Θεωρία Galois

Β. Μεταφτσής και Μ. Μπομπολάκης

Σημειώσεις Παραδόσεων
Μέρος Πρώτο
Έκδοση 1.414231

Περιεχόμενα

1 Δακτύλιοι και Σώματα

Στην ενότητα αυτή παρουσιάζεται μια ανακεφαλαίωση κάποιων γνωστών ορισμών και ιδιοτήτων των δακτυλίων και των σωμάτων. Για περισσότερες λεπτομέρειες και αποδείξεις ο αναγνώστης παραπέμπεται στο μάθημα της Άλγεβρας.

ΟΡΙΣΜΟΣ 1.1. Ένας δακτύλιος είναι ένα σύνολο R εφοδιασμένο με δύο πράξεις, πρόσθεση $+$ και πολλαπλασιασμό $\cdot$, έτσι ώστε το $(R,+)$ να είναι αβελιανή ομάδα, ο πολλαπλασιασμός να είναι προσεταιριστικός, $(ab)c = a(bc)$ και να ισχύει ο επιμερισμός

$$a(b+c) = ab + ac, \quad (b+c)a = ba + ca.$$

Αν $(R,+,\cdot)$ δακτύλιος και το $(R \setminus \{0\},\cdot)$ είναι μεταθετική ομάδα, τότε το $(R,+,\cdot)$ λέγεται σώμα.

Ένας δακτύλιος R στον οποίο ο πολλαπλασιασμός είναι μεταθετική πράξη, δηλαδή $ab = ba$ για κάθε $a, b \in R$ λέγεται μεταθετικός δακτύλιος.

Ένας δακτύλιος R ο οποίος περιέχει ουδέτερο στοιχείο ως προς τον πολλαπλασιασμό λέγεται δακτύλιος με μονάδα. Το ουδέτερο του πολλαπλασιασμού συμβολίζεται με 1.

Ένας δακτύλιος, μπορεί να περιέχει διαιρέτες του μηδενός, δηλαδή στοιχεία a, b με $a \neq 0 \neq b$ ώστε $ab = 0$. Αντίθετα μια χαρακτηριστική ιδιότητα του σώματος είναι ότι δεν περιέχει διαιρέτες του μηδενός, δηλαδή αν $ab = 0$ τότε $a = 0$ ή $b = 0$.

ΠΑΡΑΔΕΙΓΜΑ 1.1. Το απλούστερο παράδειγμα δακτυλίου είναι ο $(\mathbb{Z},+,\cdot)$. Είναι μεταθετικός δακτύλιος με μονάδα όχι όμως σώμα. Όμοια, οι δακτύλιοι $(\mathbb{Z}_n,+,\cdot)$ για κάθε $n \in \mathbb{N}$ είναι μεταθετικοί δακτύλιοι με μονάδα. Αν το n δεν είναι πρώτος αριθμός τότε σε αυτούς συναντάμε διαιρέτες του μηδενός. Παράδειγμα, στον $(\mathbb{Z}_6,+,\cdot)$ έχουμε $2 \cdot 3 \equiv 0 \pmod 6$. Αν το n είναι πρώτος τότε ο $(\mathbb{Z}_p,+,\cdot)$ είναι σώμα.

ΠΑΡΑΔΕΙΓΜΑ 1.2. Τα γνωστά σύνολα $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ με τις συνήθεις πράξεις της πρόσθεσης και του πολλαπλασιασμού είναι σώματα.

ΟΡΙΣΜΟΣ 1.2. Έστω R δακτύλιος. Ένα υποσύνολο του R λέγεται ιδεώδες του R αν $a-b \in I$, $ra \in I$ και $ar \in I$ για κάθε $a, b \in I$ και $r \in R$. Ένα ιδεώδες I του R λέγεται γνήσιο ιδεώδες αν $I \neq R$.

ΠΑΡΑΔΕΙΓΜΑ 1.3. Τα σύνολα $k\mathbb{Z}$ όπου $k > 1$ ακέραιος, είναι γνήσια ιδεώδη του δακτυλίου $\mathbb{Z}$. Το $k\mathbb{Z}$ περιέχει όλους τους ακεραίους που διαιρούνται με το k. Θα δούμε στην συνέχεια ότι αυτά είναι τα μοναδικά ιδεώδη του $\mathbb{Z}$.

Παρατηρήστε ότι ένα γνήσιο ιδεώδες ενός δακτυλίου με μονάδα R δεν μπορεί να περιέχει το 1. Διαφορετικά, $1r \in I$ για κάθε $r \in R$ και άρα $I = R$.

ΛΗΜΜΑ 1.1. Ένας μεταθετικός δακτύλιος R με μονάδα είναι σώμα αν και μόνο αν τα μοναδικά του ιδεώδη είναι το $\{0\}$ και το R.

Απόδειξη. Έστω R σώμα και I ένα μη-μηδενικό ιδεώδες του R. Τότε υπάρχει $x \in I$ με $x \neq 0$. Επειδή το R σώμα, το $x^{-1} \in R$ και άρα το $x^{-1}x = 1 \in I$. Άρα $r1 \in I$ για κάθε $r \in R$ και συνεπώς $I = R$. Άρα τα μόνα ιδεώδη του R είναι το $\{0\}$ και το R.

Αντίστροφα, έστω R δακτύλιος με μονάδα με την ιδιότητα τα μοναδικά ιδεώδη να είναι το $\{0\}$ και το R. Θεωρούμε x ένα μη-μηδενικό στοιχείο του R και συμβολίζω με $Rx = \{rx \mid r \in R\}$. Το Rx είναι ιδεώδες του R. Πράγματι, $r_1x - r_2x = (r_1 - r_2)x \in Rx$, $y(rx) = (yr)x \in Rx$ και $(rx)y = r(xy) = r(yx) = (ry)x \in Rx$ (λόγω μεταθετικότητα του δακτυλίου) για κάθε $r_1, r_2, y \in R$. Επιπλέον, $Rx \neq \{0\}$ εφόσον $x \in Rx$. Από υπόθεση συνεπάγεται ότι $Rx = R$ και άρα $1 \in Rx$. Άρα υπάρχει στοιχείο $x^{-1} \in R$ ώστε $x^{-1}x = 1$. Άρα κάθε $0 \neq x \in R$ έχει αντίστροφο στοιχείο, συνεπώς ο δακτύλιος R είναι σώμα. □

Εύκολα βλέπουμε ότι η τομή ιδεωδών ενός δακτυλίου R είναι ιδεώδες του R. Έστω X ένα υποσύνολο του δακτυλίου R. Το ιδεώδες του R που παράγεται από το X ορίζεται σαν την τομή όλων των ιδεωδών του R που περιέχουν το X. Παρατηρήστε ότι το ιδεώδες αυτό είναι καλά ορισμένο και είναι το μικρότερο ιδεώδες του R που περιέχει το X (διότι περιέχεται σε κάθε άλλο ιδεώδες που περιέχει το X).

Με $\langle f_1, \ldots, f_k \rangle$ συμβολίζουμε το ιδεώδες του R που παράγεται από το υποσύνολο $X = \{f_1, \ldots, f_k\}$ του R. Σε αυτή την περίπτωση λέμε ότι το ιδεώδες είναι πεπερασμένα παραγόμενο.

Λημμα 1.2. Έστω R ένας μεταθετικός δακτύλιος με μονάδα και X ένα υποσύνολο του R. Το ιδεώδες που παράγεται από το X ταυτίζεται με το σύνολο όλων των στοιχείων του R που μπορούν να εκφραστούν σαν πεπερασμένα αθροίσματα της μορφής $r_1x_1 + \ldots + r_kx_k$ όπου $x_1, \ldots, x_k \in X$ και $r_1, \ldots, r_k \in R$.

Απόδειξη. Έστω I το σύνολο όλων των πεπερασμένων αθροισμάτων της παραπάνω μορφής και J ένα ιδεώδες του R που περιέχει το X. Προφανώς το J περιέχει όλα τα παραπάνω αθροίσματα και άρα περιέχει και το I. Αν τώρα $a, b \in I$. Τότε $a - b \in I$ και $ra \in I$. Επίσης δεδομένου ότι ο δακτύλιος είναι μεταθετικός, $ar = ra \in I$. Συνεπώς το I είναι ιδεώδες του R, περιέχει το X και περιέχεται σε κάθε άλλο ιδεώδες του R που περιέχει το X. □

Κάθε ακέραιος n παράγει το ιδεώδες $n\mathbb{Z}$ του δακτυλίου $\mathbb{Z}$.

Λημμα 1.3. Κάθε ιδεώδες του $\mathbb{Z}$ παράγεται από κάποιο μη-αρνητικό ακέραιο n.

Απόδειξη. Προφανώς το μηδενικό ιδεώδες παράγεται από το 0. Έστω I ένα μη-μηδενικό ιδεώδες του $\mathbb{Z}$. Τότε το I περιέχει τουλάχιστον ένα θετικό ακέραιο ακέραιο, εφόσον για κάθε $m \in I$, το $-m \in I$. Έστω n ο μικρότερος θετικός ακέραιος του I. Αν $k \in I$ τότε $k = qn + r$ για κάποιους ακέραιους q, r με $0 \leq r < n$. Όμως το $r \in I$ εφόσον $r = k - qn$. Αλλά λόγω της επιλογής του n σαν τον μικρότερο θετικό ακέραιο του I έχουμε ότι $r = 0$. Άρα $k = qn$ συνεπως $I = n\mathbb{Z}$. □

Έστω $(K, +, \cdot)$ ένα σώμα. Θεωρούμε τα στοιχεία

$$a_n = \underbrace{1 + 1 + \ldots + 1}_{n-\text{παράγοντες}}.$$

Αν για κάθε n τα $a_n \neq 0$ τότε όλα τα a_n είναι διαφορετικά και τότε το σώμα K περιέχει ένα αντίγραφο του $\mathbb{Z}$ και άρα και του $\mathbb{Q}$. Ας υποθέσουμε τώρα ότι n είναι ο ελάχιστος θετικός ακέραιος τέτοιος ώστε $a_n = 0$. Τότε ο n είναι ένας πρώτος p (διαφορετικά έχουμε γινόμενο μη-μηδενικών αριθμών ίσο με μηδέν σε ένα σώμα) και το σώμα μας περιέχει ένα αντίγραφο του σώματος $\mathbb{Z}_p$.

ΛΗΜΜΑ 1.4. Έστω M σώμα και L,K υποσώματα του M. Τότε το $L \cap K$ είναι σώμα. Γενικότερα, η τομή υποσωμάτων είναι σώμα.

Απόδειξη. Η απόδειξη προκύπτει άμεσα απ' το γεγονός ότι η τομή ομάδων είναι ομάδα. □

Αν K σώμα και L ένα υποσύνολο του K το οποίο είναι επίσης σώμα με τις πράξεις του K τότε το L λέγεται *υπόσωμα* του K. Η τομή όλων των υποσωμάτων ενός σώματος K λέγεται *πρώτο υπόσωμα* του K.

ΠΡΟΤΑΣΗ 1.1. Το πρώτο υπόσωμα κάθε σώματος K είναι είτε το $\mathbb{Q}$ είτε το $\mathbb{Z}_p$ για κάποιο πρώτο p.

Απόδειξη. Άσκηση. □

ΟΡΙΣΜΟΣ 1.3. Λέμε ότι ένα σώμα K έχει χαρακτηριστική 0 αν το πρώτο υπόσωμά του είναι το $\mathbb{Q}$. Λέμε ότι έχει χαρακτηριστική p αν το πρώτο υπόσωμά του είναι το $\mathbb{Z}_p$.

2 Δακτύλιος πηλίκο και ομομορφισμοί

Έστω R δακτύλιος και I ένα ιδεώδες του R. Αν θεωρήσουμε το R σαν αβελιανή ομάδα τότε το I είναι κανονική υποομάδα και μπορούμε να ορίσουμε την ομάδα πηλίκο R/I με στοιχεία τα σύμπλοκα του I στην R, της μορφής $x + I$ για $x \in R$. Είναι γνωστό ότι το R/I είναι επίσης αβελιανή ομάδα. Επιπλέον, ορίζουμε στο R/I πολλαπλασιασμό ως εξής

$$(x + I)(y + I) = xy + I$$

για $x+I, y+I \in R/I$. Ο πολλαπλασιασμός είναι καλά ορισμένος. Πράγματι, αν $x+I = x'+I$ και $y + I = y' + I$ τότε $(x - x') \in I$ και $(y - y') \in I$. Συνεπώς $x(y - y') \in I$ και $(x - x')y' \in I$ εφόσον το I είναι ιδεώδες. Άρα

$$x(y - y') + (x - x')y' = xy - x'y' \in I$$

δηλαδή $xy + I = x'y' + I$. Συνεπώς το R/I έχει δομή δακτυλίου και ονομάζεται δακτύλιος πηλίκο.

ΟΡΙΣΜΟΣ 2.1. Μια συνάρτηση $f : R \to S$ μεταξύ δακτυλίων R και S λέγεται *ομομορφισμός* αν $f(x + y) = f(x) + f(y)$ και $f(xy) = f(x)f(y)$ για κάθε $x, y \in R$. Αν επιπλέον τα R, S δακτύλιοι με μοναδιαίο τότε $f(1) = 1$.

Αν $f : R \to S$ ομομορφισμός δακτυλίων τότε ο *πυρήνας* του ομομορφισμού είναι το σύνολο $\text{Ker}f = \{x \in R \mid f(x) = 0\}$. Επιπλέον, το $f(R)$ λέγεται *εικόνα* του ομομορφισμού και συμβολίζεται $\text{Im}f$. Ο πυρήνας ενός ομομορφισμού είναι ιδεώδες του πεδίου ορισμού της f και η εικόνα του ομομορφισμού είναι υποδακτύλιος του πεδίου τιμών της f, όχι όμως απαραίτητα ιδεώδες.

Αν I είναι ιδεώδες ενός δακτυλίου R τότε το I μπορεί να εκφραστεί και σαν πυρήνας του ομομορφισμού $f : R \to R/I$ με $f(x) = x + I$.

Ένας ομομορφισμός δακτυλίων που είναι 1-1 και επί λέγεται *ισομορφισμός* δακτυλίων και οι δύο δακτύλιοι λέγονται *ισόμορφοι*.

ΠΡΟΤΑΣΗ 2.1. Έστω $f : R \to S$ ομομορφισμός δακτυλίων και I ένα ιδεώδες του R με $I \subset \text{Ker}f$. Τότε υπάρχει μοναδικός ομομορφισμός $\overline{f} : R/I \to S$ τέτοιος ώστε $\overline{f}(x + I) = f(x)$ για κάθε $x \in R$. Επιπλέον, ο $\overline{f} : R/I \to S$ είναι 1-1 αν και μόνο αν $I = \text{Ker}f$.

