Θεωρία Galois

Θεοδώρα Θεοχαρη-Αποστολιδη

Χαρά Χαραλαμπους

Οι σημειωσεις αυτες θα συμπληρωνονται κατα τη διαρκεια των μαθηματων.

11 Νοεμβρίου 2014

Περιεχόμενα

Κεφάλαιο 1

Βασικές Έννοιες

1.1 Εισαγωγικά

Θα περιγράψουμε τα βασικά θέματα που θα προσεγγίσουμε στη διάρκεια αυτού του εξαμήνου. Το πρώτο αφορά το Θεμελιώδες Θεώρημα της Άλγεβρας

1.1.1 Το Θεμελιώδες Θεώρημα της Άλγεβρας

Το Θεμελιώδες Θεώρημα της Άλγεβρας είναι από τα σημαντικότερα θεωρήματα στα μαθηματικά.

Θεώρημα 1.1.2. *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 μιγαδικούς αριθμούς έχει τουλάχιστον μία ρίζα στο $\mathbb{C}$.*

Είναι σημαντικό να τονίσουμε ότι το Θεώρημα 1.1.2 βεβαιώνει για την ύπαρξη ρίζας, 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 $f(x)$ έχει n ρίζες στο $\mathbb{C}$. Λέμε ότι $\mathbb{C}$ είναι *αλγεβρικά κλειστό* εξαιτίας αυτής της ιδιότητας: κάθε πολυώνυμο του $\mathbb{C}[x]$ αναλύεται σε γινόμενο γραμμικών παραγόντων στο $\mathbb{C}[x]$. Αφού τα πολυώνυμα του $\mathbb{R}[x]$ ανήκουν αυτόματα και στο $\mathbb{C}[x]$, τα μη μηδενικά πολυώνυμα με πραγματικούς συντελεστές έχουν τόσες μιγαδικές ρίζες όσες είναι ο βαθμός τους, μετρώντας τις ρίζες σύμφωνα με την πολλαπλότητα 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 στο $\mathbb{R}$. Από το Θεμελιώδες Θεώρημα της Άλγεβρας προκύπτει ακόμα ότι τα μόνα ανάγωγα πολυώνυμα του $\mathbb{C}[x]$ είναι τα πολυώνυμα βαθμού 1.

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 την ανάλυση, την τοπολογία, την άλγεβρα, την θεωρία αριθμών, ακόμα και από τη θεωρία πιθανοτήτων.

Στο εξάμηνο αυτό θα δώσουμε μία αλγεβρική απόδειξη του Θεμελιώδους Θεωρήματος της Άλγεβρας χρησιμοποιώντας τις βασικές ιδέες της Θεωρίας Galois.

1.1.3 Τύποι για τις ρίζες πολυωνύμων

Έως τον 19 αιώνα, ο όρος *Άλγεβρα* είχε να κάνει με την επίλυση πολυωνυμικών εξισώσεων. Όπως είδαμε προηγουμένως το Θεμελιώδες Θεώρημα της Άλγεβρας εγγυάται την ύπαρξη ριζών όχι όμως και την εύρεση τους. Τύποι για την εύρεση ριζών πολυωνύμων βαθμού 1 και πολυωνύμων βαθμού 2 ήταν γνωστοί από την αρχαιότητα: οι Μεσοποτάμιοι, Αιγύπτιοι και αρχαίοι Έλληνες είχαν ασχοληθεί με τέτοια προβλήματα. Αναφέρουμε επίσης τον Διόφαντο και τους Άραβες μαθηματικούς για σημαντική πρόοδο σε αυτά τα προβλήματα και τη διερεύνηση των ριζών στη περίπτωση βαθμού 3. Τον 16 αιώνα Ιταλοί Μαθηματικοί (dal Ferro, Cardano, Tartaglia, Ferrari) βρήκαν τύπους για την εύρεση ριζών πολυωνύμων βαθμού 3 και 4. Σημειώνουμε ότι στους τύπους αυτούς εμπεριέχονται οι πράξεις της πρόσθεσης/αφαίρεσης, του πολλαπλασιασμού/διαίρεσης και της αναγωγής σε δυνάμεις/ριζικά χρησιμοποιώντας τους συντελεστές του πολυωνύμου. Για παράδειγμα ο τύπος για την εύρεση μίας ρίζας του πολυωνύμου $x^3 + mx - n = 0$ είναι

$$\sqrt[3]{\frac{n}{2} + \sqrt{(\frac{n}{2})^2 + (\frac{m}{3})^3}} - \sqrt[3]{-\frac{n}{2} + \sqrt{(\frac{n}{2})^2 + (\frac{m}{3})^3}} \; . \tag{1.1}$$

Οι τύποι αυτοί γίνονται ακόμα πιο πολύπλοκοι για πολυώνυμα τετάρτου βαθμού. Όλοι αυτοί οι τύποι περιγράφουν την *επίλυση* πολυωνύμων έως και τετάρτου βαθμού *με την χρήση των ριζικών*. Σημειώνουμε ότι οι τύποι αυτοί ανάγκασαν τους μαθηματικούς της εποχής να αποδεχτούν το μυστήριο της άλγεβρας των φανταστικών αριθμών. Μετά την επίλυση με ριζικά του τεταρτοβάθμιου πολυωνύμου η προσπάθεια επικεντρώθηκε στην εύρεση αντίστοιχουν τύπου για τις ρίζες των πολυωνύμων πέμπτου βαθμού. Ο πρώτος που ισχυρίστηκε γραπτά ότι δεν υπάρχει τέτοιος τύπος ήταν ο Ιταλός μαθηματικός Ruffini

το 1799 σε μία εργασία όπου εισήγαγε για πρώτη φορά η έννοια της *ομάδας* των μεταθέσεων. Ο Lagrange είχε ορίσει τις μεταθέσεις ως μεμονωμένα στοιχεία-συναρτήσεις, 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 την 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. Το θεώρημα των Abel-Ruffini λέει ότι

Θεώρημα 1.1.4. *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. Για παράδειγμα ας θεωρήσουμε το πολυώνυμο $f(x) = x^5 - 2 \in \mathbb{C}[x]$. Μία ρίζα του $f(x)$ είναι $b = \sqrt[5]{2}$. Αφού $f(x) = (x - b)q(x)$ και $\deg q(x) = 4$, το πολυώνυμο $q(x)$, και κατά συνέπεια και το $f(x)$, είναι επιλύσιμα με ριζικά.
Ο πρώτος που αντιλήφθηκε ότι η εύρεση ενός τύπου για τις ρίζες ενός πολυωνύμου $f(x)$ συνδέεται με τη δομή της ομάδας των *επιτρεπτών* μεταθέσεων των ριζών του $f(x)$ είναι ο Galois το 1831. Η ομάδα αυτών των επιτρεπτών μεταθέσεων ονομάζεται ομάδα του Galois του $f(x)$. Σε επόμενη ενότητα θα ορίσουμε αυτήν την ομάδα αναλυτικά και θα αποδείξουμε το θεώρημα που λέει τα εξής ως προς την επυλισιμότητα με ριζικά:

