

1. Δακτύλιος, Ακέραιες Περιοχές, Σώματα : Βασικές γνώσεις.

Δακτύλιος είναι ένα σύνολο $R \neq \emptyset$ εφοδιασμένο με δύο εσωτερικές πράξεις $+$ (πρόσθεση) και \cdot (πολ/σιασμός) έτσι ώστε να πληρούνται οι έξης ιδιότητες:

α) Το R με την πράξη $+$ είναι άβελιατή ομάδα.

β) Η πράξη \cdot είναι προσεταιριστική.

γ) Για όλα τα $a, b, c \in R$

$$a \cdot (b+c) = a \cdot b + a \cdot c \quad \text{και} \quad (b+c) \cdot a = b \cdot a + c \cdot a$$

(αριστερή και δεξιά επιμεριστική ιδιότητα).

Το ουδέτερο στοιχείο της ομάδας $(R, +)$ συμβολίζεται ^(συνήθως) με 0 και ονομάζεται μηδέν. Η πράξη \cdot δεν έχει, αν γενεί, ουδέτερο στοιχείο (δηλ. $e \in R$ τ.ώ. $e \cdot a = a \cdot e = a \quad \forall a \in R$). Αν έχει, συμβολίζεται (συνήθως) με 1 και ονομάζεται μονάδα του δακτυλίου R . Στην περίπτωση αυτή λέμε ότι δR είναι δακτύλιος με μονάδα. Η πράξη \cdot δεν είναι, και' αναίτηκη, αντιμεταθετική: αν είναι, δR λέγεται αντιμεταθετικός δακτύλιος. Συνηθέστατα, αντί $a \cdot b$ γράφομε ab .

Παραδείγματα:

α) Οι ακέραιοι \mathbb{Z} με τις συνήθειες πράξεις πρόσθεσης και πολλαπλασιασμού. Πρόκειται περί αντιμεταθετικού δακτυλίου με μονάδα.

β) Αν $\delta n \geq 1$ είναι ακέραιος, το σύνολο \mathbb{Z}_n των κλάσεων ισοδυναμίας modulo n εφοδιάζεται με τις πράξεις $+$ και \cdot , που ορίζονται ως έξης (τα στοιχεία του \mathbb{Z}_n θα συμβολίζομε με $\hat{a}, \hat{b}, \hat{c}, \dots$, όπου $a, b, c, \dots \in \mathbb{Z}$):

$$\hat{a} + \hat{b} = \widehat{a+b}, \quad \hat{a} \cdot \hat{b} = \widehat{ab}$$

Και αυτός δ δακτύλιος είναι αντιμεταθετικός με μονάδα.

γ) Έστω $K = \mathbb{Q}$ ή \mathbb{R} ή \mathbb{C} και $M(n, K)$ το σύνολο των $n \times n$ τετραγώνων με στοιχεία από το K . Το σύνολο αυτό εφοδιασμένο με τις συνήθεις πράξεις πρόσθεσης και πολλαπλασιασμού τετραγώνων καθίσταται δακτύλιος με μονάδα, όχι όμως αντιμεταθετικός. (αντιπαραδείγματα: Για $A = \begin{pmatrix} 2 & 1 \\ -1 & 0 \end{pmatrix}$, $B = \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix}$ είναι $AB \neq BA$).

δ) Έστω $d \in \mathbb{Z}$, όχι τέλειο τετράγωνο. Το σύνολο $\mathbb{Z}[\sqrt{d}] \cong \{x + y\sqrt{d}; x, y \in \mathbb{Z}\}$ εφοδιασμένο με τις πράξεις του \mathbb{C} γίνεται δακτύλιος (αντιμεταθετικός με μονάδα).

ε) Έστω \mathcal{F} το σύνολο όλων των συναρτήσεων $f: A \rightarrow \mathbb{R}$, όπου $A \subseteq \mathbb{R}$. Ορίζουμε τις εξής πράξεις στο \mathcal{F} :

Αν $f, g \in \mathcal{F}$, τότε $f+g$ είναι εκείνη η συνάρτηση για την οποία $(f+g)(x) \cong f(x) + g(x)$, $\forall x \in A$.