Απόδειξη. Ο $\overline{f}$ είναι καλά ορισμένος. Πράγματι, αν $x + I = x' + I$ τότε $x - x' \in I$ και άρα $\overline{f}((x-x')+I) = \overline{f}(I) = \overline{f}(0+I) = f(0) = 0$. Αλλά $\overline{f}((x-x')+I) = f(x-x') = f(x)-f(x')$ και άρα $f(x) - f(x') = 0$ δηλαδή $f(x) = f(x')$. Συνεπώς $\overline{f}(x + I) = \overline{f}(x' + I)$.

Επιπλέον, ο $\overline{f}$ είναι ομομορφισμός δακτυλίων. Πράγματι,

$$\overline{f}((x + I) + (y + I)) = \overline{f}((x + y) + I) = f(x + y) = f(x) + f(y) = \overline{f}(x + I) + \overline{f}(y + I)$$

και

$$\overline{f}((x + I)(y + I)) = \overline{f}(xy + I) = f(xy) = f(x)f(y) = \overline{f}(x + I)\overline{f}(y + I).$$

Τέλος, αν $\overline{f}$ είναι 1-1 και $x \in \text{Ker}f$ τότε $f(x) = 0$ άρα $\overline{f}(x + I) = f(x) = 0$ συνεπώς $x+I = I$ δηλαδή $x \in I$. Αντίστροφα, αν $I = \text{Ker}f$ έστω $x_1+I, x_2+I \in R/I$ με $\overline{f}(x_1+I) = \overline{f}(x_2 + I)$. Τότε $f(x_1) = f(x_2)$ άρα $f(x_1 - x_2) = 0$ δηλαδή $x_1 - x_2 \in \text{Ker}f = I$ και άρα $x_1 + I = x_2 + I$. □

ΠΟΡΙΣΜΑ 2.1 (Πρώτο Θεώρημα Ισομορφισμών). Αν $f : R \to S$ ομομορφισμός δακτυλίων τότε η f επάγει ισομορφισμό δακτυλίων $R/\text{Ker}f \cong \text{Im}f$.

3 Δακτύλιοι πολυωνύμων

Έστω R ένας δακτύλιος. Θεωρούμε το σύνολο όλων των πολυωνύμων στο R, δηλαδή όλες τις εκφράσεις

$$a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$$

με άγνωστο x και με συντελεστές $a_i \in R$. Αν $a_n \neq 0$ τότε λέμε ότι το παραπάνω πολυώνυμο έχει βαθμό n και συμβολίζουμε $\deg(a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0) = n$.

Κατά τα γνωστά, ορίζουμε πράξεις πρόσθεσης και πολλαπλασιασμού στα πολυώνυμα αυτά. Εύκολα βλέπουμε ότι το σύνολο αυτό με τις παραπάνω πράξεις είναι δακτύλιος και ονομάζεται *δακτύλιος πολυωνύμων* με συντελεστές στο R. Συμβολίζεται με $R[x]$.

ΠΑΡΑΤΗΡΗΣΗ 3.1. Ένα πολυώνυμο στο $R[x]$ μπορεί να θεωρηθεί και σαν συνάρτηση από το R στο R όπως επίσης και σαν μια έκφραση που ορίζεται από τους συντελεστές $(a_n, a_{n-1}, \ldots, a_1, a_0)$. Αυτές οι δύο προσεγγίσεις είναι ουσιαστικά διαφορετικές. Για παράδειγμα, αν το R είναι ένα πεπερασμένο σώμα τότε μπορούμε να κατασκευάσουμε πολυώνυμα τα οποία να ταυτίζονται σαν συναρτήσεις από το R στο R αλλά να είναι διαφορετικά σαν πολυώνυμα μια και ορίζονται από διαφορετικούς συντελεστές. Για παράδειγμα, αν $R = \mathbb{Z}_3$ τα πολυώνυμα $f = x^{2003}$ και $g = x^{2003} + x^3 - x$ ταυτίζονται για κάθε τιμή του $\mathbb{Z}_3 = \{0, 1, 2\}$ αλλά είναι φυσικά διαφορετικά πολυώνυμα. Η παραπάνω κατάσταση αλλάζει στα άπειρα σώματα.

Θα ασχοληθούμε τώρα με πολυώνυμα επί ενός σώματος.

ΟΡΙΣΜΟΣ 3.1. Έστω K ένα σώμα. Ένα πολυώνυμο

$$f(x) = \alpha_0 + \alpha_1 x + \cdots + \alpha_n x^n$$

επί του K θα λέγεται μονικό αν $\alpha_n = 1$.

ΠΑΡΑΤΗΡΗΣΗ 3.2. Φανερά, κάθε πολυώνυμο με συντελεστές στο σώμα K είναι ένα μονικό πολυώνυμο πολλαπλασιασμένο με μια κατάλληλη σταθερά. Το γινόμενο δύο μονικών πολυωνύμων είναι μονικό.

ΛΗΜΜΑ 3.1. Έστω K σώμα και $f \in K[x]$ ένα μη μηδενικό πολυώνυμο με συντελεστές στο K. Αν $h \in K[x]$ ένα άλλο πολυώνυμο τότε υπάρχουν μοναδικά $q, r \in K[x]$ έτσι ώστε $h = fq + r$ και είτε $r = 0$ είτε $\deg r < \deg f$.

Απόδειξη. Αν $\deg h < deg f$ τότε μπορούμε να πάρουμε $q = 0, r = h$. Στην γενική περίπτωση θα αποδείξουμε την ύπαρξη των q, r με επαγωγή στον βαθμό του h. Ας υποθέσουμε ότι $\deg h \geq \deg f$ και ότι κάθε πολυώνυμο με βαθμό μικρότερο από $\deg h$ μπορεί να εκφραστεί στην ζητούμενη μορφή.

Τώρα υπάρχει ένα $c \in K$ τέτοιο ώστε τα πολυώνυμα $h(x)$ και $cf(x)$ να έχουν τον ίδιο συντελεστή μεγιστοβαθμίου όρου. Έστω $h_1(x) = h(x) - cx^m f(x)$, όπου $m = \deg h - \deg f$. Τότε, είτε $h_1 = 0$ είτε $\deg h_1 < \deg h$. Από επαγωγική υπόθεση ξέρουμε ότι υπάρχουν πολυώνυμα $q_1, r \in K[x]$ ώστε $h_1 = fq_1 + r$ όπου είτε $r = 0$ είτε $\deg r < \deg f$. Όμως $h = fq + r$ όπου $q(x) = cx^m + q_1(x)$.

Για να δείξουμε την μοναδικότητα των q, r, υποθέτουμε ότι $fq + r = fq' + r'$, με $q', r' \in K[x]$ και είτε $r' = 0$ είτε $\deg r' < \deg f$. Τότε $(q - q')f = r - r'$. Αλλά $\deg((q - q')f) \geq \deg f$ αν $q \neq q'$ και $\deg(r - r') < \deg f$ αν $r' \neq r$. Άρα η ισότητα $(q - q')f = r - r'$ δεν μπορεί να ισχύει εκτός και αν $q = q'$ και $r = r'$. □

Κάθε πολυώνυμο $f \in K[x]$ παράγει ένα ιδεώδες $\langle f \rangle$ του $K[x]$ που αποτελείται από όλα τα πολυώνυμα στο $K[x]$ τα οποία διαιρούνται από το f.

ΛΗΜΜΑ 3.2. Έστω K σώμα και I ιδεώδες του $K[x]$. Τότε υπάρχει $f \in K[x]$ τέτοιο ώστε $I = \langle f \rangle$ όπου $\langle f \rangle$ το ιδιώδες που παράγεται από το f.

Απόδειξη. Αν το $I = \{0\}$ τότε μπορούμε να πάρουμε $f = 0$. Διαφορετικά επιλέγω $f \in I$ ώστε $f \neq 0$ και ο βαθμός του f να είναι ο μικρότερος δυνατός στο I. Κάθε πολυώνυμο $h \in I$ μπορεί να γραφεί στην μορφή $h = qf + r$ όπου είτε $r = 0$ είτε $\deg r < \deg f$. Αλλά το $r = h - fq \in I$ και άρα από την επιλογή του f, το $r = 0$. Άρα $h = qf$ και άρα $I = \langle f \rangle$. □

ΟΡΙΣΜΟΣ 3.2. Έστω K σώμα και $f_1, \ldots, f_k \in K[x]$. Τα $f_1, \ldots, f_k$ λέγονται πρώτα μεταξύ τους αν δεν υπάρχει μη-σταθερό πολυώνυμο που να διαιρεί όλα τα f_i.

ΘΕΩΡΗΜΑ 3.1. Έστω $f_1, \ldots, f_k \in K[x]$ πρώτα μεταξύ τους. Τότε υπάρχουν πολυώνυμα $g_1, \ldots, g_k \in K[x]$ τέτοια ώστε

$$f_1 g_1 + \ldots + f_k g_k = 1.$$

Απόδειξη. Έστω I το ιδεώδες που παράγεται από τα $f_1, \ldots, f_k$. Από προηγούμενο λήμμα το $I = \langle d \rangle$ για κάποιο $d \in K[x]$. Άρα κάθε f_i είναι πολλαπλάσιο του d. Όμως τα $f_i, i = 1, \ldots, k$ είναι πρώτα μεταξύ τους, άρα το d είναι σταθερό πολυώνυμο. Συνεπώς $I = K[x]$. Άρα από Λήμμα 1.2 έχουμε ότι υπάρχουν $g_1, \ldots, g_k \in K[x]$ ώστε $f_1 g_1 + \ldots + f_k g_k = 1$. □

ΟΡΙΣΜΟΣ 3.3. Έστω K σώμα. Ένα πολυώνυμο $f \in K[x]$ με $\deg(f) \geq 1$ θα λέγεται ανάγωγο επί του K αν δεν υπάρχουν πολυώνυμα $q, h \in K[x]$ ώστε

$$f(x) = q(x)h(x) \quad \text{με} \quad 0 < \deg(q), \deg(h) < \deg(f).$$

ΠΑΡΑΤΗΡΗΣΗ 3.3. Είναι προφανές ότι αν $f \in K[x]$ με $\deg f = 1$ τότε το f είναι ανάγωγο. Επιπλέον, αν $\deg f = 2$ ή 3 τότε το f είναι ανάγωγο αν και μόνο αν δεν έχει ρίζες στο K. Τα παραπάνω προκύπτουν άμεσα από το γεγονός ότι σε ένα σώμα ισχύει $\deg gh = \deg g + \deg h$ για $g, h \in K[x]$.

Με άλλα λόγια ένα πολυώνυμο είναι ανάγωγο αν δεν διαιρείται από κανένα άλλο πολυώνυμο με βαθμό μεγαλύτερο του μηδενός.

ΠΡΟΤΑΣΗ 3.1. Έστω $f, g, h \in K[x]$ όπου K σώμα. Αν το f είναι ανάγωγο επί του K και το f διαιρεί το γινόμενο gh τότε το f διαιρεί είτε το g είτε το h.

Απόδειξη. Ας υποθέσουμε ότι το f δεν διαιρεί το g. Τότε και κανένα πολλαπλάσιο του f δεν διαιρεί το g. Άρα τα f, g είναι πρώτα μεταξύ τους. Άρα υπάρχουν πολυώνυμα $x, y \in K[x]$ τέτοια ώστε $xf + yg = 1$. Άρα $h = xfh + ygh$. Αλλά το f διαιρεί το gh και άρα διαιρεί τα xfh και ygh άρα διαιρεί και το άθροισμά τους δηλαδή το h. □

ΠΡΟΤΑΣΗ 3.2. Έστω f ένα ανάγωγο πολυώνυμο του $K[x]$ και $I = \langle f \rangle$ το ιδεώδες που παράγεται από το f. Τότε το $K[x]/I$ είναι σώμα.

Απόδειξη. Ξέρουμε ότι το $K[x]/I$ είναι μεταθετικός δακτύλιος με ουδέτερο στοιχείο του πολλαπλασιασμού (μονάδα) το $1 + I$. Έστω $g \in K[x]$ με $g + I \neq I$. Τα g, f είναι πρώτα μεταξύ τους άρα υπάρχουν πολυώνυμα $x, y \in K[x]$ ώστε $1 = xg + yf$. Επομένως, στο $K[x]/I$ έχουμε $1 + I = xg + yf + I$. Όμως το $yf \in I$ και άρα $1 + I = xg + I = (x + I)(g + I)$. Άρα το $x + I$ είναι το πολλαπλασιαστικό αντίστροφο του $g + I$ στο $K[x]/I$, που σημαίνει ότι το $K[x]/I$ είναι σώμα. □

ΟΡΙΣΜΟΣ 3.4. Ένα πολυώνυμο με ακέραιους συντελεστές λέγεται πρωτόγονο αν δεν υπάρχει πρώτος αριθμός που να διαιρεί τους συντελεστές του.

ΛΗΜΜΑ 3.3 (Λήμμα του Gauss). Έστω g, h πολυώνυμα στο $\mathbb{Z}[x]$. Αν τα g, h είναι πρωτόγονα τότε και το gh είναι πρωτόγονο.

Απόδειξη. Έστω $g = b_0 + b_1x + \ldots + b_rx^r$, $h(x) = c_0 + c_1x + \ldots + c_sx^s$ και $gh = a_0 + a_1x + \ldots + a_{r+s}x^{r+s}$. Έστω p πρώτος. Τα πολυώνυμα g και h έχουν τουλάχιστον ένα συντελεστή που δεν διαιρείται με το p. Έστω j, k οι μικρότεροι δείκτες για τους οποίους $p \not| b_j$ και $p \not| c_k$. Τότε ο

$$a_{j+k} - b_jc_k = \sum_{i=0}^{j-1} b_ic_{j+k-i} + \sum_{i=0}^{k-1} b_{j+k-i}c_i$$

διαιρείται από τον p εφόσον αυτός διαιρεί όλα τα b_i με $i < j$ και όλα τα c_i με $i < k$. Όμως το p δεν διαιρεί το b_jc_k και άρα το p δεν διαιρεί τον συντελεστή a_{j+k} του gh. Άρα το gh είναι πρωτόγονο. □

ΠΡΟΤΑΣΗ 3.3. Ένα πολυώνυμο με ακέραιους συντελεστές είναι ανάγωγο στο $\mathbb{Q}$ αν και μόνο αν δεν μπορεί να παραγοντοποιηθεί σαν γινόμενο πολυωνύμων μικρότερου βαθμού με ακέραιους συντελεστές.

Απόδειξη. Έστω f πολυώνυμο με ακέραιους συντελεστές. Αν το f είναι ανάγωγο στο $\mathbb{Q}$ τότε δεν μπορεί να παραγοντοποιηθεί σε γινόμενο πολυωνύμων.