Θεώρημα 1.1.5. *Τα πολυώνυμα για τα οποία υπάρχει κάποιος τύπος εύρεσης των ριζών που να εμπεριέχει πρόσθεση/αφαίρεση, πολλαπλασιασμό/διαίρεση και αναγωγή σε δυνάμεις/ριζικά των συντελεστών τους, είναι ακριβώς εκείνα για τα οποία η αντίστοιχη ομάδα του Galois είναι επιλύσιμη.*

Η έννοια της *επιλυσιμότητας* μίας ομάδας προέρχεται όπως θα δούμε από τη Θεωρία Ομάδων. Για να αποδείξουμε το παραπάνω θεώρημα θα χρειαστούμε το Θεμελιώδες Θεώρημα της Θεωρίας Galois που περιγράφουμε σε αδρές γραμμές.

Θεώρημα 1.1.6. *Έστω $\Bbbk$ σώμα και $f(x) \in \Bbbk[x]$. Έστω E το μικρότερο σώμα που περιέχει το $\Bbbk$ και όλες τις ρίζες του $f(x)$. Υπάρχει μία πλήρης αντιστοιχία ανάμεσα στα υποσώματα του E που περιέχουν το $\Bbbk$ και στις υποομάδες της ομάδας Galois του $f(x)$.*

Παραλλείψαμε σκόπιμα κάποιες συνθήκες στο παραπάνω θεώρημα για να κάνουμε κατανοητή τη βασική ιδέα. Για παράδειγμα το θεώρημα ισχύει για μία ειδική

τάξη πολυωνύμων, τα *διαχωρίσιμα* πολυώνυμα. Ένα άλλο σημείο όπου θα επιμείνουμε αργότερα είναι η έννοια του *μικρότερου* σώματος που περιέχει το $\mathbb{k}$ 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 αναλυτικά στη συνέχεια του εξαμήνου.

1.1.7 Κατασκευές με κανόνα και διαβήτη.

Τα εργαλεία μας είναι ο κανόνας και ο διαβήτης. Ξεκινάμε με δύο καθορισμένα σημεία τα οποία δεχόμαστε ως *κατασκευάσιμα*. Με τον κανόνα μπορούμε να χαράξουμε γραμμές ανάμεσα σε δύο κατασκευάσιμα σημεία. Με τον διαβήτη μπορούμε να χαράξουμε κύκλους που το κέντρο τους να είναι κάποιο κατασκευάσιμο σημείο και που η ακτίνα του κύκλου να είναι η απόσταση ανάμεσα σε δύο κατασκευάσιμα σημεία. Ξεκινάμε λοιπόν με δύο κατασκευάσιμα σημεία, και επιθυμούμε να βρούμε όλα τα σημεία που κατασκευάζονται με τρεις τρόπους: είτε ως σημεία τομής ανάμεσα σε δύο επιτρεπόμενες ευθείες, είτε ως σημεία τομής ανάμεσα σε μία επιτρεπόμενη ευθεία και έναν επιτρεπόμενο κύκλο είτε ως σημεία τομής ανάμεσα σε δύο επιτρεπόμενους κύκλους. Με αυτόν τον τρόπο βρίσκουμε τις κατασκευάσιμες αποστάσεις που είναι αποστάσεις ανάμεσα σε δύο κατασκευάσιμα σημεία όπως και τα κατασκευάσιμα σχήματα που ορίζονται από τα κατασκευάσιμα σημεία.

Ονομάζουμε την απόσταση ανάμεσα στα δύο αρχικά σημεία 1 ενώ τα αρχικά σημεία τα ονομάζουμε $(0,0)$ και $(1,0)$. Το $(2,0)$ είναι κατασκευάσιμο αφού προκύπτει ως σημείο τομής της ευθείας που περνάει από τα δύο αρχικά σημεία με τον κύκλο που έχει κέντρο το $(1,0)$ και ακτίνα 1. Με τον ίδιο τρόπο μπορούμε να προσδιορίσουμε και το $(-1,0)$. Προκύπτει εύκολα ότι κατασκευάζονται όλα τα σημεία με συντεταγμένες $(n,0) : \ n \in \mathbb{Z}$. Μπορούμε επίσης να χαράξουμε τη διχοτόμο ενός ευθύγραμμου τμήματος, καθώς και γενικότερα μία ευθεία κάθετη ως προς μία άλλη ευθεία που να περνάει από δοθέν κατασκευασμένο σημείο. Χρησιμοποιώντας τα παραπάνω και τις ιδιότητες των ομοίων τριγώνων δεν είναι δύσκολο να δείξει κανείς ότι αν a, b είναι κατασκευάσιμες αποστάσεις $b \neq 0$ τότε $a \pm b$, $a \cdot b$, a/b, $\sqrt{a}$ είναι και αυτές κατασκευάσιμες. Δηλαδή όλα τα σημεία του συνόλου $\{(a,b) : \ a^2, b^2 \in \mathbb{Q}\}$ είναι κατασκευάσιμα. Μπορούμε επίσης εύκολα να κατασκευάσουμε σημεία που ορίζουν την διχοτόμο μίας γωνίας, δηλαδή η διχοτόμηση μίας γωνίας είναι κατασκευάσιμη. Μπορούμε επίσης να ξεφύγουμε από το επίπεδο και να φανταστούμε τώρα τα σημεία μας στο τριδιάστατο ή πολυδιάστατο Ευκλείδιο χώρο. Κάποια από τα παρακάτω ερωτήματα είχαν απασχολήσει τους μαθηματικούσ-γεωμέτρες από την αρχαιότητα. Στο εξάμηνο αυτό θα αποκτήσουμε τα εργαλεία για να δώσουμε πλήρεις απαντήσεις σε αυτά.

