ΘΕΩΡΙΑ ΔΑΚΤΥΛΙΩΝ

Σημειώσεις προπτυχιακού μαθήματος [1]

Ν.Γ. Τζανάκης

Τμήμα Μαθηματικών

Πανεπιστήμιο Κρήτης - Ηράκλειο

[1] Χειμερινό εξάμηνο 2024

Περιεχόμενα

Κεφάλαιο 1

Διαιρετότητα

Στο παρόν κεφάλαιο, το D συμβολίζει πάντα ακέραια περιοχή. Με $Q(D)$ συμβολίζομε το *σώμα πηλίκων* της D.

1.1 Τα βασικα

Ορισμός. (α') Το μη μηδενικό $\epsilon \in D$ λέγεται *μονάδα* της D, αν είναι *αντιστρέψιμο* στοιχείο του D, δηλαδή, αν και μόνο αν το ϵ^{-1}, το οποίο βεβαίως ανήκει στο $Q(D)$, είναι στοιχείο της D. Το $1 \in D$ είναι μονάδα, αλλά, συγχρόνως, είναι και *το* (μοναδικό) μοναδιαίο στοιχείο της D.

Το σύνολο των μονάδων της D συμβολίζεται D^*.

(β') Τα μη μηδενικά στοιχεία a, b χαρακτηρίζονται *συνεταιρικά*, αν $b = \epsilon\alpha$ με $\epsilon \in D^*$. Η σχέση συνεταιρικότητας είναι, προφανώς, σχέση ισοδυναμίας.
(γ') Αν $a, b \in D$ και $b \neq 0$ και υπάρχει $\gamma \in D$ ώστε να ισχύει $a = b\gamma$, τότε λέμε ότι *τό b διαιρεί το a·* συμβολικά, $b \mid a$. Ισοδύναμες διατυπώσεις:

- Το a *διαιρείται*, *ή είναι διαιρετό* από το (διά τού) b.
- Το b είναι *διαιρέτης* του a.
- Το a είναι *πολλαπλάσιο* του b.

Εύκολα βλέπει κανείς ότι οι μονάδες και τα συνεταιρικά στοιχεία του a είναι διαιρέτες του a, τους οποίους χαρακτηρίζομε *τετριμμένους διαιρέτες* του a. Οι μη τετριμμένοι διαιρέτες του a χαρακτηρίζονται *γνήσιοι διαιρέτες* του a.
Όταν γράφομε $b \nmid a$ εννοούμε ότι ο b δεν διαιρεί τον a.
(δ') Το μη μηδενικό στοιχείο p χαρακτηρίζεται *ανάγωγο στοιχείο* της D αν δεν είναι μονάδα και οι μόνοι διαιρέτες του p είναι οι τετριμμένοι.
(ε') Το μη μηδενικό στοιχείο π χαρακτηρίζεται *πρώτο στοιχείο* της D αν δεν είναι μονάδα και, επιπλέον, έχει την εξής ιδιότητα: Κάθε σχέση της μορφής $\pi \mid ab$, με $a, b \in D$, συνεπάγεται ότι το π διαιρεί τουλάχιστον ένα από τα a, b.

Άσκηση 1.1 Στην ειδική περίπτωση που η ακέραια περιοχή D είναι σώμα, αποδείξτε ότι κάθε μη μηδενικό στοιχείο είναι μονάδα, καθώς και ότι κάθε μη μηδενικό στοιχείο διαιρεί οποιοδήποτε στοιχείο της D.

Η άσκηση 1.1 μας λέει ότι η διαιρετότητα σε σώμα είναι τετριμμένη, δίχως ουσιαστικό ενδιαφέρον. Άρα, οτιδήποτε αποδειχθεί σ' αυτό το κεφάλαιο έχει ουσιαστικό νόημα στις περιπτώσεις ακεραίων περιοχών, οι οποίες *δέν* είναι σώματα.

Άσκηση 1.2 Αν $b, a_1, \dots, a_n \in D$ και $b \mid a_i$ για κάθε $i = 1, \dots, n$, τότε, οποιαδήποτε κι αν είναι τα $t_1, \dots, t_n \in D$, το b διαιρεί το $t_1a_1 + \cdots + t_na_n$.

Άσκηση 1.3 Έστω ότι $\epsilon, p \in D$ είναι μονάδα και ανάγωγο στοιχείο, αντιστοίχως. Αποδείξτε ότι το ϵp είναι ανάγωγο στοιχείο.

Άσκηση 1.4 Η σχέση διαιρετότητας $a \mid b$ δεν επηρεάζεται αν κάποιο (ή και τα δύο) από τα a, b αντικατασταθεί από συνεταιρικό του στοιχείο.

Άσκηση 1.5 Έστω ότι a, b είναι μη μηδενικά στοιχεία, το a είναι διαιρέτης του b και το b είναι διαιρέτης του a. Δείξτε ότι τα a, b είναι συνεταιρικά.

Άσκηση 1.6 Αποδείξτε ότι καθένα από τα σύνολα D^* και $D \setminus D^*$ είναι κλειστό ως προς τον πολλαπλασιασμό.

Άσκηση 1.7 Αποδείξτε ότι το $a \in D \setminus D^*$ *δεν είναι* ανάγωγο αν και μόνο αν υπάρχουν $b, c \in D \setminus D^*$ με $bc = a$.

Πρόταση 1.1 *Κάθε πρώτο στοιχείο της D είναι ανάγωγο. Το αντίστροφο δεν ισχύει εν γένει.*

Απόδειξη. Έστω p πρώτο στοιχείο της D. Θα δείξομε ότι κάθε διαιρέτης a του p είναι συνεταιρικό στοιχείο του p ή μονάδα.

Λόγω της $a \mid p$, είναι $p = ab$ με $b \in D$. Προφανώς $p \mid ab$, άρα, καθώς το p είναι πρώτο στοιχείο, $p \mid a$ είτε $p \mid b$.

Αν $p \mid a$, τότε $a = pc$ με $c \in D$, άρα η σχέση $p = ab$ μας δίνει $p = (pc)b$. Στην D ισχύει ο νόμος της διαγραφής, άρα $1 = cb$. Αυτή η σχέση μας λέει ότι $c \in D^*$, άρα, λόγω και της $a = pc$, το a είναι συνεταιρικό του p.

Αν $p \mid b$, τότε $b = pc$ με $c \in D$ και η σχέση $p = ab$ μας δίνει $p = a(pc)$, άρα $1 = ac$, σχέση η οποία μας λέει ότι το a είναι μονάδα.

Για το ότι δεν ισχύει το αντίστροφο εν γένει, βλ. παράδειγμα (ε'), παρακάτω. □

Παραδείγματα. **(α')** Οι μόνες μονάδες του $\mathbb{Z}$ είναι τα ± 1. Τα ανάγωγα στοιχεία του $\mathbb{Z}$ είναι, προφανώς, οι πρώτοι αριθμοί και οι αντίθετοί τους. Επιπλέον, τα πρώτα στοιχεία του $\mathbb{Z}$ (υπό την έννοιαν του γενικού ορισμού, που δώσαμε στην

αρχή του κεφαλαίου) ταυτίζονται με τους πρώτους αριθμούς και τους αντίθετούς τους. Πράγματι, ξέρομε από τη στοιχειώδη Θεωρία Αριθμών ότι, αν ο p είναι πρώτος και $p \mid ab$, όπου $a, b \in \mathbb{Z}$, τότε ο p διαιρεί ένα τουλάχιστον από τα a, b, δηλαδή ο p είναι πρώτο στοιχείο της ακέραιας περιοχής $\mathbb{Z}$. Επιπλέον, ουδείς μη πρώτος ακέραιος $m \neq \pm 1$ μπορεί να είναι πρώτο στοιχείο, διότι, αν $m = ab$, με τους a, b ακεραίους διάφορους των ± 1 (οπότε $1 < |a|, |b| < |m|$), τότε $m|ab$, ενώ ο m δεν διαιρεί ούτε τον a ούτε τον b.
Συμπέρασμα: Στην ακέραια περιοχή $\mathbb{Z}$, πρώτα και ανάγωγα στοιχεία ταυτίζονται και το σύνολό τους είναι το σύνολο των πρώτων αριθμών και των αντιθέτων τους.

(β′) Έστω σώμα K. Από το εισαγωγικό μάθημα της Άλγεβρας ξέρομε ότι ο δακτύλιος πολυωνύμων $K[X]$ είναι ακέραια περιοχή, οι μοναδικές μονάδες του οποίου είναι τα μη μηδενικά σταθερά πολυώνυμα, δηλαδή, τα μη μηδενικά στοιχεία του K. Τα ανάγωγα στοιχεία της ακέραιας περιοχής $K[X]$ είναι, ακριβώς, τα ανάγωγα πάνω από το K πολυώνυμα. Αξίζει να σημειωθεί ότι κάθε ανάγωγο πολυώνυμο πάνω από το K είναι πρώτο στοιχείο της ακέραιας περιοχής $K[X]$. Πράγματι, από το εισαγωγικό μάθημα της Άλγεβρας ξέρομε ότι, αν το $p(X) \in K[X]$ είναι ανάγωγο και διαιρεί το γινόμενο δύο πολυωνύμων του $K[X]$, τότε, υποχρεωτικά, το $p(X)$ διαιρεί ένα, τουλάχιστον, από τα δύο αυτά πολυώνυμα. Άρα, τα ανάγωγα πολυώνυμα του $K[X]$ είναι πρώτα στοιχεία της ακέραιας περιοχής $K[X]$. Επιπλέον, κάθε μη σταθερό, μη ανάγωγο πολυώνυμο $f(X) \in K[X]$ δεν είναι πρώτο. Διότι, αν $f(X) = g(X)h(X)$, με τα $g(X), h(X)$ πολυώνυμα του $K[X]$ βαθμού $< \deg f(X)$, τότε $f(X)|g(X)h(X)$, ενώ το $f(X)$ δεν διαιρεί ουτε το $g(X)$, ούτε το $h(X)$.
Συμπέρασμα: Στην ακέραια περιοχή $K[X]$ (K σώμα), ανάγωγα και πρώτα στοιχεία ταυτίζονται και το σύνολό τους είναι το σύνολο των αναγώγων πολυωνύμων του $K[X]$.

(γ′) Έστω θετικός ακέραιος d, όχι τέλειο τετράγωνο, και η ακέραια περιοχή

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

Θα προσδιορίσομε τις μονάδες της $\mathbb{Z}[\sqrt{d}]$. Έστω $\epsilon = x + y\sqrt{d}$ ένα μη μηδενικό στοιχείο της $\mathbb{Z}[\sqrt{d}]$. Τότε, $x - y\sqrt{d} \neq 0$. Πράγματι, στην αντίθετη περίπτωση θα είχαμε $x = y\sqrt{d}$, οπότε, $y \neq 0$ και $\sqrt{d} = x/y$, άρα $d = (x/y)^2$, που έρχεται σε αντίφαση με την υπόθεση για το d. Τώρα μπορούμε, επίσης, να συμπεράνομε ότι $x^2 - dy^2 = (x + y\sqrt{d})(x - y\sqrt{d}) \neq 0$.

Το ϵ είναι μονάδα, αν και μόνο αν $\epsilon^{-1} \in \mathbb{Z}[\sqrt{d}]$.

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

συνεπώς, $\epsilon^{-1} \in \mathbb{Z}[\sqrt{d}]$ αν και μόνο αν οι ρητοί αριθμοί $x/(x^2 - dy^2)$ και $y/(x^2 - dy^2)$ είναι ακέραιοι. Αν οι αριθμοί αυτοί είναι ακέραιοι, τότε και τα τετράγωνά τους είναι ακέραιοι, οπότε ακέραιος είναι και ο αριθμός

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

που σημαίνει ότι $x^2-dy^2=\pm 1$. Το αντίστροφο ισχύει προφανώς: Αν $x^2-dy^2=\pm 1$, οι αριθμοί $x/(x^2-dy^2)$ και $y/(x^2-dy^2)$ είναι ακέραιοι. Συμπέρασμα:

> Το $\epsilon = x+y\sqrt{d}$ είναι μονάδα, αν και μόνο αν (x,y) είναι ακέραια λύση (u,v) της εξίσωσης
> $$u^2-dv^2=\pm 1. \tag{1.1}$$

Η (1.1) λέγεται εξίσωση του Pell και γι' αυτήν ισχύουν τα εξής:

• Με το $+1$ στο δεξιό μέλος, η εξίσωση (1.1) έχει πάντοτε λύση· η λύση με το ελάχιστο θετικό u, άρα και με το ελάχιστο θετικό v, χαρακτηρίζεται *θεμελιώδης λύση* και συμβολίζεται (u_1,v_1).[1] Είναι γνωστό από τη Θεωρία Αριθμών ότι όλες οι λύσεις της (1.1) με $+1$ στο δεξιό μέλος, είναι οι (u_n,v_n), όπου

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

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

• Με το -1 στο δεξιό μέλος, η εξίσωση (1.1) δεν έχει πάντοτε λύση· στην περίπτωση που έχει, η λύση με το ελάχιστο θετικό u (άρα και το ελάχιστο θετικό v) χαρακτηρίζεται θεμελιώδης και συμβολίζεται με (u_1',v_1'). Από τη Θεωρία Αριθμών είναι γνωστό ότι όλες οι λύσεις της (1.1) με -1 στο δεξιό μέλος, είναι οι (u'_{2k+1},v'_{2k+1}), ενώ όλες οι λύσεις της (1.1) με $+1$ στο δεξιό μέλος, είναι οι (u'_{2k},v'_{2k}), όπου, και στις δύο περιπτώσεις,

$$u_n'+v_n'\sqrt{d}=\pm(u_1'+v_1'\sqrt{d})^n, \quad n\in\mathbb{Z}. \tag{1.3}$$

Ειδικότερα, αυτό μας λέει ότι, στην περίπτωση που η εξίσωση (1.1), με -1 στο δεξιό μέλος, έχει λύση, οι λύσεις της (u_n',v_n') συνδέονται με τις λύσεις (u_n,v_n) της εξίσωσης (1.1), με $+1$ στο δεξιό μέλος, μέσω της σχέσεως $(u_n,v_n)=(u'_{2n},v'_{2n})$.

(δ') Θεωρούμε την ακέραια περιοχή $\mathbb{Z}[\sqrt{d}]$ όπως στο (γ') για αρνητικό ακέραιο d. Ακριβώς όπως στο (γ') καταλήγομε στο συμπέρασμα ότι το $\epsilon=x+y\sqrt{d}\in\mathbb{Z}[\sqrt{d}]$ είναι μονάδα, αν και μόνο αν $x^2-dy^2=1$. Τώρα, όμως, οι αριθμοί x^2 και $-dy^2$ είναι *θετικοί* ακέραιοι και, μάλιστα, $-dy^2\geq 2$, αν $d\leq -2$ και $y\neq 0$. Αναγκαστικά, λοιπόν, σ' αυτή την περίπτωση, $y=0$ και $x=\pm 1$. Αν $d=-1$, τότε βλέπομε ότι η $x^2-dy^2=1$ γίνεται $x^2+y^2=1$ και, συνεπώς, οι μοναδικές λύσεις είναι οι $(x,y)=(\pm 1,0),(0,\pm 1)$.

Συμπέρασμα: Οι μοναδικές μονάδες της ακέραιας περιοχής $\mathbb{Z}[\sqrt{d}]$ είναι οι ± 1, αν $d\leq -2$, και οι ± 1, $\pm\sqrt{-1}$, αν $d=-1$.

(ε') Έστω η ακέραια περιοχή $D=\mathbb{Z}[\sqrt{-5}]$. Σκοπός του παραδείγματος αυτού είναι να καταδείξει ότι, στη D, το 2 είναι ανάγωγο στοιχείο, αλλά δεν είναι πρώτο. Κατ' αρχάς, παρατηρούμε ότι, σύμφωνα με το (δ'), οι μόνες μονάδες της D είναι ± 1.

[1] Η θεμελιώδης λύση, για κάποιες τιμές του d να είναι εντυπωσιακά μεγάλη! Λ.χ. για $d=1141$, είναι $u_1=10367823941572239632371252 15$ και $v_1=30693385322765657197397208$.

Δείχνομε τώρα ότι το 2 είναι ανάγωγο στοιχείο της D. Πράγματι, έστω ότι $\delta = a + b\sqrt{-5} \in D$ είναι διαιρέτης του 2, οπότε υπάρχει $c + d\sqrt{-5} \in D$ έτσι ώστε $2 = (a + b\sqrt{-5})(c + d\sqrt{-5})$. Αν δούμε αυτή τη σχέση ως ισότητα στους μιγαδικούς αριθμούς, τότε μπορούμε να έχομε και τη συζυγή της σχέση, δηλαδή, την $2 = (a - b\sqrt{-5})(c - d\sqrt{-5})$. Πολλαπλασιάζοντας κατά μέλη τις δύο σχέσεις παίρνομε $4 = (a^2 + 5b^2)(c^2 + 5d^2)$. Οι παράγοντες του δεξιού μέλους είναι θετικοί ακέραιοι, που το γινόμενό τους είναι 4. Άρα, $a^2 + 5b^2 = 1$, ή 2, ή 4. Το δεύτερο ενδεχόμενο προφανώς αποκλείεται. Το πρώτο ενδεχόμενο μπορεί να συμβεί μόνον αν $b = 0$ και $a = \pm 1$, που σημαίνει ότι $\delta = \pm 1$, μονάδα. Το τρίτο ενδεχόμενο συνεπάγεται ότι $c^2 + 5d^2 = 1$, άρα, $d = 0$ και $c = \pm 1$. Αλλά τότε, $2 = \pm(a + b\sqrt{-5})$, που συνεπάγεται $b = 0$ και $a = \pm 2$, δηλαδή, $\delta = \pm 2$. Συνεπώς, οι μόνοι διαιρέτες του 2 είναι οι μονάδες και τα συνεταιρικά του 2 και, εξ ορισμού, αυτό σημαίνει ότι το 2 είναι ανάγωγο.

Τώρα θα δείξομε ότι το 2 δεν είναι πρώτο. Πράγματι, ξεκινούμε από την παρατήρηση ότι το 2 διαιρεί το γινόμενο $(1 + \sqrt{-5})(1 - \sqrt{-5})$, διότι το γινόμενο αυτό ισούται με 6. Αν το 2 ήταν πρώτο στοιχείο, θα έπρεπε να διαιρεί έναν από τους παράγοντες του γινομένου. Έστω π.χ. ότι $2|1 + \sqrt{-5}$. Αυτό σημαίνει ότι υπάρχει $a + b\sqrt{-5} \in D$ ώστε να ισχύει $1 + \sqrt{-5} = 2(a + b\sqrt{-5})$. Βλέποντας την τελευταία σχέση ως ισότητα μιγαδικών, συμπεραίνομε ότι $1 = 2a$ και $1 = 2b$, άτοπο, αφού οι a, b είναι ακέραιοι.

Άσκηση 1.8 Εργαστείτε όπως στο προηγούμενο παράδειγμα (ε') και αποδείξτε ότι τα στοιχεία 3 και $1 \pm \sqrt{-5}$ της ακέραιας περιοχής $D = \mathbb{Z}[\sqrt{-5}]$ είναι ανάγωγα.

Άσκηση 1.9 Έστω ακέραια περιοχή D και p ανάγωγο στοιχείο της. Αποδείξτε ότι το p είναι ανάγωγο στοιχείο και της περιοχής $D[X]$.

Ορισμός. Μία ακέραια περιοχή D χαρακτηρίζεται *περιοχή ανάλυσης* (σέ ανάγωγα στοιχεία) αν κάθε μη μηδενικό στοιχείο της, που δεν είναι μονάδα, μπορεί να γραφεί ως γινόμενο πεπερασμένου πλήθους ανάγωγων στοιχείων της D. Η περιοχή ανάλυσης D λέγεται *περιοχή μονοσήμαντης ανάλυσης*, αν η προαναφερθείσα ανάλυση μπορεί να γίνει, «ουσιαστικά» με ένα μόνο τρόπο. Το επίρρημα «ουσιαστικά» λέγεται εδώ υπό την εξής έννοια: Αν το μη μηδενικό στοιχείο a δεν είναι μονάδα και $a = p_1 \cdots p_n$, $a = q_1 \cdots q_m$ είναι δύο αναλύσεις του a σε ανάγωγα στοιχεία της D, τότε, υποχρεωτικά, $n = m$ και υπάρχει μιά μετάθεση $\begin{pmatrix} 1 & 2 & \dots & n \\ i_1 & i_2 & \dots & i_n \end{pmatrix}$, τέτοια ώστε το q_1 να είναι συνεταιρικό με το p_{i_1}, το q_2 να είναι συνεταιρικό με το p_{i_2}, ..., το q_n να είναι συνεταιρικό με το p_{i_n}.

Άσκηση 1.10 Έστω η ακέραια περιοχή $\mathbb{Z}[\sqrt{-5}]$ του παραδείγματος (ε'), πιό πάνω.
(α') Ν' αποδειχθεί ότι $D^* = \{-1, 1\}$.
(β') Ν' αποδειχθεί ότι η D είναι περιοχή ανάλυσης.
(γ') Σύμφωνα με το παράδειγμα (ε') και την άσκηση 1.8, τα στοιχεία $2, 3, 1 + \sqrt{-5}, 1 - \sqrt{-5}$ της D είναι ανάγωγα. Προφανώς, $2 \cdot 3 = (1 + \sqrt{-5}) \cdot (1 - \sqrt{-5})$.

Αποδείξτε ότι το 2 δεν είναι συνεταιρικό με κανέναν από τους δύο παράγοντες του δεξιού μέλους· ανάλογα και για το 3. Συμπεράνατε από αυτό ότι η D δεν είναι περιοχή μονοσήμαντης ανάλυσης.

> **Σημαντική παρατήρηση**. Από το εισαγωγικό μάθημα της Άλγεβρας ξέρομε ότι ο δακτύλιος $\mathbb{Z}$ είναι περιοχή μονοσήμαντης ανάλυσης, καθώς επίσης και ότι, αν το K είναι σώμα, τότε ο δακτύλιος πολυωνύμων $K[X]$ είναι και αυτός περιοχή μονοσήμαντης ανάλυσης.

Το γεγονός ότι, και στο $\mathbb{Z}$ και στο $K[X]$ όλα τα ιδεώδη είναι κύρια, δηλαδή, $\mathbb{Z}$ και $K[X]$ είναι *περιοχές κυρίων ιδεωδών* δεν είναι τυχαίο, καθώς θα δούμε λίγο αργότερα.