Και ανάλογα ορίζεται και η συνάρτηση $f \cdot g$, δηλ. $(f \cdot g)(x) = f(x) \cdot g(x)$, $\forall x \in A$.

Το \mathcal{F} εφοδιασμένο με αυτές τις δύο πράξεις καθίσταται αντιμεταθετικός δακτύλιος με μονάδα. Έδώ, μονάδα είναι η συνάρτηση 1_A , η οποία ορίζεται: $1_A(x) = 1$, $\forall x \in A$.

ς) Έστω ότι R, S είναι δύο δακτύλιοι. Τις πράξεις και των δύο συμβολίζουμε με $+$ και \cdot , αλλά δεν υπάρχει φόβος σύγχυσης, διότι γίνεται φανερό πότε τα $+$ και \cdot αναφέρονται στον ένα δακτύλιο και πότε στον άλλο.

Το καρτεσιανό γινόμενο $R \times S$ μπορεί να εφοδιασθεί με πρόσθεση και πολλαπλασιασμό κατά τον προφανή τρόπο:

$$(r_1, s_1) + (r_2, s_2) \cong (r_1 + r_2, s_1 + s_2)$$

\uparrow + του R \uparrow + του S

$$(r_1, s_1) \cdot (r_2, s_2) \cong (r_1 \cdot r_2, s_1 \cdot s_2)$$

\uparrow \cdot του R \uparrow \cdot του S

Είναι πολύ απλό να δούμε ότι το $R \times S$ με αυτές τις πράξεις

γίνεται δακτύλιος, ο οποίος, εἰς ὄριον, λέγεται εὐθύ ἀθροισμα-
των R και S .

Συμβολισμοί: Ἄν R εἶναι δακτύλιος, γιὰ κάθε $a \in R$ τὸ $-a$
συμβολίζει τὸ συμμετρικὸ (ἀντίθετο) στοιχείο τοῦ a στὴν
ὁμάδα $(R, +)$. Ἄν n εἶναι μὴ ἀρνητικὸς ἀκέραιος καὶ $a \in R$,
ὀρίζομε $n \cdot a$ νὰ σημαίνει $\underbrace{a + a + \dots + a}_{n \text{ φορές}}$ (ἄρα $0 \cdot a \stackrel{\text{def}}{=} 0$)
 $\uparrow \in \mathbb{Z}$ $\uparrow \in R$

Ἄν δ n εἶναι ἀρνητικὸς ἀκέραιος καὶ $a \in R$, ὀρίζομε
 $n \cdot a = -((-n) \cdot a)$,

καὶ στὴ συνέχεια βλέπομε ὅτι αὕτη ἡ σχέση ἰσχύει καὶ γιὰ $n \geq 0$.
Ἡ ἐπιμένη πρόταση δίνει ὅλες τὲς στοιχειώδεις ιδιότητες τῶν
πράξεων ἐνὸς δακτυλίου.

Πρόταση 1. Ἐστω R δακτύλιος καὶ $a, b, c \in R$.

- α) Τὸ 0 τοῦ R εἶναι μοναδικό. Τὸ $1 \in R$, ἂν ὑπάρχει, εἶναι μοναδικό.
- β) Κάθε $a \in R$ ἔχει ἓνα ἀκριβῶς ἀντίθετο $-a$.
- γ) Ἄν $a+b = a+c$ τότε $b=c$, καθὼς ἐπίσης καὶ
ἂν $b+a = c+a$ τότε $b=c$.
- δ) Κάθε ἐξίσωση (ὡς πρὸς x) $a+x = b$ καὶ $x+a = b$
ἔχει ἀκριβῶς μίαν λύση.
- ε) $-(-a) = a$ καὶ $-(a+b) = (-a) + (-b) \stackrel{\text{def}}{=} -a-b$
- ς) $a \cdot a = a \cdot 0 = 0$ (ἐδῶ 0 εἶναι τὸ μηδέν τοῦ R)
- ζ) Γιὰ ὁποιοδήποτε ἀκεραίους m, n :
 $m(a+b) = m \cdot a + m \cdot b$, $(m+n) \cdot a = m \cdot a + n \cdot a$
 $m(n \cdot a) = (mn) \cdot a$, $m \cdot (ab) = (m \cdot a)b = a(m \cdot b)$, $(ma)(nb) = (mn) \cdot (ab)$
- η) $a(-b) = (-a)b = -(ab) \stackrel{\text{def}}{=} -ab$
- θ) $(-a)(-b) = ab$
- ι) $a(b-c) = ab - ac$, $(b-c)a = ba - ca$

