Διαιρετότητα σὲ ἀκέραιες περιοχές

Ν.Γ. Τζανάκης

Τμῆμα Μαθηματικῶν

Πανεπιστήμιο Κρήτης - Ἡράκλειο

Ἐαρινὸ ἑξάμηνο 2015

Σ' αὐτὲς τὶς σημειώσεις, το D συμβολίζει πάντα ἀκέραια περιοχή.

1 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 σῶμα πηλίκων τῆς D,[1] 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*, ἡ *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. Συμπεράνατε ὅτι, ἂν ἔχομε δύο συνεταιρικὰ στοιχεῖα, τότε τὸ ἕνα εἶναι ἀνάγωγο ἄν, καὶ μόν ἄν, τὸ ἄλλο εἶναι ἀνάγωγο.*

[1] Βλ. [1, §2.2] ἢ, πιὸ ἀναλυτικά, [2, §4.4].

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 (γ΄), 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 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}.

Πρόταση 1.2 *Ἔστω $d \in \mathbb{N}$ καὶ ἡ ἀκέραια περιοχὴ $D = \{a + bi\sqrt{d} : a, b \in \mathbb{Z}\}$. Ἔστω $n_0 = \min\{|\delta|^2 : 0 \neq \delta \in D \setminus D^*\}$.* [2] *Τότε:*

[2] Παρατηρῆστε ὅτι, ἂν $0 \neq \delta = a + bi\sqrt{d} \in D \setminus D^*$, τότε $|\delta|^2 = a^2 + db^2 \in \mathbb{N}$.

(α΄) $n_0 \geq 2$.
(β΄) *Ἂν γιὰ κάποιο* δ *ἰσχύει* $|\delta|^2 = n_0$, *τότε τὸ* δ *εἶναι ἀνάγωγο στοιχεῖο τῆς* D.
(γ΄) *Ἡ* D *εἶναι περιοχὴ ἀνάλυσης.*

Ἀπόδειξη. *(α΄)* Θὰ ἀποδείξομε ὅτι, γιὰ κάθε $\delta \in D \setminus D^*$ εἶναι $|\delta|^2 \geq 2$.

Ξεχωρίζομε τὴν περίπτωση $d = 1$. Στὴν περίπτωση αὐτή, τὰ στοιχεῖα τῆς D εἶναι τῆς μορφῆς $a + bi$, $a, b \in \mathbb{Z}$, ὁπότε $|a + bi|^2 = a^2 + b^2$. Ἂν ἦταν $a^2 + b^2 = 1$, τότε, ἀναγκαστικά, ἕνας ἐκ τῶν a, b θὰ ἔπρεπε νὰ εἶναι μηδέν, ἄρα θὰ εἴχαμε $\delta \in \{\pm 1, \pm i\}$· ἄτοπο, καθὼς οἱ $\pm 1, \pm i$ εἶναι μονάδες τῆς D. Ἄρα $a^2 + b^2 \geq 2$.

Ἔστω τώρα ὅτι $d \geq 2$ καὶ $0 \neq \delta = a + bi\sqrt{d} \in D \setminus D^*$. Εἶναι $|\delta|^2 = a^2 + db^2$. Ἂν $b \neq 0$, τότε $a^2 + db^2 \geq d \geq 2$. Ἂν $b = 0$, τότε $\delta = a \in \mathbb{Z}$. Ἐπειδὴ $0 \neq \delta \notin D^*$, ἕπεται ὅτι $a \neq 0, \pm 1$, ἄρα $|a| \geq 2$, ὁπότε $|\delta|^2 = a^2 \geq 4$.

(β΄) Ἔστω ὅτι $\delta \in D$ καὶ $|\delta|^2 = n_0$. Ἂν τὸ δ δὲν ἦταν ἀνάγωγο, θὰ ὑπῆρχαν $\alpha, \beta \in D \setminus D^*$, τέτοια ὥστε $\delta = \alpha\beta$, ὁπότε $n_0 = |\delta|^2 = |\alpha|^2 |\beta|^2$. Ὅμως, ἀπὸ τὸ (α΄) ξέρομε ὅτι $|\alpha|^2 \geq 2$, ὁπότε $|\beta|^2 = n_0/|\alpha|^2 \leq n_0^2/2 < n_0$. Ἄρα, γιὰ τὸ β, ποὺ εἶναι μὴ μηδενικὸ στοιχεῖο τοῦ $D \setminus D^*$, ἰσχύει $|\beta|^2 < n_0$· αὐτὸ ἔρχεται σὲ ἀντίφαση μὲ τὸν ὁρισμὸ τοῦ n_0.

(γ΄) Θὰ δείξομε ὅτι κάθε μὴ μηδενικὸ $\delta \in D \setminus D^*$ ἀναλύεται σὲ γινόμενο ἀναγώγων στοιχείων τῆς D. Ἡ ἀπόδειξη θὰ γίνει ἐπαγωγικὰ ἐπὶ τοῦ φυσικοῦ ἀριθμοῦ $|\delta|^2 = n \geq n_0$. Ἡ μορφὴ τῆς ἐπαγωγῆς, ποὺ θ' ἀκολουθήσομε, εἶναι αὐτὴ τοῦ Θεωρήματος Α΄.1.

• Ἂν $|\delta| = n_0$, τότε, λόγῳ τοῦ (β΄), τὸ δ εἶναι ἀνάγωγο, ὁπότε τὸ δ εἶναι ἤδη "ἀναλυμένο" σὲ ἀνάγωγα. Ἄρα, σ' αὐτὸ τὸ βῆμα ἀποδείξαμε ὅτι *κάθε στοιχεῖο τοῦ* $\delta \in D \setminus D^*$ *μὲ* $|\delta|^2 = n_0$ *ἀναλύεται σὲ γινόμενο ἀναγώγων.*

• Ἔστω $n > n_0$. Ὑποθέτομε (ἐπαγωγικὴ ὑπόθεση) ὅτι *κάθε μὴ μηδενικὸ στοιχεῖο* $\delta \in D \setminus D^*$ *μὲ* $|\delta|^2 < n$ *ἀναλύεται σὲ γινόμενο ἀναγώγων.*

• Τώρα θὰ ἀποδείξομε ὅτι *κάθε στοιχεῖο* $\delta \in D \setminus D^*$ *μὲ* $|\delta|^2 = n$ *ἀναλύεται σὲ γινόμενο ἀναγώγων.* Θεωροῦμε ἕνα τέτοιο στοιχεῖο δ. Ἂν τὸ δ εἶναι ἀνάγωγο, τότε δὲν ἔχομε τίποτα ν' ἀποδείξομε. Ἂν τὸ δ δὲν εἶναι ἀνάγωγο, τότε ὑπάρχουν $\alpha, \beta \in D \setminus D^*$, τέτοια ὥστε $\delta = \alpha\beta$, ἄρα $n = |\delta|^2 = |\alpha|^2 |\beta|^2$. Ἀπὸ τὸ (α΄) ξέρομε ὅτι $|\alpha|^2, |\beta|^2 \geq 2$, ἄρα $n = |\alpha|^2 |\beta|^2 \geq 2|\beta|^2$ καί, συνεπῶς, $|\beta|^2 \leq n/2 < n$· ἐντελῶς ἀνάλογα, $|\alpha|^2 < n$. Ἀπὸ τὴν ἐπαγωγικὴ ὑπόθεση ξέρομε ὅτι κάθε στοιχεῖο $\in D \setminus D^*$, τοῦ ὁποίου τὸ τετράγωνο τοῦ μέτρου εἶναι $< n$, ἀναλύεται σὲ ἀνάγωγα. Κατὰ συνέπεια, τὸ α καὶ τὸ β ἀναλύονται σὲ ἀνάγωγα. Ἀλλὰ τότε εἶναι φανερὸ ὅτι καὶ τὸ $\delta = \alpha\beta$ ἀναλύεται σὲ ἀνάγωγα.

□

Ἄσκηση 1.9 *Ἔστω ἡ ἀκέραια περιοχὴ* $D = \mathbb{Z}[\sqrt{-2}] = \{a + bi\sqrt{2} : a, b \in \mathbb{Z}\}$.
(α΄) *Ἀποδεῖξτε ὅτι* $D^* = \{-1, 1\}$.
(β΄) *Ἀποδεῖξτε ὅτι καθένα ἀπὸ τὰ στοιχεῖα* $i\sqrt{2}$ *καὶ* $1 + i\sqrt{2}$ *τῆς* D *εἶναι ἀνάγωγο.*

Ἄσκηση 1.10 *Ἔστω ἡ ἀκέραια περιοχὴ* $\mathbb{Z}[\sqrt{-5}]$ *τοῦ παραδείγματος (ε΄), πιὸ πάνω.*
(α΄) *Ν' ἀποδειχθεῖ ὅτι* $D^* = \{-1, 1\}$.
(β΄) *Σύμφωνα μὲ τὸ παράδειγμα (γ΄) 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 1.3 *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 $\nu = 1, \ldots, n$ ἀντιστοιχεῖ μονοσημάντως ἕνα $i_\nu \in \{1, \ldots, n\}$, 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 $q_1, \ldots, q_m$, 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 $n = k - 1 \geq 1$. Ὑποθέτομε, δηλαδή, τὸ ἑξῆς: Ἂν ἕνα στοιχεῖο $\delta \in D$ εἶναι γινόμενο $k - 1$ τὸ πλῆθος ἀναγώγων στοιχείων καὶ κάνομε στὸ δ μία δεύτερη ἀνάλυση σὲ ἀνάγωγα, τῶν ὁποίων τὸ πλῆθος εἶναι $\geq k - 1$, τότε, ἀναγκαστικά, τὸ πλῆθος τῶν ἀναγώγων τῆς δεύτερης ἀνάλυσης εἶναι ἴσο μὲ $k - 1$ καὶ τὰ ἀνάγωγα τῆς δεύτερης ἀνάλυσης εἶναι συνεταιρικά, ἕνα πρὸς ἕνα, μὲ τὰ ἀνάγωγα τῆς ἀρχικῆς ἀνάλυσης.
Γιὰ ν' ἀποδείξομε ὅτι ὁ ἰσχυρισμὸς ἰσχύει καὶ γιὰ $n = k$, ὑποθέτομε ὅτι $\prod_{i=1}^{k} p_i$ καὶ $\prod_{i=1}^{m} q_i$, ὅπου $m \geq k$, εἶναι δύο ἀναλύσεις σὲ ἀνάγωγα τοῦ ἴδιου στοιχείου $\delta \in D$, ἄρα $\prod_{i=1}^{k} p_i = \prod_{i=1}^{m} q_i$. 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 $m - 1 (\geq k - 1)$ 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.

□

Ἄσκηση 1.11 *Σὲ περιοχὴ μονοσήμαντης ἀνάλυσης, κάθε ἀνάγωγο στοιχεῖο εἶναι πρῶτο.*

2 Μέγιστος Κοινὸς Διαιρέτης

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 2.1, 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 2.1 *(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 2.1 *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 2.2 (Συμπληρώνει τὴν Πρόταση 2.1) *Ἂν ὁ* d *εἶναι* ΜΚΔ *τῶν* $a_1, \ldots, a_n$*, τότε καὶ κάθε συνεταιρικὸ στοιχεῖο τοῦ* d *εἶναι, ἐπίσης,* ΜΚΔ *τῶν* $a_1, \ldots, a_n$*.*

3 Δαιρετότητα σὲ περιοχὲς κυρίων ἰδεωδῶν

Δὲν εἶναι βέβαιο ὅτι σὲ ὁποιαδήποτε ἀκέραια περιοχή, 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 3.1 *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

$$\langle a_1, \ldots, a_n \rangle = dD. \tag{1}$$

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 $d = t_1 a_1 + \cdots + t_n a_n$. 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), 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 $d = t_1 a_1 + \cdots + t_n a_n$ (βλ. ἄσκηση1.2), ἄρα διαιρεῖ καὶ τὸ ἀριστερό μέλος, δηλαδή, τὸ d.