Πρόταση 1.2 *Αν η D είναι περιοχή ανάλυσης, στην οποία κάθε ανάγωγο στοιχείο είναι πρώτο, τότε η D είναι περιοχή μονοσήμαντης ανάλυσης.*

Απόδειξη. Αυτό που αρκεί ν' αποδείξομε είναι τον εξής ισχυρισμό: *Αν έχομε μια σχέση της μορφής $\prod_{i=1}^{n} p_i = \prod_{i=1}^{m} q_i$, στην οποία όλοι οι παράγοντες, και στα δύο μέλη, είναι ανάγωγα στοιχεία και $n \leq m$, τότε $m = n$ και σε κάθε $\nu = 1, \dots, n$ αντιστοιχεί μονοσημάντως ένα $i_\nu \in \{1, \dots, n\}$, έτσι ώστε τα p_ν και q_{i_ν} να είναι συνεταιρικά.*
Η απόδειξη θα γίνει με επαγωγή στο n. Έστω $n = 1$, οπότε έχομε τη σχέση $p_1 = \prod_{i=1}^{m} q_i$. Το p_1 είναι πρώτο, αφού έχει υποτεθεί ότι κάθε ανάγωγο στοιχείο είναι πρώτο, και διαιρεί το γινόμενο των $q_1, \dots, q_m$, άρα διαιρεί ένα εξ αυτών· ας πούμε ότι $p_1 | q_{i_1}$, όπου i_1 είναι κάποιος δείκτης μεταξύ 1 και m. Όμως, καθώς το q_{i_1} είναι ανάγωγο στοιχείο, δεν έχει διαιρέτες άλλους από τα συνεταιρικά του και τις μονάδες. Το p_1 δεν είναι μονάδα (αφού είναι ανάγωγο), άρα, αναγκαστικά, το p_1 είναι συνεταιρικό του q_{i_1}, δηλαδή, $p_1 = \epsilon q_{i_1}$, όπου ϵ είναι μονάδα της D. Οδηγούμαστε, λοιπόν, στη σχέση $\epsilon q_{i_1} = \prod_{i=1}^{m} q_i$, όπου, βέβαια, το q_{i_1} είναι ένας απ' τους παράγοντες στο δεξιό μέλος, άρα μπορούμε να διαγράψομε το q_{i_1} από τα δύο μέλη και να καταλήξομε στη σχέση $\epsilon =$ (γινόμενο των q_i με $i \neq i_1$). Η σχέση αυτή είναι δυνατή μόνον αν δεν υπάρχουν q_i στο δεξιό μέλος, διότι δεν είναι δυνατόν γινόμενο αναγώγων στοιχείων να ισούται με μονάδα. Άρα, αναγκαστικά, $m = 1$ και η τελευταία σχέση είναι, στην πραγματικότητα, η $\epsilon = 1$.
Ας υποθέσομε ότι ο ισχυρισμός ισχύει για $n = k - 1 \geq 1$ και ας θεωρήσομε μια σχέση $\prod_{i=1}^{k} p_i = \prod_{i=1}^{m} q_i$, στην οποία όλοι οι παράγοντες, και στα δύο μέλη, είναι ανάγωγα στοιχεία και $k \leq m$. Ακριβώς όπως στην περίπτωση $n = 1$, αποδεικνύομε ότι το p_k είναι συνεταιρικό με κάποιο από τα $q_1, \dots, q_m$, έστω με το q_{i_k}. Θέτοντας $p_k = \epsilon q_{i_k}$, όπου ϵ είναι μονάδα, και διαγράφοντας το q_{i_k} από τα δύο μέλη της σχέσης $\prod_{i=1}^{k} p_i = \prod_{i=1}^{m} q_i$, παίρνομε τη σχέση $\epsilon \prod_{i=1}^{k-1} p_i = \prod_{i_k \neq i=1}^{m} q_i$. Το αριστερό μέλος μπορούμε να το γράψομε, επίσης, με τη μορφή $(\epsilon p_1) p_2 \cdots p_{k-1}$, άρα ως γινόμενο $k-1$ το πλήθος ανάγωγων στοιχείων, ενώ το αριστερό μέλος είναι γινόμενο $m - 1$ το πλήθος ανάγωγων στοιχείων. Από την επαγωγική υπόθεση, σε κάθε $\nu = 1, \dots, k -$

1 αντιστοιχεί ένα διαφορετικό $i_\nu \in \{1,\dots,m\} \setminus \{i_k\}$, έτσι ώστε το q_{i_1} να είναι συνεταιρικό με το ϵp_1 (άρα συνεταιρικό και με το p_1), το q_{i_2} να είναι συνεταιρικό με το p_2,..., το $q_{i_{k-1}}$ να είναι συνεταιρικό με το p_{k-1}. Αυτό ολοκληρώνει την επαγωγική απόδειξη.

□

1.2 Μεγιστος Κοινος Διαιρετης

Ορισμός. Έστω D ακέραια περιοχή και $a_1,\dots,a_n \in D$ $(n \geq 2)$ όχι όλα μηδέν. Το $d \in D$ λέγεται *μέγιστος κοινός διαιρέτης των* $a_1,\dots,a_n$ αν ικανοποιεί τις εξής δύο ιδιότητες:

(α') Ο d είναι κοινός διαιρέτης των $a_1,\dots,a_n$, δηλαδή, ο d διαιρεί καθένα από αυτά τα στοιχεία.

(β') Ο d διαιρείται από κάθε άλλον κοινό διαιρέτη των $a_1,\dots,a_n$, δηλαδή, αν ο $d' \in D$ διαιρεί όλα τα $a_1,\dots,a_n$, τότε $d'|d$.

Γράφομε, συμβολικά, $d = \text{ΜΚΔ}(a_1,\dots,a_n)$ για να δηλώσομε ότι ο d είναι μέγιστος κοινός διαιρέτης των $a_1,\dots,a_n$. Όπως θα δούμε στην παρακάτω Πρόταση 1.2.1, το σύμβολο $\text{ΜΚΔ}(a_1,\dots,a_n)$ δεν είναι μονοσήμαντα ορισμένο, δηλαδή, αν $d_1 = \text{ΜΚΔ}(a_1,\dots,a_n)$ και $d_2 = \text{ΜΚΔ}(a_1,\dots,a_n)$, αυτό δεν σημαίνει ότι $d_1 = d_2$, αλλά ότι τα d_1, d_2 είναι συνεταιρικά.

Αν τα $a_1,\dots,a_n \in D$ δεν είναι όλα μηδέν και το μοναδιαίο στοιχείο της D είναι μέγιστος κοινός διαιρέτης τους, τότε τα $a_1,\dots,a_n$ χαρακτηρίζονται *πρώτα μεταξύ τους*, συμβολικά, $\text{ΜΚΔ}(a_1,\dots,a_n) = 1$. Στην περίπτωση που $n = 2$, η δήλωση «τά a_1, a_2 είναι πρώτα μεταξύ τους» διατυπώνεται ισοδύναμα και ως εξής: «Τό a_1 είναι πρώτο προς το a_2», ή «τό a_2 είναι πρώτο προς το a_1».

Άσκηση 1.11 (α') Αποδείξτε ότι $1 = \text{ΜΚΔ}(a_1,\dots,a_n)$ αν και μόνο αν οι μόνοι κοινοί διαιρέτες των $a_1,\dots,a_n$ είναι οι μονάδες.
(β') Αποδείξτε ότι, αν $d = \text{ΜΚΔ}(a_1,\dots,a_n)$ και θέσομε $a_i = db_i$ για κάθε $i = 1,\dots,n$, τότε τα $b_1,\dots,b_n$ είναι πρώτα μεταξύ τους.

Πρόταση 1.3 *Έστω ότι τα* $a_1,\dots,a_n \in D$ *δεν είναι όλα μηδενικά και* d_1, d_2 *είναι μέγιστοι κοινοί διαιρέτες των* $a_1,\dots,a_n$. *Τότε τα* d_1, d_2 *είναι συνεταιρικά στοιχεία. Με πιό συμβολική διατύπωση: Αν* $d_1 = \text{ΜΚΔ}(a_1,\dots,a_n)$ *και* $d_2 = \text{ΜΚΔ}(a_1,\dots,a_n)$, *τότε* $d_2 = \epsilon d_1$, *όπου* ϵ *είναι μονάδα της* D.

Απόδειξη. Ο d_1, ως ΜΚΔ των $a_1,\dots,a_n$, διαιρείται από κάθε κοινό διαιρέτη των $a_1,\dots,a_n$, άρα διαιρείται και από τον d_2. Με ανάλογο επιχείρημα, εναλλάσσοντας τους ρόλους των d_1, d_2, συμπεραίνομε ότι ο d_2 διαιρείται από τον d_1. Έτσι, $d_2|d_1$ και $d_1|d_2$, οπότε, εφαρμόζοντας την άσκηση 1.5, καταλήγομε στο συμπέρασμα ότι τα στοιχεία d_1, d_2 είναι συνεταιρικά.

□

Άσκηση 1.12 Έστω η ακέραια περιοχή $D = \mathbb{Z}[\sqrt{-2}] = \{a + b\sqrt{-2} : a, b \in \mathbb{Z}\}$. Αποδείξτε τα εξής:

(α') $D^* = \{-1, 1\}$.

(β') Το στοιχείο $\sqrt{-2}$ της D είναι ανάγωγο.

Έστω τώρα ότι οι μη μηδενικοί $x, y \in \mathbb{Z}$ ικανοποιούν την εξίσωση $x^2 + 2 = y^3$. Αποδείξτε τα εξής:

(γ') Ο x είναι περιττός και πρώτος προς τον y (στό $\mathbb{Z}$).

(ε') Θεωρώντας δεδομένο ότι η D είναι περιοχή μονοσήμαντης ανάλυσης,[2] αποδείξτε ότι $1 = \text{ΜΚΔ}(x + \sqrt{-2}, x - \sqrt{-2})$.

1.3 Διαιρετοτητα σε περιοχες κυριων ιδεωδων

Δεν είναι βέβαιο ότι σε οποιαδήποτε ακέραια περιοχή, οποιαδήποτε στοιχεία της έχουν μέγιστο κοινό διαιρέτη! Αν, όμως, η ακέραια περιοχή έχει την ιδιότητα να είναι περιοχή κυρίων ιδεωδών, τότε η ύπαρξη ΜΚΔ είναι εξασφαλισμένη, όπως βλέπομε στο επόμενο θεώρημα.

Θεώρημα 1.4 *Αν η D είναι περιοχή κυρίων ιδεωδών, τότε, οποιοιαδήποτε στοιχεία $a_1, \dots, a_n$ της D, που δεν είναι όλα μηδέν, έχουν μέγιστο κοινό διαιρέτη. Ποιό συγκεκριμένα, αν $\langle a_1, \dots, a_n \rangle = \langle d \rangle$, τότε $d = \text{ΜΚΔ}(a_1, \dots, a_n)$ και, συνεπώς, κάθε μέγιστος κοινός διαιρέτης των $a_1, \dots, a_n$ γράφεται ως γραμμικός συνδυασμός των $a_1, \dots, a_n$ με συντελεστές από τη D.*

Απόδειξη. Εξ υποθέσεως, το $\langle a_1, \dots, a_n \rangle$ είναι μη μηδενικό κύριο ιδεώδες, άρα υπάρχει μη μηδενικό $d \in D$ με την ιδιότητα $\langle a_1, \dots, a_n \rangle = \langle d \rangle$, δηλαδή, έχομε τη σχέση

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

Προφανώς, το $d = d \cdot 1$ ανήκει στο δεξιό μέλος, άρα ανήκει και στο αριστερό. Αυτό, όμως, σημαίνει ότι υπάρχουν $t_1, \dots, t_n \in D$ ώστε να ισχύει η σχέση $d = t_1 a_1 + \cdots + t_n a_n$. Επίσης, κάθε a_i γράφεται $a_i = 0 \cdot a_1 + \cdots 0 \cdot a_{i-1} + 1 \cdot a_i + 0 \cdot a_{i+1} + \cdots 0 \cdot a_n$, άρα ανήκει στο αριστερό μέλος της (1.4), άρα ανήκει και στο δεξιό μέλος. Αυτό σημαίνει ότι υπάρχει $b_i \in D$ για το οποίο ισχύει $a_i = db_i$, δηλαδή, $d | a_i$. Έτσι βλέπομε ότι το d είναι κοινός διαιρέτης όλων των a_i. Μένει να δείξομε ότι, αν ο $d' \in D$ είναι ένας οποιοσδήποτε κοινός διαιρέτης όλων των a_i, τότε $d' | d$. Πράγματι, διότι τότε, το d' διαιρεί το δεξιό μέλος της σχέσης $d = t_1 a_1 + \cdots + t_n a_n$ (βλ. άσκηση1.2), άρα διαιρεί και το αριστερό μέλος, δηλαδή, το d.

□

Άσκηση 1.13 Έστω D περιοχή κυρίων ιδεωδών και $a_1, \dots, a_n, b \in D$. Αποδείξτε ότι, αν $d = \text{ΜΚΔ}(a_1, \dots, a_n)$, τότε $bd = \text{ΜΚΔ}(ba_1, \dots, ba_n)$.[3]

[2] Θά το αποδείξομε αργότερα· βλ. Παράδειγμα 3 στη σελίδα 27.

[3] Πρβλ. με άσκηση 1.20.

Θεώρημα 1.5 *Σε κάθε περιοχή κυρίων ιδεωδών D ισχύουν τα εξής:*

(α′) Αν το p είναι ανάγωγο, τότε, κάθε στοιχείο $a \in D$, είτε είναι πολλαπλάσιο του p, είτε είναι πρώτο προς το p.

(β′) Κάθε ανάγωγο στοιχείο είναι πρώτο. Συνεπώς, λόγω της Πρότασης 1.1.1*, οι έννοιες «ανάγωγο στοιχείο» και «πρώτο στοιχείο» συμπίπτουν.*

(γ′) Αν τα a, b είναι πρώτα μεταξύ τους, $a|c$ και $b|c$, τότε $ab|c$.

(δ′) Αν καθένα από τα a, b είναι πρώτο προς το c, τότε το ab είναι πρώτο προς το c.

Απόδειξη. (α') Θα υποθέσομε ότι το a δεν είναι πολλαπλάσιο του p και θ' αποδείξομε ότι τα a, p είναι πρώτα μεταξύ τους. Έστω $d = \text{ΜΚΔ}(a, p)$. Επειδή το p είναι ανάγωγο και $d \mid p$, έχομε δύο ενδεχόμενα: ή το d είναι μονάδα, οπότε έχομε τελειώσει, ή το d είναι συνεταιρικό του p. Θα δείξομε ότι το δεύτερο ενδεχόμενο είναι αδύνατο. Διότι, $d \mid a$ οπότε, αν το d είναι συνεταιρικό του p, τότε το $p \mid a$ (βλ. άσκηση 1.4), αντίθεση με την υπόθεσή μας ότι το a δεν διαιρείται από το p.

(β') Έστω $p \in D$ ανάγωγο στοιχείο και ας υποθέσομε ότι, για κάποια $a, b \in D$ έχομε ότι $p|ab$. Πρέπει και αρκεί ν' αποδείξομε ότι το p διαιρεί ένα, τουλάχιστον, από τα a, b. Πράγματι, αν υποθέσομε ότι το p δεν διαιρεί το a, τότε, από το (α') οδηγούμαστε στο συμπέρασμα ότι $\text{ΜΚΔ}(p, a) = 1$, οπότε, από το Θεώρημα 1.3.1, $1 = cp + da$ για κατάλληλα $c, d \in D$. Πολλαπλασιάζοντας επί b τα δύο μέλη παίρνομε τη σχέση $b = bcp + d(ab)$, το δεξιό μέλος της οποίας διαιρείται απ' το p (αφού έχομε υποθέσει ότι $p|ab$), άρα $p|b$.

(γ') Απ' το Θεώρημα 1.3.1 $1 = da + eb$ για κατάλληλα $d, e \in D$. Πολλαπλασιάζοντας επί c τα δύο μέλη παίρνομε τη σχέση $c = dac + ebc$. Από την υπόθεση $a|c$ συμπεραίνομε ότι $c = ac_1$, για κάποιο $c_1 \in D$ και, ανάλογα, $c = bc_2$, λόγω της $b|c$. Άρα, $c = dac + ebc = da(bc_2) + eb(ac_1) = ab(c_2 d + c_1 e)$, απ' όπου έπεται ότι $ab|c$.

(δ') Επειδή $\text{ΜΚΔ}(a, b) = 1$, το Θεώρημα 1.3.1 συνεπάγεται ότι υπάρχουν $x, y \in D$ ώστε να ισχύει $xa + yb = 1$. Πολλαπλασιάζοντας επί c παίρνομε τη σχέση $xac + ybc = c$. Εξ υποθέσεως $a \mid c$ και $b \mid c$, άρα $c = c_1 a$ και $c = c_2 b$ με τα $c_1, c_2 \in D$. Άρα $c = xac + ybc = xa(c_2 b) + yb(c_1 a) = ab(xc_2 + yc_1)$, απ' την οποία βλέπομε ότι $ab \mid c$.

□

Λήμμα 1.6 *Σε κάθε περιοχή κυρίων ιδεωδών D, κάθε αύξουσα ακολουθία ιδεωδών $I_1, I_2, \ldots$ είναι στάσιμη. Δηλαδή, για κάποιον δείκτη j_0 ισχύει $I_j = I_{j_0}$ για κάθε $j \geq j_0$.*

Απόδειξη. Είναι πολύ απλό ν' αποδειχτεί ότι το $I = \cup_{j=1}^{\infty} I_j$ είναι ιδεώδες της D (άσκηση 1.14). Κάθε ιδεώδες της D είναι κύριο, άρα $I = aD$ για κάποιο $a \in D$. Προφανώς, $a \in aD$, άρα $a \in I$, οπότε, για κάποιο j_0 έχομε $a \in I_{j_0}$. Συνεπώς, $a \in I_j$ για κάθε $j \geq j_0$, άρα $aD \subseteq I_j$. Αφετέρου $I_j \subseteq I = aD$, άρα $I_j = aD = I$. Συμπεράναμε, λοιπόν, ότι $I_j = I$ για κάθε $j \geq j_0$.

□

Άσκηση 1.14 Αποδείξτε τον ισχυρισμό με τον οποίο αρχίζει η απόδειξη του

Λήμματος 1.3.3.

Θεώρημα 1.7 *Κάθε περιοχή κυρίων ιδεωδών είναι περιοχή μονοσήμαντης ανάλυσης.*

Απόδειξη. Για $a \in D$ θα χρησιμοποιούμε τον (καθιερωμένο) συμβολισμό $\langle a\rangle$ για το κύριο ιδεώδες aD. Επίσης, το σύμβολο $\subset$ θα σημαίνει *γνήσιο* υποσύνολο. Επίσης, λέγοντας ότι ένα στοιχείο «αναλύεται» εννοούμε «αναλύεται σε γινόμενο πεπερασμένου πλήθους αναγώγων της D».

Πρώτα θ' αποδείξομε, με εις άτοπον απαγωγή, ότι η D είναι περιοχή ανάλυσης. Έστω ότι κάποιο $a \in D \setminus D^*$ δεν αναλύεται. Ειδικότερα, αυτό συνεπάγεται ότι δεν είναι ανάγωγο, οπότε μπορούμε να το γράψομε ως γινόμενο $a = a_1b_1$ με $a_1, b_1 \in D$, όχι μονάδες. Τότε (άσκηση 1.15)

$$\langle a\rangle \subset \langle a_1\rangle, \quad \langle d\rangle \subset \langle b_1\rangle.$$

Ένα τουλάχιστον από τα a_1, b_1 δεν αναλύεται (αν αναλυόταν και τα δύο, τότε θα αναλυόταν και το a), ας πούμε το a_1. Αυτό, ειδικότερα, συνεπάγεται ότι δεν είναι ανάγωγο, άρα $a_1 = a_2b_2$ με τα a_2, b_2 όχι μονάδες, οπότε

$$\langle a_1\rangle \subset \langle a_2\rangle, \quad \langle a_1\rangle \subset \langle b_2\rangle.$$

Ένα τουλάχιστον από τα a_2, b_2 δεν αναλύεται (αν αναλυόταν και τα δύο, τότε θα αναλυόταν και το a_1), ας πούμε το a_2. Αυτό, ειδικότερα, συνεπάγεται ότι δεν είναι ανάγωγο, άρα $a_2 = a_3b_3$ με τα a_3, b_3 όχι μονάδες, οπότε

$$\langle a_2\rangle \subset \langle a_3\rangle, \quad \langle a_2\rangle \subset \langle b_3\rangle.$$

Έτσι δημιουργείται μια άπειρη ακολουθία

$$\langle a\rangle \subset \langle a_1\rangle \subset \langle a_2\rangle \subset \langle a_3\rangle \subset \cdots$$

γνησίως αύξουσα, συμπέρασμα που αντιβαίνει στο Λήμμα 1.3.3. Στο άτοπο οδηγηθήκαμε επειδή υποθέσαμε ότι το a δεν αναλύεται.

Τώρα που ξέρομε ότι η D είναι περιοχή ανάλυσης μπορούμε αμέσως να συμπεράνομε ότι είναι περιοχή *μονοσήμαντης* ανάλυσης, με άμεση εφαρμογή της Πρότασης 1.1.2 και του Θεωρήματος 1.3.2 (β').

□

Άσκηση 1.15 Έστω ότι a, b, d είναι στοιχεία της ακέραιας περιοχής D, τα a, b δεν είναι μονάδες και $d = ab$. Αποδείξτε ότι $\langle d\rangle \subset \langle a\rangle$ και $\langle d\rangle \subset \langle b\rangle$, όπου $\subset$ σημαίνει *γνήσιο* υποσύνολο.

Παράδειγμα 1.1 Ακέραια περιοχή, που δεν είναι σώμα και δεν έχει κανένα ανάγωγο στοιχείο.

Έστω $\bar{\mathbb{Z}} = \{c \in \mathbb{C} : c$ είναι ρίζα μονικού$f(X) \in \mathbb{Z}[X]\}$[4].

Π.χ., για κάθε $c \in \mathbb{Z}$ και κάθε ακέραιο $n \geq 2$, οποιαδήποτε n-οστή μιγαδική ρίζα του c ανήκει στο $\bar{\mathbb{Z}}$ διότι είναι ρίζα του $X^n - c$. Προφανώς, $\mathbb{Z} \subset \bar{\mathbb{Z}}$. Τα στοιχεία του $\bar{\mathbb{Z}}$ λέγονται αλγεβρικοί *ακέραιοι*. Αντιθέτως, ο αριθμός $\sqrt{3/5}$ δεν είναι αλγεβρικός ακέραιος γιατί είναι ρίζα του $5X^2 - 3$, που δεν είναι μονικό. Επίσης, το $\bar{\mathbb{Z}}$ περιέχει στοιχεία που δεν είναι μονάδες, για παράδειγμα $\sqrt[n]{c}$ για κάθε ζευγάρι ακεραίων $c, n \geq 2$, αφού το αντίστροφο ενός τέτοιου στοιχείου είναι ρίζα του $cX^n - 1$, που δεν είναι μονικό. Αποδεικνύεται[5] ότι το $\bar{\mathbb{Z}}$ είναι υποδακτύλιος του $\mathbb{C}$, επομένως, ακέραια περιοχή.

Τώρα θα δείξομε ότι κανένα στοιχείο του $\bar{Z}$ δεν είναι ανάγωγο. Έστω $c \in \bar{\mathbb{Z}}$ όχι μονάδα και $f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_2X^2 + a_1X + a_0 \in \mathbb{Z}[X]$ του οποίου ρίζα είναι το c. Τότε, για το $\sqrt{c}$ (οποιαδήποτε από τις δύο μιγαδικές ρίζες του c) ισχύει $(\sqrt{c})^{2n} + a_{n-1}(\sqrt{c})^{2(n-1)} + \cdots + a_2(\sqrt{c})^2 + a_1(\sqrt{c}) + a_0 = 0$, άρα $\sqrt{c} \in \bar{\mathbb{Z}}$. Όμως, $c = \sqrt{c} \cdot \sqrt{c}$, σχέση που μας δείχνει δύο πράγματα: πρώτον, ότι το $\sqrt{c}$ δεν είναι μονάδα (αν ήταν, τότε θα ήταν μονάδα και το c) και δεύτερον, ότι το c δεν είναι ανάγωγο, αφού είναι γινόμενο δύο μονάδων του $\bar{\mathbb{Z}}$, τα οποία δεν είναι μονάδες.

Άσκηση 1.16 Αναφερόμενοι στο παράδειγμα 1.1, δώστε αριθμητικό παράδειγμα μονάδας της $\bar{\mathbb{Z}}$, διαφορετικής από ± 1.

Χάρη στα Θεωρήματα 1.3.2 και 1.3.4 μπορούμε να μεταφέρομε όλη, ουσιαστικά, τη θεωρία διαιρετότητας των ακεραίων σε κάθε περιοχή ανάλυσης, η οποία είναι συγχρόνως και περιοχή κυρίων ιδεωδών. Η απόδειξη του Θεωρήματος 1.3.2 στηρίζεται στην ύπαρξη μεγίστου κοινού διαιρέτη για οποιαδήποτε στοιχεία $a_1, \ldots, a_n$ της θεωρούμενης περιοχής, καθώς επίσης και στη δυνατότητα γραφής αυτού του μεγίστου κοινού διαιρέτη ως γραμμικού συνδυασμού των $a_1, \ldots, a_n$. Οι ιδιότητες αυτές, με τη σειρά τους, στηρίζονται κατά ουσιαστικό τρόπο στο ότι κάθε ιδεώδες της θεωρούμενης ακέραιας περιοχής είναι κύριο. Το γεγονός αυτό μπορεί να κάνει κάποιον να εικάσει ότι, σε περιοχές, στις οποίες δεν είναι όλα τα ιδεώδη κύρια, δεν είναι δυνατή η δημιουργία μιάς ικανοποιητικής θεωρίας διαιρετότητας. Για τις ακέραιες περιοχές εν γένει, ακόμη και για τις περιοχές ανάλυσης, δίχως επιπλέον υποθέσεις, η εικασία είναι σωστή. Στις περιοχές μονοσήμαντης ανάλυσης, όμως, μια πολύ ικανοποιητική θεωρία διαιρετότητας, εντελώς ανάλογη με αυτήν των ακεραίων, μπορεί να δομηθεί. Τέτοιες περιοχές μονοσήμαντης ανάλυσης, οι οποίες δεν είναι περιοχές κυρίων ιδεωδών υπάρχουν (θά συναντήσομε αργότερα) και είναι πολύ σημαντικές στα Μαθηματικά. Για τον λόγο αυτό έχει σημασία να φτιάξομε και γι' αυτές μιά θεωρία διαιρετότητας.

[4] Μέ τον όρο *μονικό πολυώνυμο* εννοούμε πολυώνυμο με συντελεστή μεγιστοβαθμίου όρου το 1.

