}_p$$

είναι παραδείγματα άπειρων επεκτάσεων σωμάτων, η τελευταία από τις οποίες έχει χαρακτηριστική p.

V Τύπος για τις ρίζες πολυωνύμων βαθμού 3 και 4.

Σε αυτήν την ενότητα, παραθέτουμε τους τύπους για τις ρίζες των πολυωνύμων βαθμού 3 και 4. Για το πώς προέκυψαν οι τύποι, παραπέμπουμε στα [6, σελ. 266-272] και [2, σελ. 266-272] .

V.1 Πολυώνυμα βαθμού 3.

Έστω

$$f(x) = x^3 + px^2 + qx + r \in \mathbb{C}[x].$$

Θέτουμε

$$D = p^2q^2 - eq^3 - 4p^3r - 27r^2 + 18pqr,$$

$$A = -p^3 + \frac{9}{2}pq - \frac{27}{2}r + \frac{3i\sqrt{3}}{2}\sqrt{D}.$$

και

$$B = -p^3 + \frac{9}{2}pq - \frac{27}{2}r - \frac{3i\sqrt{3}}{2}\sqrt{D}.$$

Σημειώνουμε ότι τα A και B διαφέρουν στο πρόσημο του τελευταίου προσθετέου και ότι $\sqrt{D}$ είναι μία οποιαδήποτε τετραγωνική ρίζα του D, βλ. το συμβολισμό μετά την Πρόταση 6.3.2. Έστω

$$\omega = e^{2\pi i/3}$$

η τρίτη πρωταρχική ρίζα της μονάδας (βλ. Σχήμα 1.3). Μπορεί να αποδειχθεί απευθείας με αντικατάσταση, ότι οι τρεις ρίζες του $f(x)$ δίνονται από τους τύπους:

$$\frac{1}{3}\left(-p + \sqrt[3]{A} + \sqrt[3]{B}\right),$$

$$\frac{1}{3}\left(-p + \omega^2\sqrt[3]{A} + \omega\sqrt[3]{B}\right), \tag{V.1.1}$$

και

$$\frac{1}{3}\left(-p + \omega\sqrt[3]{A} + \omega^2\sqrt[3]{B}\right).$$

Όταν ο δευτεροβάθμιος όρος του $f(x)$ λείπει, όταν δηλ. $p = 0$ και το $f(x) = x^3 + qx + r \in \mathbb{Q}[x]$, τότε οι παραπάνω τύποι απλοποιούνται και οι τρεις ρίζες του $f(x)$ είναι

$$y + z,\ \omega y + \omega^2 y,\ \omega^2 y + \omega z$$

όπου

$$y = \left(\frac{1}{2}\left(-r + \sqrt{r^2 + \frac{4q^3}{27}}\right)\right)^{\frac{1}{3}}$$

και

$$z = \left(\frac{1}{2}\left(-r - \sqrt{r^2 + \frac{4q^3}{27}}\right)\right)^{\frac{1}{3}}.$$

V.2 Πολυώνυμα βαθμού 4.

Έστω τώρα

$$f(x) = x^4 + a_1x^3 + a_2x^2 + a_3xa_4 \in \mathbb{C}[x].$$

Θέτουμε

$$p = -a_2,\ q = a_1a_3 - 4a_4,\ r = -a_1^2a_4 + 4a_2a_4 - a_3^2\ ,$$

και θεωρούμε το τριτοβάθμιο πολυώνυμο

$$g(y) = y^3 + b_1y^2 + b_2y + b_3 \in \mathbb{C}[y].$$

Η εξίσωση

$$g(y) = 0$$

λέγεται ***κυβική επιλύουσα*** (cubic resolvent). Έστω η_1, η_2, η_3 οι τρεις ρίζες του $g(y)$, όπως στους τύπους (V.1.1).