- Ποιές αποστάσεις είναι κατασκευάσιμες;
- Μπορούμε να κατασκευάσουμε την τριχοτόμηση μίας γωνίας;
- Μπορούμε να κατασκευάσουμε τον κύβο με τον διπλάσιο όγκο ενός άλλου κύβου;
- Μπορούμε να τετραγωνίσουμε τον κύκλο χρησιμοποιώντας μόνο κανόνα και διαβήτη;
- Ποιά κανονικά πολύγωνα μπορούμε να κατασκευάσουμε;

1.2 Δύο παραδείγματα

Στην ενότητα αυτή θα μελετήσουμε δύο τριτοβάθμια πολυώνυμα στα οποία θα επιστρέφουμε συχνά για να τοζίσουμε επιμέρους κομμάτια της θεωρίας μας. Θυμίζουμε ότι όταν $\Bbbk$ είναι κάποιο σώμα και $0 \neq f(x) \in \Bbbk[x]$ τότε το $f(x)$ λέγεται ανάγωγο (στο $\Bbbk[x]$) αν κάθε φορά που $f(x) = q_1(x)q_2(x)$ όπου $q_1(x), q_2(x) \in \Bbbk[x]$ τότε ένα από τα δύο πολυώνυμα $q_1(x)$, $q_2(x)$ έχει βαθμό 0. Κανονικά πολυώνυμα είναι αυτά που ο συντελεστής του μεγιστοβάθμιου όρου τους είναι 1.

1.2.1 Το πολυώνυμο $x^3 - 2$.

Μελετάμε καταρχήν το κανονικό πολυώνυμο $f(x) = x^3 - 2$ και βρίσκουμε τους ανάγωγους παράγοντες του $f(x)$ στο $\mathbb{Q}[x]$, $\mathbb{R}[x]$, και στο $\mathbb{C}[x]$. Ξεκινάμε βρίσκοντας τις ρίζες του $f(x)$ στο $\mathbb{C}$. Παρατηρούμε ότι $b = \sqrt[3]{2}$ είναι μία ρίζα του $f(x)$, (είναι και η ρίζα που προκύπτει από τον τύπο 1.1 αντικαθιστώντας $m = 0$, $n = 2$). Έπεται ότι 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 εύερσης των ριζών δευτεροβάθμιου πολυωνύμου βρίσκουμε ότι οι άλλες δύο ρίζες του $x^3 - 2$ είναι:

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

Θέτουμε τώρα

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

Παρατηρούμε ότι

$$\omega^0 = \omega^3 = e^{2\pi i} = 1 \ , \omega = e^{2\pi i/3} = \cos(\frac{2\pi}{3}) + i\sin(\frac{2\pi}{3}) \ , \omega^2 = -\frac{1}{2} - \frac{i\sqrt{3}}{2} \ .$$

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:

- Καμία από τις ρίζες του $f(x)$ δεν ανήκει στο $\mathbb{Q}$. Αυτό σημαίνει ότι δεν υπάρχει πολυώνυμο βαθμού 1 στο $\mathbb{Q}[x]$ που να διαρεί το $f(x)$. Άρα $f(x)$ είναι ανάγωγο στον $\mathbb{Q}[x]$.

- Αφού το b και οι συντελεστές του $q(x)$ ανήκουν στον $\mathbb{R}$ ισχύει ότι $f(x) = (x-b)q(x)$ στον $\mathbb{R}[x]$. Άρα $f(x)$ δεν είναι ανάγωγο στον $\mathbb{R}[x]$. Οι ρίζες του $q(x)$ δεν ανήκουν στον $\mathbb{R}$ και επομένως $q(x)$ είναι ανάγωγο στον $\mathbb{R}[x]$. Στον δακτύλιο $\mathbb{R}[x]$ η ανάλυση του $f(x)$ σε ανάγωγους παράγοντες είναι το γινόμενο $f(x) = (x-b)q(x)$.

- Η ανάλυση του $f(x)$ σε ανάγωγους παράγοντες στο $\mathbb{C}[x]$ είναι είναι το γινόμενο $f(x) = (x-b)(x-\omega b)(x-\omega^2 b)$.

Θα κλείσουμε αυτό το παράδειγμα γενικεύοντας τις παρατηρήσεις μας.

Παρατηρήσεις 1.2.2. *Έστω $\Bbbk$ ένα σώμα και $f(x) \in \Bbbk[x]$.*

- *Υπάρχει $b \in \Bbbk$ έτσι ώστε $f(b) = 0$ αν και μόνο αν $f(x) = (x-b)q(x)$ όπου $q(x) \in \Bbbk[x]$.*

- *Αν $\deg f(x) = 1$ τότε $f(x)$ είναι ανάγωγο.*

- *Αν $\deg f(x) = 2,\ 3$ τότε $f(x)$ είναι ανάγωγο αν και μόνο αν $f(x)$ δεν έχει ρίζες στο $\Bbbk$.*

- *Αν $\Bbbk \subset F$ όπου το F είναι σώμα και $f(x)$ είναι ανάγωγο στο $F[x]$, τότε $f(x)$ είναι ανάγωγο στο $\Bbbk[x]$.*

1.2.3 Το πολυώνυμο $x^n - 1$.

Στο παράδειγμα αυτό θα εξετάσουμε αναλυτικά το πολυώνυμο $f(x) = x^3 - 1$. Το πολυώνυμο αυτό δεν είναι ανάγωγο στο $\mathbb{Q}[x]$ αφού $f(1) = 0$ και

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

Καλούμε το πολυώνυμο $\Phi_3(x) = x^2 + x + 1$ το *τρίτο κυκλοτομικό* πολυώνυμο της μονάδας. Γνωρίσαμε τις ρίζες του $\Phi_3(x)$ στο προηγούμενο παράδειγμα: είναι οι συζυγείς μιγαδικοί αριθμοί ω και ω^2 όπου $\omega = e^{2\pi i/3}$. Είναι χρήσιμο να γράφουμε ω_3 αντί για ω για να τονίσουμε ότι $(\omega_3)^3 = \omega^3 = 1$. Οι τρεις λοιπόν ρίζες της μονάδας, δηλαδή οι ρίζες του πολυωνύμου $x^3 - 1$, είναι ω_3, ω_3^2 και $\omega_3^3 = 1$. Εύκολα επιβεβαιώνουμε ότι

1. $(x - \omega_3)(x - \omega_3^2) = x^2 + x + 1$

2. $\omega_3^2 + \omega_3 + 1 = 0$ και

3. $\omega_3 \cdot \omega_3^2 = 1$.