Η απόδειξη αφήνεται ως άσκηση.

Συμβολισμός. Αν ο R είναι δακτύλιος, $a \in R$ και n θετικός ακέραιος, τότε a^n ορίζουμε να σημαίνει $\underbrace{a \cdot a \cdot \dots \cdot a}_n$ φορές.
(άρα $a^1 = a$).

Για n αρνητικό ακέραιο, το σύμβολο a^n έχει νόημα μόνο αν ο R έχει μονάδα και υπάρχει το συμμετρικό (αντίστροφο) του a ως προς την πράξη \cdot . (δηλ. υπάρχει $b \in R$ τέω. $b \cdot a = a \cdot b = 1$). Στην περίπτωση αυτή, το αντίστροφο του a είναι μοναδικό (άσκηση) και συμβολίζεται a^{-1} .
Για n αρνητικό $\neq -1$, ορίζουμε $a^n = (a^{-n})^{-1}$. Τέλος, ορίζουμε $a^0 = 1$ (αν ο R έχει μονάδα).

Πρόταση 2 Έστω ότι στο δακτύλιο R ορίζονται τα a^m, a^n ($a \in R, m, n \in \mathbb{Z}$). Τότε,

$$\alpha) a^m \cdot a^n = a^{m+n},$$

$$\beta) \text{ Αν υπάρχει το } a^{-1}, \text{ τότε } a^{-m} = (a^{-1})^m$$

$$\gamma) (a^m)^n = a^{mn} = (a^n)^m$$

Η απόδειξη αφήνεται ως άσκηση.

Όρισμός. Λέμε ότι ο δακτύλιος R έχει μηδενοδιαίρετες αν υπάρχουν $a, b \in R - \{0\}$ με $ab = 0$.

Πρόταση 3. Αν στο δακτύλιο R δεν υπάρχουν μηδενοδιαίρετες, τότε επιτρέπεται η διαγραφή στον πολλαπλασιασμό. Δηλαδή, αν $a, b, c \in R$, $a \neq 0$ και $ab = ac$ (άντιστοιχως, $ba = ca$) τότε $b = c$.

Απόδειξη. $ab = ac \implies ab - ac = 0 \implies (\text{πλ. 1, 2}) a(b - c) = 0$.
 Η τελευταία ισότητα, αφού δεν υπάρχουν μηδενοδιαίρετες στον R και $a \neq 0$, συνεπάγεται $b = c$. Ομοίως αν $ba = ca$: ο.έ.δ.

Όρισμός. Ένας αντιμεταθετικός δακτύλιος με μονάδα, στον οποίο $1 \neq 0$ και δεν υπάρχουν μηδενοδιαίρετες λέγεται ἀπέραια περιοχή.

Παρατηρήστε ότι ο σχολαστικός περιορισμός $1 \neq 0$ σημαίνει, απλυσάτα, ότι $R \neq \{0\}$. Πράγματι, αν $R \neq \{0\}$ και $a \in R - \{0\}$, τότε (υποίθεται ότι ο R έχει μονάδα), $1a = a \neq 0 = (\text{πλ. 1, 5}) 0 \cdot a$, άρα αποκλείεται να είναι $1 = 0$.

