ΘΕΩΡΙΑ ΔΑΚΤΥΛΙΩΝ

Σημειώσεις προπτυχιακοῦ μαθήματος [1]

Ν.Γ. Τζανάκης

Τμῆμα Μαθηματικῶν

Πανεπιστήμιο Κρήτης - Ἡράκλειο

[1]Τελευταία ἔκδοση 15-6-2014

Περιεχόμενα

Κεφάλαιο 1

Διαιρετότητα

Στὸ παρὸν κεφάλαιο, το D συμβολίζει πάντα ἀκέραια περιοχή. Μὲ $Q(D)$ συμβολίζομε τὸ *σῶμα πηλίκων* τῆς D.

I.I Τα βασικα

Ὁρισμός. (α′) Τὸ μὴ μηδενικὸ $\epsilon \in D$ λέγεται *μονάδα* τῆς D, ἂν εἶναι *ἀντιστρέψιμο* στοιχεῖο τοῦ D, δηλαδή, ἂν καὶ μόνο ἂν τὸ ϵ^{-1}, τὸ ὁποῖο βεβαίως ἀνήκει στὸ $Q(D)$, εἶναι στοιχεῖο τῆς D. Τὸ $1 \in D$ εἶναι μονάδα, ἀλλά, συγχρόνως, εἶναι καὶ *τὸ* (μοναδικὸ) μοναδιαῖο στοιχεῖο τῆς D.

Τὸ σύνολο τῶν μονάδων τῆς D συμβολίζεται D^*.

(β′) Τὰ μὴ μηδενικὰ στοιχεῖα a, b χαρακτηρίζονται *συνεταιρικά*, ἂν $b = \epsilon a$ μὲ $\epsilon \in D^*$. Ἡ σχέση συνεταιρικότητας εἶναι, προφανῶς, σχέση ἰσοδυναμίας.
(γ′) Ἂν $a, b \in D$ καὶ $b \neq 0$ καὶ ὑπάρχει $\gamma \in D$, τέτοιο ὥστε $a = b\gamma$, τότε λέμε ὅτι *τὸ b διαιρεῖ τὸ a*· συμβολικά, $b|a$. Ισοδύναμες διατυπώσεις:

- Τὸ *a διαιρεῖται*, ἢ *εἶναι διαιρετὸ* ἀπὸ τὸ (διὰ τοῦ) b.
- Τὸ b εἶναι *διαιρέτης* τοῦ a.
- Τὸ a εἶναι *πολλαπλάσιο* τοῦ b.

Εὔκολα βλέπει κανεὶς ὅτι οἱ μονάδες καὶ τὰ συνεταιρικὰ στοιχεῖα τοῦ a εἶναι διαιρέτες τοῦ a, τοὺς ὁποίους χαρακτηρίζομε *τετριμμένους διαιρέτες* τοῦ a. Οἱ μὴ τετριμμένοι διαιρέτες τοῦ a χαρακτηρίζονται *γνήσιοι διαιρέτες* τοῦ a.
Ὅταν γράφομε $b \nmid a$ ἐννοοῦμε ὅτι ὁ b δὲν διαιρεῖ τὸν a.
(δ′) Τὸ μὴ μηδενικὸ στοιχεῖο p χαρακτηρίζεται *ἀνάγωγο στοιχεῖο* τῆς D ἂν δὲν εἶναι μονάδα καὶ οἱ μόνοι διαιρέτες τοῦ p εἶναι οἱ τετριμμένοι.
(ε′) Τὸ μὴ μηδενικὸ στοιχεῖο π χαρακτηρίζεται *πρῶτο στοιχεῖο* τῆς D ἂν δὲν εἶναι μονάδα καί, ἐπιπλέον, ἔχει τὴν ἑξῆς ἰδιότητα: Κάθε σχέση τῆς μορφῆς $\pi|a\beta$, μὲ $a, b \in D$, συνεπάγεται ὅτι τὸ π διαιρεῖ τοὐλάχιστον ἕνα ἀπὸ τὰ a, b.

Ἄσκηση 1.1 Στὴν εἰδικὴ περίπτωση ποὺ ἡ ἀκέραια περιοχὴ D εἶναι σῶμα, ἀποδεῖξτε ὅτι κάθε μὴ μηδενικὸ στοιχεῖο εἶναι μονάδα, καθὼς καὶ ὅτι κάθε μὴ μηδενικὸ στοιχεῖο διαιρεῖ ὁποιοδήποτε στοιχεῖο τῆς D.

Ἡ ἄσκηση 1.1 μᾶς λέει ὅτι ἡ διαιρετότητα σὲ σῶμα εἶναι τετριμμένη, δίχως οὐσιαστικὸ ἐνδιαφέρον. Ἄρα, ὅ,τιδήποτε ἀποδειχθεῖ σ' αὐτὸ τὸ κεφάλαιο ἔχει οὐσιαστικὸ νόημα στὶς περιπτώσεις ἀκεραίων περιοχῶν, οἱ ὁποῖες *δὲν* εἶναι σώματα.

Ἄσκηση 1.2 Ἂν $b, a_1, \ldots, a_n \in D$ καὶ $b|a_i$ γιὰ κάθε $i = 1, \ldots, n$, τότε, ὁποιαδήποτε κι ἂν εἶναι τὰ $t_1, \ldots, t_n \in D$, τὸ b διαιρεῖ τὸ $t_1a_1 + \cdots + t_na_n$.

Ἄσκηση 1.3 Ἔστω ὅτι $\epsilon, p \in D$ εἶναι μονάδα καὶ ἀνάγωγο στοιχεῖο, ἀντιστοίχως. Ἀποδεῖξτε ὅτι τὸ ϵp εἶναι ἀνάγωγο στοιχεῖο.

Ἄσκηση 1.4 Ἡ σχέση διαιρετότητας $a|b$ δὲν ἐπηρεάζεται ἂν κάποιο (ἢ καὶ τὰ δύο) ἀπὸ τὰ a, b ἀντικατασταθεῖ ἀπὸ συνεταιρικό του στοιχεῖο.

Ἄσκηση 1.5 Ἔστω ὅτι a, b εἶναι μη μηδενικὰ στοιχεῖα, τέτοια ὥστε $a|b$ καὶ $b|a$. Τότε τὰ a, b εἶναι συνεταιρικά.

Ἄσκηση 1.6 Ἀποδεῖξτε ὅτι καθ' ἕνα ἀπὸ τὰ σύνολα D^* καὶ $D \setminus D^*$ εἶναι κλειστὸ ὡς πρὸς τὸν πολλαπλασιασμό.

Πρόταση 1.1 *Κάθε πρῶτο στοιχεῖο τῆς D εἶναι ἀνάγωγο. Τὸ ἀντίστροφο δὲν ἰσχύει ἐν γένει.*

Ἀπόδειξη. Ἔστω p πρῶτο στοιχεῖο τῆς D καὶ ἂς ὑποθέσομε ὅτι δὲν εἶναι ἀνάγωγο. Αὐτὸ σημαίνει ὅτι τὸ p ἔχει μὴ τετριμμένους διαιρέτες καὶ ἔστω a ἕνας ἀπ' αὐτούς, ὁπότε μπορούμε νὰ γράψομε $p = ab$ γιὰ κάποιο $b \in D$. Ἀλλὰ $p|p$, ἄρα $p|ab$, ὁπότε τὸ (ε′) τοῦ ὁρισμοῦ συνεπάγεται ὅτι τὸ p διαιρεῖ ἕνα τοὐλάχιστον ἀπ' τὰ a, b.
Ἂν $p|a$, τότε $a = pc$ γιὰ κάποιο $c \in D$, ἄρα $a = pc = (ab)c = a(bc)$, ὁπότε $1 = bc$ (ἐπιτρέπεται ἡ ἁπλοποίηση λόγῳ ἀκέραιας περιοχῆς). Ἡ τελευταία σχέση δηλώνει ὅτι τὸ b εἶναι μονάδα τῆς D καὶ τότε, λόγῳ τῆς $p = ab$, συμπεραίνομε ὅτι τὸ a εἶναι συνεταιρικὸ στοιχεῖο τοῦ p.
Ἂν $p|b$, τότε $b = pc$ γιὰ κάποιο $c \in D$, ἄρα $b = pc = (ab)c = b(ac)$, ὁπότε $1 = ac$. Ἡ τελευταία σχέση δηλώνει ὅτι τὸ a εἶναι μονάδα τῆς D.
Ἄρα, ἡ ὑπόθεση ὅτι ὁ a εἶναι διαιρέτης τοῦ p μᾶς ὁδήγησε στὸ συμπέρασμα ὅτι, εἴτε τὸ a εἶναι συνεταιρικὸ μὲ τὸ p, εἴτε τὸ a εἶναι μονάδα. Ἄρα τὸ p ἔχει μόνο τετριμμένους διαιρέτες, δηλαδή, εἶναι πρῶτο στοιχεῖο.

Γιὰ τὸ ὅτι δὲν ἰσχύει τὸ ἀντίστροφο ἐν γένει, βλ. παράδειγμα (ε′), παρακάτω.

□

Παραδείγματα. **(α′)** Οἱ μόνες μονάδες τοῦ $\mathbb{Z}$ εἶναι τὰ ± 1. Τὰ ἀνάγωγα στοιχεῖα τοῦ $\mathbb{Z}$ εἶναι, προφανῶς, οἱ πρῶτοι ἀριθμοὶ καὶ οἱ ἀντίθετοί τους. Ἐπιπλέον, τὰ πρῶτα στοιχεῖα τοῦ $\mathbb{Z}$ (ὑπὸ τὴν ἔννοιαν τοῦ γενικοῦ ὁρισμοῦ, ποὺ δώσαμε στὴν ἀρχὴ τοῦ κεφαλαίου) ταυτίζονται μὲ τοὺς πρώτους ἀριθμοὺς καὶ τοὺς ἀντίθετούς τους. Πράγματι, ξέρομε ἀπ' τὴ στοιχειώδη Θεωρία Ἀριθμῶν ὅτι, ἂν ὁ p εἶναι πρῶτος καὶ $p|ab$, ὅπου $a, b \in \mathbb{Z}$, τότε ὁ p διαιρεῖ ἕναν τοὐλάχιστον ἐκ τῶν a καὶ b, δηλαδή, ὁ p εἶναι πρῶτο στοιχεῖο τῆς ἀκέραιας περιοχῆς $\mathbb{Z}$. Ἐπιπλέον, οὐδεὶς μὴ πρῶτος ἀκέραιος $m \neq \pm 1$ μπορεῖ νὰ εἶναι πρῶτο στοιχεῖο, διότι, ἂν $m = ab$, μὲ τοὺς a, b ἀκεραίους διάφορους τῶν ± 1 (ὁπότε $1 < |a|, |b| < |m|$), τότε $m|ab$, ἐνῶ ὁ m δὲν διαιρεῖ οὔτε τὸν a οὔτε τὸν b.
Συμπέρασμα: Στὴν ἀκέραια περιοχὴ $\mathbb{Z}$, πρῶτα καὶ ἀνάγωγα στοιχεῖα ταυτίζονται καὶ τὸ σύνολό τους εἶναι τὸ σύνολο τῶν πρώτων ἀριθμῶν καὶ τῶν ἀντιθέτων τους.

(β′) Ἔστω σῶμα K. Ἀπὸ τὸ εἰσαγωγικὸ μάθημα τῆς Ἄλγεβρας ξέρομε ὅτι ὁ δακτύλιος πολυωνύμων $K[X]$ εἶναι ἀκέραια περιοχή, οἱ μοναδικὲς μονάδες τοῦ ὁποίου εἶναι τὰ μὴ μηδενικὰ σταθερὰ πολυώνυμα, δηλαδή, τὰ μὴ μηδενικὰ στοιχεῖα τοῦ K. Τὰ ἀνάγωγα στοιχεῖα τῆς ἀκέραιας περιοχῆς $K[X]$ εἶναι, ἀκριβῶς, τὰ ἀνάγωγα πάνω ἀπ' τὸ K πολυώνυμα. Ἀξίζει νὰ σημειωθεῖ ὅτι κάθε ἀνάγωγο πολυώνυμο πάνω ἀπ' τὸ K εἶναι πρῶτο στοιχεῖο τῆς ἀκέραιας περιοχῆς $K[X]$. Πράγματι, ἀπ' τὸ εἰσαγωγικὸ μάθημα τῆς Ἄλγεβρας ξέρομε ὅτι, ἂν τὸ $p(X) \in K[X]$ εἶναι ἀνάγωγο καὶ διαιρεῖ τὸ γινόμενο δύο πολυωνύμων τοῦ $K[X]$, τότε, ὑποχρεωτικά, τὸ $p(X)$ διαιρεῖ ἕνα, τοὐλάχιστον, ἀπὸ τὰ δύο αὐτὰ πολυώνυμα. Ἄρα, τὰ ἀνάγωγα πολυώνυμα τοῦ $K[X]$ εἶναι πρῶτα στοιχεῖα τῆς ἀκέραιας περιοχῆς $K[X]$. Ἐπιπλέον, κάθε μὴ σταθερό, μὴ ἀνάγωγο πολυώνυμο $f(X) \in K[X]$ δὲν εἶναι πρῶτο. Διότι, ἂν $f(X) = g(X)h(X)$, μὲ τὰ $g(X), h(X)$ πολυώνυμα τοῦ $K[X]$ βαθμοῦ $< \deg f(X)$, τότε $f(X)|g(X)h(X)$, ἐνῶ τὸ $f(X)$ δὲν διαιρεῖ οὔτε τὸ $g(X)$, οὔτε τὸ $h(X)$.
Συμπέρασμα: Στὴν ἀκέραια περιοχὴ $K[X]$ (K σῶμα), ἀνάγωγα καὶ πρῶτα στοιχεῖα ταυτίζονται καὶ τὸ σύνολό τους εἶναι τὸ σύνολο τῶν ἀναγώγων πολυωνύμων τοῦ $K[X]$.

(γ′) Ἔστω θετικὸς ἀκέραιος d, ὄχι τέλειο τετράγωνο, καὶ ἡ ἀκέραια περιοχὴ

$$\mathbb{Z}[\sqrt{d}] = \{x + y\sqrt{d} : x, y \in \mathbb{Z}\}.$$

Θὰ προσδιορίσομε τὶς μονάδες τῆς $\mathbb{Z}[\sqrt{d}]$. Ἔστω $\epsilon = x + y\sqrt{d}$ ἕνα μὴ μηδενικὸ στοιχεῖο τῆς $\mathbb{Z}[\sqrt{d}]$. Τότε, $x - y\sqrt{d} \neq 0$. Πράγματι, στὴν ἀντίθετη περίπτωση θὰ εἴχαμε $x = y\sqrt{d}$, ὁπότε, $y \neq 0$ καὶ $\sqrt{d} = x/y$, ἄρα $d = (x/y)^2$, ποὺ ἔρχεται σὲ ἀντίφαση μὲ τὴν ὑπόθεση γιὰ τὸ d. Τώρα μποροῦμε, ἐπίσης, νὰ συμπεράνομε ὅτι $x^2 - dy^2 = (x + y\sqrt{d})(x - y\sqrt{d}) \neq 0$.

Τὸ ϵ εἶναι μονάδα, ἂν καὶ μόνο ἂν $\epsilon^{-1} \in \mathbb{Z}[\sqrt{d}]$.

$$\epsilon^{-1} = \frac{1}{x + y\sqrt{d}} = \frac{x - y\sqrt{d}}{x^2 - dy^2},$$

συνεπῶς, $\epsilon^{-1} \in \mathbb{Z}[\sqrt{d}]$ ἂν καὶ μόνο ἂν οἱ ρητοὶ ἀριθμοὶ $x/(x^2 - dy^2)$ καὶ $y/(x^2 - dy^2)$ εἶναι ἀκέραιοι. Ἂν οἱ ἀριθμοὶ αὐτοὶ εἶναι ἀκέραιοι, τότε καὶ τὰ τετράγωνά τους εἶναι ἀκέραιοι, ὁπότε ἀκέραιος εἶναι καὶ ὁ ἀριθμὸς

$$\left(\frac{x}{x^2 - dy^2}\right)^2 - d\left(\frac{y}{x^2 - dy^2}\right)^2 = \frac{1}{x^2 - dy^2},$$

ποὺ σημαίνει ὅτι $x^2 - dy^2 = \pm 1$. Τὸ ἀντίστροφο ἰσχύει προφανώς: Ἂν $x^2 - dy^2 = \pm 1$, οἱ ἀριθμοὶ $x/(x^2 - dy^2)$ καὶ $y/(x^2 - dy^2)$ εἶναι ἀκέραιοι. Συμπέρασμα:

> Τὸ $\epsilon = x + y\sqrt{d}$ εἶναι μονάδα, ἂν καὶ μόνο ἂν (x, y) εἶναι ἀκέραια λύση (u, v) τῆς ἐξίσωσης
> $$u^2 - dv^2 = \pm 1. \tag{1.1}$$

Ἡ (1.1) λέγεται ἐξίσωση τοῦ Pell καὶ γι' αὐτὴν ἰσχύουν τὰ ἑξῆς:

• Μὲ τὸ $+1$ στὸ δεξιὸ μέλος, ἡ ἐξίσωση (1.1) ἔχει πάντοτε λύση· ἡ λύση μὲ τὸ ἐλάχιστο θετικὸ u, ἄρα καὶ μὲ τὸ ἐλάχιστο θετικὸ v, χαρακτηρίζεται *θεμελιώδης λύση* καὶ συμβολίζεται (u_1, v_1).[1] Εἶναι γνωστὸ ἀπ' τὴ Θεωρία Ἀριθμῶν ὅτι ὅλες οἱ λύσεις τῆς (1.1) μὲ $+1$ στὸ δεξιὸ μέλος, εἶναι οἱ (u_n, v_n), ὅπου

$$u_n + v_n\sqrt{d} = \pm(u_1 + v_1\sqrt{d})^n, \quad n \in \mathbb{Z}. \tag{1.2}$$

[1] Ἡ θεμελιώδης λύση, γιὰ κάποιες τιμὲς τοῦ d νὰ εἶναι ἐντυπωσιακὰ μεγάλη! Λ.χ. γιὰ $d = 1141$, εἶναι $u_1 = 1036782394157223963237125215$ καὶ $v_1 = 30693385322765657197397208$.

Παρατηρῆστε ὅτι $(u_1 + v_1\sqrt{d})^{-k} = (u_1 - v_1\sqrt{d})^k$.

• Μὲ τὸ -1 στὸ δεξιὸ μέλος, ἡ ἐξίσωση (1.1) δὲν ἔχει πάντοτε λύση· στὴν περίπτωση που ἔχει, ἡ λύση μὲ τὸ ἐλάχιστο θετικὸ u (ἄρα καὶ τὸ ἐλάχιστο θετικὸ v) χαρακτηρίζεται θεμελιώδης καὶ συμβολίζεται μὲ (u'_1, v'_1). Ἀπὸ τὴ Θεωρία Ἀριθμῶν εἶναι γνωστὸ ὅτι ὅλες οἱ λύσεις τῆς (1.1) μὲ -1 στὸ δεξιὸ μέλος, εἶναι οἱ (u'_{2k+1}, v'_{2k+1}), ἐνῶ ὅλες οἱ λύσεις τῆς (1.1) μὲ $+1$ στὸ δεξιὸ μέλος, εἶναι οἱ (u'_{2k}, v'_{2k}), ὅπου, καὶ στὶς δύο περιπτώσεις,

$$u'_n + v'_n\sqrt{d} = \pm(u'_1 + v'_1\sqrt{d})^n, \quad n \in \mathbb{Z}. \tag{1.3}$$

Ειδικώτερα, αὐτὸ μας λέει ότι, στὴν περίπτωση ποὺ ἡ ἐξίσωση (1.1), μὲ -1 στὸ δεξιὸ μέλος, ἔχει λύση, οἱ λύσεις της (u'_n, v'_n) συνδέονται μὲ τὶς λύσεις (u_n, v_n) τῆς ἐξίσωσης (1.1), μὲ $+1$ στὸ δεξιὸ μέλος, μέσῳ τῆς σχέσεως $(u_n, v_n) = (u'_{2n}, v'_{2n})$.

(δ′) Θεωροῦμε τὴν ἀκέραια περιοχὴ $\mathbb{Z}[\sqrt{d}]$ ὅπως στὸ (γ′) γιὰ ἀρνητικὸ ἀκέραιο d. Ἀκριβῶς ὅπως στὸ (γ′) καταλήγομε στὸ συμπέρασμα ὅτι τὸ $\epsilon = x + y\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$ εἶναι μονάδα, ἂν καὶ μόνο ἂν $x^2 - dy^2 = 1$. Τώρα, ὅμως, οἱ ἀριθμοὶ x^2 καὶ $-dy^2$ εἶναι *θετικοὶ* ἀκέραιοι καί, μάλιστα, $-dy^2 \geq 2$, ἂν $d \leq -2$ καὶ $y \neq 0$. Ἀναγκαστικά, λοιπόν, σ' αὐτὴ τὴν περίπτωση, $y = 0$ καὶ $x = \pm 1$. Ἂν $d = -1$, τότε βλέπομε ὅτι ἡ $x^2 - dy^2 = 1$ γίνεται $x^2 + y^2 = 1$ καί, συνεπῶς, οἱ μοναδικὲς λύσεις εἶναι οἱ $(x, y) = (\pm 1, 0), (0, \pm 1)$.

Συμπέρασμα: Οἱ μοναδικὲς μονάδες τῆς ἀκέραιας περιοχῆς $\mathbb{Z}[\sqrt{d}]$ εἶναι οἱ ± 1, ἂν $d \leq -2$, καὶ οἱ $\pm 1, \pm\sqrt{-1}$, ἂν $d = -1$.

(ε′) Ἔστω ἡ ἀκέραια περιοχὴ $D = \mathbb{Z}[\sqrt{-5}]$. Σκοπὸς τοῦ παραδείγματος αὐτοῦ εἶναι νὰ καταδείξει ὅτι, στὴ D, τὸ 2 εἶναι ἀνάγωγο στοιχεῖο, ἀλλὰ δὲν εἶναι πρῶτο. Κατ' ἀρχάς, παρατηροῦμε ὅτι, σύμφωνα μὲ τὸ (δ′), οἱ μόνες μονάδες τῆς D εἶναι ± 1.

Δείχνομε τώρα ὅτι τὸ 2 εἶναι ἀνάγωγο στοιχεῖο τῆς D. Πράγματι, ἔστω ὅτι $\delta = a + b\sqrt{-5} \in D$ εἶναι διαιρέτης τοῦ 2, ὁπότε ὑπάρχει $c + d\sqrt{-5} \in D$ ἔτσι ὥστε $2 = (a + b\sqrt{-5})(c + d\sqrt{-5})$. Ἂν δοῦμε αὐτὴ τὴ σχέση ὡς ἰσότητα στοὺς μιγαδικοὺς ἀριθμούς, τότε μποροῦμε νὰ ἔχομε καὶ τὴ συζυγῆ της σχέση, δηλαδή, τὴν $2 = (a - b\sqrt{-5})(c - d\sqrt{-5})$. Πολλαπλασιάζοντας κατὰ μέλη τὶς δύο σχέσεις παίρνομε $4 = (a^2 + 5b^2)(c^2 + 5d^2)$. Οἱ παράγοντες τοῦ δεξιοῦ μέλους εἶναι θετικοὶ ἀκέραιοι, ποὺ τὸ γινόμενό τους εἶναι 4. Ἄρα, $a^2 + 5b^2 = 1$, ἢ 2, ἢ 4. Τὸ δεύτερο ἐνδεχόμενο προφανῶς ἀποκλείεται. Τὸ πρῶτο ἐνδεχόμενο μπορεῖ νὰ συμβεῖ μόνον ἂν $b = 0$ καὶ $a = \pm 1$, ποὺ σημαίνει ὅτι $\delta = \pm 1$, μονάδα. Τὸ τρίτο ἐνδεχόμενο συνεπάγεται ὅτι $c^2 + 5d^2 = 1$, ἄρα, $d = 0$ καὶ $c = \pm 1$. Ἀλλὰ τότε, $2 = \pm(a + b\sqrt{-5})$, ποὺ συνεπάγεται $b = 0$ καὶ $a = \pm 2$, δηλαδή, $\delta = \pm 2$. Συνεπῶς, οἱ μόνοι διαιρέτες τοῦ 2 εἶναι οἱ μονάδες καὶ τὰ συνεταιρικὰ τοῦ 2 καί, ἐξ ὁρισμοῦ, αὐτὸ σημαίνει ὅτι τὸ 2 εἶναι ἀνάγωγο.

Τώρα θὰ δείξομε ὅτι τὸ 2 δὲν εἶναι πρῶτο. Πράγματι, ξεκινοῦμε ἀπ' τὴν παρατήρηση ὅτι τὸ 2 διαιρεῖ τὸ γινόμενο $(1 + \sqrt{-5})(1 - \sqrt{-5})$, διότι τὸ γινόμενο αὐτὸ ἰσοῦται μὲ 6. Ἂν τὸ 2 ἦταν πρῶτο στοιχεῖο, θὰ ἔπρεπε νὰ διαιρεῖ ἕναν ἀπὸ τοὺς παράγοντες τοῦ γινομένου. Ἔστω π.χ. ὅτι $2|1 + \sqrt{-5}$. Αὐτὸ σημαίνει ὅτι ὑπάρχει $a + b\sqrt{-5} \in D$ τέτοιο ὥστε $1 + \sqrt{-5} = 2(a + b\sqrt{-5})$. Βλέποντας τὴν τελευταία σχέση ὡς ἰσότητα μιγαδικῶν, συμπεραίνομε ὅτι $1 = 2a$ καὶ $1 = 2b$, ἄτοπο, ἀφοῦ οἱ a, b εἶναι ἀκέραιοι.

Ἄσκηση 1.7 Ἐργαστεῖτε ὅπως στὸ προηγούμενο παράδειγμα (ε′) καὶ ἀποδεῖξτε ὅτι τὰ στοιχεῖα 3 καὶ $1 \pm \sqrt{-5}$ τῆς ἀκέραιας περιοχῆς $D = \mathbb{Z}[\sqrt{-5}]$ εἶναι ἀνάγωγα.

Ἄσκηση 1.8 Ἔστω ἀκέραια περιοχὴ D καὶ p ἀνάγωγο στοιχεῖο της. Ἀποδεῖξτε ὅτι τὸ p εἶναι ἀνάγωγο στοιχεῖο καὶ τῆς περιοχῆς $D[X]$.

Ὁρισμός. Μία ἀκέραια περιοχὴ D χαρακτηρίζεται *περιοχὴ ἀνάλυσης* (σὲ ἀνάγωγα στοιχεῖα) ἂν κάθε μὴ μηδενικὸ στοιχεῖο της, ποὺ δὲν εἶναι μονάδα, μπορεῖ νὰ γραφεῖ ὡς γινόμενο πεπερασμένου πλήθους ἀναγώγων στοιχείων τῆς D. Ἡ περιοχὴ ἀνάλυσης D λέγεται *περιοχὴ μονοσήμαντης ἀνάλυσης*, ἂν ἡ προαναφερθεῖσα ἀνάλυση μπορεῖ νὰ γίνει, "οὐσιαστικὰ" μὲ ἕνα μόνο τρόπο. Τὸ ἐπίρρημα "οὐσιαστικὰ" λέγεται ἐδῶ ὑπὸ τὴν ἑξῆς ἔννοια: Ἂν τὸ μὴ μηδενικὸ στοιχεῖο a δὲν εἶναι μονάδα καὶ $a = p_1 \cdots p_n$, $a = q_1 \cdots q_m$ εἶναι δύο ἀναλύσεις τοῦ a σὲ ἀνάγωγα στοιχεῖα τῆς D, τότε, ὑποχρεωτικά, $n = m$ καὶ ὑπάρχει μιὰ μετάθεση $\begin{pmatrix} 1 & 2 & \dots & n \\ i_1 & i_2 & \dots & i_n \end{pmatrix}$, τέτοια ὥστε τὸ q_1 νὰ εἶναι συνεταιρικὸ μὲ τὸ p_{i_1}, τὸ q_2 νὰ εἶναι συνεταιρικὸ μὲ τὸ p_{i_2}, ..., τὸ q_n νὰ εἶναι συνεταιρικὸ μὲ τὸ p_{i_n}.