Αντίστροφα, αν το f δεν μπορεί να παραγοντοποιηθεί σε γινόμενο πολυωνύμων με ακέραιους συντελεστές αλλά μπορεί να παραγοντοποιηθεί στην μορφή $f = gh$ όπου $g, h \in \mathbb{Q}[x]$. Τότε υπάρχουν $r, s \in \mathbb{Z}$ τέτοιοι ώστε τα rg και sh να έχουν ακέραιους συντελεστές. Έστω u, v οι μέγιστοι κοινοί διαιρέτες των συντελεστών των rg και sh αντίστοιχα. Τότε $rg = ug_*$ και $sh = vh_*$ όπου g_*, h_* πρωτόγονα πολυώνυμα με ακέραιους συντελεστές. Τότε $(rs)f = (uv)g_*h_*$.

Έστω ℓ ο μικρότερος διαιρέτης του rs ώστε το $\ell f = mg_*h_*$ για κάποιο ακέραιο m. Υποθέτουμε ότι το $\ell > 1$. Τότε υπάρχει πρώτος p που διαιρεί το ℓ. Όμως το p δεν μπορεί να διαιρεί το m. Διαφορετικά, $(\ell/p)f = (m/p)g_*h_*$ το οποίο έρχεται σε αντίθεση με τον ορισμό του ℓ. Άρα το p πρέπει να διαιρεί κάθε έναν από τους συντελεστές του g_*h_* πράγμα άτοπο από το λήμμα του Gauss 3.3 εφόσον τα g_*, h_* πρωτόγονα. Άρα $\ell = 1$ και $f = mg_*h_*$. Όμως το f δεν παραγοντοποιείται σαν γινόμενο πολυωνύμων με ακέραιους συντελεστές. Άρα είτε $\deg f = \deg g_* = \deg g$ είτε $\deg f = \deg h_* = \deg h$. Συνεπώς το f είναι ανάγωγο στο $\mathbb{Q}$. □

ΠΡΟΤΑΣΗ 3.4 (Κριτήριο διαιρετότητας του Eisenstein). Έστω $f(x) = a_nx^n + \ldots + a_1x + a_0$ πολυώνυμο με ακέραιους συντελεστές και p πρώτος τέτοιος ώστε

1. το p διαιρεί τα $a_0, \ldots, a_{n-1}$,
2. το p δεν διαιρεί το a_n,
3. το p^2 δεν διαιρεί το a_0.

Τότε το πολυώνυμο f είναι ανάγωγο στο $\mathbb{Q}$.

Απόδειξη. Υποθέτουμε ότι $f(x) = g(x)h(x)$ όπου $g = b_r x^r + \ldots + b_1 x + b_0$, $h(x) = c_s x^s + \ldots + c_1 x + c_0$ πολυώνυμα με ακέραιους συντελεστές. Τότε $a_0 = b_0 c_0$. Όμως το a_0 διαιρείται με το p αλλά όχι με το p^2. Επομένως μόνο ένα από τα b_0, c_0 διαιρείται με το p, ας υποθέσουμε το b_0 (η άλλη περίπτωση είναι ανάλογη). Το p δεν μπορεί να διαιρεί όλους τους συντελεστές του g εφόσον δεν διαιρεί όλους τους συντελεστές του f. Ας υποθέσουμε j τον μικρότερο δείκτη για τον οποίο το p δεν διαιρεί το b_i. Τότε το p διαιρεί το $a_j - b_j c_0 = \sum_{i=0}^{j-1} b_i c_{j-i}$. Αλλά το $b_j c_0$ δεν διαιρείται από το p αφού το p δεν διαιρεί ούτε το b_j ούτε το c_0. Άρα το a_j δεν διαιρείται από το p και συνεπώς από την υπόθεση έχουμε $j = n$ και $\deg g \geq n = \deg f$. Άρα $\deg g = \deg f$ και $\deg h = 0$. Άρα το πολυώνυμο f δεν παραγοντοποιείται σαν γινόμενο πολυωνύμων μικρότερου βαθμού με ακέραιους συντελεστές και άρα είναι ανάγωγο στο $\mathbb{Q}$ από την προηγούμενη πρόταση. □

ΟΡΙΣΜΟΣ 3.5. Έστω $f(x) = a_0 + a_1 x + \ldots + a_n x^n \in \mathbb{Z}[x]$ με $n \in \mathbb{N}$. Ορίζουμε $\overline{f} \in \mathbb{Z}_k[x]$ με

$$\overline{f} = \overline{a_0} + \overline{a_1} x + \ldots + \overline{a_n} x^n$$

όπου $\overline{a_i} = a_i \pmod{k}$ for $i = 0, \ldots, n$. Η απεικόνιση $\mathbb{Z}[x] \to \mathbb{Z}_k[x]$ με $f \mapsto \overline{f}$ λέγεται ομομορφισμός αναγωγής.

Η παραπάνω απεικόνιση είναι ομομορφισμός, πράγμα που προκύπτει άμεσα από το γεγονός ότι η απεικόνιση $\mathbb{Z} \to \mathbb{Z}_n$ με $a \mapsto a \pmod{k}$ είναι ομομορφισμός.

ΘΕΩΡΗΜΑ 3.2. Έστω $f(x) = a_0 + a_1 x + \ldots + a_n x^n \in \mathbb{Z}[x]$ με $n > 1$. Αν p θετικός πρώτος τέτοιος ώστε

1. το p δεν διαιρεί το a_n,
2. το $\overline{f}$ είναι ανάγωγο στο $\mathbb{Z}_p[x]$

τότε το f είναι ανάγωγο στο $\mathbb{Q}[x]$.

Απόδειξη. Ας υποθέσουμε ότι το f είναι παραγοντοποιήσιμο και άρα γράφεται σαν $f = gh$ με $\deg g, \deg h > 0$. Εφόσον το $0 \not\equiv a_n \pmod{p}$, έχουμε ότι $\deg \overline{f} = \deg f$. Επιπλέον, $\overline{f} = \overline{g}\overline{h}$ είναι μια παραγοντοποίηση του $\overline{f}$ σε πολυώνυμα μικρότερου βαθμού, εφόσον $\deg \overline{g} \leq \deg g$ και $\deg \overline{h} \leq \deg h$. Άρα το $\overline{f} \in \mathbb{Z}_p[x]$ είναι παραγοντοποιήσιμο, άτοπο. □

ΠΑΡΑΤΗΡΗΣΗ 3.4. Είναι γνωστό από το γυμνάσιο ότι αν $f(x) = a_0 + a_1 x + \ldots + a_n x^n \in \mathbb{Z}[x]$ με $a_0, a_n \neq 0$ και έχει ρίζες στο $\mathbb{Q}$ τότε αυτές ανήκουν στο σύνολο

$$\{\frac{r}{s} \mid r, s \in \mathbb{Z} \setminus \{0\} \text{ με } r|a_0, s|a_n\}.$$

Πράγματι, αν $\frac{r}{s} \in \mathbb{Q}$ με $r, s \in \mathbb{Z}$ είναι μια ρίζα του f με $(r, s) = 1$ τότε $f(\frac{r}{s}) = 0$ και πολλαπλασιάζοντας και τις δύο πλευρές της παραπάνω με s^n παίρνουμε

$$a_0 s^n + a_1 r s^{n-1} + \ldots + a_{n-1} r^{n-1} s + a_n r^n = 0.$$

Άρα $a_0 s^n = -r(a_1 s^{n-1} + \ldots + a_n r^{n-1})$. Εφόσον, $a_0, s \neq 0$ έχουμε ότι $r \neq 0$ και άρα $r|(a_0 s^n)$. Επειδή $(r, s) = 1$ συνεπάγεται ότι $r|a_0$. Όμοια, $a_n r^n = -s(a_0 s^{n-1} + \ldots + a_{n-1} r^{n-1})$ άρα $s|(a_n r^n)$ και άρα $s|a_n$.

4 Επεκτάσεις Σωμάτων

ΟΡΙΣΜΟΣ 4.1. Έστω L ένας διανυσματικός χώρος πάνω σε ένα σώμα K και M να είναι ένα μη κενό υποσύνολο του L. Λέμε ότι το $v \in L$ είναι γραμμικός συνδυασμός των στοιχείων $v_1, v_2, \ldots, v_n \in M$ αν υπάρχουν $\lambda_1, \lambda_2, \ldots, \lambda_n \in K$ ώστε

$$v = \lambda_1 v_1 + \lambda_2 v_2 + \cdots + \lambda_n v_n.$$

Θα συμβολίζουμε με $spanM$ το σύνολο όλων των γραμμικών συνδυασμών των στοιχείων του M.

ΟΡΙΣΜΟΣ 4.2. Έστω K και L σώματα. Επέκταση σώματος ονομάζουμε έναν μονομορφισμό $\sigma : K \longrightarrow L$. Μπορούμε να ταυτίσουμε το σώμα K με την εικόνα του $\sigma(K)$, έτσι ο σ μπορεί να θεωρηθεί ως η ταυτοτική απεικόνιση και το K μπορεί να θεωρηθεί ως ένα υπόσωμα του L. Υπό αυτή την έννοια συμβολίζουμε

$$L : K$$

την επέκταση και λέμε ότι το L είναι επέκταση του K.

ΠΑΡΑΔΕΙΓΜΑ 4.1.

1. Οι απεικονίσεις $\sigma_1 : \mathbb{Q} \longrightarrow \mathbb{R}$, $\sigma_2 : \mathbb{R} \longrightarrow \mathbb{C}$ και $\sigma_3 : \mathbb{Q} \longrightarrow \mathbb{C}$ με $\sigma_1, \sigma_2, \sigma_3$ να είναι οι ταυτοτικές απεικονίσεις πάνω στα $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ αντίστοιχα, είναι επεκτάσεις σωμάτων. Έτσι μπορούμε να τις συμβολίσουμε με $\mathbb{R} : \mathbb{Q}$, $\mathbb{C} : \mathbb{R}$, $\mathbb{C} : \mathbb{Q}$ αντίστοιχα.

2. Αν $F_9 = \mathbb{Z}_3[x]/\langle x^2+1\rangle = \left\{\alpha_1 x + \alpha_0 + \langle x^2+1\rangle \mid \alpha_1, \alpha_2 \in \mathbb{Z}_3\right\}$ τότε η απεικόνιση $\sigma : \mathbb{Z}_3 \longrightarrow F_9$ με
$$\sigma(\alpha) = \alpha + \langle x^2+1\rangle$$
είναι μια επέκταση σώματος.

ΟΡΙΣΜΟΣ 4.3. Έστω K, L και M σώματα με $K \subseteq L \subseteq M$. Ένας $K-$ομομορφισμός $\sigma : L \longrightarrow M$, είναι ένας ομομορφισμός για τον οποίο ισχύει

$$\sigma(\alpha) = \alpha \quad \forall \alpha \in K.$$

- Αν ο σ είναι $1-1$ τότε λέγεται $K-$μονομορφισμός.
- Αν ο σ είναι επί τότε λέγεται $K-$επιμορφισμός.
- Αν ο σ είναι $1-1$ και επί τότε λέγεται $K-$ισομορφισμός.
- Αν ο σ είναι $1-1$, επί και $L = M$ τότε λέγεται $K-$αυτομορφισμός.

ΠΑΡΑΔΕΙΓΜΑ 4.2. Ο $\sigma : \mathbb{R} \longrightarrow \mathbb{C}$ με $\sigma(1) = i$ δεν είναι $\mathbb{Q}-$μονομορφισμός, διότι

$$i = \sigma(1) = \sigma(1^2)$$

όμως

$$\sigma^2(1) = \sigma(1)\sigma(1) = ii = -1 \neq i = \sigma(1^2).$$

Συνεπώς ο σ δεν είναι καν ομομορφισμός.

ΠΑΡΑΤΗΡΗΣΗ 4.1. Έστω $L : K$ μια επέκταση σώματος. Τότε το L μπορεί να θεωρηθεί ως διανυσματικός χώρος επί του K. Προφανώς το $(L, +)$ είναι αβελιανή ομάδα. Επίσης, ο εξωτερικός πολλαπλασιασμός $\cdot : K \times L \to L$ είναι ο πολλαπλασιασμός των στοιχείων του K με αυτά του L. Το αποτέλεσμα ανήκει στο L εφόσον το $(L \setminus \{0\}, \cdot)$ είναι επίσης ομάδα και $0 \cdot x = 0$ για κάθε $x \in L$.

ΟΡΙΣΜΟΣ 4.4 (Βαθμός Επέκτασης). Έστω $L : K$ μια επέκταση. Αν η διάσταση του L ως διανυσματικού χώρου επί του K είναι πεπερασμένη, τότε λέμε ότι η επέκταση $L : K$ είναι πεπερασμένη. Ο βαθμός της επέκτασης $L : K$ συμβολίζεται με $[L : K]$ και είναι η διάσταση του διανυσματικού χώρου L επί του K.

ΠΑΡΑΔΕΙΓΜΑ 4.3.

1. Έστω η επέκταση $\mathbb{C} : \mathbb{R}$. Μια βάση του $\mathbb{C}$, ως διανυσματικού χώρου επί του $\mathbb{R}$ είναι η $\{1, i\}$. Κάθε στοιχείο του $\mathbb{C}$ γράφεται σαν γραμμικός συνδυασμός της μορφής $\alpha \cdot 1 + \beta \cdot i$, όπου τα $\alpha, \beta \in \mathbb{R}$. Άρα $[\mathbb{C} : \mathbb{R}] = 2$.

2. Έστω η επέκταση $\mathbb{R} : \mathbb{Q}$. Θα δείξουμε ότι ο βαθμός της επέκτασης δεν είναι πεπερασμένος. Έστω $v_1, \ldots, v_n$ μια βάση του $\mathbb{R}$ επί του $\mathbb{Q}$. Τότε κάθε στοιχείο του $\mathbb{R}$ μπορεί να γραφεί μοναδικά σαν γραμμικός συνδυασμός της μορφής $q_1v_1+q_2v_2+\ldots+q_nv_n$ για κάποια $q_1, \ldots, q_n \in \mathbb{Q}$. Άρα η πληθικότητα του συνόλου όλων των δυνατών τέτοιων συνδυασμών είναι $|\mathbb{Q}|^n$. Εφόσον το $\mathbb{Q}$ είναι αριθμήσιμο και το $\mathbb{Q}^n$ είναι αριθμήσιμο. Όμως το $\mathbb{R}$ είναι υπεραριθμήσιμο, άρα δεν μπορεί να έχει πεπερασμένη διάσταση επί του $\mathbb{Q}$.