[5] Η απόδειξη υπερβαίνει τους στόχους αυτού του μαθήματος.

1.4 Διαιρετοτητα σε περιοχες μονοσημαντης αναλυσης

Πρόταση 1.8 *Σε κάθε περιοχή μονοσήμαντης ανάλυσης, τα ανάγωγα στοιχεία είναι πρώτα στοιχεία. Συνεπώς, λόγω της* Πρότασης 1.1.1, *οι έννοιες «ανάγωγο στοιχείο» και «πρώτο στοιχείο» συμπίπτουν, στις περιοχές μονοσήμαντης ανάλυσης. (Πρβλ. Θεώρημα 1.3.2 (β′).)*

Απόδειξη. Έστω D περιοχή μονοσήμαντης ανάλυσης, $p \in D$ ανάγωγο, $a, b \in D$ και $p|ab$. Πρέπει και αρκεί να δείξομε ότι το p διαιρεί ένα τουλάχιστον από τα a, b. Από την υπόθεση συμπεραίνομε ότι υπάρχει $c \in D$, έτσι ώστε $ab = pc$. Έστω ότι η ανάλυση των a, b, c σε ανάγωγα στοιχεία της D είναι: $a = p_1 \cdots p_\ell$, $b = q_1 \cdots q_m$, $c = r_1 \cdots r_n$, οπότε η σχέση $ab = pc$ γίνεται

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

άρα έχομε δύο αναλύσεις του ab σε ανάγωγα. Όμως, στη D ισχύει η μονοσήμαντη ανάλυση. Άρα, αφού το ανάγωγο p εμφανίζεται στο δεξιό μέλος, πρέπει στο αριστερό μέλος κάποιο από τα ανάγωγα στοιχεία να είναι συνεταιρικό (δέν αποκλείεται να είναι ίσο) με το p. Δηλαδή, το p είναι συνεταιρικό, ή με κάποιο από τα $p_1, \dots, p_\ell$, ή με κάποιο από τα $q_1, \dots, q_m$. Στην πρώτη περίπτωση το p διαιρεί το a, ενώ στη δεύτερη διαιρεί το b.

□

> Από τώρα και μέχρι το τέλος της ενότητας 1.4, D θα είναι περιοχή μονοσήμαντης ανάλυσης.

Ορισμός. Το $\mathcal{P} \subset D$ λέγεται *πλήρες σύστημα πρώτων (= αναγώγων) στοιχείων της D* άν:

(α') Κάθε ανάγωγο στοιχείο της D είναι συνεταιρικό με κάποιο στοιχείο του $\mathcal{P}$ και (β').

(β') Ανά δύο τα στοιχεία του $\mathcal{P}$ *δέν* είναι συνεταιρικά.

Έστω ότι $a \in D \setminus D^*$, $a \neq 0$ και αναλύομε το a σε ανάγωγα στοιχεία: $a = q_1 \cdots q_n$. Εξ ορισμού του $\mathcal{P}$, καθένα από τα $q_1, \dots, q_n$ είναι συνεταιρικό με κάποιο $p_i \in \mathcal{P}$, δηλαδή, για κάθε $i = 1, \dots, n$ υπάρχει $p_i \in \mathcal{P}$ και $\epsilon_i \in D^*$, τέτοια ώστε $q_i = \epsilon_i p_i$. Προσέξτε, όμως, ότι δεν είναι απαραίτητο σε διαφορετικά q_i ν' αντιστοιχούν διαφορετικά p_i, δηλαδή, δεν αποκλείεται να είναι $i \neq j$ και $p_i = p_j$· αυτό θα συμβεί αν τα q_i, q_j είναι συνεταιρικά. Άρα,

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

Αν στην παραπάνω σχέση ομαδοποιήσομε τα ίσα μεταξύ τους p_i, τότε βλέπομε ότι το a γράφεται ως γινόμενο της μονάδας ϵ_a και δυνάμεων *διαφορετικών* στοιχείων $p \in \mathcal{P}$. Εφόσον το $p \in \mathcal{P}$ εμφανίζεται στην ανάλυση (1.5), ο εκθέτης του, τον οποίον στο εξής θα συμβολίζομε με $v_p(a)$, είναι θετικός και, ενδεχομένως, μεγαλύτερος

του 1. Για λόγους ομοιομορφίας, αν ο $p \in \mathcal{P}$ δεν εμφανίζεται στην ανάλυση (1.5), τότε θέτομε $v_p(a) = 0$, οπότε μπορούμε να γράψομε την ανάλυση του a ως εξής:

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

όπου οι ακέραιοι εκθέτες $v_p(a)$ είναι "σχεδόν όλοι" μηδέν (δηλαδή, πεπερασμένοι το πλήθος εκθέτες $v_p(a)$ είναι γνησίως θετικοί). Ο $v_p(a)$ καλείται *εκθέτης του p στο a*.

Η ανάλυση (1.6) λέγεται *κανονική ανάλυση του a* σε πρώτα (= ανάγωγα) στοιχεία και είναι μονοσήμαντα ορισμένη, αν παραβλέψομε τη σειρά με την οποίαν είναι γραμμένοι οι παράγοντες.

Προφανώς για κάθε μονάδα ϵ είναι $v_p(\epsilon) = 0 \ \ \forall p \in \mathcal{P}$. Για το $0 \in D$ θέτομε $v_p(0) = \infty$ για κάθε $p \in \mathcal{P}$ και κάνομε τη σύμβαση $\infty + n = \infty$ για κάθε ακέραιο n.

Παραδείγματα: Αν $D = \mathbb{Z}$, τότε η "φυσιολογικότερη" επιλογή για το $\mathcal{P}$ είναι είναι το σύνολο των (θετικών) πρώτων αριθμών. Εξίσου "νόμιμο", όμως, είναι να επιλέξομε ως $\mathcal{P}$ το σύνολο $\{-p : p \text{ πρώτος}\}$ ή $\mathcal{P} = \{-2, -3\} \cup \{p : p \text{ πρώτος} \geq 5\}$. Αν $D = K[X]$, όπου το K είναι σώμα, τότε μια "φυσιολογική" επιλογή για το $\mathcal{P}$ είναι το σύνολο των αναγώγων μονικών πολυωνύμων του $K[X]$.

Άσκηση 1.17 Στην περιοχή $D = \mathbb{Z}$, με $\mathcal{P}$ το σύνολο των (θετικών) πρώτων, υπολογίστε τους (άπειρους) εκθέτες $v_p(a)$ για $a \in \{52, -106, 720, 101, -103\}$.

Άσκηση 1.18 Έστω $D = \mathbb{Z}$ και $\mathcal{P}$ το σύνολο των (θετικών) πρώτων. Με στοιχειώδη Θεωρία Αριθμών αποδεικνύεται ότι, για κάθε $n > 1$ και κάθε πρώτο p ισχύει $v_p(n!) = \sum_{k=1}^{\infty} \left[\frac{n}{p^k}\right]$, όπου $[x]$ συμβολίζει το ακέραιο μέρος του x. Εξηγήστε γιατί το άπειρο άθροισμα στο δεξιό μέλος έχει πεπερασμένο πλήθος μη μηδενικών προσθετέων και είναι $< 1/(p-1)$. Υπολογίστε τους εκθέτες $v_p(30!)$ για κάθε $p \in \mathcal{P}$.

Θεώρημα 1.9 *Έστω D περιοχή μονοσήμαντης ανάλυσης, $\mathcal{P}$ ένα πλήρες σύστημα πρώτων της D και $a, b \in D$ με $b \neq 0$. Τότε, $b|a \Leftrightarrow v_p(b) \leq v_p(a) \ \ \forall p \in \mathcal{P}$.*

Απόδειξη. Ας θεωρήσομε τις κανονικές αναλύσεις $a = \epsilon_a \prod_{p \in \mathcal{P}} p^{v_p(a)}$, $b = \epsilon_b \prod_{p \in \mathcal{P}} p^{v_p(b)}$ $(\epsilon_a, \epsilon_b \in D^*)$.

$(\Rightarrow)$ Έστω ότι $b|a$, οπότε υπάρχει $c \in D$ τέτοιο ώστε $a = bc$. Αν θεωρήσομε την κανονική ανάλυση $c = \epsilon_c \prod_{p \in \mathcal{P}} p^{v_p(c)}$ $(\epsilon_c \in D^*)$, τότε η σχέση $a = bc$ συνεπάγεται τη σχέση

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

Επειδή ισχύει η μονοσήμαντη ανάλυση σε πρώτα στοιχεία, η παραπάνω σχέση μας οδηγεί στο συμπέρασμα ότι, για κάθε $p \in \mathcal{P}$ ισχύει $v_p(a) = v_p(b) + v_p(c) \geq v_p(b)$.

($\Leftarrow$) Αντιστρόφως, έστω ότι $v_p(a) \geq v_p(b)$ για κάθε $p \in \mathcal{P}$. Τότε, $n_p \stackrel{\text{def}}{=} v_p(a) - v_p(b) \geq 0$ για κάθε $p \in \mathcal{P}$ και $n_p = 0$ για σχεδόν όλα τα p. Άρα μπορούμε να θεωρήσομε το στοιχείο $c \stackrel{\text{def}}{=} \epsilon_a \epsilon_b^{-1} \prod_{p\in\mathcal{P}} p^{n_p} \in D$ και, προφανώς, ισχύει $bc = a$, που σημαίνει ότι $b|a$.

□

Παρατήρηση. Κατά την απόδειξη του Θεωρήματος 1.4.2 δείξαμε ότι, αν $a = bc$, τότε $v_p(a) = v_p(b) + v_p(c) \ \ \forall p \in \mathcal{P}$.

Άσκηση 1.19 Έστω D και $\mathcal{P}$ όπως στο Θεώρημα 1.4.2.
(α') Αποδείξτε ότι ένα στοιχείο $p \in \mathcal{P}$ διαιρεί ένα στοιχείο a αν και μόνο αν, $v_p(a) > 0$.
(β') Αποδείξτε ότι, αν τα στοιχεία $a, b \in D$ είναι πρώτα μεταξύ τους, τότε, για κάθε $p \in \mathcal{P}$, ένα, το πολύ, από τα $v_p(a), v_p(b)$ είναι διάφορο του μηδενός. Αλλά και αντιστρόφως: Αν για τα στοιχεία a, b ισχύει ότι, για κάθε $p \in \mathcal{P}$, ένα, το πολύ, από τα $v_p(a), v_p(b)$ είναι διάφορο του μηδενός, τότε τα a, b είναι πρώτα μεταξύ τους.
(γ') Αποδείξτε ότι, αν $a_1, \ldots, a_n, b \in D$ και το b είναι πρώτο προς κάθε a_i, τότε το b είναι πρώτο και προς το γινόμενο $a_1 \cdots a_n$.
(δ') Αποδείξτε ότι, αν $a_1, \ldots, a_n, b \in D$, τα a_i είναι ανά δύο πρώτα μεταξύ τους και το b διαιρείται από κάθε a_i, τότε το b διαιρείται και από το γινόμενο $a_1 \cdots a_n$.
Υπόδειξη. Πρέπει και αρκεί να δείξετε ότι, για κάθε $p \in \mathcal{P}$ ισχύει $v_p(a_1 \cdots a_n) \leq v_p(b)$. Αυτό είναι άμεσο στην περίπτωση που το p δεν διαιρεί κανένα a_i. Αν το p διαιρεί κάποιο a_i, έστω το a_{i_0}, τότε, βάσει του (β'), συμπεράνατε ότι $v_p(a_i) = 0$ για κάθε $i \neq i_0$. Συνεπώς, $v_p(a_1 \cdots a_n) = \ldots$.

Τώρα είμαστε σε θέση να αποδείξομε ότι για οποιαδήποτε $a_1, \ldots, a_n \in D$, που δεν είναι όλα μηδέν, υπάρχει ο μέγιστος κοινός διαιρέτης τους.

Πρόταση 1.10 *Έστω D περιοχή μονοσήμαντης ανάλυσης και $\mathcal{P}$ πλήρες σύστημα πρώτων στοιχείων της. Αν $n \geq 2$ και $a_1, \ldots, a_n \in D$ δεν είναι όλα μηδενικά, τότε το στοιχείο*

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

είναι μέγιστος κοινός διαιρέτης των $a_1, \ldots, a_n$.

Απόδειξη. Για κάθε $p \in \mathcal{P}$ και κάθε $i = 1, \ldots, n$ είναι, προφανώς, $v_p(d) = n_p \leq v_p(a_i)$, οπότε (Θεώρημα 1.4.2) $d|a_i$. Συνεπώς, το d είναι κοινός διαιρέτης των $a_1, \ldots, a_n$. Έστω τώρα d' ένας οποιοσδήποτε κοινός διαιρέτης των $a_1, \ldots, a_n$. Το Θεώρημα 1.4.2 μας λέει ότι, για κάθε $p \in \mathcal{P}$ ισχύει $v_p(d') \leq v_p(a_i) \, \forall i = 1, \ldots, n$, άρα και $v_p(d') \leq \min_{1\leq i\leq n} v_p(a_i) = n_p = v_p(d)$. Συνεπώς, πάλι από το ίδιο θεώρημα συμπεραίνομε ότι $d'|d$.

Τελικά, το d είναι κοινός διαιρέτης των $a_1, \ldots, a_n$ και διαιρείται από οποιονδήποτε κοινό διαιρέτη αυτών των στοιχείων, που σημαίνει ότι το d είναι μέγιστος κοινός διαιρέτης τους.

□

Άσκηση 1.20 Έστω D περιοχή μονοσήμαντης ανάλυσης και $a_1, \ldots, a_n, b \in D$.

Αποδείξτε ότι, αν $d = \text{ΜΚΔ}(a_1, \dots, a_n)$, τότε $bd = \text{ΜΚΔ}(ba_1, \dots, ba_n)$.[6]

Άσκηση 1.21 Αναφερόμενοι στους ακεραίους, υπενθυμίζομε ότι το ελάχιστο κοινό πολλαπλάσιο δύο μη μηδενικών ακεραίων a, b ($\text{ΕΚΠ}(a, b)$) είναι ο θετικός ακέραιος m για τον οποίο ισχύουν οι εξής δύο συνθήκες: (i) Ο m είναι πολλαπλάσιο του a και πολλαπλάσιο του b (κοινό πολλαπλάσιο των a, b) και (ii) Κάθε κοινό πολλαπλάσιο των a, b είναι πολλαπλάσιο του m.
Μιμηθείτε την απόδειξη της Πρότασης 1.4.3 και αποδείξτε ότι

$$\text{ΕΚΠ}(a, b) = \prod_{p \in \mathcal{P}} p^{\max\{v_p(a), v_p(b)\}}.$$

Δείτε, με τη βοήθεια της παραπάνω σχέσης και της Πρότασης 1.4.3, ότι $\text{ΜΚΔ}(a, b) \cdot \text{ΕΚΠ}(a, b) = ab$.

Το επόμενο θεώρημα θα μας επιτρέψει να έχομε σε περιοχές μονοσήμαντης ανάλυσης θεωρία διαιρετότητας εντελώς ανάλογη με εκείνη των ακεραίων αριθμών.

Θεώρημα 1.11 *Σε κάθε περιοχή μονοσήμαντης ανάλυσης D ισχύουν τα εξής:*

(α′) Αν το p είναι ανάγωγο, τότε, κάθε στοιχείο $a \in D$, είτε είναι πολλαπλάσιο του p, είτε είναι πρώτο προς το p.[7]

(β′) Αν τα a, b είναι πρώτα μεταξύ τους, $a|c$ και $b|c$, τότε $ab|c$.[8]

(γ′) Αν καθένα από τα a, b είναι πρώτο προς το c, τότε το ab είναι πρώτο προς το c.[9]

Απόδειξη. Έστω $\mathcal{P}$ πλήρες σύστημα πρώτων για την D.

(α') Πρέπει και αρκεί να δείξομε ότι, αν $p \nmid a$, τότε $\text{ΜΚΔ}(a, p) = 1$. Για τον σκοπό αυτό θεωρούμε $p_0 \in \mathcal{P}$, συνεταιρικό του p. Προφανώς $p_0 \nmid a$ (άσκηση 1.4), οπότε $v_{p_0}(a) = 0$, ενώ $v_{p_0}(p) = 1\cdot$ άρα $\min\{v_{p_0}(a), v_{p_0}(p)\} = 0$. Για κάθε $q \in \mathcal{P}$ διαφορετικό του p_0 είναι, προφανώς, $v_q(p) = 0$, αφού το q είναι ανάγωγο, άρα $\min\{v_q(a), v_q(p)\} = 0$. Τώρα, από την Πρόταση 1.4.3,

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

(β') Λόγω του Θεωρήματος 1.4.2, αρκεί να δείξομε ότι, για οποιοδήποτε $p \in \mathcal{P}$, ισχύει $v_p(ab) \leq v_p(c)$. Έστω, λοιπόν, $p \in \mathcal{P}$. Οι σχέσεις $a|c$ και $b|c$ συνεπάγονται (λόγω του Θεωρήματος 1.4.2) τις σχέσεις $v_p(a) \leq v_p(c)$ και $v_p(b) \leq v_p(c)$, αντιστοίχως. Επειδή, όμως, τα a, b είναι πρώτα μεταξύ τους, έπεται ότι ένα τουλάχιστον από τα $v_p(a), v_p(b)$ είναι μηδέν (βλ. άσκηση 1.19), άρα $v_p(ab) = v_p(a) + v_p(b) = \max\{v_p(a), v_p(b)\} \leq v_p(c)$, δηλαδή, αποδείξαμε τον ισχυρισμό μας.

(γ') Από την άσκηση 1.19 (β'), αρκεί να δείξομε ότι, για κάθε $p \in \mathcal{P}$, ένα τουλάχιστον από τα $v_p(ab), v_p(c)$ είναι μηδέν. Πράγματι, αυτό ισχύει, διότι, έστω

[6] Πρβλ. με άσκηση 1.13.
[7] Πρβλ. Θεώρημα 1.3.2 (α').
[8] Πρβλ. Θεώρημα 1.3.2 (γ').
[9] Πρβλ. Θεώρημα 1.3.2 (δ').

ότι $v_p(c) > 0$. Τότε, η υπόθεση ότι τα a, c είναι πρώτα μεταξύ τους, συνδυασμένη με την άσκηση 1.19 (β'), μας οδηγεί στο συμπέρασμα ότι $v_p(a) = 0$. Εντελώς ανάλογα, $v_p(b) = 0$, άρα $v_p(ab) = v_p(a) + v_p(b) = 0$.

□

Η παρακάτω πρόταση είναι πολύ χρήσιμη στην επίλυση Διοφαντικών εξισώσεων:

Πρόταση 1.12 *Έστω D περιοχή μονοσήμαντης ανάλυσης και $a, b, c \in D$, τέτοια ώστε, τα a, b είναι πρώτα μεταξύ τους και $ab = c^n$, όπου ο n είναι ακέραιος ≥ 2. Τότε καθένα από τα a, b είναι συνεταιρικό με n-οστή δύναμη στοιχείου της D.*

Απόδειξη. Έστω $\mathcal{P}$ πλήρες σύστημα πρώτων για την D. Για ν' αποδείξομε ότι το a είναι συνεταιρικό n-οστής δύναμης κάποιου στοιχείου της D, αρκεί να δείξομε ότι, για κάθε $p \in \mathcal{P}$ είναι $v_p(a) =$ ακέραιο πολλαπλάσιο του n. Θεωρούμε, λοιπόν, $p \in \mathcal{P}$ και έχομε

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

όπου τουλάχιστον ένα εκ των $v_p(a), v_p(b)$ είναι μηδέν, αφού τα a, b είναι πρώτα μεταξύ τους (βλ. άσκηση 1.19 (β')). Αν $v_p(a) = 0$, τότε, προφανώς, $v_p(a)$ είναι πολλαπλάσιο του n. Αν, πάλι, $v_p(a) \neq 0$, τότε, αναγκαστικά, $v_p(b) = 0$, οπότε η παραπάνω σχέση γίνεται $n \cdot v_p(c) = v_p(a)$, δηλαδή, και πάλι, $v_p(a)$ είναι πολλαπλάσιο του n.

□

Παράδειγμα 1.2 Υπολογισμός όλων των θετικών ακεραίων λύσεων της εξίσωσης

$$x^2 + y^2 = z^2, \quad \text{ΜΚΔ}(x, y) = 1. \tag{1.7}$$

Λύση. Έστω (x, y, z) λύση όπως στην εκφώνηση. Οι x, y δεν είναι και οι δύο άρτιοι, αφού έχουν υποτεθεί πρώτοι μεταξύ τους. Δεν είναι και οι δύο περιττοί, για τον εξής λόγο. Αν $x = 2k + 1, y = 2l + 1$, τότε η εξίσωση (1.7) γίνεται $4(k^2 + k + l^2 + l) + 2 = z^2$, άρα ο z είναι άρτιος. Αλλά τότε το δεξιό μέλος είναι πολλαπλάσιο του 4, ενώ το δεξιό είναι άρτιο, αλλά όχι πολλαπλάσιο του 4, άτοπο. Άρα ένας, ακριβώς, από τους x, y είναι άρτιος. Λόγω συμμετρίας της εξίσωσης ως προς τους x, y, υποθέτομε δίχως βλάβη της γενικότητας ότι ο y είναι άρτιος και ο x περιττός.

Γράφομε την (1.7) ως

$$(z + y)(z - y) = x^2, \tag{1.8}$$

όπου οι παράγοντες στο αριστερό μέλος είναι θετικοί και περιττοί. Επίσης, είναι πρώτοι μεταξύ τους για τον εξής λόγο. Αν είχαν κοινό διαιρέτη > 1 θα είχαν και *πρώτο* κοινό διαιρέτη p. Είναι $p > 2$ γιατί οι παράγοντες είναι περιττοί. Οι σχέσεις $p \mid (z+y)$ και $p \mid (z-y)$ συνεπάγονται (αθροίζοντας και αφαιρώντας, αντιστοίχως)

τις $p \mid 2z$ και $p \mid 2y$, άρα (αφού ο p είναι πρώτος προς το 2) $p \mid z$ και $p \mid y$. Αλλά τότε, από την (1.8) $p \mid x$ και ερχόμαστε σε αντίφαση με την υπόθεση ΜΚΔ$(x, y) = 1$.

Τώρα έξασφαλίασμε ότι στη σχέση (1.8) μπορεί να εφαρμοστεί η Πρόταση 1.4.5, άρα καθένας από τους δύο παράγοντες στο αριστερό μέλος είναι συνεταιρικός με τετράγωνο. Καθώς οι μόνες μονάδες του $\mathbb{Z}$ είναι ± 1 και οι παράγοντες είναι θετικοί, συμπεραίνομε ότι $z + y = m^2, z - y = n^2$, όπου οι m, n είναι θετικοί ακέραιοι πρώτοι μεταξύ τους. Έπεται ότι $x^2 = m^2 n^2$, άρα (είναι $x > 0$) $x = mn$. Έτσι καταλήξαμε στους εξής τύπους:

$$x = mn,\ y = \tfrac{1}{2}(m^2 - n^2),\ z = \tfrac{1}{2}(m^2, n^2), \quad m > n > 0 \text{ περιττοί, } \text{ΜΚΔ}(x, y) = 1.$$

Οι τύποι αυτοί δίνουν όλες τις θετικές ακέραιες λύσεις της (1.7) με τους x, y πρώτους μεταξύ τους και τον y άρτιο.

Άσκηση 1.22 Έστω D περιοχή μονοσήμαντης ανάλυσης και $a, b, c, d \in D$, τέτοια ώστε, τα a, b είναι πρώτα μεταξύ τους και $ab = dc^n$, όπου $<$ο n είναι ακέραιος ≥ 2. Τότε υπάρχουν $c_1, c_2, d_1, d_2 \in D$, με τις εξής ιδιότητες:

- c_1, c_2 είναι πρώτα μεταξύ τους και $c_1 c_2 = c$.
- d_1, d_2 είναι πρώτα μεταξύ τους και $d_1 d_2 = d$.
- Το a είναι συνεταιρικό με το $d_1 {c_1}^n$ και το b είναι συνεταιρικό με το $d_2 {c_2}^n$.

Άσκηση 1.23 (εφαρμογή της άσκησης 1.22) Υπολογίστε, κατά το Παράδειγμα 1.2, τίς θετικές ακέραιες λύσεις της εξίσωσης

$$x^2 + 2y^2 = z^2,\ \text{ΜΚΔ}(x, y) = 1.$$

Υπόδειξη. Δείξτε πρώτα ότι ο x δεν μπορεί να είναι άρτιος, γιατί, σε τέτοια περίπτωση, αυτό συνεπάγεται ότι και ο y είναι άρτιος, που αντιβαίνει στην υπόθεση ΜΚΔ$(x, y) = 1$.