Ἄσκηση 1.9 Ἔστω ἡ ἀκέραια περιοχὴ $\mathbb{Z}[\sqrt{-5}]$ τοῦ παραδείγματος (ε′), πιὸ πάνω.
(α′) Ν' ἀποδειχθεῖ ὅτι $D^* = \{-1, 1\}$.
(β′) Ν' ἀποδειχθεῖ ὅτι ἡ D εἶναι περιοχὴ ἀνάλυσης.
(γ′) Σύμφωνα μὲ τὸ παράδειγμα (ε′) καὶ τὴν ἄσκηση 1.7, τὰ στοιχεῖα $2, 3, 1 + \sqrt{-5}, 1 - \sqrt{-5}$ τῆς D εἶναι ἀνάγωγα. Προφανῶς, $2 \cdot 3 = (1 + \sqrt{-5}) \cdot (1 - \sqrt{-5})$. Ἀποδεῖξτε ὅτι τὸ 2 δὲν εἶναι συνεταιρικὸ μὲ κανέναν ἀπὸ τοὺς δύο παράγοντες τοῦ δεξιοῦ μέλους· ἀνάλογα καὶ γιὰ τὸ 3. Συμπεράνατε ἀπὸ αὐτὸ ὅτι ἡ D δὲν εἶναι περιοχὴ μονοσήμαντης ἀνάλυσης.

> **Σημαντικὴ παρατήρηση**. Ἀπὸ τὸ εἰσαγωγικὸ μάθημα τῆς Ἄλγεβρας ξέρομε ὅτι ὁ δακτύλιος $\mathbb{Z}$ εἶναι περιοχὴ μονοσήμαντης ἀνάλυσης, καθὼς ἐπίσης καὶ ὅτι, ἂν τὸ K εἶναι σῶμα, τότε ὁ δακτύλιος πολυωνύμων $K[X]$ εἶναι, καὶ αὐτός, περιοχὴ μονοσήμαντης ἀνάλυσης.

Τὸ γεγονὸς ὅτι, καὶ στὸ $\mathbb{Z}$ καὶ στὸ $K[X]$ ὅλα τὰ ἰδεώδη εἶναι κύρια, δηλαδή, $\mathbb{Z}$ καὶ $K[X]$ εἶναι *περιοχὲς κυρίων ἰδεωδῶν* δὲν εἶναι τυχαῖο, καθὼς θὰ δοῦμε λίγο ἀργότερα.

Πρόταση 1.2 *Ἂν ἡ D εἶναι περιοχὴ ἀνάλυσης, στὴν ὁποία κάθε ἀνάγωγο στοιχεῖο εἶναι πρῶτο, τότε ἡ D εἶναι περιοχὴ μονοσήμαντης ἀνάλυσης.*

Ἀπόδειξη. Αὐτὸ ποὺ ἀρκεῖ ν' ἀποδείξομε εἶναι τὸν ἑξῆς ἰσχυρισμό: *Ἂν ἔχομε μιὰ σχέση τῆς μορφῆς $\prod_{i=1}^{n} p_i = \prod_{i=1}^{m} q_i$, στὴν ὁποία ὅλοι οἱ παράγοντες, καὶ στὰ δύο μέλη, εἶναι ἀνάγωγα στοιχεῖα καὶ $n \leq m$, τότε $m = n$ καὶ σὲ κάθε $\nu = 1, \dots, n$ ἀντιστοιχεῖ μονοσημάντως ἕνα $i_\nu \in \{1, \dots, n\}$, ἔτσι ὥστε τὰ p_ν καὶ q_{i_ν} νὰ εἶναι συνεταιρικά.*
Ἡ ἀπόδειξη θὰ γίνει μὲ ἐπαγωγὴ στὸ n. Ἔστω $n = 1$, ὁπότε ἔχομε τὴ σχέση $p_1 = \prod_{i=1}^{m} q_i$. Τὸ p_1 εἶναι πρῶτο, ἀφοῦ ἔχει ὑποτεθεῖ ὅτι κάθε ἀνάγωγο στοιχεῖο εἶναι πρῶτο, καὶ διαιρεῖ τὸ γινόμενο τῶν $q_1, \dots, q_m$, ἄρα διαιρεῖ ἕνα ἐξ αὐτων· ἂς ποῦμε ὅτι $p_1 | q_{i_1}$, ὅπου i_1 εἶναι κάποιος δείκτης μεταξὺ 1 καὶ m. Ὅμως, καθὼς τὸ q_{i_1} εἶναι ἀνάγωγο στοιχεῖο, δὲν ἔχει διαιρέτες ἄλλους ἀπὸ τὰ συνεταιρικά του καὶ τὶς μονάδες. Τὸ p_1 δὲν εἶναι μονάδα (ἀφοῦ εἶναι ἀνάγωγο), ἄρα, ἀναγκαστικά, τὸ p_1 εἶναι συνεταιρικὸ τοῦ q_{i_1}, δηλαδή, $p_1 = \epsilon q_{i_1}$, ὅπου ϵ εἶναι μονάδα τῆς D. Ὁδηγούμαστε, λοιπόν, στὴ σχέση $\epsilon q_{i_1} = \prod_{i=1}^{m} q_i$, ὅπου, βέβαια, τὸ q_{i_1} εἶναι ἕνας ἀπ' τοὺς παράγοντες στὸ δεξιὸ μέλος, ἄρα μποροῦμε νὰ διαγράψομε τὸ q_{i_1} ἀπὸ τὰ δύο μέλη καὶ νὰ καταλήξομε στὴ σχέση $\epsilon =$ (γινόμενο τῶν q_i μὲ $i \neq i_1$). Ἡ σχέση αὐτὴ εἶναι δυνατὴ μόνον ἂν δὲν ὑπάρχουν q_i στὸ δεξιὸ μέλος, διότι δὲν εἶναι δυνατὸν γινόμενο ἀναγώγων στοιχείων νὰ ἰσοῦται μὲ μονάδα. Ἄρα, ἀναγκαστικά, $m = 1$ καὶ ἡ τελευταία σχέση εἶναι, στην παραγματικότητα, ἡ $\epsilon = 1$.

Ἂς ὑποθέσομε ὅτι ὁ ἰσχυρισμὸς ἰσχύει γιὰ $n = k - 1 \geq 1$ καὶ ἂς θεωρήσομε μιὰ σχέση $\prod_{i=1}^{k} p_i = \prod_{i=1}^{m} q_i$, στὴν ὁποία ὅλοι οἱ παράγοντες, καὶ στὰ δύο μέλη, εἶναι ἀνάγωγα στοιχεῖα καὶ $k \leq m$. Ἀκριβῶς ὅπως στην περίπτωση $n = 1$, ἀποδεικνύομε ὅτι, τὸ p_k εἶναι συνεταιρικὸ μὲ κάποιο ἀπὸ τὰ $q_1, \ldots, q_m$, ἔστω μὲ τὸ q_{i_k}. Θέτοντας $p_k = \epsilon q_{i_k}$, ὅπου ϵ εἶναι μονάδα, καὶ διαγράφοντας τὸ q_{i_k} ἀπὸ τὰ δύο μέλη τῆς σχέσης $\prod_{i=1}^{k} p_i = \prod_{i=1}^{m} q_i$, παίρνομε τὴ σχέση $\epsilon \prod_{i=1}^{k-1} p_i = \prod_{i_k \neq i=1}^{m} q_i$. Τὸ ἀριστερὸ μέλος μποροῦμε νὰ τὸ γράψομε, ἐπίσης, μὲ τὴ μορφὴ $(\epsilon p_1)p_2 \cdots p_{k-1}$, ἄρα ὡς γινόμενο $k - 1$ τὸ πλῆθος ἀναγώγων στοιχείων, ἐνῶ τὸ ἀριστερὸ μέλος εἶναι γινόμενο $m - 1$ τὸ πλῆθος ἀναγώγων στοιχείων. Ἀπὸ τὴν ἐπαγωγικὴ ὑπόθεση, σὲ κάθε $\nu = 1, \ldots, k - 1$ ἀντιστοιχεῖ ἕνα διαφορετικὸ $i_\nu \in \{1, \ldots, m\} \setminus \{i_k\}$, ἔτσι ὥστε τὸ q_{i_1} νὰ εἶναι συνεταιρικὸ μὲ τὸ ϵp_1 (ἄρα συνεταιρικὸ καὶ μὲ τὸ p_1), τὸ q_{i_2} νὰ εἶναι συνεταιρικὸ μὲ τὸ p_2,..., τὸ $q_{i_{k-1}}$ νὰ εἶναι συνεταιρικὸ μὲ τὸ p_{k-1}. Αὐτὸ ὁλοκληρώνει τὴν ἐπαγωγικὴ ἀπόδειξη.

□

I.2 Μεγιστος Κοινος Διαιρετης

Ὁρισμός. Ἔστω D ἀκέραια περιοχὴ καὶ $a_1, \ldots, a_n \in D$ ($n \geq 2$) ὄχι ὅλα μηδέν. Τὸ $d \in D$ λέγεται *μέγιστος κοινὸς διαιρέτης τῶν* $a_1, \ldots, a_n$ ἂν ἱκανοποιεῖ τὶς ἑξῆς δύο ἰδιότητες:

(α′) Ὁ d εἶναι κοινὸς διαιρέτης τῶν $a_1, \ldots, a_n$, δηλαδή, ὁ d διαιρεῖ καθένα ἀπὸ αὐτὰ τὰ στοιχεῖα.

(β′) Ὁ d διαιρεῖται ἀπὸ κάθε ἄλλον κοινὸ διαιρέτη τῶν $a_1, \ldots, a_n$, δηλαδή, ἂν ὁ $d' \in D$ διαιρεῖ ὅλα τὰ $a_1, \ldots, a_n$, τότε $d'|d$.

Γράφομε, συμβολικά, $d = \text{ΜΚΔ}(a_1, \ldots, a_n)$ γιὰ νὰ δηλώσομε ὅτι ὁ d εἶναι μέγιστος κοινὸς διαιρέτης τῶν $a_1, \ldots, a_n$. Ὅπως θὰ δοῦμε στὴν παρακάτω Πρόταση 1.3, τὸ σύμβολο $\text{ΜΚΔ}(a_1, \ldots, a_n)$ δὲν εἶναι μονοσήμαντα ὁρισμένο, δηλαδή, ἂν $d_1 = \text{ΜΚΔ}(a_1, \ldots, a_n)$ καὶ $d_2 = \text{ΜΚΔ}(a_1, \ldots, a_n)$, αὐτὸ δὲν σημαίνει ὅτι $d_1 = d_2$, ἀλλὰ ὅτι τὰ d_1, d_2 εἶναι συνεταιρικά.

Ἂν τὰ $a_1, \ldots, a_n \in D$ δὲν εἶναι ὅλα μηδὲν καὶ τὸ μοναδιαῖο στοιχεῖο τῆς D εἶναι μέγιστος κοινὸς διαιρέτης τους, τότε τὰ $a_1, \ldots, a_n$ χαρακτηρίζονται *πρῶτα μεταξύ τους*, συμβολικά, $\text{ΜΚΔ}(a_1, \ldots, a_n) = 1$. Στὴν περίπτωση ποὺ $n = 2$, ἡ δήλωση «τὰ a_1, a_2 εἶναι πρῶτα μεταξύ τους» διατυπώνεται ἰσοδύναμα καὶ ὡς ἑξῆς: «Τὸ a_1 εἶναι πρῶτο πρὸς τὸ a_2», ἢ «τὸ a_2 εἶναι πρῶτο πρὸς τὸ a_1».

Ἄσκηση 1.10 (α′) Ἀποδεῖξτε ὅτι $1 = \text{ΜΚΔ}(a_1, \ldots, a_n)$ ἂν καὶ μόνο ἂν οἱ μόνοι κοινοὶ διαιρέτες τῶν $a_1, \ldots, a_n$ εἶναι οἱ μονάδες.
(β′) Ἀποδεῖξτε ὅτι, ἂν $d = \text{ΜΚΔ}(a_1, \ldots, a_n)$ καὶ θέσομε $a_i = db_i$ γιὰ κάθε $i = 1, \ldots, n$, τότε τὰ $b_1, \ldots, b_n$ εἶναι πρῶτα μεταξύ τους.

Πρόταση 1.3 *Ἔστω ὅτι τὰ $a_1, \ldots, a_n \in D$ δὲν εἶναι ὅλα μηδενικὰ καὶ d_1, d_2 εἶναι μέγιστοι κοινοὶ διαιρέτες τῶν $a_1, \ldots, a_n$. Τότε τὰ d_1, d_2 εἶναι συνεταιρικὰ στοιχεῖα. Μὲ πιὸ συμβολικὴ διατύπωση: Ἂν $d_1 = \text{ΜΚΔ}(a_1, \ldots, a_n)$ καὶ $d_2 = \text{ΜΚΔ}(a_1, \ldots, a_n)$, τότε $d_2 = \epsilon d_1$, ὅπου ϵ εἶναι μονάδα τῆς D.*

Ἀπόδειξη. Ὁ d_1, ὡς ΜΚΔ τῶν $a_1, \ldots, a_n$, διαιρεῖται ἀπὸ κάθε κοινὸ διαιρέτη τῶν $a_1, \ldots, a_n$, ἄρα διαιρεῖται καὶ ἀπὸ τὸν d_2. Μὲ ἀνάλογο ἐπιχείρημα, ἐναλλάσσοντας τοὺς ρόλους τῶν d_1, d_2, συμπεραίνομε ὅτι ὁ d_2 διαιρεῖται ἀπὸ τὸν d_1. Ἔτσι, $d_2|d_1$ καὶ $d_1|d_2$, ὁπότε, ἐφαρμόζοντας τὴν ἄσκηση 1.5, καταλήγομε στὸ συμπέρασμα ὅτι τὰ στοιχεῖα d_1, d_2 εἶναι

συνεταιρικά.

□

Ἄσκηση 1.11 Ἔστω η ἀκέραια περιοχὴ $D = \mathbb{Z}[\sqrt{-2}] = \{a + b\sqrt{-2} : a, b \in \mathbb{Z}\}$. Ἀποδεῖξτε τὰ ἑξῆς:

(α′) $D^* = \{-1, 1\}$.

(β′) Τὸ στοιχεῖο $\sqrt{-2}$ τῆς D εἶναι ἀνάγωγο.

Ἔστω τώρα ὅτι οἱ μὴ μηδενικοὶ $x, y \in \mathbb{Z}$ ἱκανοποιοῦν τὴν ἐξίσωση $x^2 + 2 = y^3$. Ἀποδεῖξτε τὰ ἑξῆς:

(γ′) Ὁ x εἶναι περιττός καὶ πρῶτος πρὸς τὸν y (στὸ $\mathbb{Z}$).

(ε′) Θεωρώντας δεδομένο ὅτι ἡ D εἶναι περιοχὴ μονοσήμαντης ἀνάλυσης,[2] ἀποδεῖξτε ὅτι $1 = \text{ΜΚΔ}(x + \sqrt{-2}, x - \sqrt{-2})$.

I.3 Δαιρετοτητα σε περιοχες κυριων ιδεωδων

Δὲν εἶναι βέβαιο ὅτι σὲ ὁποιαδήποτε ἀκέραια περιοχὴ, ὁποιαδήποτε στοιχεῖα της ἔχουν μέγιστο κοινὸ διαιρέτη! Ἂν, ὅμως, ἡ ἀκέραια περιοχὴ ἔχει τὴν ἰδιότητα νὰ εἶναι περιοχὴ κυρίων ἰδεωδῶν, τότε ἡ ὕπαρξη ΜΚΔ εἶναι ἐξασφαλισμένη, ὅπως βλέπομε στὸ ἑπόμενο θεώρημα.

Θεώρημα 1.4 *Ἂν ἡ D εἶναι περιοχὴ κυρίων ἰδεωδῶν, τότε, ὁποιοιαδήποτε στοιχεῖα $a_1, \ldots, a_n$ τῆς D, ποὺ δὲν εἶναι ὅλα μηδέν, ἔχουν μέγιστο κοινὸ διαιρέτη. Ποιὸ συγκεκριμένα, ἂν $\langle a_1, \ldots, a_n\rangle = \langle d\rangle$, τότε $d = \text{ΜΚΔ}(a_1, \ldots, a_n)$ καί, συνεπῶς, κάθε μέγιστος κοινὸς διαιρέτης τῶν $a_1, \ldots, a_n$ γράφεται ὡς γραμμικὸς συνδυασμὸς τῶν $a_1, \ldots, a_n$ μὲ συντελεστὲς ἀπὸ τὴ D.*

Ἀπόδειξη. Ἐξ ὑποθέσεως, τὸ $\langle a_1, \ldots, a_n\rangle$ εἶναι μὴ μηδενικὸ κύριο ἰδεῶδες, ἄρα ὑπάρχει μὴ μηδενικὸ $d \in D$, τέτοιο ὥστε $\langle a_1, \ldots, a_n\rangle = \langle d\rangle$, δηλαδή, ἔχομε τὴ σχέση

$$\langle a_1, \ldots, a_n\rangle = dD. \tag{1.4}$$

Προφανῶς, τὸ $d = d \cdot 1$ ἀνήκει στὸ δεξιὸ μέλος, ἄρα ἀνήκει καὶ στὸ ἀριστερό. Αὐτό, ὅμως, σημαίνει ὅτι ὑπάρχουν $t_1, \ldots, t_n \in D$, τέτοια ὥστε $d = t_1a_1 + \cdots + t_na_n$. Ἐπίσης, κάθε a_i γράφεται $a_i = 0 \cdot a_1 + \cdots 0 \cdot a_{i-1} + 1 \cdot a_i + 0 \cdot a_{i+1} + \cdots 0 \cdot a_n$, ἄρα ἀνήκει στὸ ἀριστερὸ μέλος τῆς (1.4), ἄρα ἀνήκει καὶ στὸ δεξιὸ μέλος. Αὐτὸ σημαίνει ὅτι ὑπάρχει $b_i \in D$, τέτοιο ὥστε $a_i = db_i$, δηλαδή, $d|a_i$. Ἔτσι βλέπομε ὅτι τὸ d εἶναι κοινὸς διαιρέτης ὅλων τῶν a_i. Μένει νὰ δείξομε ὅτι, ἂν ὁ $d' \in D$ εἶναι ἕνας ὁποιοσδήποτε κοινὸς διαιρέτης ὅλων τῶν a_i, τότε $d'|d$. Πράγματι, διότι τότε, τὸ d' διαιρεῖ τὸ δεξιὸ μέλος τῆς σχέσης $d = t_1a_1 + \cdots + t_na_n$ (βλ. ἄσκηση1.2), ἄρα διαιρεῖ καὶ τὸ ἀριστερό μέλος, δηλαδή, τὸ d.

□

Ἄσκηση 1.12 Ἔστω D περιοχὴ κυρίων ἰδεωδῶν καὶ $a_1, \ldots, a_n, b \in D$. Ἀποδεῖξτε ὅτι, ἂν $d = \text{ΜΚΔ}(a_1, \ldots, a_n)$, τότε $bd = \text{ΜΚΔ}(ba_1, \ldots, ba_n)$.[3]

Θεώρημα 1.5 *Σὲ κάθε περιοχὴ κυρίων ἰδεωδῶν D ἰσχύουν τὰ ἑξῆς:*

(α′) Ἂν τὸ p εἶναι ἀνάγωγο, τότε, κάθε στοιχεῖο $a \in D$, εἴτε εἶναι πολλαπλάσιο τοῦ p, εἴτε εἶναι πρῶτο πρὸς τὸ p.

[2] Θὰ τὸ ἀποδείξομε ἀργότερα· βλ Παράδειγμα 3 στὴ σελίδα 20.

[3] Πρβλ. μὲ ἄσκηση 1.14.

(β΄) Κάθε ἀνάγωγο στοιχεῖο εἶναι πρῶτο. Συνεπῶς, λόγῳ τῆς Προτάσεως 1.1*, οἱ ἔννοιες «ἀνάγωγο στοιχεῖο» καὶ «πρῶτο στοιχεῖο» συμπίπτουν.*

(γ΄) Ἂν τὰ a, b εἶναι πρῶτα μεταξύ τους, $a|c$ καὶ $b|c$, τότε $ab|c$.

(δ΄) Ἂν καθένα ἀπὸ τὰ a, b εἶναι πρῶτο πρὸς τὸ c, τότε τὸ ab εἶναι πρῶτο πρὸς τὸ c.

Ἀπόδειξη. (α′) Θὰ ὑποθέσομε ὅτι τὸ a δὲν εἶναι πολλαπλάσιο τοῦ p καὶ θ' ἀποδείξομε ὅτι τὰ a, p εἶναι πρῶτα μεταξύ τους. Ἔστω $d = \text{μκδ}(a, p)$. Ἔχομε ὅτι $d|p$, ἀλλά, ἀφοῦ τὸ p ἔχει ὑποτεθεῖ ἀνάγωγο, εἴμαστε ἀναγκασμένοι νὰ συμπεράνομε ὅτι τὸ d εἶναι συνεταιρικὸ τοῦ p. Ἀπ' τὴν ἄλλη, $d|a$, ὁπότε βλέπομε ὅτι ἕνα στοιχεῖο συνεταιρικὸ τοῦ p διαιρεῖ τὸ a, ἄρα (βλ. ἄσκηση 1.4) καὶ τὸ p διαιρεῖ τὸ a· ἀντίφαση.

(β′) Ἔστω $p \in D$ ἀνάγωγο στοιχεῖο καὶ ἂς ὑποθέσομε ὅτι, γιὰ κάποια $a, b \in D$ ἔχομε ὅτι $p|ab$. Πρέπει καὶ ἀρκεῖ ν' ἀποδείξομε ὅτι τὸ p διαιρεῖ ἕνα, τοὐλάχιστον, ἀπὸ τὰ a, b. Πράγματι, ἂν ὑποθέσομε ὅτι τὸ p δὲν διαιρεῖ τὸ a, τότε, ἀπὸ τὸ (α′) ὁδηγούμαστε στὸ συμπέρασμα ὅτι $\text{μκδ}(p, a) = 1$, ὁπότε τὸ Θεώρημα 1.4, ὑπάρχουν $c, d \in D$, τέτοια ὥστε $1 = cp + da$. Πολλαπλασιάζοντας ἐπὶ b τὰ δύο μέλη παίρνομε τὴ σχέση $b = bcp + d(ab)$, τὸ δεξιὸ μέλος τῆς ὁποίας διαιρεῖται ἀπ' τὸ p (ἀφοῦ ἔχομε ὑποθέσει ὅτι $p|ab$), ἄρα $p|b$.

(γ′) Ἀπ' τὸ Θεώρημα 1.4, ὑπάρχουν $d, e \in D$, τέτοια ὥστε $1 = da + eb$. Πολλαπλασιάζοντας ἐπὶ c τὰ δύο μέλη παίρνομε τὴ σχέση $c = dac + ebc$. Ἀπ' τὴν ὑπόθεση $a|c$ συμπεραίνομε ὅτι $c = ac_1$, γιὰ κάποιο $c_1 \in D$ καί, ἀνάλογα, $c = bc_2$, λόγῳ τῆς $b|c$. Ἄρα, $c = dac + ebc = da(bc_2) + eb(ac_1) = ab(c_2d + c_1e)$, ποὺ δείχνει ὅτι $ab|c$.

(δ′) Ἂν τὸ ab δὲν εἶναι πρῶτο πρὸς τὸ c, τότε, ἀπὸ τὴν ἄσκηση 1.10, ὑπάρχει κοινὸς διαιρέτης d τῶν ab καὶ c, ποὺ δὲν εἶναι μονάδα. Ἀπ' τὴν ἄλλη, ἀφοῦ $\text{μκδ}(a, c) = 1$, τὸ Θεώρημα 1.4 μᾶς λέει ὅτι ὑπάρχουν $x, y \in D$, τέτοια ὥστε $xa + yc = 1$. Πολλαπλασιάζοντας ἐπὶ b τὰ δύο μέλη παίρνομε τὴ σχέση $b = xab + ycb$, τὸ δεξιὸ μέλος τῆς ὁποίας διαιρεῖται ἀπ' τὸ d, διότι $d|ab$ καὶ $d|c$. Ἄρα, $d|b$ καί, συνεπῶς, καταλήξαμε στὸ συμπέρασμα ὅτι τὸ d, ποὺ δὲν εἶναι μονάδα, διαιρεῖ τὸ b καὶ τὸ c, ἀντιφάσκοντας τὴν ὑπόθεσή μας ὅτι τὰ b, c εἶναι πρῶτα μεταξύ τους.

□

Θεώρημα 1.6 *Ἂν μιὰ περιοχὴ ἀνάλυσης εἶναι περιοχὴ κυρίων ἰδεωδῶν, τότε εἶναι καὶ περιοχῆς μονοσήμαντης ἀνάλυσης.*

Ἀπόδειξη. Προκύπτει ἀπὸ προφανῆ συνδυασμὸ τῆς Πρότασης 1.2 καὶ τοῦ Θεωρήματος 1.5 (β′).

□

Χάρη στὰ Θεωρήματα 1.5 καὶ 1.6, μποροῦμε νὰ μεταφέρομε ὅλη, οὐσιαστικά, τὴ θεωρία διαιρετότητας τῶν ἀκεραίων σὲ κάθε περιοχὴ ἀνάλυσης, ἡ ὁποία εἶναι συγχρόνως καὶ περιοχὴ κυρίων ἰδεωδῶν. Ἡ ἀπόδειξη τοῦ Θεωρήματος 1.5 στηρίζεται στὴν ὕπαρξη μεγίστου κοινοῦ διαιρέτη γιὰ ὁποιαδήποτε στοιχεῖα $a_1, \ldots, a_n$ τῆς θεωρούμενης περιοχῆς, καθὼς ἐπίσης καὶ στὴ δυνατότητα γραφῆς αὐτοῦ τοῦ μεγίστου κοινοῦ διαιρέτη ὡς γραμμικοῦ συνδυασμοῦ τῶν $a_1, \ldots, a_n$. Οἱ ἰδιότητες αὐτές, μὲ τὴ σειρά τους, στηρίζονται κατὰ οὐσιαστικὸ τρόπο στὸ ὅτι κάθε ἰδεῶδες τῆς θεωρούμενης ἀκέραιας περιοχῆς εἶναι κύριο. Τὸ γεγονὸς αὐτὸ μπορεῖ νὰ κάνει κάποιον νὰ εἰκάσει ὅτι, σὲ περιοχές, στὶς ὁποῖες δὲν εἶναι ὅλα τὰ ἰδεώδη κύρια, δὲν εἶναι δυνατὴ ἡ δημιουργία μιᾶς ἱκανοποιητικῆς θεωρίας διαιρετότητας. Γιὰ τὶς ἀκέραιες περιοχὲς ἐν γένει, ἀκόμη καὶ γιὰ τὶς περιοχὲς ἀνάλυσης, δίχως ἐπιπλέον ὑποθέσεις, ἡ εἰκασία εἶναι σωστή. Στὶς περιοχὲς μονοσήμαντης ἀνάλυσης, ὅμως, μιὰ πολὺ ἱκανοποιητικὴ θεωρία διαιρετότητας, ἐντελῶς ἀνάλογη μὲ αὐτὴν τῶν

ἀκεραίων, μπορεῖ νὰ φτιαχτεῖ. Τέτοιες περιοχὲς μονοσήμαντης ἀνάλυσης, οἱ ὁποῖες δὲν εἶναι περιοχὲς κυρίων ἰδεωδῶν ὑπάρχουν (θὰ συναντήσομε ἀργότερα) καὶ εἶναι πολὺ σημαντικὲς στὰ Μαθηματικά. Γιὰ τὸν λόγο αὐτὸ ἔχει σημασία νὰ φτιάξομε καὶ γι' αὐτὲς μιὰ θεωρία διαιρετότητας.