ΠΡΟΤΑΣΗ 4.1 (Short Tower Law). Έστω $M : L$ και $L : K$ επεκτάσεις σωμάτων. Τότε η επέκταση $M : K$ είναι πεπερασμένη αν και μόνο αν οι επεκτάσεις $M : L$ και $L : K$ είναι πεπερασμένες και στην περίπτωση αυτή

$$[M : K] = [M : L][L : K]$$

Απόδειξη. ($\Longrightarrow$) Υποθέτω ότι η $M : K$ είναι μια πεπερασμένη επέκταση. Τότε το L ως διανυσματικός χώρος επί του K, είναι υπόχωρος του M και εφόσον ο M έχει πεπερασμένη διάσταση επί του K, θα έχουμε ότι και η επέκταση $L : K$ θα είναι πεπερασμένη.
Τώρα επειδή η επέκταση $M : K$ είναι πεπερασμένη, θα υπάρχει πεπερασμένη βάση του M η οποία παράγει το M σαν διανυσματικό χώρο επί του K. Άρα το A θα παράγει το M και σαν διανυσματικό χώρο επί του L, αφού $K \subseteq L$. Άρα και η επέκταση $M : L$ είναι πεπερασμένη.
($\Longleftarrow$) Υποθέτω ότι οι επεκτάσεις $M : L$ και $L : K$ είναι πεπερασμένες. Έστω $\{x_i \mid i = 1, \ldots, m\}$ μια βάση του L επί του K και $\{y_j \mid j = 1, \ldots, n\}$ μια βάση του M επί του L. Θα δείξουμε ότι το $B = \{x_iy_j \mid i = 1, \ldots, m,\ j = 1, \ldots, n\}$ είναι βάση του M επί K.

Αρχικά θα δείξουμε ότι τα στοιχεία του B είναι γραμμικώς ανεξάρτητα. Πράγματι, έστω

$$\sum_{i,j} k_{ij}x_iy_j = 0 \qquad \text{με} \quad k_{ij} \in K.$$

Αναδιατάσσοντας το άθροισμα θα έχουμε

$$\sum_{j=1}^{n} \Big(\sum_{i=1}^{m} k_{ij}x_i \Big) y_j = 0$$

Καθώς για κάθε $j = 1, \ldots, n$, το $\sum_{i=1}^{m} k_{ij}x_i \in L$ και τα y_j είναι γραμμικώς ανεξάρτητα μεταξύ τους, θα έχουμε ότι

$$\sum_{i=1}^{m} k_{ij}x_i = 0 \qquad \forall j.$$

Όμως τα x_i είναι μεταξύ τους γραμμικώς ανεξάρτητα, άρα θα έχουμε $k_{ij} = 0$ για κάθε i, j, συνεπώς τα στοιχεία του B είναι μεταξύ τους γραμμικώς ανεξάρτητα.

Μένει να δείξουμε ότι ο υπόχωρος που παράγεται από το σύνολο B είναι όλος ο χώρος M. Έστω $x \in M$. Τα $\{y_j\}_{j=1}^{n}$ είναι βάση του M επί του L, άρα θα υπάρχουν $l_1, l_2, \ldots, l_n \in L$ ώστε

$$x = \sum_{j=1}^{n} l_j y_j.$$

Τώρα επειδή τα $\{x_i | i = 1 \ldots m\}$ είναι βάση του L επί του K, θα υπάρχουν $k_{1j}, k_{2j}, \ldots, k_{mj} \in K$ ώστε

$$l_j = \sum_{i=1}^{m} k_{ij}x_i.$$

Συνεπώς

$$x = \sum_{j=1}^{n}\sum_{i=1}^{m} k_{ij}x_i y_j = \sum_{i,j} k_{ij}x_i y_j.$$

Άρα τα στοιχεία του B παράγουν τον M και είναι γραμμικώς ανεξάρτητα. Συνεπώς αποτελούν βάση του M και η διάσταση του M ως διανυσματικός χώρος επί του K, είναι nm.

Τώρα η σχέση $[M : K] = [M : L][L : K]$ προκύπτει άμεσα. □

ΠΟΡΙΣΜΑ 4.1 (Tower Law). Έστω $K_n : K_{n-1},\ K_{n-1} : K_{n-2}, \ldots, K_2 : K_1,\ K_n : K_1$ επεκτάσεις σωμάτων. Τότε η επέκταση $K_n : K_1$ είναι πεπερασμένη αν και μόνο αν οι επεκτάσεις $K_n : K_{n-1},\ K_{n-1} : K_{n-2}, \ldots, K_2 : K_1$ είναι πεπερασμένες. Στην περίπτωση αυτή

$$[K_n : K_1] = [K_n : K_{n-1}][K_{n-1} : K_{n-2}] \cdots [K_2 : K_1].$$

Απόδειξη. ($\Longrightarrow$) Υποθέτουμε ότι η επέκταση $K_n : K_1$ είναι πεπερασμένη και θα δείξουμε ότι οι επεκτάσεις $K_n : K_{n-1},\ K_{n-1} : K_{n-2}, \ldots, K_2 : K_1$ είναι πεπερασμένες. Η απόδειξη θα γίνει με επαγωγή στο n. Για $n = 3$ το ζητούμενο ισχύει από την Πρόταση 4.1. Υποθέτουμε τώρα ότι αν η επέκταση $K_{n-1} : K_1$ είναι πεπερασμένη τότε και οι επεκτάσεις $K_{n-1} : K_{n-2},\ K_{n-2} : K_{n-3}, \ldots, K_2 : K_1$ είναι πεπερασμένες και θα δείξουμε ότι αν η επέκταση $K_n : K_1$ είναι πεπερασμένη τότε και οι επεκτάσεις $K_n : K_{n-1},\ K_{n-1} : K_{n-2}, \ldots, K_2 : K_1$ είναι πεπερασμένες.

Αν λοιπόν η επέκταση $K_n : K_1$ είναι πεπερασμένη τότε και η επέκταση $K_{n-1} : K_1$ είναι πεπερασμένη, διότι ο K_{n-1} ως διανυσματικός χώρος επί του K_1 είναι υπόχωρος του διανυσματικού χώρου K_n επί του K_1. Συνεπώς από την επαγωγική υπόθεση θα έχουμε ότι οι επεκτάσεις $K_{n-1} : K_{n-2},\ K_{n-2} : K_{n-3}, \ldots, K_2 : K_1$ είναι πεπερασμένες. Έστω τώρα A να είναι μια (πεπερασμένη) βάση του διανυσματικού χώρου K_n επί του K_1, τότε το σύνολο A

θα είναι βάση και του διανυσματικού χώρου K_n επί του K_{n-1}, διότι $K_1 \subseteq K_n$.
($\Longleftarrow$) Υποθέτουμε ότι οι επεκτάσεις $K_n : K_{n-1},\ K_{n-1} : K_{n-2}, \ldots, K_2 : K_1$ είναι πεπερασμένες και θα δείξουμε ότι η επέκταση $K_n : K_1$ είναι πεπερασμένη. Η απόδειξη θα γίνει με επαγωγή στο n. Για $n = 3$ το ζητούμενο ισχύει από την Πρόταση 4.1. Υποθέτουμε ότι αν οι επεκτάσεις $K_{n-1} : K_{n-2},\ K_{n-2} : K_{n-3}, \ldots, K_2 : K_1$ είναι πεπερασμένες, τότε και η επέκταση $K_{n-1} : K_1$ είναι πεπερασμένη και θα δείξουμε ότι αν οι επεκτάσεις $K_n : K_{n-1},\ K_{n-1} : K_{n-2}, \ldots, K_2 : K_1$ είναι πεπερασμένες, τότε και η επέκταση $K_n : K_1$ είναι πεπερασμένη. Εφόσον οι επεκτάσεις $K_{n-1} : K_{n-2}, \ldots, K_2 : K_1$ είναι πεπερασμένες από την επαγωγική υπόθεση θα έχουμε ότι και η επέκταση $K_{n-1} : K_1$ είναι πεπερασμένη. Έτσι έχουμε ότι οι επεκτάσεις $K_n : K_{n-1},\ K_{n-1} : K_1$ είναι πεπερασμένες, οπότε από την Πρόταση 4.1 θα έχουμε ότι και η επέκταση $K_n : K_1$ είναι πεπερασμένη.
Μένει να δείξουμε ότι $[K_n : K_1] = [K_n : K_{n-1}][K_{n-1} : K_{n-2}] \cdots [K_2 : K_1]$. Πάλι η απόδειξη θα γίνει με επαγωγή. Για $n = 3$ το ζητούμενο ισχύει από την Πρόταση 4.1. Υποθέτουμε ότι

$$[K_{n-1} : K_1] = [K_{n-1} : K_{n-2}][K_{n-2} : K_{n-3}] \cdots [K_2 : K_1]$$

και θα δείξουμε ότι $[K_n : K_1] = [K_n : K_{n-1}][K_{n-1} : K_{n-2}] \cdots [K_2 : K_1]$. Από την επαγωγική υπόθεση θα έχουμε

$$[K_n : K_{n-1}][K_{n-1} : K_{n-2}] \cdots [K_2 : K_1] = [K_n : K_{n-1}][K_{n-1} : K_1]$$

και τώρα από την Πρόταση 4.1 θα έχουμε ότι

$$[K_n : K_{n-1}][K_{n-1} : K_1] = [K_n : K_1],$$

άρα

$$[K_n : K_1] = [K_n : K_{n-1}][K_{n-1} : K_{n-2}] \cdots [K_2 : K_1].$$

□

ΠΑΡΑΤΗΡΗΣΗ 4.2. Η σχέση

$$[K_n : K_1] = [K_n : K_{n-1}] \cdots [K_3 : K_2][K_2 : K_1]$$

που αποδείξαμε στο προηγούμενο Πόρισμα ισχύει ακόμα και αν κάποιες από τις επεκτάσεις

$$K_n : K_1,\ K_n : K_{n-1},\ \ldots,\ K_2 : K_1$$

είναι άπειρου βαθμού. Το αποτέλεσμα προκύπτει από την θεωρία συνόλων και πιο συγκεκριμένα από το πως πολλαπλασιάζονται οι πληθάριθμοι μεταξύ τους.

ΟΡΙΣΜΟΣ 4.5. Έστω $L : K$ να είναι μια επέκταση σώματος και $A \subseteq L$.

Τότε το σύνολο $K \cup A$ παράγει ένα υπόσωμα του L που το συμβολίζουμε $K(A)$ και είναι το σύνολο

$$K(A) = \bigcap \{Y \ \text{ υπόσωμα του } \ L \mid K \cup A \subseteq Y\}.$$

Το $K(A)$ λέμε ότι προκύπτει από το K προσαρτώντας το A.

- Αν $A = \{\alpha_1, \alpha_2, \ldots, \alpha_n\} \subseteq L$, θα συμβολίζουμε το $K(A)$ με $K(\alpha_1, \alpha_2, \ldots, \alpha_n)$ αντί $K\big(\{\alpha_1, \alpha_2, \ldots, \alpha_n\}\big)$
- Αν $A = \{\alpha\}$ και $L = K(\alpha)$, τότε το L λέγεται απλή επέκταση του K.

ΠΑΡΑΔΕΙΓΜΑ 4.4. 1. Η επέκταση $\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}$ είναι απλή επέκταση. Πράγματι αν $L = \mathbb{Q}(\sqrt{2} + \sqrt{3})$ τότε

$$\begin{aligned}\sqrt{2} + \sqrt{3} \in L &\Longrightarrow (\sqrt{2} + \sqrt{3})^2 \in L \Longrightarrow 5 + 2\sqrt{6} \in L \\ &\Longrightarrow (5 + 2\sqrt{6}) - 5 \in L \Longrightarrow 2\sqrt{6} \in L \\ &\Longrightarrow \sqrt{6} \in L \Longrightarrow \sqrt{6}(\sqrt{2} + \sqrt{3}) \in L \\ &\Longrightarrow 2\sqrt{3} + 3\sqrt{2} \in L\end{aligned}$$

όμως

$$\begin{aligned}-2(\sqrt{2} + \sqrt{3}) = -2\sqrt{2} - 2\sqrt{3} \in L &\Longrightarrow -2\sqrt{2} - 2\sqrt{3} + 2\sqrt{3} + 3\sqrt{2} \in L \\ &\Longrightarrow \sqrt{2} \in L \\ &\Longrightarrow \sqrt{3} \in L\end{aligned}$$

2. Έστω η απλή επέκταση $\mathbb{R}(i)$. Από τον παραπάνω ορισμό θα έχουμε ότι

$$\mathbb{R}(i) = \bigcap \big\{ Y \text{ υπόσωμα του } \mathbb{C} \mid \mathbb{R} \cup \{i\} \subseteq Y \big\}.$$

Καθώς το $\mathbb{R}(i)$ είναι υπόσωμα του $\mathbb{C}$ και $\mathbb{R} \cup \{i\} \subseteq \mathbb{R}(i)$, θα έχουμε ότι

$$span\big(\mathbb{R} \cup \{i\}\big) \subseteq \mathbb{R}(i),$$

όμως $\mathbb{C} = span\big(\mathbb{R} \cup \{i\}\big)$ άρα

$$\mathbb{C} = \mathbb{R}(i).$$

3. Έστω η απλή επέκταση $\mathbb{Q}(\sqrt{2})$. Θα δείξουμε ότι $\mathbb{Q}(\sqrt{2}) = \{\alpha_1\sqrt{2} + \alpha_0 \mid \alpha_0, \alpha_1 \in \mathbb{Q}\}$. Το

$$\mathbb{Q}(\sqrt{2}) \supseteq span\{\mathbb{Q}, \sqrt{2}\} = \{\alpha_0 + \alpha_1\sqrt{2} \mid \alpha_0, \alpha_1 \in \mathbb{Q}\} = A.$$

Θα δείξουμε ότι το $A = \{\alpha_0 + \alpha_1\sqrt{2} \mid \alpha_0, \alpha_1 \in \mathbb{Q}\}$ είναι σώμα. Εύκολα βλέπει κανείς ότι το $(A, +)$ είναι αβελιανή ομάδα. Καθώς ο πολλαπλασιασμός επιμερίζεται ως προς τη πρόσθεση μένει να δείξουμε ότι το $(A\backslash\{0\}, \cdot)$ είναι αβελιανή ομάδα. Έστω $x, y \in A$, τότε υπάρχουν $x_0, x_1, y_0, y_1 \in \mathbb{Q}$ ώστε

$$\begin{aligned}x &= x_0 + x_1\sqrt{2} \\ y &= y_0 + y_1\sqrt{2}.\end{aligned}$$

Είναι προφανές ότι το $xy \in A$, ισχύει ο προσεταιρισμός ως προς τον πολλαπλασιασμό και ότι το $1 \in A$. Μένει να βρούμε τον (πολλαπλασιαστικό) αντίστροφο του y.