Παράδειγμα 1.3 Θα υπολογίσομε τις ακέραιες λύσεις (x, y) της εξίσωσης

$$.x^2 + 2 = y^3 \tag{1.9}$$

Λύση. Θα εργαστούμε στην περιοχή μονοσήμαντης ανάλυσης $D = \mathbb{Z}[\sqrt{-2}]$, βοηθούμενοι από την άσκηση 1.12. Παραγοντοποιούμε την εξίσωση

$$(x + \sqrt{-2})(x - \sqrt{-2}) = y^3. \tag{1.10}$$

Από το ερώτημα (ε') της παραπάνω άσκησης, οι παράγοντες στο αριστερό μέλος της (1.10) είναι πρώτοι μεταξύ τους, άρα, από την Πρόταση 1.4.5, καθένας από αυτούς είναι συνεταιρικός με κάποια κυβική δύναμη στοιχείου της D. Οι μόνες μονάδες της D είναι ± 1, σύμφωνα με το ερώτημα (α') της άσκησης, άρα, $x + y\sqrt{-2} =$

$\pm(a+b\sqrt{-2})^3$, με $a,b\in\mathbb{Z}$. Αν ισχύει το πρόσημο $-$, τότε το δεξιό μέλος ισούται με $(-a-b\sqrt{-2})^3$, που είναι όμοιας μορφής, άρα, δίχως βλάβη της γενικότητας, μπορούμε να συμπεράνομε ότι

$$x+\sqrt{-2}=(a+b\sqrt{-2})^3=a^3-6ab^2+(3a^2b-2b^3)\sqrt{-2}.$$

Βλέποντας το $\sqrt{-2}$ ως $i\sqrt{2}$ και εξισώνοντας πραγματικά και φανταστικά μέρη στην παραπάνω ισότητα οδηγούμαστε στις σχέσεις

$$x=a^3-6ab^2,\quad 1=3a^2b-2b^3=b(3a^2-2b^2). \tag{1.11}$$

Οι $b, 3a^2-2b^2$ είναι ακέραιοι με γινόμενο 1, άρα, ή $b=1=3a^2-2b^2$, ή $b=-1=3a^2-2b^2$. Στην πρώτη περίπτωση παίρνομε πολύ εύκολα, $a^2=1$, άρα, από την πρώτη σχέση (1.11), $x=5$ ή -5, ανάλογα με το αν $a=-1$ ή 1. Τότε, από την (1.9), $y=3$. Στη δεύτερη περίπτωση, η σχέση $-1=3a^2-2b^2$ συνεπάγεται $3a^2=1$, που είναι αδύνατη για $a\in\mathbb{Z}$.

Συμπέρασμα. Οι μοναδικές ακέραιες λύσεις της εξίσωσης (1.9) είναι $(x,y)=(\pm5,3)$.

1.5 Πολυώνυμα σε περιοχες μονοσημαντης αναλυσης

Όπως επισημάναμε στην "Σημαντική παρατήρηση" της σελίδας 8, στην περίπτωση που $D=K=$ σώμα, ο δακτύλιος πολυωνύμων $K[X]$ είναι περιοχή μονοσήμαντης ανάλυσης (ως συνέπεια του ότι ο $K[X]$ είναι περιοχή κυρίων ιδεωδών). Θα αποδείξομε ότι, όταν η D είναι περιοχή μονοσήμαντης ανάλυσης, ακόμη κι αν δεν είναι σώμα, και πάλι ο δακτύλιος πολυωνύμων $D[X]$ είναι περιοχή μονοσήμαντης ανάλυσης.

Στην ενότητα 1.5 το D συμβολίζει περιοχή μονοσήμαντης ανάλυσης.

Ορισμός. Ως *περιεχόμενο* ενός μη σταθερού πολυωνύμου της $D[X]$ ορίζεται (κατά προσέγγιση μονάδας της D) ο ΜΚΔ των συντελεστών του πολυωνύμου. Το μη σταθερό πολυώνυμο $f(X)\in D[X]$ λέμε ότι είναι *πρωταρχικό* αν το περιεχόμενό του είναι 1.

Άσκηση 1.24 (α') Αν $d_1,d_2\in D$ είναι και τα δύο περιεχόμενα του ίδιου πολυωνύμου της $D[X]$, τότε αυτά είναι συνεταιρικά στοιχεία της D.
(β') Αν το $d\in D$ είναι περιεχόμενο του $f(X)\in D[X]$, τότε το $d^{-1}f(X)$ είναι πρωταρχικό πολυώνυμο της $D[X]$.
(γ') Αν το $f(X)$ είναι πρωταρχικό πολυώνυμο της $D[X]$ και $d\in D$ (μη μηδενικό), τότε το d είναι περιεχόμενο του $d\cdot f(X)$.

Λήμμα 1.13 *Κάθε μη μηδενικό $f(X)\in Q(D)[X]$[10] γράφεται ως γινόμενο $f(X)=\alpha\cdot g(X)$, όπου $\alpha\in Q(D)$ και $g(X)$ είναι πρωταρχικό πολυώνυμο της $D[X]$. Αν*

[10] Υπενθυμίζομε ότι $Q(D)$ συμβολίζει το σώμα πηλίκων της D.

$f(X) = \beta \cdot h(X)$, όπου $\beta \in Q(D)$ και $h(X)$ είναι πρωταρχικό πολυώνυμο της $D[X]$, τότε υπάρχει $\epsilon \in D^*$, τέτοιο ώστε $\beta = \epsilon\alpha$, οπότε $h(X) = \epsilon^{-1}g(X)$.

Απόδειξη. Για απλούστευση του συμβολισμού, έστω $K = Q(D)$. Κάθε στοιχείο του K είναι πηλίκο στοιχείων της D, άρα, αν συμβολίσομε με c το γινόμενο των παρονομαστών των συντελεστών του $f(X)$, τότε το $c \cdot f(X)$ έχει συντελεστές στη D. Οπότε, αν το $d \in D$ είναι περιεχόμενο του $c \cdot f(X)$, τότε, από την άσκηση 1.24 (β'), το $d^{-1}(c \cdot f(X))$ είναι πρωταρχικό πολυώνυμο, έστω $g(X) \in D[X]$ και $f(X) = \alpha \cdot g(X)$, με $\alpha = c^{-1}d$.

Έστω τώρα ότι $f(X) = \beta \cdot h(X)$, όπου $\beta \in K$ και $h(X) \in D[X]$ πρωταρχικό. Θεωρούμε $e \in D$, τέτοιο ώστε $e\alpha = d_1 \in D$ και $e\beta = d_2 \in D$. Προφανώς $d_1 g(X) = d_2 h(X)$. Από την άσκηση 1.24 (γ'), το d_1 είναι περιεχόμενο του $d_1 g(X)$ και το d_2 είναι περιεχόμενο του $d_2 h(X)$, άρα, τα d_1, d_2, ως περιεχόμενα του ίδιου πολυωνύμου, είναι συνεταιρικά (άσκηση 1.24 (α')). Έστω $d_2 = \epsilon d_1$, $\epsilon \in D^*$. Τότε, $e\beta = d_2 = \epsilon d_1 = \epsilon e\alpha$, άρα $\beta = \epsilon\alpha$.

□

Θεώρημα 1.14 *Το γινόμενο πρωταρχικών πολυωνύμων είναι πρωταρχικό πολυώνυμο.*

Απόδειξη. Έστω

$$(a_m X^m + \cdots + a_1 X + a_0) \cdot (b_n X^n + \cdots + b_1 X + b_0) = c_\ell X^\ell + \cdots c_1 X + c_0, \quad (1.12)$$

όπου $m, n \geq 1$ και $a_m b_n c_\ell \neq 0$ (συνεπώς, $\ell = m + n$) και οι δύο παράγοντες (πολυώνυμα) στο αριστερό μέλος είναι πρωταρχικά πολυώνυμα της $D[X]$. Θα δείξομε ότι και το πολυώνυμο στο δεξιό μέλος είναι πρωταρχικό. Αν δεν είναι, υπάρχει πρώτο στοιχείο p που διαιρεί όλους τους συντελεστές στο πολυώνυμο του δεξιού μέλους της (1.12), άρα και όλους τους συντελεστές του πολυωνύμου, που θα προκύψει αν κάνομε τον πολλαπλασιασμό στο αριστερό μέλος της (1.12). Κατ' αρχάς, παρατηρούμε ότι το p δεν μπορεί να διαιρεί όλα τα a_i, διότι $1 = \text{ΜΚΔ}(a_0, \ldots, a_m)$· ομοίως και για τα b_i. Άρα, υπάρχουν δείκτες μ και ν, τέτοιοι ώστε

$$0 \leq \mu \leq m, \quad p \nmid a_\mu \ \ \& \ \ p | a_i \ \ \text{άν } i < \mu$$

$$0 \leq \nu \leq n, \quad p \nmid b_\nu \ \ \& \ \ p | b_j \ \ \text{άν } j < \nu.$$

Εξισώνοντας τους συντελεστές του $X^{\mu+\nu}$ στα δύο μέλη της (1.12) παίρνομε τη σχέση

$$c_{\mu+\nu} = \sum_{i+j=\mu+\nu} a_i b_j, \quad (1.13)$$

το αριστερό μέλος της οποίας είναι, προφανώς, διαιρετό από το p. Άρα και το δεξιό μέλος πρέπει να διαιρείται από το p. Όμως, παρατηρούμε τα εξής: Αν $i < \mu$, τότε $p | a_i$, άρα $p | a_i b_j$. Αν, $i > \mu$, τότε $j < \nu$ (διότι $i + j = \mu + \nu$), οπότε $p | b_j$, άρα $p | a_i b_j$. Αν, τέλος, $i = \mu$, οπότε $j = \nu$, τότε $p \nmid a_i$ και $p \nmid b_j$, άρα $p \nmid a_i b_j$. Έτσι, στο άθροισμα

του δεξιού μέλους της (1.13), ο p δεν διαιρεί τον όρο $a_\mu b_\nu$, ενώ διαιρεί όλους τους υπόλοιπους προσθετέους. Συνεπώς, ο p δεν διαιρεί το δεξιό μέλος· άτοπο.

□

Θεώρημα 1.15 [11] *Το πολυώνυμο $f(X) \in D[X]$ είναι ανάγωγο στοιχείο της περιοχής $D[X]$, αν και μόνο αν, ή το $f(X)$ είναι σταθερό, ίσο με ανάγωγο στοιχείο της D, ή το $f(X)$ είναι μη σταθερό πρωταρχικό πολυώνυμο, το οποίο, ως πολυώνυμο του $Q(D)[X]$, είναι ανάγωγο πάνω από το σώμα $Q(D)$.*

Απόδειξη. Για απλοποίηση του συμβολισμού, ας θέσομε $Q(D) = K$.

($\Leftarrow$) Αν $f(X) = p$, όπου p είναι ανάγωγο στοιχείο της D, τότε το $f(X)$ είναι ανάγωγο και ως στοιχείο της $D[X]$, σύμφωνα με την άσκηση 1.9. Αν, πάλι, το $f(X)$ είναι μη σταθερό πρωταρχικό πολυώνυμο του $D[X]$, ανάγωγο πάνω από το K, τότε αποκλείεται να είναι το $f(X)$ γινόμενο δύο μη σταθερών πολυωνύμων του $D[X]$. Αποκλείεται, επίσης, η περίπτωση $f(X) = c \cdot g(X)$ με $g(X) \in D[X]$ και $c \in D$ όχι μονάδα, διότι, τότε, όλοι οι συντελεστές του $f(X)$ θα ήταν πολλαπλάσια του c, άρα δεν θα ήταν πρώτοι μεταξύ τους, που αντιβαίνει στην υπόθεση πρωταρχικότητας του $f(X)$. Συνεπώς, και στις δύο περιπτώσεις, το $f(X)$ είναι ανάγωγο στοιχείο της περιοχής $D[X]$.

($\Rightarrow$) Τώρα υποθέτομε ότι το $f(X)$ είναι ανάγωγο στοιχείο της $D[X]$. Αν είναι σταθερό πολυώνυμο, έστω $f(X) = c \in D$, τότε το c είναι, υποχρεωτικά, ανάγωγο στοιχείο της D. Διότι, αν ήταν $c = ab$ με τα $a, b \in D$ όχι μονάδες, τότε τα a, b μπορούμε να τα δούμε και ως μη αντιστρέψιμα στοιχεία της περιοχής $D[X]$, άρα θα είχαμε μη τετριμμένη ανάλυση του $c = f(X)$ στην περιοχή $D[X]$· αντίφαση.
Έστω τώρα ότι το $f(X)$ δεν είναι σταθερό. Βλέποντας το $f(X)$ ως πολυώνυμο του $K[X]$, το αναλύομε σε ανάγωγα πολυώνυμα του $K[X]$, έστω $f(X) = q_1(X) \cdots q_m(X)$ ($m \geq 1$). Βάσει του Λήμματος 1.5.1, για κάθε $i = 1, \ldots, m$, έχομε $q_i(X) = \alpha_i \cdot g_i(X)$, όπου $\alpha_i \in K$ και $g_i(X)$ πρωταρχικό πολυώνυμο της $D[X]$. Θέτοντας τώρα $g(X) = g_1(X) \cdots g_m(X)$, έχομε, από το Θεώρημα 1.5.2, ότι το $g(X)$ είναι πρωταρχικό πολυώνυμο της $D[X]$. Θέτοντας, επίσης, $\alpha_1 \cdots \alpha_m = \alpha$, οδηγούμαστε στη σχέση $1 \cdot f(X) = \alpha \cdot g(X)$, με τα $f(X), g(X)$ πρωταρχικά. Άρα, το Λήμμα 1.5.1 μας οδηγεί στο συμπέρασμα ότι $\alpha = \epsilon \in D^*$ και, συνεπώς, $f(X) = \epsilon g(X) = \epsilon g_1(X) \cdots g_m(X)$. Όμως, τα πολυώνυμα στο δεξιό μέλος ανήκουν στη $D[X]$, ενώ το $f(X)$ έχει υποτεθεί ανάγωγο στοιχείο της $D[X]$. Αναγκαστικά, λοιπόν, $m = 1$ και $f(X) = \epsilon g_1(X)$. Καθώς $g_1(X) = \alpha_1^{-1} q_1(X)$ με το $q_1(X)$ ανάγωγο στο $K[X]$, έπεται ότι και το $g_1(X)$ είναι ανάγωγο στο $K[X]$, άρα, τελικά, το $f(X)$ θεωρούμενο ως πολυώνυμο του $K[X]$, είναι ανάγωγο.

□

Παράδειγμα 1.4 Έστω $D = \mathbb{Z}$, οπότε $Q(D) = \mathbb{Q}$. Η ανάλυση του $f(X) = 6X + 3$ σε ανάγωγα της $D[X]$ είναι $f(X) = 3(2X + 1)$. Εδώ, το $3 \in D[X]$ είναι ανάγωγο γιατί είναι ανάγωγο και ως στοιχείο της D. Το $2X + 1$ είναι πρωταρχικό και ανάγωγο στο $\mathbb{Q}[X]$, άρα ανάγωγο στοιχείο της $D[X]$. Συνεπώς, το $f(X)$, ως

[11] Στή βιβλιογραφία, κάποιες φορές, αυτό το θεώρημα αναφέρεται ως Λήμμα του Gauss.

στοιχείο της $D[X]$ είναι γινόμενο δύο ανάγωγων στοιχείων της $D[X]$. Θεωρούμενο, όμως, ως στοιχείο της περιοχής $\mathbb{Q}[X]$, το $f(X)$ είναι ανάγωγο, ως πολυώνυμο πρώτου βαθμού. Η σχέση $f(X) = 3(2X + 1)$, η οποία, φυσικά, εξακολουθεί να ισχύει, δεν μας επηρρεάζει διότι το 3 ως στοιχείο του $\mathbb{Q}$ δεν είναι ανάγωγο, αφού είναι μονάδα (= αντιστρέψιμο) στοιχείο του $\mathbb{Q}$.

Συνεχίζοντας με την $D = \mathbb{Z}$, το $g(X) = 6X + 5$ είναι ανάγωγο στοιχείο της $\mathbb{Z}[X]$ γιατί είναι πρωταρχικό και ανάγωγο ως πολυώνυμο του $\mathbb{Q}[X]$.

Άσκηση 1.25 Αναλύστε σε ανάγωγα τα εξής στοιχεία της περιοχής $\mathbb{Z}[X]$:

$$f(X) = 20X^2-40X-300, \quad g(X) = 3X^3-6X^2+3X-6, \quad h(X) = 4X^3-28*X+24.$$

Άσκηση 1.26 Σ' αυτή την άσκηση $D = \mathbb{Z}[\sqrt{-2}]$ και θεωρήστε δεδομένο ότι η D είναι περιοχή μονοσήμαντης ανάλυσης. Έστω $K = Q(D)$.

(α') Αποδείξτε ότι $K = \mathbb{Q}[\sqrt{-2}] = \{r + s\sqrt{-2} : r, s \in \mathbb{Q}\}$.

(β') Αποδείξτε ότι τα στοιχεία $1 \pm \sqrt{-2}$ της D είναι ανάγωγα. (Παρεμπιπτόντως, και το $\sqrt{-2}$ είναι ανάγωγο, σύμφωνα με την άσκηση 1.12 (β'), κάτι που θα χρειαστεί σε επόμενο ερώτημα.)

(γ') Αναλύστε τα στοιχεία 2 και 3 σε ανάγωγα στοιχεία της D.

(δ') Αποδείξτε ότι το $X^2 - 2$ είναι ανάγωγο στοιχείο της $D[X]$.

(ε') Αναλύστε το $X^2 + 4$ σε ανάγωγα στοιχεία της $D[X]$.

(ϛ') Αναλύστε το $f(X) = 6X^4 - 24$ σε ανάγωγα στοιχεία της $D[X]$.

(ζ') Το $f(X)$, ως στοιχείο της $K[X]$, πώς αναλύεται σε ανάγωγα;

Τελειώνομε αυτή την ενότητα με το παρακάτω πολύ σημαντικό:

Θεώρημα 1.16 *Αν D είναι περιοχή μονοσήμαντης ανάλυσης και $X, Y, Z, ...$ είναι πεπερασμένες το πλήθος μεταβλητές, τότε $D[X, Y, Z, ...]$ είναι περιοχή μονοσήμαντης ανάλυσης.*

Απόδειξη. Αποδεικνύομε ότι η $D[X]$ είναι περιοχή μονοσήμαντης ανάλυσης: Κατ' αρχάς, για απλοποίηση του συμβολισμού, θέτομε $K = Q(D)$.

Έστω $f(X) \in D[X]$, όχι μονάδα της $D[X]$. Αν το $f(X)$ είναι σταθερό, τότε $f(X) = c \in D \setminus D^*$, άρα το c αναλύεται μονοσήμαντα σε ανάγωγα στοιχεία της D (άρα, ανάγωγα στοιχεία και της $D[X]$). Έστω τώρα ότι το $f(X)$ δεν είναι σταθερό και $d \in D$ το περιεχόμενό του. Τότε, από την άσκηση 1.24 (β'), το $d^{-1}f(X)$ είναι κάποιο πρωταρχικό πολυώνυμο, έστω $g(X) \in D[X]$. Τώρα έχομε $f(X) = d \cdot g(X)$ και έστω $g(X) = p_1(X) \cdots p_m(X)$ η ανάλυση του $g(X)$ σε ανάγωγα πολυώνυμα του $K[X]$. Για κάθε $i = 1, ..., m$, υπάρχει $k_i \in K$ και πρωταρχικό πολυώνυμο $h_i(X) \in D[X]$, έτσι ώστε $p_i(X) = k_i h_i(X)$ (βλ. Λήμμα 1.5.1) και, βεβαίως, αφού το $p_i(X)$ είναι ανάγωγο πολυώνυμο του $K[X]$, το ίδιο ισχύει και για το $h_i(X)$. Καταλήγομε έτσι στη σχέση

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

και παρατηρούμε ότι το $h(X) \in D[X]$ είναι πρωταρχικό πολυώνυμο, λόγω του Θεωρήματος 1.5.2. Αλλά και το $g(X) \in D[X]$ είναι πρωταρχικό και $1 \cdot g(X) = k \cdot h(X)$. Από το Λήμμα 1.5.1 έπεται τώρα ότι $k = 1 \cdot \epsilon$, για κάποια μονάδα ϵ της D, δηλαδή, $k = \epsilon \in D^*$. Τελικά,

$$f(X) = c \cdot g(X) = \epsilon c \cdot h_1(X) \cdots h_m(X). \tag{1.14}$$

Καθώς τα $h_1(X), \ldots, h_m(X)$ είναι πρωταρχικά πολυώνυμα της $D[X]$ και είναι ανάγωγα στο $K[X]$, συμπεραίνομε, βάσει του Θεωρήματος 1.5.3, ότι αυτά είναι ανάγωγα στοιχεία της ακέραιας περιοχής $D[X]$. Αναλύοντας τώρα και το c σε ανάγωγα στοιχεία της D, παίρνομε από την (1.14) μιά ανάλυση του $f(X)$ σε ανάγωγα στοιχεία της $D[X]$.

Η μοναδικότητα της ανάλυσης: Έστω

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

όπου τα $q_1, \ldots, q_n$ και τα $q'_1, \ldots, q'_\nu$ είναι ανάγωγα στοιχεία της D και όλα τα πολυώνυμα $h_1(X), \ldots, h_m(X)$ και $h'_1(X), \ldots h'_\mu(X)$ είναι ανάγωγα στοιχεία της ακέραιας περιοχής $D[X]$. Τούτο το τελευταίο σημαίνει, βάσει του Θεωρήματος 1.5.3, ότι αυτά τα πολυώνυμα είναι πρωταρχικά και ανάγωγα στο $K[X]$, οπότε και τα γινόμενα $h_1(X) \cdots h_m(X)$ και $h'_1(X) \cdots h'_\mu(X)$ είναι πρωταρχικά. Αλλά τότε, το Λήμμα 1.5.1 μας λέει ότι $q'_1 \cdots q'_\nu = \epsilon q_1 \cdots q_n$, για κάποιο $\epsilon \in D^*$, και

$$h_1(X) \cdots h_m(X) = \epsilon \cdot h'_1(X) \cdots h'_\mu(X) \tag{1.15}$$

Δεδομένου ότι η D είναι περιοχή μονοσήμαντης ανάλυσης, η σχέση $q'_1 \cdots q'_\nu = \epsilon q_1 \cdots q_n$ μας οδηγεί στο συμπέρασμα ότι $\nu = n$ και, δίχως βλάβη της γενικότητας, τα $q'_1, \ldots, q'_m$ είναι ένα προς ένα συνεταιρικά με τα $q_1, \ldots, q_m$.
Μένει να δείξομε ότι κάτι ανάλογο συμβαίνει και με τα πολυώνυμα $h_i(X)$ και $h'_j(X)$.

Βλέποντας την (1.15) ως σχέση στο $K[X]$ και γνωρίζοντας από τη βασική Άλγεβρα ότι στο $K[X]$ ισχύει η μονοσήμαντη ανάλυση σε ανάγωγα πολυώνυμα, συμπεραίνομε ότι, $\mu = m$ και, δίχως βλάβη της γενικότητας, $h'_i(X) = k_i \cdot h_i(X)$ $(k_i \in K)$ για κάθε $i = 1, \ldots, m$. Πάλι εφαρμόζοντας το Λήμμα 1.5.1 συμπεραίνομε ότι $k_i = \epsilon'_i \epsilon_i$ με $\epsilon'_i \in D^*$, άρα $k_i \in D^*$. Αυτό σημαίνει ότι, για κάθε $i = 1, \ldots, m$, το $h'_i(X)$, ως στοιχείο της $D[X]$, είναι συνεταιρικό με το $h_i(X)$.

Καταλήξαμε, λοιπόν, στο συμπέρασμα ότι

> *Αν η D είναι περιοχή μονοσήμαντης ανάλυσης, τότε τα πολυώνυμα μιας μεταβλητής πάνω από τη D είναι περιοχή μονοσήμαντης ανάλυσης.*

Εφαρμόζοντας το παραπάνω συμπέρασμα, θέτοντας στη θέση της D τη $D[X]$ και παίρνοντας ως μεταβλητή των πολυωνύμων πάνω από τη $D[X]$ τη μεταβλητή Y, συμπεραίνομε ότι και η $(D[X])[Y]$, δηλαδή, η $D[X, Y]$, είναι περιοχή μονοσήμαντης ανάλυσης. Επαναλαμβάνοντας με τη $D[X, Y]$ στη θέση της D και με το Z ως μεταβλητή των πολυωνύμων πάνω από τη $D[X, Y]$, συμπεραίνομε ότι και η $D[X, Y, Z]$

είναι περιοχή μονοσήμαντης ανάλυσης κ.ο.κ.