Όρισμός. Έστω S ένα μη κενό υποσύνολο του δακτυλίου R . Αν το S με τις πράξεις $+$ και \cdot του R είναι δακτύλιος (ειδικότερα, συνεπώς, το αποτέλεσμα των πράξεων μεταξύ όποιωνδήποτε στοιχείων του S πρέπει να ανήκει στο S), τότε το S χαρακτηρίζεται ως υποδακτύλιος του R .

Πρόταση 4. Το μη κενό υποσύνολο S του R είναι υποδακτύλιος του R αν και μόνο αν το S είναι κλειστό ως προς τις δύο πράξεις του R , καθώς και ως προς το αντίθετο (δηλαδή, $a \in S \implies -a \in S$).

Η απόδειξη είναι άπλη και αφήνεται ως άσκηση.

Σώμα είναι ένας αντιμεταθετικός δακτύλιος $\neq \{0\}$, του οποίου τα μη μηδενικά στοιχεία, εφωδιασμένα με τον πολλαπλασιασμό, αποτελούν ομάδα.

Πρόταση 5. Ένας δακτύλιος είναι σώμα αν και μόνο αν είναι ακέραια περιοχή, της οποίας κάθε μη μηδενικό στοιχείο έχει αντίστροφο.

Η απόδειξη αφήνεται ως άσκηση.

Πρόταση 6. Κάθε πεπερασμένη ακέραια περιοχή είναι σώμα.

Απόδειξη. Σύμφωνα με την πρόταση 5, αρκεί ν' αποδείξουμε ότι κάθε μη μηδενικό στοιχείο της ακέραιας περιοχής, την οποία εσ' συμβολίσουμε με R , έχει αντίστροφο. Έστω λοιπόν $a \in R - \{0\}$. Για κάθε $x \in R - \{0\}$ είναι $a \cdot x \neq 0$ (R είναι ακέραια περιοχή), άρα έχουμε μια απεικόνιση $\phi: R - \{0\} \rightarrow R - \{0\}$, $\phi(x) = ax$. Εύκολα φαίνεται ότι η ϕ είναι αμφιμονοσήμαντη (λόγω του ότι R είναι ακέραια περιοχή). Άρα, το πλήθος των στοιχείων του $R - \{0\}$ είναι το ίδιο με το πλήθος των στοιχείων του $\phi(R - \{0\})$ (εδώ έπαιξε ρόλο το ότι το R είναι πεπερασμένο). Όμως, $\phi(R - \{0\}) \subseteq R - \{0\}$, άρα (αφού έχουν το ίδιο πληθυσμικό αριθμό) $\phi(R - \{0\}) = R - \{0\}$. Τώρα, επειδή $1 \in R - \{0\}$, θα υπάρχει $x \in R - \{0\}$ τέτοιο ώστε $\phi(x) = 1$. Δηλαδή $a \cdot x = 1$, που σημαίνει ότι το a έχει αντίστροφο το x , ο.έ.δ.

Πόρισμα. Ο δακτύλιος \mathbb{Z}_n είναι σώμα αν και μόνο αν n είναι πρώτος.

Απόδειξη. Είναι απλούστατο να 'δει κανείς ότι ο \mathbb{Z}_n είναι άκεραλα περιοχή αν και μόνο αν ο n είναι πρώτος και στη συνέχεια να εφαρμόσει την πρόταση 6.

Όρισμός. Έστω F σώμα και $\emptyset \neq K \subseteq F$. Το K λέγεται υπόσωμα του F αν, εφοδιασμένο με τις πράξεις του F , είναι σώμα.

Πρόταση 7. Έστω F σώμα και $\emptyset \neq K \subseteq F$. Το K είναι υπόσωμα του F αν και μόνο αν όλες οι παρακάτω συνθήκες ικανοποιούνται:

α) $0, 1 \in K$

β) Αν $a, b \in K$ τότε $a+b \in K$ και $ab \in K$.

γ) Αν $a \in K$ τότε $-a \in K$ και (στην περίπτωση που $a \neq 0$) $a^{-1} \in K$.