I.4 Διαιρετοτητα σε περιοχες μονοσημαντης αναλυσης

Πρόταση 1.7 *Σὲ κάθε περιοχὴ μονοσήμαντης ἀνάλυσης, τὰ ἀνάγωγα στοιχεῖα εἶναι πρῶτα στοιχεῖα. Συνεπῶς, λόγῳ τῆς* Προτάσεως 1.1*, οἱ ἔννοιες «ἀνάγωγο στοιχεῖο» καὶ «πρῶτο στοιχεῖο» συμπίπτουν, σ' αὐτὲς τὶς περιοχές.*

Ἀπόδειξη. Ἔστω D περιοχὴ μονοσήμαντης ἀνάλυσης, $p \in D$ ἀνάγωγο, $a, b \in D$ καὶ $p|ab$. Πρέπει καὶ ἀρκεῖ νὰ δείξομε ὅτι τὸ p διαιρεῖ ἕνα τοὐλάχιστον ἀπὸ τὰ a, b. Ἀπὸ τὴν ὑπόθεση συμπεραίνομε ὅτι ὑπάρχει $c \in D$, ἔτσι ὥστε $ab = pc$. Ἔστω ὅτι ἡ ἀνάλυση τῶν a, b, c σὲ ἀνάγωγα στοιχεῖα τῆς D εἶναι: $a = p_1 \cdots p_\ell$, $b = q_1 \cdots q_m$, $c = r_1 \cdots r_n$, ὁπότε ἡ σχέση $ab = pc$ γίνεται

$$p_1 \cdots p_\ell \cdot q_1 \cdots q_m = ab = p \cdot r_1 \cdots r_n,$$

ἄρα ἔχομε δύο ἀναλύσεις τοῦ ab σὲ ἀνάγωγα. Ὅμως, στὴ D ἰσχύει ἡ μονοσήμαντη ἀνάλυση. Ἄρα, ἀφοῦ τὸ ἀνάγωγο p ἐμφανίζεται στὸ δεξιὸ μέλος, πρέπει στὸ ἀριστερὸ μέλος κάποιο ἀπὸ τὰ ἀνάγωγα στοιχεῖα νὰ εἶναι συνεταιρικὸ (δὲν ἀποκλείεται νὰ εἶναι ἴσο) μὲ τὸ p. Δηλαδή, τὸ p εἶναι συνεταιρικό, ἢ μὲ κάποιο ἀπὸ τὰ $p_1, \ldots, p_\ell$, ἢ μὲ κάποιο ἀπὸ τὰ $q_1, \ldots, q_m$. Στὴν πρώτη περίπτωση τὸ p διαιρεῖ τὸ a, ἐνῶ στὴ δεύτερη διαιρεῖ τὸ b. □

Ἀπὸ τώρα, μέχρι τέλους τῆς ἑνότητας 1.4, D θὰ εἶναι περιοχὴ μονοσήμαντης ἀνάλυσης.

Ὁρισμός. Τὸ $\mathcal{P} \subset D$ λέγεται *πλῆρες σύστημα πρώτων (= ἀναγώγων) στοιχείων τῆς* D ἂν:

(α′) Κάθε ἀνάγωγο στοιχεῖο τῆς D εἶναι συνεταιρικὸ μὲ κάποιο στοιχεῖο τοῦ $\mathcal{P}$ καὶ (β′).
(β′) Ἀνὰ δύο τὰ στοιχεῖα τοῦ $\mathcal{P}$ *δὲν* εἶναι συνεταιρικά.

Ἔστω ὅτι $a \in D \setminus D^*$, $a \neq 0$ καὶ ἀναλύομε τὸ a σὲ ἀνάγωγα στοιχεῖα: $a = q_1 \cdots q_n$. Ἐξ ὁρισμοῦ τοῦ $\mathcal{P}$, καθένα ἀπὸ τὰ $q_1, \ldots, q_n$ εἶναι συνεταιρικὸ μὲ κάποιο $p_i \in \mathcal{P}$, δηλαδή, γιὰ κάθε $i = 1, \ldots, n$ ὑπάρχει $p_i \in \mathcal{P}$ καὶ $\epsilon_i \in D^*$, τέτοια ὥστε $q_i = \epsilon_i p_i$. Προσέξτε, ὅμως, ὅτι δὲν εἶναι ἀπαραίτητο σὲ διαφορετικὰ q_i ν' ἀντιστοιχοῦν διαφορετικὰ p_i, δηλαδή, δὲν ἀποκλείεται νὰ εἶναι $i \neq j$ καὶ $p_i = p_j$· αὐτὸ θὰ συμβεῖ ἂν τὰ q_i, q_j εἶναι συνεταιρικά. Ἄρα,

$$a = q_1 q_2 \ldots q_n = (\epsilon_1 p_1)(\epsilon_2 p_2) \cdots (\epsilon_n p_n) = \epsilon_a p_1 p_2 \cdots p_n \qquad (\epsilon_a = \epsilon_1 \epsilon_2 \cdots \epsilon_n \in D^*). \quad (1.5)$$

Ἂν στὴν παραπάνω σχέση ὁμαδοποιήσομε τὰ ἴσα μεταξύ τους p_i, τότε βλέπομε ὅτι τὸ a γράφεται ὡς γινόμενο τῆς μονάδας ϵ_a καὶ δυνάμεων *διαφορετικῶν* στοιχείων $p \in \mathcal{P}$. Ἐφόσον τὸ $p \in \mathcal{P}$ ἐμφανίζεται στὴν ἀνάλυση (1.5), ὁ ἐκθέτης του, τὸν ὁποῖον στὸ ἑξῆς θὰ συμβολίζομε μὲ $v_p(a)$, εἶναι θετικὸς καί, ἐνδεχομένως, μεγαλύτερος τοῦ 1. Γιὰ λόγους ὁμοιομορφίας, ἂν ὁ $p \in \mathcal{P}$ δὲν ἐμφανίζεται στὴν ἀνάλυση (1.5), τότε θέτομε $v_p(a) = 0$, ὁπότε μποροῦμε νὰ γράψομε τὴν ἀνάλυση τοῦ a ὡς ἑξῆς:

$$a = \epsilon_a \cdot \prod_{p \in \mathcal{P}} p^{v_p(a)}, \quad \epsilon_a \in D^*, \quad v_p(a) \geq 0 \ \ \forall p \in \mathcal{P}, \quad (1.6)$$

ὅπου οἱ ἀκέραιοι ἐκθέτες $v_p(a)$ εἶναι "σχεδὸν ὅλοι" μηδὲν (δηλαδή, πεπερασμένοι τὸ πλῆθος ἐκθέτες $v_p(a)$ εἶναι γνησίως θετικοί).

Ἡ ἀνάλυση (1.6) λέγεται *κανονικὴ ἀνάλυση τοῦ* a σὲ πρῶτα (ἢ σὲ ἀνάγωγα) στοιχεῖα καὶ εἶναι μονοσήμαντα ὁρισμένη, ἂν παραβλέψομε τὴ σειρὰ μὲ τὴν ὁποίαν εἶναι γραμμένοι οἱ παράγοντες.

Προφανῶς γιὰ κάθε μονάδα ϵ εἶναι $v_p(\epsilon) = 0 \ \forall p \in \mathcal{P}$. Γιὰ τὸ $0 \in D$ θέτομε $v_p(0) = \infty$ γιὰ κάθε $p \in \mathcal{P}$ καὶ κάνομε τὴ σύμβαση $\infty + n = \infty$ γιὰ κάθε ἀκέραιο n.

Παραδείγματα: Ἂν $D = \mathbb{Z}$, τότε $\mathcal{P}$ εἶναι τὸ σύνολο τῶν (θετικῶν) πρώτων ἀριθμῶν. Ἂν $D = K[X]$, ὅπου τὸ K εἶναι σῶμα, τότε τὸ $\mathcal{P}$ εἶναι τὸ σύνολο τῶν ἀναγώγων μονικῶν πολυωνύμων τοῦ $K[X]$[4]

Θεώρημα 1.8 *Ἔστω D περιοχὴ μονοσήμαντης ἀνάλυσης, $\mathcal{P}$ ἕνα πλῆρες σύστημα πρώτων τῆς D καὶ $a, b \in D$ μὲ $b \neq 0$. Τότε, $b|a \Leftrightarrow v_p(b) \leq v_p(a) \ \forall p \in \mathcal{P}$.*

Ἀπόδειξη. Ἂς θεωρήσομε τὶς κανονικὲς ἀναλύσεις $a = \epsilon_a \prod_{p\in\mathcal{P}} p^{v_p(a)}$, $b = \epsilon_b \prod_{p\in\mathcal{P}} p^{v_p(b)}$ ($\epsilon_a, \epsilon_b \in D^*$).

($\Rightarrow$) Ἔστω ὅτι $b|a$, ὁπότε ὑπάρχει $c \in D$ τέτοιο ὥστε $a = bc$. Ἂν θεωρήσομε τὴν κανονικὴ ἀνάλυση $c = \epsilon_c \prod_{p\in\mathcal{P}} p^{v_p(c)}$ ($\epsilon_c \in D^*$), τότε ἡ σχέση $a = bc$ συνεπάγεται τὴ σχέση

$$\epsilon_a \prod_{p\in\mathcal{P}} p^{v_p(a)} = \epsilon_b\epsilon_c \prod_{p\in\mathcal{P}} p^{v_p(b)+v_p(c)}.$$

Ἐπειδὴ ἰσχύει ἡ μονοσήμαντη ἀνάλυση σὲ πρῶτα στοιχεῖα, ἡ παραπάνω σχέση μᾶς ὁδηγεῖ στὸ συμπέρασμα ὅτι, γιὰ κάθε $p \in \mathcal{P}$ ἰσχύει $v_p(a) = v_p(b) + v_p(c) \geq v_p(b)$.

($\Leftarrow$) Ἀντιστρόφως, ἔστω ὅτι $v_p(a) \geq v_p(b)$ γιὰ κάθε $p \in \mathcal{P}$. Τότε, $n_p \overset{\text{ορ}}{=} v_p(a) - v_p(b) \geq 0$ γιὰ κάθε $p \in \mathcal{P}$ καὶ $n_p = 0$ γιὰ σχεδὸν ὅλα τὰ p. Ἄρα μποροῦμε νὰ θεωρήσομε τὸ στοιχεῖο $c \overset{\text{ορ}}{=} \epsilon_a\epsilon_b^{-1} \prod_{p\in\mathcal{P}} p^{n_p} \in D$ καί, προφανῶς, ἰσχύει $bc = a$, ποὺ σημαίνει ὅτι $b|a$.

□

Παρατήρηση. Κατὰ τὴν ἀπόδειξη τοῦ Θεωρήματος 1.8 δείξαμε ὅτι, ἂν $a = bc$, τότε $v_p(a) = v_p(b) + v_p(c) \ \forall p \in \mathcal{P}$.

Ἄσκηση 1.13 Ἔστω D καὶ $\mathcal{P}$ ὅπως στὸ Θεώρημα 1.8.
(α′) Ἀποδεῖξτε ὅτι ἕνα στοιχεῖο $p \in \mathcal{P}$ διαιρεῖ ἕνα στοιχεῖο a ἂν καὶ μόνο ἄν, $v_p(a) > 0$.
(β′) Ἀποδεῖξτε ὅτι, ἂν τὰ στοιχεῖα $a, b \in D$ εἶναι πρῶτα μεταξύ τους, τότε, γιὰ κάθε $p \in \mathcal{P}$, ἕνα, τὸ πολύ, ἀπὸ τὰ $v_p(a), v_p(b)$ εἶναι διάφορο τοῦ μηδενός. Ἀλλὰ καὶ ἀντιστρόφως: Ἂν γιὰ τὰ στοιχεῖα a, b ἰσχύει ὅτι, γιὰ κάθε $p \in \mathcal{P}$, ἕνα, τὸ πολύ, ἀπ' τὰ $v_p(a), v_p(b)$ εἶναι διάφορο τοῦ μηδενός, τότε τὰ a, b εἶναι πρῶτα μεταξύ τους.
(γ′) Ἀποδεῖξτε ὅτι, ἂν $a_1, \ldots, a_n, b \in D$ καὶ τὸ b εἶναι πρῶτο πρὸς κάθε a_i, τότε τὸ b εἶναι πρῶτο καὶ πρὸς τὸ γινόμενο $a_1 \cdots a_n$.
(δ′) Ἀποδεῖξτε ὅτι, ἂν $a_1, \ldots, a_n, b \in D$, τὰ a_i εἶναι ἀνὰ δύο πρῶτα μεταξύ τους καὶ τὸ b διαιρεῖται ἀπὸ κάθε a_i, τότε τὸ b διαιρεῖται καὶ ἀπὸ τὸ γινόμενο $a_1 \cdots a_n$.
Ὑπόδειξη. Πρέπει καὶ ἀρκεῖ νὰ δείξετε ὅτι, γιὰ κάθε $p \in \mathcal{P}$ ἰσχύει $v_p(a_1 \cdots a_n) \leq v_p(b)$. Αὐτὸ εἶναι ἄμεσο στὴν περίπτωση ποὺ τὸ p δὲν διαιρεῖ κανένα a_i. Ἂν τὸ p διαιρεῖ κάποιο a_i, ἔστω τὸ a_{i_0}, τότε, βάσει τοῦ (β′), συμπεράνατε ὅτι $v_p(a_i) = 0$ γιὰ κάθε $i \neq i_0$. Συνεπῶς, $v_p(a_1 \cdots a_n) = \ldots$.

Τώρα εἱμαστε σὲ θέση νὰ ἀποδείξομε ὅτι γιὰ ὁποιαδήποτε $a_1, \ldots, a_n \in D$, ποὺ δὲν εἶναι ὅλα μηδέν, ὑπάρχει ὁ μέγιστος κοινὸς διαιρέτης τους.

[4] Μὲ τὸν ὅρο *μονικὸ πολυώνυμο* ἐννοοῦμε πολυώνυμο μὲ συντελεστὴ μεγιστοβαθμίου ὅρου τὸ 1.

Πρόταση 1.9 *Ἔστω D περιοχὴ μονοσήμαντης ἀνάλυσης καὶ $\mathcal{P}$ πλῆρες σύστημα πρώτων στοιχείων της. Ἂν $n \geq 2$ καὶ $a_1, \ldots, a_n \in D$ δὲν εἶναι ὅλα μηδενικά, τότε τὸ στοιχεῖο*

$$d \overset{\text{ορ}}{=} \prod_{p \in \mathcal{P}} p^{n_p}, \quad n_p \overset{\text{ορ}}{=} \min\{v_p(a_1), \ldots, v_p(a_n)\} \ \forall p \in \mathcal{P}$$

εἶναι μέγιστος κοινὸς διαιρέτης τῶν $a_1, \ldots, a_n$.

Ἀπόδειξη. Γιὰ κάθε $p \in \mathcal{P}$ καὶ κάθε $i = 1, \ldots, n$ εἶναι, προφανῶς, $v_p(d) = n_p \leq v_p(a_i)$, ὁπότε (Θεώρημα 1.8) $d|a_i$. Συνεπῶς, τὸ d εἶναι κοινὸς διαιρέτης τῶν $a_1, \ldots, a_n$. Ἔστω τώρα d' ἕνας ὁποιοσδήποτε κοινὸς διαιρέτης τῶν $a_1, \ldots, a_n$. Τὸ Θεώρημα 1.8 μᾶς λέει ὅτι, γιὰ κάθε $p \in \mathcal{P}$ ἰσχύει $v_p(d') \leq v_p(a_i) \forall i = 1, \ldots, n$, ἄρα καὶ $v_p(d') \leq \min_{1 \leq i \leq n} v_p(a_i) = n_p = v_p(d)$. Συνεπῶς, πάλι ἀπ' τὸ ἴδιο θεώρημα συμπεραίνομε ὅτι $d'|d$.

Τελικά, τὸ d εἶναι κοινὸς διαιρέτης τῶν $a_1, \ldots, a_n$ καὶ διαιρεῖται ἀπὸ ὁποιονδήποτε κοινὸ διαιρέτη αὐτῶν τῶν στοιχείων, ποὺ σημαίνει ὅτι τὸ d εἶναι μέγιστος κοινὸς διαιρέτης τους.

□

Ἄσκηση 1.14 Ἔστω D περιοχὴ μονοσήμαντης ἀνάλυσης καὶ $a_1, \ldots, a_n, b \in D$. Ἀποδεῖξτε ὅτι, ἂν $d = \text{ΜΚΔ}(a_1, \ldots, a_n)$, τότε $bd = \text{ΜΚΔ}(ba_1, \ldots, ba_n)$.[5]

Τὸ ἑπόμενο θεώρημα θὰ μᾶς ἐπιτρέψει νὰ ἔχομε σὲ περιοχὲς μονοσήμαντης ἀνάλυσης θεωρία διαιρετότητας ἐντελῶς ἀνάλογη μὲ ἐκείνη τῶν ἀκεραίων ἀριθμῶν.

Θεώρημα 1.10 *Σὲ κάθε περιοχὴ μονοσήμαντης ἀνάλυσης D ἰσχύουν τὰ ἑξῆς:*

(α΄) Ἂν τὸ p εἶναι ἀνάγωγο, τότε, κάθε στοιχεῖο $a \in D$, εἴτε εἶναι πολλαπλάσιο τοῦ p, εἴτε εἶναι πρῶτο πρὸς τὸ p.[6]

(β΄) Ἂν τὰ a, b εἶναι πρῶτα μεταξύ τους, $a|c$ καὶ $b|c$, τότε $ab|c$.[7]

(γ΄) Ἂν καθένα ἀπὸ τὰ a, b εἶναι πρῶτο πρὸς τὸ c, τότε τὸ ab εἶναι πρῶτο πρὸς τὸ c.[8]

Ἀπόδειξη. Ἔστω $\mathcal{P}$ πλῆρες σύστημα πρώτων γιὰ τὴν D.

(α′) Πρέπει καὶ ἀρκεῖ νὰ δείξομε ὅτι, ἂν $p \nmid a$, τότε $\text{ΜΚΔ}(a, p) = 1$. Γιὰ τὸν σκοπὸ αὐτὸ θεωροῦμε $p_0 \in \mathcal{P}$, συνεταιρικὸ τοῦ p. Προφανῶς $p_0 \nmid a$ (ἄσκηση 1.4), ὁπότε $v_{p_0}(a) = 0$, ἐνῶ $v_{p_0}(p) = 1$· ἄρα $\min\{v_{p_0}(a), v_{p_0}(p)\} = 0$. Γιὰ κάθε $q \in \mathcal{P}$ διαφορετικὸ τοῦ p_0 εἶναι, προφανῶς, $v_q(p) = 0$, ἀφοῦ τὸ q εἶναι ἀνάγωγο, ἄρα $\min\{v_q(a), v_q(p)\} = 0$. Τώρα, ἀπὸ τὴν Πρόταση 1.9,

$$\text{ΜΚΔ}(a, p) = p_0^{\min\{v_{p_0}(a), v_{p_0}(p)\}} \prod_{p_0 \neq q \in \mathcal{P}} q^{\min\{v_q(a), v_q(p)\}} = p_0^0 \prod_{p_0 \neq q \in \mathcal{P}} q^0 = 1.$$

(β′) Λόγῳ τοῦ Θεωρήματος 1.8, ἀρκεῖ νὰ δείξομε ὅτι, γιὰ ὁποιοδήποτε $p \in \mathcal{P}$, ἰσχύει $v_p(ab) \leq v_p(c)$. Ἔστω, λοιπόν, $p \in \mathcal{P}$. Οἱ σχέσεις $a|c$ καὶ $b|c$ συνεπάγονται (λόγῳ τοῦ Θεωρήματος 1.8) τὶς σχέσεις $v_p(a) \leq v_p(c)$ καὶ $v_p(b) \leq v_p(c)$, ἀντιστοίχως. Ἐπειδή, ὅμως, τὰ a, b εἶναι πρῶτα μεταξύ τους, ἔπεται ὅτι ἕνα τοὐλάχιστον ἀπ' τὰ $v_p(a), v_p(b)$ εἶναι μηδέν (βλ. ἄσκηση 1.13), ἄρα $v_p(ab) = v_p(a) + v_p(b) = \max\{v_p(a), v_p(b)\} \leq v_p(c)$, δηλαδή, ἀποδείξαμε τὸν ἰσχυρισμό μας.

[5] Πρβλ. μὲ ἄσκηση 1.12.
[6] Πρβλ. Θεώρημα 1.5 (α′).
[7] Πρβλ. Θεώρημα 1.5 (γ′).
[8] Πρβλ. Θεώρημα 1.5 (δ′).

(γ′) Ἀπὸ τὴν ἄσκηση 1.13 (β′), ἀρκεῖ νὰ δείξομε ὅτι, γιὰ κάθε $p \in \mathcal{P}$, ἕνα τοὐλάχιστον ἀπ' τὰ $v_p(ab), v_p(c)$ εἶναι μηδέν. Πράγματι, αὐτὸ ἰσχύει, διότι, ἔστω ὅτι $v_p(c) > 0$. Τότε, ἡ ὑπόθεση ὅτι τὰ a, c εἶναι πρῶτα μεταξύ τους, συνδυασμένη μὲ τὴν ἄσκηση 1.13 (β′), μᾶς ὁδηγεῖ στὸ συμπέρασμα ὅτι $v_p(a) = 0$. Ἐντελῶς ἀνάλογα, $v_p(b) = 0$, ἄρα $v_p(ab) = v_p(a) + v_p(b) = 0$.

□

Ἡ παρακάτω πρόταση εἶναι πολὺ χρήσιμη στὴν ἐπίλυση Διοφαντικῶν ἐξισώσεων:

Πρόταση 1.11 *Ἔστω D περιοχὴ μονοσήμαντης ἀνάλυσης καὶ $a, b, c \in D$, τέτοια ὥστε, τὰ a, b εἶναι πρῶτα μεταξύ τους καὶ $ab = c^n$, ὅπου ὁ n εἶναι ἀκέραιος ≥ 2. Τότε καθένα ἀπὸ τὰ a, b εἶναι συνεταιρικὸ μὲ n-οστὴ δύναμη στοιχείου τῆς D.*

Ἀπόδειξη. Ἔστω $\mathcal{P}$ πλῆρες σύστημα πρώτων γιὰ τὴν D. Γιὰ ν' ἀποδείξομε ὅτι τὸ a εἶναι συνεταιρικὸ n-οστῆς δύναμης κάποιου στοιχείου τῆς D, ἀρκεῖ νὰ δείξομε ὅτι, γιὰ κάθε $p \in \mathcal{P}$ εἶναι $v_p(a) =$ ἀκέραιο πολλαπλάσιο τοῦ n. Θεωροῦμε, λοιπόν, $p \in \mathcal{P}$ καὶ ἔχομε

$$n \cdot v_p(c) = v_p(c^n) = v_p(ab) = v_p(a) + v_p(b),$$

ὅπου τοὐλάχιστον ἕνα ἐκ τῶν $v_p(a), v_p(b)$ εἶναι μηδέν, ἀφοῦ τὰ a, b εἶναι πρῶτα μεταξύ τους (βλ. ἄσκηση 1.13 (β′)). Ἂν $v_p(a) = 0$, τότε, προφανῶς, $v_p(a)$ εἶναι πολλαπλάσιο τοῦ n. Ἄν, πάλι, $v_p(a) \neq 0$, τότε, ἀναγκαστικά, $v_p(b) = 0$, ὁπότε ἡ παραπάνω σχέση γίνεται $n \cdot v_p(c) = v_p(a)$, δηλαδή, καὶ πάλι, $v_p(a)$ εἶναι πολλαπλάσιο τοῦ n.

□

Ἄσκηση 1.15 Ἔστω D περιοχὴ μονοσήμαντης ἀνάλυσης καὶ $a, b, c, d \in D$, τέτοια ὥστε, τὰ a, b εἶναι πρῶτα μεταξύ τους καὶ $ab = dc^n$, ὅπου ὁ n εἶναι ἀκέραιος ≥ 2. Τότε ὑπάρχουν $c_1, c_2, d_1, d_2 \in D$, μὲ τὶς ἑξῆς ἰδιότητες:

- c_1, c_2 εἶναι πρῶτα μεταξύ τους καὶ $c_1 c_2 = c$.
- d_1, d_2 εἶναι πρῶτα μεταξύ τους καὶ $d_1 d_2 = d$.
- Τὸ a εἶναι συνεταιρικὸ μὲ τὸ $d_1 {c_1}^n$ καὶ τὸ b εἶναι συνεταιρικὸ μὲ τὸ $d_2 {c_2}^n$.

I.5 Πολυώνυμα πάνω από περιοχες μονοσημαντης αναλυσης

Ὅπως ἐπισημάναμε στὴν «Σημαντικὴ παρατήρηση» τῆς σελίδας 7, στὴν περίπτωση ποὺ $D = K =$ σῶμα, ὁ δακτύλιος πολυωνύμων $K[X]$ εἶναι περιοχὴ μονοσήμαντης ἀνάλυσης (ὡς συνέπεια τοῦ ὅτι ὁ $K[X]$ εἶναι περιοχὴ κυρίων ἰδεωδῶν). Θὰ ἀποδείξομε ὅτι, ὅταν ἡ D εἶναι περιοχὴ μονοσήμαντης ἀνάλυσης, ἀκόμη κι ἂν δὲν εἶναι σῶμα, καὶ πάλι ὁ δακτύλιος πολυωνύμων $D[X]$ εἶναι περιοχὴ μονοσήμαντης ἀνάλυσης.

> Στὴν παροῦσα ἑνότητα 1.5, πάντα τὸ D συμβολίζει περιοχὴ μονοσήμαντης ἀνάλυσης.

Ὁρισμός. Τὸ $d \in D$ χαρακτηρίζεται *περιεχόμενο τοῦ μὴ μηδενικοῦ πολυωνύμου* $f(X) \in D[X]$ εἶναι c, ὅπου $c \in D$, ἂν c εἶναι ΜΚΔ τῶν συντελεστῶν τοῦ $f(X)$. Τὸ μὴ σταθερὸ πολυώνυμο $f(X) \in D[X]$ χαρακτηρίζεται *πρωταρχικό*, ἂν τὸ περιεχόμενό του εἶναι $1 \in D$.

Ἄσκηση 1.16 (α′) Ἂν $d_1, d_2 \in D$ εἶναι καὶ τὰ δύο περιεχόμενα τοῦ ἴδιου πολυωνύμου τῆς $D[X]$, τότε αὐτὰ εἶναι συνεταιρικὰ στοιχεῖα τῆς D.
(β′) Ἂν τὸ $d \in D$ εἶναι περιεχόμενο τοῦ $f(X) \in D[X]$, τότε τὸ $d^{-1}f(X)$ εἶναι πρωταρχικὸ πολυώνυμο τῆς $D[X]$.
(γ′) Ἂν τὸ $f(X)$ εἶναι πρωταρχικὸ πολυώνυμο τῆς $D[X]$ καὶ $d \in D$ (μη μηδενικό), τότε τὸ d εἶναι περιεχόμενο τοῦ $d \cdot f(X)$.

Λήμμα 1.12 *Κάθε μὴ μηδενικὸ $f(X) \in Q(D)[X]$ γράφεται ὡς γινόμενο $f(X) = \alpha \cdot g(X)$, ὅπου $\alpha \in Q(D)$ καὶ $g(X)$ εἶναι πρωταρχικὸ πολυώνυμο τῆς $D[X]$. Ἂν $f(X) = \beta \cdot h(X)$, ὅπου $\beta \in Q(D)$ καὶ $h(X)$ εἶναι πρωταρχικὸ πολυώνυμο τῆς $D[X]$, τότε ὑπάρχει $\epsilon \in D^*$, τέτοιο ὥστε $\beta = \epsilon\alpha$, ὁπότε $h(X) = \epsilon^{-1}g(X)$.*

Ἀπόδειξη. Γιὰ ἁπλούστευση τοῦ συμβολισμοῦ, ἔστω $K = Q(D)$. Κάθε στοιχεῖο τοῦ K εἶναι πηλῖκο στοιχείων τῆς D, ἄρα, ἂν συμβολίσομε μὲ c τὸ γινόμενο τῶν παρονομαστῶν τῶν συντελεστῶν τοῦ $f(X)$, τότε τὸ $c \cdot f(X)$ ἔχει συντελεστὲς στὴ D. Ὁπότε, ἂν τὸ $d \in D$ εἶναι περιεχόμενο τοῦ $c \cdot f(X)$, τότε, ἀπὸ τὴν ἄσκηση 1.16 (β′), τὸ $d^{-1}(c \cdot f(X))$ εἶναι πρωταρχικὸ πολυώνυμο, ἔστω $g(X) \in D[X]$ καὶ $f(X) = \alpha \cdot g(X)$, μὲ $\alpha = c^{-1}d$.

Ἔστω τώρα ὅτι $f(X) = \beta \cdot h(X)$, ὅπου $\beta \in K$ καὶ $h(X) \in D[X]$ πρωταρχικό. Θεωροῦμε $e \in D$, τέτοιο ὥστε $e\alpha = d_1 \in D$ καὶ $e\beta = d_2 \in D$. Προφανῶς $d_1 g(X) = d_2 h(X)$. Ἀπὸ τὴν ἄσκηση 1.16 (γ′), τὸ d_1 εἶναι περιεχόμενο τοῦ $d_1 g(X)$ καὶ τὸ d_2 εἶναι περιεχόμενο τοῦ $d_2 h(X)$, ἄρα, τὰ d_1, d_2, ὡς περιεχόμενα τοῦ ἴδιου πολυωνύμου, εἶναι συνεταιρικά (ἄσκηση 1.16 (α′)). Ἔστω $d_2 = \epsilon d_1$, $\epsilon \in D^*$. Τότε, $e\beta = d_2 = \epsilon d_1 = \epsilon e\alpha$, ἄρα $\beta = \epsilon\alpha$.