□

Παράδειγμα 1.5 *Περιοχή μονοσήμαντης ανάλυσης, η οποία δεν είναι περιοχή κυρίων ιδεωδών.* Ο δακτύλιος των πολυωνύμων δύο μεταβλητών με συντελεστές από ένα σώμα είναι περιοχή μονοσήμαντης ανάλυσης, αλλά δεν είναι περιοχή κυρίων ιδεωδών.

Απόδειξη. Έστω σώμα K και $D = K[X, Y]$ ο δακτύλιος των πολυωνύμων μεταβλητών X, Y. Το ότι η D είναι περιοχή μονοσήμαντης ανάλυσης προκύπτει αμέσως από το Θεώρημα 1.5.4.

Θα δείξομε, με εις άτοπον απαγωγή, ότι το ιδεώδες

$$\langle X, Y\rangle \stackrel{\text{def}}{=} \{X \cdot h_1(X, Y) + Y \cdot h_2(X, Y) : h_1(X, Y), h_2(X, Y) \in K[X, Y]\}$$

δεν είναι κύριο. Έστω ότι είναι κύριο, ίσο με

$$\langle f(X)\rangle \stackrel{\text{def}}{=} \{f(X) \cdot h(X, Y) : h(X, Y) \in K[X, Y]\},$$

για κάποιο μη μηδενικό $f(X, Y) \in K[X, Y]$. Τότε, επειδή τα X, Y ανήκουν, προφανώς, στο $\langle X, Y\rangle$ υπάρχουν $g(X, Y), h(X, Y)$ ώστε να ισχύουν οι σχέσεις

$$X = f(X, Y) \cdot g(X, Y) \tag{1.16}$$
$$Y = f(X, Y) \cdot h(X, Y) \tag{1.17}$$

Ο βαθμός του $f(X, Y)$ ως προς X δεν είναι 0 διότι, αν ήταν, τότε $f(X, Y) = f(Y)$ και από την (1.16), $X = f(Y) \cdot g(X, Y)$. Ο ομομορφισμός αντικατάστασης $0 \leftarrow X$ δίνει $0 = f(Y) \cdot h(0, Y)$ (σχέση στον δακτύλιο $K[Y]$), άρα $f(Y) = 0$, οπότε $f(X, Y) = 0$, άτοπο. Συμπεραίνομε, λοιπόν, ότι ο βαθμός του $f(X, Y)$ ως προς X είναι θετικός. Δεν μπορεί να είναι > 1 διότι στο αριστερό μέλος ο βαθμός ως προς X είναι 1. Συγκρίνοντας ξανά τους βαθμούς ως προς X στην (1.16), βλέπομε ότι ο βαθμός του $g(X, Y)$ ως προς X είναι 0, άρα $g(X, Y) = g(Y)$. Ανάλογα συμπεράσματα προκύπτουν και για την (1.17), δηλαδή, ο βαθμός του $f(X, Y)$ ως προς Y είναι 1 και $h(X, Y) = h(X)$. Βάσει αυτών των συμπερασμάτων μας είναι τώρα

$$f(X, Y) = \alpha X + \beta Y + \gamma XY + \delta$$

και οι (1.16) και (1.17) γίνονται

$$X = (\alpha X + \beta Y + \gamma XY + \delta) \cdot g(Y) \tag{1.18}$$
$$Y = (\alpha X + \beta Y + \gamma XY + \delta) \cdot h(X) \tag{1.19}$$

Στην (1.18) ο ομομορφισμός αντικατάστασης $0 \leftarrow X$ δίνει $0 = (\beta Y + \delta) \cdot g(Y)$ (σχέση στο $K[Y]$), άρα $\beta = \delta = 0$, και στην (1.18) ο ομομορφισμός αντικατάστασης $0 \leftarrow Y$ δίνει $0 = (\alpha X + \delta) \cdot h(X)$ (σχέση στο $K[X]$), άρα $\alpha = \delta = 0$. Τελικά,

$\alpha X+\beta Y+\gamma XY+\delta = \gamma XY$ και η (1.18) γίνεται $X = \gamma XY\cdot g(Y)$, άρα $1 = Y\cdot g(Y)$, που είναι σχέση αδύνατη στην ακέραια περιοχή $K[Y]$.

Άσκηση 1.27 Αναλύστε το $X^4 - X^3 + 3X^2 - 2X + 2 \in \mathbb{Q}[X]$ σε γινόμενο δύο δευτεροβαθμίων μονικών πολυωνύμων με ακέραιους συντελεστές, τα οποία είναι ανάγωγα πολυώνυμα του $\mathbb{Q}[X]$.

Στη συνέχεια, έστω $f(X) = 12(X^4 - X^3 + 3X^2 - 2X + 2) \in \mathbb{Q}[X]$. Αναλύστε το $f(X)$ σε ανάγωγα στοιχεία της περιοχής $D[X]$, υπό τη μορφή

$f(X) = \epsilon\cdot$γινόμενο αναγώγων της $D\cdot$γινόμενο μη σταθερών αναγώγων της $D[X]$,

όπου $\epsilon \in D^*$, σε κάθε μία από τις παρακάτω περιπτώσεις:
(i) $D = \mathbb{Z}$. (ii) $D = \mathbb{Q}$. (iii) $D = \mathbb{Z}[i\sqrt{2}]$. (iv) $D = \mathbb{Z}[\omega]$, με το ω όπως στην άσκηση 1.29.

Για την περίπτωση (iii): Θεωρήστε δεδομένο ότι η D είναι περιοχή μονοσήμαντης ανάλυσης. Πρίν προχωρήσετε στην ανάλυση του $f(X)$, αποδείξτε ότι τα $i\sqrt{2}, 1+i\sqrt{2}, 1-i\sqrt{2}$ είναι ανάγωγα στοιχεία της D και αναλύστε το 2 και το 3 σε ανάγωγα της D. Αποδείξτε ότι το $X^2 - X + 1$ δεν έχει ρίζες στη D.

Για την περίπτωση (iv): Θεωρήστε δεδομένο ότι η D είναι περιοχή μονοσήμαντης ανάλυσης. Θεωρήστε δεδομένα τα (α') και (β') της άσκησης 1.29. Πρίν προχωρήσετε στην ανάλυση του $f(X)$, αποδείξτε ότι τα 2 και $1-\omega$ είναι ανάγωγα στοιχεία της D και παρατηρήστε ότι $3 = -\omega^2(1-\omega)^2$. Αποδείξτε ότι το X^2+2 δεν έχει ρίζες στη D.

1.6 Ευκλειδειες περιοχες

Ορισμός. Η ακέραια περιοχή E λέγεται *ευκλείδεια* αν υπάρχει απεικόνιση

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

με τις εξής ιδιότητες:

1. Αν τα $a, b \in E$ είναι μη μηδενικά και $a|b$, τότε $\mathrm{N}(a) \leq \mathrm{N}(b)$.
2. Αν $a, b \in E$ και $b \neq 0$, τότε υπάρχουν $q, r \in E$, τέτοια ώστε $a = bq + r$ και είτε $r = 0$ είτε $\mathrm{N}(r) < \mathrm{N}(b)$.

Η απεικόνιση N λέγεται *στάθμη*.

Λήμμα 1.17 *Έστω E ευκλείδεια περιοχή στάθμης* N. *Αν τα $a, b \in E$ είναι μη μηδενικά, $a|b$ και $\mathrm{N}(a) = \mathrm{N}(b)$, τότε τα a, b είναι συνεταιρικά.*

Απόδειξη. Έστω ότι $a = bq + r$, με τα q, r όπως προβλέπονται από τον Ορισμό 1.6. Αν $r = 0$, τότε $b|a$. Εξ υποθέσεως, όμως, ισχύει και $a|b$, άρα (άσκηση 1.5) τα a, b είναι συνεταιρικά. Αν $r \neq 0$, τότε $\mathrm{N}(r) < \mathrm{N}(b)$. Εξ υποθέσεως, $b = ac$

για κάποιο $c \in E$, οπότε $a = bq + r = (ac)q + r$, απ' όπου $r = a(1 - cq)$. Αλλά τώρα βλέπομε ότι $a|r$, άρα $\mathrm{N}(r) \geq \mathrm{N}(a) = \mathrm{N}(b)$, που έρχεται σε αντίφαση με την $\mathrm{N}(r) < \mathrm{N}(b)$.

□

Θεώρημα 1.18 *Κάθε ευκλείδεια περιοχή είναι περιοχή κυρίων ιδεωδών, άρα και μονοσήμαντης ανάλυσης.*

Απόδειξη. Έστω ευκλείδεια περιοχή E και I μη μηδενικό ιδεώδες της E. Θεωρούμε ένα μη μηδενικό στοιχείο $b \in I$, του οποίου η στάθμη είναι η ελάχιστη δυνατή μεταξύ όλων των μη μηδενικών στοιχείων του I. Δηλαδή,

$$b \neq 0 \quad \& \quad \mathrm{N}(b) \leq \mathrm{N}(a) \quad \forall\, a \in I \setminus \{0\}. \tag{1.20}$$

Θα δείξομε ότι $I = bE$. Προφανώς, αφού $b \in I$, ισχύει ότι $bE \subseteq I$, οπότε μένει να δείξομε ότι κάθε $a \in I$ είναι της μορφής bq με $q \in E$. Επειδή είμαστε σε ευκλείδεια περιοχή, υπάρχουν $q, r \in E$, με $a = bq + r$ και, στην περίπτωση που $r \neq 0$, ισχύει $\mathrm{N}(r) \leq \mathrm{N}(b)$. Παρατηρούμε ότι $r = a - bq \in I$, διότι $a \in I$ και $b \in I$. Αν, λοιπόν, ήταν $r \neq 0$, τότε το r θα ήταν ένα μη μηδενικό στοιχείο του I, με στάθμη $< \mathrm{N}(b)$, κάτι που αντιβαίνει στην (1.20). Άρα $r = 0$ και, συνεπώς, $a = bq$.

Το Θεώρημα 1.3.4 συνεπάγεται, τώρα, ότι η E είναι περιοχή μονοσήμαντης ανάλυσης.

□

Παραδείγματα. **1**. Η ακέραια περιοχή $\mathbb{Z}$ είναι ευκλείδεια, με στάθμη την απεικόνιση

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

2. Αν το K είναι σώμα, τότε η ακέραια περιοχή $K[X]$ είναι ευκλείδεια, με στάθμη την απεικόνιση

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

3. Έστω η ακέραια περιοχή

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

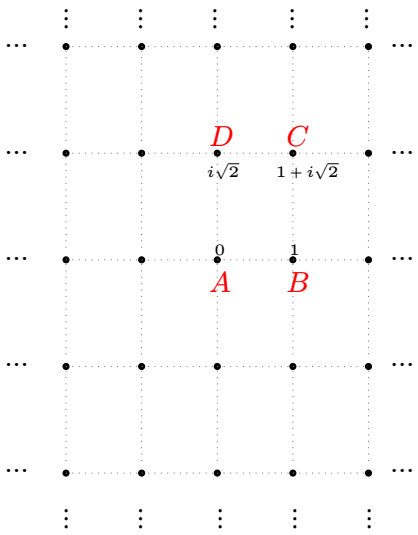
Η απεικόνιση $\mathrm{N} : \mathbb{Z}[\sqrt{-2}] \setminus \{0\} \to \mathbb{N}_0$, που ορίζεται

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

είναι στάθμη και, συνεπώς, από το Θεώρημα 1.3.4 η $\mathbb{Z}[\sqrt{-2}]$ είναι περιοχή μονοσήμαντης ανάλυσης.

Απόδειξη. Η ιδιότητα (1) της στάθμης είναι απλό ν' αποδειχθεί ότι ικανοποιείται από τη συγκεκριμένη απεικόνιση N (άσκηση).

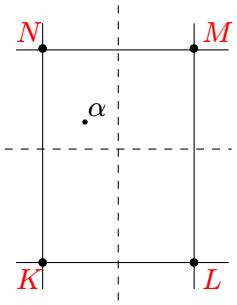
Για ν' αποδείξομε την ιδιότητα (2) απεικονίζομε τα στοιχεία της $\mathbb{Z}[\sqrt{-2}]$ πάνω στο μιγαδικό επίπεδο. Τα στοιχεία αυτά είναι, ακριβώς, οι «κόμβοι» του παρακάτω πλέγματος:



Απεικόνιση της $\mathbb{Z}[\sqrt{-2}]$ στο μιγαδικό επίπεδο

το οποίο προκύπτει από την *επ' άπειρον* οριζόντια και κατακόρυφη επανάληψη του παραλληλογράμμου $ABCD$. Μιά προφανής παρατήρηση, πολύ χρήσιμη, όμως, είναι ότι κάθε σημείο του μιγαδικού επιπέδου ανήκει σε κάποιο από τα ορθογώνια παραλληλόγραμμα (περιλαμβανομένου και του περιγράμματός του).

Τώρα θα δείξομε ότι, η απεικόνιση N, που ορίσαμε πιό πάνω, ικανοποιεί τη συνθήκη (2) του ορισμού της στάθμης.
Έστω ότι $a+bi\sqrt{2}, c+di\sqrt{2} \in E$ με το δεύτερο μη μηδενικό. Θεωρούμε τον μιγαδικό $\alpha = (a+bi\sqrt{2})/(c+di\sqrt{2})$, ο οποίος, σύμφωνα με την παραπάνω παρατήρηση ανήκει σ' ένα από τα παραλληλόγραμμα του πλέγματος, έστω το $KLMN$.



Οι μεσοκάθετες των πλευρών του $KLMN$ το χωρίζουν σε τέσσερα μικρότερα παραλληλόγραμμα και το α ανήκει σ' ένα από αυτά, π.χ. στο άνω αριστερό (βλ. σχήμα). Η απόσταση του α από το πλησιέστερο σημείο του δικτυωτού (πού στο συγκεκριμένο σχήμα είναι το N) δεν μπορεί να υπερβαίνει το μήκος της διαγωνίου του άνω

αριστερού «μικρού» παραλληλογράμμου, η οποία είναι το μισό της διαγωνίου NL. Αλλά η διαγώνιος NL έχει ίσο μήκος με το μήκος της διαγωνίου BD, το οποίο είναι $|1-i\sqrt{2}| = \sqrt{3}$. Άρα, η απόσταση του σημείου α από το N είναι, το πολύ, $\sqrt{3}/2$. Αλλά το σημείο N αναπαριστά ένα στοιχείο της ακέραιας περιοχής, έστω το $u+vi\sqrt{2}$, με $u, v \in \mathbb{Z}$. Συνεπώς $|u+vi\sqrt{2}-\alpha| \leq \sqrt{3}/2$, οπότε

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

Απαλείφοντας τον παρονομαστή παίρνομε τη σχέση

$$|\, a+bi\sqrt{2}-(c+di\sqrt{2})(u+vi\sqrt{2})\,|^2 \leq \frac{3}{4}|\, c+di\sqrt{2}\,|^2 < |\, c+di\sqrt{2}\,|^2 = \mathrm{N}(c+di\sqrt{2}). \tag{1.21}$$

Προφανώς, $a+bi\sqrt{2}-(c+di\sqrt{2})(u+vi\sqrt{2}) = r+si\sqrt{2}$ με τα $r, s \in \mathbb{Z}$.
Αν $r+si\sqrt{2}=0$, τότε $a+bi\sqrt{2} = (c+di\sqrt{2})(u+vi\sqrt{2})$.
Αν $r+si\sqrt{2} \neq 0$, τότε, από τη σχέση (1.21), βλέπομε ότι

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

Άσκηση 1.28 Μιμηθείτε το Παράδειγμα 3 και αποδείξτε ότι η περιοχή $\mathbb{Z}[i]$ (ακέραιοι του Gauss) είναι ευκλείδεια.

Άσκηση 1.29 Έστω $\omega = (-1+i\sqrt{3})/2 \in \mathbb{C}$.
(α') Αποδείξτε ότι ω είναι ρίζα του X^2+X+1 (άρα $\omega^3=1$) και η δεύτερη ρίζα του πολυωνύμου αυτού είναι η ω^2. Συμπεράνατε ότι ο μιγαδικός συζυγής του ω είναι ο ω^2.
(β') Αποδείξτε ότι οι μονάδες της ακέραιας περιοχής $\mathbb{Z}[\omega] = \{a+b\omega : a, b \in \mathbb{Z}\}$ είναι οι $\pm 1, \pm\omega, \pm\omega^2$.
(γ') Αποδείξτε ότι η απεικόνιση $\mathrm{N} : \mathbb{Z}[\omega] \setminus \{0\} \to \mathbb{N}_0$, που ορίζεται

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

είναι στάθμη.

Υπόδειξη. Μιμηθήτε την απόδειξη του παραπάνω Παραδείγματος 3. Αυτή τη φορά, το πλέγμα που θα θεωρήσετε, παράγεται από την επανάληψη του πλαγίου παραλληλογράμμου $ABCD$, όπου τώρα οι κορυφές του έχουν συντεταγμένες 0, 1, $1+\omega$, ω.

Άσκηση 1.30 Σύμφωνα με την άσκηση 1.10 η ακέραια περιοχή $\mathbb{Z}[\sqrt{-5}]$ δεν είναι μονοσήμαντης ανάλυσης, οπότε δεν είναι ευκλείδεια (Θεώρημα 1.6.2). Άρα, αν επιχειρήσετε να μιμηθείτε τη μέθοδο του Παραδείγματος 3, κάπου θα σκοντάψετε· πού;

Πρόταση 1.19 *Οι μόνες ακέραιες λύσεις της εξίσωσης*

$$x^2+2 = y^3 \tag{1.22}$$

είναι οι $(x, y) = (\pm 5, 3)$.

Απόδειξη. Έστω (x, y) ακέραια λύση της (1.22). Τότε ο x είναι περιττός. Διότι, αν ήταν άρτιος, θα ήταν άρτιος και ο y, οπότε θα είχαμε $x = 2x_1$ και $y = 2y_1$ $(x_1, y_1 \in \mathbb{Z})$ και η εξίσωσή μας θα έπαιρνε τη μορφή $4x_1^2 + 2 = 8y_1^3$. Αυτό, όμως, είναι άτοπο, διότι το αριστερό μέλος της τελευταίας σχέσης δεν διαιρείται από το 4, ενώ το δεξιό μέλος της διαιρείται από το 8. Στο εξής, λοιπόν, ο x είναι περιττός.

Η εξίσωση (1.22) γράφεται

$$(x + i\sqrt{2})(x - i\sqrt{2}) = y^3. \tag{1.23}$$

Αποδεικνύομε τώρα ότι οι παράγοντες στο αριστερό μέλος είναι πρώτοι μεταξύ τους (δηλαδή, αποδεικνύομε την άσκηση 1.12 (ε')). Αν δεν ήταν, θα υπήρχε ένα ανάγωγο στοιχείο $\pi \in \mathbb{Z}[\sqrt{-2}]$, που θα διαιρούσε το $x+i\sqrt{2}$ και το $x-i\sqrt{2}$. Τότε, όμως, το π θα διαιρούσε κα' το άθροισμά τους, που είναι $2i\sqrt{2} = -(i\sqrt{2})^3$. Καθώς είμαστε σε περιοχή μονοσήμαντης ανάλυσης, το ανάγωγο π είναι και πρώτο, άρα, από τη σχέση $\pi| - (i\sqrt{2})^3$ συμπεραίνομε ότι $\pi|i\sqrt{2}$. Όμως και το $i\sqrt{2}$ είναι ανάγωγο (άσκηση 1.12 (β')), άρα οι μόνοι πρώτοι διαιρέτες του είναι τα συνεταιρικά του στοιχεία. Συνεπώς, το π είναι συνεταιρικό του $i\sqrt{2}$ και διαιρεί το $x + i\sqrt{2}$. Άρα, το $i\sqrt{2}$ διαιρεί το $x + i\sqrt{2}$, άρα διαιρεί και το $(x + i\sqrt{2}) - i\sqrt{2} = x$. Αυτό σημαίνει ότι υπάρχει $a+bi\sqrt{2} \in E$, τέτοιο ώστε $x = i\sqrt{2}(a+bi\sqrt{2}) = -2b+ai\sqrt{2}$. Η τελευταία σχέση συνεπάγεται $a = 0$ και $x = -2b$, που αντιβαίνει στο γεγονός ότι ο x είναι περιττός.

Ξέροντας τώρα ότι οι παράγοντες στο αριστερό μέλος της (1.23) είναι πρώτοι μεταξύ τους, εφαρμόζομε την Πρόταση 1.4.5 και συμπεραίνομε ότι,

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

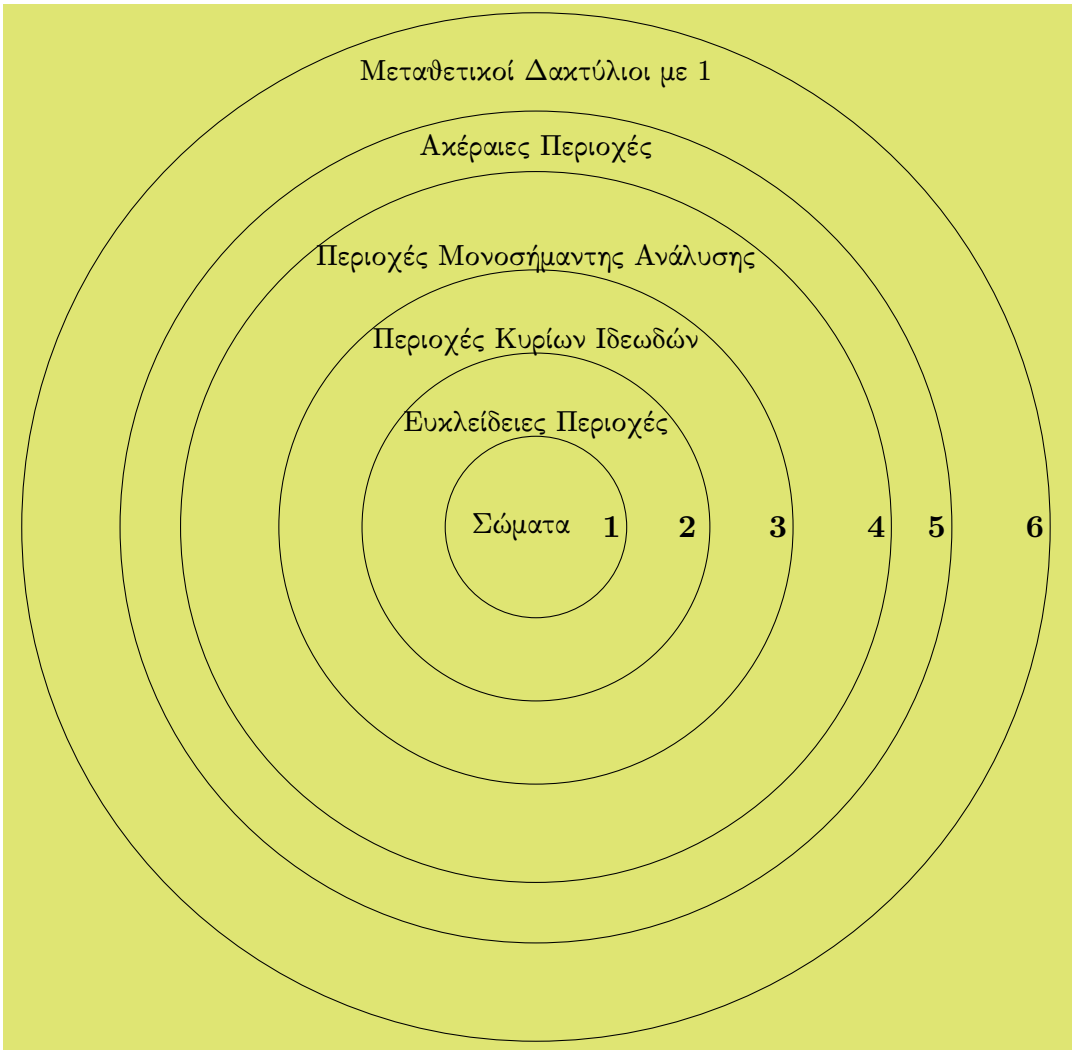
όπου $a, b \in \mathbb{Z}$. Αναπτύσσοντας το δεξιό μέλος και εξισώνοντας πραγματικά και φανταστικά μέρη στα δύο μέλη, παίρνομε

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

Από την πρώτη σχέση, $(3a^2 - 2b^2)b = 1$, άρα $3a^2 - 2b^2 = b = \pm 1$, απ' όπου $a, b \in \{-1, 1\}$ και $x = a^3 - 6ab^2 \in \{-5, 5\}$.