Υποθέτουμε ότι $(y_0, y_1) \neq (0,0)$. Χωρίς βλάβη της γενικότητας θεωρούμε ότι $y_1 \neq 0$. Αν υπάρχει ο αντίστροφος του y, y^{-1} στο A τότε αυτός θα γράφεται στη μορφή

$$y^{-1} = a + \beta\sqrt{2},$$

για κάποια $a, \beta \in \mathbb{Q}$. Για να είναι το y^{-1} αντίστροφο του y θα πρέπει

$$yy^{-1} = 1 \Longrightarrow (y_0 + y_1\sqrt{2})(a + \beta\sqrt{2}) = 1 \Longrightarrow$$
$$\left\{ \begin{array}{rcl} \alpha y_0 + 2y_1\beta & = & 1 \\ y_0\beta + y_1\alpha & = & 0 \end{array} \right. \Rightarrow \left\{ \begin{array}{rcl} y_1y_0\alpha + 2y_1^2\beta & = & y_1 \\ y_1\alpha & = & -y_0\beta \end{array} \right. \Rightarrow \left\{ \begin{array}{rcl} (2y_1^2 - y_0^2)\beta & = & y_1 \\ y_1\alpha & = & -y_0\beta \end{array} \right.$$

όμως $y_0 \in \mathbb{Q}$, άρα $y_0 \neq y_1\sqrt{2}$ και $y_1 \neq 0$ έτσι

$$\left\{ \begin{array}{rcl} \beta & = & y_1/(2y_1^2 - y_0^2) = y_1/(\sqrt{2}y_1 - y_0)(\sqrt{2}y_1 + y_0) \\ \alpha & = & -y_0/(2y_1^2 - y_0^2) = -y_0/(\sqrt{2}y_1 - y_0)(\sqrt{2}y_1 + y_0) \end{array} \right.$$

Έτσι βρήκαμε τον αντίστροφο του y στο A. Άρα το A είναι σώμα.

Από τον παραπάνω ορισμό θα έχουμε ότι

$$\mathbb{Q}(\sqrt{2}) = \bigcap \{Y \text{ υπόσωμα του } \mathbb{C} \mid \mathbb{Q} \cup \{\sqrt{2}\} \subseteq Y\},$$

έτσι επειδή το $\mathbb{Q}(\sqrt{2})$ είναι σώμα και το $\mathbb{Q} \cup \sqrt{2} \subseteq \mathbb{Q}(\sqrt{2})$ θα έχουμε ότι

$$A = \{\alpha_1\sqrt{2} + \alpha_0 \mid \alpha_0, \alpha_1 \in \mathbb{Q}\} \subseteq \mathbb{Q}(\sqrt{2})$$

άρα το A είναι υπόσωμα του $\mathbb{Q}(\sqrt{2})$. Όμως το $\mathbb{Q}(\sqrt{2})$ είναι το μικρότερο σώμα που περιέχει το $\mathbb{Q} \cup \sqrt{2}$, οπότε

$$\mathbb{Q}(\sqrt{2}) = A = \{\alpha_1\sqrt{2} + \alpha_0 \mid \alpha_0, \alpha_1 \in \mathbb{Q}\}.$$

ΠΑΡΑΤΗΡΗΣΗ 4.3. Σε αυτό το σημείο ας κάνουμε μια πολύ σημαντική παρατήρηση. Είδαμε ότι το αν το K είναι ένα σώμα τότε το $K[x]$ είναι ένας δακτύλιος. Ο δακτύλιος $K[x]$ μπορεί να επεκταθεί σε σώμα αν για κάθε στοιχείο που περιέχει, του προσαρτήσουμε το αντίστροφό του. Το σώμα αυτό το συμβολίζουμε με $K(x)$, ονομάζεται το σύνολο των ρητών εκφράσεων του $K[x]$ και είναι ακριβώς το

$$K(x) = \left\{ \frac{f(x)}{q(x)} \mid f, q \in K[x],\ q \neq 0 \right\}.$$

Παραπάνω ορίσαμε το $K(x)$ να είναι το μικρότερο σώμα που περιέχει το σύνολο $K \cup \{x\}$. Σε αυτό το σημείο αναμενόμενη είναι η ερώτηση: «Τα δυο αυτά σώματα έχουν κάποια σχέση μεταξύ τους»; Πράγματι, τα δύο αυτά σώματα είναι ίδια, δηλαδή το $\left\{ \frac{f(x)}{q(x)} \mid f, q \in K[x],\ q \neq 0 \right\}$ είναι υπόσωμα του $K(x)$ με $K \cup \{x\} \subseteq \left\{ \frac{f(x)}{q(x)} \mid f, q \in K[x],\ q \neq 0 \right\}$, όμως επειδή το μικρότερο σώμα που περιέχει το $K \cup \{x\}$ είναι το $K(x)$, θα έχουμε ότι

$$K(x) = \left\{ \frac{f(x)}{q(x)} \mid f, q \in K[x],\ q \neq 0 \right\}.$$

5 Αλγεβρικές Επεκτάσεις

ΟΡΙΣΜΟΣ 5.1. Έστω $L : K$ μια επέκταση σώματος και $\alpha \in L$. Αν υπάρχει $f \in K[x]$ μη μηδενικό πολυώνυμο, ώστε $f(\alpha) = 0$, τότε το α λέγεται αλγεβρικό επί του K, διαφορετικά το α λέγεται υπερβατικό. Αν για κάθε $\alpha \in L$ το α είναι αλγεβρικό επί του K τότε η επέκταση $L : K$ λέγεται αλγεβρική, ενώ αν υπάρχει $\alpha \in L$ ώστε το α να είναι υπερβατικό επί του K τότε η επέκταση $L : K$ λέγεται υπερβατική.

ΠΑΡΑΔΕΙΓΜΑ 5.1. Θεωρούμε την επέκταση $\mathbb{R} : \mathbb{Q}$. Το $\sqrt{2}$ είναι αλγεβρικό επί του $\mathbb{Q}$, καθώς το $f(x) = x^2 - 2 \in \mathbb{Q}[x]$ και $f(\sqrt{2}) = 0$. Τα e, π είναι υπερβατικά επί του $\mathbb{Q}$. Για το π η πρώτη απόδειξη δόθηκε το 1882 από τον Lindemann και για το e το 1873 από τον Hermitte. Οι αποδείξεις δεν παρουσιάζονται εδώ μιας και ξεπερνούν τους σκοπούς του μαθήματος. Σε κάθε περίπτωση έχουμε ότι η επέκταση $\mathbb{R} : \mathbb{Q}$ είναι υπερβατική.

ΛΗΜΜΑ 5.1. Κάθε πεπερασμένη επέκταση σώματος είναι αλγεβρική.
Απόδειξη. Έστω $L : K$ να είναι μια πεπερασμένη επέκταση σώματος, n να είναι ο βαθμός της και έστω $\alpha \in L$. Θεωρώ τα $n + 1$ στοιχεία $1, \alpha, \alpha^2, \ldots, \alpha^n \in L$. Τότε τα $1, \alpha, \alpha^2, \ldots, \alpha^n$ τα οποία είναι $n+1$ το πλήθος είτε είναι γραμμικώς εξαρτημένα είτε δεν είναι όλα διακριτά. Σε κάθε περίπτωση θα υπάρχουν $c_0, c_1, \ldots, c_n \in K$ όχι όλα μηδέν, ώστε

$$c_0 + c_1\alpha + c_2\alpha^2 + \cdots + c_n\alpha^n = 0$$

Πράγματι αν τα $1, \alpha, \alpha^2, \ldots, \alpha^n$ είναι γραμμικώς εξαρτημένα τότε το ζητούμενο προκύπτει άμεσα από τον ορισμό των γραμμικώς εξαρτημένων διανυσμάτων.

Αν τώρα δεν είναι όλα διακριτά, θα υπάρχουν τουλάχιστον δύο στοιχεία, έστω τα $\alpha^{i_1}, \alpha^{i_2}$ ώστε, $\alpha^{i_1} = \alpha^{i_2}$. Επιλέγω λοιπόν $c_{i_1} = 1,\ c_{i_2} = -1$ και για κάθε $i \neq i_1, i_2$ το $c_i = 0$. Έτσι θα έχω ότι

$$\alpha^{i_1} - \alpha^{i_2} = 0$$

που είναι το είναι το ζητούμενο. Σε κάθε περίπτωση ο α είναι ρίζα του πολυωνύμου

$$f(x) = c_0 + c_1x + c_2x^2 + \cdots + c_nx^n$$

και άρα είναι αλγεβρικό. □

ΠΑΡΑΤΗΡΗΣΗ 5.1. Έστω $K(\alpha) : K$ μια απλή αλγεβρική επέκταση. Τότε υπάρχει ένα πολυώνυμο p επί του K ώστε $p(\alpha) = 0$. Μπορούμε να υποθέσουμε ότι το p είναι μονικό (αν δεν είναι το πολλαπλασιάζουμε με κατάλληλη σταθερά ώστε να γίνει μονικό). Από όλα τα δυνατά μονικά πολυώνυμα με ρίζα το α, επιλέγουμε ένα με ελάχιστο βαθμό. Έστω m το πολυώνυμο αυτό. Θα δείξουμε ότι το πολυώνυμο m είναι μοναδικό.

Αν δεν ήταν μοναδικό, τότε θα υπήρχε ένα άλλο μονικό πολυώνυμο $q \neq m$ επί του K, ώστε το q να έχει ρίζα το α και να έχει τον ίδιο βαθμό με το m. Τότε όμως το πολυώνυμο

$$h = m - q,$$

πολλαπλασιασμένο με κατάλληλη σταθερά, είναι μονικό, έχει ρίζα το α και έχει μικρότερο βαθμό από το m (τα m, q είναι μονικά του ίδιου βαθμού, άρα η διαφορά $m-q$ απαλείφει τον μεγιστοβάθμιο όρο), το οποίο όμως είναι άτοπο, διότι υποθέσαμε ότι το m είναι ελαχίστου βαθμού.

ΟΡΙΣΜΟΣ 5.2. Έστω $L : K$ μια επέκταση σώματος και έστω $\alpha \in L$ να είναι αλγεβρικό επί του K. Τότε το ελάχιστο πολυώνυμο του α επί του K, είναι το μοναδικό, μονικό πολυώνυμο m επί του K, ελαχίστου βαθμού ώστε

$$m(\alpha) = 0.$$

ΛΗΜΜΑ 5.2. Έστω $L : K$ μια επέκταση σώματος και έστω $\alpha \in L$ να είναι αλγεβρικό επί του K. Τότε το ελάχιστο πολυώνυμο του α επί του K, έστω m, είναι ανάγωγο.
Απόδειξη. Εύκολα βλέπουμε ότι το πολυώνυμο m, είναι ανάγωγο επί του K. Πράγματι αν το m δεν ήταν ανάγωγο, τότε θα υπήρχαν πολυώνυμα f, g επί του K, με βαθμό μικρότερο του m, ώστε

$$m = fg \quad \text{και} \quad \deg(f), \deg(g) \geq 1.$$

Άρα $m(\alpha) = f(\alpha)g(\alpha) = 0$. Όμως τα $f(\alpha), g(\alpha)$ ανήκουν στο σώμα $K(\alpha)$, άρα

$$f(\alpha) = 0 \qquad \text{ή} \qquad g(\alpha) = 0.$$

Το οποίο είναι άτοπο, διότι το m είναι το ελάχιστο πολυώνυμο του α επί του K.

□

ΛΗΜΜΑ 5.3. Έστω $L : K$ μια επέκταση σώματος και έστω $\alpha \in L$ αλγεβρικό επί του K. Θεωρούμε m το ελάχιστο πολυώνυμο του α επί του K και f ένα πολυώνυμο επί του K. Τότε το πολυώνυμο f έχει ρίζα το α αν και μόνο αν το m διαιρεί το f στο $K[x]$, δηλαδή

$$f(\alpha) = 0 \iff m \mid f \qquad \text{στο } K[x].$$

Απόδειξη. ($\Longrightarrow$) Έστω f ένα πολυώνυμο επί του K με $f(\alpha) = 0$. Από τον αλγόριθμο της διαίρεσης θα έχουμε ότι υπάρχουν πολυώνυμα h και r επί του K ώστε

$$f = hm + r \qquad \text{όπου είτε} \quad r = 0 \quad \text{είτε} \quad \deg(r) < \deg(m).$$

Άρα

$$f(\alpha) = h(\alpha)m(\alpha) + r(\alpha) \Longrightarrow 0 = 0 + r(\alpha) \Longrightarrow r(\alpha) = 0.$$

Αν το πολυώνυμο $r \neq 0$, τότε αν πολλαπλασιαστεί με κατάλληλη σταθερά θα γίνει μονικό πολυώνυμο με ρίζα το α και βαθμό μικρότερο από το βαθμό του m. Αυτό όμως είναι άτοπο, διότι το m είναι το ελάχιστο πολυώνυμο. Συνεπώς $r = 0$ και έτσι το m διαιρεί το f.
($\Longleftarrow$) Τώρα αν το m διαιρεί το f, θα έχουμε ότι υπάρχει πολυώνυμο q επί του K ώστε

$$f = qm.$$

Συνεπώς είναι φανερό ότι $f(\alpha) = q(\alpha)m(\alpha) = 0$

□

ΠΑΡΑΤΗΡΗΣΗ 5.2. Συνέπεια των παραπάνω είναι το εξής. Έστω $L : K$ μια επέκταση. Αν ένα πολυώνυμο m επί του K είναι ανάγωγο, μονικό και έχει ρίζα το α, τότε το m είναι το ελάχιστο πολυώνυμο του α επί του K.

ΘΕΩΡΗΜΑ 5.1. Μια απλή επέκταση $K(\alpha) : K$ είναι πεπερασμένη αν και μόνο αν το α είναι αλγεβρικό επί του K. Σε αυτή τη περίπτωση ο βαθμός της επέκτασης είναι ίσος με τον βαθμό του ελαχίστου πολυωνύμου του α επί του K.

Απόδειξη. ($\Longrightarrow$) Αν η επέκταση είναι πεπερασμένη, τότε από το Λήμμα 5.1 θα έχουμε ότι η επέκταση $K(\alpha) : K$ είναι αλγεβρική και συνεπώς το α είναι αλγεβρικό επί του K.

($\Longleftarrow$) Ας υποθέσουμε ότι το α είναι αλγεβρικό επί του K. Θεωρούμε το σύνολο

$$R = \{f(\alpha) \mid f \in K[x]\}.$$

Εύκολα βλέπουμε ότι το R είναι δακτύλιος του $K(\alpha)$. Επίσης, το $f(\alpha) = 0$ αν και μόνο αν το ελάχιστο πολυώνυμο m του α διαιρεί το f. Άρα $f(\alpha) = 0$ αν και μόνο αν $f \in \langle m \rangle$, όπου $\langle m \rangle$ το ιδεώδες του $K[x]$ που παράγεται από το m.