□

Θεώρημα 1.13 *Τὸ γινόμενο πρωταρχικῶν πολυωνύμων εἶναι πρωταρχικὸ πολυώνυμο.*

Ἀπόδειξη. Ἔστω

$$(a_m X^m + \cdots + a_1 X + a_0) \cdot (b_n X^n + \cdots + b_1 X + b_0) = c_\ell X^\ell + \cdots c_1 X + c_0, \quad \ell = m + n, \quad (1.7)$$

ὅπου $a_m b_n c_\ell \neq 0$ (συνεπῶς, $\ell = m + n$) καὶ οἱ δύο παράγοντες (πολυώνυμα) στὸ ἀριστερὸ μέλος εἶναι πρωταρχικὰ πολυώνυμα τῆς $D[X]$. Θὰ δείξομε ὅτι καὶ τὸ πολυώνυμο στὸ δεξιὸ μέλος εἶναι πρωταρχικό. Ἂν δὲν ἦταν, θὰ ὑπῆρχε πρῶτο στοιχεῖο p, ποὺ θὰ διαιροῦσε ὅλους τοὺς συντελεστὲς στὸ πολυώνυμο τοῦ ἀριστεροῦ μέλους τῆς (1.7), ἄρα καὶ ὅλους τοὺς συντελεστὲς τοῦ πολυωνύμου, ποὺ θὰ προκύψει ἂν κάνομε τὸν πολλαπλασιασμὸ στὸ δεξιὸ μέλος τῆς (1.7). Κατ' ἀρχάς, παρατηροῦμε ὅτι τὸ p δὲν μπορεῖ νὰ διαιρεῖ ὅλα τὰ a_i, διότι $1 = \text{μκδ}(a_0, \ldots, a_m)$· ὁμοίως καὶ γιὰ τὰ b_i. Ἄρα, ὑπάρχουν δεῖκτες μ καὶ ν, τέτοιοι ὥστε

$$0 \leq \mu \leq m, \quad p \nmid a_\mu \ \ \& \ \ p | a_i \ \ \text{ἂν } i < \mu$$
$$0 \leq \nu \leq n, \quad p \nmid b_\nu \ \ \& \ \ p | b_j \ \ \text{ἂν } j < \nu.$$

Ἐξισώνοντας τοὺς συντελεστὲς τοῦ $X^{\mu+\nu}$ στὰ δύο μέλη τῆς (1.7) παίρνομε τὴ σχέση

$$c_{\mu+\nu} = \sum_{i+j=\mu+\nu} a_i b_j, \quad (1.8)$$

τὸ ἀριστερὸ μέλος τῆς ὁποίας εἶναι, προφανῶς, διαιρετὸ ἀπ' τὸ p. Ἄρα καὶ τὸ δεξιὸ μέλος πρέπει νὰ διαιρεῖται ἀπὸ τὸ p. Ὅμως, παρατηροῦμε τὰ ἑξῆς: Ἂν $i < \mu$, τότε $p | a_i$, ἄρα

$p|a_ib_j$. Ἂν, $i > \mu$, τότε $j < \nu$ (διότι $i + j = \mu + \nu$), ὁπότε $p|b_j$, ἄρα $p|a_ib_j$. Ἂν, τέλος, $i = \mu$, ὁπότε $j = \nu$, τότε $p \nmid a_i$ καὶ $p \nmid b_j$, ἄρα $p \nmid a_ib_j$. Ἔτσι, στὸ ἄθροισμα τοῦ δεξιοῦ μέλους τῆς (1.8), ὁ p δὲν διαιρεῖ τὸν ὅρο $a_\mu b_\nu$, ἐνῶ διαιρεῖ ὅλους τοὺς ὑπόλοιπους προσθετέους. Συνεπῶς, ὁ p δὲν διαιρεῖ τὸ δεξιὸ μέλος· ἄτοπο.

□

Θεώρημα 1.14 [9] *Τὸ πολυώνυμο $f(X) \in D[X]$ εἶναι ἀνάγωγο στοιχεῖο τῆς περιοχῆς $D[X]$, ἂν καὶ μόνο ἄν, ἢ τὸ $f(X)$ εἶναι σταθερό, ἴσο μὲ ἀνάγωγο στοιχεῖο τῆς D, ἢ τὸ $f(X)$ εἶναι μὴ σταθερὸ πρωταρχικὸ πολυώνυμο, τὸ ὁποῖο, ὡς πολυώνυμο τοῦ $Q(D)[X]$,[10] εἶναι ἀνάγωγο πάνω ἀπ' τὸ σῶμα $Q(D)$.*

Ἀπόδειξη. Γιὰ ἁπλοποίηση τοῦ συμβολισμοῦ, ἂς θέσομε $Q(D) = K$.

($\Leftarrow$) Ἂν $f(X) = p$, ὅπου p εἶναι ἀνάγωγο στοιχεῖο τῆς D, τότε τὸ $f(X)$ εἶναι ἀνάγωγο καὶ ὡς στοιχεῖο τῆς $D[X]$, σύμφωνα μὲ τὴν ἄσκηση 1.8. Ἂν, πάλι, τὸ $f(X)$ εἶναι μὴ σταθερὸ πρωταρχικὸ πολυώνυμο τοῦ $D[X]$, ἀνάγωγο πάνω ἀπ' τὸ K, τότε ἀποκλείεται νὰ εἶναι τὸ $f(X)$ γινόμενο δύο μὴ σταθερῶν πολυωνύμων τοῦ $D[X]$. Ἀποκλείεται, ἐπίσης, ἡ περίπτωση $f(X) = c \cdot g(X)$ μὲ $g(X) \in D[X]$ καὶ $c \in D$ ὄχι μονάδα, διότι, τότε, ὅλοι οἱ συντελεστὲς τοῦ $f(X)$ θὰ ἦταν πολλαπλάσια τοῦ c, ἄρα δὲν θὰ ἦταν πρῶτοι μεταξύ τους, ποὺ ἀντιβαίνει στὴν ὑπόθεση πρωταρχικότητας τοῦ $f(X)$. Συνεπῶς, καὶ στὶς δύο περιπτώσεις, τὸ $f(X)$ εἶναι ἀνάγωγο στοιχεῖο τῆς περιοχῆς $D[X]$.

($\Rightarrow$) Τώρα ὑποθέτομε ὅτι τὸ $f(X)$ εἶναι ἀνάγωγο στοιχεῖο τῆς $D[X]$. Ἂν εἶναι σταθερὸ πολυώνυμο, ἔστω $f(X) = c \in D$, τότε τὸ c εἶναι, ὑποχρεωτικά, ἀνάγωγο στοιχεῖο τῆς D. Διότι, ἂν ἦταν $c = ab$ μὲ τὰ $a, b \in D$ ὄχι μονάδες, τότε τὰ a, b μποροῦμε νὰ τὰ δοῦμε καὶ ὡς μὴ ἀντιστρέψιμα στοιχεῖα τῆς περιοχῆς $D[X]$, ἄρα θὰ εἴχαμε μὴ τετριμμένη ἀνάλυση τοῦ $c = f(X)$ στὴν περιοχὴ $D[X]$· ἀντίφαση.
Ἔστω τώρα ὅτι τὸ $f(X)$ δὲν εἶναι σταθερό. Βλέποντας τὸ $f(X)$ ὡς πολυώνυμο τοῦ $K[X]$, τὸ ἀναλύομε σὲ ἀνάγωγα πολυώνυμα τοῦ $K[X]$, ἔστω $f(X) = q_1(X) \cdots q_m(X)$ ($m \geq 1$). Βάσει τοῦ Λήμματος 1.12, γιὰ κάθε $i = 1, \ldots, m$, ἔχομε $q_i(X) = \alpha_i \cdot g_i(X)$, ὅπου $\alpha_i \in K$ καὶ $g_i(X)$ πρωταρχικὸ πολυώνυμο τῆς $D[X]$. Θέτοντας τώρα $g(X) = g_1(X) \cdots g_m(X)$, ἔχομε, ἀπὸ τὸ Θεώρημα 1.13, ὅτι τὸ $g(X)$ εἶναι πρωταρχικὸ πολυώνυμο τῆς $D[X]$. Θέτοντας, ἐπίσης, $\alpha_1 \cdots \alpha_m = \alpha$, ὁδηγούμαστε στὴ σχέση $1 \cdot f(X) = \alpha \cdot g(X)$, μὲ τὰ $f(X), g(X)$ πρωταρχικά. Ἄρα, τὸ Λῆμμα 1.12 μᾶς ὁδηγεῖ στὸ συμπέρασμα ὅτι $\alpha = \epsilon \in D^*$ καί, συνεπῶς, $f(X) = \epsilon g(X) = \epsilon g_1(X) \cdots g_m(X)$. Ὅμως, τὰ πολυώνυμα στὸ δεξιὸ μέλος ἀνήκουν στὴ $D[X]$, ἐνῶ τὸ $f(X)$ ἔχει ὑποτεθεῖ ἀνάγωγο στοιχεῖο τῆς $D[X]$. Ἀναγκαστικά, λοιπόν, $m = 1$ καὶ $f(X) = \epsilon g_1(X)$. Καθὼς $g_1(X) = \alpha_1^{-1} q_1(X)$ μὲ τὸ $q_1(X)$ ἀνάγωγο στὸ $K[X]$, ἕπεται ὅτι καὶ τὸ $g_1(X)$ εἶναι ἀνάγωγο στὸ $K[X]$, ἄρα, τελικά, τὸ $f(X)$ θεωρούμενο ὡς πολυώνυμο τοῦ $K[X]$, εἶναι ἀνάγωγο.

□

Τελειώνομε αὐτὴ τὴν ἑνότητα μὲ τὸ παρακάτω πολὺ σημαντικὸ θεώρημα.

Θεώρημα 1.15 *Ἂν D εἶναι περιοχὴ μονοσήμαντης ἀνάλυσης καὶ $X, Y, Z, \ldots$ εἶναι πεπερασμένες τὸ πλῆθος μεταβλητές, τότε $D[X, Y, Z, \ldots]$ εἶναι περιοχὴ μονοσήμαντης ἀνάλυσης.*

Ἀπόδειξη. Ἀποδεικνύομε ὅτι ἡ $D[X]$ εἶναι περιοχὴ μονοσήμαντης ἀνάλυσης: Κατ' ἀρχάς, γιὰ ἁπλοποίηση τοῦ συμβολισμοῦ, θέτομε $K = Q(D)$.

[9] Στὴ βιβλιογραφία, κάποιες φορές, αὐτὸ τὸ θεώρημα ἀναφέρεται ὡς Λῆμμα τοῦ Gauss.
[10] Ὑπενθυμίζομε ὅτι $Q(D)$ συμβολίζει τὸ σῶμα πηλίκων τῆς D.

Ἔστω $f(X) \in D[X]$, ὄχι μονάδα τῆς $D[X]$. Ἂν τὸ $f(X)$ εἶναι σταθερό, τότε $f(X) = c \in D \setminus D^*$, ἄρα τὸ c ἀναλύεται μονοσήμαντα σὲ ἀνάγωγα στοιχεῖα τῆς D (ἄρα, ἀνάγωγα στοιχεῖα καὶ τῆς $D[X]$). Ἔστω τώρα ὅτι τὸ $f(X)$ δὲν εἶναι σταθερὸ καὶ $d \in D$ τὸ περιεχόμενό του. Τότε, ἀπὸ τὴν ἄσκηση 1.16 (β′), τὸ $d^{-1}f(X)$ εἶναι κάποιο πρωταρχικὸ πολυώνυμο, ἔστω $g(X) \in D[X]$. Τώρα ἔχομε $f(X) = d \cdot g(X)$ καὶ ἔστω $g(X) = p_1(X) \cdots p_m(X)$ ἡ ἀνάλυση τοῦ $g(X)$ σὲ ἀνάγωγα πολυώνυμα τοῦ $K[X]$. Γιὰ κάθε $i = 1, \ldots, m$, ὑπάρχει $k_i \in K$ καὶ πρωταρχικὸ πολυώνυμο $h_i(X) \in D[X]$, ἔτσι ὥστε $p_i(X) = k_i h_i(X)$ (βλ. Λῆμμα 1.12) καί, βεβαίως, ἀφοῦ τὸ $p_i(X)$ εἶναι ἀνάγωγο πολυώνυμο τοῦ $K[X]$, τὸ ἴδιο ἰσχύει καὶ γιὰ τὸ $h_i(X)$. Καταλήγομε ἔτσι στὴ σχέση

$$g(X) = k \cdot h(X) \quad \text{ὅπου} \quad k = k_1 \cdots k_m, \quad h(X) = h_1(X) \cdots h_m(X)$$

καὶ παρατηροῦμε ὅτι τὸ $h(X) \in D[X]$ εἶναι πρωταρχικὸ πολυώνυμο, λόγῳ τοῦ Θεωρήματος 1.13. Ἀλλὰ καὶ τὸ $g(X) \in D[X]$ εἶναι πρωταρχικὸ καὶ $1 \cdot g(X) = k \cdot h(X)$. Ἀπὸ τὸ Λῆμμα 1.12 ἕπεται τώρα ὅτι $k = 1 \cdot \epsilon$, γιὰ κάποια μονάδα ϵ τῆς D, δηλαδή, $k = \epsilon \in D^*$. Τελικά,

$$f(X) = c \cdot g(X) = \epsilon c \cdot h_1(X) \cdots h_m(X). \tag{1.9}$$

Καθὼς τὰ $h_1(X), \ldots, h_m(X)$ εἶναι πρωταρχικὰ πολυώνυμα τῆς $D[X]$ καὶ εἶναι ἀνάγωγα στὸ $K[X]$, συμπεραίνομε, βάσει τοῦ Θεωρήματος 1.14, ὅτι αὐτὰ εἶναι ἀνάγωγα στοιχεῖα τῆς ἀκέραιας περιοχῆς $D[X]$. Ἀναλύοντας τώρα καὶ τὸ c σὲ ἀνάγωγα στοιχεῖα τῆς D, παίρνομε ἀπὸ τὴν (1.9) μιὰ ἀνάλυση τοῦ $f(X)$ σὲ ἀνάγωγα στοιχεῖα τῆς $D[X]$.

Ἡ μοναδικότητα τῆς ἀνάλυσης: Ἔστω

$$f(X) = q_1 \cdots q_n \cdot h_1(X) \cdots h_m(X) \quad \text{καὶ} \quad f(X) = q'_1 \cdots q'_\nu \cdot h'_1(X) \cdots h'_\mu(X),$$

ὅπου τὰ $q_1, \ldots, q_n$ καὶ τὰ $q'_1, \ldots, q'_\nu$ εἶναι ἀνάγωγα στοιχεῖα τῆς D καὶ ὅλα τὰ πολυώνυμα $h_1(X), \ldots, h_m(X)$ καὶ $h'_1(X), \ldots h'_\mu(X)$ εἶναι ἀνάγωγα στοιχεῖα τῆς ἀκέραιας περιοχῆς $D[X]$. Τοῦτο τὸ τελευταῖο σημαίνει, βάσει τοῦ Θεωρήματος 1.14, ὅτι αὐτὰ τὰ πολυώνυμα εἶναι πρωταρχικὰ καὶ ἀνάγωγα στὸ $K[X]$, ὁπότε καὶ τὰ γινόμενα $h_1(X) \cdots h_m(X)$ καὶ $h'_1(X) \cdots h'_\mu(X)$ εἶναι πρωταρχικά. Ἀλλὰ τότε, τὸ Λῆμμα 1.12 μᾶς λέει ὅτι $q'_1 \cdots q'_\nu = \epsilon q_1 \cdots q_n$, γιὰ κάποιο $\epsilon \in D^*$, καὶ

$$h_1(X) \cdots h_m(X) = \epsilon \cdot h'_1(X) \cdots h'_\mu(X) \tag{1.10}$$

Δεδομένου ὅτι ἡ D εἶναι περιοχὴ μονοσήμαντης ἀνάλυσης, ἡ σχέση $q'_1 \cdots q'_\nu = \epsilon q_1 \cdots q_n$ μᾶς ὁδηγεῖ στὸ συμπέρασμα ὅτι $\nu = n$ καί, δίχως βλάβη τῆς γενικότητας, τὰ $q'_1, \ldots, q'_m$ εἶναι ἕνα πρὸς ἕνα συνεταιρικὰ μὲ τὰ $q_1, \ldots, q_m$.
Μένει νὰ δείξομε ὅτι κάτι ἀνάλογο συμβαίνει καὶ μὲ τὰ πολυώνυμα $h_i(X)$ καὶ $h'_j(X)$.

Βλέποντας τὴν (1.10) ὡς σχέση στὸ $K[X]$ καὶ γνωρίζοντας ἀπὸ τὴ βασικὴ Ἄλγεβρα ὅτι στὸ $K[X]$ ἰσχύει ἡ μονοσήμαντη ἀνάλυση σὲ ἀνάγωγα πολυώνυμα, συμπεραίνομε ὅτι, $\mu = m$ καί, δίχως βλάβη τῆς γενικότητας, $h'_i(X) = k_i \cdot h_i(X)$ ($k_i \in K$) γιὰ κάθε $i = 1, \ldots, m$. Πάλι ἐφαρμόζοντας τὸ Λῆμμα 1.12 συμπεραίνομε ὅτι $k_i = \epsilon'_i \epsilon_i$ μὲ $\epsilon'_i \in D^*$, ἄρα $k_i \in D^*$. Αὐτὸ σημαίνει ὅτι, γιὰ κάθε $i = 1, \ldots, m$, τὸ $h'_i(X)$, ὡς στοιχεῖο τῆς $D[X]$, εἶναι συνεταιρικὸ μὲ τὸ $h_i(X)$.

Καταλήξαμε, λοιπόν, στὸ συμπέρασμα ὅτι

> *Ἂν ἡ D εἶναι περιοχὴ μονοσήμαντης ἀνάλυσης, τότε τὰ πολυώνυμα μιᾶς μεταβλητῆς πάνω ἀπὸ τὴ D εἶναι περιοχὴ μονοσήμαντης ἀνάλυσης.*

Ἐφαρμόζοντας τὸ παραπάνω συμπέρασμα, θέτοντας στὴ θέση τῆς D τὴ $D[X]$ καὶ παίρνοντας ὡς μεταβλητὴ τῶν πολυωνύμων πάνω ἀπὸ τὴ $D[X]$ τὴ μεταβλητὴ Y, συμπεραίνομε ὅτι καὶ ἡ $(D[X])[Y]$, δηλαδή, ἡ $D[X,Y]$, εἶναι περιοχὴ μονοσήμαντης ἀνάλυσης. Ἐπαναλαμβάνοντας μὲ τὴ $D[X,Y]$ στὴ θέση τῆς D καὶ μὲ τὸ Z ὡς μεταβλητὴ τῶν πολυωνύμων πάνω ἀπὸ τὴ $D[X,Y]$, συμπεραίνομε ὅτι καὶ ἡ $D[X,Y,Z]$ εἶναι περιοχὴ μονοσήμαντης ἀνάλυσης κ.ο.κ.

□

Ἄσκηση 1.17 Ἀναλῦστε τὸ $X^4-X^3+3X^2-2X+2 \in \mathbb{Q}[X]$ σὲ γινόμενο δύο δευτεροβαθμίων μονικῶν πολυωνύμων μὲ ἀκέραιους συντελεστές, τὰ ὁποῖα εἶναι ἀνάγωγα πολυώνυμα τοῦ $\mathbb{Q}[X]$.

Στὴ συνέχεια, ἔστω $f(X) = 12(X^4 - X^3 + 3X^2 - 2X + 2) \in \mathbb{Q}[X]$. Ἀναλῦστε τὸ $f(X)$ σὲ ἀνάγωγα στοιχεῖα τῆς περιοχῆς $D[X]$, ὑπὸ τὴ μορφὴ

$$f(X) = \epsilon \cdot \text{γινόμενο ἀναγώγων τῆς } D \cdot \text{γινόμενο μὴ σταθερῶν ἀναγώγων τῆς } D[X],$$

ὅπου $\epsilon \in D^*$, σὲ κάθε μία ἀπ' τὶς παρακάτω περιπτώσεις:
(i) $D = \mathbb{Z}$. (ii) $D = \mathbb{Q}$. (iii) $D = \mathbb{Z}[i\sqrt{2}]$. (iv) $D = \mathbb{Z}[\omega]$, μὲ τὸ ω ὅπως στὴν ἄσκηση 1.18.

Γιὰ τὴν περίπτωση (iii): Θεωρῆστε δεδομένο ὅτι ἡ D εἶναι περιοχὴ μονοσήμαντης ἀνάλυσης. Πρὶν προχωρήσετε στὴν ἀνάλυση τοῦ $f(X)$, ἀποδεῖξτε ὅτι τὰ $i\sqrt{2}, 1+i\sqrt{2}, 1-i\sqrt{2}$ εἶναι ἀνάγωγα στοιχεῖα τῆς D καὶ ἀναλῦστε τὸ 2 καὶ τὸ 3 σὲ ἀνάγωγα τῆς D. Ἀποδεῖξτε ὅτι τὸ $X^2 - X + 1$ δὲν ἔχει ρίζες στὴ D.

Γιὰ τὴν περίπτωση (iv): Θεωρῆστε δεδομένο ὅτι ἡ D εἶναι περιοχὴ μονοσήμαντης ἀνάλυσης. Θεωρῆστε δεδομένα τὰ (α′) καὶ (β′) τῆς ἀσκήσεως 1.18. Πρὶν προχωρήσετε στὴν ἀνάλυση τοῦ $f(X)$, ἀποδεῖξτε ὅτι τὰ 2 καὶ $1-\omega$ εἶναι ἀνάγωγα στοιχεῖα τῆς D καὶ παρατηρῆστε ὅτι $3 = -\omega^2(1-\omega)^2$. Ἀποδεῖξτε ὅτι τὸ X^2+2 δὲν ἔχει ρίζες στὴ D.

I.6 Ευκλειδειες περιοχες

Ὁρισμός. Ἡ ἀκέραια περιοχὴ E λέγεται *εὐκλείδεια* ἂν ὑπάρχει ἀπεικόνιση

$$\mathrm{N} : E \setminus \{0\} \to \mathbb{N}_0,$$

μὲ τὶς ἑξῆς ἰδιότητες:

1. Ἂν τὰ $a, b \in E$ εἶναι μὴ μηδενικὰ καὶ $a|b$, τότε $\mathrm{N}(a) \leq \mathrm{N}(b)$.
2. Ἂν $a, b \in E$ καὶ $b \neq 0$, τότε ὑπάρχουν $q, r \in E$, τέτοια ὥστε $a = bq + r$ καὶ εἴτε $r = 0$ εἴτε $\mathrm{N}(r) < \mathrm{N}(b)$.

Ἡ ἀπεικόνιση N λέγεται *στάθμη*.

Πρόταση 1.16 *Ἔστω E εὐκλείδεια περιοχὴ στάθμης* N.
(α′) *Ἂν τὰ $a, b \in E$ εἶναι μὴ μηδενικά, $a|b$ καὶ $\mathrm{N}(a) = \mathrm{N}(b)$, τότε τὰ a, b εἶναι συνεταιρικά.*
(β′) *Ἡ E εἶναι περιοχὴ ἀνάλυσης.*
(γ′) *Ἡ E εἶναι περιοχὴ κυρίων ἰδεωδῶν.*

Ἀπόδειξη. *(α΄)* Ἔστω ὅτι $a = bq + r$, μὲ τὰ q, r ὅπως προβλέπονται ἀπὸ τὸν Ὁρισμὸ 1.6. Ἂν $r = 0$, τότε $b|a$. Ἐξ ὑποθέσεως, ὅμως, ἰσχύει καὶ $a|b$, ἄρα (ἄσκηση 1.5) τὰ a, b εἶναι συνεταιρικά. Ἂν $r \neq 0$, τότε $\mathrm{N}(r) < \mathrm{N}(b)$. Ἐξ ὑποθέσεως, $b = ac$ γιὰ κάποιο $c \in E$, ὁπότε $a = bq + r = (ac)q + r$, ἀπ' ὅπου $r = a(1 - cq)$. Ἀλλὰ τώρα βλέπομε ὅτι $a|r$, ἄρα $\mathrm{N}(r) \geq \mathrm{N}(a) = \mathrm{N}(b)$, ποὺ ἔρχεται σὲ ἀντίφαση μὲ τὴν $\mathrm{N}(r) < \mathrm{N}(b)$.

(β΄) Ἔστω $\min \mathrm{N}(E) = n_0$.

Ἰσχυρισμός: Ἂν γιὰ κάποιο $a \in E$ εἶναι $\mathrm{N}(a) = n_0$, τότε τὸ a εἶναι μονάδα ἢ ἀνάγωγο στοιχεῖο τῆς E.

Ἀπόδειξη τοῦ ἰσχυρισμοῦ: Ἔστω ὅτι τὸ a δὲν εἶναι μονάδα καὶ ἂς θεωρήσομε ἕνα διαιρέτη b τοῦ a. Θὰ δείξομε ὅτι b εἶναι συνεταιρικὸ στοιχεῖο τοῦ a. Ἀπὸ ἰδιότητα τῆς στάθμης ἔχομε ὅτι $\mathrm{N}(b) \leq \mathrm{N}(a) = n_0$, ἄρα, ἀπ' τὴν ἐπιλογὴ τοῦ n_0, πρέπει νὰ εἶναι $\mathrm{N}(b) = n_0$. Ἔτσι τώρα, $\mathrm{N}(b) = \mathrm{N}(a)$ καὶ $b|a$, ὁπότε, λόγῳ τοῦ (α΄), συμπεραίνομε ὅτι τὸ b εἶναι συνεταιρικὸ τοῦ a.

Τώρα προχωροῦμε στὴν κυρίως ἀπόδειξη τοῦ *(β΄)* ἐπαγωγικά. Λόγῳ τοῦ παραπάνω ἰσχυρισμοῦ, ἡ πρόταση ἰσχύει γιὰ ὅλα τὰ στοιχεῖα τῆς E στάθμης n_0. Ἔστω $n > n_0$ καὶ ἂς ὑποθέσομε ὅτι ὅλα τὰ στοιχεῖα μὲ στάθμη $< n$, ἂν δὲν εἶναι μονάδες, ἀναλύονται σὲ ἀνάγωγα στοιχεῖα. Θεωροῦμε τώρα στοιχεῖο $a \in E$ μὲ $\mathrm{N}(a) = n$. Ἂν τὸ a εἶναι μονάδα ἢ ἀνάγωγο στοιχεῖο, τότε ἔχομε τελειώσει. Στὴν ἀντίθετη περίπτωση, ὑπάρχουν $b, c \in E$, ὄχι συνεταιρικὰ τοῦ a, τέτοια ὥστε $a = bc$. Οἱ σχέσεις $b|a$ καὶ $c|a$ συνεπάγονται, ἀντιστοίχως, $\mathrm{N}(b) \leq \mathrm{N}(a)$ καὶ $\mathrm{N}(c) \leq \mathrm{N}(a)$. Ἂν ἦταν $\mathrm{N}(b) = \mathrm{N}(a)$, τότε, ἀπὸ τὸ *(α΄)* θὰ συμπεραίναμε ὅτι τὰ a, b εἶναι συνεταιρικά· ἀντίφαση. Ἄρα $\mathrm{N}(b) < \mathrm{N}(a) < n$ καὶ ὁμοίως, $\mathrm{N}(c) < \mathrm{N}(a) < n$. Ἀπ' τὴν ἐπαγωγικὴ ὑπόθεση τώρα, καθένα ἀπὸ τὰ b, c ἀναλύεται σὲ γινόμενο ἀναγώγων, ὁπότε καὶ τὸ $bc = a$ ἀναλύεται.

(γ΄) Ἔστω I μὴ μηδενικὸ ἰδεῶδες τῆς E. Θεωροῦμε ἕνα μὴ μηδενικὸ στοιχεῖο $b \in I$, τοῦ ὁποίου ἡ στάθμη εἶναι ἡ ἐλάχιστη δυνατὴ μεταξὺ ὅλων τῶν μὴ μηδενικῶν στοιχείων τοῦ I. Δηλαδή,

$$b \neq 0 \quad \& \quad \mathrm{N}(b) \leq \mathrm{N}(a) \quad \forall\, a \in I \setminus \{0\}. \tag{1.11}$$

Θὰ δείξομε ὅτι $I = bE$. Προφανῶς, ἀφοῦ $b \in I$, ἰσχύει ὅτι $bE \subseteq I$, ὁπότε μένει νὰ δείξομε ὅτι κάθε $a \in I$ εἶναι τῆς μορφῆς bq μὲ $q \in E$. Ἐπειδὴ εἴμαστε σὲ εὐκλείδεια περιοχή, ὑπάρχουν $q, r \in E$, μὲ $a = bq + r$ καί, στὴν περίπτωση ποὺ $r \neq 0$, ἰσχύει $\mathrm{N}(r) \leq \mathrm{N}(b)$. Παρατηροῦμε ὅτι $r = a - bq \in I$, διότι $a \in I$ καὶ $b \in I$. Ἂν, λοιπόν, ἦταν $r \neq 0$, τότε τὸ r θὰ ἦταν ἕνα μὴ μηδενικὸ στοιχεῖο τοῦ I, μὲ στάθμη $< \mathrm{N}(b)$, κάτι ποὺ ἀντιβαίνει στὴν (1.11). Ἄρα $r = 0$ καί, συνεπῶς, $a = bq$.