□

Λογική συσχέτιση των κατηγοριών των δομών που συναντήσαμε σε αυτό το κεφάλαιο



- Δομή της κατηγορίας **6** που δεν ανήκει στην κατηγορία **5**: $\mathbb{Z}_m$ με m σύνθετο. Στάνταρ παράδειγμα της Άλγεβρας Ι.
- Δομή της κατηγορίας **5** που δεν ανήκει στην κατηγορία **4**: $\mathbb{Z}[\sqrt{-5}]$. Άσκηση 1.10
- Δομή της κατηγορίας **4** που δεν ανήκει στην κατηγορία **3**: $K[X,Y]$ με το K σώμα. Παράδειγμα 1.5.
- Δομή της κατηγορίας **3** που δεν ανήκει στην κατηγορία **2**: $\mathbb{Z}[\frac{1+\sqrt{-19}}{2}]$. Η απόδειξη των δύο ισχυρισμών πάει πολύ πέρα από τους στόχους του μαθήματος.
- Δομή της κατηγορίας **2** που δεν ανήκει στην κατηγορία **1**: $\mathbb{Z}$. Τετριμμένο.

Κεφάλαιο 2

Εφαρμογές των Ιδεωδών

2.1 Υπαρξη ριζων πολυωνυμου

Πρίν προχωρήσετε στα παρακάτω, μελετήστε τα εισαγωγικά της ενότητας 2.10, μέχρι και το Πόρισμα 2.10.7, του βιβλίου [1].

Πρόταση 2.1 *Έστω σώμα K και $p(X) \in K[X]$ ανάγωγο. Τότε το ιδεώδες $\langle p(X) \rangle$ είναι μεγιστικό ιδεώδες του $K[X]$.*

Απόδειξη. Έστω I ιδεώδες του $K[X]$, που περιέχει το $\langle p(X) \rangle$. Είναι γνωστό ότι τα ιδεώδη του $K[X]$ είναι κύρια, άρα υπάρχει $f(X) \in K[X]$, τέτοιο ώστε $I = \langle f(X) \rangle$. Σύμφωνα με τον ορισμό του μεγιστικού ιδεώδους, πρέπει και αρκεί να δείξομε ότι το $\langle f(X) \rangle$ είναι ίσο ή με το $\langle p(X) \rangle$, ή με ολόκληρο τον δακτύλιο $K[X]$.

Επειδή το $p(X)$ είναι ανάγωγο, το $f(X)$ ή είναι πολλαπλάσιο του $p(X)$, ή είναι πρώτο προς το $p(X)$. Αν συμβαίνει το πρώτο, τότε $f(X) \in \langle p(X) \rangle$, άρα $I = \langle f(X) \rangle \subseteq \langle p(X) \rangle$. Εξ υποθέσεως, όμως, $\langle p(X) \rangle \subseteq I$, άρα $I = \langle p(X) \rangle$. Αν συμβαίνει το δεύτερο, τότε υπάρχουν $h_1(X), h_2(X) \in K[X]$, τέτοια ώστε $h_1(X)f(X) + h_2(X)p(X) = 1$. Το αριστερό μέλος ανήκει στο I, αφού $f(X), p(X) \in I$, άρα $1 \in I$. Τότε, όμως, για κάθε $g(X) \in K[X]$ έχομε ότι $g(X) \cdot 1 \in I$, άρα όλα τα πολυώνυμα του $K[X]$ ανήκουν στο I, οπότε $I = K[X]$.

□

Θεώρημα 2.2 *Έστω K σώμα και $p(X) \in K[X]$ ανάγωγο, βαθμού n. Τότε υπάρχει σώμα L, που περιέχει ως υπόσωμά του το K, και $u \in L$, έτσι ώστε:*

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

Απόδειξη. Από την Πρόταση 2.1.1, το ιδεώδες $\langle p(X) \rangle$ είναι μεγιστικό, άρα ο δακτύλιος-πηλίκο $L = K[X]/\langle p(X) \rangle$ είναι σώμα (βλ. Θεώρημα 2.10.6 του [1]. Για να ελαφρύνομε τον συμβολισμό, θέτομε $\langle p(X) \rangle = I$.

Θεωρούμε τον ομομορφισμό σωμάτων $K \ni c \mapsto c + I \in K/I = L$. Είναι απλούστατο ν" αποδείξει κανείς ότι αυτή η απεικόνιση είναι *μονο*μορφισμός, άρα, το L περιέχει ένα ισόμορφο αντίγραφο του K. Συνεπώς, όπως έχομε εξηγήσει στο μάθημα, μπορούμε να θεωρήσομε ότι το K περιέχεται στο L και να ταυτίσομε κάθε στοιχείο $c \in K$ με το $c + I \in L$.

Τη μεταβλητή των πολυωνύμων με συντελεστές από το L τη συμβολίζομε με Y, προς αποφυγή συγχύσεως. Άρα, αν το $p(X) =$ (έστω) $a_0 + a_1X + \cdots + a_nX^n \in K[X]$ το βλέπομε ως πολυώνυμο πάνω από το L, θα το γράφομε

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

Το στοιχείο $X + I \in L$ το συμβολίζομε u και υπολογίζομε:

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

(είναι $p(X) + I = 0 + I$ διότι $p(X) \in \langle p(X) \rangle = I$), άρα το $u \in L$ είναι ρίζα του πολυωνύμου $p(Y) \in L[Y]$. Έτσι αποδείχθηκε ο πρώτος ισχυρισμός του θεωρήματος.

Έστω τώρα ένα τυχόν στοιχείο του L. Αυτό είναι της μορφής $f(X) + I$, όπου $f(X) \in K[X]$. Εκτελούμε την ευκλείδεια διαίρεση του $f(X)$ δια $p(X)$ και έστω $f(X) = p(X)q(X) + r(X)$, όπου $q(X), r(X) \in K[X]$ και $\deg r(X) < \deg p(X)$, άρα $r(X) = c_0 + c_1X + \cdots + c_{n-1}X^{n-1}$, με τα $c_0, c_1, \ldots, c_{n-1} \in K$. Τώρα υπολογίζομε (σύμφωνα με τα σχόλια στην αρχή της απόδειξης, μπορούμε να ταυτίσομε τα $c_i \in K$ με τα $c_i + I \in L$):

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

Έτσι ολοκληρώσαμε και την απόδειξη του δεύτερου ισχυρισμού.

□

Άσκηση 2.1 Με τον συμβολισμό της εκφώνησης του Θεωρήματος 2.1.2, αποδείξτε ότι, αν $c_0 + c_1u + \cdots + c_{n-1}u^{n-1} = d_0 + d_1u + \cdots + d_{n-1}u^{n-1}$, με τα $c_0, c_1, \ldots, c_{n-1}, d_0, d_1, \ldots, d_{n-1} \in K$, τότε $c_i = d_i$ για κάθε $i = 0, 1, \ldots, n-1$.

Υπόδειξη. Αν υπάρχουν $i \in \{0, 1, \ldots, n-1\}$, τέτοια ώστε $c_i \neq d_i$, τότε το πολυώνυμο $f(X) = \sum_{i=0}^{n-1}(c_i - d_i)X^i$ είναι μη μηδενικό, βαθμού $\leq \deg p(X)$, και έχει ρίζα το u. Το ανάγωγο $p(X)$ δεν

διαιρεί το $f(X)$ (λόγω βαθμών), άρα, είναι πρώτο προς το $f(X)$. Συνεπώς, υπάρχουν $g(X), q(X) \in K[X]$, τέτοια ώστε $g(X)f(X) + q(X)p(X) = 1$. Γιατί αυτή η σχέση είναι αδύνατη?

Άσκηση 2.2 Βασισμένοι στο Θεώρημα 2.1.2, περιγράψτε ένα σώμα με ακριβώς 8 στοιχεία. Ύστερα κατασκευάστε τον πίνακα πρόσθεσης και τον πίνακα πολλαπλασιασμού του σώματος L.

Υπόδειξη. Εφαρμόζοντας το Θεώρημα 2.1.2 με $K = \mathbb{Z}_2$ και $p(X) = X^3 + X + 1 \in \mathbb{Z}_2[X]$ (παρατηρήστε ότι το $p(X)$ είναι ανάγωγο), βλέπομε ότι υπάρχει σώμα L, που περιέχει το $\mathbb{Z}_2$ ως υπόσωμά του και ένα στοιχείο $u \in L$, τέτοιο ώστε $p(u) = 0$ και $L = \{c_0 + c_1u + c_2u^2 | c_0, c_1, c_2 \in \mathbb{Z}_2\}$. Καθώς έχομε δύο επιλογές για κάθε c_i, οι συνολικές επιλογές για το $c_0 + c_1u + c_2u^2$ είναι $2 \cdot 2 \cdot 2 = 8$. Κάθε μία από τις 8 διαφορετικές επιλογές (c_0, c_1, c_2) δίνει διαφορετικό στοιχείο $c_0 + c_1u + c_2u^2$, σύμφωνα με την άσκηση 2.1.
Για να φτιάξομε τους πίνακες των πράξεων παρατηρούμε ότι $u^3+u+1 = 0$, άρα, $u^3 = -u-1 = u+1$, οπότε, π.χ., $(u^2 + 1) + (u + 1) = u^2 + u + 2 = u^2 + u$ και $(u^2 + 1)(u + 1) = u^3 + u^2 + u + 1 = (u + 1) + u^2 + u + 1 = u^2 + 2u + 2 = u^2$.

2.2 Απαλειφουσα

Πρόταση 2.3 *Έστω ακέραια περιοχή D. Αν τα $f(X), g(X) \in D[X]$ δεν έχουν μη σταθερό κοινό διαιρέτη, τότε, θεωρούμενα ως πολυώνυμα του $Q(D)[X]$ [1] είναι πρώτα μεταξύ τους.*

Απόδειξη. Για ν" απλοποιήσομε τον συμβολισμό μας, ας θέσομε $Q(D) = K$. Έστω ότι τα $f(X), g(X)$ δεν είναι πρώτα μεταξύ τους στο $K[X]$. Αυτό σημαίνει ότι υπάρχει μη σταθερό $d(X) \in K[X]$, και πολυώνυμα $f_1(X), g_1(X) \in K[X]$, τέτοια ώστε

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

Σκοπός μας είναι να καταλήξομε σε άτοπο.

Εφαρμόζομε το Λήμμα 1.5.1 στα πολυώνυμα $d(X), f_1(X), g_1(X)$ και συμπεραίνομε ότι υπάρχουν $\delta, \alpha, \beta \in K$ και πρωταρχικά πολυώνυμα $d_1(X), h_1(X), h_2(X) \in D[X]$, έτσι ώστε

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

Επίσης, αν a είναι το περιεχόμενο του $f(X)$ (ΜΚΔ των συντελεστών του) και b είναι το περιεχόμενο του $g(X)$, 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 τις σχέσεις (2.3), (2.2), (2.1), καταλήγομε εύκολα στις σχέσεις

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

[1] Υπενθύμιση: $Q(D)$ είναι το σώμα πηλίκων της D

Από το Θεώρημα 1.5.2, τα $d_1(X)h_1(X)$ και $d_1(X)h_2(X)$ είναι πρωταρχικά πολυώνυμα της $D[X]$, άρα, λόγω του Λήμματος 1.5.1,

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

Αυτές είναι σχέσεις στην ακέραια περιοχή $D[X]$, οι οποίες δείχνουν ότι το $d_1(X) \in D[X]$ διαιρεί τα $f'(X), g'(X)$, άρα διαιρεί και τα $f(X), g(X)$, και αυτό αντιβαίνει στην υπόθεση.

□

Θεώρημα 2.4 *Έστω σώμα K και $f(X,Y), g(X,Y) \in K[X,Y]$, που δεν έχουν κοινό μη σταθερό διαιρέτη. Τότε το σύστημα των εξισώσεων*

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

έχει πεπερασμένο, το πολύ, πλήθος λύσεων.

Απόδειξη. Θέτομε $K[Y] = D$, οπότε $K[X,Y] = (K[Y])[X] = D[X]$ και τα $f(X,Y), g(X,Y)$ τα βλέπομε ως πολυώνυμα του $D[X]$ (δηλαδή, πολυώνυμα του X με συντελεστές πολυώνυμα $\in K[Y]$).

Εφαρμόζοντας την Πρόταση 2.2.1, συμπεραίνομε ότι υπάρχουν $h_i(X) \in Q(D)[X]$ $(i = 1, 2)$, τέτοια ώστε

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

Ας δούμε τώρα ποια είναι τα στοιχεία του σώματος $Q(D)$. Αφού η D είναι η ακέραια περιοχή των πολυωνύμων μεταβλητής Y, με συντελεστές στο K, έπεται ότι το σώμα πηλίκων της αποτελείται από *πηλίκα* πολυωνύμων της μορφής $q(Y)/r(Y)$, όπου $q(Y), r(Y) \in K[Y]$, $r(Y) \neq 0$. Άρα, για $i \in \{1,2\}$, το $h_i(X)$ είναι της μορφής

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

Αν θέσομε $s_i(Y) = r_0(Y)r_1(Y)\cdots r_m(Y)$, τότε βλέπομε ότι $h_i(X)s_i(Y) = \ell_i(X,Y) \in K[X,Y]$. Πολλαπλασιάζοντας τα δύο μέλη της (2.4) επί $s_1(Y)s_2(Y)$, παίρνομε τη σχέση

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

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

Έστω τώρα $(a,b) \in K^2$, τέτοιο ώστε $f(a,b) = 0 = g(a,b)$. Η αντικατάσταση $(a,b) \leftarrow (X,Y)$ στη (2.5), δίνει $h_1(b)h_2(b) = t_1(a,b)f(a,b) + t_2(a,b)g(a,b) = 0$,

οπότε βλέπομε ότι το b είναι ρίζα του πολυωνύμου $h_1(Y)h_2(Y)$. Κάθε μη μηδενικό πολυώνυμο, όμως, του $K[Y]$ έχει πεπερασμένες το πλήθος ρίζες μέσα στο K, άρα οι πιθανές τιμές του b είναι πεπερασμένες το πλήθος, έστω $b_1, \ldots b_k$. Κάθε εξίσωση $f(a, b_i) = 0$ έχει πεπερασμένες το πλήθος λύσεις ως προς a, άρα, τελικά, πεπερασμένα το πλήθος ζεύγη $(a, b) \in K^2$ είναι δυνατόν να ικανοποιούν συγχρόνως $f(a, b) = 0$ και $g(a, b) = 0$.

□

Απαλείφουσα. Στη σχέση (2.5), έστω $R_X(f, g) = h_1(Y)h_2(Y)$. Το πολυώνυμο αυτό καλείται *απαλείφουσα των f, g, ως προς X* και ο υποδείκτης $_X$ υποδηλώνει ότι το πολυώνυμο είναι απαλλαγμένο από τη μεταβλητή X, άρα είναι πολυώνυμο $\in K[Y]$. Είδαμε στην απόδειξη του Θεωρήματος 2.2.2 ότι,

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

Λόγω του συμμετρικού ρόλου των μεταβλητών X, Y στο θεώρημα, θα μπορούσαμε, εντελώς ανάλογα, να αποδείξομε ότι υπάρχει πολυώνυμο $R_Y(f, g) \in K[X]$, τέτοιο ώστε

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

το οποίο καλείται *απαλείφουσα των f, g, ως προς Y*

Το ερώτημα είναι: Στην πράξη, αν μας δοθούν τα f, g, πώς μπορούμε να υπολογίσομε το $R_X(f, g)$ ή το $R_Y(f, g)$? Δίχως να κάνομε ανάπτυξη της σχετικής θεωρίας, δίνομε ένα παράδειγμα πρακτικού υπολογισμού.

Παράδειγμα. Θεωρούμε τα πολυώνυμα $f(X, Y) = 3X^2 + Y^2 - 13$ και $g(X, Y) = X^3 - X^2Y - 4$ πάνω από το $\mathbb{R}$ και θα υπολογίσομε την απαλείφουσα $R_Y(f, g)$.
Έστω $f(a, b) = 0 = g(a, b)$. Τότε $b^2 + (3a^2 - 13) = 0$ και $-a^2b + (a^3 - 4) = 0$. Πολλαπλασιάζοντας επί b τη δεύτερη, παίρνομε άλλη μία σχέση, τη $-a^2b^2 + (a^3 - 4)b = 0$. Γράφομε τις τρεις σχέσεις, διατάσσοντάς τις κατά τις κατιούσες δυνάμεις του b:

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

Με χρήση πινάκων, το παραπάνω σύστημα γράφεται ως γραμμικό σύστημα

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

το οποίο έχει μη μηδενική λύση $(b^2, b, 1)$, άρα η ορίζουσα των συντελεστών πρέπει να είναι μηδενική. Έτσι,

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

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

Είναι $R_Y(f,g)(2) = 0$. Η εξίσωση $f(2,b) = 0$ μας δίνει $b^2 = 1$, άρα $b = \pm 1$. Από τα δύο ζεύγη $(a,b) = (2,1), (2,-1)$, μόνο το πρώτο επαληθεύει την $g(a,b) = 0$.

2.3 Μικρη Εισαγωγη στην Αλγεβρικη Γεωμετρια

Σε όλη την παρούσα ενότητα, K είναι σώμα. Τα σύμβολα $f, g, h, \ldots$ με ή χωρίς υποδείκτες θα συμβολίζουν πολυώνυμα $\in K[X_1, \ldots, X_n]$. Συνήθως θα γράφομε, για παράδειγμα, f αντί $f(X_1, \ldots, X_n)$. Με K^n συμβολίζομε το καρτεσιανό γινόμενο $\underbrace{K \times \cdots \times K}_{n}$

Ορισμός. Έστω $S \subseteq K[X_1, \ldots, X_n]$. Ορίζομε

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

Τα υποσύνολα του K^n αυτής της μορφής χαρακτηρίζονται *αλγεβρικά σύνολα*. Δηλαδή, το $A \subseteq K^n$ χαρακτηρίζεται αλγεβρικό σύνολο, αν υπάρχει υποσύνολο S του $K[X_1, \ldots, X_n]$ (όχι, κατ" ανάγκη πεπερασμένο), έτσι ώστε $A = \mathbb{V}(S)$. Στην περίπτωση που $S = \{f\}$, γράφομε απλώς $\mathbb{V}(f)$ αντί $\mathbb{V}(\{f\})$. Ένα σύνολο της μορφής $\mathbb{V}(f)$ χαρακτηρίζεται *υπερεπιφάνεια* . Στην ειδική περίπτωση $n = 3$, το $\mathbb{V}(f)$ λέγεται απλώς *επιφάνεια* – παραλείπεται, δηλαδή, το πρόθεμα ((υπέρ)) –, ενώ στην περίπτωση $n = 2$, το $\mathbb{V}(f)$ λέγεται *καμπύλη*.

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

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

Άσκηση 2.4 $\mathbb{V}(S_1 \cup S_2) = \mathbb{V}(S_1) \cap \mathbb{V}(S_2)$. Άρα, η τομή αλγεβρικών συνόλων είναι αλγεβρικό σύνολο.

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

Άσκηση 2.6 Αποδείξτε ότι κάθε μονοσύνολο του K^n είναι αλγεβρικό σύνολο. Δείξτε ότι, αν $(a_1, \ldots, a_n) \in K^n$, τότε $\{(a_1, \ldots, a_n)\} = \mathbb{V}(\{X_1 - a_1, \ldots, X_n - a_n\})$.

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

[2] Αυτό δικαιολογείται ως εξής: Σε αυστηρά τυπική γλώσσα, το $(a_1, \ldots, a_n)$ είναι στοιχείο του $\mathbb{V}(S)$ αν και μόνο αν η εξής συνεπαγωγή είναι αληθής: $f \in S \Rightarrow f(a_1, \ldots, a_n) = 0$. Άρα, στην περίπτωση που $S = \emptyset$, το $(a_1, \ldots, a_n)$ ανήκει στο $\mathbb{V}(\emptyset)$ αν και μόνο αν η εξής συνεπαγωγή είναι αληθής: $f \in \emptyset \Rightarrow f(a_1, \ldots, a_n) = 0$. Αλλά η πρόταση $f \in \emptyset$ είναι ψευδής και στα Μαθηματικά δεχόμαστε ότι μιά συνεπαγωγή $\Pi_1 \Rightarrow \Pi_2$, με Π_1 ψευδή πρόταση και Π_2 οποιαδήποτε πρόταση, είναι αληθής.

[3] Υπενθύμιση: $\langle S \rangle$ είναι το ιδεώδες που παράγεται από το S, άρα $\langle S \rangle = \{\sum_i h_i \cdot f_i\}$, με το i να διατρέχει πεπερασμένο σύνολο δεικτών, τα $f_i \in S$ και τα $h_i \in K[X_1, \ldots, X_n]$.

Απόδειξη. Είναι $S \subseteq \langle S\rangle$, άρα, από την άσκηση 2.3, $\mathbb{V}(S) \supseteq \mathbb{V}(\langle S\rangle)$. Αντιστρόφως, θα δείξομε ότι, αν $(a_1, \dots, a_n) \in \mathbb{V}(S)$, τότε $(a_1, \dots, a_n) \in \mathbb{V}(\langle S\rangle)$. Για την απόδειξη της τελευταίας σχέσης, θεωρούμε $g \in \langle S\rangle$ και θ" αποδείξομε ότι $g(a_1, \dots, a_n) = 0$. Αλλά $g \in \langle S\rangle$ σημαίνει ότι υπάρχουν $f_1, \dots, f_r \in S$ και $h_1, \dots, h_r \in K[X_1, \dots, X_n]$, τέτοια ώστε $g = \sum_{i=1}^{r} h_i f_i$. Επειδή τα $f_i \in S$ και το $(a_1, \dots, a_n) \in \mathbb{V}(S)$, έπεται ότι $f_i(a_1, \dots, a_n) = 0$ για κάθε i, άρα $g(a_1, \dots, a_n) = \sum_i h(a_1, \dots, a_n) f(a_1, \dots, a_n) = 0$.

□

Ορισμός. Έστω $A \subseteq K^n$. Ορίζομε

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

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

Πρόταση 2.6 *Αν $A \subseteq K^n$, τότε το $\mathbb{I}(A)$ είναι ιδεώδες του $K[X_1, \dots, X_n]$.*

Απόδειξη. Κατ" αρχάς, το $\mathbb{I}(A)$ είναι μη κενό διότι περιέχει το μηδενικό πολυώνυμο. Μετά έχομε να δείξομε τα εξής:

(α') Αν $f \in \mathbb{I}(A)$ και $h \in K[X_1, \dots, X_n]$, τότε $h \cdot f \in \mathbb{I}(A)$. Αυτό είναι προφανές, διότι η υπόθεση $f \in \mathbb{I}(A)$ σημαίνει ότι $f(a_1, \dots, a_n) = 0$ για κάθε $(a_1, \dots, a_n) \in A$, οπότε και $h(a_1, \dots, a_n) f(a_1, \dots, a_n) = 0$ για κάθε $(a_1, \dots, a_n) \in A$. Αυτό το τελευταίο συμπέρασμα, όμως, σημαίνει ότι $h \cdot f \in \mathbb{I}(A)$.

(β') Αν $f_i \in \mathbb{I}(A)$ $(i = 1, 2)$, τότε $f_1 - f_2 \in \mathbb{I}(A)$. Η απόδειξη είναι εξίσου απλή: Από την υπόθεση, για $i = 1, 2$ έχομε ότι $f_i(a_1, \dots, a_n) = 0$ για όλα τα $(a_1, \dots, a_n) \in A$. Αλλά τότε, για κάθε $(a_1, \dots, a_n) \in A$, έχομε $(f_1 - f_2)(a_1, \dots, a_n) = f_1(a_1, \dots, a_n) - f_2(a_1, \dots, a_n) = 0 - 0 = 0$.

□

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

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

Άσκηση 2.9 Για κάθε $f \in K[X_1, \dots, X_n]$ ισχύει $\langle f\rangle \subseteq \mathbb{I}(\mathbb{V}(f))$.

Πρόταση 2.7 (α') *Για κάθε $S \subseteq K[X_1, \dots, X_n]$ ισχύει $\mathbb{I}(\mathbb{V}(S)) \supseteq S$.*
(β') *Για κάθε $A \subseteq K^n$ ισχύει $\mathbb{V}(\mathbb{I}(A)) \supseteq A$.*

Απόδειξη. (α') Έστω $f \in S$. Θα δείξομε ότι $f \in \mathbb{I}(\mathbb{V}(S))$. Αυτό ισοδυναμεί με το να δείξομε ότι, αν $(a_1, \dots, a_n) \in \mathbb{V}(S)$, τότε $f(a_1, \dots, a_n) = 0$. Αλλά $(a_1, \dots, a_n) \in \mathbb{V}(S)$ σημαίνει ότι το $(a_1, \dots, a_n)$ μηδενίζει κάθε πολυώνυμο $\in S$, άρα (αφού $f \in S$), έπεται ότι $f(a_1, \dots, a_n) = 0$, που είναι η αποδεικτέα σχέση.