□

Ἄσκηση 3.1 *Ἔστω* D *περιοχὴ κυρίων ἰδεωδῶν καὶ* $a_1, \ldots, a_n, b \in D$, *ὄχι ὅλα μηδέν. Ἀποδεῖξτε ὅτι, ἂν* $d = \text{ΜΚΔ}(a_1, \ldots, a_n)$, *τότε* $bd = \text{ΜΚΔ}(ba_1, \ldots, ba_n)$.

Ἄσκηση 3.2 *Ἔστω* D *περιοχὴ κυρίων ἰδεωδῶν καὶ* $a_1, \ldots, a_n \in D$, *ὄχι ὅλα μηδέν. Ἀποδεῖξτε ὅτι, ἂν* $d = \text{ΜΚΔ}(a_1, \ldots, a_n)$ *καὶ* $\epsilon_1, \ldots, \epsilon_n \in D^*$, *τότε* $d = \text{ΜΚΔ}(\epsilon_1 a_1, \ldots, \epsilon_n a_n)$. *Μ' ἄλλα λόγια, ἂν τὰ* $a_1, \ldots, a_n$ *ἀντικατασταθοῦν ἀπὸ συνεταιρικά τους, τότε τὰ στοιχεῖα ποὺ θὰ προκύψουν, θὰ ἐξακολουθήσουν νὰ ἔχουν τὸ* d *ὡς* ΜΚΔ *τους.*

Θεώρημα 3.2 *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.

(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΄) Ἔστω ὅτι τὰ a, p δὲν εἶναι πρῶτα μεταξύ τους. Τότε ἔχουν κάποιο κοινὸ διαιρέτη, ἔστω d, ὁ ὁποῖος δὲν εἶναι μονάδα (βλ. ἄσκηση 2.1 (α΄)). Ἀφοῦ $d|p$ καὶ τὸ p εἶναι ἀνάγωγο, ἕπεται ὅτι τὸ d εἶναι συνεταιρικὸ τοῦ p. Ἀλλά, ἐπίσης, $d|a$, ἄρα ἕνα στοιχεῖο συνεταιρικὸ τοῦ p διαιρεῖ τὸ a, ὁπότε καὶ τὸ p διαιρεῖ τὸ a (βλ. ἄσκηση 1.4).

(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 3.1, 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 3.1, 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, $c = dac + ebc = da(bc_2) + eb(ac_1) = ab(c_2 d + c_1 e)$, ποὺ δείχνει ὅτι $ab|c$.

(δ΄) Ἂν τὸ ab δὲν εἶναι πρῶτο πρὸς τὸ c, τότε, ἀπὸ τὴν ἄσκηση 2.1, ὑπάρχει κοινὸς διαιρέτης d τῶν ab καὶ c, ποὺ δὲν εἶναι μονάδα. Ἀπ' τὴν ἄλλη, ἀφοῦ $\text{μκδ}(a,c) = 1$, τὸ Θεώρημα 3.1 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 3.3 *Ἂν μιὰ περιοχὴ ἀνάλυσης εἶναι περιοχὴ κυρίων ἰδεωδῶν, τότε εἶναι καὶ περιοχῆς μονοσήμαντης ἀνάλυσης.*

Ἀπόδειξη. Προκύπτει ἀπὸ προφανῆ συνδυασμὸ τῆς Πρότασης 1.3 καὶ τοῦ Θεωρήματος 3.2 (β΄).

□

Μία πρόταση ἐξαιρετικὰ σημαντικὴ γιὰ τὶς ἐφαρμογὲς εἶναι ἡ ἑπόμενη.

Πρόταση 3.4 *Ἔστω D περιοχὴ ἀνάλυσης, ἡ ὁποία εἶναι καὶ περιοχὴ κυρίων ἰδεωδῶν, καὶ $a, b, c \in D$ μὴ μηδενικά, τὰ a, b δὲν εἶναι μονάδες, εἶναι πρῶτα μεταξύ τους καὶ $ab = c^n$, ὅπου ὁ $n \in \mathbb{N}$. Τότε καθένα ἀπὸ τὰ a, b εἶναι συνεταιρικὸ μὲ n-οστὴ δύναμη στοιχείου τῆς D.*

Ἀπόδειξη. Ἡ D εἶναι περιοχὴ μονοσήμαντης ἀνάλυσης λόγῳ τοῦ Θεωρήματος 3.3. Φανταζόμαστε ἀναλύσεις τῶν a, b, c σὲ ἀνάγωγα τῆς D. Λόγῳ τῆς μονοσήμαντης ἀνάλυσης, ἡ σχέση $ab = c^n$ μᾶς ὁδηγεῖ, κατ' ἀρχάς, στὰ ἑξῆς συμπεράσματα: Κάθε ἀνάγωγο, ποὺ ἐμφανίζεται στὴν ἀνάλυση τοῦ a εἴτε τοῦ b, ἔχει ἕνα συνεταιρικό του στὴν ἀνάλυση τοῦ c^n, ἄρα καὶ στὴν ἀνάλυση τοῦ c. Ἄρα, τὰ ἀνάγωγα στὶς ἀναλύσεις τῶν a, b πρέπει νὰ εἶναι συνεταιρικὰ ἀναγώγων, ποὺ ἐμφανίζονται στὴν ἀνάλυση τοῦ c. Ἀλλὰ καὶ ἀντιστρόφως, γιὰ κάθε ἀνάγωγο, ἔστω π, ποὺ ἐμφανίζεται στὴν ἀνάλυση τοῦ c ὑπάρχει ἕνα συνεταιρικό του, ἔστω π', ποὺ ἐμφανίζεται στὴν ἀνάλυση τοῦ ab. Τὸ π' ἐμφανίζεται στὴν ἀνάλυση ἑνός, ἀκριβῶς, ἀπὸ τὰ a, b, διότι τὰ a, b εἶναι πρῶτα μεταξύ τους. Γιὰ τὸν ἴδιο λόγο, ἀφοῦ τὸ π^n ἐμφανίζεται στὴν ἀνάλυση τοῦ c^n, τὸ π'^n ἐμφανίζεται στὴν ἀνάλυση ἑνός, ἀκριβῶς, ἀπὸ τὰ a, b.

Ἔστω, λοιπόν, ὅτι $c = p_1 \cdots p_k q_1 \cdots q_l$ ἡ ἀνάλυση τοῦ c σὲ ἀνάγωγα, ὅπου $p_1, \ldots, p_k$ εἶναι ἐκεῖνα ἀκριβῶς τὰ ἀνάγωγα, τῶν ὁποίων τὰ συνεταιρικὰ ἐμφανίζονται στὴν ἀνάλυση τοῦ a καὶ $q_1, \ldots, q_l$ εἶναι ἐκεῖνα ἀκριβῶς τὰ ἀνάγωγα, τῶν ὁποίων τὰ συνεταιρικὰ ἐμφανίζονται στὴν ἀνάλυση τοῦ b. Ἀπὸ τὴ σχέση $ab = p_1^n \cdots p_k^n q_1^n \cdots q_l^n$ καὶ τὶς παραπάνω παρατηρήσεις, συμπεραίνομε ὅτι $a = (\epsilon_1 p_1^n) \cdots (\epsilon_k p_k^n)$ καὶ $b = (\zeta_1 q_1^n) \cdots (\zeta_l q_l^n)$, ὅπου $\epsilon_1, \ldots, \epsilon_k, \zeta_1, \ldots, \zeta_l \in D^*$. Συνεπῶς, $a = (\text{μονάδα}) \cdot (p_1 \cdots p_k)^n$ καὶ $b = (\text{μονάδα}) \cdot (q_1 \cdots q_l)^n$.

□

Ἄσκηση 3.3 *(α΄) Θεωρῆστε τὸν ὁμομορφισμὸ δακτυλίων: $\mathbb{Z} \ni a \overset{f}{\mapsto} [a] \in \mathbb{Z}_4$. Ποιὲς εἶναι οἱ δυνατὲς τιμὲς τοῦ $f(a^2)$;*
(β΄) Ἔστω ὅτι $x, y, z \in \mathbb{Z}$, οἱ x, y εἶναι πρῶτοι μεταξύ τους καὶ $x^2 + y^2 = z^2$. Ἀποδεῖξτε ὅτι ὁ ἕνας ἐκ τῶν x, y εἶναι ἄρτιος καὶ ὁ ἄλλος περιττός. Συμπεράνατε ὅτι ὁ z εἶναι περιττός.
Ὑπόδειξη: Κατ' ἀρχάς, παρατηρῆστε ὅτι οἱ x, y δὲν μπορεῖ νὰ εἶναι καὶ οἱ δύο ἄρτιοι. Ἂν εἶναι καὶ οἱ δύο περιττοί, τότε νὰ ἐφαρμόσετε τὸν ὁμομορφισμὸ f τοῦ ἐρωτήματος (α΄) στὴ σχέση $x^2 + y^2 = z^2$ καὶ θὰ ὁδηγηθῆτε σὲ ἄτοπο.

(γ΄) Ἔστω ὅτι $x, y, z \in \mathbb{N}$, οἱ x, y εἶναι πρῶτοι μεταξύ τους καὶ $x^2 + y^2 = z^2$. Χρησιμοποιώντας τὸ ἐρώτημα (β΄), μπορεῖτε νὰ ὑποθέσετε ὅτι ὁ x εἶναι περιττὸς καὶ ὁ x εἶναι ἄρτιος. Ἀποδεῖξτε ὅτι, $\text{ΜΚΔ}(z + y, z - y) = 1$. *Χρησιμοποιώντας τὴν Πρόταση 3.4, ἀποδεῖξτε ὅτι ὑπάρχουν ἀκέραιοι m, n, πρῶτοι μεταξύ τους, τέτοιοι ὥστε $z + y = m^2$ καὶ $z - y = n^2$ καὶ ὑπολογῖστε τὰ x, y, z συναρτήσει τῶν m, n.*

4 Εὐκλείδειες περιοχές

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

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

μὲ τὶς ἑξῆς ἰδιότητες:

1. Ἂν τὰ $a, b \in E$ εἶναι μὴ μηδενικὰ καὶ $a|b$, τότε $\delta(a) \leq \delta(b)$.
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 $\delta(r) < \delta(b)$.

Ἡ ἀπεικόνιση δ λέγεται *στάθμη* ἢ (κατὰ τὴν ὁρολογία τοῦ [1, §3.2.5]) *εὐκλείδεια συνάρτηση* τῆς E.

Ἄσκηση 4.1 *Ἀποδεῖξτε ὅτι $\delta(1) \leq \delta(e)$ γιὰ κάθε $e \in E \setminus \{0\}$.*

Πρόταση 4.1 *Ἔστω E εὐκλείδεια περιοχὴ στάθμης δ.*
(α΄) *Ἂν τὰ $a, b \in E$ εἶναι μὴ μηδενικά, $a|b$ καὶ $\delta(a) = \delta(b)$, 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 4. 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 $\delta(r) < \delta(b)$. 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 $\delta(r) \geq \delta(a) = \delta(b)$, ποὺ ἔρχεται σὲ ἀντίφαση μὲ τὴν $\delta(r) < \delta(b)$.

(β΄) Ἔστω $\min \delta(E) = n_0$.