Οι τέσσερις ρίζες του $f(x)$ δίνονται από τους παρακάτω τύπους:

$$\frac{1}{4}\left(-a_1+\sqrt{a_1^2-4a_2+4\eta_1}+\sqrt{a_1^2-4a_2+4\eta_2}+\sqrt{a_1^2-4a_2+4\eta_3}\right),$$

$$\frac{1}{4}\left(-a_1+\sqrt{a_1^2-4a_2+4\eta_1}-\sqrt{a_1^2-4a_2+4\eta_2}-\sqrt{a_1^2-4a_2+4\eta_3}\right),$$

$$\frac{1}{4}\left(-a_1-\sqrt{a_1^2-4a_2+4\eta_1}+\sqrt{a_1^2-4a_2+4\eta_2}-\sqrt{a_1^2-4a_2+4\eta_3}\right),$$

και

$$\frac{1}{4}\left(-a_1-\sqrt{a_1^2-4a_2+4\eta_1}-\sqrt{a_1^2-4a_2+4\eta_2}+\sqrt{a_1^2-4a_2+4\eta_3}\right).$$

Σημειώνουμε ότι οι παραπάνω τύποι είναι συμμετρικοί ως προς την επιλογή της αρίθμησης των η_1, η_2, η_3 της κυβικής επιλύουσας.

Για την ιστορία που οδήγησε στην επίλυση των πολυωνύμων τρίτου και τετάρτου βαθμού παραπέμπουμε σε πολυμεσικές διαλέξεις του ψηφιακού μαθήματος (open courses) Ιστορία των Μαθηματικών του Τμήματος Μαθηματικών, Α.Π.Θ. και συγκεκριμένα, για την επίλυση του τριτοβάθμιου πολυωνύμου, στις Ενότητες 5.3 και 5.4 ενώ για τα πολυώνυμα τετάρτου βαθμού παραπέμπουμε στην Ενότητα 5.5.

Βιβλιογραφία Παραρτήματος

[1] Βάρσος, Δ., Δεριζιώτης, Δ., Μαλιάκας, Μ., Ταλέλλη Ο., Εμμανουήλ, Ι., Μελάς, Α. *Μία Εισαγωγή στην Άλγεβρα*. ΕΚΠΑ, Εκδ. Σοφία, 2012.

[2] Bewersdorff, J. *Galois Theory for Beginniers, A Historical Perspective*. AMS, 2006.

[3] Dummit, D.S., Foote, R.M. *Abstract Algebra*. J. Wiley and Sons, INc, 2004.

[4] Fraleigh, J. *Εισαγωγή στην Άλγεβρα*. Πανεπιστημιακές εκδόσεις Κρήτης, 2011.

[5] Hungerford,T. *Algebra*. Springer, 1974.

[6] Λάκκης, Κ. *Άλγεβρα*. Θεσσαλονίκη, 1980.

[7] Menini, C. Van Oystaeyen, F. *Abstract Algebra*. Marcel Dekker, 2004.

[8] Πουλάκης, Δ. *Άλγεβρα*. Ζήτη, 2015.

Υποδείξεις λύσεων επιλεγμένων ασκήσεων

Ενότητα 1.5

1. α) Έστω A ένα σημείο μίας ευθείας. Ορίζουμε αριστερά του A επί της ευθείας σημείο B, ώστε το μήκος BA να είναι ίσο με 1. Με κέντρο το B και ακτίνα μεγαλύτερη του 1 χαράσσουμε περιφέρεια κύκλου, που τέμνει την ευθεία δεξιά του σημείου A στο σημείο, έστω G. Με την ίδια ακτίνα και κέντρο το σημείο G χαράσσουμε νέα περιφέρεια κύκλου. Οι δύο περιφέρειες τέμνονται στα σημεία, έστω D και E. Η ευθεία DE είναι η ζητούμενη.

β) Εργαζόμαστε όπως στο α) θεωρώντας το τμήμα BG.

γ) Από το σημείο A εκτός ευθείας χαράσσουμε περιφέρεια με κέντρο το A τέτοια ώστε να τμήσει την ευθεία σε δύο σημεία, έστω BG. Η μεσοκάθετος στο BG τέμνει την ευθεία στο σημείο, έστω D. Από το A φέρουμε κάθετη στο AD. Αυτή είναι η ζητούμενη.

δ) Έστω η γωνία AOB με κορυφή O. Με κέντρο το O και ακτίνα μήκους 1 χαράσσουμε περιφέρεια κύκλου που το τμήμα OA στο σημείο έστω A' και το OB στο σημείο, έστω B'. Η μεσοκάθετος από το O στο $A'B'$ είναι η ζητούμενη.

2. Σε μία ευθεία ορίζουμε τρία σημεία A, B, G ώστε το AB να έχει μήκος 1 και το BG να έχει μήκος a. Με διάμετρο το AG χαράσσουμε περιφέρεια κύκλου (βρίσκουμε το μέσον του AB όπως στο β). Από το σημείο B φέρουμε κάθετο στο AG (βλ. 1α)), αυτή τέμνει την περιφέρεια, έστω στο D. Το μήκος DB είναι το ζητούμενο.