[4] Αιτιολόγηση εντελώς ανάλογη με αυτή που δώσαμε για τη σχέση $\mathbb{V}(\emptyset) = K^n$; βλ. υποσημείωση στη σελ.38.

(β') Έστω $(a_1, \dots, a_n) \in A$. Θα δείξομε ότι $(a_1, \dots, a_n) \in \mathbb{V}(\mathbb{I}(A))$. Αυτό ισοδυναμεί με το να δείξομε ότι, αν $f \in \mathbb{I}(A)$, τότε $f(a_1, \dots, a_n) = 0$. Αλλά $f \in \mathbb{I}(A)$ σημαίνει ότι το f μηδενίζεται από κάθε n-άδα $\in A$, άρα (αφού $(a_1, \dots, a_n) \in A$) έπεται ότι $f(a_1, \dots, a_n) = 0$, που είναι η αποδεικτέα σχέση.

□

Πόρισμα 2.8 (α') *Αν το $A \subseteq K^n$ είναι αλγεβρικό σύνολο, τότε $\mathbb{V}(\mathbb{I}(A)) = A$.*
(β') *Αν το J είναι ιδεώδες αλγεβρικού υποσυνόλου του K^n, τότε $\mathbb{I}(\mathbb{V}(J)) = J$.*

Απόδειξη. (α') Εξ υποθέσεως, $A = \mathbb{V}(S)$ για κάποιο $S \subseteq K[X_1, \dots, X_n]$. Από την Πρόταση 2.3.3 (α') έχομε $\mathbb{I}(A) = \mathbb{I}(\mathbb{V}(S)) \supseteq S$, άρα, από την άσκηση 2.3, $\mathbb{V}(\mathbb{I}(A)) \subseteq \mathbb{V}(S) = A$. Όμως, την από την Πρόταση 2.3.3 (β'), ισχύει και η σχέση $\mathbb{V}(\mathbb{I}(A)) \supseteq A$, άρα $\mathbb{V}(\mathbb{I}(A)) = A$.
(β') Εξ υποθέσεως, $J = \mathbb{I}(A)$ για κάποιο αλγεβρικό σύνολο $A \subseteq K^n$, άρα $\mathbb{V}(J) = \mathbb{V}(\mathbb{I}(A)) = A$, λόγω του (α') που μόλις αποδείξαμε. Άρα, $\mathbb{I}(\mathbb{V}(J)) = \mathbb{I}(A) = J$.

□

Ορισμός. Έστω R μεταθετικός δακτύλιος με μοναδιαίο. Ο R λέμε ότι είναι δακτύλιος Noether αν κάθε ιδεώδες του είναι πεπερασμένα παραγόμενο, δηλαδή, αν για κάθε ιδεώδες J του R υπάρχουν $j_1, \dots, j_m \in J$, τέτοια ώστε $J = \langle j_1, \dots, j_m \rangle$.[5]

Παρατήρηση. Στην περίπτωση που ο δακτύλιος είναι σώμα K, τα μόνα ιδεώδη είναι το μηδενικό $\{0\} = \langle 0 \rangle$ και ολόκληρος ο δακτύλιος $K = \langle 1 \rangle$, άρα, τετριμμένα, κάθε σώμα είναι δακτύλιος Noether.

Θεώρημα 2.9 *Έστω ότι ο R είναι μεταθετικός δακτύλιος με μοναδιαίο και είναι δακτύλιος Noether. Τότε και ο $R[X]$ είναι δακτύλιος Noether.*

Απόδειξη. Σ" αυτή την απόδειξη, αν $f \in KX$, θα συμβολίζομε με $\text{ΣΜΟ}(f)$ τον συντελεστή του μεγιστοβαθμίου όρου του f. Για το μηδενικό πολυώνυμο θέτομε $\text{ΣΜΟ}(0) = 0$.

Έστω I μη μηδενικό ιδεώδες του $R[X]$. Θα αποδείξομε ότι το I είναι πεπερασμένα παραγόμενο ιδεώδες. Προς τούτο θεωρούμε το ιδεώδες J, όπως στην άσκηση 2.10, το οποίο, εξ υποθέσεως, είναι πεπερασμένα παραγόμενο, έστω $J = \langle a_1, \dots, a_r \rangle$. Αυτό σημαίνει ότι υπάρχουν $f_1, \dots, f_r \in I$, τέτοια ώστε $a_i = \text{ΣΜΟ}(f_i)$ για $i = 1, \dots, r$.
Σταθεροποιούμε τώρα έναν ακέραιο $N > \max_{1 \le i \le r} \deg f_i$ και για κάθε $m \le N$ ορίζομε

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

Προφανώς, το J_m είναι ιδεώδες του R, άρα είναι πεπερασμένα παραγόμενο, έστω $J_m = \langle a_{m,1}, \dots, a_{m,r_m} \rangle$, όπου κάθε $a_{m,i} = \text{ΣΜΟ}(f_{m,i})$ για κάποιο $f_{m,i} \in I$ με $\deg f_{m,i} \le m$.

[5] $\langle j_1, \dots, j_m \rangle \stackrel{\text{def}}{=} \{r_1 j_1 + \cdots r_m j_m : r_1, \dots, r_m \in R\}$.

Τέλος, ορίζομε

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

και ϑ" αποδείξομε ότι $I = I'$, οπότε ϑα έχομε δείξει ότι το I είναι πεπερασμένα παραγόμενο και η απόδειξη ϑα έχει ολοκληρωθεί.
Από τον ορισμό του I' ξέρομε ήδη ότι $I' \subseteq I$. Θα υποθέσομε ότι στην τελευταία σχέση δεν ισχύει το $=$ και ϑα οδηγηθούμε σε άτοπο. Έστω $g \in I \setminus I'$ και ο βαθμός d του g είναι ο ελάχιστος δυνατός, δηλαδή, κάθε πολυώνυμο του $I \setminus I'$ είναι βαθμού $\geq d$. Διακρίνομε δύο περιπτώσεις.
Περίπτωση πρώτη; $d > N$. Τότε, λόγω της επιλογής του N, είναι $d > \deg f_i$, οπότε, επιλέγοντας κατάλληλα $c_1, \dots, c_r \in R$ μπορούμε να κάνομε το πολυώνυμο $h = \sum_{i=1}^{r} c_i f_i(X) X^{d-\deg f_i}$ να έχει συντελεστή του X^d ίσο με τον συντελεστή του X^d στο g, άρα $\text{ΣΜΟ}(h) = \text{ΣΜΟ}(g)$. Όμως, το h είναι πολυώνυμο του ιδεώδους I, άρα $g - h \in I$ και $\deg(g-h) < d$, άρα, λόγω της επιλογής του d, συμπεραίνομε ότι $g - h \notin I \setminus I'$, δηλαδή, $g - h \in I'$. Αλλά $h \in I'$ (βλ. ορισμό του I' στην (2.6)), άρα και $g \in I'$, σε αντίφαση με την επιλογή του g.
Περίπτωση δεύτερη; $d = m \leq N$. Τότε επιλέγομε κατάλληλα $c_1, \dots, c_{r_m} \in R$ έτσι ώστε το πολυώνυμο $h = \sum_{i=1}^{r_m} c_i X^{m-\deg f_{m,i}} f_{m,i}(X)$ να έχει συντελεστή του X^m ίσο με τον συντελεστή του X^m στο πολυώνυμο g. Τότε, κατ" αναλογίαν με την προηγούμενη περίπτωση, $g - h \in I$ και $\deg(g-h) < m = d$, άρα $g - h \notin I \setminus I'$. Αυτό σημαίνει ότι $g - h \in I'$, άρα (δεδομένου ότι $h \in I'$) $g \in I'$; αντίφαση.

□

Πόρισμα 2.10 - ***Θεώρημα Βάσεως του Hilbert.*** *Έστω ότι ο R είναι μεταθετικός δακτύλιος με μοναδιαίο και είναι δακτύλιος Noether. Τότε, για οποιοδήποτε $n \in \mathbb{N}$, ο $R[X_1, \dots, X_n]$ είναι δακτύλιος Noether. Ειδικώτερα, για κάθε σώμα K, ο $K[X_1, \dots, X_n]$ είναι δακτύλιος Noether.*

Απόδειξη. Εφαρμόζοντας το Θεώρημα 2.3.5 συμπεραίνομε ότι ο $R[X_1]$ είναι δακτύλιος Noether. Εφαρμόζοντας ξανά το ίδιο ϑεώρημα, αλλά με τον δακτύλιο $R[X_1]$ στη ϑέση του R και τη μεταβλητή X_2 στη ϑέση της μεταβλητής X, συμπεραίνομε ότι και ο δακτύλιος $(R[X_1])[X_2]$ –δηλαδή, ο $R[X_1, X_2]$– είναι δακτύλιος Noether. Εφαρμόζοντας το Θεώρημα 2.3.5 στον δακτύλιο $R[X_1, X_2]$ και τη μεταβλητή X_3, συμπεραίνομε ότι ο $R[X_1, X_2, X_3]$ είναι δακτύλιος Noether, κ.ο.κ.

□

Άσκηση 2.10 Έστω R μεταθετικός δακτύλιος με μοναδιαίο, I ιδεώδες του δακτυλίου $K[X]$ και $J = \{a \in R : \exists\, f \in I$ γιά το οποίο $a = \text{ΣΜΟ}(f)\}$.[6] Αποδείξτε ότι το J είναι ιδεώδες του R.

[6]Γιά τον συμβολισμό ΣΜΟ() δείτε την αρχή της απόδειξης του Θεωρήματος 2.3.5.

Υπόδειξη. Για να δείξετε ότι, αν $a, b \in J$ τότε και $a + b \in J$: Έστω ότι $a = \text{ΣΜΟ}(f)$, $b = \text{ΣΜΟ}(g)$ και m, n οι βαθμοί των f, g, αντιστοίχως. Θεωρήστε το πολυώνυμο $X^n f(X) + X^m g(X)$.

Θεώρημα 2.11 *Κάθε αλγεβρικό σύνολο του K^n είναι τομή πεπερασμένου πλήθους υπερεπιφανειών.*[7]

Απόδειξη. Έστω αλγεβρικό σύνολο $A \subseteq K^n$. Αυτό σημαίνει ότι $A = \mathbb{V}(S)$ για κάποιο $S \subseteq K[X_1, \dots, X_n]$. Από την Πρόταση 2.3.1 ξέρομε ότι $\mathbb{V}(S) = \mathbb{V}(\langle S \rangle)$ και το Θεώρημα 2.3.6 μας λέει ότι υπάρχει πεπερασμένο πλήθος πολυωνύμων $f_1, \dots, f_m \in K[X_1, \dots, X_n]$, έτσι ώστε να ισχύει $\langle S \rangle = \langle f_1, \dots, f_m \rangle$. Άρα,

$$\begin{aligned} A = \mathbb{V}(\langle f_1, \dots, f_m \rangle) &= \text{ (από την Πρόταση 2.3.1) } \mathbb{V}(\{f_1, \dots, f_m\}) \\ &= \mathbb{V}(\{f_1\} \cup \dots \cup \{f_m\}) = \text{ (από την άσκηση 2.8) } \mathbb{V}(f_1) \cap \dots \cap \mathbb{V}(f_m). \end{aligned}$$

Εξ ορισμού, κάθε $\mathbb{V}(f_i)$ είναι μιά υπερεπιφάνεια, άρα η απόδειξη είναι πλήρης.

□

Ορισμός. Έστω αλγεβρικό σύνολο $A \subseteq K^n$. Αν είναι αδύνατον να βρεθούν αλγεβρικά σύνολα A_1, A_2, τα οποία είναι *γνήσια* υποσύνολα του A και $A_1 \cup A_2 = A$, τότε το A χαρακτηρίζεται ανάγωγο αλγεβρικό σύνολο.

Θεώρημα 2.12 *Το αλγεβρικό σύνολο $A \subseteq K^n$ είναι ανάγωγο αν και μόνο αν το $\mathbb{I}(A)$ είναι πρώτο ιδεώδες του $K[X_1, \dots, X_n]$.*

Απόδειξη. Έστω ότι το $\mathbb{I}(A)$ δεν είναι πρώτο ιδεώδες του $K[X_1, \dots, X_n]$. Τότε, θα δείξομε ότι το A δεν είναι ανάγωγο αλγεβρικό σύνολο. Εξ υποθέσεως, υπάρχουν $f_1, f_2 \in K[X_1, \dots, X_n]$, τα οποία δεν ανήκουν στο $\mathbb{I}(A)$, αλλά το γινόμενό τους $f_1 f_2 \in \mathbb{I}(A)$. Η σχέση $f_1 \notin \mathbb{I}(A)$ σημαίνει ότι υπάρχει $(a_1, \dots, a_n) \in A$, τέτοιο ώστε $f(a_1, \dots, a_n) \neq 0$, οπότε το $(a_1, \dots, a_n) \notin \mathbb{V}(f_1)$ και, συνεπώς, $A \cap \mathbb{V}(f_1) \subsetneq A$. Εντελώς ανάλογα, $A \cap \mathbb{V}(f_2) \subsetneq A$. Χρησιμοποιώντας τώρα τη συνολοθεωρητική ταυτότητα $(\mathbb{A} \cap \mathbb{B}) \cup (\mathbb{A} \cap \mathbb{C}) = \mathbb{A} \cap (\mathbb{B} \cup \mathbb{C})$ συμπεραίνομε ότι

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

Το δεξιώτερο μέλος της παραπάνω σχέσης ισούται με A. Πράγματι, εξ υποθέσεως, $f_1 f_2 \in \mathbb{I}(A)$, άρα $\{f_1 f_2\} \subseteq \mathbb{I}(A)$ οπότε

$$\mathbb{V}(f_1 f_2) \supseteq \text{ (άσκηση 2.3) } \mathbb{V}(\mathbb{I}(A)) = \text{(Πόρισμα 2.3.4) } A$$

άρα $\mathbb{V}(f_1 f_2) \cap A = A$ και, συνεπώς, απ" την (2.7),

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

[7] Βλ. Ορισμό 2.3.

Έτσι, το A γράφτηκε ως ένωση δύο γνησίων (όπως είδαμε παραπάνω) υποσυνόλων του, καθένα εκ των οποίων είναι αλγεβρικό, αφού είναι τομή αλγεβρικών συνόλων (άσκηση 2.4).

Αντιστρόφως, θα δείξομε ότι, αν $A = A_1 \cup A_2$, όπου τα A_1, A_2 είναι *γνήσια* αλγεβρικά υποσύνολα του A, τότε το $\mathbb{I}(A)$ δεν είναι πρώτο ιδεώδες του $K[X_1, \dots, X_n]$. Ισχυρισμός: Για $i = 1, 2$ είναι $\mathbb{I}(A_i) \supsetneqq \mathbb{I}(A)$. Διότι, η σχέση $A_i \subseteq A$ συνεπάγεται (άσκηση 2.7) τη σχέση $\mathbb{I}(A_i) \supseteq \mathbb{I}(A)$. Αν για κάποιο $i \in \{1, 2\}$ η τελευταία σχέση είναι ισότητα, τότε, από το Πόρισμα 2.3.4, συμπεραίνομε ότι $A_i = A$, που αντίκειται στην υπόθεσή μας. Συνεπώς, για $i = 1, 2$, μπορούμε να βρούμε $f_i \in \mathbb{I}(A_i) \setminus \mathbb{I}(A)$. Θα δείξομε τώρα ότι $f_1 f_2 \in \mathbb{I}(A)$, που οδηγεί στο συμπέρασμα ότι το $\mathbb{I}(A)$ δεν είναι πρώτο ιδεώδες. Προς τούτο, θεωρούμε $(a_1, \dots, a_n) \in A$ και δείχνομε ότι $(f_1 f_2)(a_1, \dots, a_n) = 0$, ως εξής: Από τη σχέση $(a_1, \dots, a_n) \in A = A_1 \cup A_2$ συμπεραίνομε ότι για κάποιο $i \in \{1, 2\}$ ισχύει $(a_1, \dots, a_n) \in A_i$. Αλλά $f_i \in \mathbb{I}(A_i)$, άρα $f_i(a_1, \dots, a_n) = 0$, οπότε $(f_1 f_2)(a_1, \dots, a_n) = f_1(a_1, \dots, a_n) f_2(a_1, \dots, a_n) = 0$.

□

Εστιάζομε στο εξής την προσοχή μας στην περίπτωση $n = 2$ δίνοντας εφαρμογές του Θεωρήματος 2.2.2. Κατ" αρχάς, μιά προφανής επαναδιατύπωση εκείνου του θεωρήματος είναι η εξής:

Θεώρημα 2.13 - ***Επαναδιατύπωση του Θεωρήματος 2.2.2.*** *Αν τα $f, g \in K[X, Y]$ δεν έχουν κοινό μη σταθερό διαιρέτη, τότε οι καμπύλες $\mathbb{V}(f)$ και $\mathbb{V}(g)$ έχουν πεπερασμένο πλήθος κοινών σημείων $\in K^2$.* [8]

Τώρα διατυπώνομε τρία θεωρήματα γεωμετρικού ενδιαφέροντος, των οποίων η απόδειξη στηρίζεται στα μέχρι τώρα αποτελέσματα της ενότητας 2.3 και στο παραπάνω Θεώρημα.

Θεώρημα 2.14 *Αν το $f \in K[X, Y]$ είναι ανάγωγο και το $\mathbb{V}(f)$ είναι άπειρο, τότε $\mathbb{I}(\mathbb{V}(f)) = \langle f \rangle$ και το $\mathbb{V}(f)$ είναι ανάγωγο αλγεβρικό σύνολο.*

Απόδειξη. ($\subseteq$) Αν $g \in \mathbb{I}(\mathbb{V}(f))$ τότε $\mathbb{V}(g) \supseteq \mathbb{V}(\mathbb{I}(\mathbb{V}(f)))$. Εφαρμόζοντας το Πόρισμα 2.3.4 με A το $\mathbb{V}(f)$, συμπεραίνομε ότι $\mathbb{V}(\mathbb{I}(\mathbb{V}(f))) = \mathbb{V}(f)$, άρα $\mathbb{V}(g) \supseteq \mathbb{V}(f)$, οπότε $\mathbb{V}(f) \cap \mathbb{V}(g) = \mathbb{V}(f)$. Εξ υποθέσεως, το $\mathbb{V}(f)$ είναι άπειρο, άρα οι καμπύλες $\mathbb{V}(f)$ και $\mathbb{V}(g)$ έχουν άπειρα κοινά σημεία $\in K^2$. Λόγω του Θεωρήματος 2.3.9, αυτό μας οδηγεί στο συμπέρασμα ότι τα f, g έχουν κοινό διαιρέτη στο $K[X, Y]$. Όμως το f είναι ανάγωγο, άρα αυτό ο κοινός διαιρέτης είναι, αναγκαστικά, το ίδιο το f και τα συνεταιρικά του. Αυτό σημαίνει ότι $f | g$, άρα $g \in \langle f \rangle$.

($\supseteq$) Βλ. άσκηση 2.9.

Μέχρι στιγμής, λοιπόν, έχομε αποδείξει ότι $\mathbb{I}(\mathbb{V}(f)) = \langle f \rangle$ και μένει ακόμη να δείξομε ότι το $\mathbb{V}(f)$ είναι ανάγωγο σύνολο. Αφού το f είναι ανάγωγο στο $K[X, Y]$ και το $K[X, Y]$ είναι περιοχή μονοσήμαντης ανάλυσης (Θεώρημα **??**), έπεται ότι

[8] Εδώ και στο εξής, λέγοντας ((πεπερασμένο πλήθος σημείων)), εννοούμε ((πεπερασμένο, το πολύ, πλήθος σημείων)), δηλαδή, δεν αποκλείομε το κενό σύνολο σημείων.

το f είναι πρώτο στοιχείο της ακέραιας περιοχής $K[X,Y]$. Αυτό συνεπάγεται ότι, αν $f|gh$, τότε $f|g$ είτε $f|h$. Ισοδύναμη διατύπωση: Αν $gh \in \langle f\rangle$ τότε $g \in \langle f\rangle$ είτε $h \in \langle f\rangle$; μ" άλλα λόγια, το $\langle f\rangle$ είναι πρώτο ιδεώδες του $K[X,Y]$, δηλαδή, το $\mathbb{I}(\mathbb{V}(f))$ είναι πρώτο ιδεώδες του $K[X,Y]$. Αλλά τότε, από το Θεώρημα 2.3.8 συμπεραίνομε ότι το $\mathbb{V}(f)$ είναι ανάγωγο σύνολο.

□

Άσκηση 2.11 (α') Αποδείξτε ότι το $Y - X^2 \in \mathbb{C}[X,Y]$ είναι ανάγωγο.
(β') Αποδείξτε ότι το αλγεβρικό σύνολο $\mathbb{V}(Y-X^2)$ είναι ανάγωγο σύνολο του $\mathbb{C}^2$.

Άσκηση 2.12 Αποδείξτε ότι το $f(X,Y) = Y^2 + X^2(X-1)^2 \in \mathbb{R}[X,Y]$ είναι ανάγωγο πολυώνυμο, αλλά το $\mathbb{V}(f)$ δεν είναι ανάγωγο υποσύνολο του $\mathbb{R}^2$. Γιατί αυτό δεν αντιφάσκει στο Θεώρημα 2.3.10?

Πρόταση 2.15 *Αν το K είναι άπειρο σώμα, τότε $\mathbb{I}(K^2) = \langle 0\rangle$*

Απόδειξη. Προφανώς, το μηδενικό πολυώνυμο του $K[X,Y]$ μηδενίζεται σε όλα τα σημεία του K^2, άρα $\langle 0\rangle \subseteq \mathbb{I}(K^2)$. Αντιστρόφως, θα δείξομε με εις άτοπον απαγωγή ότι το $\mathbb{I}(K^2)$ περιέχει μόνο το μηδενικό πολυώνυμο. Έστω ότι το $f(X,Y) \in \mathbb{I}(K^2)$ είναι μη μηδενικό. Τότε το f είναι μη σταθερό, άρα, δίχως βλάβη της γενικότητος μπορούμε να υποθέσομε ότι ο βαθμός του ως προς X είναι $n \geq 1$ και γράφομε

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

Έστω $b \in K$, τέτοιο ώστε $g_n(b) \neq 0$, οπότε το πολυώνυμο $h(X) = g_n(b)X^n + \cdots + g_1(b)X + g_0(b) \in K[X]$ είναι μη μηδενικό. Κρατώντας σταθερό το b και αφήνοντας το a να διατρέχει το K, έχομε $h(a) = f(a,b) = 0$, διότι, εξ υποθέσεως, το f μηδενίζεται σε όλο το K^2. Άρα, το $h(X)$ μηδενίζεται για κάθε τιμή του K, δηλαδή, το $h(X)$ έχει άπειρες ρίζες; άτοπο.

□

Θεώρημα 2.16 *Αν το K είναι άπειρο σώμα, τότε τα ανάγωγα υποσύνολα του K^2 είναι τα K^2, $\emptyset$, όλα τα μονοσύνολα (σημεία) και όλα τα άπειρα $\mathbb{V}(f)$ με το $f \in K[X,Y]$ ανάγωγο.*

Απόδειξη. Από την Πρόταση 2.3.11 ξέρομε ότι $\mathbb{I}(K^2) = \langle 0\rangle$. Όμως το $\langle 0\rangle$ είναι πρώτο ιδεώδες, άρα, βάσει του Θεωρήματος 2.3.8, το K^2 είναι ανάγωγο σύνολο.

Το κενό σύνολο είναι αλγεβρικό διότι $\emptyset = \mathbb{V}(1)$ και προφανώς είναι ανάγωγο, βάσει του ορισμού του αναγώγου συνόλου.

Κάθε μονοσύνολο είναι αλγεβρικό σύνολο. Πράγματι, έστω το $\{(a,b)\}$, όπου $a,b \in K$. Τότε, τετριμμένα, $\{(a,b)\} = \mathbb{V}(\{X-a, Y-b\})$, άρα το $\{(a,b)\}$ είναι αλγεβρικό σύνολο, το οποίο είναι προφανώς ανάγωγο, βάσει του ορισμού του αναγώγου συνόλου.

Τέλος, αν το $f \in K[X,Y]$ είναι ανάγωγο πολυώνυμο και το $\mathbb{V}(f)$ είναι άπειρο, τότε το Θεώρημα 2.3.10 μας εξασφαλίζει ότι το $\mathbb{V}(f)$ είναι ανάγωγο.

Συνεπώς, μέχρι στιγμής έχομε δείξει ότι όλα τα σύνολα, που περιγράφονται στην εκφώνηση του θεωρήματος, είναι όντως ανάγωγα.

Αντιστρόφως, έστω μη κενό ανάγωγο αλγεβρικό σύνολο $A \subsetneq K^2$.