Ἰσχυρισμός: Ἂν γιὰ κάποιο $a \in E$ εἶναι $\delta(a) = n_0$, 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 τὴν πρώτη ἰδιότητα τῆς στάθμης ἔχομε ὅτι $\delta(b) \leq \delta(a) = n_0$, ἄρα, ἀπ' τὴν ἐπιλογὴ τοῦ n_0, πρέπει νὰ εἶναι $\delta(b) = n_0$. Ἔτσι τώρα, $\delta(b) = \delta(a)$ 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 $\delta(a) = n$. 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,

$\delta(b) \leq \delta(a)$ καὶ $\delta(c) \leq \delta(a)$. Ἂν ἦταν $\delta(b) = \delta(a)$, τότε, ἀπὸ τὸ *(α΄)* θὰ συμπεραίναμε ὅτι τὰ a, b εἶναι συνεταιρικά· ἀντίφαση. Ἄρα $\delta(b) < \delta(a) < n$ καὶ ὁμοίως, $\delta(c) < \delta(a) < n$. 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,

$$b \neq 0 \quad \& \quad \delta(b) \leq \delta(a) \quad \forall\, a \in I \setminus \{0\}. \tag{2}$$

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 $\delta(r) \leq \delta(b)$. 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 $< \delta(b)$, κάτι ποὺ ἀντιβαίνει στὴν (2). Ἄρα $r = 0$ καί, συνεπῶς, $a = bq$.

□

Ἄσκηση 4.2 *Γιὰ κάθε $e \in E^*$ ἰσχύει $\delta(e) = \delta(1)$. Ἰσχύει καὶ τὸ ἀντίστροφο: Ἂν $e \in E \setminus \{0\}$ καὶ $\delta(e) = \delta(1)$, τότε $e \in E^*$.*
Ὑπόδειξη. Γιὰ τὸ ἀντίστροφο χρησιμοποιεῖστε τὴν Πρόταση 4.1 (α΄).

Ἄσκηση 4.3 *Ἔστω E εὐκλείδεια περιοχή, τῆς ὁποίας ἡ στάθμη δ ἔχει τὴν ἐπιπλέον ἰδιότητα $\delta(ab) = \delta(a)\delta(b)$.*[3] *Ἀποδεῖξτε ὅτι, στὴν περίπτωση αὐτή, ἰσχύουν τὰ ἑξῆς:*
(α΄) $\delta(1) = 1$.
(β΄) *Ἂν γιά κάποιο $e \in E$ ἰσχύει $\delta(e) = p$, πρῶτος (τοῦ $\mathbb{Z}$), τότε τὸ e εἶναι ἀνάγωγο στοιχεῖο τῆς E, ἄρα καὶ πρῶτο στοιχεῖο τῆς E, λογῳ τῆς Προτάσεως 4.1 καὶ τοῦ Θεωρήματος 3.2 (β΄)*

Πόρισμα 4.2 *Κάθε εὐκλείδεια περιοχὴ εἶναι περιοχὴ μονοσήμαντης ἀνάλυσης.*

Ἀπόδειξη. Προφανὴς συνδυασμὸς τῶν (β΄) καὶ (γ΄) τῆς Προτάσεως 4.1 καὶ τοῦ Θεωρήματος 3.3.

□

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 τὸ 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

$$\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\},$$

ἡ ὁποία ὀνομάζεται, συνήθως, περιοχὴ τῶν *ἀκεραίων τοῦ Gauss*.
Ἡ ἀπεικόνιση $\delta : \mathbb{Z}[i] \setminus \{0\} \to \mathbb{N}$, ποὺ ὁρίζεται

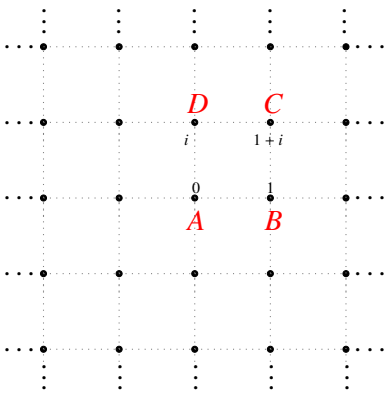
$$\delta(a + bi) = |a + bi|^2 = a^2 + b^2,$$

[3] Προσοχή! Ἡ ἰδιότητα αὐτὴ δὲν ἰσχύει γιὰ ὅλες τὶς στάθμες εὐκλειδείων περιοχῶν.

εἶναι στάθμη, ὅπως θ' ἀποδείξομε ἀμέσως παρακάτω, καί, συνεπῶς, ἀπὸ τὸ Πόρισμα 4.2, ἡ $\mathbb{Z}[i]$ εἶναι περιοχὴ μονοσήμαντης ἀνάλυσης.

Ἀπόδειξη τοῦ ἰσχυρισμοῦ: Ἡ ἰδιότητα (1) τῆς στάθμης εἶναι ἁπλὸ ν' ἀποδειχθεῖ ὅτι ἱκανοποιεῖται ἀπὸ τὴ συγκεκριμένη ἀπεικόνιση δ· ἡ ἀπόδειξη στηρίζεται στὶς βασικὲς ἰδιότητες τῆς μιγαδικῆς ἀπόλυτης τιμῆς.

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

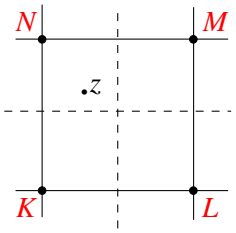


Ἀπεικόνιση τῆς $\mathbb{Z}[i]$ στὸ μιγαδικὸ ἐπίπεδο

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 δ, ποὺ ὁρίσαμε πιὸ πάνω, ἱκανοποιεῖ τὴ συνθήκη (2) τοῦ ὁρισμοῦ τῆς στάθμης.

Ἔστω ὅτι $a + bi, c + di \in \mathbb{Z}[i]$ μὲ τὸ δεύτερο μὴ μηδενικό. Θεωροῦμε τὸν μιγαδικὸ $z = (a + bi)/(c + di)$, 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 z ἀνήκει σ' ἕνα ἀπὸ αὐτά, π.χ. στὸ ἄνω ἀριστερό (βλ. σχῆμα). Ἡ ἀπόσταση τοῦ z 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 $|1 - i| = \sqrt{2}$. Ἄρα, ἡ ἀπόσταση τοῦ σημείου

z ἀπὸ τὸ N εἶναι, τὸ πολύ, $\sqrt{2}/2$. Ἀλλὰ τὸ σημεῖο N ἀναπαριστᾶ ἕνα στοιχεῖο τῆς ἀκέραιας περιοχῆς, ἔστω τὸ $u + vi$, μὲ $u, v \in \mathbb{Z}$. Συνεπῶς $|u + vi - z| \leq \sqrt{2}/2$, ὁπότε

$$\left| \frac{a + bi}{c + di} - (u + vi) \right|^2 \leq \frac{1}{2}.$$

Ἀπαλείφοντας τὸν παρονομαστὴ παίρνομε τὴ σχέση

$$|\, a + bi - (c + di)(u + vi)\,|^2 \leq \tfrac{1}{2}|\, c + di\,|^2 < |\, c + di\,|^2 = \delta(c + di). \tag{3}$$

Προφανῶς, $a + bi - (c + di)(u + vi) = r + si$ μὲ τὰ $r, s \in \mathbb{Z}$.
Ἂν $r + si = 0$, τότε $a + bi = (c + di)(u + vi)$.
Ἂν $r + si \neq 0$, τότε, ἀπὸ τὴ σχέση (3), βλέπομε ὅτι

$$a + bi = (c + di)(u + vi) + (r + si), \quad \delta(r + si) < \delta(c + di)$$

καὶ αὐτὸ ὁλοκληρώνει τὴν ἀπόδειξη τοῦ ἰσχυρισμοῦ μας.

Ἄσκηση 4.4 *Ἔστω ἡ περιοχὴ $D = \mathbb{Z}[i]$ τῶν ἀκεραίων τοῦ Gauss.*
(α΄) Ἂν οἱ $a, b \in \mathbb{Z}$ εἶναι πρῶτοι μεταξύ τους, δεῖξτε ὅτι οἱ ἀριθμοὶ αὐτοί, θεωρούμενοι ὡς στοιχεῖα τῆς D παραμένουν πρῶτοι μεταξύ τους. Ἐπιπλέον, γιὰ κάθε $d \in D$, ἀποδεῖξτε ὅτι $d = \text{ΜΚΔ}(da, db)$.
Ὑπόδειξη γιὰ τὸν δεύτερο ἰσχυρισμό: Χρησιμοποιεῖστε τὴν ἄσκηση 3.1.
(β΄) Ἀποδεῖξτε ὅτι $D^* = \{\pm 1, \pm i\}$. Ἀποδεῖξτε, ἐπίσης, ὅτι κάθε μονάδα ἰσοῦται μὲ κύβο μονάδας.
(γ΄) Ἀποδεῖξτε ὅτι τὸ $1 + i$ εἶναι ἀνάγωγο στοιχεῖο τῆς D (ἄρα καὶ πρῶτο) καὶ ἡ ἀνάλυση τοῦ $2 \in D$ σὲ ἀνάγωγα (πρῶτα) στοιχεῖα εἶναι $2 = -i(1 + i)^2$.

> Σὲ ὅλα τὰ παρακάτω ἐρωτήματα θεωροῦμε ὅτι $x, y, z \in \mathbb{Z}$, οἱ x, y εἶναι μὴ μηδενικοί, πρῶτοι μεταξύ τους καὶ $x^2 + y^2 = z^3$.

(δ΄) Ἀποδεῖξτε ὅτι, ἀπὸ τοὺς x, y, ὁ ἕνας εἶναι ἄρτιος καὶ ὁ ἄλλος περιττός.
Ὑπόδειξη. Νὰ ἐργαστεῖτε ἀκριβῶς ὅπως στὴν ἄσκηση 3.3.
Μετά, ἀποδεῖξτε ὅτι $1 + i \nmid x \pm iy$.
Ὑπόδειξη. Ἔστω, γιὰ παράδειγμα, ὅτι $1 + i \,|\, x + iy$. Γράψτε $x + iy = (1 + i)(a + bi)$, ὅπου $a, b \in \mathbb{Z}$. Θεωρῆστε καὶ τὴ συζυγῆ σχέση καὶ πολλαπλασιάστε κατὰ μέλη τὶς δύο σχέσεις.
(ε΄) Ἀποδεῖξτε ὅτι οἱ $x + iy, x - iy$ εἶναι πρῶτοι μεταξύ τους.
Ὑπόδειξη. Ὑποθέστε ὅτι ὁ d εἶναι κοινὸς διαιρέτης τῶν $x + iy, x - iy$ καὶ ἀποδεῖξτε ὅτι, ὑποχρεωτικά, $d \in D^*$. Αὐτὸ θὰ τὸ πετύχετε ἀποδεικνύοντας πρῶτα ὅτι τὸ d εἶναι κοινὸς διαιρέτης τῶν $2x, 2y$, ἄρα $d | \text{ΜΚΔ}(2x, 2y)$. Μὲ χρήση τοῦ ἐρωτήματος (α΄), ἀποδεῖξτε ὅτι $d|2$. Συνεπῶς, ἂν $d \notin D^*$, τότε τὸ d ἔχει κάποιον πρῶτο διαιρέτη. Χρησιμοποιώντας τὸ ἐρώτημα (γ΄), δεῖξτε ὅτι αὐτὸς ὁ ὑποθετικὸς πρῶτος διαιρέτης τοῦ d εἶναι, ἀναγκαστικά, ὁ $1 + i$. Ἀλλὰ αὐτὸ εἶναι ἄτοπο, βάσει τοῦ ἐρωτήματος (δ΄).
(ζ΄) Γράψτε τώρα τὴ σχέση $x^2 + y^2 = z^3$, ὡς $(x + iy)(x - iy) = z^3$. Μὲ τὴ βοήθεια τοῦ ἐρωτήματος (ε΄) καὶ τῆς Πρότασης 3.4, ἀποδεῖξτε ὅτι ὑπάρχουν $\epsilon \in D^*$ καὶ $m, n \in \mathbb{Z}$, τέτοια ὥστε $x + iy = (\text{μονάδα}) \cdot (m + ni)^3$. Ἐκμεταλλευόμενοι τὸ ἐρώτημα b, δεῖξτε ὅτι ὑπάρχουν $a, b \in \mathbb{Z}$, τέτοια ὥστε $x + iy = (a + bi)^3$. Συμπεράνατε ὅτι

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

Ἐπιπλέον, δεῖξτε ὅτι, στοὺς παραπάνω τύπους, οἱ ἀκέραιοι a, b εἶναι πρῶτοι μεταξύ τους. Ἂν ὁ x εἶναι ἄρτιος καὶ ὁ y περιττός, τότε ὁ a εἶναι ἄρτιος καὶ ὁ b περιττός, ἐνῶ τὸ ἀντίστροφο συμβαίνει ἂν ὁ x εἶναι περιττὸς καὶ ὁ y ἄρτιος.