Το πολυώνυμο $\Phi_3(x)$ είναι ανάγωγο στον $\mathbb{R}[x]$ και στον $\mathbb{Q}[x]$, αλλά όχι βέβαια στον $\mathbb{C}[x]$. Οι επόμενες παρατηρήσεις γενικεύουν όσα έχουμε πει. Ορίζουμε την n-στή *πρωταρχική* ρίζα της μονάδας ω_n ως εξής:

$$\omega_n = e^{2\pi i/n} = \cos(\frac{2\pi}{n}) + i \sin(\frac{2\pi}{n})$$

και το n-στό *n-στο κυκλοτομικό* πολυώνυμο $\Phi_n(x)$:

$$\Phi_n(x) = x^{n-1} + x^{n-2} + \cdots + x + 1 \ .$$

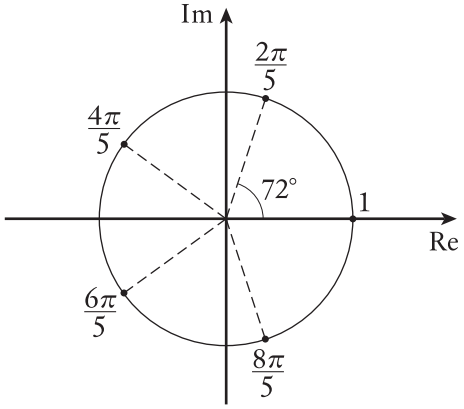
Ισχύουν τα παρακάτω:

- $x^n - 1 = (x - 1)\Phi_n(x)$,

- οι ρίζες του $\Phi_n(x)$ στο $\mathbb{C}$ είναι οι ω_n, ω_n^2, $\ldots$, ω_n^{n-1}, που μαζί με το 1 είναι οι n-στές ρίζες της μονάδας,

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

Θα δούμε ότι το πολυώνυμο $\Phi_n(x)$ είναι ανάγωγο στο $\mathbb{Q}[x]$ όταν n είναι πρώτος. Είναι επίσης χρήσιμο να έχουμε κατά νου τη γραφική παράσταση των n-στών ριζών της μονάδας στο επίπεδο. Βρίσκονται επί του μοναδιαίου κύκλου σε γωνίες που αντιστοιχούν σε πολλαπλάσια του $2\pi/n$. Για παράδειγμα για $n = 5$ έχουμε ότι



Έτσι όταν $n = 4$ τότε $\omega_4 = e^{\pi i/2} = i$. Παρατηρούμε ότι $\Phi_4(x) = x^3 + x^2 + x + 1 = (x + 1)(x^2 + 1)$ και ότι $\Phi_4(x)$ δεν είναι ανάγωγο στο $\mathbb{Q}[x]$. Τέλος τονίζουμε ότι από τη γραφική παράσταση των ριζών της μονάδας προκύπτει ότι οι μόνες πιθανές ρίζες του $\Phi_n(x)$ που βρίσκονται στον άξονα των πραγματικών αριθμών είναι ± 1.

1.3 Βασικές ιδιότητες των πολυωνύμων

Έστω ότι $\Bbbk$ είναι σώμα. Συγκεντρώνουμε κάποιες από τις βασικές ιδιότητες του δακτυλίου πολυωνύμων $\Bbbk[x]$. Θυμίζουμε ότι ένα υποσύνολο I του $\Bbbk[x]$ είναι ιδεώδες αν ικανοποιούνται οι παρακάτω ιδιότητες:

- $f_1(x), f_2(x) \in I$ τότε $f_1(x) - f_2(x) \in I$,
- $f(x) \in I$, $g(x) \in \Bbbk[x]$ τότε $g(x) \cdot f(x) \in I$.

Έστω ότι $f(x) \in \Bbbk[x]$. Τότε το σύνολο $(f(x)) := \{q(x)f(x) : \ q(x) \in \Bbbk[x]\}$ είναι ιδεώδες του $\Bbbk[x]$ και $f(x)$ καλείται γεννήτορας ή παράγον στοιχείο για αυτό το ιδεώδες ενώ $I = (f(x))$ λέγεται κύριο ιδεώδες. Δύο πολυώνυμα $f(x)$, $g(x)$ είναι *γεννήτορες* για το ίδιο ιδεώδες, $(f(x)) = (g(x))$, όταν $f(x) = cg(x)$, $c \in \Bbbk$. Για παράδειγμα στον δακτύλιο $\mathbb{C}[x]$ ισχύει η ισότητα των παρακάτω δύο ιδεωδών: $(x^2 + 1) = (2x^2 + 2)$. Ισχύουν τα εξής:

Παρατηρήσεις 1.3.1.

1. Ο δακτύλιος $\Bbbk[x]$ είναι $\Bbbk$-διανυσματικός χώρος. Μία $\Bbbk$-βάση του $\Bbbk[x]$ είναι το σύνολο $\{x^i : \ i \in \mathbb{N}\}$ και $\dim_{\Bbbk}\Bbbk[x] = \infty$.
2. Ο δακτύλιος $\Bbbk[x]$ είναι ακεραία περιοχή. Ο βαθμός του γινομένου δύο πολυωνύμων είναι ίσος με το άθροισμα των βαθμών των δύο πολυωνύμων.

3. Ο δακτύλιος $\Bbbk[x]$ είναι δακτύλιος κυρίων ιδεωδών. Για κάθε λοιπόν ιδεώδες I του $\Bbbk[x]$ υπάρχει κάποιο $f(x) \in \Bbbk[x]$ έτσι ώστε $I = (f(x))$. Όταν $I \neq 0$, μας ενδιαφέρει ο κανονικός γεννήτορας $f(x)$ του I.

4. Το ιδεώδες $I = (f(x))$ του $\Bbbk[x]$ είναι μέγιστο αν και μόνο αν $f(x)$ είναι ανάγωγο. Άρα όταν $f(x)$ είναι ανάγωγο πολυώνυμο του $\Bbbk[x]$ τότε $\Bbbk[x]/I$ είναι σώμα.

5. Τα πρώτα ιδεώδη του $\Bbbk[x]$ είναι εκείνα τα ιδεώδη I με την ιδιότητα $\Bbbk[x]/I$ να είναι ακεραία περιοχή. Εκτός από το μηδενικό ιδεώδες όλα τα άλλα πρώτα ιδεώδη του $\Bbbk[x]$ είναι μέγιστα και ίσα με κάποιο ιδεώδες της μορφής $(f(x))$ όπου $f(x)$ είναι ανάγωγο πολυώνυμο.

6. Όταν $f(x)$ είναι ανάγωγο τότε μπορούμε να θεωρήσουμε ότι $\Bbbk$ είναι υπόσωμα του $\Bbbk[x]/(f(x))$ αφού ο ομομορφισμός δακτυλίων $\phi : \Bbbk \longrightarrow \Bbbk[x]/(f(x))$, όπου $\phi(c) = c + (f(x))$, είναι εμφύτευση: ο πυρήνας του ϕ είναι το μηδενικό ιδεώδες.

7. Ισχύει ο Ευκλείδειος αλγόριθμος στον $\Bbbk[x]$: έστω $f(x), g(x) \in R$, $f(x) \neq 0$. Τότε υπάρχουν μοναδικά πολυώνυμα $q(x), r(x) \in R$ έτσι ώστε $g(x) = f(x)q(x) + r(x)$, όπου είτε $r(x) = 0$ είτε $\deg r(x) < \deg q(x)$.