□

Πόρισμα 1.17 *Κάθε εὐκλείδεια περιοχὴ εἶναι περιοχὴ μονοσήμαντης ἀνάλυσης.*

Ἀπόδειξη. Προφανὴς συνδυασμὸς τῶν (β΄) καὶ (γ΄) τῆς Προτάσεως 1.16 καὶ τοῦ Θεωρήματος 1.6.

□

Παραδείγματα. **1**. Ἡ ἀκέραια περιοχὴ $\mathbb{Z}$ εἶναι εὐκλείδεια, μὲ στάθμη τὴν ἀπεικόνιση

$$\mathbb{Z} \setminus \{0\} \ni a \mapsto |a| \in \mathbb{N}_0.$$

2. Ἂν K εἶναι σῶμα, τότε ἡ ἀκέραια περιοχὴ $K[X]$ εἶναι εὐκλείδεια, μὲ στάθμη τὴν ἀπεικόνιση

$$K[X] \setminus \{0\} \ni f(X) \mapsto \deg f(X) \in \mathbb{N}_0.$$

3. Ἔστω ἡ ἀκέραια περιοχὴ

$$\mathbb{Z}[\sqrt{-2}] = \{a + bi\sqrt{2} : a, b \in \mathbb{Z}\}.$$

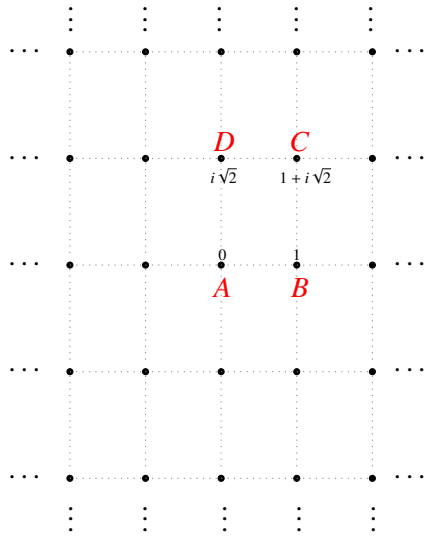
Ἡ ἀπεικόνιση $\mathrm{N} : \mathbb{Z}[\sqrt{-2}] \setminus \{0\} \to \mathbb{N}_0$, ποὺ ὁρίζεται

$$\mathrm{N}(a + bi\sqrt{2}) = |a + bi\sqrt{2}|^2 = a^2 + 2b^2,$$

εἶναι στάθμη καί, συνεπῶς, ἀπὸ τὸ Πόρισμα 1.17, ἡ $\mathbb{Z}[\sqrt{-2}]$ εἶναι περιοχὴ μονοσήμαντης ἀνάλυσης.

Ἀπόδειξη. Ἡ ἰδιότητα (1) τῆς στάθμης εἶναι ἁπλὸ ν' ἀποδειχθεῖ ὅτι ἱκανοποιεῖται ἀπὸ τὴ συγκεκριμένη ἀπεικόνιση N (ἄσκηση).

Γιὰ ν' ἀποδείξομε τὴν ἰδιότητα (2) ἀπεικονίζομε τὰ στοιχεῖα τῆς $\mathbb{Z}[\sqrt{-2}]$ πάνω στὸ μιγαδικὸ ἐπίπεδο. Τὰ στοιχεῖα αὐτὰ εἶναι, ἀκριβῶς, οἱ «κόμβοι» τοῦ παρακάτω πλέγματος:

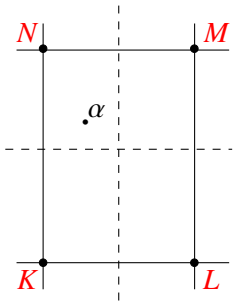


Ἀπεικόνιση τῆς $\mathbb{Z}[\sqrt{-2}]$ στὸ μιγαδικὸ ἐπίπεδο

τὸ ὁποῖο προκύπτει ἀπὸ τὴν *ἐπ' ἄπειρον* ὁριζόντια καὶ κατακόρυφη ἐπανάληψη τοῦ παραλληλογράμμου $ABCD$. Μιὰ προφανὴς παρατήρηση, πολὺ χρήσιμη, ὅμως, εἶναι ὅτι κάθε σημεῖο τοῦ μιγαδικοῦ ἐπιπέδου ἀνήκει σὲ κάποιο ἀπὸ τὰ ὀρθογώνια παραλληλόγραμμα (περιλαμβανομένου καὶ τοῦ περιγράμματός του).

Τώρα θὰ δείξομε ὅτι, ἡ ἀπεικόνιση N, ποὺ ὁρίσαμε πιὸ πάνω, ἱκανοποιεῖ τὴ συνθήκη (2) τοῦ ὁρισμοῦ τῆς στάθμης.

Ἔστω ὅτι $a + bi\sqrt{2}, c + di\sqrt{2} \in E$ μὲ τὸ δεύτερο μὴ μηδενικό. Θεωροῦμε τὸν μιγαδικὸ $\alpha = (a + bi\sqrt{2})/(c + di\sqrt{2})$, ὁ ὁποῖος, σύμφωνα μὲ τὴν παραπάνω παρατήρηση ἀνήκει σ' ἕνα ἀπὸ τὰ παραλληλόγραμμα τοῦ πλέγματος, ἔστω τὸ $KLMN$.



Οἱ μεσοκάθετες τῶν πλευρῶν τοῦ $KLMN$ τὸ χωρίζουν σὲ τέσσερα μικρότερα παραλληλόγραμμα καὶ τὸ α ἀνήκει σ' ἕνα ἀπὸ αὐτά, π.χ. στὸ ἄνω ἀριστερό (βλ. σχῆμα). Ἡ ἀπόσταση τοῦ α ἀπὸ τὸ πλησιέστερο σημεῖο τοῦ δικτυωτοῦ (ποὺ στὸ συγκεκριμένο σχῆμα εἶναι τὸ N) δὲν μπορεῖ νὰ ὑπερβαίνει τὸ μῆκος τῆς διαγωνίου τοῦ ἄνω ἀριστεροῦ «μικροῦ» παραλληλογράμμου, ἡ ὁποία εἶναι τὸ μισὸ τῆς διαγωνίου NL. Ἀλλὰ ἡ διαγώνιος NL ἔχει ἴσο μῆκος μὲ τὸ μῆκος τῆς διαγωνίου BD, τὸ ὁποῖο εἶναι $|1 - i\sqrt{2}| = \sqrt{3}$. Ἄρα, ἡ ἀπόσταση τοῦ σημείου α ἀπὸ τὸ N εἶναι, τὸ πολύ, $\sqrt{3}/2$. Ἀλλὰ τὸ σημεῖο N ἀναπαριστᾶ ἕνα στοιχεῖο τῆς ἀκέραιας περιοχῆς, ἔστω τὸ $u + vi\sqrt{2}$, μὲ $u, v \in \mathbb{Z}$. Συνεπῶς $|u + vi\sqrt{2} - \alpha| \leq \sqrt{3}/2$, ὁπότε

$$\left| \frac{a + bi\sqrt{2}}{c + di\sqrt{2}} - (u + vi\sqrt{2}) \right|^2 \leq \frac{3}{4}.$$

Ἀπαλείφοντας τὸν παρονομαστὴ παίρνομε τὴ σχέση

$$|\, a + bi\sqrt{2} - (c + di\sqrt{2})(u + vi\sqrt{2})\,|^2 \leq \frac{3}{4}|\, c + di\sqrt{2}\,|^2 < |\, c + di\sqrt{2}\,|^2 = \mathrm{N}(c + di\sqrt{2}). \quad (1.12)$$

Προφανῶς, $a + bi\sqrt{2} - (c + di\sqrt{2})(u + vi\sqrt{2}) = r + si\sqrt{2}$ μὲ τὰ $r, s \in \mathbb{Z}$.
Ἂν $r + si\sqrt{2} = 0$, τότε $a + bi\sqrt{2} = (c + di\sqrt{2})(u + vi\sqrt{2})$.
Ἂν $r + si\sqrt{2} \neq 0$, τότε, ἀπὸ τὴ σχέση (1.12), βλέπομε ὅτι

$$a + bi\sqrt{2} = (c + di\sqrt{2})(u + vi\sqrt{2}) + (r + si\sqrt{2}), \quad \mathrm{N}(r + si\sqrt{2}) < \mathrm{N}(c + di\sqrt{2}).$$

□

Ἄσκηση 1.18 Ἔστω $\omega = (-1 + i\sqrt{3})/2 \in \mathbb{C}$.
(α') Ἀποδεῖξτε ὅτι ω εἶναι ρίζα τοῦ $X^2 + X + 1$ (ἄρα $\omega^3 = 1$) καὶ ἡ δεύτερη ρίζα τοῦ πολυωνύμου αὐτοῦ εἶναι ἡ ω^2. Συμπεράνατε ὅτι ὁ μιγαδικὸς συζυγὴς τοῦ ω εἶναι ὁ ω^2.
(β') Ἀποδεῖξτε ὅτι οἱ μονάδες τῆς ἀκέραιας περιοχῆς $\mathbb{Z}[\omega] = \{a + b\omega : a, b \in \mathbb{Z}\}$ εἶναι οἱ $\pm 1, \pm\omega, \pm\omega^2$.
(γ') Ἀποδεῖξτε ὅτι ἡ ἀπεικόνιση $\mathrm{N} : \mathbb{Z}[\omega] \setminus \{0\} \to \mathbb{N}_0$, ποὺ ὁρίζεται

$$\mathrm{N}(a + b\omega) = |a + b\omega|^2 = (a + b\omega)(a + b\omega^2) = a^2 - ab + b^2,$$

εἶναι στάθμη.
Ὑπόδειξη. Μιμηθῆτε τὴν ἀπόδειξη τοῦ παραπάνω παραδείγματος 3. Αὐτὴ τὴ φορά, τὸ πλέγμα ποὺ θὰ θεωρήσετε, παράγεται ἀπὸ τὴν ἐπανάληψη τοῦ πλαγίου παραλληλογράμμου $ABCD$, ὅπου τώρα οἱ κορυφές του ἔχουν συντεταγμένες 0, 1, $1 + \omega$, ω.

Πρόταση 1.18 *Οἱ μόνες ἀκέραιες λύσεις τῆς ἐξίσωσης*

$$x^2 + 2 = y^3 \quad (1.13)$$

εἶναι οἱ $(x, y) = (\pm 5, 3)$.

Ἀπόδειξη. Ἔστω (x, y) ἀκέραια λύση τῆς (1.13). Τότε ὁ x εἶναι περιττός. Διότι, ἂν ἦταν ἄρτιος, θὰ ἦταν ἄρτιος καὶ ὁ y, ὁπότε θὰ εἴχαμε $x = 2x_1$ καὶ $y = 2y_1$ $(x_1, y_1 \in \mathbb{Z})$ καὶ ἡ ἐξίσωσή μας θὰ ἔπαιρνε τὴ μορφὴ $4x_1^2 + 2 = 8y_1^3$. Αὐτό, ὅμως, εἶναι ἄτοπο, διότι τὸ ἀριστερὸ μέλος τῆς τελευταίας σχέσης δὲν διαιρεῖται ἀπ' τὸ 4, ἐνῶ τὸ δεξιὸ μέλος της διαιρεῖται ἀπὸ τὸ 8. Στὸ ἑξῆς, λοιπόν, ὁ x εἶναι περιττός.

Ἡ ἐξίσωση (1.13) γράφεται

$$(x + i\sqrt{2})(x - i\sqrt{2}) = y^3. \tag{1.14}$$

Ἀποδεικνύομε τώρα ὁτι οἱ παράγοντες στὸ ἀριστερὸ μέλος εἶναι πρῶτοι μεταξύ τους (δηλαδή, ἀποδεικνύομε τὴν ἄσκηση 1.11). Ἂν δ˜εν ἦταν, θὰ ὑπῆρχε ἕνα ἀνάγωγο στοιχεῖο $\pi\mathbb{Z}[\sqrt{-2}]$, ποὺ θὰ διαιροῦσε τὸ $x + i\sqrt{2}$ καὶ τὸ $x - i\sqrt{2}$. Τότε, ὅμως, τὸ π θὰ διαιροῦσε κα' τὸ ἄθροισμά τους, ποὺ εἶναι $2i\sqrt{2} = -(i\sqrt{2})^3$. Καθὼς εἴμαστε σὲ περιοχὴ μονοσήμαντης ἀνάλυσης, τὸ ἀνάγωγο π εἶναι καὶ πρῶτο, ἄρα, ἀπὸ τὴ σχέση $\pi|-(i\sqrt{2})^3$ συμπεραίνομε ὅτι $\pi|i\sqrt{2}$. Ὅμως καὶ τὸ $i\sqrt{2}$ εἶναι ἀνάγωγο (ἄσκηση 1.11 (β′)), ἄρα οἱ μόνοι πρῶτοι διαιρέτες τοῦ εἶναι τὰ συνεταιρικά του στοιχεῖα. Συνεπῶς, τὸ π εἶναι συνεταιρικὸ τοῦ $i\sqrt{2}$ καὶ διαιρεῖ τὸ $x + i\sqrt{2}$. Ἄρα, τὸ $i\sqrt{2}$ διαιρεῖ τὸ $x + i\sqrt{2}$, ἄρα διαιρεῖ καὶ τὸ $(x + i\sqrt{2}) - i\sqrt{2} = x$. Αὐτὸ σημαίνει ὅτι ὑπάρχει $a + bi\sqrt{2} \in E$, τέτοιο ὥστε $x = i\sqrt{2}(a + bi\sqrt{2}) = -2b + ai\sqrt{2}$. Ἡ τελευταία σχέση συνεπάγεται $a = 0$ καὶ $x = -2b$, ποὺ ἀντιβαίνει στὸ γεγονὸς ὅτι ὁ x εἶναι περιττός.

Ξέροντας τώρα ὅτι οἱ παράγοντες στὸ ἀριστερὸ μέλος τῆς (1.14) εἶναι πρῶτοι μεταξύ τους, ἐφαρμόζομε τὴν Πρόταση 1.11 καὶ συμπεραίνομε ὅτι,

$$x + i\sqrt{2} = (a + bi\sqrt{2})^3,$$

ὅπου $a, b \in \mathbb{Z}$. Ἀναπτύσσοντας τὸ δεξιὸ μέλος καὶ ἐξισώνοντας πραγματικὰ καὶ φανταστικὰ μέρη στὰ δύο μέλη, παίρνομε

$$1 = 3a^2b - 2b^3, \quad x = a^3 - 6ab^2.$$

Ἀπὸ τὴν πρώτη σχέση, $(3a^2 - 2b^2)b = 1$, ἄρα $3a^2 - 2b^2 = b = \pm 1$, ἀπ' ὅπου $a, b \in \{-1, 1\}$ καὶ $x = a^3 - 6ab^2 \in \{-5, 5\}$.

□

Κεφάλαιο 2

Ἐφαρμογὲς τῶν Ἰδεωδῶν

2.1 Ὑπαρξη ριζων πολυωνυμου

Πρὶν προχωρήσετε στὰ παρακάτω, μελετῆστε τὰ εἰσαγωγικὰ τῆς ἑνότητας 2.10, μέχρι καὶ τὸ Πόρισμα 2.10.7, τοῦ βιβλίου [1].

Πρόταση 2.1 *Ἔστω σῶμα K καὶ $p(X) \in K[X]$ ἀνάγωγο. Τότε τὸ ἰδεῶδες $\langle p(X)\rangle$ εἶναι μεγιστικὸ ἰδεῶδες τοῦ $K[X]$.*

Ἀπόδειξη. Ἔστω I ἰδεῶδες τοῦ $K[X]$, ποὺ περιέχει τὸ $\langle p(X)\rangle$. Εἶναι γνωστὸ ὅτι τὰ ἰδεώδη τοῦ $K[X]$ εἶναι κύρια, ἄρα ὑπάρχει $f(X) \in K[X]$, τέτοιο ὥστε $I = \langle f(X)\rangle$. Σύμφωνα μὲ τὸν ὁρισμὸ τοῦ μεγιστικοῦ ἰδεώδους, πρέπει καὶ ἀρκεῖ νὰ δείξομε ὅτι τὸ $\langle f(X)\rangle$ εἶναι ἴσο ἢ μὲ τὸ $\langle p(X)\rangle$, ἢ μὲ ὁλόκληρο τὸν δακτύλιο $K[X]$.

Ἐπειδὴ τὸ $p(X)$ εἶναι ἀνάγωγο, τὸ $f(X)$ ἢ εἶναι πολλαπλάσιο τοῦ $p(X)$, ἢ εἶναι πρῶτο πρὸς τὸ $p(X)$. Ἂν συμβαίνει τὸ πρῶτο, τότε $f(X) \in \langle p(X)\rangle$, ἄρα $I = \langle f(X)\rangle \subseteq \langle p(X)\rangle$. Ἐξ ὑποθέσεως, ὅμως, $\langle p(X)\rangle \subseteq I$, ἄρα $I = \langle p(X)\rangle$. Ἂν συμβαίνει τὸ δεύτερο, τότε ὑπάρχουν $h_1(X), h_2(X) \in K[X]$, τέτοια ὥστε $h_1(X)f(X) + h_2(X)p(X) = 1$. Τὸ ἀριστερὸ μέλος ἀνήκει στὸ I, ἀφοῦ $f(X), p(X) \in I$, ἄρα $1 \in I$. Τότε, ὅμως, γιὰ κάθε $g(X) \in K[X]$ ἔχομε ὅτι $g(X) \cdot 1 \in I$, ἄρα ὅλα τὰ πολυώνυμα τοῦ $K[X]$ ἀνήκουν στὸ I, ὁπότε $I = K[X]$.

□

Θεώρημα 2.2 *Ἔστω K σῶμα καὶ $p(X) \in K[X]$ ἀνάγωγο, βαθμοῦ n. Τότε ὑπάρχει σῶμα L, ποὺ περιέχει ὡς ὑπόσωμά του τὸ K, καὶ $u \in L$, ἔτσι ὥστε:*

- $p(u) = 0$.
- $L = \{c_0 + c_1u + \cdots + c_{n-1}u^{n-1} | c_0, c_1, \ldots c_{n-1} \in K\}$.

Ἀπόδειξη. Ἀπὸ τὴν Πρόταση 2.1, τὸ ἰδεῶδες $\langle p(X)\rangle$ εἶναι μεγιστικό, ἄρα ὁ δακτύλιος-πηλίκο $L = K[X]/\langle p(X)\rangle$ εἶναι σῶμα (βλ. Θεώρημα 2.10.6 τοῦ [1]. Γιὰ νὰ ἐλαφρύνομε τὸν συμβολισμό, θέτομε $\langle p(X)\rangle = I$.

Θεωροῦμε τὸν ὁμομορφισμὸ σωμάτων $K \ni c \mapsto c + I \in K/I = L$. Εἶναι ἁπλούστατο ν' ἀποδείξει κανεὶς ὅτι αὐτὴ ἡ ἀπεικόνιση εἶναι *μονο*μορφισμός, ἄρα, τὸ L περιέχει ἕνα ἰσόμορφο ἀντίγραφο τοῦ K. Συνεπῶς, ὅπως ἔχομε ἐξηγήσει στὸ μάθημα, μποροῦμε νὰ θεωρήσομε ὅτι τὸ K περιέχεται στὸ L καὶ νὰ ταυτίσομε κάθε στοιχεῖο $c \in K$ μὲ τὸ $c + I \in L$.

Τὴ μεταβλητὴ τῶν πολυωνύμων μὲ συντελεστὲς ἀπὸ τὸ L τὴ συμβολίζομε μὲ Y, πρὸς ἀποφυγὴ συγχύσεως. Ἄρα, ἂν τὸ $p(X) = (\text{ἔστω})\, a_0 + a_1X + \cdots + a_nX^n \in K[X]$ τὸ βλέπομε ὡς πολυώνυμο πάνω ἀπὸ τὸ L, θὰ τὸ γράφομε

$$p(Y) = (a_0 + I) + (a_1 + I)Y + (a_2 + I)Y^2 + \cdots + (a_n + I)Y^n.$$

Τὸ στοιχεῖο $X + I \in L$ τὸ συμβολίζομε u καὶ ὑπολογίζομε:

$$\begin{aligned} p(u) &= (a_0 + I) + (a_1 + I)(X + I) + (a_2 + I)(X + I)^2 + \cdots + (a_n + I)(X + I)^n \\ &= (a_0 + I) + (a_1 + I)(X + I) + (a_2 + I)(X^2 + I) + \cdots + (a_n + I)(X^n + I) \\ &= (a_0 + I) + (a_1X + I) + (a_2X^2 + I) + \cdots + (a_nX^n + I) \\ &= (a_0 + a_1X + a_2X^2 + \cdots + a_nX^n) + I = p(X) + I = 0 + I = 0_L \end{aligned}$$

(εἶναι $p(X) + I = 0 + I$ διότι $p(X) \in \langle p(X)\rangle = I$), ἄρα τὸ $u \in L$ εἶναι ρίζα τοῦ πολυωνύμου $p(Y) \in L[Y]$. Ἔτσι ἀποδείχθηκε ὁ πρῶτος ἰσχυρισμὸς τοῦ θεωρήματος.

Ἔστω τώρα ἕνα τυχὸν στοιχεῖο τοῦ L. Αὐτὸ εἶναι τῆς μορφῆς $f(X) + I$, ὅπου $f(X) \in K[X]$. Ἐκτελοῦμε τὴν εὐκλείδεια διαίρεση τοῦ $f(X)$ διὰ $p(X)$ καὶ ἔστω $f(X) = p(X)q(X) + r(X)$, ὅπου $q(X), r(X) \in K[X]$ καὶ $\deg r(X) < \deg p(X)$, ἄρα $r(X) = c_0 + c_1X + \cdots + c_{n-1}X^{n-1}$, μὲ τὰ $c_0, c_1, \ldots, c_{n-1} \in K$. Τώρα ὑπολογίζομε (σύμφωνα μὲ τὰ σχόλια στὴν ἀρχὴ τῆς ἀπόδειξης, μποροῦμε νὰ ταυτίσομε τὰ $c_i \in K$ μὲ τὰ $c_i + I \in L$):

$$\begin{aligned} f(X) + I &= (p(X)q(X) + r(X)) + I = (p(X) + I)(q(X) + I) + (r(X) + I) \\ &= (0 + I)(q(X) + I) + (r(X) + I) = O_L \cdot (q(X) + I) + (r(X) + I) \\ &= r(X) + I = (c_0 + c_1X + c_2X^2 + \cdots + c_{n-1}X^{n-1}) + I \\ &= (c_0 + I) + (c_1 + I)(X + I) + (c_2 + I)(X^2 + I) + \cdots + (c_{n-1} + I)(X^{n-1} + I) \\ &= (c_0 + I) + (c_1 + I)u + (c_2 + I)u^2 + \cdots + (c_{n-1} + I)u^{n-1} \\ &= c_0 + c_1u + c_2u^2 + \cdots + c_{n-1}u^{n-1}. \end{aligned}$$

Ἔτσι ὁλοκληρώσαμε καὶ τὴν ἀπόδειξη τοῦ δεύτερου ἰσχυρισμοῦ.

□

Ἄσκηση 2.1 Μὲ τὸν συμβολισμὸ τῆς ἐκφώνησης τοῦ Θεωρήματος 2.2, ἀποδεῖξτε ὅτι, ἂν $c_0 + c_1u + \cdots + c_{n-1}u^{n-1} = d_0 + d_1u + \cdots + d_{n-1}u^{n-1}$, μὲ τὰ $c_0, c_1, \ldots, c_{n-1}, d_0, d_1, \ldots, d_{n-1} \in K$, τότε $c_i = d_i$ γιὰ κάθε $i = 0, 1, \ldots, n-1$.

Ὑπόδειξη. Ἂν ὑπάρχουν $i \in \{0, 1, \ldots, n-1\}$, τέτοια ὥστε $c_i \neq d_i$, τότε τὸ πολυώνυμο $f(X) = \sum_{i=0}^{n-1}(c_i - d_i)X^i$ εἶναι μὴ μηδενικό, βαθμοῦ $\leq \deg p(X)$, καὶ ἔχει ρίζα τὸ u. Τὸ ἀνάγωγο $p(X)$ δὲν διαιρεῖ τὸ $f(X)$ (λόγῳ βαθμῶν), ἄρα, εἶναι πρῶτο πρὸς τὸ $f(X)$. Συνεπῶς, ὑπάρχουν $g(X), q(X) \in K[X]$, τέτοια ὥστε $g(X)f(X) + q(X)p(X) = 1$. Γιατὶ αὐτὴ ἡ σχέση εἶναι ἀδύνατη;

Ἄσκηση 2.2 Βασισμένοι στὸ Θεώρημα 2.2, περιγρᾶψτε ἕνα σῶμα μὲ ἀκριβῶς 8 στοιχεῖα. Ὕστερα κατασκευᾶστε τὸν πίνακα πρόσθεσης καὶ τὸν πίνακα πολλαπλασιασμοῦ τοῦ σώματος L.

Ὑπόδειξη. Ἐφαρμόζοντας τὸ Θεώρημα 2.2 μὲ $K = \mathbb{Z}_2$ καὶ $p(X) = X^3 + X + 1 \in \mathbb{Z}_2[X]$ (παρατηρῆστε ὅτι τὸ $p(X)$ εἶναι ἀνάγωγο), βλέπομε ὅτι ὑπάρχει σῶμα L, ποὺ περιέχει τὸ $\mathbb{Z}_2$ ὡς ὑπόσωμά του καὶ ἕνα στοιχεῖο $u \in L$, τέτοιο ὥστε $p(u) = 0$ καὶ $L = \{c_0 + c_1u + c_2u^2 | c_0, c_1, c_2 \in \mathbb{Z}_2\}$. Καθὼς ἔχομε δύο ἐπιλογὲς γιὰ κάθε c_i, οἱ συνολικὲς ἐπιλογὲς γιὰ τὸ $c_0 + c_1u + c_2u^2$ εἶναι $2 \cdot 2 \cdot 2 = 8$. Κάθε μία ἀπὸ τὶς 8 διαφορετικὲς ἐπιλογὲς (c_0, c_1, c_2)

δίνει διαφορετικὸ στοιχεῖο $c_0 + c_1u + c_2u^2$, σύμφωνα μὲ τὴν ἄσκηση 2.1.
Γιὰ νὰ φτιάξομε τοὺς πίνακες τῶν πράξεων παρατηροῦμε ὅτι $u^3 + u + 1 = 0$, ἄρα, $u^3 = -u - 1 = u + 1$, ὁπότε, π.χ., $(u^2+1)+(u+1) = u^2+u+2 = u^2+u$ καὶ $(u^2+1)(u+1) = u^3+u^2+u+1 = (u+1)+u^2+u+1 = u^2+2u+2 = u^2$.

2.2 Απαλειφουσα

Πρόταση 2.3 *Ἔστω ἀκέραια περιοχὴ D. Ἂν τὰ $f(X), g(X) \in D[X]$ δὲν ἔχουν μὴ σταθερὸ κοινὸ διαιρέτη, τότε, θεωρούμενα ὡς πολυώνυμα τοῦ $Q(D)[X]$ [1] εἶναι πρῶτα μεταξύ τους.*

Ἀπόδειξη. Γιὰ ν' ἁπλοποιήσομε τὸν συμβολισμό μας, ἂς θέσομε $Q(D) = K$. Ἔστω ὅτι τὰ $f(X), g(X)$ δὲν εἶναι πρῶτα μεταξύ τους στὸ $K[X]$. Αὐτὸ σημαίνει ὅτι ὑπάρχει μὴ σταθερὸ $d(X) \in K[X]$, καὶ πολυώνυμα $f_1(X), g_1(X) \in K[X]$, τέτοια ὥστε

$$f(X) = d(X)f_1(X), \quad g(X) = d(X)g_1(X). \tag{2.1}$$

Σκοπός μας εἶναι να καταλήξομε σὲ ἄτοπο.