Απόδειξη. Απλή άσκηση.

2. Ομομορφισμός - Ισομορφισμός - Χαρακτηριστική.

Έστω ότι R, S είναι δακτύλιοι και $\phi: R \rightarrow S$ μια απεικόνιση τέτοια ώστε, για κάθε ζευγάρι $a, b \in R$,

$$\underbrace{\phi(a+b)}_{\text{πρόσθεση του } R} = \underbrace{\phi(a)}_{\text{πρόσθεση του } S} + \underbrace{\phi(b)}_{\text{πρόσθεση του } S} \quad \text{και} \quad \underbrace{\phi(ab)}_{\text{πολλαπλασιασμός του } R} = \underbrace{\phi(a)}_{\text{πολλαπλασιασμός του } S} \cdot \underbrace{\phi(b)}_{\text{πολλαπλασιασμός του } S}$$

λέγεται ομομορφισμός του R στον S .

Αν, επιπλέον, η ϕ είναι αμφιμοροσήμαντη, τότε έχουμε ένα μονομορφισμό του R στον S , αν η ϕ είναι "έπι", είναι επιμορφισμός

και, τέλος, αν η ϕ είναι αμφιμονοσήμαντη και "έπι", έναν, ισομορφισμό του R επί του S .

Ύεξ ορισμού, αν η ϕ είναι ομομορφισμός του R στον S , θα είναι ομομορφισμός της ομάδας $(R, +)$ στην ομάδα $(S, +)$.

Αντιστρόφως, όμως, αν μια απεικόνιση $\phi: R \rightarrow S$ είναι ομομορφισμός της ομάδας $(R, +)$ στην ομάδα $(S, +)$, δεν έπεται κατ' ανάγκη ότι θα είναι και ομομορφισμός του δακτυλίου R στο δακτύλιο S .

Παράδειγμα: Έστω $R = \mathbb{Z}$ και $S = 2\mathbb{Z}$

(δηλ. S είναι ο δακτύλιος των άρτιων ακεραίων). Η απεικόνιση $\phi: \mathbb{Z} \rightarrow 2\mathbb{Z}$, $\phi(a) = 2a$, είναι, προφανώς, ομομορφισμός της προσθετικής ομάδας $(\mathbb{Z}, +)$ στην προσθετική ομάδα $(2\mathbb{Z}, +)$, δίχως να είναι ομομορφισμός δακτυλίων. Πράγματι, για $a, b \in \mathbb{Z}$ ισχύει $\phi(a \cdot b) = 2ab$ και $\phi(a)\phi(b) = 4ab$, άρα, εν γένει, $\phi(a \cdot b) \neq \phi(a) \cdot \phi(b)$.

Αντίστοιχοι όρισμοί ισχύουν αν οι R, S είναι ακεραίες περιοχές ή σώματα.

Παράδειγματα

α) Έστω ακεραίος $n > 1$. Η απεικόνιση $\phi: \mathbb{Z} \rightarrow \mathbb{Z}_n$

(βλ. παράδειγμα β στην § 1), η οποία ορίζεται απ' τη σχέση $\phi(a) = \bar{a}$ είναι ομομορφισμός δακτυλίων.

β) Έστω ότι R, S είναι δακτύλιοι και $R \times S$ το εϋθύ τους άθροισμα (παράδειγμα 5, § 1). Κάθε μια απ' τις απεικονίσεις $\pi_1: R \times S \rightarrow R$, $\pi_1(r, s) = r$

$$\pi_2: R \times S \rightarrow S, \pi_2(r, s) = s$$

είναι ομομορφισμοί.

γ) Έστω $d \in \mathbb{Z}$, όχι τέλει αριθμο. Θεωρώ τον δακτύλιο

$\mathbb{Z}[\sqrt{d}]$ (βλ. παράδειγμα δ, § 1) και την απεικόνιση

$$\phi: \mathbb{Z}[\sqrt{d}] \longrightarrow \mathbb{Z}[\sqrt{d}], \quad \phi(x+y\sqrt{d}) = x-y\sqrt{d}$$

Η ϕ είναι ισομορφισμός του δακτυλίου $\mathbb{Z}[\sqrt{d}]$ στον εαυτό του.