Ἄσκηση 4.5 *Ἔστω ἡ ἀκέραια περιοχὴ* $\mathbb{Z}[\sqrt{-2}] = \{a + bi\sqrt{2} : a, b \in \mathbb{Z}\}$. *Ἀποδεῖξτε ὅτι ἡ ἀπεικόνιση* $\delta : \mathbb{Z}[\sqrt{-2}] \setminus \{0\} \to \mathbb{N}_0$, *ποὺ ὁρίζεται*

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

εἶναι στάθμη.

Ὑπόδειξη. Μιμηθῆτε τὴν ἀπόδειξη τοῦ παραπάνω παραδείγματος 3. Αὐτὴ τὴ φορά, τὸ πλέγμα ποὺ θὰ θεωρήσετε, παράγεται ἀπὸ τὴν ἐπανάληψη τοῦ ABCD, ὅπου τώρα οἱ κορυφές του ἔχουν συντεταγμένες $0,\ 1,\ 1 + i\sqrt{2},\ i\sqrt{2}$.

5 Πολυώνυμα πάνω ἀπὸ περιοχὲς μονοσήμαντης ἀνάλυσης

Ὅπως ἐπισημάναμε στὴν «Σημαντικὴ παρατήρηση» τῆς σελίδας 4, 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 5, πάντα τὸ D συμβολίζει περιοχὴ μονοσήμαντης ἀνάλυσης. Π.χ. ἡ D θὰ μποροῦσε νὰ εἶναι περιοχὴ κυρίων ἰδεωδῶν, ἡ ὁποία εἶναι συγχρόνως καὶ περιοχὴ ἀνάλυσης (βλ. Θεώρημα 3.3). Θὰ πάρομε δεδομένο ὅτι, σὲ μία περιοχὴ μονοσήμαντης ἀνάλυσης, μία ὁποιαδήποτε n-άδα στοιχείων, ποὺ δὲν εἶναι ὅλα μηδενικά, ἔχει ΜΚΔ.[4] Ὑπενθυμίζεται ὅτι αὐτὸ ἰσχύει, ὁπωσδήποτε, ὅταν εἴμαστε σὲ περιοχὴ κυρίων ἰδεωδῶν (βλ. Θεώρημα 3.1).
>
> Μὲ K συμβολίζομε τὸ *σῶμα πηλίκων* τῆς D. Δεῖτε [1, §2.2] ἢ, πιὸ ἀναλυτικά, [2, §4.4].

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

Ἄσκηση 5.1 *Ἀποδεῖξτε ὅτι* $(D[X])^* = D^*$. *Συμπεράνατε ὅτι τὰ στοιχεῖα τῆς* $D[X]$, *ποὺ δὲν εἶναι μονάδες, εἶναι τὰ μὴ σταθερὰ πολυώνυμα τῆς* $D[X]$ *καὶ τὰ στοιχεῖα τοῦ* $D \setminus D^*$.

Ἄσκηση 5.2 *Ἔστω* $c \in D$. *Ἀποδεῖξτε ὅτι τὸ* c, *θεωρούμενο ὡς στοιχεῖο τῆς* $D[X]$, *εἶναι ἀνάγωγο ἄν, καὶ μόνο ἄν, τὸ* c *εἶναι ἀνάγωγο στοιχεῖο τῆς* D.

Ἄσκηση 5.3 *(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* $d \in D$ *(μὴ μηδενικό), τότε τὸ* d *εἶναι περιεχόμενο τοῦ* $d \cdot f(X)$.

[4] Εἶναι λίγο τεχνικὴ ἡ ἀπόδειξή του, ἀλλὰ ὄχι πραγματικὰ δύσκολη.

Λήμμα 5.1 *Κάθε μὴ μηδενικὸ $f(X) \in K[X]$ γράφεται ὡς γινόμενο $f(X) = \alpha \cdot g(X)$, ὅπου $\alpha \in K$ καὶ $g(X)$ εἶναι πρωταρχικὸ πολυώνυμο τῆς $D[X]$. Ἂν $f(X) = \beta \cdot h(X)$, ὅπου $\beta \in K$ 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. 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 5.3 (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 5.3 (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 5.3 (α′)). Ἔστω $d_2 = \epsilon d_1$, $\epsilon \in D^*$. Τότε, $e\beta = d_2 = \epsilon d_1 = \epsilon e\alpha$, ἄρα $\beta = \epsilon\alpha$.

□

Ἄσκηση 5.4 *Ἔστω ὅτι τὰ $f(X), g(X) \in D[X]$ εἶναι πρωταρχικά, $k \in K$ καὶ $g(X) = k \cdot f(X)$. Ἀποδεῖξτε ὅτι, τότε, $k \in D^*$.*

Θεώρημα 5.2 *Τὸ γινόμενο πρωταρχικῶν πολυωνύμων εἶναι πρωταρχικὸ πολυώνυμο.*

Ἀπόδειξη. Ἔστω

$$(a_m X^m + \cdots + a_1 X + a_0) \cdot (b_n X^n + \cdots + b_1 X + b_0) = c_\ell X^\ell + \cdots c_1 X + c_0, \quad \ell = m + n, \quad (4)$$

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 (4), ἄρα καὶ ὅλους τοὺς συντελεστὲς τοῦ πολυωνύμου, ποὺ θὰ προκύψει ἂν κάνομε τὸν πολλαπλασιασμὸ στὸ δεξιὸ μέλος τῆς (4). 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 (4) παίρνομε τὴ σχέση

$$c_{\mu+\nu} = \sum_{i+j=\mu+\nu} a_i b_j, \quad (5)$$

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 $p | a_i b_j$. Ἂν, $i > \mu$, τότε $j < \nu$ (διότι $i + j = \mu + \nu$), ὁπότε $p | b_j$, ἄρα $p | a_i b_j$. Ἂν, τέλος, $i = \mu$, ὁπότε $j = \nu$, τότε $p \nmid a_i$ καὶ $p \nmid b_j$, ἄρα $p \nmid a_i b_j$. Ἔτσι, στὸ ἄθροισμα τοῦ δεξιοῦ μέλους τῆς (5), 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 5.3 [5] *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 $K[X]$,[6] εἶναι ἀνάγωγο πάνω ἀπ' τὸ σῶμα K.*

Ἀπόδειξη. ($\Leftarrow$) 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 5.1. Ἔστω τώρα ὅτι τὸ $f(X)$ εἶναι μὴ σταθερὸ πρωταρχικὸ πολυώνυμο τοῦ $D[X]$, ἀνάγωγο στὸ $K[X]$. Ἂν δὲν εἶναι ἀνάγωγο στοιχεῖο τῆς $D[X]$, τότε γράφεται ὡς γινόμενο δύο στοιχείων τῆς $D[X]$, κανένα ἐκ τῶν ὁποίων δὲν εἶναι μονάδα τῆς $D[X]$. Αὐτὸ σημαίνει (βλ. ἄσκηση 5.1) ὅτι, ἢ τὸ $f(X)$ εἶναι γινόμενο δύο μὴ σταθερῶν πολυωνύμων τοῦ $D[X]$, ἢ $f(X) = c \cdot g(X)$ μὲ $g(X) \in D[X]$ καὶ $c \in D$ ὄχι μονάδα. Τὸ πρῶτο ἐνδεχόμενο προφανῶς ἀντίκειται στὴν ὑπόθεση ὅτι τὸ $f(X)$ εἶναι ἀνάγωγο πολυώνυμο τοῦ $K[X]$. Ἀποκλείεται, ἐπίσης, καὶ τὸ δεύτερο ἐνδεχόμενο, διότι αὐτὸ συνεπάγεται ὅτι ὅλοι οἱ συντελεστὲς τοῦ $f(X)$ εἶναι πολλαπλάσια τοῦ $c \in D^*$, ἄρα δὲν εἶναι πρῶτοι μεταξύ τους, συμπέρασμα ποὺ ἀντιβαίνει στὴν ὑπόθεση πρωταρχικότητας τοῦ $f(X)$. Συνεπῶς, τὸ $f(X)$ εἶναι ἀνάγωγο στοιχεῖο τῆς περιοχῆς $D[X]$.

($\Rightarrow$) Τώρα ὑποθέτομε ὅτι τὸ $f(X)$ εἶναι ἀνάγωγο στοιχεῖο τῆς $D[X]$. Εἰδικώτερα, αὐτὸ συνεπάγεται ὅτι τὸ $f(X)$ δὲν εἶναι μονάδα τῆς $D[X]$, ἄρα ἢ $f(X) = c \in D \setminus D^*$, ἢ $f(X)$ εἶναι μὴ σταθερό (βλ. ἄσκηση 5.1). Στὴν πρώτη περίπτωση, τὸ c εἶναι ἀνάγωγο στοιχεῖο τῆς D (ἄσκηση 5.2).

Μένει ἡ περίπτωση κατὰ τὴν ὁποία τὸ $f(X)$ εἶναι μὴ σταθερό. Κατ' ἀρχάς θὰ ἀποδείξομε ὅτι τὸ $f(X)$ εἶναι πρωταρχικό. Ἔστω $f(X) = a_n X^n + \cdots + a_1 X + a_0$, ὅπου $n \geq 1$, $a_0, a_1, \ldots, a_n \in D$ καὶ $a_n \neq 0$. Ἂν τὸ $f(X)$ δὲν εἶναι πρωταρχικό, τότε οἱ συντελεστὲς a_i δὲν εἶναι πρῶτοι μεταξύ τους, ἄρα ἔχουν ΜΚΔ, ποὺ δὲν εἶναι μονάδα. Ἔστω $d = \text{ΜΚΔ}(a_0, \ldots, a_n)$ καὶ $a_i = db_i$, $b_i \in D$ $(i = 0, \ldots, n)$. Τότε $f(X) = d \cdot (b_n X^n + \cdots + b_1 X + b_0)$, ἄρα ἔχομε ἀνάλυση τοῦ $f(X)$ σὲ γινόμενο δύο στοιχείων τῆς $D[X]$, ποὺ δὲν εἶναι μονάδες. Αὐτὸ ἀντιβαίνει στὴν ὑπόθεση ὅτι τὸ $f(X)$ εἶναι ἀνάγωγο στοιχεῖο τῆς $D[X]$.