Θεωρούμε τον ομομορφισμό $K[x] \to R$ με $f \mapsto f(\alpha)$. Αυτός είναι ομομορφισμός δακτυλίων και ο πυρήνας του είναι το ιδεώδες $\langle m \rangle$. Από το πρώτο θεώρημα Ισομορφισμών έχουμε $K[x]/\langle m \rangle \cong R$. Όμως το m είναι ανάγωγο άρα το $K[m]/\langle m \rangle$ είναι σώμα. Άρα το R είναι σώμα, υπόσωμα του $K(\alpha)$, το οποίο περιέχει το $K \cup \{\alpha\}$. Άρα $K(\alpha) = R$.

Έστω $z \in K(\alpha)$. Το $z = g(\alpha)$ για κάποιο $g \in K[x]$. Αλλά αν διαιρέσω το g με το m έχω ότι υπάρχουν $q, r \in K[x]$ με $g = qm + r$ και είτε $r = 0$ είτε $\deg r < \deg m$. Ξέρουμε όμως ότι $m(\alpha) = 0$ συνεπώς $z = g(\alpha) = r(\alpha)$. Αν υπάρχει και άλλο $h \in K[x]$ με $z = h(\alpha)$ όπου είτε $h = 0$ είτε $\deg h < \deg m$ τότε το m διαιρεί το $h - r$ εφόσον το α είναι ρίζα του $h - r$. Αλλά αν $h - r \neq 0$ τότε ο βαθμός του είναι μικρότερος από τον βαθμό του m, άτοπο στην επιλογή του m. Άρα το r είναι μοναδικό. Με άλλα λόγια, κάθε στοιχείο $z \in K(\alpha)$ μπορεί να εκφραστεί σαν $z = r(\alpha)$ για μοναδικό $r \in K[x]$ όπου είτε $r = 0$ είτε $\deg r < \deg m$. Επομένως, αν $n = \deg m$ τότε τα $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$ αποτελούν βάση του $K(\alpha)$ επί του K. Άρα $[K(\alpha) : K] = \deg m$. □

ΠΟΡΙΣΜΑ 5.1. Αν $K(\alpha) : K$ μια απλή αλγεβρική επέκταση και m το ελάχιστο πολυώνυμο του α επί του K τότε κάθε στοιχείο του σώματος $K(\alpha)$ γράφεται κατά μοναδικό τρόπο στην μορφή $p(\alpha)$ όπου $p \in K[x]$ με $\deg p < \deg m$.

ΠΟΡΙΣΜΑ 5.2. Μια επέκταση $L : K$ είναι πεπερασμένη αν και μόνο αν υπάρχει ένα πεπερασμένο υποσύνολο $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ του L, ώστε κάθε α_j, $j = 1, 2, \ldots, n$ να είναι αλγεβρικό επί του K και $L = K(\alpha_1, \alpha_2, \ldots, \alpha_n)$.

Απόδειξη. ($\Longrightarrow$) Υποθέτουμε ότι η επέκταση $L : K$ είναι πεπερασμένη και έστω $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ να είναι μια βάση του L επί του K. Αφού η επέκταση $L : K$ είναι πεπερασμένη, από το Λήμμα 5.1 θα έχουμε ότι η επέκταση $L : K$ είναι αλγεβρική. Συνεπώς θα έχουμε ότι το α_j είναι αλγεβρικό επί του K για κάθε $j = 1, 2 \ldots, n$ και επειδή το σύνολο $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ είναι βάση του L επί του K, θα έχουμε ότι

$$K(\alpha_1, \alpha_2, \ldots, \alpha_n) = L.$$

($\Longleftarrow$) Υποθέτουμε ότι $L = K(\alpha_1, \ldots, \alpha_k)$ όπου α_i, $i = 1, \ldots, k$ αλγεβρικά επί του K. Έστω $K_i = K(\alpha_i, \ldots, a_i)$, $i = 1, \ldots, k$. Προφανώς $K_{i-1}(\alpha_i) \subset K_i$ για κάθε $i > 1$ εφόσον $K_{i-1} \subset K_i$ και $\alpha_i \in K_i$.

Όμως και $K_i \subset K_{i-1}(\alpha_i)$ εφόσον το $K_{i-1}(\alpha_i)$ είναι υπόσωμα του L που περιέχει το $K \cup \{\alpha_1, \ldots, \alpha_i\}$. Άρα $K_i = K_{i-1}(\alpha_i)$ για $i = 2, \ldots, k$. Επίσης, κάθε α_i είναι αλγεβρικό επί του K_{i-1} εφόσον είναι αλγεβρικό επί του K και $K \subset K_{i-1}$. Άρα $K_i : K_{i-1}$ είναι αλγεβρική επέκταση για κάθε i άρα και πεπερασμένη. Από το tower law έχουμε ότι

$$[K_n : K] = [K_n : K_{n-1}] \ldots [K_2 : K_1][K_1 : K] < \infty$$

δηλαδή η $K_n : K$ πεπερασμένη επέκταση. □

6 Κατασκευές με κανόνα και διαβήτη

Αρχικά με στόχο να κεντρίσουμε το ενδιαφέρον του αναγνώστη θα παρουσιάσουμε μερικά γεωμετρικά προβλήματα της αρχαιότητας που απασχολούσαν τους μαθηματικούς για πολλά χρόνια.

1. Δεδομένου ενός κύκλου, είναι δυνατόν με κανόνα και διαβήτη να κατασκευάσουμε ένα τετράγωνο που να έχει το ίδιο εμβαδόν με τον κύκλο? (τετραγωνισμός του κύκλου)

2. Δεδομένου ενός κύβου, είναι δυνατόν με κανόνα και διαβήτη να κατασκευάσουμε έναν νέο κύβο με διπλάσιο όγκο?

3. Δεδομένης μιας γωνίας θ, είναι δυνατόν με κανόνα και διαβήτη να τριχοτομήσουμε την γωνία θ, δηλαδή να κατασκευάσουμε την γωνία $\theta/3$?

Για πολλούς αιώνες τα προβλήματα αυτά απασχολούσαν τους μαθηματικούς οι οποίοι προσπαθούσαν να τα λύσουν με γεωμετρικά εργαλεία.

Σε πρώτη φάση, θα εκφράσουμε αλγεβρικά την ιδέα της κατασκευής με κανόνα και διαβήτη. Έστω $\mathscr{P}$ ένα σύνολο σημείων του Ευκλείδειου επιπέδου $\mathbb{R}^2$. Ορίζουμε τις εξής δύο διαδικασίες:

1. **Διαδικασία** 1 (κανόνας)
   Ενώνουμε οποιουσδήποτε δυο σημεία του συνόλου $\mathscr{P}$, με ευθεία γραμμή.

2. **Διαδικασία** 2 (διαβήτης)
   Κατασκευάζουμε ένα κύκλο, του οποίου το κέντρο είναι κάποιο από τα σημεία του $\mathscr{P}$ και διέρχεται από οποιοδήποτε άλλο σημείο του $\mathscr{P}$.

ΟΡΙΣΜΟΣ 6.1. Τα σημεία της τομής οποιασδήποτε ευθείας με ευθεία ή ευθείας με κύκλο ή κύκλου με κύκλο (τα σχήματα είναι διακριτά μεταξύ τους), που κατασκευάστηκαν με τις Διαδικασίες 1 και 2, τα ονομάζουμε κατασκευάσιμα σε ένα βήμα από το $\mathscr{P}$.

Ένα σημείο $P \in \mathbb{R}^2$ θα λέμε ότι είναι κατασκευάσιμο από το $\mathscr{P}$, αν υπάρχει μια πεπερασμένη ακολουθία σημείων του $\mathbb{R}^2$

$$P_0, P_1, \ldots, P_r = P$$

ώστε για κάθε $i = 0, 1, \ldots, r$ το σημείο P_i να είναι κατασκευάσιμο σε ένα βήμα από το σύνολο

$$\mathscr{P} \cup \{P_0, P_1, \ldots, P_{i-1}\}.$$

ΘΕΩΡΗΜΑ 6.1. Έστω (x, y) να είναι ένα κατασκευάσιμο σημείο του επιπέδου από το σύνολο σημείων

$$\mathscr{P} = \big\{P_0 = (0, 0), P_1 = (1, 0)\big\}.$$

Τότε η επέκταση $\mathbb{Q}(x, y) : \mathbb{Q}$ έχει βαθμό

$$[\mathbb{Q}(x, y) : \mathbb{Q}] = 2^r,$$

για κάποιο $r \in \mathbb{N}$.

Απόδειξη. Έστω ότι $P = (x, y)$ και $P_0, P_1, \ldots, P_n = P$ μια ακολουθία κατασκευάσιμων σημείων από το $\mathscr{P}$. Ορίζουμε $K_0 = K_1 = \mathbb{Q}$ και $K_j = K_{j-1}(x_j, y_j)$, όπου $P_j = (x_j, y_j)$ για κάθε $j = 2, \ldots, n$. Από την αναλυτική γεωμετρία ξέρουμε ότι για κάθε j οι πραγματικοί αριθμοί x_j, y_j είναι είτε ρίζες γραμμικών εξισώσεων, είτε είναι ρίζες τετραγωνικών πολυωνύμων με συντελεστές στο K_{j-1}. Άρα

$$[K_{j-1}(x_j) : K_{j-1}] = 1 \text{ ή } 2 \qquad \text{και} \qquad [K_{j-1}(x_j, y_j) : K_{j-1}(x_j)] = 1 \text{ ή } 2.$$

Από το Πόρισμα 4.1 θα έχουμε ότι

$$[K_n : \mathbb{Q}] = [K_{n-1}(x_n, y_n) : K_{n-1}(x_n)][K_{n-2}(x_{n-1}, y_{n-1}) : K_{n-2}(x_{n-1})] \cdots [K_2 : \mathbb{Q}] = 2^\kappa$$

για κάποιο $\kappa \in \mathbb{N}$. Όμως από την Πρόταση 4.1

$$2^\kappa = [K_n : \mathbb{Q}] = [K_n : \mathbb{Q}(x, y)][\mathbb{Q}(x, y) : \mathbb{Q}],$$

άρα το $[\mathbb{Q}(x, y) : \mathbb{Q}]$ διαιρεί το 2^κ άρα υπάρχει $r \in \mathbb{N}$ ώστε

$$[\mathbb{Q}(x, y) : \mathbb{Q}] = 2^r.$$

□

Τώρα είμαστε σε θέση να απαντήσουμε στα προβλήματα που θέσαμε στην αρχή της ενότητας.

Τα Προβλήματα

1. Ο τετραγωνισμός του κύκλου δεν είναι κατασκευάσιμος στο $\{(0, 0), (1, 0)\}$, διότι αν ήταν θα μπορούσαμε να κατασκευάσουμε το σημείο $(\sqrt{\pi}, 0)$. Όμως ένα σημαντικό θεώρημα του Lindemann μας λέει ότι ο π είναι υπερβατικός επί του $\mathbb{Q}$. Οπότε $[\mathbb{Q}(\sqrt{\pi} : \mathbb{Q})] = \infty$, άρα ο $\sqrt{\pi}$ δεν κατασκευάζεται στο $\{(0, 0), (0, 1)\}$.

2. Ο διπλασιασμός του όγκου του κύβου, επίσης δεν είναι κατασκευάσιμος στο $\{(0,0),(1,0)\}$, καθώς αν ήταν θα σήμαινε ότι μπορώ να κατασκευάσω κύβο με όγκο 2, δηλαδή κύβο πλευράς $\sqrt[3]{2}$. Όμως το x^3-2 είναι το ελάχιστο πολυώνυμο του $\sqrt[3]{2}$ επί του $\mathbb{Q}$, άρα

$$[\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q}] = \deg(x^3-2) = 3.$$

Έτσι καθώς δεν υπάρχει $r \in \mathbb{N}$ ώστε $2^r = 3$, το σημείο $(\sqrt[3]{2},0)$ δεν μπορεί να κατασκευαστεί.

3. Η τριχοτόμηση γωνίας δεν είναι κατασκευάσιμη στο $\{(0,0),(1,0)\}$. Θεωρούμε την γωνία $\pi/3$ και ας προσπαθήσουμε να την τριχοτομήσουμε. Έστω $a = \cos(\pi/9)$ και $b = \sin(\pi/9)$. Ξέρουμε ότι το σημείο $\big(\cos(\pi/3),\sin(\pi/3)\big) = (\sqrt{3}/2,1/2)$ είναι κατασκευάσιμο. Αν η γωνία $\pi/3$ μπορούσε να τριχοτομηθεί τότε το σημείο (a,b) θα ήταν κατασκευάσιμο. Όμως

$$\begin{aligned}\cos(3\theta) &= \cos(\theta)\cos(2\theta) - \sin(\theta)\sin(2\theta)\\ &= \cos(\theta)\big(\cos^2(\theta)-\sin^2(\theta)\big) - 2\sin^2(\theta)\cos(\theta)\\ &= 4\cos^3(\theta) - 3\cos(\theta)\end{aligned}$$

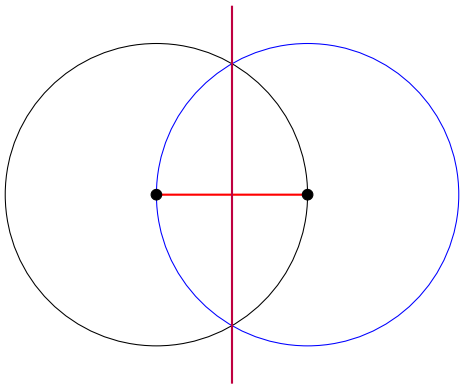
για κάθε $\theta \in [0,2\pi]$. Αν $\theta = \pi/9$ τότε

$$\frac{1}{2} = 4a^3 - 3a \iff 8a^3 - 6a - 1 = 0.$$

Άρα το a είναι ρίζα του πολυωνύμου $8x^3-6x-1$. Θεωρούμε το πολυώνυμο $f(x) = x^3+3x^2-3$. Εύκολα βλέπουμε ότι $f(2a-1) = 8x^3-6x-1$. Επιπλέον, από το θεώρημα του Eisenstein έχουμε ότι το f είναι ανάγωγο επί του $\mathbb{Q}$ και άρα $[\mathbb{Q}(a):\mathbb{Q}] = [\mathbb{Q}(2a-1):\mathbb{Q}] = 3$. Άρα το σημείο $(\cos\frac{\pi}{9},\sin\frac{\pi}{9})$ δεν είναι κατασκευάσιμο με κανόνα και διαβήτη, άρα η γωνία $\frac{\pi}{3}$ δεν τριχοτομείται.

Τελικά τίθεται το ερώτημα "τι είναι κατασκευάσιμο στο $\{(0,0),(1,0)\}$"; Για να μπορέσουμε να απαντήσουμε χρειαζόμαστε δύο βασικά κατασκευαστικά αποτελέσματα.

Λημμα 6.1. Αν μας δοθούν τα τελικά σημεία ενός ευθύγραμμου τμήματος, τότε μπορούμε να κατασκευάσουμε το μέσον του με κανόνα και διαβήτη.
Απόδειξη.