3. Να χρησιμοποιήσετε τον τριγωνομετρικό κύκλο.

4. Έστω A μία πλευρά του κανονικού n-γώνου και O το κέντρο του. Να φέρετε τη μεσοκάθετο από το O στο AB και να εργαστείτε όπως στην άσκηση 3 για τα ίσα ορθογώνια τρίγωνα που σχηματίζονται.

5. N,N, O, N, N, N,N

Οι ανάγωγοι παράγοντες του $x^4 + 4$ έχουν βαθμό 2. Για το $f(x) = x^4 + 1$ μελετήστε το πολυώνυμο $f(x + 1)$. Για το πολυώνυμο $f(x) = (4/3)x^5 + (6/5)x^2 + 2$ μελετήστε το πολυώνυμο $15f(x)$.

6. Να υπολογίσετε πρώτα τα ανάγωγα πολυώνυμα βαθμού 2. Στη συνέχεια, στο $f(x) = x^4 + ax^3 + bx^2 + cx + d$ θέστε στη θέση των συντελεστών τα στοιχεία 0 ή 1 και ελέγξτε ποια είναι ανάγωγα. Αν δεν είναι ανάγωγα, τότε είτε έχουν ρίζα στο $\mathbb{Z}_2[x]$ είτε έχουν έναν ανάγωγο παράγοντα βαθμού 2.

8. Για το x^4+4 δείτε την άσκηση 5.

10. $\Phi_{13}(x)$.

12. Να αναλύσετε σε γινόμενο παραγόντων τα πολυώνυμα: $(x^8-1)/(x-1)$ και $(x^9-1)/(x-1)$. Οι ανάγωγοι παράγοντες στον $\mathbb{R}[x]$ έχουν βαθμό το πολύ 2. Οι ανάγωγοι παράγοντες στον $\mathbb{C}[x]$ έχουν βαθμό ακριβώς 1. Στον $\mathbb{Q}[x]$, το $x^7+x^6+\cdots+x+1$ έχει ακριβώς έναν ανάγωγο παράγοντα βαθμού 4, ενώ το $x^8+x^7+\cdots+1$ έχει ακριβώς έναν ανάγωγο παράγοντα βαθμού 6. Η Ενότητα 5.2 ασχολείται με τους ανάγωγους παράγοντες του x^n-1 στον $\mathbb{Q}[x]$.

Ενότητα 2.4

2. $\mathbb{Q}(\sqrt{5},\sqrt{7}) = \{a_0+a_1\sqrt{5}+a_2\sqrt{7}+a_3\sqrt{35} : a_i \in \mathbb{Q}, i=1,\ldots,4\}$.
$\mathbb{Q}(i\sqrt{11}) = \{a_0+a_1\sqrt{11} : a_0,a_1 \in \mathbb{Q}\}$.

3. Για το $a=\sqrt{7}+1/2$, βλέπουμε ότι $2a-1=2\sqrt{7}$ και επομένως το a είναι ρίζα του $4x^2-4a-27$.

4. Να χρησιμοποιήσετε τον ισομορφισμό $\mathbb{Q}[x]/\langle x^3-2\rangle \cong \mathbb{Q}(\sqrt[3]{2})$, $x+\langle x^3-2\rangle \mapsto \sqrt[3]{2}$. Να γράψετε τη μονάδα ως γραμμικό συνδυασμό των x^3-2 και x^2+1. Στη συνέχεια να βρείτε τον αντίστροφο του $\sqrt[3]{2}^2+1$ από αυτήν τη σχέση.

6. ∞, ∞, 1, 7.

7. Αν ϕ είναι ένας τέτοιος ισομορφισμός, τότε $\phi(\sqrt{3}) = a+b\sqrt{5}$, για κάποιους ρητούς a,b. Άρα $3=\phi(\sqrt{3})^2=(a+b\sqrt{5})^2=a^2+5b^2+2ab\sqrt{5}$, άτοπο γιατί ο $\sqrt{5}$ δεν είναι ρητός.

14. Να αποδείξετε με επαγωγή ότι αν $p_1,\ldots,p_n$ είναι διακριτοί πρώτοι, τότε

$$\sqrt{p} \notin \mathbb{Q}(\sqrt{p_1},\ldots,\sqrt{p_{n-1}}).$$

Να συμπεράνετε ότι $[\overline{\mathbb{Q}}:\mathbb{Q}]=\infty$.