Γενικά, ένας ισομορφισμός δακτυλίου (άντιστ. άκεραίας περιοχής, σώματος) στον εαυτό του λέγεται αυτομορφισμός του δακτυλίου (άντιστ. της άκεραίας περιοχής, του σώματος).

δ) Ένας πολύ γνωστός αυτομορφισμός του σώματος \mathbb{C} των μιγαδικών αριθμών είναι η απεικόνιση $\bar{\cdot}: \mathbb{C} \rightarrow \mathbb{C}$, η οποία ορίζεται απ' τη σχέση $\overline{x+iy} = x-iy$.

ε) Στο παράδειγμα αυτό θα χρησιμοποιήσουμε συγχρόνως τους τρεις δακτυλίους $\mathbb{Z}_2, \mathbb{Z}_3, \mathbb{Z}_6$. Για να μη γίνει σύγχυση στο συμβολισμό, τις κλάσεις του τυχόνως $a \in \mathbb{Z}$ modulo 2, 3 και 6, αντίστοιχως, θα συμβολίζουμε με $[a]_2, [a]_3, [a]_6$. Θεωρώ τώρα την απεικόνιση

$$\phi: \mathbb{Z}_6 \longrightarrow \mathbb{Z}_2 \times \mathbb{Z}_3, \quad \phi([a]_6) = ([a]_2, [a]_3)$$

Η ϕ είναι ισομορφισμός.

Γενικότερα, αν οι m, n είναι άκεραίοι > 1 , πρώτοι μεταξύ τους, τότε η απεικόνιση $\phi: \mathbb{Z}_{mn} \longrightarrow \mathbb{Z}_m \times \mathbb{Z}_n$,

$$\phi([a]_{mn}) = ([a]_m, [a]_n)$$

είναι ισομορφισμός. Έδω, το δυσκολώτερο είναι να αποδείξει κανείς ότι η ϕ είναι αμφιμοροσημαντική και στο σημείο αυτό σημαντικό ρόλο παίζει η υπόθεση ότι οι m, n είναι πρώτοι μεταξύ τους.

Πρόταση 1. Έστω ότι R, S είναι δακτύλιοι και $\phi: R \longrightarrow S$ ομομορφισμός. Τότε

$$\alpha) \quad \phi(0) = 0 \in S$$

\uparrow
 $0 \in R$

$$\beta) \quad \phi(-r) = -\phi(r) \quad \forall r \in R.$$

γ) Έστω ότι ο R έχει μονάδα και ότι ο S είναι απέραια περιοχή. Αν ο ϕ δεν είναι ο μηδενικός ομομορφισμός (δηλ. αν $\phi(R) \neq \{0\}$), τότε $\phi(1) = 1$.

$\uparrow \in R$ $\uparrow \in S$

δ) Μέχρι υποθέσεις του γ), έστω επιπλέον ότι για το $r \in R$ υπάρχει το αντίστροφο του r^{-1} . Τότε υπάρχει και το αντίστροφο του $\phi(r) \in S$ και, μάλιστα, $\phi(r)^{-1} = \phi(r^{-1})$.

ε) Έστω ότι ο ϕ είναι ισομορφισμός. Αν ο R έχει μονάδα, τότε και ο S έχει και, μάλιστα, η μονάδα του S είναι η $\phi(1)$, όπου 1 η μονάδα του R .

ς) Έστω ότι ο ϕ είναι ισομορφισμός. Αν ο R είναι αντιμεταθετικός δακτύλιος ή απέραια περιοχή ή σώμα, τότε και ο S είναι αντιμεταθετικός δακτύλιος ή απέραια περιοχή ή σώμα, αντιστοίχως.