Ἐφαρμόζομε τὸ Λῆμμα 1.12 στὰ πολυώνυμα $d(X), f_1(X), g_1(X)$ καὶ συμπεραίνομε ὅτι ὑπάρχουν $\delta, \alpha, \beta \in K$ καὶ πρωταρχικὰ πολυώνυμα $d_1(X), h_1(X), h_2(X) \in D[X]$, ἔτσι ὥστε

$$d(X) = \delta \cdot d_1(X), \quad f_1(X) = \alpha \cdot h_1(X), \quad g_1(X) = \beta \cdot h_2(X). \tag{2.2}$$

Ἐπίσης, ἂν a εἶναι τὸ περιεχόμενο τοῦ $f(X)$ (μκδ τῶν συντελεστῶν του) καὶ b εἶναι τὸ περιεχόμενο τοῦ $g(X)$, τότε

$$f(X) = a \cdot f'(X), \quad g(X) = b \cdot g'(X), \qquad f'(X), g'(X) \in D[X] \text{ πρωταρχικά.} \tag{2.3}$$

Συνδυάζοντας τὶς σχέσεις (2.3), (2.2), (2.1), καταλήγομε εὔκολα στὶς σχέσεις

$$a \cdot f'(X) = \delta\alpha \cdot (d_1(X)h_1(X)), \quad b \cdot g'(X) = \delta\beta \cdot (d_1(X)h_2(X)).$$

Ἀπὸ τὸ Θεώρημα 1.13, τὰ $d_1(X)h_1(X)$ καὶ $d_1(X)h_2(X)$ εἶναι πρωταρχικὰ πολυώνυμα τῆς $D[X]$, ἄρα, λόγῳ τοῦ Λήμματος 1.12,

$$f'(X) = (\text{μονάδα τῆς } D) \cdot d_1(X)h_1(X), \quad g'(X) = (\text{μονάδα τῆς } D) \cdot d_1(X)h_2(X).$$

Αὐτὲς εἶναι σχέσεις στὴν ἀκέραια περιοχὴ $D[X]$, οἱ ὁποῖες δείχνουν ὅτι τὸ $d_1(X) \in D[X]$ διαιρεῖ τὰ $f'(X), g'(X)$, ἄρα διαιρεῖ καὶ τὰ $f(X), g(X)$, καὶ αὐτὸ ἀντιβαίνει στὴν ὑπόθεση. □

Θεώρημα 2.4 *Ἔστω σῶμα K καὶ $f(X,Y), g(X,Y) \in K[X,Y]$, ποὺ δὲν ἔχουν κοινὸ μὴ σταθερό διαιρέτη. Τότε τὸ σύστημα τῶν ἐξισώσεων*

$$\begin{aligned} f(x,y) &= 0 \\ g(x,y) &= 0 \end{aligned} \qquad (x,y) \in K^2$$

ἔχει πεπερασμένο, τὸ πολύ, πλῆθος λύσεων.

[1] Ὑπενθύμιση: $Q(D)$ εἶναι τὸ σῶμα πηλίκων τῆς D

Ἀπόδειξη. Θέτομε $K[Y] = D$, ὁπότε $K[X,Y] = (K[Y])[X] = D[X]$ καὶ τὰ $f(X,Y), g(X,Y)$ τὰ βλέπομε ὡς πολυώνυμα τοῦ $D[X]$ (δηλαδή, πολυώνυμα τοῦ X μὲ συντελεστὲς πολυώνυμα $\in K[Y]$).

Ἐφαρμόζοντας τὴν Πρόταση 2.3, συμπεραίνομε ὅτι ὑπάρχουν $h_i(X) \in Q(D)[X]$ $(i = 1,2)$, τέτοια ὥστε

$$h_1(X)f(X,Y) + h_2(X)g(X,Y) = 1. \tag{2.4}$$

Ἂς δοῦμε τώρα ποιὰ εἶναι τὰ στοιχεῖα τοῦ σώματος $Q(D)$. Ἀφοῦ ἡ D εἶναι ἡ ἀκέραια περιοχὴ τῶν πολυωνύμων μεταβλητῆς Y, μὲ συντελεστὲς στὸ K, ἔπεται ὅτι τὸ σῶμα πηλίκων τῆς ἀποτελεῖται ἀπὸ *πηλίκα* πολυωνύμων τῆς μορφῆς $q(Y)/r(Y)$, ὅπου $q(Y), r(Y) \in K[Y]$, $r(Y) \neq 0$. Ἄρα, γιὰ $i \in \{1,2\}$, τὸ $h_i(X)$ εἶναι τῆς μορφῆς

$$h_i(X) = \frac{q_0(Y)}{r_0(Y)} + \frac{q_1(Y)}{r_1(Y)}X + \frac{q_2(Y)}{r_2(Y)}X^2 + \cdots + \frac{q_m(Y)}{r_m(Y)}X^m.$$

Ἂν θέσομε $s_i(Y) = r_0(Y)r_1(Y)\cdots r_m(Y)$, τότε βλέπομε ὅτι $h_i(X)s_i(Y) = \ell_i(X,Y) \in K[X,Y]$. Πολλαπλασιάζοντας τὰ δύο μέλη τῆς (2.4) ἐπὶ $s_1(Y)s_2(Y)$, παίρνομε τὴ σχέση

$$\begin{aligned} h_1(Y)h_2(Y) &= (h_1(X)s_1(X))s_2(Y)\cdot f(X,Y) + (h_2(X)s_2(X))s_1(Y)\cdot g(X,Y) \\ &= (\ell_1(X,Y)s_2(Y))f(X,Y) + (\ell_2(X,Y)s_1(Y))g(X,Y) \\ &= t_1(X,Y)f(X,Y) + t_2(X,Y)g(X,Y), \end{aligned} \tag{2.5}$$

ὅπου $t_1(X,Y) = \ell_1(X,Y)s_2(Y)$, $t_2(X,Y) = \ell_2(X,Y)s_1(Y) \in K[X,Y]$.

Ἔστω τώρα $(a,b) \in K^2$, τέτοιο ὥστε $f(a,b) = 0 = g(a,b)$. Ἡ ἀντικατάσταση $(a,b) \leftarrow (X,Y)$ στὴ (2.5), δίνει $h_1(b)h_2(b) = t_1(a,b)f(a,b) + t_2(a,b)g(a,b) = 0$, ὁπότε βλέπομε ὅτι τὸ b εἶναι ρίζα τοῦ πολυωνύμου $h_1(Y)h_2(Y)$. Κάθε μὴ μηδενικὸ πολυώνυμο, ὅμως, τοῦ $K[Y]$ ἔχει πεπερασμένες τὸ πλῆθος ρίζες μέσα στὸ K, ἄρα οἱ πιθανὲς τιμὲς τοῦ b εἶναι πεπερασμένες τὸ πλῆθος, ἔστω $b_1, \ldots b_k$. Κάθε ἐξίσωση $f(a,b_i) = 0$ ἔχει πεπερασμένες τὸ πλῆθος λύσεις ὡς πρὸς a, ἄρα, τελικά, πεπερασμένα τὸ πλῆθος ζεύγη $(a,b) \in K^2$ εἶναι δυνατὸν νὰ ἱκανοποιοῦν συγχρόνως $f(a,b) = 0$ καὶ $g(a,b) = 0$.

□

Ἀπαλείφουσα. Στὴ σχέση (2.5), ἔστω $R_X(f,g) = h_1(Y)h_2(Y)$. Τὸ πολυώνυμο αὐτὸ καλεῖται *ἀπαλείφουσα τῶν f,g, ὡς πρὸς X* καὶ ὁ ὑποδείκτης $_X$ ὑποδηλώνει ὅτι τὸ πολυώνυμο εἶναι ἀπαλλαγμένο ἀπὸ τὴ μεταβλητὴ X, ἄρα εἶναι πολυώνυμο $\in K[Y]$. Εἴδαμε στὴν ἀπόδειξη τοῦ Θεωρήματος 2.4 ὅτι,

$$\{f(a,b) = 0 \quad \& \quad g(a,b) = 0\} \;\Rightarrow\; R_X(f,g)(b) = 0$$

Λόγῳ τοῦ συμμετρικοῦ ρόλου τῶν μεταβλητῶν X, Y στὸ θεώρημα, θὰ μπορούσαμε, ἐντελῶς ἀνάλογα, νὰ ἀποδείξομε ὅτι ὑπάρχει πολυώνυμο $R_Y(f,g) \in K[X]$, τέτοιο ὥστε

$$\{f(a,b) = 0 \quad \& \quad g(a,b) = 0\} \;\Rightarrow\; R_Y(f,g)(a) = 0,$$

τὸ ὁποῖο καλεῖται *ἀπαλείφουσα τῶν f,g, ὡς πρὸς Y*

Τὸ ἐρώτημα εἶναι: Στὴν πράξη, ἂν μᾶς δοθοῦν τὰ f,g, πῶς μποροῦμε νὰ ὑπολογίσομε τὸ $R_X(f,g)$ ἢ τὸ $R_Y(f,g)$; Δίχως νὰ κάνομε ἀνάπτυξη τῆς σχετικῆς θεωρίας, δίνομε ἕνα παράδειγμα πρακτικοῦ ὑπολογισμοῦ.

Παράδειγμα. Θεωροῦμε τὰ πολυώνυμα $f(X,Y) = 3X^2 + Y^2 - 13$ καὶ $g(X,Y) = X^3 - X^2Y - 4$ πάνω ἀπὸ τὸ $\mathbb{R}$ καὶ θὰ ὑπολογίσομε τὴν ἀπαλείφουσα $R_Y(f,g)$.

Ἔστω $f(a,b) = 0 = g(a,b)$. Τότε $b^2 + (3a^2 - 13) = 0$ καὶ $-a^2b + (a^3 - 4) = 0$. Πολλαπλασιάζοντας ἐπὶ b τὴ δεύτερη, παίρνομε ἄλλη μία σχέση, τὴ $-a^2b^2 + (a^3 - 4)b = 0$. Γράφομε τὶς τρεῖς σχέσεις, διατάσσοντάς τις κατὰ τὶς κατιοῦσες δυνάμεις τοῦ b:

$$\begin{array}{rcrcrcl} b^2 & + & & & (3a^2-13) & = & 0 \\ -a^2b^2 & + & (a^3-4)b & & & = & 0 \\ & & -a^2b & + & (a^3-4) & = & 0 \end{array}$$

Μὲ χρήση πινάκων, τὸ παραπάνω σύστημα γράφεται ὡς γραμμικὸ σύστημα

$$\begin{pmatrix} 1 & 0 & 3a^2-13 \\ -a^2 & a^3-4 & 0 \\ 0 & -a^2 & a^3-4 \end{pmatrix} \begin{pmatrix} b^2 \\ b \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix},$$

τὸ ὁποῖο ἔχει μὴ μηδενικὴ λύση $(b^2, b, 1)$, ἄρα ἡ ὁρίζουσα τῶν συντελεστῶν πρέπει νὰ εἶναι μηδενική. Ἔτσι,

$$0 = \begin{vmatrix} 1 & 0 & 3a^2-13 \\ -a^2 & a^3-4 & 0 \\ 0 & -a^2 & a^3-4 \end{vmatrix} = 4a^6 - 13a^4 + 8a^3 + 16,$$

δηλαδή, $R_Y(f,g) = 4X^6 - 13X^4 - 8X^3 + 16$.

Εἶναι $R_Y(f,g)(2) = 0$. Ἡ ἐξίσωση $f(2,b) = 0$ μᾶς δίνει $b^2 = 1$, ἄρα $b = \pm 1$. Ἀπὸ τὰ δύο ζεύγη $(a,b) = (2,1), (2,-1)$, μόνο τὸ πρῶτο ἐπαληθεύει τὴν $g(a,b) = 0$.

2.3 Μικρη Εισαγωγη στην Αλγεβρικη Γεωμετρια

Σὲ ὅλη τὴν παροῦσα ἑνότητα, K εἶναι σῶμα. Τὰ σύμβολα $f, g, h, \ldots$ μὲ ἢ χωρὶς ὑποδεῖκτες θὰ συμβολίζουν πολυώνυμα $\in K[X_1, \ldots, X_n]$. Συνήθως θὰ γράφομε, γιὰ παράδειγμα, f ἀντὶ $f(X_1, \ldots, X_n)$. Μὲ K^n συμβολίζομε τὸ καρτεσιανὸ γινόμενο $\underbrace{K \times \cdots \times K}_{n}$

Ὁρισμός. Ἔστω $S \subseteq K[X_1, \ldots, X_n]$. Ὁρίζομε

$$\mathbb{V}(S) = \{(a_1, \ldots, a_n) \in K^n : f(a_1, \ldots, a_n) = 0 \ \forall f \in S\}.$$

Τὰ ὑποσύνολα τοῦ K^n αὐτῆς τῆς μορφῆς χαρακτηρίζονται *ἀλγεβρικὰ σύνολα*. Δηλαδή, τὸ $A \subseteq K^n$ χαρακτηρίζεται ἀλγεβρικὸ σύνολο, ἂν ὑπάρχει ὑποσύνολο S τοῦ $K[X_1, \ldots, X_n]$ (ὄχι, κατ' ἀνάγκη πεπερασμένο), ἔτσι ὥστε $A = \mathbb{V}(S)$. Στὴν περίπτωση ποὺ $S = \{f\}$, γράφομε ἁπλῶς $\mathbb{V}(f)$ ἀντὶ $\mathbb{V}(\{f\})$. Ἕνα σύνολο τῆς μορφῆς $\mathbb{V}(f)$ χαρακτηρίζεται *ὑπερεπιφάνεια* . Στὴν εἰδικὴ περίπτωση $n = 3$, τὸ $\mathbb{V}(f)$ λέγεται ἁπλῶς *ἐπιφάνεια* – παραλείπεται, δηλαδή, τὸ πρόθεμα «ὑπέρ» –, ἐνῶ στὴν περίπτωση $n = 2$, τὸ $\mathbb{V}(f)$ λέγεται *καμπύλη*.

Παρατήρηση. Εἶναι $\mathbb{V}(\emptyset) = K^n$. [2]

Ἄσκηση 2.3 $S_1 \subseteq S_2 \subseteq K[X_1, \ldots, X_n] \Rightarrow \mathbb{V}(S_1) \supseteq \mathbb{V}(S_2)$.

[2] Αὐτὸ δικαιολογεῖται ὡς ἑξῆς: Σὲ αὐστηρὰ τυπικὴ γλῶσσα, τὸ $(a_1, \ldots, a_n)$ εἶναι στοιχεῖο τοῦ $\mathbb{V}(S)$ ἂν καὶ μόνο ἂν ἡ ἑξῆς συνεπαγωγὴ εἶναι ἀληθής: $f \in S \Rightarrow f(a_1, \ldots, a_n) = 0$. Ἄρα, στὴν περίπτωση ποὺ $S = \emptyset$, τὸ $(a_1, \ldots, a_n)$ ἀνήκει στὸ $\mathbb{V}(\emptyset)$ ἂν καὶ μόνο ἂν ἡ ἑξῆς συνεπαγωγὴ εἶναι ἀληθής: $f \in \emptyset \Rightarrow f(a_1, \ldots, a_n) = 0$. Ἀλλὰ ἡ πρόταση $f \in \emptyset$ εἶναι ψευδὴς καὶ στὰ Μαθηματικὰ δεχόμαστε ὅτι μιὰ συνεπαγωγὴ $\Pi_1 \Rightarrow \Pi_2$, μὲ Π_1 ψευδῆ πρόταση καὶ Π_2 ὁποιαδήποτε πρόταση, εἶναι ἀληθής.

Ἄσκηση 2.4 $\mathbb{V}(S_1 \cup S_2) = \mathbb{V}(S_1) \cap \mathbb{V}(S_2)$. Ἄρα, ἡ τομὴ ἀλγεβρικῶν συνόλων εἶναι ἀλγεβρικὸ σύνολο.

Ἄσκηση 2.5 $\mathbb{V}(f \cdot g) = \mathbb{V}(f) \cup \mathbb{V}(g)$.

Ἄσκηση 2.6 Ἀποδεῖξτε ὅτι κάθε μονοσύνολο τοῦ K^n εἶναι ἀλγεβρικὸ σύνολο.
Δεῖξτε ὅτι, ἂν $(a_1, \ldots, a_n) \in K^n$, τότε $\{(a_1, \ldots, a_n)\} = \mathbb{V}(\{X_1 - a_1, \ldots, X_n - a_n\})$.

Πρόταση 2.5 *Ἂν $S \subseteq K[X_1, \ldots, X_n]$, τότε $\mathbb{V}(S) = \mathbb{V}(\langle S \rangle)$.*[3]

Ἀπόδειξη. Εἶναι $S \subseteq \langle S \rangle$, ἄρα, ἀπὸ τὴν ἄσκηση 2.3, $\mathbb{V}(S) \supseteq \mathbb{V}(\langle S \rangle)$. Ἀντιστρόφως, θὰ δείξομε ὅτι, ἂν $(a_1, \ldots, a_n) \in \mathbb{V}(S)$, τότε $(a_1, \ldots, a_n) \in \mathbb{V}(\langle S \rangle)$. Γιὰ τὴν ἀπόδειξη τῆς τελευταίας σχέσης, θεωροῦμε $g \in \langle S \rangle$ καὶ θ' ἀποδείξομε ὅτι $g(a_1, \ldots, a_n) = 0$. Ἀλλὰ $g \in \langle S \rangle$ σημαίνει ὅτι ὑπάρχουν $f_1, \ldots, f_r \in S$ καὶ $h_1, \ldots, h_r \in K[X_1, \ldots, X_n]$, τέτοια ὥστε $g = \sum_{i=1}^{r} h_i f_i$. Ἐπειδὴ τὰ $f_i \in S$ καὶ τὸ $(a_1, \ldots, a_n) \in \mathbb{V}(S)$, ἔπεται ὅτι $f_i(a_1, \ldots, a_n) = 0$ γιὰ κάθε i, ἄρα $g(a_1, \ldots, a_n) = \sum_i h(a_1, \ldots, a_n) f(a_1, \ldots, a_n) = 0$.

□

Ὁρισμός. Ἔστω $A \subseteq K^n$. Ὁρίζομε

$$\mathbb{I}(A) = \{f \in K[X_1, \ldots, X_n] : f(a_1, \ldots, a_n) = 0 \ \forall (a_1, \ldots, a_n) \in A\}.$$

Παρατήρηση. Εἶναι $\mathbb{I}(\emptyset) = K[X_1, \ldots, X_n]$. [4]

Πρόταση 2.6 *Ἂν $A \subseteq K^n$, τότε τὸ $\mathbb{I}(A)$ εἶναι ἰδεῶδες τοῦ $K[X_1, \ldots, X_n]$.*

Ἀπόδειξη. Κατ' ἀρχάς, τὸ $\mathbb{I}(A)$ εἶναι μὴ κενὸ διότι περιέχει τὸ μηδενικὸ πολυώνυμο. Μετὰ ἔχομε νὰ δείξομε τὰ ἑξῆς:

(α′) Ἂν $f \in \mathbb{I}(A)$ καὶ $h \in K[X_1, \ldots, X_n]$, τότε $h \cdot f \in \mathbb{I}(A)$. Αὐτὸ εἶναι προφανές, διότι ἡ ὑπόθεση $f \in \mathbb{I}(A)$ σημαίνει ὅτι $f(a_1, \ldots, a_n) = 0$ γιὰ κάθε $(a_1, \ldots, a_n) \in A$, ὁπότε καὶ $h(a_1, \ldots, a_n) f(a_1, \ldots, a_n) = 0$ γιὰ κάθε $(a_1, \ldots, a_n) \in A$. Αὐτὸ τὸ τελευταῖο συμπέρασμα, ὅμως, σημαίνει ὅτι $h \cdot f \in \mathbb{I}(A)$.

(β′) Ἂν $f_i \in \mathbb{I}(A)$ $(i = 1, 2)$, τότε $f_1 - f_2 \in \mathbb{I}(A)$. Ἡ ἀπόδειξη εἶναι ἐξίσου ἁπλῆ: Ἀπὸ τὴν ὑπόθεση, γιὰ $i = 1, 2$ ἔχομε ὅτι $f_i(a_1, \ldots, a_n) = 0$ γιὰ ὅλα τὰ $(a_1, \ldots, a_n) \in A$. Ἀλλὰ τότε, γιὰ κάθε $(a_1, \ldots, a_n) \in A$, ἔχομε $(f_1 - f_2)(a_1, \ldots, a_n) = f_1(a_1, \ldots, a_n) - f_2(a_1, \ldots, a_n) = 0 - 0 = 0$.

□

Ἄσκηση 2.7 Ἂν $A_1 \subseteq A_2 \subseteq K^n$ τότε $\mathbb{I}(A_1) \supseteq \mathbb{I}(A_2)$.

Ἄσκηση 2.8 Ἂν $A_1, A_2 \subseteq K^n$, τότε $\mathbb{I}(A_1 \cup A_2) = \mathbb{I}(A_1) \cap \mathbb{I}(A_2)$.

Ἄσκηση 2.9 Γιὰ κάθε $f \in K[X_1, \ldots, X_n]$ ἰσχύει $\langle f \rangle \subseteq \mathbb{I}(\mathbb{V}(f))$.

---

[3] Ὑπενθύμιση: $\langle S \rangle$ εἶναι τὸ ἰδεῶδες ποὺ παράγεται ἀπὸ τὸ S, ἄρα $\langle S \rangle = \{\sum_i h_i \cdot f_i\}$, μὲ τὸ i νὰ διατρέχει πεπερασμένο σύνολο δεικτῶν, τὰ $f_i \in S$ καὶ τὰ $h_i \in K[X_1, \ldots, X_n]$.

[4] Αἰτιολόγηση ἐντελῶς ἀνάλογη μὲ αὐτὴ ποὺ δώσαμε γιὰ τὴ σχέση $\mathbb{V}(\emptyset) = K^n$· βλ. ὑποσημείωση στὴ σελ.27.

Πρόταση 2.7 (α′) *Γιὰ κάθε* $S \subseteq K[X_1, \ldots, X_n]$ *ἰσχύει* $\mathbb{I}(\mathbb{V}(S)) \supseteq S$.
(β′) *Γιὰ κάθε* $A \subseteq K^n$ *ἰσχύει* $\mathbb{V}(\mathbb{I}(A)) \supseteq A$.

Ἀπόδειξη. (α′) Ἔστω $f \in S$. Θὰ δείξομε ὅτι $f \in \mathbb{I}(\mathbb{V}(S))$. Αὐτὸ ἰσοδυναμεῖ μὲ τὸ νὰ δείξομε ὅτι, ἂν $(a_1, \ldots, a_n) \in \mathbb{V}(S)$, τότε $f(a_1, \ldots, a_n) = 0$. Ἀλλὰ $(a_1, \ldots, a_n) \in \mathbb{V}(S)$ σημαίνει ὅτι τὸ $(a_1, \ldots, a_n)$ μηδενίζει κάθε πολυώνυμο $\in S$, ἄρα (ἀφοῦ $f \in S$), ἔπεται ὅτι $f(a_1, \ldots, a_n) = 0$, ποὺ εἶναι ἡ ἀποδεικτέα σχέση.

(β′) Ἔστω $(a_1, \ldots, a_n) \in A$. Θὰ δείξομε ὅτι $(a_1, \ldots, a_n) \in \mathbb{V}(\mathbb{I}(A))$. Αὐτὸ ἰσοδυναμεῖ μὲ τὸ νὰ δείξομε ὅτι, ἂν $f \in \mathbb{I}(A)$, τότε $f(a_1, \ldots, a_n) = 0$. Ἀλλὰ $f \in \mathbb{I}(A)$ σημαίνει ὅτι τὸ f μηδενίζεται ἀπὸ κάθε n-άδα $\in A$, ἄρα (ἀφοῦ $(a_1, \ldots, a_n) \in A$) ἔπεται ὅτι $f(a_1, \ldots, a_n) = 0$, ποὺ εἶναι ἡ ἀποδεικτέα σχέση.

□

Πόρισμα 2.8 (α′) *Ἂν τὸ* $A \subseteq K^n$ *εἶναι ἀλγεβρικὸ σύνολο, τότε* $\mathbb{V}(\mathbb{I}(A)) = A$.
(β′) *Ἂν τὸ* J *εἶναι ἰδεῶδες ἀλγεβρικοῦ ὑπσυνόλου τοῦ* K^n*, τότε* $\mathbb{I}(\mathbb{V}(J)) = J$.

Ἀπόδειξη. (α′) Ἐξ ὑποθέσεως, $A = \mathbb{V}(S)$ γιὰ κάποιο $S \subseteq K[X_1, \ldots, X_n]$. Ἀπὸ τὴν Πρόταση 2.7 (α′) ἔχομε $\mathbb{I}(A) = \mathbb{I}(\mathbb{V}(S)) \supseteq S$, ἄρα, ἀπὸ τὴν ἄσκηση 2.3, $\mathbb{V}(\mathbb{I}(A)) \subseteq \mathbb{V}(S) = A$. Ὅμως, τὴν ἀπὸ τὴν Πρόταση 2.7 (β′), ἰσχύει καὶ ἡ σχέση $\mathbb{V}(\mathbb{I}(A)) \supseteq A$, ἄρα $\mathbb{V}(\mathbb{I}(A)) = A$.
(β′) Ἐξ ὑποθέσεως, $J = \mathbb{I}(A)$ γιὰ κάποιο ἀλγεβρικὸ σύνολο $A \subseteq K^n$, ἄρα $\mathbb{V}(J) = \mathbb{V}(\mathbb{I}(A)) = A$, λόγῳ τοῦ (α′) ποὺ μόλις ἀποδείξαμε. Ἄρα, $\mathbb{I}(\mathbb{V}(J)) = \mathbb{I}(A) = J$.

□

Ὁρισμός. Ἔστω R μεταθετικὸς δακτύλιος μὲ μοναδιαῖο. Ὁ R λέμε ὅτι εἶναι δακτύλιος Noether ἂν κάθε ἰδεῶδες του εἶναι πεπερασμένα παραγόμενο, δηλαδή, ἂν γιὰ κάθε ἰδεῶδες J τοῦ R ὑπάρχουν $j_1, \ldots, j_m \in J$, τέτοια ὥστε $J = \langle j_1, \ldots, j_m \rangle$.[5]

Παρατήρηση. Στὴν περίπτωση ποὺ ὁ δακτύλιος εἶναι σῶμα K, τὰ μόνα ἰδεώδη εἶναι τὸ μηδενικὸ $\{0\} = \langle 0 \rangle$ καὶ ὁλόκληρος ὁ δακτύλιος $K = \langle 1 \rangle$, ἄρα, τετριμμένα, κάθε σῶμα εἶναι δακτύλιος Noether.

Θεώρημα 2.9 *Ἔστω ὅτι ὁ* R *εἶναι μεταθετικὸς δακτύλιος μὲ μοναδιαῖο καὶ εἶναι δακτύλιος Noether. Τότε καὶ ὁ* $R[X]$ *εἶναι δακτύλιος Noether.*

Ἀπόδειξη. Σ' αὐτὴ τὴν ἀπόδειξη, ἂν $f \in KX$, θὰ συμβολίζομε μὲ $\text{ΣΜΟ}(f)$ τὸν συντελεστὴ τοῦ μεγιστοβαθμίου ὅρου τοῦ f. Γιὰ τὸ μηδενικὸ πολυώνυμο θέτομε $\text{ΣΜΟ}(0) = 0$.

Ἔστω I μὴ μηδενικὸ ἰδεῶδες τοῦ $R[X]$. Θὰ ἀποδείξομε ὅτι τὸ I εἶναι πεπερασμένα παραγόμενο ἰδεῶδες. Πρὸς τοῦτο θεωροῦμε τὸ ἰδεῶδες J, ὅπως στὴν ἄσκηση 2.10, τὸ ὁποῖο, ἐξ ὑποθέσεως, εἶναι πεπερασμένα παραγόμενο, ἔστω $J = \langle a_1, \ldots, a_r \rangle$. Αὐτὸ σημαίνει ὅτι ὑπάρχουν $f_1, \ldots, f_r \in I$, τέτοια ὥστε $a_i = \text{ΣΜΟ}(f_i)$ γιὰ $i = 1, \ldots, r$.
Σταθεροποιοῦμε τώρα ἕναν ἀκέραιο $N > \max_{1 \le i \le r} \deg f_i$ καὶ γιὰ κάθε $m \le N$ ὁρίζομε

$$J_m = \{\, a \in R : \ a = \text{ΣΜΟ}(\text{πολυωνύμου τοῦ } I \text{ βαθμοῦ} \le m) \,\}.$$

Προφανῶς, τὸ J_m εἶναι ἰδεῶδες τοῦ R, ἄρα εἶναι πεπερασμένα παραγόμενο, ἔστω $J_m = \langle a_{m,1}, \ldots, a_{m,r_m} \rangle$, ὅπου κάθε $a_{m,i} = \text{ΣΜΟ}(f_{m,i})$ γιὰ κάποιο $f_{m,i} \in I$ μὲ $\deg f_{m,i} \le m$.