Τώρα ξέρομε ὅτι τὸ $f(X)$ εἶναι πρωταρχικὸ καὶ μένει νὰ δείξομε ὅτι τὸ $f(X)$, ποὺ εἶναι ἀνάγωγο ὡς στοιχεῖο τῆς $D[X]$, εἶναι ἀνάγωγο καὶ ὡς στοιχεῖο τῆς $K[X]$. Ἂν αὐτὸ δὲν ἰσχύει, τότε $f(X) = g_1(X)g_2(X)$ μὲ $g_1(X), g_2(X) \in K[X]$, μὴ σταθερά. Γιὰ $i = 1, 2$, μποροῦμε νὰ γράψομε $g_i(X) = \alpha_i h_i(X)$, μὲ $\alpha_i \in K$ καὶ $h_i(X) \in D[X]$ μὴ σταθερὸ καὶ πρωταρχικό, βάσει τοῦ Λήμματος 5.1. Ἂς θέσομε $\alpha_1\alpha_2 = \alpha \in K$ καὶ $h_1(X)h_2(X) = h(X) \in D[X]$. Τὸ $h(X)$ εἶναι πρωταρχικὸ βάσει τοῦ Λήμματος 5.2. Ἄρα $f(X) = \alpha \cdot h(X)$, μὲ τὰ $f(X), h(X) \in D[X]$ πρωταρχικά. Συνεπῶς, ἀπὸ τὴν ἄσκηση 5.4 συμπεραίνομε ὅτι $\alpha = \epsilon \in D^*$, ὁπότε $f(X) = \epsilon h(X)$, ποὺ σημαίνει ὅτι τὰ $f(X), h(X)$ εἶναι συνεταιρικὰ στοιχεῖα τῆς $D[X]$. Ὅμως τὸ $h(X)$ δὲν εἶναι ἀνάγωγο στοιχεῖο τῆς $D[X]$, ἀφοῦ $h(X) = h_1(X)h_2(X)$, ἄρα οὔτε τὸ $f(X)$ εἶναι ἀνάγωγο στοιχεῖο τῆς $D[X]$ (βλ. ἄσκηση 1.3). Ὁδηγηθήκαμε, λοιπόν, σὲ ἀντίφαση, ὑποθέτοντας ὅτι τὸ $f(X)$ εἶναι μὴ ἀνάγωγο στοιχεῖο τῆς $K[X]$.

□

Πόρισμα 5.4 *Ἔστω μὴ σταθερὸ $f(X) \in D[X]$ καὶ τὸ $d \in D$ εἶναι περιεχόμενο τοῦ $f(X)$. Θέτομε $f(X) = d \cdot g(X)$. Τότε, τὸ $f(X)$, θεωρούμενο ὡς πολυώνυμο τοῦ $K[X]$, εἶναι ἀνάγωγο, ἂν καὶ μόνο ἄν, τὸ $g(X)$ εἶναι ἀνάγωγο στοιχεῖο τῆς $D[X]$.*

Ἀπόδειξη. Ἀπὸ τὴν ἄσκηση 5.3 (β΄) συμπεραίνομε ὅτι τὸ $g(X) \in D[X]$ εἶναι πρωταρχικὸ πολυώνυμο τῆς $D[X]$. Ἂν τὸ $g(X)$ εἶναι ἀνάγωγο τῆς $D[X]$, τότε, βάσει τοῦ Θεωρήματος

[5] Στὴ βιβλιογραφία, κάποιες φορές, αὐτὸ τὸ θεώρημα ἀναφέρεται ὡς Λῆμμα τοῦ Gauss.

[6] Ὑπενθυμίζομε ὅτι K συμβολίζει τὸ σῶμα πηλίκων τῆς D.

5.3, τὸ $g(X)$, εἶναι ἀνάγωγο τῆς ἀκέραιας περιοχῆς $K[X]$. Ἐπειδὴ τὸ d εἶναι μονάδα τῆς ἀκέραιας περιοχῆς[7], τὸ $f(X) = d \cdot g(X)$ εἶναι συνεταιρικὸ τοῦ $g(X)$ στὴν $K[X]$, ἄρα καὶ τὸ $f(X)$ εἶναι ἀνάγωγο τῆς $K[X]$.
Ἀντιστρόφως. Ἔστω ὅτι τὸ $g(X)$, θεωρούμενο ὡς στοιχεῖο τῆς ἀκέραιας περιοχῆς $K[X]$, εἶναι ἀνάγωγο. Τότε τὸ $g(X)$ εἶναι ἀνάγωγο στοιχεῖο τῆς $D[X]$. Διότι, ἂν δὲν εἶναι, θὰ ἀναλύεται σὲ γινόμενο δύο στοιχείων τῆς $D[X]$, ἔστω $g(X) = h_1(X)h_2(X)$, κανένα ἐκ τῶν ὁποίων δὲν εἶναι μονάδα. Ἐπειδὴ τὸ $g(X)$ εἶναι πρωταρχικό, κανένα ἀπὸ τὰ $h_i(X)$ δὲν μπορεῖ νὰ ἀνήκει στὸ $D \setminus D^*$, ἄρα τὸ $g(X)$ εἶναι ἀναλυμένα σε δύο μὴ σταθερὰ πολυώνυμα $\in D[X]$. Ἀλλὰ τότε εἶναι ἀναλυμένο καὶ σὲ δύο μὴ σταθερὰ πολυώνυμα τοῦ $K[X]$. Αὐτὸ σημαίνει ὅτι τὸ $g(X)$, ὡς πολυώνυμο τοῦ $K[X]$ δὲν εἶναι ἀνάγωγο, ὁπότε, οὔτε τὸ συνεταιρικό του $f(X)$ εἶναι ἀνάγωγο, συμπέρασμα ποὺ ἀντιφάσκει μὲ τὴν ὑπόθεση.

□

Τελειώνομε αὐτὴ τὴν ἑνότητα μὲ τὸ παρακάτω πολὺ σημαντικὸ θεώρημα.

Θεώρημα 5.5 *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.

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 5.3 (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 5.1) 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 5.2. Ἀλλὰ καὶ τὸ $g(X) \in D[X]$ εἶναι πρωταρχικό, καὶ $1 \cdot g(X) = k \cdot h(X)$, ἄρα, ἀπὸ τὴ ἄσκηση 5.4 ἕπεται ὅτι $k = \epsilon \in D^*$. Τελικά,

$$f(X) = c \cdot g(X) = \epsilon c \cdot h_1(X) \cdots h_m(X). \tag{6}$$

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 5.3, ὅτι αὐτὰ εἶναι ἀνάγωγα στοιχεῖα τῆς ἀκέραιας περιοχῆς $D[X]$. Ἀναλύοντας τώρα καὶ τὸ c σὲ ἀνάγωγα στοιχεῖα τῆς D, παίρνομε ἀπὸ τὴν (6) 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 5.3, ὅτι αὐτὰ τὰ πολυώνυμα εἶναι πρωταρχικὰ καὶ ἀνάγωγα στὸ $K[X]$, ὁπότε καὶ τὰ γινόμενα $h_1(X) \cdots h_m(X)$ καὶ $h'_1(X) \cdots h'_\mu(X)$

[7] Ὅλα τὰ μὴ μηδενικὰ σταθερὰ εἶναι ἀντιστρέψιμα τοῦ K!

εἶναι πρωταρχικά. Ἀλλὰ τότε, τὸ Λῆμμα 5.1 μᾶς λέει ὅτι $q'_1 \cdots q'_\nu = \epsilon q_1 \cdots q_n$, γιὰ κάποιο $\epsilon \in D^*$, καὶ

$$h_1(X) \cdots h_m(X) = \epsilon \cdot h'_1(X) \cdots h'_\mu(X) \tag{7}$$

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 (7) 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 τὴν ἄσκηση 5.4, συμπεραίνομε ὅτι $k_i \in D^*$. 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 5.5 *Ἔστω ἡ ἀκέραια περιοχὴ $D = \mathbb{Z}[i\sqrt{2}] = \{a + bi\sqrt{2} : a, b \in \mathbb{Z}\}$.*
(α΄) Ἀποδεῖξτε ὅτι τὸ $K = \{r + si\sqrt{2} : r, s \in \mathbb{Q}\}$ εἶναι σῶμα πηλίκων τῆς D.
(β΄) Θεωρῆστε δεδομένο ὅτι ἡ D εἶναι περιοχὴ μονοσήμαντης ἀνάλυσης. (Πρβλ. ἄσκηση 4.5.)
(γ΄) Ἀποδεῖξτε ὅτι $D^* = \{-1, 1\}$ καὶ ὅτι τὰ $i\sqrt{2}$ καὶ $1 \pm i\sqrt{2}$ εἶναι ἀνάγωγα στοιχεῖα τῆς D.
(δ΄) Ἔστω τὸ $f(X) = 6(X^2 + 2)(X^2 + 3) \in \mathbb{Z}[X]$. Ἀναλῦστε τὸ $f(X)$ σὲ γινόμενο τῆς μορφῆς

$$f(X) = \{\text{μονάδα τῆς } R[X]\} \times \{\text{γινόμενο ἀναγώγων τῆς } R[X]\},$$

σὲ κάθε μία ἀπὸ τὶς περιπτώσεις $R = \mathbb{Q}$, $R = \mathbb{Z}$, $R = D$ καὶ $R = \mathbb{C}$.
Ὑπόδειξη. Παρατηρῆστε ὅτι $3 = (1 + i\sqrt{2})(1 - i\sqrt{2})$.

Ἄσκηση 5.6 *(α΄) (Τὸ ἐρώτημα αὐτὸ θὰ χρειαστεῖ στὴν ἀπόδειξη τοῦ (β΄).) Ἔστω ὅτι $F(X), G(X) \in \mathbb{R}[X]$ καὶ $F(X)^2 + G(X)^2 = 0 \in \mathbb{R}[X]$. Ἀποδεῖξτε ὅτι $F(X) = G(X) = 0$.*
Προσοχή! Ἡ σχέση $F(X)^2 + G(X)^2 = 0$ δὲν εἶναι ἐξίσωση, ἀλλὰ ἰσότητα πολυωνύμων. Ἄρα, μὴν ἐπικαλεστεῖτε τὸ ἐπιχείρημα ὅτι (τάχα) ἐδῶ ἔχομε ἄθροισμα τετραγώνων πραγματικῶν ἀριθμῶν! Παρατηρῆστε ὅτι $G(X) = -F(X)^2$, ἄρα, ἂν τὸ ἕνα πολυώνυμο εἶναι μὴ μηδενικό, τότε εἶναι καὶ τὸ ἄλλο μὴ μηδενικό. Στην περίπτωση αὐτή, συγκρίνετε τοὺς μεγιστοβάθμιους ὅρους τῶν πολυωνύμων $F(X)^2$ καὶ $G(X)^2$.
(β΄) Ἀποδεῖξτε ὅτι τὸ $f(X, Y) = Y^2 + X^2(X - 1)^2 \in \mathbb{R}[X, Y]$ εἶναι ἀνάγωγο στοιχεῖο τῆς ἀκέραιας περιοχῆς $\mathbb{R}[X, Y]$.
Ὑπόδειξη: (1) Δεῖτε τὸ $f(X, Y)$ ὡς πολυώνυμο $g(Y)$ τῆς μεταβλητῆς Y, μὲ συντελεστὲς ἀπὸ τὴν ἀκέραια περιοχὴ $D = \mathbb{R}[X]$ καὶ ἀποδεῖξτε (εἶναι ἁπλούστατο) ὅτι τὸ $g(Y)$ δὲν ἀνήκει στὴ D καὶ εἶναι πρωταρχικὸ πολυώνυμο τῆς $D[Y]$.

(2) Παρατηρῆστε ὅτι τὸ σῶμα πηλίκων τῆς D εἶναι τὸ $K = \{h_1(X)/h_2(X) : h_i(X) \in \mathbb{R}[X],\ h_2(X) \neq 0\}$ καὶ ἀποδεῖξτε ὅτι τὸ $g(Y)$ δὲν ἔχει ρίζες στὸ K. Ἐδῶ θὰ κάνετε, κάποια στιγμή, χρήση τοῦ ἐρωτήματος (α΄). Τέλος, ἐφαρμόστε τὸ Θεώρημα 5.3 μὲ τὴν $\mathbb{R}[X]$ στὴ θέση τῆς D, τὴ μεταβλητὴ Y στὴ θέση τῆς X καὶ τὸ $g(Y)$ στὴ θέση τοῦ $f(X)$.