18 . $\mathbb{Z}_2$, $\mathbb{Z}_2$, $\mathbb{Z}_4$, S_3.

19. Να χρησιμοποιήσετε την Πρόταση 2.3.2.

24. Έστω $G=\mathrm{Gal}(\mathbb{R}/\mathbb{Q})$.

(α΄) Αν $a \le b \in \mathbb{R}$ και $\sigma \in G$, να δείξετε ότι $\sigma(a) \le \sigma(b)$ (να χρησιμοποιήσετε το στοιχείο $\sqrt{b-a}$ και την εικόνα του $\sigma(\sqrt{b-a})$).

(β΄) Αν $a \in R$ και $\sigma \in G$, να θεωρήσετε μία αύξουσα ακολουθία ρητών αριθμών που συγκλίνει στο a για να καταλήξετε ότι $a \le \sigma(a)$. Στη συνέχεια να θεωρήσετε μία φθίνουσα ακολουθία ρητών αριθμών που συγκλίνει στο a για να καταλήξετε ότι $a \ge \sigma(a)$.

26. Οι ομάδες των ασκήσεων 2.4.25 και 2.4.25 θα εξεταστούν αναλυτικότερα στο Κεφάλαιο 5.

27. **O,N,O,N,O,O,O,N,O,N,O,O,O,O,N**.

Ενότητα 3.7

1. Αν $h \in H$, τότε $h \in G$ και $h(a) = a$, $\forall a \in F$. Άρα $F \subset E^H \subset E$.

Έστω $H_1 < H_2 < G$ και $a \in E^{H_2}$. Τότε $h(a) = a$, $\forall h \in H_2$, άρα $h(a) = a$, $\forall h \in H_1$. Άρα $E^{H_2} \subset E^{H_1}$.

2.
- $B = \mathbb{Q}(\sqrt{2})$, $E = \mathbb{Q}(\sqrt[4]{2})$.
- Αδύνατον.
- E το σώμα ανάλυσης του $x^3 - 2$ πάνω από το $\mathbb{Q}$ και $B = \mathbb{Q}(\sqrt{2})$.

3. $E = \mathbb{Q}(\sqrt{2}, i)$, αφού

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

Παρατηρήστε ότι $\mathrm{irr}_{(\mathbb{Q},\sqrt{2})}(x) = x^2 - 2$. Οι εικόνες του $\alpha = \sqrt{2} + i$ είναι τα

$$\alpha, \sqrt{2} - i, -\sqrt{2} + i, -\sqrt{2} - i.$$

Επίσης, $\mathrm{irr}_{\mathbb{Q},\alpha)}(x) = x^4 - 6x^2 + 17$ και επομένως $\alpha(\alpha^3 - 2\alpha) = -17$ και $a^{-1} = -(\alpha^3 - 2\alpha)/17$.

4. Το E είναι σώμα ανάλυσης του $(x^2 - 3)(x^2 - 5)$ και συνεπώς η $E/\mathbb{Q}$ είναι επέκταση του Galois.

5. Η ομάδα $\mathrm{Gal}(E/F)$ καθορίζεται από τις μεταθέσεις των ριζών του $f(x)$. Αφού $\mathrm{char}\, F \neq 2$, μία μετάθεση των ριζών του $f(x)$ είναι περιττή αν και μόνο αν $\sigma(\Delta) = -\Delta$. Αφού η $\Delta \in F$ έπεται ότι $\sigma(\Delta) = \Delta$, για κάθε $\sigma \in \mathrm{Gal}(E/F)$.

9. Ο βαθμός $[E : \mathbb{Q}]$ διαιρείται από το 4 και το 5, άρα $[E : \mathbb{Q}] = 20$. Η G είναι ισόμορφη με γνήσια υποομάδα της S_5. Υπάρχουν αυτομορφισμοί $\sigma, \tau \in G$ τέτοιοι ώστε $\sigma(\sqrt[5]{3}) = \sqrt[5]{3}$, $\sigma(\omega) = \omega^2$ και $\tau(\sqrt[5]{3}) = \sqrt[5]{3}$, $\tau(\omega) = \omega$.

11. Παρατηρήστε ότι το $N(\alpha)$ ανήκει στο E^G.

12. Προκύπτει από το Θεώρημα 3.4.5.

13. Προκύπτει από το Θεώρημα 3.5.3 με $K = F(\alpha)$.