8. Ο δακτύλιος $\Bbbk[x]$ είναι δακτύλιος μονοσήμαντης ανάλυσης: έστω $0 \neq f(x) \in R$, $f(x)$ κανονικό. Τότε $f(x)$ παραγοντοποιείται σε γινόμενο αναγώγων κανονικών πολυωνύμων με μοναδικό τρόπο. Δηλαδή υπάρχουν κανονικά ανάγωγα $q_1(x), \ldots, q_s(x) \in \Bbbk[x]$ και εκθέτες $n_1, \ldots, n_s \in \mathbb{N}$, όπου $q_i(x) \neq q_j(x)$ για $i \neq j$ και $n_i > 0$ για $i = 1, \ldots, s$, έτσι ώστε

$$f(x) = q_1(x)^{n_1} \cdots q_s(x)^{n_s} \ .$$

   Αν δε $f(x) = g_1(x)^{m_1} \cdots g_t(x)^{m_t}$ είναι μία άλλη παραγοντοποίηση του $f(x)$ σε γινόμενο κανονικών αναγώγων πολυωνύμων όπου για $i \neq j$, $g_i(x) \neq g_j(x)$ και $0 < m_i \in \mathbb{N}$ για $i = 1, \ldots, t$ τότε $t = s$, $\{q_1, \ldots, q_s\} = \{g_1, \ldots, q_s\}$ ενώ οι αντίστοιχοι εκθέτες ταυτίζονται.

9. Έστω ότι $f(x), g(x) \in \Bbbk[x]$. Ο μέγιστος κοινός διαιρέτης των $f(x)$ και $g(x)$ στο $\Bbbk[x]$ υπάρχει, συμβολίζεται με $\text{ΜΚΔ}(f(x), g(x))$ και είναι το κανονικό πολυώνυμο μέγιστο βαθμού που διαιρεί το $f(x)$ και το $g(x)$. Ισχύει επίσης ότι ο γεννήτορας του ιδεώδους $(f(x), g(x)) = \{q_1(x)f(x) + q_2(x)g(x) : \ q_1(x), q_2(x) \in \Bbbk[x]\}$ είναι ο $\text{ΜΚΔ}(f(x), g(x))$. Τα πολυώνυμα $f(x)$ και $g(x)$ είναι πρώτα μεταξύ τους όταν $\text{ΜΚΔ}(f(x), g(x)) = 1$ και επομένως $(f(x), g(x)) = \Bbbk[x]$.

Παραδείγματα 1.3.2.

- Το ιδεώδες $I = (x^2 + 1)$ είναι μέγιστο στον $\mathbb{R}[x]$. Μπορούμε να θεωρήσουμε ότι το $\mathbb{R}$ είναι υπόσωμα του $\mathbb{R}[x]/I$ μέσω της εμφύτευσης $\phi_1 : \mathbb{R} \to \mathbb{R}[x]/I$, $\phi_1(c) = c + I$. Παρατηρούμε ότι τα στοιχεία του $\mathbb{R}[x]/I$ είναι της μορφής $f(x) + I$. Σύμφωνα όμως με τον Ευκλείδειο αλγόριθμο διαίρεσης $f(x) = (x^2 + 1)q(x) + r(x)$ όπου $r(x) \in \mathbb{Q}[x]$, $\deg(r(x)) \leq 1$, άρα $f(x) + I = r(x) + I$. Τα στοιχεία του $\mathbb{R}[x]/I$ είναι λοιπόν της μορφής $a + bx + I$: $a, b \in \mathbb{R}$. Ακόμα παρατηρούμε ότι η συνάρτηση $\phi_2 : \mathbb{R}[x]/I \to \mathbb{C}$, $\phi_2(a + bx + I) = a + bi$ είναι ισομορφισμός σωμάτων. Έτσι $\phi_3 = \phi_2 \circ \phi_1 : \mathbb{R} \to \mathbb{C}$, $\phi_3(c) = \phi_2 \circ \phi_1(c) = \phi_2(c+I) = c$ είναι η συνήθης εμφύτευση του $\mathbb{R}$ στο $\mathbb{C}$.

- Έστω $I = (x^2 - 3)$. Ο δακτύλιος $E = \mathbb{Q}[x]/I$ είναι σώμα αφού $x^2 - 3 \in \mathbb{Q}[x]$ είναι ανάγωγο. Τα στοιχεία του E είναι της μορφής $f(x) + I$ όπου $f(x) \in \mathbb{Q}[x]$. Σύμφωνα με τον Ευκλείδειο αλγόριθμο διαίρεσης $f(x) = (x^2 - 3)q(x) + r(x)$, όπου $r(x) \in \mathbb{Q}[x]$, $\deg(r(x)) < 2$ και $f(x) + I = r(x) + I$. Για παράδειγμα $x^2 + I = 3 + I$. Όπως είπαμε το E είναι σώμα. Δεν είναι δύσκολο να δει κανείς ότι $(x + I)^{-1} = \frac{1}{3}x + I$ ενώ $(x + 2 + I)^{-1} = -x + 2 + I$. Μπορούμε να θεωρήσουμε ότι το $\mathbb{Q}$ είναι υπόσωμα του E μέσω της εμφύτευσης $c \mapsto c + I$, ταυτίζοντας δηλαδή τα στοιχεία $c + I$ με τον αντιπρόσωπο c.

1.4 Ανάγωγα πολυώνυμα

Έστω ότι το $\Bbbk$ είναι σώμα. Τα ανάγωγα πολυώνυμα του $\Bbbk[x]$ παίζουν ένα σημαντικό ρόλο στη μελέτη μας. Σε προηγούμενη ενότητα δώσαμε ένα κριτήριο για πολυώνυμα βαθμού ≤ 3. Παρακάτω θυμίζουμε κάποια χρήσιμα κριτήρια κυρίως για πολυώνυμα στο $\mathbb{Q}[x]$. Ξεκινάμε με το θεώρημα του Gauss.

Θεώρημα 1.4.1. *Έστω ότι $f(x) = a_n x^n + \cdots + a_0 \in \mathbb{Z}[x]$ είναι πρωταρχικό, δηλαδή ο μέγιστος κοινός διαρέτης των $a_0, \ldots, a_n$ είναι 1, και έστω ότι $\deg f(x) > 0$. Τότε το $f(x)$ είναι ανάγωγο στο $\mathbb{Z}[x]$ αν και μόνο αν $f(x)$ είναι ανάγωγο στο $\mathbb{Q}[x]$.*

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

Πρόταση 1.4.2. *Έστω ότι $f(x) = a_n x^n + \cdots + a_0 \in \mathbb{Z}[x]$ με $\deg f(x) = n$. Αν $\frac{r}{s} \in \mathbb{Q}$ με $(r, s) = 1$ είναι ρίζα του $f(x)$ τότε $r \mid a_0$ και $s \mid a_n$. 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 $\mathbb{Q}$.*

Παραδείγματα 1.4.3.