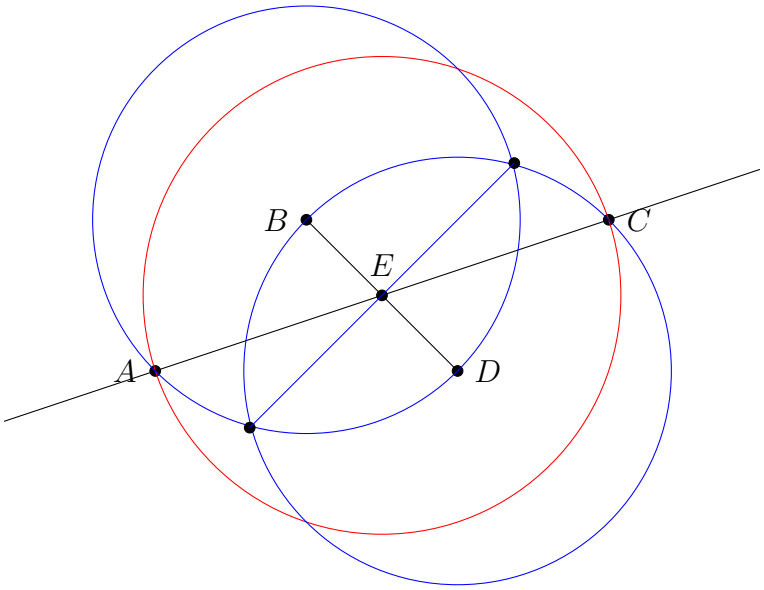


Η απόδειξη είναι γνωστή από το γυμνάσιο και αφήνεται σαν άσκηση.

□

Λημμα 6.2. Αν οποιεσδήποτε 3 κορυφές ενός παραλληλογράμμου είναι κατασκευάσιμες τότε και τέταρτη κορυφή είναι κατασκευάσιμη.

Απόδειξη. Έστω A, B, C, D οι κορυφές του παραλληλογράμμου (δεξιόστροφα ή αριστερόστροφα) και υποθέτουμε ότι οι A, B, D είναι κατασκευάσιμες. Θα δείξουμε ότι και η C είναι κατασκευάσιμη. Παρατηρήστε ότι το μέσο του ευθυγράμμου τμήματος BD είναι κατασκευάσιμο και ας το ονομάσουμε E. Τότε ο κύκλος κέντρου E που περνά από το A τέμνει την AE στο C. Άρα το C είναι κατασκευάσιμο.



□

Θεωρημα 6.2. Έστω $K = \{x \in \mathbb{R} \mid \text{το } (x,0) \text{ να είναι κατασκευάσιμο στο } \{(0,0),(1,0)\}\}$. Τότε το K είναι υπόσωμα του $\mathbb{R}$ και ένα σημείο $(x,y) \in \mathbb{R}^2$ είναι κατασκευάσιμο στο σύνολο $\{(0,0),(1,0)\}$ αν και μόνο αν $x, y \in K$. Επιπλέον αν $x > 0$ και $x \in K$ τότε και $\sqrt{x} \in K$.

Απόδειξη. Προφανώς $0, 1 \in K$. Έστω $x, y \in K$. Τότε τα $(x,0)$ και $(y,0)$ είναι κατασκευάσιμα. Αν M το μέσο του ευθύγραμμου τμήματος με άκρα τα $(x,0)$ και $(y,0)$ τότε το x είναι κατασκευάσιμο και $M = (\frac{x+y}{2}, 0)$. Θεωρούμε τον κύκλο κέντρου M που περνά από το σημείο $(0,0)$ περνά από $(x+y,0)$. Άρα το $(x+y,0)$ είναι κατασκευάσιμο, δηλαδή $x+y \in K$. Άρα το K είναι ομάδα ως προς την πρόσθεση.

Ας θεωρήσουμε τώρα τον κύκλο κέντρου $(0,0)$ που περνά από το $(x,0)$. Αυτός τέμνει τον οριζόντιο άξονα στα $(-x,0)$ και $(x,0)$. Άρα το $(-x,0)$ είναι κατασκευάσιμο και άρα το $-x \in K$.

Αν το $x \in K$ με $x \neq 0$ τότε τα σημεία $(x,0)$ και $(-x,0)$ είναι κατασκευάσιμα. Επιπλέον, ο κύκλος κέντρου $(0,0)$ που περνά από τα $(x,0)$ και $(-x,0)$ τέμνει τον κάθετο άξονα στα $(0,x)$ και $(0,-x)$ άρα αν $x \in K$ το $(0,x)$ είναι κατασκευάσιμο.

Έστω $x, y \in K$. Τα $(x, 0)$, $(0, y)$ και $(0, 1)$ είναι κατασκευάσιμα. Τότε και το $(x, y-1)$ είναι κατασκευάσιμο μιας και είναι η τέταρτη κορυφή του παραλληλογράμμου με τρεις κατασκευάσιμες κορυφές, τις $(x, 0), (0, y), (0, 1)$. Επιπλέον, η ευθεία που περνά από τα σημεία $(0, y)$ και $(x, y-1)$ τέμνει τον οριζόντιο άξονα στο $(xy, 0)$. Άρα το $(xy, 0)$ είναι κατασκευάσιμο και $xy \in K$.

Αν τώρα $x, y \in K$ με $y \neq 0$ τότε το σημείο $(x, 1-y)$ είναι επίσης κατασκευάσιμο διότι είναι η τέταρτη κορυφή του παραλληλογράμμου με κορυφές $(x, 0), (0, y), (0, 1)$. Το ευθύγραμμο τμήμα που ενώνει τα $(0, 1)$ και $(x, 1-y)$ τέμνει τον οριζόντιο άξονα στο $(xy^{-1}, 0)$ και άρα $xy^{-1} \in K$.

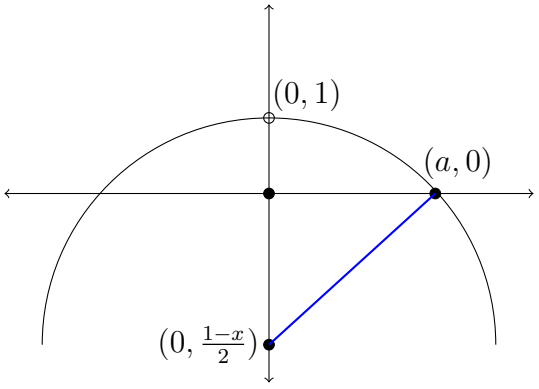
Τα παραπάνω δείχνουν ότι το K είναι υπόσωμα του $\mathbb{R}$. Επιπλέον αν $x, y \in K$ τότε το (x, y) είναι κατασκευάσιμο σαν τέταρτη κορυφή του παραλληλογράμμου με κορυφές τα κατασκευάσιμα σημεία $(0, 0), (x, 0), (0, y)$.

Αντίστροφα, ας υποθέσουμε ότι το σημείο (x, y) είναι κατασκευάσιμο. Θα δείξουμε ότι το $(x, 0)$ είναι κατασκευάσιμο. Αυτό προφανώς ισχύει αν $y = 0$. Αν $y \neq 0$ τότε οι κύκλοι με κέντρα στα $(0, 0)$ και $(1, 0)$ που περνούν από το σημείο (x, y) τέμνονται στα (x, y) και $(x, -y)$. Το ευθύγραμμο τμήμα που περνά από τα (x, y) και $(x, -y)$ τέμνει τον οριζόντιο άξονα στο $(x, 0)$. Άρα είναι κατασκευάσιμο. Επιπλέον το σημείο $(0, y)$ είναι η τέταρτη κορυφή παραλληλογράμμου με 3 κορυφές τις $(0, 0), (x, 0), (x, y)$ και άρα είναι κατασκευάσιμο. Επίσης, ο κύκλος κέντρου $(0, 0)$ που περνά από το σημείο $(0, y)$ τέμνει τον οριζόντιο άξονα στο $(y, 0)$ και άρα και αυτό είναι κατασκευάσιμο δηλαδή $y \in K$. Επομένως το (x, y) είναι κατασκευάσιμο αν και μόνο αν $x, y \in K$.

Ας υποθέσουμε τώρα ότι $x \in K$ με $x > 0$. Τότε το $\frac{1-x}{2} \in K$. Άρα το $C = (0, \frac{1-x}{2})$ είναι κατασκευάσιμο. Έστω ο κύκλος κέντρου C που περνά από το $(0, 1)$. Αυτός τέμνει τον οριζόντιο άξονα στο $(a, 0)$. Η ακτίνα του κύκλου αυτού είναι $\frac{1+x}{2}$ και επομένως από το Πυθαγόρειο Θεώρημα έχουμε ότι

$$\frac{(1-x)^2}{4} + a^2 = \frac{(1+x)^2}{4} \Rightarrow a^2 = x.$$

Αλλά το $(a, 0)$ είναι όπως είδαμε κατασκευάσιμο. Συνεπώς, το $\sqrt{x}$ είναι κατασκευάσιμο δηλαδή $\sqrt{x} \in K$. □



Κατασκευή του $\sqrt{x}$

7 Σώματα διάσπασης

ΟΡΙΣΜΟΣ 7.1. Έστω K ένα σώμα και f ένα πολυώνυμο επί του K. Θα λέμε ότι το f διασπάται στο K αν υπάρχουν $c, \alpha_1, \alpha_2, \ldots, \alpha_n \in K$ ώστε

$$f(x) = c(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n).$$

(c είναι ο συντελεστής του μεγιστοβαθμίου όρου.)

ΟΡΙΣΜΟΣ 7.2. Έστω L ένα σώμα, K ένα υπόσωμα του L και έστω f ένα πολυώνυμο επί του K. Τότε το L θα λέγεται σώμα διάσπασης του f αν

1. Το f διασπάται επί του L,
2. Το f δεν διασπάται σε κανένα γνήσιο υπόσωμα του L που περιέχει το K.

ΟΡΙΣΜΟΣ 7.3. Μια επέκταση $L : K$ θα λέγεται *διασπαστική επέκταση* αν υπάρχει κάποιο πολυώνυμο f επί του K ώστε το L να είναι το σώμα διάσπασης του f.

ΠΑΡΑΔΕΙΓΜΑ 7.1. Έστω $x^2 - 2 \in \mathbb{Q}[x]$. Αν θεωρήσω το $x^2 - 2$ επί του $\mathbb{C}$ ή του $\mathbb{R}$, τότε αυτό διασπάται καθώς $x^2-2 = (x-\sqrt{2})(x+\sqrt{2})$. Όμως το $\mathbb{C}$ δεν είναι το σώμα διάσπασης του $x^2 - 2$, καθώς το $x - 2$ διασπάται επί του $\mathbb{Q}[x] \subseteq \mathbb{C}$.

ΠΡΟΤΑΣΗ 7.1. Έστω $M : K$ μια επέκταση, $f \in K[x]$ ώστε να διασπάται στο M. Τότε υπάρχει υπόσωμα L του M ώστε το L να είναι το σώμα διάσπασης του f.
Απόδειξη. Αφού το f διασπάται στο M, το f θα γράφεται στη μορφή

$$f(x) = c(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n), \quad \text{όπου} \quad \alpha_1, \alpha_2, \ldots, \alpha_n \in M, \;\; c \in K.$$

Τότε το σώμα διάσπασης του f επί του K είναι το $K(\alpha_1, \alpha_2, \ldots, \alpha_n)$.
(Φανερά το f διασπάται στο $K(\alpha_1, \alpha_2, \ldots, \alpha_n)$ και το $K(\alpha_1, \alpha_2, \ldots, \alpha_n)$ είναι υπόσωμα του m).

□

ΛΗΜΜΑ 7.1. Έστω $M : K$ επέκταση σώματος και $f \in K[x]$. Αν το f διασπάται στο M τότε υπάρχει μοναδικό υπόσωμα L του M το οποίο είναι το σώμα διάσπασης του f

Απόδειξη. Αρκεί να πάρω την τομή όλων των υποσωμάτων του M στα οποία το f διασπάται □

ΘΕΩΡΗΜΑ 7.1 (Kronecker). Έστω K ένα σώμα και f ένα πολυώνυμο επί του K. Τότε υπάρχει μια επέκταση L του K και $\alpha \in L$ ώστε

$$f(\alpha) = 0.$$

Απόδειξη. Έστω $f \in K[x]$. Αν κάποια από τις ρίζες του πολυωνύμου f ανήκει στο K τότε αρκεί να πάρω $K = L$.

Διαφορετικά η παραγοντοποίηση του f θα έχει ανάγωγους παράγοντες. Έστω m να είναι ένας από αυτούς και $I = \langle m \rangle$ το ιδεώδες του $K[x]$ που παράγεται από το m. Από το Θεώρημα 3.2 το $L = K[x]/I$ είναι σώμα. Ορίζουμε $i : K \to L$ με $i(a) = a + I$ για κάθε $a \in K$. Ο i είναι μονομορφισμός και άρα μπορούμε να εμφυτεύσουμε το K στο L ταυτίζοντας το K με το $i(K)$ και άρα κάθε $a \in K$ με το $a + I \in L$.

Θεωρούμε το στοιχείο $x + I \in L$. Τότε το $m(x + I) = m(x) + I = I$ άρα το $x + I$ είναι ρίζα του m στο L, άρα είναι και ρίζα του f στο L. □

Θεωρημα 7.2. Έστω K ένα σώμα και f ένα πολυώνυμο επί του K. Τότε υπάρχει σώμα διάσπασης του f επί του K.

Απόδειξη. Έστω $\deg(f) = n$. Η απόδειξη θα γίνει με επαγωγή στον βαθμού του πολυωνύμου f. Για $n = 1$ δεν έχουμε να αποδείξουμε τίποτα, καθώς το σώμα διάσπασης του f είναι το K. Υποθέτουμε ότι κάθε πολυώνυμο βαθμού n έχει σώμα διάσπασης. Αν q είναι ένα πολυώνυμο με $\deg(q) = n + 1$, τότε από το Θεώρημα 7.1 (Kronecker), υπάρχει ένα σώμα Σ και $\alpha \in \Sigma$ ώστε $q(\alpha) = 0$. Άρα το q γράφεται στη μορφή

$$q(x) = (x - \alpha)h(x),$$

όπου $h \in K(\alpha)[x]$ με $\deg(h) = n$. Τώρα όμως από την επαγωγική υπόθεση θα έχουμε ότι υπάρχει σώμα διάσπασης, έστω L, του h επί του $K(\alpha)$. Έτσι το q διασπάται στο L. Μένει να δείξουμε ότι το L είναι το μικρότερο σώμα στο οποίο διασπάται το q. Έστω ότι το q διασπάται σε κάποιο σώμα M με $K \subset M \subset L$, τότε το $\alpha \in M$ και συνεπώς $K(\alpha) \subset M$. Αλλά τό M πρέπει να περιέχει και τις ρίζες του h εφόσον αυτές είναι ρίζες και του q. Άρα από τον ορισμό του σώματος διάσπασης $L = M$. □

Λημμα 7.2. Κάθε ομομορφισμός σωμάτων $\sigma : K \to M$ επεκτείνεται σε ομομορφισμό δακτυλίων $\sigma_* : K[x] \to M[x]$. Επιπλέον, αν ο σ είναι ισομορφισμός και ο σ_* είναι ισομορφισμός και διατηρεί τους ανάγωγους παράγοντες.