Ενότητα 4.4

2. Το πολυώνυμο $g(x) = x^2 + x + 2$ είναι ανάγωγο πάνω από το $GF(5)$, όπως διαπιστώνεται δοκιμάζοντας όλα τα στοιχεία του $GF(5)$. Άρα το σώμα αναλύσεως E του $g(x)$ που αναζητούμε, είναι επέκταση βαθμού 2 του $GF(5)$, δηλ. $E = \{k + la : k, l \in GF(5)\}$ και a είναι μία ρίζα του $g(x)$. Το E έχει 25 στοιχεία και είναι ισόμορφο με το $GF(5^2)$.

3. Προκύπτει από την Πρόταση 4.2.8 και το Πόρισμα 4.2.9.

8. Έστω ότι το F είναι τέλειο σώμα. Αν $\mathrm{char}(F) = 0$, το συμπέρασμα ισχύει. Έστω $\mathrm{char}(F) = p$, όπου p πρώτος και $f(x)$ ένα ανάγωγο και μη διαχωρίσιμο πολυώνυμο του $F[x]$, τότε $f'(x) = 0$ και το $f(x)$ ανήκει στον $F[x^p]$. Όμως $F = F^p$, άρα $f(x) = a_0 + a_1x^p + \cdots + a_nx^{np}$, για $a_i \in F = F^p$, $a_i = b_i^p$, $0 \leq i \leq n$. Επομένως $f(x) = (b_0 + \cdots + b_nx^n)^p$ και το $f(x)$ δεν είναι ανάγωγο, άτοπο. Άρα το $f(x)$ είναι διαχωρίσιμο. Αντίστροφα, έστω ότι κάθε ανάγωγο πολυώνυμο του $F[x]$ είναι διαχωρίσιμο και ότι το F δεν είναι τέλειο. Παρατηρούμε ότι, αν $a \in F \setminus F^p$, τότε το $x^p - a$ είναι ανάγωγο (βλ. Παράδειγμα 4.3.7) και μη διαχωρίσιμο πολυώνυμο του $F(x)$, αφού $f'(x) = 0$. Καταλήξαμε σε άτοπο, άρα το F είναι τέλειο.

Ενότητα 5.4

2. Συγκρίνετε με το πολυώνυμο $\Phi_{p^2}(x)$.

3. Για το (β) παρατηρήστε ότι ο ένας παράγοντας της σειράς είναι ισόμορφος με την $\mathrm{Gal}(F(\omega)/F)$ που είναι υποομάδα αβελιανής ομάδας (βλ. Θεώρημα 5.1.4), ενώ για τον άλλο παράγοντα χρησιμοποιείστε το Θεώρημα 5.3.1.

6. Να παρατηρήσετε ότι $\Phi_{2p}(x)\Phi_p(x)\Phi_2(x)\Phi_1(x) = x^{2p}-1$ και ότι $\Phi_p(x)\Phi_1(x) = x^p-1$.

7. Να παρατηρήσετε ότι $\phi(12) = 4$ και να ω είναι μία πρωταρχική 12-ρίζα της μονάδας, τότε $G = \mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q}) = \{\mathrm{id}_{\mathbb{Q}(\omega)}, \sigma, \tau, \sigma\tau\}$, όπου $\sigma(\omega) = \omega^2$, $\tau(\omega) = \omega^7$, $\sigma\tau(\omega) = \omega^{11}$. Να δείξετε ότι τα ενδιάμεσα σώματα είναι τα: $\mathbb{Q}(\omega^3)$, $\mathbb{Q}(\omega^2)$, $\mathbb{Q}(\omega^6)$.

8. Έστω $E = \mathbb{Q}(\omega)$. Γνωρίζουμε ότι $[E : \mathbb{Q}] = \phi(n)$, όπου ϕ είναι η συνάρτηση του Euler. Έστω $\zeta = \omega + \omega^{-1}$, τότε εκτελώντας τις πράξεις, έχουμε $\omega^2 - \zeta\omega + 1 = 0$ και επομένως $[E : \mathbb{Q}(\zeta)] \leq 2$. Επίσης $\zeta \in \mathbb{R}$ και επομένως $[E : \mathbb{Q}(\zeta)] \geq 2$. Να συμπεράνετε ότι $[E : \mathbb{Q}(\zeta)] = 2$ και άρα $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \phi(n)/2$.

Ενότητα 6.4

3. Στην Ενότητα V του Παραρτήματος δίνονται οι τύποι για τις ρίζες του τεταρτοβάθμιου πολυωνύμου $f(x)$.