Τέλος, ὁρίζομε

$$S = \{f_1, \ldots, f_r\} \bigcup_{m=1}^{N} \{f_{m,1}, \ldots, f_{m,r_m}\}, \ \text{καὶ } I' = \langle S \rangle \tag{2.6}$$

[5] $\langle j_1, \ldots, j_m \rangle \overset{\text{ορ}}{=} \{r_1 j_1 + \cdots r_m j_m : r_1, \ldots, r_m \in R\}$.

καὶ θ' ἀποδείξομε ὅτι $I = I'$, ὁπότε θὰ ἔχομε δείξει ὅτι τὸ I εἶναι πεπερασμένα παραγόμενο καὶ ἡ ἀπόδειξη θὰ ἔχει ὁλοκληρωθεῖ.
Ἀπὸ τὸν ὁρισμὸ τοῦ I' ξέρομε ἤδη ὅτι $I' \subseteq I$. Θὰ ὑποθέσομε ὅτι στὴν τελευταία σχέση δὲν ἰσχύει τὸ = καὶ θὰ ὁδηγηθοῦμε σὲ ἄτοπο. Ἔστω $g \in I \setminus I'$ καὶ ὁ βαθμὸς d τοῦ g εἶναι ὁ ἐλάχιστος δυνατός, δηλαδή, κάθε πολυώνυμο τοῦ $I \setminus I'$ εἶναι βαθμοῦ $\geq d$. Διακρίνομε δύο περιπτώσεις.
Περίπτωση πρώτη· $d > N$. Τότε, λόγῳ τῆς ἐπιλογῆς τοῦ N, εἶναι $d > \deg f_i$, ὁπότε, ἐπιλέγοντας κατάλληλα $c_1, \ldots, c_r \in R$ μποροῦμε νὰ κάνομε τὸ πολυώνυμο $h = \sum_{i=1}^{r} c_i f_i(X) X^{d-\deg f_i}$ νὰ ἔχει συντελεστὴ τοῦ X^d ἴσο μὲ τὸν συντελεστὴ τοῦ X^d στὸ g, ἄρα $\text{ΣΜΟ}(h) = \text{ΣΜΟ}(g)$. Ὅμως, τὸ h εἶναι πολυώνυμο τοῦ ἰδεώδους I, ἄρα $g - h \in I$ καὶ $\deg(g-h) < d$, ἄρα, λόγῳ τῆς ἐπιλογῆς τοῦ d, συμπεραίνομε ὅτι $g - h \notin I \setminus I'$, δηλαδή, $g - h \in I'$. Ἀλλὰ $h \in I'$ (βλ. ὁρισμὸ τοῦ I' στὴν (2.6)), ἄρα καὶ $g \in I'$, σὲ ἀντίφαση μὲ τὴν ἐπιλογὴ τοῦ g.
Περίπτωση δεύτερη· $d = m \leq N$. Τότε ἐπιλέγομε κατάλληλα $c_1, \ldots, c_{r_m} \in R$ ἔτσι ὥστε τὸ πολυώνυμο $h = \sum_{i=1}^{r_m} c_i X^{m-\deg f_{m,i}} f_{m,i}(X)$ νὰ ἔχει συντελεστὴ τοῦ X^m ἴσο μὲ τὸν συντελεστὴ τοῦ X^m στὸ πολυώνυμο g. Τότε, κατ' ἀναλογίαν μὲ τὴν προηγούμενη περίπτωση, $g - h \in I$ καὶ $\deg(g-h) < m = d$, ἄρα $g - h \notin I \setminus I'$. Αὐτὸ σημαίνει ὅτι $g - h \in I'$, ἄρα (δεδομένου ὅτι $h \in I'$) $g \in I'$· ἀντίφαση.

□

Πόρισμα 2.10 - ***Θεώρημα Βάσεως τοῦ Hilbert***. *Ἔστω ὅτι ὁ R εἶναι μεταθετικὸς δακτύλιος μὲ μοναδιαῖο καὶ εἶναι δακτύλιος Noether. Τότε, γιὰ ὁποιοδήποτε $n \in \mathbb{N}$, ὁ $R[X_1, \ldots, X_n]$ εἶναι δακτύλιος Noether. Εἰδικώτερα, γιὰ κάθε σῶμα K, ὁ $K[X_1, \ldots, X_n]$ εἶναι δακτύλιος Noether.*

Ἀπόδειξη. Ἐφαρμόζοντας τὸ Θεώρημα 2.9 συμπεραίνομε ὅτι ὁ $R[X_1]$ εἶναι δακτύλιος Noether. Ἐφαρμόζοντας ξανὰ τὸ ἴδιο θεώρημα, ἀλλὰ μὲ τὸν δακτύλιο $R[X_1]$ στὴ θέση τοῦ R καὶ τὴ μεταβλητὴ X_2 στὴ θέση τῆς μεταβλητῆς X, συμπεραίνομε ὅτι καὶ ὁ δακτύλιος $(R[X_1])[X_2]$ –δηλαδή, ὁ $R[X_1, X_2]$– εἶναι δακτύλιος Noether. Ἐφαρμόζοντας τὸ Θεώρημα 2.9 στὸν δακτύλιο $R[X_1, X_2]$ καὶ τὴ μεταβλητὴ X_3, συμπεραίνομε ὅτι ὁ $R[X_1, X_2, X_3]$ εἶναι δακτύλιος Noether, κ.ο.κ.

□

Ἄσκηση 2.10 Ἔστω R μεταθετικὸς δακτύλιος μὲ μοναδιαῖο, I ἰδεῶδες τοῦ δακτυλίου $K[X]$ καὶ $J = \{a \in R : \exists\, f \in I$ γιὰ τὸ ὁποῖο $a = \text{ΣΜΟ}(f)\}$.[6] Ἀποδείξτε ὅτι τὸ J εἶναι ἰδεῶδες τοῦ R.
Ὑπόδειξη. Γιὰ νὰ δείξετε ὅτι, ἂν $a, b \in J$ τότε καὶ $a + b \in J$: Ἔστω ὅτι $a = \text{ΣΜΟ}(f)$, $b = \text{ΣΜΟ}(g)$ καὶ m, n οἱ βαθμοὶ τῶν f, g, ἀντιστοίχως. Θεωρῆστε τὸ πολυώνυμο $X^n f(X) + X^m g(X)$.

Θεώρημα 2.11 *Κάθε ἀλγεβρικὸ σύνολο τοῦ K^n εἶναι τομὴ πεπερασμένου πλήθους ὑπερεπιφανειῶν.*[7]

Ἀπόδειξη. Ἔστω ἀλγεβρικὸ σύνολο $A \subseteq K^n$. Αὐτὸ σημαίνει ὅτι $A = \mathbb{V}(S)$ γιὰ κάποιο $S \subseteq K[X_1, \ldots, X_n]$. Ἀπὸ τὴν Πρόταση 2.5 ξέρομε ὅτι $\mathbb{V}(S) = \mathbb{V}(\langle S \rangle)$ καὶ τὸ Θεώρημα 2.10

[6] Γιὰ τὸν συμβολισμὸ ΣΜΟ() δεῖτε τὴν ἀρχὴ τῆς ἀπόδειξης τοῦ Θεωρήματος 2.9.
[7] Βλ. Ὁρισμὸ 2.3.

μᾶς λέει ὅτι ὑπάρχει πεπερασμένο πλῆθος πολυωνύμων $f_1, \ldots, f_m \in K[X_1, \ldots, X_n]$, ἔτσι ὥστε νὰ ἰσχύει $\langle S \rangle = \langle f_1, \ldots, f_m \rangle$. Ἄρα,

$$\begin{aligned} A = \mathbb{V}(\langle f_1, \ldots, f_m \rangle) &= \text{ (ἀπὸ τὴν Πρόταση 2.5) } \mathbb{V}(\{f_1, \ldots, f_m\}) \\ &= \mathbb{V}(\{f_1\} \cup \cdots \cup \{f_m\}) = \text{ (ἀπὸ τὴν ἄσκηση 2.8) } \mathbb{V}(f_1) \cap \cdots \cap \mathbb{V}(f_m). \end{aligned}$$

Ἐξ ὁρισμοῦ, κάθε $\mathbb{V}(f_i)$ εἶναι μιὰ ὑπερεπιφάνεια, ἄρα ἡ ἀπόδειξη εἶναι πλήρης.

□

Ὁρισμός. Ἔστω ἀλγεβρικὸ σύνολο $A \subseteq K^n$. Ἂν εἶναι ἀδύνατον νὰ βρεθοῦν ἀλγεβρικὰ σύνολα A_1, A_2, τὰ ὁποῖα εἶναι *γνήσια* ὑποσύνολα τοῦ A καὶ $A_1 \cup A_2 = A$, τότε τὸ A χαρακτηρίζεται ἀνάγωγο ἀλγεβρικὸ σύνολο.

Θεώρημα 2.12 *Τὸ ἀλγεβρικὸ σύνολο $A \subseteq K^n$ εἶναι ἀνάγωγο ἂν καὶ μόνο ἂν τὸ $\mathbb{I}(A)$ εἶναι πρῶτο ἰδεῶδες τοῦ $K[X_1, \ldots, X_n]$.*

Ἀπόδειξη. Ἔστω ὅτι τὸ $\mathbb{I}(A)$ δὲν εἶναι πρῶτο ἰδεῶδες τοῦ $K[X_1, \ldots, X_n]$. Τότε, θὰ δείξομε ὅτι τὸ A δὲν εἶναι ἀνάγωγο ἀλγεβρικὸ σύνολο. Ἐξ ὑποθέσεως, ὑπάρχουν $f_1, f_2 \in K[X_1, \ldots, X_n]$, τὰ ὁποῖα δὲν ἀνήκουν στὸ $\mathbb{I}(A)$, ἀλλὰ τὸ γινόμενό τους $f_1 f_2 \in \mathbb{I}(A)$. Ἡ σχέση $f_1 \notin \mathbb{I}(A)$ σημαίνει ὅτι ὑπάρχει $(a_1, \ldots, a_n) \in A$, τέτοιο ὥστε $f(a_1, \ldots, a_n) \neq 0$, ὁπότε τὸ $(a_1, \ldots, a_n) \notin \mathbb{V}(f_1)$ καί, συνεπῶς, $A \cap \mathbb{V}(f_1) \subsetneq A$. Ἐντελῶς ἀνάλογα, $A \cap \mathbb{V}(f_2) \subsetneq A$. Χρησιμοποιώντας τώρα τὴ συνολοθεωρητικὴ ταυτότητα $(\mathbb{A} \cap \mathbb{B}) \cup (\mathbb{A} \cap \mathbb{C}) = \mathbb{A} \cap (\mathbb{B} \cup \mathbb{C})$ συμπεραίνομε ὅτι

$$(A \cap \mathbb{V}(f_1)) \cup (A \cap \mathbb{V}(f_2)) = A \cap (\mathbb{V}(f_1) \cup \mathbb{V}(f_2)) = \text{ (ἄσκηση 2.5) }) A \cap \mathbb{V}(f_1 f_2). \qquad (2.7)$$

Τὸ δεξιώτερο μέλος τῆς παραπάνω σχέσης ἰσοῦται μὲ A. Πράγματι, ἐξ ὑποθέσεως, $f_1 f_2 \in \mathbb{I}(A)$, ἄρα $\{f_1 f_2\} \subseteq \mathbb{I}(A)$ ὁπότε

$$\mathbb{V}(f_1 f_2) \supseteq \text{ (ἄσκηση 2.3) } \mathbb{V}(\mathbb{I}(A)) = \text{(Πόρισμα 2.8) } A$$

ἄρα $\mathbb{V}(f_1 f_2) \cap A = A$ καί, συνεπῶς, ἀπ' τὴν (2.7),

$$A = (A \cap \mathbb{V}(f_1)) \cup (A \cap \mathbb{V}(f_2)).$$

Ἔτσι, τὸ A γράφτηκε ὡς ἕνωση δύο γνησίων (ὅπως εἴδαμε παραπάνω) ὑποσυνόλων του, καθένα ἐκ τῶν ὁποίων εἶναι ἀλγεβρικό, ἀφοῦ εἶναι τομὴ ἀλγεβρικῶν συνόλων (ἄσκηση 2.4).

Ἀντιστρόφως, θὰ δείξομε ὅτι, ἂν $A = A_1 \cup A_2$, ὅπου τὰ A_1, A_2 εἶναι *γνήσια* ἀλγεβρικὰ ὑποσύνολα τοῦ A, τότε τὸ $\mathbb{I}(A)$ δὲν εἶναι πρῶτο ἰδεῶδες τοῦ $K[X_1, \ldots, X_n]$.
Ἰσχυρισμός: Γιὰ $i = 1, 2$ εἶναι $\mathbb{I}(A_i) \supsetneq \mathbb{I}(A)$. Διότι, ἡ σχέση $A_i \subseteq A$ συνεπάγεται (ἄσκηση 2.7) τὴ σχέση $\mathbb{I}(A_i) \supseteq \mathbb{I}(A)$. Ἂν γιὰ κάποιο $i \in \{1, 2\}$ ἡ τελευταία σχέση εἶναι ἰσότητα, τότε, ἀπὸ τὸ Πόρισμα 2.8, συμπεραίνομε ὅτι $A_i = A$, ποὺ ἀντίκειται στὴν ὑπόθεσή μας. Συνεπῶς, γιὰ $i = 1, 2$, μποροῦμε νὰ βροῦμε $f_i \in \mathbb{I}(A_i) \setminus \mathbb{I}(A)$. Θὰ δείξομε τώρα ὅτι $f_1 f_2 \in \mathbb{I}(A)$, ποὺ ὁδηγεῖ στὸ συμπέρασμα ὅτι τὸ $\mathbb{I}(A)$ δὲν εἶναι πρῶτο ἰδεῶδες. Πρὸς τοῦτο, θεωροῦμε $(a_1, \ldots, a_n) \in A$ καὶ δείχνομε ὅτι $(f_1 f_2)(a_1, \ldots, a_n) = 0$, ὡς ἑξῆς: Ἀπὸ τὴ σχέση $(a_1, \ldots, a_n) \in A = A_1 \cup A_2$ συμπεραίνομε ὅτι γιὰ κάποιο $i \in \{1, 2\}$ ἰσχύει $(a_1, \ldots, a_n) \in A_i$. Ἀλλὰ $f_i \in \mathbb{I}(A_i)$, ἄρα $f_i(a_1, \ldots, a_n) = 0$, ὁπότε $(f_1 f_2)(a_1, \ldots, a_n) = f_1(a_1, \ldots, a_n) f_2(a_1, \ldots, a_n) = 0$.

□

Ἐστιάζομε στὸ ἑξῆς τὴν προσοχή μας στὴν περίπτωση $n = 2$ δίνοντας ἐφαρμογὲς τοῦ Θεωρήματος 2.4. Κατ' ἀρχάς, μιὰ προφανὴς ἐπαναδιατύπωση ἐκείνου τοῦ θεωρήματος εἶναι ἡ ἑξῆς:

Θεώρημα 2.13 - ***Ἐπαναδιατύπωση τοῦ Θεωρήματος 2.4.*** *Ἂν τὰ $f, g \in K[X,Y]$ δὲν ἔχουν κοινὸ μὴ σταθερὸ διαιρέτη, τότε οἱ καμπῦλες $\mathbb{V}(f)$ καὶ $\mathbb{V}(g)$ ἔχουν πεπερασμένο πλῆθος κοινῶν σημείων $\in K^2$.* [8]

Τώρα διατυπώνομε τρία θεωρήματα γεωμετρικοῦ ἐνδιαφέροντος, τῶν ὁποίων ἡ ἀπόδειξη στηρίζεται στὰ μέχρι τώρα ἀποτελέσματα τῆς ἑνότητας 2.3 καὶ στὸ παραπάνω Θεώρημα.

Θεώρημα 2.14 *Ἂν τὸ $f \in K[X,Y]$ εἶναι ἀνάγωγο καὶ τὸ $\mathbb{V}(f)$ εἶναι ἄπειρο, τότε $\mathbb{I}(\mathbb{V}(f)) = \langle f \rangle$ καὶ τὸ $\mathbb{V}(f)$ εἶναι ἀνάγωγο ἀλγεβρικὸ σύνολο.*

Ἀπόδειξη. ($\subseteq$) Ἂν $g \in \mathbb{I}(\mathbb{V}(f))$ τότε $\mathbb{V}(g) \supseteq \mathbb{V}(\mathbb{I}(\mathbb{V}(f)))$. Ἐφαρμόζοντας τὸ Πόρισμα 2.8 μὲ A τὸ $\mathbb{V}(f)$, συμπεραίνομε ὅτι $\mathbb{V}(\mathbb{I}(\mathbb{V}(f))) = \mathbb{V}(f)$, ἄρα $\mathbb{V}(g) \supseteq \mathbb{V}(f)$, ὁπότε $\mathbb{V}(f) \cap \mathbb{V}(g) = \mathbb{V}(f)$. Ἐξ ὑποθέσεως, τὸ $\mathbb{V}(f)$ εἶναι ἄπειρο, ἄρα οἱ καμπῦλες $\mathbb{V}(f)$ καὶ $\mathbb{V}(g)$ ἔχουν ἄπειρα κοινὰ σημεῖα $\in K^2$. Λόγῳ τοῦ Θεωρήματος 2.13, αὐτὸ μᾶς ὁδηγεῖ στὸ συμπέρασμα ὅτι τὰ f, g ἔχουν κοινὸ διαιρέτη στὸ $K[X,Y]$. Ὅμως τὸ f εἶναι ἀνάγωγο, ἄρα αὐτὸ ὁ κοινὸς διαιρέτης εἶναι, ἀναγκαστικά, τὸ ἴδιο τὸ f καὶ τὰ συνεταιρικά του. Αὐτὸ σημαίνει ὅτι $f|g$, ἄρα $g \in \langle f \rangle$.

($\supseteq$) Βλ. ἄσκηση 2.9.

Μέχρι στιγμῆς, λοιπόν, ἔχομε ἀποδείξει ὅτι $\mathbb{I}(\mathbb{V}(f)) = \langle f \rangle$ καὶ μένει ἀκόμη νὰ δείξομε ὅτι τὸ $\mathbb{V}(f)$ εἶναι ἀνάγωγο σύνολο. Ἀφοῦ τὸ f εἶναι ἀνάγωγο στὸ $K[X,Y]$ καὶ τὸ $K[X,Y]$ εἶναι περιοχὴ μονοσήμαντης ἀνάλυσης (Θεώρημα 1.15), ἕπεται ὅτι τὸ f εἶναι πρῶτο στοιχεῖο τῆς ἀκέραιας περιοχῆς $K[X,Y]$. Αὐτὸ συνεπάγεται ὅτι, ἂν $f|gh$, τότε $f|g$ εἴτε $f|h$. Ἰσοδύναμη διατύπωση: Ἂν $gh \in \langle f \rangle$ τότε $g \in \langle f \rangle$ εἴτε $h \in \langle f \rangle$· μ' ἄλλα λόγια, τὸ $\langle f \rangle$ εἶναι πρῶτο ἰδεῶδες τοῦ $K[X,Y]$, δηλαδή, τὸ $\mathbb{I}(\mathbb{V}(f))$ εἶναι πρῶτο ἰδεῶδες τοῦ $K[X,Y]$. Ἀλλὰ τότε, ἀπὸ τὸ Θεώρημα 2.12 συμπεραίνομε ὅτι τὸ $\mathbb{V}(f)$ εἶναι ἀνάγωγο σύνολο.

□

Ἄσκηση 2.11 (α′) Ἀποδεῖξτε ὅτι τὸ $Y - X^2 \in \mathbb{C}[X,Y]$ εἶναι ἀνάγωγο.
(β′) Ἀποδεῖξτε ὅτι τὸ ἀλγεβρικὸ σύνολο $\mathbb{V}(Y - X^2)$ εἶναι ἀνάγωγο σύνολο τοῦ $\mathbb{C}^2$.

Ἄσκηση 2.12 Ἀποδεῖξτε ὅτι τὸ $f(X,Y) = Y^2 + X^2(X-1)^2 \in \mathbb{R}[X,Y]$ εἶναι ἀνάγωγο πολυώνυμο, ἀλλὰ τὸ $\mathbb{V}(f)$ δὲν εἶναι ἀνάγωγο ὑποσύνολο τοῦ $\mathbb{R}^2$. Γιατὶ αὐτὸ δὲν ἀντιφάσκει στὸ Θεώρημα 2.14;

Πρόταση 2.15 *Ἂν τὸ K εἶναι ἄπειρο σῶμα, τότε $\mathbb{I}(K^2) = \langle 0 \rangle$*

Ἀπόδειξη. Προφανῶς, τὸ μηδενικὸ πολυώνυμο τοῦ $K[X,Y]$ μηδενίζεται σὲ ὅλα τὰ σημεῖα τοῦ K^2, ἄρα $\langle 0 \rangle \subseteq \mathbb{I}(K^2)$. Ἀντιστρόφως, θὰ δείξομε μὲ εἰς ἄτοπον ἀπαγωγὴ ὅτι τὸ $\mathbb{I}(K^2)$ περιέχει μόνο τὸ μηδενικὸ πολυώνυμο. Ἔστω ὅτι τὸ $f(X,Y) \in \mathbb{I}(K^2)$ εἶναι μὴ μηδενικό. Τότε τὸ f εἶναι μὴ σταθερό, ἄρα, δίχως βλάβη τῆς γενικότητος μποροῦμε νὰ ὑποθέσομε ὅτι ὁ βαθμός του ὡς πρὸς X εἶναι $n \geq 1$ καὶ γράφομε

$$f(X,Y) = g_n(Y)\,X^n + \cdots + g_1(Y)\,X + g_0(Y), \quad g_0(Y), \ldots, g_n(Y) \in K[Y], \quad g_n(Y) \neq 0.$$

Ἔστω $b \in K$, τέτοιο ὥστε $g_n(b) \neq 0$, ὁπότε τὸ πολυώνυμο $h(X) = g_n(b)X^n + \cdots + g_1(b)X + g_0(b) \in K[X]$ εἶναι μὴ μηδενικό. Κρατώντας σταθερὸ τὸ b καὶ ἀφήνοντας τὸ a νὰ διατρέχει

[8] Ἐδῶ καὶ στὸ ἑξῆς, λέγοντας «πεπερασμένο πλῆθος σημείων», ἐννοοῦμε «πεπερασμένο, τὸ πολύ, πλῆθος σημείων», δηλαδή, δὲν ἀποκλείομε τὸ κενὸ σύνολο σημείων.

τὸ K, ἔχομε $h(a) = f(a, b) = 0$, διότι, ἐξ ὑποθέσεως, τὸ f μηδενίζεται σὲ ὅλο τὸ K^2. Ἄρα, τὸ $h(X)$ μηδενίζεται γιὰ κάθε τιμὴ τοῦ K, δηλαδή, τὸ $h(X)$ ἔχει ἄπειρες ρίζες· ἄτοπο.

□

Θεώρημα 2.16 *Ἂν τὸ K εἶναι ἄπειρο σῶμα, τότε τὰ ἀνάγωγα ὑποσύνολα τοῦ K^2 εἶναι τὰ K^2, $\emptyset$, ὅλα τὰ μονοσύνολα (σημεῖα) καὶ ὅλα τὰ ἄπειρα $\mathbb{V}(f)$ μὲ τὸ $f \in K[X, Y]$ ἀνάγωγο.*

Ἀπόδειξη. Ἀπὸ τὴν Πρόταση 2.15 ξέρομε ὅτι $\mathbb{I}(K^2) = \langle 0 \rangle$. Ὅμως τὸ $\langle 0 \rangle$ εἶναι πρῶτο ἰδεῶδες, ἄρα, βάσει τοῦ Θεωρήματος 2.12, τὸ K^2 εἶναι ἀνάγωγο σύνολο.

Τὸ κενὸ σύνολο εἶναι ἀλγεβρικό διότι $\emptyset = \mathbb{V}(1)$ καὶ προφανῶς εἶναι ἀνάγωγο, βάσει τοῦ ὁρισμοῦ τοῦ ἀναγώγου συνόλου.

Κάθε μονοσύνολο εἶναι ἀλγεβρικὸ σύνολο. Πράγματι, ἔστω τὸ $\{(a, b)\}$, ὅπου $a, b \in K$. Τότε, τετριμμένα, $\{(a, b)\} = \mathbb{V}(\{X - a, Y - b\})$, ἄρα τὸ $\{(a, b)\}$ εἶναι ἀλγεβρικὸ σύνολο, τὸ ὁποῖο εἶναι προφανῶς ἀνάγωγο, βάσει τοῦ ὁρισμοῦ τοῦ ἀναγώγου συνόλου.

Τέλος, ἂν τὸ $f \in K[X, Y]$ εἶναι ἀνάγωγο πολυώνυμο καὶ τὸ $\mathbb{V}(f)$ εἶναι ἄπειρο, τότε τὸ Θεώρημα 2.14 μᾶς ἐξασφαλίζει ὅτι τὸ $\mathbb{V}(f)$ εἶναι ἀνάγωγο.

Συνεπῶς, μέχρι στιγμῆς ἔχομε δείξει ὅτι ὅλα τὰ σύνολα, ποὺ περιγράφονται στὴν ἐκφώνηση τοῦ θεωρήματος, εἶναι ὄντως ἀνάγωγα.

Ἀντιστρόφως, ἔστω μὴ κενὸ ἀνάγωγο ἀλγεβρικὸ σύνολο $A \subsetneq K^2$.

Ἂν $\mathbb{I}(A) = \langle 0 \rangle$, τότε $\mathbb{I}(A) = \mathbb{I}(K^2)$ (τὸ δείξαμε παραπάνω), ἄρα, $A =$ (Πόρισμα 2.8) $\mathbb{V}(\mathbb{I}(A)) = \mathbb{V}(\mathbb{I}(K^2)) =$ (Πόρισμα 2.8) K^2. Στὴν περίπτωση αὐτή, δηλαδή, $A = K^2$.

Ἂν τὸ A εἶναι πεπερασμένο, ἔστω $A = \{(a_1, b_1), \ldots, (a_r, b_r)\}$, τότε, ἀναγκαστικά, $r = 1$, διότι, διαφορετικὰ τὸ A θὰ γραφόταν ὡς ἕνωση $r > 1$ ἀναγώγων ὑποσυνόλων του: $A = \cup_{i=1}^{r} \{(a_i, b_i)\}$. Συνεπῶς $r = 1$ καὶ τὸ A εἶναι μονοσύνολο.