Απόδειξη. Έστω $f \in K[x]$ με $f(x) = a_0 + a_1x + \ldots + a_nx^n$. Ορίζουμε

$$\sigma_*(f) = \sigma(a_0) + \sigma(a_1)x + \ldots + \sigma(a_n)x^n$$

για κάθε $f \in K[x]$. Εύκολα βλέπουμε ότι $\sigma_*(f+g) = \sigma_*(f)+\sigma_*(g)$ και $\sigma_*(fg) = \sigma_*(f)\sigma_*(g)$. Εύκολα βλέπουμε ότι αν η σ ισομορφισμός τότε και η σ_* ισομορφισμός.

Τέλος έστω $f \in K[x]$ ανάγωγο και $\sigma_*(f) = gh$ όπου $g, h \in M[x]$ και $\deg g, \deg h > 0$. Εφόσον η σ_* ισομορφισμός και η σ_*^{-1} είναι ισομορφισμός και άρα $\sigma_*^{-1}(\sigma_*(f)) = \sigma_*^{-1}(g)\sigma_*^{-1}(h)$ δηλαδή $f = \sigma_*^{-1}(g)\sigma_*^{-1}(h)$. Άρα το f δεν είναι ανάγωγο, άτοπο. □

Θεωρημα 7.3. Έστω K_1 και K_2 να είναι δύο ισομορφικά σώματα και $\sigma : K_1 \longrightarrow K_2$ ο ισομορφισμός. Έστω επίσης $f \in K_1[x]$ και L_1, L_2 τα σώματα διάσπασης των f και $\sigma_*(f)$ επί των K_1 και K_2 αντίστοιχα. Τότε υπάρχει ισομορφισμός $\tau : L_1 \longrightarrow L_2$ ο οποίος επεκτείνει τον σ, δηλαδή $\tau\,|_{K_1} = \sigma$.

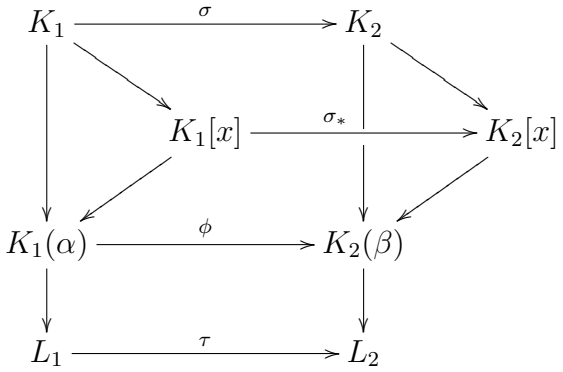
Απόδειξη. Θα δείξουμε το αποτέλεσμα με επαγωγή στον βαθμό $[L_1 : K_1]$. Αν $[L_1 : k_1] = 1$ τότε $K_1 = L_1$ και άρα $K_2 = L_2$ και ο ζητούμενος ισομορφισμός τ είναι είναι ο σ. Υποθέτουμε ότι $[L_1 : K_1] > 1$ και το αποτέλεσμα ισχύει για όλες τις διασπαστικές επεκτάσεις μικρότερου βαθμού.

Έστω α μια ρίζα του f στο $L_1 \setminus K_1$ και έστω m το ελάχιστο πολυώνυμο του α επί του K_1. Τότε το m διαιρεί το f και άρα υπάρχει $q \in K_1[x]$ ώστε $f = mq$. Συνεπώς, $\sigma_*(f) = \sigma_*(mq) = \sigma_*(m)\sigma_*(q)$ και το $\sigma_*(m)$ διαιρεί το $\sigma_*(f)$. Όμως το f διασπάται επί του L_1 και το $\sigma_*(f)$ διασπάται επί του L_2. Επομένως το $\sigma_*(m)$ διασπάται επί του L_2. Επιπλέον, το πολυώνυμο $\sigma_*(m)$ είναι ανάγωγο στο K_2 εφόσον ο ισομορφισμός σ επάγει ισομορφισμό μεταξύ των δακτυλίων πολυωνύμων $K_1[x]$ και $K_2[x]$ και άρα ανάγωγοι παράγοντες του $K_1[x]$ απεικονίζονται σε ανάγωγους παράγοντες του $K_2[x]$ (Λήμμα 7.2).

Επιλέγω β μια ρίζα του $\sigma_*(m)$. Ορίζω $\phi : K_1(\alpha) \to K_2(\beta)$ με $\phi(g(a)) = \sigma_*(g)(\beta)$. Παρατηρήστε ότι $\phi|_{K_1} = \sigma$ και $\phi(\alpha) = \beta$. Θα δείξουμε πρώτα ότι η ϕ είναι καλά ορισμένη. Έστω $g, h \in K_1[x]$ με $g(\alpha) = h(\alpha)$. Τότε $(g - h)(\alpha) = 0$ και άρα το m διαιρεί το $g - h$ εφόσον το m είναι το ελάχιστο πολυώνυμο του α. Όμως τότε $\sigma_*(m)$ διαιρεί το $\sigma_*(g - h)$ και άρα $\sigma_*(g - h)(\beta) = 0$, δηλαδή $\sigma_*(g)(\beta) = \sigma_*(h)(\beta)$ συνεπώς $\phi(g(\alpha)) = \phi(h(\alpha))$. Άρα η ϕ καλά ορισμένη. Εύκολα βλέπουμε ότι η ϕ είναι ισομορφισμός που επεκτείνει την σ.

Έστω τώρα L_1 και L_2 τα σώματα διάσπασης των πολυωνύμων f και $\sigma_*(f)$ επί των $K_1(\alpha)$ και $K_2(\beta)$ αντίστοιχα. Τότε $[L_1 : K_1(\alpha)] < [L_1 : K_1]$. Άρα από την επαγωγική υπόθεση υπάρχει $\tau : L_1 \to L_2$ που επεκτείνει τον $\phi : K_1(\alpha) \to K_2(\beta)$. Άρα ο τ είναι η ζητούμενη επέκταση.

Το παρακάτω μεταθετικό διάγραμμα περιγράφει την επαγωγική κατασκευή της τ.



□

ΠΟΡΙΣΜΑ 7.1. Έστω $L : K$ να είναι διασπαστική επέκταση και $\alpha, \beta \in L$. Τότε υπάρχει $K-$αυτομορφισμός του L που στέλνει το α στο β αν και μόνο αν τα α και β έχουν το ίδιο ελάχιστο πολυώνυμο επί του K.

Απόδειξη. Εφόσον η $L : K$ είναι διασπαστική επέκταση θα υπάρχει πολυώνυμο f ώστε το L είναι το σώμα διάσπασης του f. Άρα υπάρχουν $\alpha_1, \alpha_2, \ldots, \alpha_n \in L$, ώστε

$$f(x) = c(x - \alpha_1)^{m_1}(x - \alpha_2)^{m_2} \cdots (x - \alpha_n)^{m_n}$$

και συνεπώς $L = K(\alpha_1, \alpha_2, \ldots, \alpha_n)$.
($\Longrightarrow$) Έστω $\alpha, \beta \in L$, υποθέτουμε ότι υπάρχει $K-$αυτομορφισμός $\sigma : L \longrightarrow L$ με $\sigma(\alpha) = \beta$. Έστω m_α να είναι το ελάχιστο πολυώνυμο του α και m_β να είναι το ελάχιστο πολυώνυμο του β. Αν

$$m_\alpha = c_0 + c_1 x + c_2 x^2 + \cdots + c_n x^n \qquad c_0, c_1, \ldots, c_n \in K,$$

τότε

$$\sigma\big(m_\alpha(\alpha)\big) = \sigma(c_0 + c_1\alpha + c_2\alpha^2 + \cdots + c_n\alpha^n)$$

όμως ο σ είναι $K-$αυτομορφισμός, άρα

$$\begin{aligned}
\sigma(c_0 + c_1\alpha + c_2\alpha^2 + \cdots + c_n\alpha^n) &= \sigma(c_0) + \sigma(c_1)\sigma(a) + \sigma(c_2)\sigma(a^2) + \cdots + \sigma(c_n)\sigma(a^n) \\
&= c_0 + c_1\sigma(a) + c_2\big(\sigma(a)\big)^2 + \cdots + c_n\big(\sigma(a)\big)^n \\
&= c_0 + c_1\beta + c_2\beta^2 + \cdots + c_n\beta^n \\
&= m_\alpha(\beta).
\end{aligned}$$

Επίσης

$$\sigma\big(m_\alpha(\alpha)\big) = \sigma(0) = 0,$$

άρα

$$m_\alpha(\beta) = \sigma\big(m_\alpha(\alpha)\big) = 0$$

Επομένως,

$$m_\beta = q m_\alpha + r \quad \text{όπου} \quad r = 0 \quad \text{ή} \quad \deg r < \deg m_\alpha.$$

Όμως $m_\alpha(\alpha) = m_\beta(\alpha) = 0$ συνεπώς $r = 0$ διαφορετικά το α είναι ρίζα ενός πολυωνύμου βαθμού μικρότερου του $\deg m_\alpha$ άτοπο μιας και το m_α είναι το ελάχιστο πολυώνυμο του α. Άρα $m_\beta \mid m_\alpha$. Παρόμοια και $m_\alpha \mid m_\beta$, άρα $m_\alpha = m_\beta$.

($\Longleftarrow$) Ας υποθέσουμε ότι τα α, β είναι στοιχεία του L με το ίδιο ελάχιστο πολυώνυμο m επί του K. Ορίζουμε $\phi : K(\alpha) \to K(\beta)$ με $\phi(h(\alpha)) = h(\beta)$ για κάθε πολυώνυμο $h \in K[x]$. Προφανώς, αν $h_1, h_2 \in K[x]$ τότε $h_1(\alpha) = h_2(\alpha)$ αν και μόνο αν το $h_1 - h_2$ διαιρείται από το m αν και μόνο αν $h_1(\beta) = h_2(\beta)$. Άρα η ϕ είναι καλά ορισμένη. Εύκολα βλέπουμε ότι είναι ένα K ισομορφισμός και $\phi(\alpha) = \beta$.

Αν τώρα L είναι το σώμα διάσπασης επί του K κάποιου πολυωνύμου $f \in K[x]$ τότε το L είναι και σώμα διάσπασης του f επί του $K(\alpha)$ και του $K(\beta)$. Άρα από το Θεώρημα 7.3 ο $K-$ισομορφισμός ϕ επεκτείνεται σε $K-$αυτομορφισμό από του L που στέλνει το α στο β. □

ΠΑΡΑΔΕΙΓΜΑ 7.2. 1. Έστω $f(x) = (x^2 - 3)(x^3 + 1) \in \mathbb{Q}[x]$. Ποιο είναι το σώμα διάσπασης του f επί του $\mathbb{Q}$; Παρατηρώ ότι το f διασπάται στο $\mathbb{Q}$ μιας και το -1 είναι ρίζα του $x^3 + 1$. Άρα

Άρα

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

λύνω

$$x^2 - x + 1 = 0 \iff x_{1,2} = \frac{1 \pm i\sqrt{3}}{2}.$$

Άρα οι ρίζες του f στο $\mathbb{C}$ είναι οι $\pm 3, -1, \frac{1\pm i\sqrt{3}}{2}$. Άρα το σώμα διάσπασης του f είναι το

$$\mathbb{Q}\Big(\sqrt{3}, \frac{1 + i\sqrt{3}}{2}\Big) = \mathbb{Q}\big(\sqrt{3}, i\big).$$

2. Έστω $f(x) = (x^2 - 2x - 2)(x^2 + 1) \in \mathbb{Q}[x]$. Οι ρίζες του f στο $\mathbb{C}$ είναι οι $\pm i, 1 \pm \sqrt{3}$. Άρα το σώμα διάσπασης του f είναι το

$$\mathbb{Q}(i, 1 + \sqrt{3}) = \mathbb{Q}\big(\sqrt{3}, i\big).$$

ΠΑΡΑΤΗΡΗΣΗ 7.1. Από τα παραδείγματα 2 και 3 συμπεραίνουμε ότι δύο διαφορετικά πολυώνυμα μπορούν να έχουν το ίδιο σώμα διάσπασης.

3. Έστω $f(x) = x^2 + x + 1 \in \mathbb{Z}_2[x]$. Ποιο το σώμα διάσπασης του f; Θα βρούμε το σώμα διάσπασης του f με τη μέθοδο του Kronecker. Φανερά το f είναι ανάγωγο επί του $\mathbb{Z}_2[x]$. Έστω $I = \langle f \rangle$ να είναι το ιδεώδες που παράγεται από το f. Τότε θεωρούμε το σώμα

$$F = \mathbb{Z}_2[x]/\langle f \rangle = \{(\alpha x + \beta) + I \mid \alpha, \beta \in \mathbb{Z}_2\}.$$

Αν ονομάσουμε j το $x + I$ βλέπουμε ότι το F αποτελείται από 4 στοιχεία το οποία συμβολίζουμε με $F = \{0, 1, j, j + 1\}$, όπου

$$\begin{aligned} 0 &= 0 + I \\ 1 &= 1 + I \\ j &= x + I \\ j + 1 &= x + 1 + I. \end{aligned}$$

Το j είναι ρίζα του f στο F. Πράγματι, $f(j) = j^2 + j + 1 = x^2 + x + 1 + I = I$. Επίσης επειδή κάθε στοιχείο του F έχει τάξη 2 (εκτός από το 0), συμπεραίνουμε ότι

$$(F, +) \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \quad \text{και} \quad (F\backslash\{0\}, \cdot) \cong \mathbb{Z}_3.$$

Συνεπώς το σώμα διάσπασης του f είναι το $F = \mathbb{Z}_2(j)$. Ας δούμε τώρα και πως διασπάται το f στο $\mathbb{Z}_2(j)$. Διαιρούμε το f με το $x - j$.

$$\begin{array}{r|l} x^2 + x + 1 & x - j \\ \cline{2-2} -x^2 + jx & x + (j + 1) \\ \hline (j + 1)x + 1 & \\ -(j + 1)x - (j^2 + j) & \\ \hline -j^2 - j + 1 = j^2 + j + 1 = 0 & \end{array}$$

Άρα το f διασπάται ως εξής

$$f(x) = (x - j)(x + j + 1).$$