Ἄσκηση 5.7 *(α΄) (Αὐτὸ τὸ ἐρώτημα θὰ χρειαστεῖ στὴν ἀπόδειξη τοῦ ἐρωτήματος (β΄).) Ἔστω D περιοχὴ μονοσήμαντης ἀνάλυσης καὶ $p_1, \dots, p_n \in D$ ($n \geq 1$) ἀνάγωγα. Στὴν περίπτωση ποὺ $n \geq 2$, ἔστω ὅτι τὸ p_1 δὲν εἶναι συνεταιρικὸ μὲ κανένα ἀπὸ τὰ $p_2, \dots, p_n$. Ἔστω, ἀκόμη, ἀκέραιος $k \geq 2$ Ἀποδεῖξτε ὅτι εἶναι ἀδύνατον νὰ ὑπάρχουν $a, b \in D$, τέτοια ὥστε $a^k = p_1 \cdots p_n b^k$.*

Ὑπόδειξη. Ἀφοῦ ἡ D εἶναι περιοχὴ μονοσήμαντης ἀνάλυσης, κάθε ἀνάγωγο εἶναι πρῶτο. Ποιὰ εἶναι ἡ μεγαλύτερη δύναμη τοῦ p_1, ποὺ διαιρεῖ τὸ $p_1 \cdots p_n$; Στὴν ἀπάντησή σας παίζει σημαντικὸ ρόλο τὸ ὅτι τὰ p_i εἶναι ἀνὰ δύο μὴ συνεταιρικά. Ἀποδεῖξτε ὅτι $p_1 | a$ καὶ ἔστω p_1^μ ἡ μεγαλύτερη δύναμη τοῦ p_1, ποὺ διαιρεῖ τὸ a. Ἔστω, ἀκόμη, p_1^ν εἶναι ἡ μεγαλύτερη δύναμη τοῦ p_1, ποὺ διαιρεῖ τὸ b (ἂν $p_1 b \nmid$, τότε $\nu = 0$). Ποιὰ εἶναι ἡ μεγαλύτερη δύναμη τοῦ p_1, ποὺ διαιρεῖ τὸ ἀριστερὸ μέλος τῆς σχέσης $a^k = p_1 \cdots p_n b^k$ καὶ ποιὰ ἡ μεγαλύτερη δύναμη, ποὺ διαιρεῖ τὸ δεξιό; Συγκρίνετε.

(β΄) Ἀποδεῖξτε ὅτι κάθε ἕνα ἀπὸ τὰ παρακάτω στοιχεῖα τῆς $\mathbb{C}[X, Y]$ εἶναι ἀνάγωγο:

$$Y^3 - (X^2 + 1)X, \quad Y^2 - (X - a)(X - b)(X - c),\ a, b, c \in \mathbb{C}, \quad Y^3 + X^4.$$

6 Συμπληρωματικὴ ὕλη σὲ δακτυλίους-πηλίκα καὶ ἰδεώδη

Πρόταση 6.1 *Ἔστω σῶμα K καὶ $p(X) \in K[X]$ ἀνάγωγο. Ἔστω ὅτι τὸ K εἶναι ὑπόσωμα ἑνὸς σώματος L καὶ $\lambda \in L$ τέτοιο ὥστε $p(\lambda) = 0$ (μ' ἄλλα λόγια, μέσα στὸ L, τὸ $p(X)$, θεωρούμενο ὡς πολυώνυμο τοῦ $L[X]$, ἔχει κάποια ρίζα λ). Ἔστω, τέλος, καὶ ἕνα πολυώνυμο $f(X) \in K[X]$, τέτοιο ὥστε $f(\lambda) = 0$. Τότε, στὴν ἀκέραια περιοχὴ $K[X]$ ἰσχύει $p(X) \,|\, f(X)$.*

Ἀπόδειξη. Ἡ $K[X]$ εἶναι περιοχὴ κυρίων ἰδεωδῶν καὶ τὸ $p(X)$ εἶναι ἀνάγωγο στοιχεῖο της. Ἄρα, ἀπὸ τὸ Θεώρημα 3.2 (α΄), ἢ τὸ $p(X)$ εἶναι πρῶτο πρὸς τὸ $f(X)$, ἢ $p(X) \,|\, f(X)$. Ἀρκεῖ ν' ἀποκλείσομε τὸ πρῶτο ἐνδεχόμενο. Ἂν ὑποθέσομε ὅτι $1 = \text{μκδ}(p(X), f(X))$, τότε, ἀπὸ τὸ Θεώρημα 3.1 συμπεραίνομε ὅτι ὑπάρχουν $h_1(X), h_2(X) \in K[X]$, τέτοια ὥστε $h_1(X)p(X) + h_2(X)f(X) = 1$. Ἡ ἀντικατάσταση $X \leftarrow \lambda$ στὴν τελευταία σχέση (ἀκριβέστερα, ἐφαρμόζοντας στὴ σχέση τὸν ὁμομορφισμὸ ἐκτίμησης $\epsilon_\lambda : K[X] \to K$· βλ. στὸ [1] τὸ παράδειγμα 9 τῆς ἑνότητας 2.5.2) δίνει $h_1(\lambda) \cdot 0 + h_2(\lambda) \cdot 0 = 1$, ὁπότε ὁδηγούμαστε στὸ ἄτοπο $0 = 1$.

□

Παράδειγμα. *Ἡ ἀντιστοιχία*

$$\mathbb{R}[X]/\langle X^2 + 1\rangle \ni f(X) + \langle X^2 + 1\rangle \overset{\phi}{\mapsto} f(i) \in \mathbb{C}$$

εἶναι καλὰ ὁρισμένη ἀπεικόνιση καὶ ἰσομορφισμὸς δακτυλίων. Λόγῳ αὐτοῦ τοῦ ἰσομορφισμοῦ συμπεραίνομε, εἰδικώτερα, ὅτι ὁ δακτύλιος πηλίκο $\mathbb{R}[X]/\langle X^2 + 1\rangle$ εἶναι σῶμα.

Ἀπόδειξη. • *Ἡ ϕ εἶναι καλὰ ὁρισμένη.* Ἂν $f_1(X) + \langle X^2 + 1\rangle = f_2(X) + \langle X^2 + 1\rangle$, αὐτὸ σημαίνει ὅτι $f_1(X) - f_2(X) \in \langle X^2 + 1\rangle$, ἄρα ὑπάρχει $g(X) \in \mathbb{R}[X]$, τέτοιο ὥστε $f_1(X) - f_2(X) = (X^2 + 1)g(X)$. Ἀλλὰ τότε, ἀπὸ τὴν ἀντικατάσταση $X \to i$ σ' αὐτὴ τὴ σχέση προκύπτει ὅτι $f_1(i) = f_2(i)$, ἄρα $\phi(f_1(X) + \langle X^2 + 1\rangle) = \phi(f_2(X) + \langle X^2 + 1\rangle)$.

• *Ἡ ϕ εἶναι ὁμομορφισμὸς δακτυλίων.*

$$\begin{aligned}\phi[(f_1(X)+\langle X^2+1\rangle)+(f_2(X)+\langle X^2+1\rangle)] &= \phi[(f_1(X)+f_2(X))+\langle X^2+1\rangle] \\ &= (f_1+f_2)(i) = f_1(i)+f_2(i) \\ &= \phi(f_1(X)+\langle X^2+1\rangle)+\phi(f_2(X)+\langle X^2+1\rangle).\end{aligned}$$

Ἐντελῶς ἀνάλογα δουλεύομε καὶ στὴν περίπτωση τοῦ πολλαπλασιασμοῦ.
• *Ἡ ϕ εἶναι 1-1.* Ἂν $\phi(f_1(X)+\langle X^2+1\rangle) = \phi(f_2(X)+\langle X^2+1\rangle)$, τότε $f_1(i) = f_2(i)$, ποὺ σημαίνει ὅτι τὸ i εἶναι ρίζα τοῦ $f_1(X)-f_2(X)$. Ἐφαρμόζοντας τὴν Πρόταση 6.1 μὲ $K = \mathbb{R}$, $p(X) = X^2+1$, $f(X) = f_1(X) - f_2(X)$, $L = \mathbb{C}$ καὶ $\lambda = i$ συμπεραίνομε ὅτι $X^2+1 \mid f_1(X) - f_2(X)$, ἄρα $f_1(X)-f_2(X) \in \langle X^2+1\rangle$. Αὐτό, ὅμως, ἰσοδυναμεῖ μὲ τὸ ὅτι $f_1(X)+\langle X^2+1\rangle = f_2(X)+\langle X^2+1\rangle$.
• *Ἡ ϕ εἶναι ἐπί.* Ἔστω τυχαῖος μιγαδικὸς $a+bi$ ($a,b \in \mathbb{R}$). Τότε, γιὰ $f(X) = bX+a$ ἔχομε $f(X)+\langle X^2+1\rangle = f(i) = a+bi$.

□

Ἄσκηση 6.1 *Σὲ κάθε δακτύλιο R ἰσχύει $R/\langle 0\rangle \cong R$. Ἐπίσης, $R/R = \{0+R\}$, δηλαδή, ὁ δακτύλιος R/R περιέχει μόνο τὸ μηδενικὸ στοιχεῖο (τὴ μηδενικὴ κλάση)· εἶναι, ὅπως λέμε, ὁ μηδενικὸς δακτύλιος.*

Ἄσκηση 6.2 *Ἔστω R δακτύλιος μὲ μοναδιαῖο καὶ I ἰδεῶδες τοῦ R, τὸ ὁποῖο περιέχει κάποια μονάδα τοῦ R. Ἀποδεῖξτε ὅτι, τότε, $I = R$.*

Ἄσκηση 6.3 *Ἔστω μεταθετικὸς δακτύλιος R μὲ μοναδιαῖο καὶ ἰδεῶδες I τοῦ R. Ἀποδεῖξτε ὅτι, ἂν $a \in I$, τότε $\langle a\rangle \subseteq I$.*

Πρόταση 6.2 *(α΄) Ἔστω ἀκέραια περιοχὴ D καὶ $a \in D$ ὄχι ἀνάγωγο. Τότε τὸ ἰδεῶδες $\langle a\rangle$ τῆς D δὲν εἶναι πρῶτο.*

(β΄) Ἔστω περιοχὴ κυρίων ἰδεωδῶν D καὶ $a \in D$ ἀνάγωγο. Τότε τὸ ἰδεῶδες $\langle a\rangle$ τῆς D εἶναι μεγιστικό (maximal).

Ἀπόδειξη. (α΄) Ἐξ ὑποθέσεως ὑπάρχουν $b, c \in D$, ποὺ δὲν εἶναι μονάδες, τέτοια ὥστε $a = bc$. Προφανῶς, $a \in \langle a\rangle$ ἄρα $bc \in \langle a\rangle$. Ἂν τὸ $\langle a\rangle$ εἶναι πρῶτο, τότε συμπεραίνομε ὅτι τουλάχιστον ἕνα ἐκ τῶν b, c ἀνήκει στὸ $\langle a\rangle$. Ἂν, γιὰ παράδειγα, $b \in \langle a\rangle$, τότε $b = ad$ γιὰ κάποιο $d \in D$. Ἀντικαθιστώντας αὐτὴ τὴν ἔκφραση τοῦ b στὴ σχέση $a = bc$ παίρνομε $a = (ad)c$, ἄρα $1 = bc$. Αὐτὸ μᾶς λέει ὅτι $c \in D^*$ καὶ φθάνομε σὲ ἀντίφαση.