- Το πολυώνυμο $x^3 - 3x - 1$ είναι ανάγωγο στον $\mathbb{Q}[x]$.
- Τα πολυώνυμα $x^2 - p$ και $x^3 - p$ είναι ανάγωγα στον $\mathbb{Q}[x]$, για p πρώτο.

Το επόμενο Θεώρημα είναι γνωστό ως Κριτήριο του Eisenstein.

Θεώρημα 1.4.4. *Έστω ότι $f(x) = a_n x^n + \cdots + a_0 \in \mathbb{Z}[x]$, $p \in \mathbb{Z}$ πρώτος. Αν ο p διαιρεί τους συντελεστές a_i για $i = 0, \ldots, n-1$, p δεν διαιρεί το a_n και p^2 δεν διαιρεί το a_0, τότε το $f(x)$ είναι ανάγωγο στο $\mathbb{Q}[x]$.*

Παράδειγμα 1.4.5. Έστω το πολυώνυμο $f(x) = 2/9x^5 + 5/3x^4 + x^3 + 1/3 \in \mathbb{Q}[x]$. Παρατηρούμε ότι $f(x)$ είναι ανάγωγο στο $\mathbb{Q}[x]$ αν και μόνο αν $9f(x) = 2x^5 + 15x^4 + 9x^3 + 3$ είναι ανάγωγο στο $\mathbb{Q}[x]$. Το κριτήριο του Eisenstein εφαρμόζεται στο $9f(x)$ για $p = 3$ και επομένως είναι ανάγωγο, άρα $f(x)$ είναι ανάγωγο.

Πρόταση 1.4.6. *Έστω $\Bbbk$ σώμα και $f(x) =\in \Bbbk[x]$. Το $f(x)$ είναι ανάγωγο αν και μόνο αν $g(x) = f(ax + b)$ είναι ανάγωγο, όπου $a, b \in \Bbbk$ και $a \neq 0$.*

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

Παραδείγματα 1.4.7.

- Στο $f(x) = x^{16} + x^{15} + \cdots + x + 1 \in \mathbb{Q}[x]$ δεν εφαρμόζεται το κριτήριο του Eisenstein. Όμως αν εφαρμόσουμε το κριτήριο του Eisenstein στο $f(x + 1)$ για $p = 17$ αποδεικνύουμε ότι αυτό είναι ανάγωγο στον $\mathbb{Z}[x]$, άρα $f(x)$ είναι ανάγωγο στον $\mathbb{Q}[x]$.
- Ομοίως, όταν $p \in \mathbb{Z}$ είναι πρώτος, το κυκλοτομικό πολυώνυμο $\Phi_p(x) = x^{p-1} + x^{p-2} + \cdots + x + 1 \in \mathbb{Q}[x]$ είναι ανάγωγο όπως προκύπτει εφαρμόζοντας το κριτήριο του Eisenstein στο $\Phi_p(x + 1)$ για p. Πράγματι $\Phi_p(x)(x - 1) = x^p - 1$. Άρα

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

$$= x^{p-1} + \binom{p}{1}x^{p-2} + \binom{p}{2}x^{p-3} + \cdots + p$$

Εφαρμόζουμε το κριτήριο του Eisenstein στο $\Phi_q(x+1)$ για p και προκύπτει ότι $\Phi_p(x + 1)$ είναι ανάγωγο άρα $\Phi_p(x)$ είναι ανάγωγο.

Το επόμενο κριτήριο ανάγει το πρόβλημα του αν $f(x) \in \mathbb{Z}[x]$ είναι ανάγωγο στο αντίστοιχο πρόβλημα στον δακτύλιο $\mathbb{Z}_p[x]$ για κάποιον πρώτο $p \in \mathbb{Z}$. Θεωρούμε τον φυσικό ομομορφισμό $\phi : \mathbb{Z} \to \mathbb{Z}_p$, $a \mapsto \overline{a} \equiv a \mod p$. Ο ψ επεκτείνεται στον ομομορφισμό δακτυλίων

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

Πρόταση 1.4.8. *Έστω $f(x) \in \mathbb{Z}[x]$, p πρώτος και $\deg f(x) = \deg \Phi(f(x))$. Αν $\Phi(f(x))$ είναι ανάγωγο στο $\mathbb{Z}_p[x]$, τότε $f(x)$ είναι ανάγωγο στον δακτύλιο $\mathbb{Z}[x]$.*

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 $\Phi(f(x))$ είναι ευκολότερη εργασία.

Παραδείγματα 1.4.9.

- Τα πολυώνυμα $x^2 + x + 1$, $x^3 + x + 1$ και $x^3 + x^2 + 1$ είναι ανάγωγα στο $\mathbb{Z}_2[x]$ αφού δεν έχουν ρίζες στο $\mathbb{Z}_2$. Έπεται ότι $x^2 + x + 1$, $x^3 + x + 1$ και $x^3 + x^2 + 1$ είναι ανάγωγα στο $\mathbb{Z}[x]$ όπως και στο $\mathbb{Q}[x]$.

- Το πολυώνυμο x^2+1 δεν είναι ανάγωγο στο $\mathbb{Z}_2[x]$ αφού $x^2+1 = (x+1)^2$ στο $\mathbb{Z}_2[x]$. Είναι όμως ανάγωγο στο $\mathbb{Z}[x]$. Το αντίστροφο λοιπόν της Πρότασης 1.4.8 δεν ισχύει.

- Τα ανάγωγα πολυώνυμα βαθμού ≤ 4 του $\mathbb{Z}_2[x]$ είναι τα x, $x+1$, x^2+x+1, $x^3 + x + 1$, $x^3 + x^2 + 1$ $x^4 + x^3 + 1$, $x^4 + x + 1$, $x^4 + x^3 + x^2 + x + 1$. Ελέγχοντας πιθανούς παράγοντες βαθμού 1,2,3 εύκολα προκύπτει ότι το πολυώνυμο x^6+x^3+1 είναι και αυτό ανάγωγο στο $\mathbb{Z}_2[x]$. Τα πολυώνυμα $7x^4+5x^3+3$ και x^6+11x^3-1 του $\mathbb{Q}[x]$ είναι ανάγωγα, αφού τα πολυώνυμα $x^4 + x^3 + 1$ και $x^6 + x^3 + 1$ είναι ανάγωγα στο $\mathbb{Z}_2[x]$.

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

Τονίζουμε ότι για να ελέγξουμε αν $f(x)$ είναι ανάγωγο στο $\Bbbk[x]$ όπου $\Bbbk$ σώμα, αρκεί να ελέγξουμε αν κάποιο ανάγωγο πολυώνυμο βαθμού $\leq 1/2 \deg f(x)$ διαρεί $f(x)$.