Μένει, τέλος, ἡ περίπτωση ποὺ $\emptyset \subsetneq A \subsetneq K^2$, $\mathbb{I}(A) \neq \langle 0 \rangle$ καὶ τὸ A εἶναι ἄπειρο. Στόχος μας, σ' αὐτὴ τὴν περίπτωση, εἶναι να δείξομε ὅτι $A = \mathbb{V}(p)$, γιὰ κάποιο ἀνάγωγο πολυώνυμο $p \in K[X, Y]$. Κατ' ἀρχὰς παρατηροῦμε ὅτι τὸ ἰδεῶδες $\mathbb{I}(A)$ περιέχει μὴ σταθερὰ πολυώνυμα καὶ ἔστω $f \in \mathbb{I}(A)$ ἕνα τέτοιο πολυώνυμο. Ἔστω $f = p_1 \cdots p_r$ ἡ ἀνάλυση τοῦ f σὲ ἀνάγωγα πολυώνυμα τοῦ $K[X, Y]$. Ἐπειδὴ τὸ A εἶναι ἀνάγωγο, τὸ $\mathbb{I}(A)$ εἶναι πρῶτο ἰδεῶδες, βάσει τοῦ Θεωρήματος 2.12. Ἔχομε λοιπόν, $p_1 \cdots p_r = f \in \mathbb{I}(A)$, μὲ τὸ $\mathbb{I}(A)$ πρῶτο, ἄρα ἕνα τοὐλάχιστον $p_i \in \mathbb{I}(A)$. Συνοψίζοντας, καταλήξαμε στὸ συμπέρασμα ὅτι ὑπάρχει $p \in \mathbb{I}(A)$ ἀνάγωγο στὸ $K[X, Y]$ καὶ μένει νὰ δείξομε ὅτι $\mathbb{I}(A) = \langle p \rangle$, διότι τότε, $A =$ (Πόρισμα 2.8) $\mathbb{V}(\mathbb{I}(A)) = \mathbb{V}(p)$. Κατ' ἀρχάς, ἀφοῦ $p \in \mathbb{I}(A)$, ἔπεται ὅτι $\langle p \rangle \subseteq \mathbb{I}(A)$. Ἂν δὲν ἴσχυε ἡ ἰσότητα στὴν τελευταία σχέση, θὰ μπορούσαμε νὰ βροῦμε $g \in \mathbb{I}(A) \setminus \langle p \rangle$ καὶ αὐτό, εἰδικώτερα, συνεπάγεται ὅτι τὸ g δὲν διαιρεῖται ἀπὸ τὸ p, ἄρα τὰ g καὶ p δὲν ἔχουν κοινὸ παράγοντα, ὁπότε τὸ $\mathbb{V}(g) \cap \mathbb{V}(p)$ εἶναι πεπερασμένο, βάσει τοῦ Θεωρήματος 2.13. Ἀφ' ἑτέρου ἔχομε $\{p, g\} \subseteq \mathbb{I}(A)$, ἄρα (ἄσκηση 2.3) $\mathbb{V}(\mathbb{I}(A)) \subseteq \mathbb{V}(\{p, g\})$ καί, συνεπῶς, $A =$ (Πόρισμα 2.8) $\mathbb{V}(\mathbb{I}(A)) \subseteq \mathbb{V}(\{p, g\}) = \mathbb{V}(p) \cap \mathbb{V}(g)$. Ἔτσι ὁδηγούμαστε στὸ συμπέρασμα ὅτι τὸ ἄπειρο σύνολο A περιέχεται στὸ πεπερασμένο σύνολο $\mathbb{V}(p) \cap \mathbb{V}(g)$· ἀντίφαση.

□

Ἄσκηση 2.13 Ἔστω K ἄπειρο σῶμα καὶ $V_1 \neq V_2$ μὴ κενὰ ἀνάγωγα γνήσια ὑποσύνολα τοῦ K^2. Ἀποδεῖξτε ὅτι $V_1 \not\subseteq V_2$.

Ὑπόδειξη. Συνδυᾶστε τὰ Θεωρήματα 2.16 καὶ 2.13.

Ὁρισμός. Ἕνα σῶμα K χαρακτηρίζεται *ἀλγεβρικῶς κλειστό*, ἂν κάθε μὴ σταθερὸ πολυώνυμο τοῦ $K[X]$ ἔχει ρίζα στὸ K.

Τὸ ‘‘διασημότερο’’ παράδειγμα ἀλγεβρικῶς κλειστοῦ σώματος εἶναι τὸ $\mathbb{C}$.

Ἄσκηση 2.14 Κάθε ἀλγεβρικῶς κλειστὸ σῶμα εἶναι ἄπειρο.

Ὑπόδειξη. Ἂν $1, a_2, \ldots, a_m$ ἦταν ὅλα τὰ στοιχεῖα τοῦ ἀλγεβρικῶς κλειστοῦ σώματος K, θεωρῆστε τὸ $f(X) = (X-1)(X-a_2)\cdots(X-a_m)+1$.

Ἄσκηση 2.15 Ἂν τὸ K εἶναι ἀλγεβρικῶς κλειστὸ σῶμα K καὶ $f \in K[X_1, \ldots, X_n]$, τότε $\mathbb{V}(f) \neq \emptyset$.

Ἄσκηση 2.16 Ἂν τὸ K εἶναι ἀλγεβρικῶς κλειστὸ σῶμα καὶ τὸ $f \in K[X,Y]$ εἶναι μὴ σταθερό, τότε τὸ $\mathbb{V}(f)$ εἶναι ἄπειρο.

Ὑπόδειξη. Γρᾶψτε τὸ f ὅπως στὴν ἀπόδειξη τοῦ Θεωρήματος 2.16.

Θεώρημα 2.17 *Ἔστω K ἀλγεβρικῶς κλειστὸ σῶμα καὶ μὴ σταθερὸ $f \in K[X,Y]$. Ἔστω $f = p_1^{n_1}\cdots p_r^{n_r}$ ἡ ἀνάλυση τοῦ f σὲ ἀνάγωγα τοῦ $K[X,Y]$, ὅπου τὰ ἀνάγωγα πολυώνυμα $p_1, \ldots, p_r$ εἶναι διαφορετικὰ μεταξύ τους καὶ οἱ ἐκθέτες τους $n_1, \ldots, n_r$ εἶναι ὅλοι θετικοί. Τότε,*

$$\mathbb{V}(f) = \mathbb{V}(p_1) \cup \cdots \cup \mathbb{V}(p_r), \quad \mathbb{I}(\mathbb{V}(f)) = \langle p_1 \cdots p_r \rangle$$

καὶ καθένα ἀπὸ τὰ $\mathbb{V}(p_i)$ εἶναι ἀνάγωγο ἀλγεβρικὸ σύνολο.

Ἀπόδειξη. Κάποιες προκαταρκτικὲς παρατηρήσεις: Κάθε $\mathbb{V}(p_i)$ εἶναι ἄπειρο σύνολο (ἄσκηση 2.16). Ἐπίσης, γιὰ $i \neq j$, τὰ p_i, p_j δὲν ἔχουν κοινὸ μὴ σταθερὸ διαιρέτη, ἀφοῦ εἶναι διαφορετικὰ ἀνάγωγα πολυώνυμα. Ἄρα τὸ $\mathbb{V}(p_i) \cap \mathbb{V}(p_j)$ εἶναι πεπερασμένο σύνολο, βάσει τοῦ Θεωρήματος 2.13. Μποροῦμε τώρα νὰ συμπεράνομε ὅτι, ἂν $i \neq j$, τότε $\mathbb{V}(p_i) \not\subseteq \mathbb{V}(p_j)$. Διότι, ἂν ἦταν $\mathbb{V}(p_i) \subseteq \mathbb{V}(p_j)$, τότε τὸ ἄπειρο σύνολο $\mathbb{V}(p_i) \subseteq \mathbb{V}(p_i) \cap \mathbb{V}(p_j) =$ πεπερασμένο σύνολο.

Εἶναι προφανὲς ὅτι $\mathbb{V}(p_i^{n_i}) = \mathbb{V}(p_i)$, ἄρα

$$\mathbb{V}(f) = \mathbb{V}(p_1^{n_1}\cdots p_r^{n_r}) = \text{ (ἄσκηση 2.5) } \mathbb{V}(p_1^{n_1}) \cup \cdots \cup \mathbb{V}(P_r^{n_r}) = \mathbb{V}(p_1) \cup \cdots \cup \mathbb{V}(p_r).$$

Καθένα ἀπὸ τὰ $\mathbb{V}(p_i)$ εἶναι ἄπειρο, ἄρα, ἀπὸ τὸ Θεώρημα 2.14, εἶναι ἀνάγωγο ἀλγεβρικὸ σύνολο. Ἐπίσης, ἀπὸ τὴν παραπάνω σχέση ἕπεται ὅτι

$$\begin{aligned}\mathbb{I}(\mathbb{V}(f)) &= \mathbb{I}(\mathbb{V}(p_1) \cup \cdots \cup \mathbb{V}(p_r)) = \text{ (ἄσκηση 2.8) } \mathbb{I}(\mathbb{V}(p_1)) \cap \cdots \cap \mathbb{I}(\mathbb{V}(p_r)) \\ &= \text{ (Θεώρημα 2.14) } \langle p_1 \rangle \cap \cdots \cap \langle p_r \rangle,\end{aligned}$$

ὁπότε μένει νὰ δείξομε ὅτι $\langle p_1 \rangle \cap \cdots \cap \langle p_r \rangle = \langle p_1 \cdots p_r \rangle$. Πράγματι, κάθε p_i διαιρεῖ τὸ γινόμενο $p_1 \cdots p_r$, ὁπότε $\langle p_1 \cdots p_r \rangle \subseteq \langle p_i \rangle$ γιὰ κάθε $i = 1, \ldots, r$. Ἄρα, $\langle p_1 \cdots p_r \rangle \subseteq \langle p_1 \rangle \cap \cdots \cap \langle p_r \rangle$. Ἀντιστρόφως, ἂν $g \in \langle p_1 \rangle \cap \cdots \cap \langle p_r \rangle$ τότε τὸ g διαιρεῖται ἀπὸ ὅλα τὰ p_i, ἄρα διαιρεῖται καὶ ἀπὸ τὸ γινόμενό τους, ἀφοῦ τὰ p_i εἶναι ἀνὰ δύο πρῶτα μεταξύ τους (βλ. ἄσκηση 1.13 (δ′)). Ἀλλὰ ἡ σχέση $p_1 \cdots p_r | g$ σημαίνει ὅτι $g \in \langle p_1 \cdots p_r \rangle$. Ἔτσι, κάθε στοιχεῖο τοῦ $\langle p_1 \rangle \cap \cdots \cap \langle p_r \rangle$ ἀνήκει στὸ $\langle p_1 \cdots p_r \rangle$· αὐτὸ ὁλοκληρώνει τὴν ἀπόδειξη.

□

Ἄσκηση 2.17 Γρᾶψτε τὸ ἀλγεβρικὸ σύνολο $\mathbb{V}(\{Y^4 - X^2, Y^4 - X^2Y^2 + XY^2 - X^3\}) \subseteq \mathbb{C}^2$ ὡς ἕνωση ἀναγώγων ἀλγεβρικῶν ὑποσυνόλων τοῦ $\mathbb{C}^2$.

Ὑπόδειξη. Ἀναλύστε τὰ πολυώνυμα $Y^4 - X^2$ καὶ $Y^4 - X^2Y^2 + XY^2 - X^3$ σὲ γινόμενο ἀναγώγων πολυωνύμων. Χρησιμοποιεῖστε τὴν ἄσκηση 2.5 καὶ τὸ Θεώρημα 2.17. Χρησιμοποιεῖστε τὴ συνολοθεωρητικὴ ταυτότητα $[\cup_i A_i] \cap [\cup_j B_j] = \cup_{i,j}(A_i \cap B_j)$ (ὅπου τὰ i, j διατρέχουν κάποια σύνολα δεικτῶν).

Τὸ Nullstellensatz τοῦ Hilbert

Πρόταση-Ὁρισμός 2.18 *Ἔστω R μεταθετικὸς δακτύλιος μὲ μοναδιαῖο καὶ J ἰδεῶδες τοῦ R. Τὸ σύνολο*

$$\mathrm{Rad}(J) = \{r \in R : \exists\, n = n(r),\ \text{τέτοιο ὥστε } r^n \in J\}$$

εἶναι ἰδεῶδες, ποὺ περιέχει τὸ J καὶ λέγεται ριζικὸ τοῦ J. Ἂν ἰσχύει $\mathrm{Rad}(J) = J$, τότε τὸ ἰδεῶδες J χαρακτηρίζεται ριζικό.

Ἀπόδειξη. Ἀρχικὰ κάνομε τὴν παρατήρηση, ποὺ ἀφορᾷ γενικὰ σὲ μεταθετικοὺς δακτυλίους μὲ μοναδιαῖο, ὅτι, γιὰ $a, b \in R$ καὶ $n \in \mathbb{N}$ ἰσχύει τὸ διωνυμικὸ ἀνάπτυγμα

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k.$$

Τώρα θ' ἀποδείξομε ὅτι, ἂν $a, b \in \mathrm{Rad}(J)$, τότε $a + b \in \mathrm{Rad}(J)$. Ἀπὸ τὴν ὑπόθεση ξέρομε ὅτι ὑπάρχουν $m, n \in \mathbb{N}$, τέτοια ὥστε $a^m \in \mathrm{Rad}(J)$ καὶ $b^n \in \mathrm{Rad}(J)$. Ἀρκεῖ ν' ἀποδείξομε ὅτι $(a+b)^{m+n} \in J$. Πράγματι, ἂν θεωρήσομε τὸ διωνυμικὸ ἀνάπτυγμα $(a+b)^{m+n}$, ὁ τυπικὸς προσθετέος του εἶναι $\binom{m+n}{k} a^{m+n-k} b^k$ $(0 \le k \le m+n)$. Διακρίνομε δύο περιπτώσεις: Ἂν $k \ge n$, τότε $b^k = b^{k-n} b^n \in J$, διότι $b^{k-n} \in R$ καὶ $b^n \in J$· ἔπεται ἐξ αὐτοῦ ὅτι ὅλος ὁ προσθετέος ἀνήκει στὸ J. Ἂν $k \le n$, τότε $a^{m+n-k} = a^{n-k} a^m \in J$, διότι $a^{n-k} \in R$ καὶ $a^m \in J$· ἄρα, πάλι ὅλος ὁ προσθετέος ἀνήκει στὸ J.
Τέλος, ἂν $r \in R$ καὶ $a \in \mathrm{Rad}(J)$, τότε $ra \in \mathrm{Rad}(J)$. Διότι, ἀπὸ τὴ σχέση $a \in \mathrm{Rad}(J)$ ἔπεται ὅτι $a^m \in J$ γιὰ κάποιο $m \in \mathbb{N}$. Τότε, ὅμως, $(ra)^m = r^m a^m \in J$.

□

Πρόταση 2.19 *Ἂν $A \subseteq K^n$, τότε τὸ $\mathbb{I}(A)$ εἶναι ριζικὸ ἰδεῶδες τοῦ $K[X_1, \ldots, X_n]$.*

Ἀπόδειξη. Ξέρομε ἀπὸ τὴν προηγούμενη Πρόταση-Ὁρισμό ὅτι $\mathbb{I}(A) \subseteq \mathrm{Rad}(\mathbb{I}(A))$. Ἀντιστρόφως, θεωροῦμε $f \in \mathrm{Rad}(\mathbb{I}(A))$ καὶ θ' ἀποδείξομε ὅτι $f \in \mathbb{I}(A)$. Γιὰ τὴν ἀπόδειξη τῆς τελευταίας σχέσης πρέπει νὰ πάρομε $(a_1, \ldots, a_n) \in A$ καὶ νὰ δείξομε ὅτι $f(a_1, \ldots, a_n) = 0$. Ὅμως, ἀπὸ τὴν ὑπόθεση $f \in \mathrm{Rad}(\mathbb{I}(A))$ ἔχομε ὅτι, γιὰ κάποιο $m \in \mathbb{N}$ εἶναι $f^m \in \mathbb{I}(A)$, ὁπότε $f^m(a_1, \ldots, a_n) = 0$. Ἀλλὰ $f^m(a_1, \ldots, a_n) = f(a_1, \ldots, a_n)^m$ καί, συνεπῶς, ἡ σχέση $f^m(a_1, \ldots, a_n) = 0$ συνεπάγεται ὅτι $f(a_1, \ldots, a_n) = 0$.

□

Ἄσκηση 2.18 Ἔστω J ἰδεῶδες τοῦ $K[X_1, \ldots, X_n]$. Ἀποδεῖξτε ὅτι $\mathbb{V}(J) = \mathbb{V}(\mathrm{Rad}(J))$.

Θεώρημα 2.20 - ***Nullstellensatz τοῦ Hilbert***. *Ἂν τὸ K εἶναι ἀλγεβρικῶς κλειστὸ σῶμα καὶ J εἶναι ἰδεῶδες τοῦ $K[X_1, \ldots, X_n]$, τότε $\mathbb{I}(\mathbb{V}(J)) = \mathrm{Rad}(J)$.*

Ἡ ἀπόδειξη αὐτοῦ τοῦ θεωρήματος δὲν ἐμπίπτει στοὺς σκοποὺς τοῦ μαθήματος, πλὴν ὅμως, θὰ δοῦμε δύο ἐφαρμογές, οἱ ὁποῖες σχετίζονται μὲ τὴν ὕλη τῆς ἑνότητας 2.3.

Πόρισμα 2.21 *Ἔστω ὅτι τὸ K εἶναι ἀλγεβρικῶς κλειστὸ σῶμα καὶ $S, S' \subseteq K[X_1, \ldots, X_n]$. Τότε ἰσχύει ἡ ἑξῆς ἰσοδυναμία:*

$$\mathbb{V}(S) = \mathbb{V}(S') \ \Leftrightarrow\ \mathrm{Rad}(\langle S \rangle) = \mathrm{Rad}(\langle S' \rangle).$$

Ἀπόδειξη. Προκαταρκτικὴ παρατήρηση: Γιὰ κάθε $S \subseteq K[X_1, \ldots, X_n]$ ἰσχύει

$$\mathbb{V}(S) = \text{ (Πρόταση 2.5) } \mathbb{V}(\langle S \rangle) = \text{ (ἄσκηση 2.18) } \mathbb{V}(\mathrm{Rad}(\langle S \rangle)). \tag{2.8}$$

Ἂν $\mathrm{Rad}(\langle S \rangle) = \mathrm{Rad}(\langle S' \rangle)$, τότε $\mathbb{V}(\mathrm{Rad}\langle S \rangle)) = \mathbb{V}(\mathrm{Rad}(\langle S' \rangle))$, καὶ ἐφαρμόζοντας τὴν (2.8) γιὰ τὰ S καὶ S', βλέπομε ἀμέσως ὅτι $\mathbb{V}(S) = \mathbb{V}(S')$.

Ἀντιστρόφως, ἔστω ὅτι $\mathbb{V}(S) = \mathbb{V}(S')$. Τότε $\mathbb{V}(\langle S \rangle) = \mathbb{V}(\langle S' \rangle)$, ἄρα $\mathbb{I}(\mathbb{V}(\langle S \rangle)) = \mathbb{I}(\mathbb{V}(\langle S' \rangle))$. Ἐφαρμόζοντας τὸ Θεώρημα 2.20 μὲ τὰ $\langle S \rangle$ καὶ $\langle S' \rangle$ στὴ θέση τοῦ J, συμπεραίνομε ὅτι $\mathrm{Rad}(\langle S \rangle) = \mathrm{Rad}(\langle S' \rangle)$.

□

Πόρισμα 2.22 *Ἂν τὸ K εἶναι ἀλγεβρικῶς κλειστὸ σῶμα καὶ J ἰδεῶδες τοῦ $K[X_1, \ldots, X_n]$, τότε ἰσχύει ἡ ἰσοδυναμία:*

$$\mathbb{V}(J) = \emptyset \;\Leftrightarrow\; J = K[X_1, \ldots, X_n].$$

Συνεπῶς, ἂν τὸ J εἶναι γνήσιο ἰδεῶδες τοῦ $K[X_1, \ldots, X_n]$, τότε $\mathbb{V}(J) \neq \emptyset$.

Ἀπόδειξη. Μιὰ προφανὴς προκαταρκτικὴ παρατήρηση εἶναι ὅτι $K[X_1, \ldots, X_n] = \langle 1 \rangle = \mathrm{Rad}(\langle 1 \rangle)$. Ἄρα,

$$\begin{aligned} \mathbb{V}(J) = \emptyset &\Rightarrow \mathbb{V}(J) = \mathbb{V}(\langle 1 \rangle) \Rightarrow \text{(Πόρισμα 2.21) } \mathrm{Rad}(J) = \mathrm{Rad}(\langle 1 \rangle) = K[X_1, \ldots, X_n] \\ &\Rightarrow 1 \in \mathrm{Rad}(J) \Rightarrow 1 \in J \Rightarrow J = K[X_1, \ldots, X_n]. \end{aligned}$$

Γιὰ τὴν ἀπόδειξη τοῦ ἀντιστρόφου δὲν χρειάζεται τὸ Nullstellensatz· στὴν πραγματικότητα, ἡ ἀπόδειξη εἶναι τετριμμένη:

$$J = K[X_1, \ldots, X_n] \Rightarrow 1 \in J \Rightarrow \{1\} \subseteq J \Rightarrow \text{(ἄσκηση 2.3) } \mathbb{V}(J) \subseteq \mathbb{V}(\langle 1 \rangle) = \emptyset \Rightarrow \mathbb{V}(J) = \emptyset.$$

□

Ἄσκηση 2.19 Ἔστω ὅτι $f_1, \ldots, f_m \in \mathbb{C}[X_1, \ldots, X_n]$ καὶ σᾶς δίδεται ἡ πληροφορία ὅτι τὸ σύστημα

$$\begin{cases} f_1(z_1, \ldots, z_n) &= 0 \\ \quad\vdots & \vdots \;\; \vdots \\ f_m(z_1, \ldots, z_n) &= 0 \end{cases}$$

δὲν ἔχει λύση $(z_1, \ldots, z_n) \in \mathbb{C}^n$. Ἀποδεῖξτε ὅτι ὑπάρχουν $g_1, \ldots, g_m \in \mathbb{C}[X_1, \ldots, X_n]$, τέτοια ὥστε $g_1 f_1 + \cdots + g_m f_m = 1$.
Ὁ ἀντίστροφος ἰσχυρισμός, δηλαδή, ἂν ὑπάρχουν $g_1, \ldots, g_m \in \mathbb{C}[X_1, \ldots, X_n]$, τέτοια ὥστε $g_1 f_1 + \cdots + g_m f_m = 1$, τότε τὸ παραπάνω σύστημα εἶναι ἀδύνατο, βλέπετε ὅτι εἶναι προφανής;

Ἄσκηση 2.20 (α′) Ἔστω σῶμα K, $f(x_1, \ldots, X_n) \in K[X_1, \ldots, X_n]$ καὶ $a_1, \ldots, a_n \in K^n$. Ἀποδεῖξτε ὅτι ὑπάρχουν πολυώνυμα $g_i(X_i, \ldots, X_n) \in K[X_i, \ldots, X_n]$ $(i = 1, \ldots, n)$ καὶ $r \in K$, τέτοια ὥστε

$$f = (X_1 - a_1) \cdot g_1(X_1, \ldots, X_n) + (X_2 - a_2) \cdot g_2(X_2, \ldots, X_n) + \cdots (X_n - a_n) \cdot g_n(X_n) + r.$$

Ὑπόδειξη. Ἀπόδειξη ἐπαγωγική. Θὰ ἔχετε ὑπ' ὄψιν ὅτι ἡ εὐκλείδεια διαίρεση ἰσχύει καὶ σὲ ἀκέραιες περιοχές (π.χ. $K[X_\nu, X_{\nu+1}, \ldots, X_n]$) ὅταν ὁ διαιρέτης (π.χ. $X_\nu - a_\nu$) ἔχει συντελεστὴς τοῦ μεγιστοβαθμίου ὅρου εἶναι μονάδα τῆς ἀκέραιας περιοχῆς.

(β′) Ἔστω ἀλγεβρικῶς κλειστὸ σῶμα K καὶ J maximal ἰδεῶδες τοῦ $K[X_1, \ldots, X_n]$. Ἀποδεῖξτε ὅτι ὑπάρχουν $a_1, \ldots, a_n \in K$, τέτοια ὥστε $J = \langle X_1 - a_1, \ldots, X_n - a_n \rangle$.

Ὑπόδειξη. Ἔστω $f \in J$. Ἀπὸ τὴν ἄσκηση 2.15, $\mathbb{V}(f) \neq \emptyset$. Ἔστω $(a_1, \ldots, a_n) \in \mathbb{V}(f)$. Ἀποδεῖξτε ὅτι $J = \langle X_1 - a_1, \ldots, X_n - a_n \rangle$. Εκμεταλλευθεῖτε τὸ ἐρώτημα (α′).

Ἄσκηση 2.21 Ἔστω $f = Y^4 - X^2$, $g = Y^4 - X^2Y^2 + XY^2 - X^3 \in \mathbb{C}[X, Y]$. Γράψτε τὸ ἀλγεβρικὸ σύνολο $\mathbb{V}(\{f, g\})$ ὡς ἕνωση ἀναγώγων ἀλγεβρικῶν συνόλων τοῦ $\mathbb{C}^2$, κανένα ἐκ τῶν ὁποίων δὲν περιέχεται σὲ κάποιο ἀπὸ τὰ ὑπόλοιπα.

Ἀπάντηση: $\mathbb{V}(\{f, g\}) = \mathbb{V}(Y^2 + X) \cup \{(1, -1)\} \cup \{(1, 1)\}$.

Ἄσκηση 2.22 Ἀποδεῖξτε ὅτι, γιὰ κάθε $c \in \mathbb{C}$, τὸ $\mathbb{V}(Y^2 - X(X-1)(X-c))$ εἶναι ἀνάγωγο ἀλγεβρικὸ σύνολο (καμπύλη) τοῦ $\mathbb{C}^2$.

Ἄσκηση 2.23 Ἔστω D περιοχὴ μονοσήμαντης ἀνάλυσης καὶ P μὴ μηδενικὸ πρῶτο καὶ κύριο ἰδεῶδες τῆς D.

(α′) Ἀποδεῖξτε ὅτι ὑπάρχει πρῶτο στοιχεῖο $\pi \in D$, τέτοιο ὥστε $P = \langle \pi \rangle$.

Ὑπόδειξη. Ἐξ ὑποθέσεως ὑπάρχει $r \in D$, τέτοιο ὥστε $P = \langle r \rangle$. Θεωρῆστε τὴ μονοσήμαντη ἀνάλυση $r = \pi_1 \cdots \pi_m$ σὲ πρῶτα στοιχεῖα τῆς D. Χρησιμοποιώντας τὴν ὑπόθεση ὅτι τὸ P εἶναι πρῶτο, ἀποδεῖξτε ὅτι, ἀναγκαστικά, $m = 1$.

(β′) Ἀποδεῖξτε ὅτι δὲν ὑπάρχει πρῶτο ἰδεῶδες Q τῆς D, τέτοιο ὥστε $\langle 0 \rangle \subsetneq Q \subsetneq P$.

Ὑπόδειξη. Βάσει τοῦ (α′), ἔστω $P = \langle \pi \rangle$. Εἶναι $Q \subsetneq D$, διότι τὸ Q εἶναι πρῶτο. Ἄρα ὑπάρχει $q \in Q$, ποὺ δὲν εἶναι μονάδα. Προφανῶς, $q \in P = \langle \pi \rangle$, ἄρα $\pi | q$. Συνεπῶς, ἂν θεωρήσει κανεὶς τὴν ἀνάλυση τοῦ q σὲ πρῶτα στοιχεῖα τῆς D, αὐτὴ θὰ εἶναι, ἢ τῆς μορφῆς $q = (\text{μονάδα}) \cdot \pi$, ἢ $q = \pi\pi_2 \cdots \pi_m$ μὲ $m \geq 2$ καὶ $\pi_2, \ldots, \pi_m$ πρῶτα στοιχεῖα τῆς D. Ἀποδεῖξτε ὅτι καὶ τὰ δύο ἐνδεχόμενα ὁδηγοῦν στὴ σχέση $\pi \in Q$, ἄρα στὴν $P = Q$, ποὺ ἀντιβαίνει στὴν ὑπόθεση.

(γ′) Ἔστω σῶμα K καὶ $f \in K[X_1, \ldots, X_n]$ ἀνάγωγο μὴ σταθερὸ πολυώνυμο μὲ $\mathbb{V}(f)$ ἄπειρο. Ἀποδεῖξτε ὅτι τὸ $\mathbb{V}(f)$ δὲν περιέχεται γνησίως σὲ κανένα γνήσιο ἀλγεβρικὸ ὑποσύνολο τοῦ K^n.

Ὑπόδειξη. Ἔστω ἀλγεβρικὸ ὑποσύνολο $A \subsetneq K^n$, τέτοιο ὥστε $\mathbb{V}(f) \subsetneq A$. Ἐκμεταλλευόμενοι τὸ Πόρισμα 2.8, ἀποδεῖξτε ὅτι $\mathbb{I}(K^n) \subsetneq \mathbb{I}(A) \subsetneq \mathbb{I}(\mathbb{V}(f))$. Τί ἰδεῶδες εἶναι τὸ $\mathbb{I}(A)$; Μετά, δεῖτε μὲ ποιὰ ἰδεώδη εἶναι ἴσα τὰ $\mathbb{I}(K^n)$ καὶ $\mathbb{I}(\mathbb{V}(f))$, καὶ ἐφαρμόστε τὸ ἐρώτημα (β′).

Εὑρετήριο

Βιβλιογραφία

[1] Δ. Βάρσος, Δ. Δεριζιώτης, Γ. Ἐμμανουήλ, Μ. Μαλιάκας, Ὀ. Ταλέλλη, *Μιὰ Εἰσαγωγὴ στὴν Ἄλγεβρα*, Ἐκδόσεις ΣΟΦΙΑ, Ἀθήνα 2012.