(β΄) Ἔστω ἰδεῶδες I τῆς D, τέτοιο ὥστε $\langle a\rangle \subsetneq I$. Πρέπει καὶ ἀρκεῖ νὰ δείξομε ὅτι, τότε, $I = D$. Ἐπειδὴ ἡ D εἶναι περιοχὴ κυρίων ἰδεωδῶν, τὸ I εἶναι κύριο ἰδεῶδες, ἄρα ὑπάρχει $b \in D$, τέτοιο ὥστε $I = \langle b\rangle$. Ἔτσι ἔχομε $\langle a\rangle \subsetneq \langle b\rangle$. Ἀπὸ τὴν ἄσκηση 6.3 βλέπομε ὅτι, ἂν ἦταν $b \in \langle a\rangle$, τότε $\langle b\rangle \subsetneq \langle a\rangle$ καὶ θὰ ἐρχόμαστε σὲ ἀντίφαση μ᾽ τὴν ὑπόθεση ὅτι τὸ $\langle b\rangle$ περιέχει *γνησίως* τὸ $\langle a\rangle$. Συνεπῶς $b \notin \langle a\rangle$, ποὺ ἰσοδυναμεῖ μὲ τὸ ὅτι $a \nmid b$. Ἀπὸ τὴν ἄλλη, $a \in \langle b\rangle$, ἄρα ὑπάρχει $c \in D$, τέτοιο ὥστε $a = bc$. Ὅμως $a|a$, ἄρα $a|bc$. Ἐπειδὴ ἡ D εἶναι περιοχὴ κυρίων ἰδεωδῶν, τὸ a, ὡς ἀνάγωγο εἶναι καὶ πρῶτο (Θεώρημα 3.2 (β΄)), ἄρα $a|b$ εἴτε $a|c$. Παραπάνω εἴδαμε ὅτι $a \nmid b$, ἄρα $a|c$, ὁπότε θέτομε $c = ad$, γιὰ κάποιο $d \in D$. Ἀντικαθιστώντας αὐτὴ τὴν τιμὴ τοῦ c στὴ σχέση $a = bc$ παίρνομε $a = b(ad)$, ἄρα $1 = bd$. Συνεπῶς, $b \in D^*$, ἄρα ἀπὸ τὴν ἄσκηση 6.2, $\langle b\rangle = D$, ἄρα $I = D$.

□

Ἄσκηση 6.4 *Ἔστω σῶμα K. (α΄) Ἂν τὸ $f(X) \in K[X]$ δὲν εἶναι ἀνάγωγο πολυώνυμο, τότε τὸ ἰδεῶδες $\langle f(X)\rangle$ τοῦ $K[X]$ δὲν εἶναι πρῶτο καὶ ὁ δακτύλιος $K[X]/\langle f(X)\rangle$ ἔχει μηδενοδιαιρέτες.*

(β΄) Ἂν τὸ $f(X) \in K[X]$ εἶναι ἀνάγωγο πολυώνυμο, τότε τὸ ἰδεῶδες $\langle f(X)\rangle$ τοῦ $K[X]$ εἶναι μεγιστικὸ (maximal) καὶ ὁ δακτύλιος $K[X]/\langle f(X)\rangle$ εἶναι σῶμα.

Ἄσκηση 6.5 *Ἔστω περιοχὴ μονοσήμαντης ἀνάλυσης D καὶ a ἀνάγωγο στοιχεῖο τῆς D. Ἀποδεῖξτε ὅτι τὸ ἰδεῶδες $\langle a\rangle$ τῆς D εἶναι πρῶτο.*

Σημείωση: Συγκρίνετε τὴν ἐκφώνηση τῆς ἀσκήσεως 6.5 μὲ τὴν Πρόταση 6.2 (β΄) καὶ παρατηρῆστε τὶς διαφορὲς στὶς ἐκφωνήσεις καὶ τὰ συμπεράσματα.

> Στὶς παρακάτω ἀσκήσεις βασικὰ ἐργαλεῖα σας θὰ εἶναι ἕνα ἢ περισσότερα ἀπὸ τὰ ἑξῆς: Πρόταση 6.2, ἄσκηση 6.5, Θεωρήματα 2.10.3 καὶ 2.10.6 τοῦ βιβλίου [1] καὶ Πόρισμα 2.10.7 τοῦ ἴδιου βιβλίου.

Ἄσκηση 6.6 *(α΄) Ἀποδεῖξτε ὅτι τὸ ἰδεῶδες $\langle X, 2\rangle$ τοῦ $\mathbb{Z}[X]$ δὲν εἶναι κύριο. Συμπεράνατε ὅτι ἡ ἀκέραια περιοχὴ $\mathbb{Z}[X]$ δὲν εἶναι περιοχὴ κυρίων ἰδεωδῶν, ἐνῶ εἶναι περιοχὴ μονοσήμαντης ἀνάλυσης (Γιατί; Βάσει τίνος Θεωρήματος;) Γιατὶ εἶναι τὸ ἰδεῶδες $\langle X\rangle$ τῆς $\mathbb{Z}[X]$ πρῶτο;*
(β΄) Βάσει τίνος θεωρήματος εἶναι ἡ ἀκέραια περιοχὴ $\mathbb{Q}[X]$ περιοχὴ κυρίων ἰδεωδῶν; Γιατὶ εἶναι τὸ ἰδεῶδες $\langle X\rangle$ τῆς $\mathbb{Q}[X]$ μεγιστικό (maximal);

Ἄσκηση 6.7 *Ἀποδεῖξτε ὅτι ὁ δακτύλιος $\mathbb{Z}[X, Y]/\langle X\rangle$ εἶναι ἀκέραια περιοχή. Μετά, ἀποδεῖξτε ὅτι τὸ στοιχεῖο $Y + \langle X\rangle$ αὐτῆς τῆς ἀκέραιας περιοχῆς δὲν ἔχει ἀντίστροφο. Συμπεράνατε ὅτι ἡ ἀκέραια περιοχὴ $\mathbb{Z}[X, Y]/\langle X\rangle$ δὲν εἶναι σῶμα.*

Ἄσκηση 6.8 *Βρεῖτε ἕνα ζεῦγος μηδενοδιαιρετῶν στὸν δακτύλιο $\mathbb{Z}[X, Y]/\langle XY\rangle$. Συμπεράνατε ὅτι ὁ δακτύλιος $\mathbb{Z}[X, Y]/\langle XY\rangle$ δὲν εἶναι ἀκέραια περιοχή.*

Ἄσκηση 6.9 *(α΄) Ἔστω R μεταθετικὸς δακτύλιος μὲ μοναδιαῖο. Ἀποδεῖξτε ὅτι κάθε $f(X, Y) \in R[X, Y]$ μπορεῖ νὰ γραφεῖ ὡς ἑξῆς: $f(X, Y) = g(X, Y) \cdot Y + h(X) \cdot X + c$, ὅπου $g(X, Y) \in R[X, Y]$, $h(X) \in R[X]$ καὶ $r \in R$.*
Ὑπόδειξη: Δεῖτε τὸ $f(X, Y)$ ὡς πολυώνυμο τοῦ Y μὲ συντελεστὲς στὸν δακτύλιο $R[X]$.
Συμπεράνατε ὅτι, κάθε $f(X, Y) \in R[X, y]$ γράφεται μὲ τὴ μορφὴ $f(X, Y) = f_0(X, Y) + c$, ὅπου $f_0(X, Y) \in \langle X, Y\rangle$ καὶ c εἶναι ὁ "σταθερὸς ὅρος" τοῦ $f(X, Y)$.
(β΄) Ἀποδεῖξτε ὅτι ὁ μοναδικὸς ἀκέραιος, ποὺ ἀνήκει στὸ ἰδεῶδες $\langle X, Y\rangle$ τοῦ $\mathbb{Z}[X, Y]$, εἶναι τὸ 0.
(γ΄) Ἀποδεῖξτε ὅτι τὸ ἰδεῶδες $\langle X, Y\rangle$ τοῦ $\mathbb{Z}[X, Y]$ εἶναι πρῶτο.
Ὑπόδειξη: Ἔστω $f(X, y)g(X, Y) \in \langle X, Y\rangle$. Πρέπει ν' ἀποδείξετε ὅτι ἕνας, τουλάχιστον, ἀπὸ τοὺς παράγοντες ἀνήκει στὸ $\langle X, Y\rangle$. Γράψτε καθέναν ἀπὸ τοὺς παράγοντες μὲ τὴ μορφὴ ποὺ περιγράφεται στὸ ἐρώτημα (α΄).
Συμπεράνατε ὅτι ὁ δακτύλιος $\mathbb{Z}[X, Y]/\langle X, Y\rangle$ εἶναι ἀκέραια περιοχή.
(δ΄) Ἀποδεῖξτε ὅτι, στὴν ἀκέραια περιοχὴ $\mathbb{Z}[X, Y]$ ἔχομε $\langle X, Y\rangle \subsetneq \langle X, Y, 2\rangle \subsetneq \mathbb{Z}[X, Y]$. Συμπεράνατε ὅτι τὸ $\langle X, Y\rangle$ δὲν εἶναι μεγιστικὸ (maximal) ἰδεῶδες τῆς $\mathbb{Z}[X, Y]$ καὶ ἡ ἀκέραια περιοχὴ $\mathbb{Z}[X, Y]/\langle X, Y\rangle$ δὲν εἶναι σῶμα.
(ε΄) Ἀποδεῖξτε ὅτι, στὴν ἀκέραια περιοχὴ $\mathbb{Q}[X, Y]$, τὸ ἰδεῶδες $\langle X, Y\rangle$ εἶναι μεγιστικὸ (maximal) καὶ συμπεράνατε ὅτι ὁ δακτύλιος $\mathbb{Q}[X, Y]/\langle X, Y\rangle$ εἶναι σῶμα. Συγκρίνετε αὐτό, μὲ τὸ συμπέρασμα τοῦ ἐρωτήματος (δ΄).

Ἄσκηση 6.10 *(α΄) Ἔστω ὅτι R, S εἶναι δακτύλιοι μὲ μοναδιαῖο καὶ $\phi : R \to S$ ὁμομορφισμὸς δακτυλίων, ὄχι ὁ μηδενικὸς ὁμομορφισμός (δηλαδή, δὲν εἶναι $\phi(r) = 0$ γιὰ ὅλα τὰ $r \in R$). Ἀποδεῖξτε ὅτι $\phi(1) = 1$.*
(β΄) Ἔστω ὅτι τὰ σώματα K, L περιέχουν τὸ $\mathbb{Q}$ ὡς ὑπόσωμά τους καὶ $\phi : K \to L$ εἶναι ὁμομορφισμὸς σωμάτων, ὄχι ὁ μηδενικός. Ἀποδεῖξτε ὅτι $\phi(q) = q$ γιὰ κάθε $q \in \mathbb{Q}$.
Ὑπόδειξη: Χρησιμοποιώντας τὸ ἐρώτημα (α΄), ἀποδεῖξτε ὅτι $\phi(n) = n$ γιὰ κάθε $n \in \mathbb{N}$, μετά, $\phi(a) = a$ γιὰ κάθε $a \in \mathbb{Z}$ καί, τέλος, γράψτε $q = m/n$, μὲ $m, n \in \mathbb{Z}$, $n \neq 0$ καὶ ἐφαρμόστε τὸν ϕ στὴ σχέση $nq = m$.
(γ΄) Ἀποδεῖξτε ὅτι, ἂν ὁ d εἶναι ἀκέραιος > 1, ὄχι τετράγωνο ἀκεραίου, τότε τὸ $\mathbb{Q}[\sqrt{d}] = \{q + r\sqrt{d} : q, r \in \mathbb{Q}\}$ εἶναι ὑπόσωμα τοῦ $\mathbb{R}$. Μετά, ἀποδεῖξτε ὅτι δὲν ὑπάρχει μονομορφισμὸς σωμάτων $\phi : \mathbb{Q}[\sqrt{2}] \to \mathbb{Q}[\sqrt{3}]$.
Ὑπόδειξη: Ἔστω ὅτι $\phi(\sqrt{2}) = a + b\sqrt{3}$, ὅπου $a, b \in \mathbb{Q}$. Τότε, χρησιμοποιώντας καὶ τὸ ἐρώτημα (β΄), ἔχομε $2 = \phi(2) = \phi(\sqrt{2}\sqrt{2}) = \ldots$. Αὐτὸ θὰ σᾶς ὁδηγήσει σὲ ἄτοπο. Πάρετε δεδομένο ὅτι $\sqrt{3/2} \notin \mathbb{Q}$.