1.5 Εύρεση ριζών

Έστω ότι το $\Bbbk$ είναι σώμα. Λέμε ότι το $q(x)$ διαιρεί το $f(x)$ στον $\Bbbk[x]$ και συμβολίζουμε $q(x) | f(x)$ αν υπάρχει $q(x) \in \Bbbk[x]$ έτσι ώστε $f(x) = q(x)q(x)$.

Πρόταση 1.5.1. *Έστω $f(x) \in \Bbbk[x]$. Το $a \in \Bbbk$ είναι ρίζα του $f(x)$ αν και μόνο αν $(x-a) | f(x)$ στον $\Bbbk[x]$.*

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

Πρόταση 1.5.2. *Έστω $f(x) \in \Bbbk[x]$ και $\deg f(x) = n < \infty$. Τότε το $f(x)$ έχει το πολύ n ρίζες στο $\Bbbk$.*

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

Ορισμός 1.5.3. *Λέμε ότι το $f(x) \in \Bbbk[x]$ με $\deg f(x) = n < \infty$ αναλύεται σε γινόμενο γραμμικών παραγόντων στο $\Bbbk[x]$ αν $f(x) = c(x-a_1)\cdots(x-a_n)$ όπου $c, a_1, \ldots, a_n \in \Bbbk$.*

Παραδείγματα 1.5.4.

- Το x^2+1 αναλύεται σε γινόμενο γραμμικών παραγόντων στο $\mathbb{C}[x]$.
- Σε προηγούμενο παράδειγμα εξετάσαμε το σώμα $E = \mathbb{R}[y]/(y^2+1)$. Σε αυτό το παράδειγμα θα δείξουμε ότι το πολυώνυμο $f(x) = x^2+1$ αναλύεται σε γινόμενο γραμμικών παραγόντων στο $E[x]$. Όπου χρειάζεται χρησιμοιούμε δείκτες για να τονίσουμε το σώμα στο οποίο ανήκουν τα στοιχεία μας. Έτσι $1_E = 1_{\mathbb{R}} + I$, όπου I είναι το ιδεώδες $I = (y^2 + 1_{\mathbb{R}})$ του $\mathbb{R}[y]$. Έστω $a = y + I$. Αφού $-y^2 + I = 1_{\mathbb{R}} + I = 1_E$ έχουμε ότι

$$(x-a)(x+a) = (x-(y+I))(x+(y+I))$$

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

  Από τα παραπάνω έπεται ότι a είναι ρίζα του $f(x)$ στο E.
- Έστω $I = (x^2-3)$ και $E = \mathbb{Q}[x]/I$. Όπως προηγουμένως προκύπτει ότι $y^2 - 3 = (y-b)(y+b)$ όπου $b = x + I$ και $\pm b$ είναι οι ρίζες του y^2-3 στο E.

Θα γενικεύσουμε το προηγούμενο παράδειγμα με το εξής θεώρημα:

Θεώρημα 1.5.5. *Έστω $\Bbbk$ σώμα και $p(x)$ ένα ανάγωγο πολυώνυμο του $\Bbbk[x]$. Τότε το $p(x)$ έχει μία ρίζα στο $\Bbbk[y]/(p(y))$.*

Απόδειξη. Έστω ότι $I = (p(y))$ και $E = \Bbbk[y]/I$. Εμφυτεύουμε $\Bbbk$ στο E: $\Bbbk \to E$, $c \mapsto c + (p(y))$. Παρατηρούμε ότι $y + I \in E$ είναι ρίζα του $p(x)$. Πράγματι έστω ότι $p(x) = a_0 + a_1x + \cdots + a_nx^n \in \Bbbk[x]$. Τότε

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

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

□

Λέμε ότι το σώμα F είναι *επέκταση* του σώματος $\Bbbk$ και συμβολίζουμε με $L/\ \Bbbk$ αν ισχύει ο εγκλεισμός σωμάτων $\Bbbk \subset F$. Το επόμενο Θεώρημα είναι γνωστό ως Θεώρημα του Kronecker.

Θεώρημα 1.5.6. *(Kronecker) Έστω $f(x) \in \Bbbk[x]$ όπου το $\Bbbk$ είναι σώμα. Υπάρχει μία επέκταση $L/\ \Bbbk$ τέτοια 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 $L = \Bbbk$. Έστω ότι $\deg f(x) > 1$ και $f(x) = g(x)p(x)$ όπου τα $p(x), g(x) \in \Bbbk[x]$ 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 1.5.5, υπάρχει μία επέκταση $M/\ \Bbbk$ 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 $\Bbbk$. □

Από το Θεώρημα του Kronecker προκύπτει ότι 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 $c \in \Bbbk$ και $a_i \in L$, $a_i \neq a_J$, $1 \leq i \leq t$. 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 των ριζών $a_1, \ldots, a_t$ αντίστοιχα.
Η επόμενη πρόταση είναι χρήσιμη προκειμένου να δούμε αν $f(x)$ έχει πολλαπλές ρίζες σε ένα σώμα L, όπου το $f(x)$ αναλύεται σε γραμμικούς παράγοντες.

Πρόταση 1.5.7. *Έστω $f(x) = c_0 + c_1x + \cdots + c_nx^n \in \Bbbk[x]$ όπου $\Bbbk$ σώμα, L σώμα όπου $f(x)$ αναλύεται σε γραμμικούς παράγοντες. Συμβολίζουμε με $f'(x)$ την παράγωγο του $f(x)$, δηλαδή $f'(x) = c_1 + 2c_2x + \cdots + nc_nx^{n-1}$. Το $f(x)$ έχει πολλαπλές ρίζες στο L αν και μόνο αν ΜΚΔ$(f(x), f'(x)) \neq 1$.*

Απόδειξη. Ο υπολογισμός του ΜΚΔ$(f(x), f'(x))$ είναι ο ίδιος είτε αυτός γίνεται στο $\Bbbk$ είτε στο L. 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 $x - a_i$ διαιρεί το $f(x)$ και το $f'(x)$, δηλαδή ΜΚΔ$(f(x), f'(x)) \neq 1$. Το αντίστροφο προκύπτει ανάλογα. □