Αν $\mathbb{I}(A) = \langle 0 \rangle$, τότε $\mathbb{I}(A) = \mathbb{I}(K^2)$ (τό δείξαμε παραπάνω), άρα, $A =$ (Πόρισμα 2.3.4) $\mathbb{V}(\mathbb{I}(A)) = \mathbb{V}(\mathbb{I}(K^2)) =$ (Πόρισμα 2.3.4) K^2. Στην περίπτωση αυτή, δηλαδή, $A = K^2$.

Αν το A είναι πεπερασμένο, έστω $A = \{(a_1, b_1), \dots, (a_r, b_r)\}$, τότε, αναγκαστικά, $r = 1$, διότι, διαφορετικά το A θα γραφόταν ως ένωση $r > 1$ αναγώγων υποσυνόλων του: $A = \cup_{i=1}^{r} \{(a_i, b_i)\}$. Συνεπώς $r = 1$ και το A είναι μονοσύνολο.

Μένει, τέλος, η περίπτωση που $\emptyset \subsetneq A \subsetneq K^2$, $\mathbb{I}(A) \neq \langle 0 \rangle$ και το A είναι άπειρο. Στόχος μας, σ" αυτή την περίπτωση, είναι να δείξομε ότι $A = \mathbb{V}(p)$, για κάποιο ανάγωγο πολυώνυμο $p \in K[X,Y]$. Κατ" αρχάς παρατηρούμε ότι το ιδεώδες $\mathbb{I}(A)$ περιέχει μη σταθερά πολυώνυμα και έστω $f \in \mathbb{I}(A)$ ένα τέτοιο πολυώνυμο. Έστω $f = p_1 \cdots p_r$ η ανάλυση του f σε ανάγωγα πολυώνυμα του $K[X,Y]$. Επειδή το A είναι ανάγωγο, το $\mathbb{I}(A)$ είναι πρώτο ιδεώδες, βάσει του Θεωρήματος 2.3.8. Έχομε λοιπόν, $p_1 \cdots p_r = f \in \mathbb{I}(A)$, με το $\mathbb{I}(A)$ πρώτο, άρα ένα τουλάχιστον $p_i \in \mathbb{I}(A)$. Συνοψίζοντας, καταλήξαμε στο συμπέρασμα ότι υπάρχει $p \in \mathbb{I}(A)$ ανάγωγο στο $K[X,Y]$ και μένει να δείξομε ότι $\mathbb{I}(A) = \langle p \rangle$, διότι τότε, $A =$ (Πόρισμα 2.3.4) $\mathbb{V}(\mathbb{I}(A)) = \mathbb{V}(p)$. Κατ" αρχάς, αφού $p \in \mathbb{I}(A)$, έπεται ότι $\langle p \rangle \subseteq \mathbb{I}(A)$. Αν δεν ίσχυε η ισότητα στην τελευταία σχέση, θα μπορούσαμε να βρούμε $g \in \mathbb{I}(A) \setminus \langle p \rangle$ και αυτό, ειδικώτερα, συνεπάγεται ότι το g δεν διαιρείται από το p, άρα τα g και p δεν έχουν κοινό παράγοντα, οπότε το $\mathbb{V}(g) \cap \mathbb{V}(p)$ είναι πεπερασμένο, βάσει του Θεωρήματος 2.3.9. Αφ" ετέρου έχομε $\{p, g\} \subseteq \mathbb{I}(A)$, άρα (άσκηση 2.3) $\mathbb{V}(\mathbb{I}(A)) \subseteq \mathbb{V}(\{p, g\})$ και, συνεπώς, $A =$ (Πόρισμα 2.3.4) $\mathbb{V}(\mathbb{I}(A)) \subseteq \mathbb{V}(\{p, g\}) = \mathbb{V}(p) \cap \mathbb{V}(g)$. Έτσι οδηγούμαστε στο συμπέρασμα ότι το άπειρο σύνολο A περιέχεται στο πεπερασμένο σύνολο $\mathbb{V}(p) \cap \mathbb{V}(g)$; αντίφαση.

□

Άσκηση 2.13 Έστω K άπειρο σώμα και $V_1 \neq V_2$ μη κενά ανάγωγα γνήσια υποσύνολα του K^2. Αποδείξτε ότι $V_1 \not\subseteq V_2$.

Υπόδειξη. Συνδυάστε τα Θεωρήματα 2.3.12 και 2.3.9.

Ορισμός. Ένα σώμα K χαρακτηρίζεται *αλγεβρικώς κλειστό*, αν κάθε μη σταθερό πολυώνυμο του $K[X]$ έχει ρίζα στο K.

Το ""διασημότερο"" παράδειγμα αλγεβρικώς κλειστού σώματος είναι το $\mathbb{C}$.

Άσκηση 2.14 Κάθε αλγεβρικώς κλειστό σώμα είναι άπειρο.

Υπόδειξη. Αν $1, a_2, \dots, a_m$ ήταν όλα τα στοιχεία του αλγεβρικώς κλειστού σώματος K, θεωρήστε το $f(X) = (X-1)(X-a_2)\cdots(X-a_m)+1$.

Άσκηση 2.15 Αν το K είναι αλγεβρικώς κλειστό σώμα K και $f \in K[X_1, \dots, X_n]$, τότε $\mathbb{V}(f) \neq \emptyset$.

Άσκηση 2.16 Αν το K είναι αλγεβρικώς κλειστό σώμα και το $f \in K[X,Y]$ είναι μη σταθερό, τότε το $\mathbb{V}(f)$ είναι άπειρο.
Υπόδειξη. Γράψτε το f όπως στην απόδειξη του Θεωρήματος 2.3.12.

Θεώρημα 2.17 *Έστω K αλγεβρικώς κλειστό σώμα και μη σταθερό $f \in K[X,Y]$. Έστω $f = p_1^{n_1} \cdots p_r^{n_r}$ η ανάλυση του f σε ανάγωγα του $K[X,Y]$, όπου τα ανάγωγα πολυώνυμα $p_1, \ldots, p_r$ είναι διαφορετικά μεταξύ τους και οι εκθέτες τους $n_1, \ldots, n_r$ είναι όλοι θετικοί. Τότε,*

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

και καθένα από τα $\mathbb{V}(p_i)$ είναι ανάγωγο αλγεβρικό σύνολο.

Απόδειξη. Κάποιες προκαταρκτικές παρατηρήσεις: Κάθε $\mathbb{V}(p_i)$ είναι άπειρο σύνολο (άσκηση 2.16). Επίσης, για $i \neq j$, τα p_i, p_j δεν έχουν κοινό μη σταθερό διαιρέτη, αφού είναι διαφορετικά ανάγωγα πολυώνυμα. Άρα το $\mathbb{V}(p_i) \cap \mathbb{V}(p_j)$ είναι πεπερασμένο σύνολο, βάσει του Θεωρήματος 2.3.9. Μπορούμε τώρα να συμπεράνομε ότι, αν $i \neq j$, τότε $\mathbb{V}(p_i) \not\subseteq \mathbb{V}(p_j)$. Διότι, αν ήταν $\mathbb{V}(p_i) \subseteq \mathbb{V}(p_j)$, τότε το άπειρο σύνολο $\mathbb{V}(p_i) \subseteq \mathbb{V}(p_i) \cap \mathbb{V}(p_j) =$ πεπερασμένο σύνολο.

Είναι προφανές ότι $\mathbb{V}(p_i^{n_i}) = \mathbb{V}(p_i)$, άρα

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

Καθένα από τα $\mathbb{V}(p_i)$ είναι άπειρο, άρα, από το Θεώρημα 2.3.10, είναι ανάγωγο αλγεβρικό σύνολο. Επίσης, από την παραπάνω σχέση έπεται ότι

$$\begin{aligned}\mathbb{I}(\mathbb{V}(f)) = \mathbb{I}(\mathbb{V}(p_1) \cup \cdots \cup \mathbb{V}(p_r)) &= \text{ (άσκηση 2.8) } \mathbb{I}(\mathbb{V}(p_1)) \cap \cdots \cap \mathbb{I}(\mathbb{V}(p_r)) \\ &= \text{ (Θεώρημα 2.3.10) } \langle p_1 \rangle \cap \cdots \cap \langle p_r \rangle,\end{aligned}$$

οπότε μένει να δείξομε ότι $\langle p_1 \rangle \cap \cdots \cap \langle p_r \rangle = \langle p_1 \cdots p_r \rangle$. Πράγματι, κάθε p_i διαιρεί το γινόμενο $p_1 \cdots p_r$, οπότε $\langle p_1 \cdots p_r \rangle \subseteq \langle p_i \rangle$ για κάθε $i = 1, \ldots, r$. Άρα, $\langle p_1 \cdots p_r \rangle \subseteq \langle p_1 \rangle \cap \cdots \cap \langle p_r \rangle$. Αντιστρόφως, αν $g \in \langle p_1 \rangle \cap \cdots \cap \langle p_r \rangle$ τότε το g διαιρείται από όλα τα p_i, άρα διαιρείται και από το γινόμενό τους, αφού τα p_i είναι ανά δύο πρώτα μεταξύ τους (βλ. άσκηση 1.19 (δ')). Αλλά η σχέση $p_1 \cdots p_r | g$ σημαίνει ότι $g \in \langle p_1 \cdots p_r \rangle$. Έτσι, κάθε στοιχείο του $\langle p_1 \rangle \cap \cdots \cap \langle p_r \rangle$ ανήκει στο $\langle p_1 \cdots p_r \rangle$; αυτό ολοκληρώνει την απόδειξη.

□

Άσκηση 2.17 Γράψτε το αλγεβρικό σύνολο $\mathbb{V}(\{Y^4 - X^2, Y^4 - X^2Y^2 + XY^2 - X^3\}) \subseteq \mathbb{C}^2$ ως ένωση αναγώγων αλγεβρικών υποσυνόλων του $\mathbb{C}^2$.
Υπόδειξη. Αναλύστε τα πολυώνυμα $Y^4 - X^2$ και $Y^4 - X^2Y^2 + XY^2 - X^3$ σε γινόμενο αναγώγων πολυωνύμων. Χρησιμοποιείστε την άσκηση 2.5 και το Θεώρημα 2.3.13. Χρησιμοποιείστε τη συνολοθεωρητική ταυτότητα $[\cup_i A_i] \cap [\cup_j B_j] = \cup_{i,j}(A_i \cap B_j)$ (όπου τα i, j διατρέχουν κάποια σύνολα δεικτών).

Το Nullstellensatz του Hilbert

Πρόταση-Ορισμός 2.18 *Έστω R μεταθετικός δακτύλιος με μοναδιαίο και J ιδεώδες του R. Το σύνολο*

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

είναι ιδεώδες, που περιέχει το J και λέγεται ριζικό του J. Αν ισχύει $\mathrm{Rad}(J) = J$, τότε το ιδεώδες J χαρακτηρίζεται ριζικό.

Απόδειξη. Αρχικά κάνομε την παρατήρηση, που αφορά| γενικά σε μεταθετικούς δακτυλίους με μοναδιαίο, ότι, για $a, b \in R$ και $n \in \mathbb{N}$ ισχύει το διωνυμικό ανάπτυγμα

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

Τώρα ϑ" αποδείξομε ότι, αν $a, b \in \mathrm{Rad}(J)$, τότε $a+b \in \mathrm{Rad}(J)$. Από την υπόθεση ξέρομε ότι υπάρχουν $m, n \in \mathbb{N}$, τέτοια ώστε $a^m \in \mathrm{Rad}(J)$ και $b^n \in \mathrm{Rad}(J)$. Αρκεί ν" αποδείξομε ότι $(a+b)^{m+n} \in J$. Πράγματι, αν ϑεωρήσομε το διωνυμικό ανάπτυγμα $(a+b)^{m+n}$, ο τυπικός προσθετέος του είναι $\binom{m+n}{k} a^{m+n-k} b^k \ \ (0 \le k \le m+n)$. Διακρίνομε δύο περιπτώσεις: Αν $k \ge n$, τότε $b^k = b^{k-n} b^n \in J$, διότι $b^{k-n} \in R$ και $b^n \in J$; έπεται εξ αυτού ότι όλος ο προσθετέος ανήκει στο J. Αν $k \le n$, τότε $a^{m+n-k} = a^{n-k} a^m \in J$, διότι $a^{n-k} \in R$ και $a^m \in J$; άρα, πάλι όλος ο προσθετέος ανήκει στο J.
Τέλος, αν $r \in R$ και $a \in \mathrm{Rad}(J)$, τότε $ra \in \mathrm{Rad}(J)$. Διότι, από τη σχέση $a \in \mathrm{Rad}(J)$ έπεται ότι $a^m \in J$ για κάποιο $m \in \mathbb{N}$. Τότε, όμως, $(ra)^m = r^m a^m \in J$.

□

Πρόταση 2.19 *Αν $A \subseteq K^n$, τότε το $\mathbb{I}(A)$ είναι ριζικό ιδεώδες του $K[X_1, \ldots, X_n]$.*

Απόδειξη. Ξέρομε από την προηγούμενη Πρόταση-Ορισμό ότι $\mathbb{I}(A) \subseteq \mathrm{Rad}(\mathbb{I}(A))$. Αντιστρόφως, ϑεωρούμε $f \in \mathrm{Rad}(\mathbb{I}(A))$ και ϑ" αποδείξομε ότι $f \in \mathbb{I}(A)$. Για την απόδειξη της τελευταίας σχέσης πρέπει να πάρομε $(a_1, \ldots, a_n) \in A$ και να δείξομε ότι $f(a_1, \ldots, a_n) = 0$. Όμως, από την υπόθεση $f \in \mathrm{Rad}(\mathbb{I}(A))$ έχομε ότι, για κάποιο $m \in \mathbb{N}$ είναι $f^m \in \mathbb{I}(A)$, οπότε $f^m(a_1, \ldots, a_n) = 0$. Αλλά $f^m(a_1, \ldots, a_n) = f(a_1, \ldots, a_n)^m$ και, συνεπώς, η σχέση $f^m(a_1, \ldots, a_n) = 0$ συνεπάγεται ότι $f(a_1, \ldots, a_n) = 0$.

□

Άσκηση 2.18 Έστω J ιδεώδες του $K[X_1, \ldots, X_n]$. Αποδείξτε ότι $\mathbb{V}(J) = \mathbb{V}(\mathrm{Rad}(J))$.

Θεώρημα 2.20 - ***Nullstellensatz του Hilbert.*** *Αν το K είναι αλγεβρικώς κλειστό σώμα και J είναι ιδεώδες του $K[X_1, \ldots, X_n]$, τότε $\mathbb{I}(\mathbb{V}(J)) = \mathrm{Rad}(J)$.*

Η απόδειξη αυτού του θεωρήματος δεν εμπίπτει στους σκοπούς του μαθήματος, πλήν όμως, θα δούμε δύο εφαρμογές, οι οποίες σχετίζονται με την ύλη της ενότητας 2.3.

Πόρισμα 2.21 *Έστω ότι το K είναι αλγεβρικώς κλειστό σώμα και $S, S' \subseteq K[X_1, \dots, X_n]$. Τότε ισχύει η εξής ισοδυναμία:*

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

Απόδειξη. Προκαταρκτική παρατήρηση: Για κάθε $S \subseteq K[X_1, \dots, X_n]$ ισχύει

$$\mathbb{V}(S) = \text{ (Πρόταση 2.3.1) } \mathbb{V}(\langle S\rangle) = \text{ (άσκηση 2.18) } \mathbb{V}(\mathrm{Rad}(\langle S\rangle)). \tag{2.8}$$

Αν $\mathrm{Rad}(\langle S\rangle) = \mathrm{Rad}(\langle S'\rangle)$, τότε $\mathbb{V}(\mathrm{Rad}\langle S\rangle)) = \mathbb{V}(\mathrm{Rad}(\langle S'\rangle))$, και εφαρμόζοντας την (2.8) για τα S και S', βλέπομε αμέσως ότι $\mathbb{V}(S) = \mathbb{V}(S')$.

Αντιστρόφως, έστω ότι $\mathbb{V}(S) = \mathbb{V}(S')$. Τότε $\mathbb{V}(\langle S\rangle) = \mathbb{V}(\langle S'\rangle)$, άρα $\mathbb{I}(\mathbb{V}(\langle S\rangle)) = \mathbb{I}(\mathbb{V}(\langle S'\rangle))$. Εφαρμόζοντας το Θεώρημα 2.3.16 με τα $\langle S\rangle$ και $\langle S'\rangle$ στη θέση του J, συμπεραίνομε ότι $\mathrm{Rad}(\langle S\rangle) = \mathrm{Rad}(\langle S'\rangle)$.

□

Πόρισμα 2.22 *Αν το K είναι αλγεβρικώς κλειστό σώμα και J ιδεώδες του $K[X_1, \dots, X_n]$, τότε ισχύει η ισοδυναμία:*

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

Συνεπώς, αν το J είναι γνήσιο ιδεώδες του $K[X_1, \dots, X_n]$, τότε $\mathbb{V}(J) \neq \emptyset$.

Απόδειξη. Μιά προφανής προκαταρκτική παρατήρηση είναι ότι $K[X_1, \dots, X_n] = \langle 1\rangle = \mathrm{Rad}(\langle 1\rangle)$. Άρα,

$$\begin{aligned}\mathbb{V}(J) = \emptyset \Rightarrow \mathbb{V}(J) = \mathbb{V}(\langle 1\rangle) \Rightarrow (\text{Πόρισμα 2.3.17}) \ \mathrm{Rad}(J) = \mathrm{Rad}(\langle 1\rangle) = K[X_1, \dots, X_n] \\ \Rightarrow 1 \in \mathrm{Rad}(J) \Rightarrow 1 \in J \Rightarrow J = K[X_1, \dots, X_n].\end{aligned}$$

Για την απόδειξη του αντιστρόφου δεν χρειάζεται το Nullstellensatz; στην πραγματικότητα, η απόδειξη είναι τετριμμένη:

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

□

Άσκηση 2.19 Έστω ότι $f_1, \dots, f_m \in \mathbb{C}[X_1, \dots, X_n]$ και σας δίδεται η πληροφορία ότι το σύστημα

$$\left\{\begin{array}{rcl} f_1(z_1, \dots, z_n) & = & 0 \\ \vdots & \vdots & \vdots \\ f_m(z_1, \dots, z_n) & = & 0 \end{array}\right.$$

δεν έχει λύση $(z_1, \dots, z_n) \in \mathbb{C}^n$. Αποδείξτε ότι υπάρχουν $g_1, \dots, g_m \in \mathbb{C}[X_1, \dots, X_n]$, τέτοια ώστε $g_1 f_1 + \cdots + g_m f_m = 1$.

Ο αντίστροφος ισχυρισμός, δηλαδή, αν υπάρχουν $g_1, \dots, g_m \in \mathbb{C}[X_1, \dots, X_n]$, τέτοια ώστε $g_1 f_1 + \cdots + g_m f_m = 1$, τότε το παραπάνω σύστημα είναι αδύνατο, βλέπετε ότι είναι προφανής?

Άσκηση 2.20 (α') Έστω σώμα K, $f(x_1, \dots, X_n) \in K[X_1, \dots, X_n]$ και $a_1, \dots, a_n \in K^n$. Αποδείξτε ότι υπάρχουν πολυώνυμα $g_i(X_i, \dots, X_n) \in K[X_i, \dots, X_n]$ $(i = 1, \dots, n)$ και $r \in K$, τέτοια ώστε

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

Υπόδειξη. Απόδειξη επαγωγική. Θα έχετε υπ" όψιν ότι η ευκλείδεια διαίρεση ισχύει και σε ακέραιες περιοχές (π.χ. $K[X_\nu, X_{\nu+1}, \dots, X_n]$) όταν ο διαιρέτης (π.χ. $X_\nu - a_\nu$) έχει συντελεστής του μεγιστοβαθμίου όρου είναι μονάδα της ακέραιας περιοχής.

(β') Έστω αλγεβρικώς κλειστό σώμα K και J maximal ιδεώδες του $K[X_1, \dots, X_n]$. Αποδείξτε ότι υπάρχουν $a_1, \dots, a_n \in K$, τέτοια ώστε $J = \langle X_1 - a_1, \dots, X_n - a_n \rangle$.
Υπόδειξη. Έστω $f \in J$. Από την άσκηση 2.15, $\mathbb{V}(f) \neq \emptyset$. Έστω $(a_1, \dots, a_n) \in \mathbb{V}(f)$. Αποδείξτε ότι $J = \langle X_1 - a_1, \dots, X_n - a_n \rangle$. Εκμεταλλευθείτε το ερώτημα (α').

Άσκηση 2.21 Έστω $f = Y^4 - X^2$, $g = Y^4 - X^2Y^2 + XY^2 - X^3 \in \mathbb{C}[X, Y]$. Γράψτε το αλγεβρικό σύνολο $\mathbb{V}(\{f, g\})$ ως ένωση αναγώγων αλγεβρικών συνόλων του $\mathbb{C}^2$, κανένα εκ των οποίων δεν περιέχεται σε κάποιο από τα υπόλοιπα.
Απάντηση: $\mathbb{V}(\{f, g\}) = \mathbb{V}(Y^2 + X) \cup \{(1, -1)\} \cup \{(1, 1)\}$.

Άσκηση 2.22 Αποδείξτε ότι, για κάθε $c \in \mathbb{C}$, το $\mathbb{V}(Y^2 - X(X-1)(X-c))$ είναι ανάγωγο αλγεβρικό σύνολο (καμπύλη) του $\mathbb{C}^2$.

Άσκηση 2.23 Έστω D περιοχή μονοσήμαντης ανάλυσης και P μη μηδενικό πρώτο και κύριο ιδεώδες της D.

(α') Αποδείξτε ότι υπάρχει πρώτο στοιχείο $\pi \in D$, τέτοιο ώστε $P = \langle \pi \rangle$.
Υπόδειξη. Εξ υποθέσεως υπάρχει $r \in D$, τέτοιο ώστε $P = \langle r \rangle$. Θεωρήστε τη μονοσήμαντη ανάλυση $r = \pi_1 \cdots \pi_m$ σε πρώτα στοιχεία της D. Χρησιμοποιώντας την υπόθεση ότι το P είναι πρώτο, αποδείξτε ότι, αναγκαστικά, $m = 1$.

(β') Αποδείξτε ότι δεν υπάρχει πρώτο ιδεώδες Q της D, τέτοιο ώστε $\langle 0 \rangle \subsetneqq Q \subsetneqq P$.
Υπόδειξη. Βάσει του (α'), έστω $P = \langle \pi \rangle$. Είναι $Q \subsetneqq D$, διότι το Q είναι πρώτο. Άρα υπάρχει $q \in Q$, που δεν είναι μονάδα. Προφανώς, $q \in P = \langle \pi \rangle$, άρα $\pi | q$. Συνεπώς, αν θεωρήσει κανείς την ανάλυση του q σε πρώτα στοιχεία της D, αυτή θα είναι, ή της μορφής $q = (\text{μονάδα}) \cdot \pi$, ή $q = \pi\pi_2 \cdots \pi_m$ με $m \geq 2$ και $\pi_2, \dots, \pi_m$ πρώτα στοιχεία της D. Αποδείξτε ότι και τα δύο ενδεχόμενα οδηγούν στη σχέση $\pi \in Q$, άρα στην $P = Q$, που αντιβαίνει στην υπόθεση.

(γ') Έστω σώμα K και $f \in K[X_1, \dots, X_n]$ ανάγωγο μη σταθερό πολυώνυμο με $\mathbb{V}(f)$ άπειρο. Αποδείξτε ότι το $\mathbb{V}(f)$ δεν περιέχεται γνησίως σε κανένα γνήσιο αλγεβρικό υποσύνολο του K^n.
Υπόδειξη. Έστω αλγεβρικό υποσύνολο $A \subsetneqq K^n$, τέτοιο ώστε $\mathbb{V}(f) \subsetneqq A$. Εκμεταλλευόμενοι το Πόρισμα 2.3.4, αποδείξτε ότι $\mathbb{I}(K^n) \subsetneqq \mathbb{I}(A) \subsetneqq \mathbb{I}(\mathbb{V}(f))$. Τί ιδεώδες είναι το $\mathbb{I}(A)$? Μετά, δείτε με ποια ιδεώδη είναι ίσα τα $\mathbb{I}(K^n)$ και $\mathbb{I}(\mathbb{V}(f))$, και εφαρμόστε το ερώτημα (β').

Βιβλιογραφία

[1] Δ. Βάρσος, Δ. Δεριζιώτης, Γ. Εμμανουήλ, Μ. Μαλιάκας, Ο. Ταλέλλη, *Μιά Εισαγωγή στην Άλγεβρα*, Εκδόσεις ΣΟΦΙΑ, Αθήνα 2012.