Ἄσκηση 6.11 *Ποιὸς ἀπὸ τοὺς ἑπόμενους δακτυλίους-πηλίκα εἶναι σῶμα ἢ/καὶ ἀκέραια περιοχή;*
(α΄) $\mathbb{Z}[X]/\langle X\rangle$ (β΄) $\mathbb{Q}[X]/\langle X^2 - 9\rangle$ (γ΄) $\mathbb{Q}[X]/\langle X^3 - 2\rangle$ (δ΄) $\mathbb{R}[X]/\langle X^3 - 2\rangle$
(ε΄) $\mathbb{Z}_3[X]/\langle X^2 + X + 1\rangle$ (ς΄) $\mathbb{Z}_5[X]/\langle X^2 + X + 1\rangle$

Ὁμομορφισμὸς ἐκτίμησης (ὑπενθύμιση). Ἔστω R μεταθετικὸς δακτύλιος μὲ μοναδιαῖο. Γιὰ κάθε $r \in R$ ἔχομε τὴν ἀπεικόνιση $\epsilon_r : R \to R[X]$, ποὺ ὁρίζεται ἀπὸ τὴ σχέση $\epsilon_r(f(X)) = f(r)$ γιὰ κάθε $f(X) \in R[X]$. Ἡ ἀπεικόνιση αὐτὴ ἀποδεικνύεται ὅτι εἶναι ὁμομορφισμὸς δακτυλίων καὶ λέγεται *ἐκτίμηση στὸ r* ἢ *ὁμομορφισμὸς ἐκτίμησης στὸ r* (βλ. Παράδειγμα 9, τῆς ἑνότητας 2.5.2 τοῦ [1]). Εἶναι πολὺ ἁπλὸ νὰ δοῦμε ὅτι, ἂν S εἶναι ὑποδακτύλιος τοῦ R, τότε $S[X]$ εἶναι ὑποδακτύλιος τοῦ $R[X]$ καὶ ὁ περιορισμὸς τοῦ ὁμομορφισμοῦ ϵ_r στὸν $S[Q]$ εἶναι, ἐπίσης, ὁμομορφισμὸς δακτυλίων $\phi : S[X] \to R$, γιὰ τὸν ὁποῖον ἰσχύει $\phi(f(X)) = f(r)$ γιὰ κάθε $f(X) \in S[X]$.

Ξαναβλέποντας το παράδειγμα τῆς σελίδας 18. Θὰ ἀποδείξομε τὸν ἰσομορφισμὸ $\mathbb{R}[X]/\langle X^2 + 1\rangle \cong \mathbb{C}$ χρησιμοποιώντας τὸ *Πρῶτο Θεώρημα Ἰσομορφισμοῦ Δακτυλίων* (βλ. [1, Θεώρημα 2.6.6]).
Θεωροῦμε τὸν ὁμομορφισμὸ $\phi : \mathbb{R}[X] \to \mathbb{C}$, γιὰ τὸν ὁποῖον $\phi(f(X)) = f(i)$ γιὰ κάθε $f(X) \in \mathbb{R}[X]$. Μ' ἄλλα λόγια, ϕ εἶναι ὁ περιορισμὸς τοῦ ὁμομορφισμοῦ ἐκτίμησης $\epsilon_i : \mathbb{C}[X] \to \mathbb{C}$ (βλ. παραπάνω).
Ὁ ϕ εἶναι ἐπιμορφισμός (ἄρα $\mathrm{Im}\phi = \mathbb{C}$), διότι, γιὰ κάθε $a + bi \in \mathbb{C}$ $(a, b \in \mathbb{R})$ εἶναι $\phi(a + bX) = a + bi$. Ἀκόμη, $\mathrm{Ker}\phi = \langle X^2 + 1\rangle$. Πράγματι, $f(X) \in \mathrm{Ker}\phi \Leftrightarrow f(i) = 0$. Ἐφαρμόζοντας τὴν Πρόταση 6.1 μὲ $K = \mathbb{R}$, $p(X) = X^2 + 1$, $L = \mathbb{C}$ καὶ $\lambda = i$ συμπεραίνομε ὅτι $f(i) = 0$ ἂν καὶ μόνο ἂν $X^2 + 1 \mid f(X)$ (διαιρετότητα στὴν ἀκέραια περιοχὴ $\mathbb{R}[X]$), ἄρα, ἂν καὶ μόνο ἂν $f(X) \in \langle X^2 + 1\rangle$.
Ἀπὸ τὸ Πρῶτο Θεώρημα Ἰσομορφισμοῦ Δακτυλίων ἕπεται ὅτι $\mathbb{R}[X]/\mathrm{Ker}\phi \cong \mathrm{Im}\phi$, ἄρα $\mathbb{R}[X]/\langle X^2 + 1\rangle \cong \mathbb{C}$.

Ἄσκηση 6.12 *Μὲ συλλογισμοὺς παρόμοιους ἐκείνων τοῦ παραπάνω παραδείγματος ἀποδεῖξτε ὅτι $\mathbb{R}[X]/\langle X^2 + 2\rangle \cong \mathbb{C}$. Συμπεράνατε ὅτι $\mathbb{R}[X]/\langle X^2 + 1\rangle \cong \mathbb{C} \cong \mathbb{R}[X]/\langle X^2 + 2\rangle \cong \mathbb{C}$, ἐνῶ $\langle X^2 + 1\rangle \neq \langle X^2 + 2\rangle$ (ἀποδεῖξτε αὐτὸν τὸν ἰσχυρισμό).*

Ἄσκηση 6.13 -Σῶμα 8 στοιχείων. *Ὁ δακτύλιος-πηλίκο $K = \mathbb{Z}_2[X]/\langle X^3 + X + 1\rangle$ ἀποδεῖξτε ὅτι εἶναι σῶμα. Ἔστω $u = X + \langle X^3 + X + 1\rangle \in K$.*
(α΄) Ἀποδεῖξτε ὅτι κάθε στοιχεῖο τοῦ K μπορεῖ νὰ γραφτεῖ μὲ τὴ μορφὴ $a + bu + cu^2$, μὲ

$a, b, c \in \mathbb{Z}_2$.

Ὑπόδειξη: Ἔστω $f(X) + \langle X^3 + X + 1\rangle \in K$. *Ἔστω ὅτι, στὸ σῶμα* $\mathbb{Z}_2[X]$, *ἡ εὐκλείδεια διαίρεση τοῦ* $f(X)$ *διὰ* $X^3 + X + 1$ *δίνει ὑπόλοιπο* $a + bX + cX^2$. *Δεῖξτε ὅτι* $f(X) \equiv a + bX + cX^2 \pmod{\langle X^3 + X + 1\rangle}$, *συνεπῶς,* $f(X) + \langle X^3 + X + 1\rangle \equiv a + bX + cX^2 + \langle X^3 + X + 1\rangle$. *Τέλος, ἀποδεῖξτε ὅτι* $a + bX + cX^2 + \langle X^3 + X + 1\rangle = a + bu + cu^2$.
(β΄) Ἀποδεῖξτε ὅτι $a_1 + b_1u + c_1u^2 = a_2 + b_2u + c_2u^2 \Leftrightarrow (a_1, b_1, c_1) = (a_2, b_2, c_2)$. *Ἀπὸ αὐτὸ συμπεράνατε ὅτι τὸ σῶμα* K *ἔχει ἀκριβῶς 8 στοιχεῖα καὶ συμπληρῶστε τοὺς πίνακες τῶν πράξεων* $+$ *καὶ* $\cdot$ *τοῦ* K.

Ὑπόδειξη: Κατ' ἀρχάς, δεῖτε ὅτι $u^3 = u + 1$ *καὶ* $u^4 = u^2 + u$. *Στὴ συνέχεια, συμπληρῶστε κάθε τετραγωνάκι τοῦ πίνακα μὲ τὴ μορφὴ* $a + bu + cu^2$. *Γιὰ παράδειγμα, στὸν πίνακα πρόσθεσης, στὸ τετραγωνάκι, ποὺ διασταυρώνεται ἡ γραμμὴ τοῦ* $1 + u^2$ *μὲ τὴ στήλη τοῦ* $1 + u$, *θὰ μπεῖ* $u + u^2$, *ἐνῶ στὸ ἀντίστοιχο τετραγωνάκι τοῦ πίνακα πολλαπλασιασμοῦ, θὰ μπεῖ τὸ* $(1 + u^2)(1 + u) = u^2$.

Ἄσκηση 6.14 -Σῶμα 9 **στοιχείων.** *Κάνοντας χρήση τοῦ δακτυλίου* $K = \mathbb{Z}_3[X]/\langle X^2 + 1\rangle$ *καὶ μὲ βήματα ἐντελῶς ἀνάλογα ἐκείνων τῆς ἀσκήσεως 6.13, κατασκευάστε ἕνα σῶμα μὲ ἀκριβῶς* 9 *στοιχεῖα. Συμπληρῶστε τοὺς πίνακες πράξεων.*

Ἄσκηση 6.15 *Ἀποδεῖξτε ὅτι τὸ* $Y^2 - (X - a)(X - b)(X - c)(X - d) \in \mathbb{C}[X, Y]$, $a \neq b, c, d$ *εἶναι ἀνάγωγο στοιχεῖο τῆς ἀκέραιας περιοχῆς* $\mathbb{C}[X, Y]$.

Α΄

Παράρτημα: Μία χρήσιμη μορφὴ Μαθηματικῆς Ἐπαγωγῆς

Θεώρημα Α΄.1 *Ἔστω μία πρόταση* $\Pi(n)$*, ποὺ ἐξαρτᾶται ἀπὸ τὸν φυσικὸ ἀριθμὸ* n *καὶ κάποιος συγκεκριμένος φυσικὸς ἀριθμὸς* n_0*. Γιὰ ν' ἀποδείξομε ὅτι ἡ πρόταση* $\Pi(n)$ *εἶναι ἀληθὴς γιὰ κάθε φυσικὸ ἀριθμὸ* $n \geq n_0$*, κάνομε τὰ ἑξῆς:*

- *Ἀποδεικνύομε ὅτι ἡ πρόταση* $\Pi(n_0)$ *εἶναι ἀληθής.*
- (Ἐπαγωγικὴ ὑπόθεση). *Θεωροῦμε* γενικὸ $n > n_0$ *καὶ ὑποθέτομε ὅτι ἡ πρόταση* $\Pi(k)$ *εἶναι ἀληθὴς γιὰ κάθε φυσικὸ* k *μὲ* $n_0 \leq k < n$*.*
- *Βασιζόμενοι στὴν παραπάνω ἐπαγωγικὴ ὑπόθεση, ἀποδεικνύομε ὅτι ἡ πρόταση* $\Pi(n)$ *εἶναι ἀληθής.*

Εὑρετήριο

Ἀναφορὲς

[1] Δ. Βάρσος, Δ. Δεριζιώτης, Γ. Ἐμμανουήλ, Μ. Μαλιάκας, Ὀ. Ταλέλλη, *Μια Εισαγωγή στην Άλγεβρα*, Εκδόσεις ΣΟΦΙΑ, Αθήνα 2012.

[2] J.B. Fraleigh, *Εισαγωγή στην Άλγεβρα*, Πανεπιστημιακές Εκδόσεις Κρήτης, Ηράκλειο 1994.