Παρατηρούμε ότι όταν $g(x) \in \Bbbk[x]$ είναι ανάγωγο, τότε οι μόνοι διαιρέτες του στο $\Bbbk[x]$ είναι τα σταθερά μη μηδενικά πολυώνυμα και το $g(x)$. Αν η χαρακτηριστική του $\Bbbk$ είναι 0 τότε $g'(x) \neq 0$ και $\deg g'(x) = \deg g(x) - 1$. Συγκρίνοντας τους βαθμούς, έπεται ότι $g(x)$ δεν διαιρεί το $g'(x)$ και άρα ΜΚΔ$(g(x), g'(x)) = 1$. Έτσι σύμφωνα με τη Πρόταση 1.5.7, όλες οι ρίζες του $g(x)$ είναι απλές. Ένα ανάγωγο πολυώνυμο $g(x) \in \Bbbk[x]$ λέγεται *διαχωρίσιμο* αν οι ρίζες του σε ένα σώμα ανάλυσης του $g(x)$ είναι απλές. Γενικότερα το πολυώνυμο $f(x) \in \Bbbk[x]$ λέγεται *διαχωρίσιμο* αν όλοι οι ανάγωγοι παράγοντες του $f(x)$ είναι διαχωρίσιμοι σε ένα σώμα ανάλυσης του $f(x)$. Ισχύει λοιπόν το εξής:

Πόρισμα 1.5.8. *Έστω $\Bbbk$ σώμα, $f(x) \in \Bbbk[x]$. Αν $\Bbbk$ έχει χαρακτηριστική 0 τότε $f(x)$ είναι διαχωρίσιμο.*

Αν $\Bbbk$ έχει χαρακτηριστική p, όπου p πρώτος, τότε πρέπει να είμαστε πιο προσεκτικοί. Εάν η παράγωγος $f'(x)$ είναι μηδέν τότε ο μέγιστος κοινός διαιρέτης των $f(x)$ και $f'(x)$ είναι το $f(x)$ και το $f(x)$ έχει πολλαπλές ρίζες. Όταν λοιπόν $f(x)$ είναι ανάγωγο και $f'(x) = 0$ τότε το $f(x)$ δεν είναι διαχωρίσιμο.

Παραδείγματα 1.5.9.

- 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.
- Έστω $f(x) = x^{p^n} + x \in \mathbb{Z}_p[x]$ όπου p πρώτος. Οι ρίζες του $f(x)$ είναι απλές. Πράγματι η χαρακτηριστική του $\mathbb{Z}_p[x]$ είναι p, $f'(x) = p^n x^{p^n - 1} + 1 = 1$ και ΜΚΔ$(f(x), f'(x)) = 1$.
- Έστω $f(x) = x^p - x + a \in \mathbb{Z}_p[x]$ όπου p πρώτος. Αφού $f'(x) = -1$, έπεται ότι οι ρίζες του $f(x)$ είναι απλές.

- Έστω $\Bbbk = \mathbb{Z}_2(t) = \{a(t)/b(t) : \ a(t), b(t) \in \mathbb{Z}_2[t], b(t) \neq 0\}$. Μπορεί εύκολα να αποδειχτεί ότι το πολυώνυμο $f(x) = x^2 - t \in \Bbbk[x]$ είναι ανάγωγο αφού δεν έχει ρίζες στο $\Bbbk$. Αφού $f'(x) = 0$, $f(x)$ δεν είναι διαχωρίσιμο.

Έστω $\Bbbk$ σώμα, $f(x) \in \Bbbk[x]$. Σύμφωνα με το θεώρημα του Kronecker υπάρχει επέκταση $L/\ \Bbbk$ όπου το $f(x)$ αναλύεται σε γραμμικούς παράγοντες. Εάν δεν υπάρχει ενδιάμεση επέκταση $\Bbbk \subsetneqq F \subsetneqq L$ έτσι ώστε $f(x)$ να αναλύεται σε γραμμικούς παράγοντες στο $F[x]$ τότε $L/\ \Bbbk$ λέγεται *σώμα ανάλυσης* του $f(x)$ πάνω από το $\Bbbk$.

Παράδειγμα 1.5.10. 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 $\mathbb{R}[x]$. Στο επόμενο κεφάλαιο θα δούμε ότι το $\mathbb{R}$ δεν είναι σώμα ανάλυσης του $x^2 + 1$ πάνω από το $\mathbb{Q}$ και θα μάθουμε πως να κατασκευάζουμε σώματα ανάλυσης πολυωνύμων.

1.6 Ασκήσεις

1. Να εξετάσετε αν τα παρακάτω πολυώνυμα του $\mathbb{Q}[x]$ είναι ανάγωγα:
   - $f_1(x) = x^9 + 4x + 6$,
   - $f_2(x) = x + 1$,
   - $f_3(x) = x^4 + 4$,
   - $f_4(x) = 8x^3 - 6x - 1$,
   - $f_5(x) = x^4 - 2x^2 + 9$,
   - $f_6(x) = x^4 + 1$,
   - $f_7(x) = x^7 + 7x + 14$,
   - $f_8(x) = x^{(p-1)p} + x^{(p-2)^p} + \cdots + x^{2p} + x^p + 1$, ($p$ πρώτος),
   - $f_9(x) = 4/3x^5 + 6/5x^2 + 2$, $f_{10}(x) = x^5 - 10x + 2$,
   - $f_{11}(x) = x^5 - 10x + 1$.
2. Να εξετάσετε αν τα παρακάτω πολυώνυμα είναι ανάγωγα:
   - $x^4 + 4 \in Z_3[x]$,
   - $x^4 + 4 \in Z_{13}[x]$,
   - $x^2 + 3 \in Z_7[x]$.
3. Να δείξετε ότι το πολυώνυμο $x^2 - 5$ είναι ανάγωγο υπεράνω του $\mathbb{Q}(\sqrt{2})$.

4. Να βρείτε ανάγωγο πολυώνυμο βαθμού 12 υπεράνω του $\mathbb{Q}$.

5. Να βρείτε ανάγωγο πολυώνυμο βαθμού 12 υπεράνω του $\mathbb{Z}_3$.

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

7. Να ελέγξετε αν $\mathbb{Q}[\sqrt{3}]$ είναι ισόμορφος με τον δακτύλιο $\mathbb{Q}[\sqrt{5}]$.

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

9. Να βρείτε τον αντίστροφο του $\sqrt[5]{2}^{\,3} + 4$ στον δακτύλιο $\mathbb{Q}[\sqrt[5]{2}]$.

10. Να βρείτε ένα σώμα ανάλυσης για το πολυώνυμο $f(x) = x^2 - t$ πάνω από το $\Bbbk = \mathbb{Z}_2(t)$ και να δείξετε ότι $f(x)$ έχει μία διπλή ρίζα.

11. Να εντοπίσετε γραφικά στο μιγαδικό επίπεδο τις ρίζες του $\sqrt[3]{a+bi}$. Να δείξετε ότι ερμηνεύοντας σωστά τον τύπο $\sqrt[3]{a+bi} + \sqrt[3]{a-bi}$ προκύπτει πραγματικός αριθμός.