7. Θεωρήστε την ομάδα $\mathrm{Gal}(L/\mathbb{Q})$ και εφαρμόστε το Θεώρημα I.28. Σύμφωνα με το Θεώρημα I.28 η ομάδα $\mathrm{Gal}(L/\mathbb{Q})$ έχει μία κανονική σειρά

$$G = G_t \rhd G_{t-1} \rhd \cdots \rhd \{e\} = G_0,$$

τέτοια ώστε η ομάδα G_i/G_{i-1} να έχει τάξη 2, για $i = 1, \ldots, t$. Από το Θεμελιώδες Θεώρημα της Θεωρίας Galois έπεται ότι υπάρχει μία ακολουθία σωμάτων

$$\mathbb{Q} = K_0 \subset K_1 \cdots \subset K_t = \mathbb{Q}(\omega) \ ,$$

με $[K_i : K_{i-1}] = 2$, για $i = 1, \ldots, t$.

10. Το L περιέχει αναγκαστικά και τον συζυγή του z, επομένως περιέχει και το a και το bi. Να αποδείξετε ότι το a και το b ικανοποιούν το κριτήριο της άσκησης 6.4.7 για τα αντίστοιχα σώματα ανάλυσης.

Ενότητα 7.3

4. Για κάθε n, υπάρχει $a \in \mathbb{R}$ έτσι ώστε $\deg \operatorname{irr}_{(\mathbb{Q},a)}(x) > n$. Για το αριθμήσιμο κομμάτι της ερώτησης, να μετρήσετε τα πολυώνυμα του $\mathbb{Q}[x]$.

6. Έστω F υπόσωμα του $\mathbb{C}$. Αν a, b είναι δύο υπερβατικά στοιχεία πάνω από το F, τότε να αποδείξετε ότι υπάρχει ισομορφισμός $F(a) \to F(b)$. Αν a, b είναι διακεκριμένες ρίζες του ίδιου ανάγωγου πολυωνύμου με συντελεστές στο F, να αποδείξετε ότι η $\phi : F(a) \to F(b)$, με $\phi(a) = \phi(b)$, μπορεί να επεκταθεί σε αυτομορφισμό του $\overline{F}_{\mathbb{C}}$, χρησιμοποιώντας το Λήμμα του Zorn.

Ενότητα 8.3

3. Θυμίζουμε από τη Θεωρία Ομάδων ότι κάθε πεπερασμένη αβελιανή ομάδα G είναι ευθύ άθροισμα κυκλικών ομάδων, δηλ.

$$G \cong \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_s},$$

για κάποιους φυσικούς αριθμούς n_i, $i = 1, \ldots, s$. Θεωρούμε πρώτους φυσικούς p_1, $p_2, \ldots, p_s$ τέτοιους ώστε $p_i \equiv 1 \bmod n_i$, $1 \leq i \leq s$ (υπάρχουν άπειροι τέτοιοι πρώτοι). Έστω $n = p_1 p_2 \cdots p_s$ και ω μία πρωταρχική n-ρίζα της μονάδας. Γνωρίζουμε ότι

$$M := \operatorname{Gal}(\mathbb{Q}(\omega)/\mathbb{Q} \cong \mathbb{Z}_n^\sharp \cong \mathbb{Z}_{p_1}^* \times \cdots \times \mathbb{Z}_{p_s}^*$$

και $\mathbb{Z}_{p_i}^* \cong \mathbb{Z}_{p_i - 1}$, αφού η $\mathbb{Z}_{p_i}^*$ είναι κυκλική ομάδα τάξης $p_i - 1$. Όμως, αφού $p_i - 1 = k_i n_i$, για κάποιον ακέραιο k_i, έπεται ότι η ομάδα $\mathbb{Z}_{n_i}$ είναι ισόμορφη με υποομάδα της $\mathbb{Z}_{p-1}$, έστω την H_i, για $i = 1, \ldots, s$. Θεωρούμε, τώρα, την υποομάδα

$$H = H_1 \times \cdots H_s$$

της M, η οποία αντιστοιχεί σε ένα σώμα $\mathbb{Q} \leq K \leq \mathbb{Q}(\omega)$. Να αποδείξετε ότι $\operatorname{Gal}(K/\mathbb{Q})$ είναι ισόμορφη με την G.

Ευρετήριο Συμβολισμών

Ευρετήριο Όρων

Ευρετήριο Αγγλικής Ορολογίας