ζ) Έστω ότι ο ϕ είναι ισομορφισμός. Τότε και η απεικόνιση $\phi^{-1}: S \rightarrow R$ (η οποία είναι καλά ορισμένη, αφού η ϕ είναι αμφιμονοσήμαντη και "έπι") είναι ισομορφισμός.

Επιπλέον, αν T είναι δακτύλιος και $\psi: S \rightarrow T$ ισομορφισμός, τότε η απεικόνιση $\psi \circ \phi: R \rightarrow T$ είναι ισομορφισμός.

[Το (ζ) έχει, λοιπόν, ως άμεση συνέπεια το ότι η σχέση ισομορφίας μεταξύ δακτύλιων (και, εντελώς ανάλογα, μεταξύ απεραίων περιοχών ή σωμάτων) είναι σχέση ισοδυναμίας, η οποία συμβολίζεται με \cong].

Απόδειξη. Δίνεται ως άσκηση.

Όρισμός. Έστω δακτύλιος R . Αν υπάρχει θετικός ακέραιος n τέτοιος ώστε $n \cdot a = 0 \quad \forall a \in R$, τότε ο ελάχιστος τέτοιος n λέγεται χαρακτηριστική του R . Αν δεν υπάρχει τέτοιος n , τότε, εξ' ορισμού, η χαρακτηριστική του R είναι 0.

Στην περίπτωση δακτύλιων με μονάδα, χρήσιμη είναι η εξής πρόταση:

Πρόταση 2. Έστω R δακτύλιος με μονάδα. Η χαρακτηριστική του R ισούται με τον ελάχιστο μη αρνητικό ακέραιο n για τον οποίο $n \cdot 1 = 0$.

Απόδειξη. Έστω n η χαρακτηριστική του R . Τότε $n \cdot 1 = 0$. Ισχυρίζομαι ότι δεν υπάρχει μη αρνητικός ακέραιος $m < n$ με $m \cdot 1 = 0$. Πράγματι, αν υπήρχε, τότε για κάθε $r \in R$ θα είχαμε $m \cdot r = m \cdot (1 \cdot r)$ (τό 1 είναι η μονάδα του R)
 $= (m \cdot 1) \cdot r$ (Πρόταση 15, §1)
 $= 0 \cdot r = 0$ (Πρόταση 15, §1),
 και θα ερχόμαστε σε αντίφαση με τον ορισμό του n , δι.έ.δ.

Παράδειγμα: Αν ο n είναι ακέραιος > 1 , τότε η χαρακτηριστική του δακτύλιου \mathbb{Z}_n είναι n . Πράγματι, η μονάδα του \mathbb{Z}_n είναι $\hat{1}$ και $n \cdot \hat{1} = \hat{n} = \hat{0}$. Αφ' ετέρου, αν υπήρχε θετικό $m < n$ τέτοιο ώστε $m \cdot \hat{1} = \hat{0}$, αυτό θα σήμαινε ότι $m \cdot 1 = 0$, δηλαδή, ότι $n | m$, κάτι αδύνατον, αφού $0 < m < n$. Σε αντίθεση με αυτό το παράδειγμα, ο δακτύλιος \mathbb{Z} και τα σώματα $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ έχουν χαρακτηριστική 0.

Πρόταση 3. Έστω D ακεραία περιοχή. Τότε η χαρακτηριστική της D είναι ή 0 ή πρώτος p . Στην πρώτη περίπτωση η D περιέχει έναν υποδακτύλιο ισόμορφο προς τον \mathbb{Z} και στη δεύτερη περίπτωση περιέχει έναν υποδακτύλιο ισόμορφο προς το σώμα \mathbb{Z}_p (βλ. πρόταση της Πρότασης 6, § 1).

Απόδειξη. Έστω ότι η D έχει χαρακτηριστική $p > 0$. Αν ο p ήταν σύνθετος, $p = q \cdot r$ με $1 < q, r < p$, τότε $0 = p \cdot 1 = (q \cdot r) \cdot 1 = (q \cdot r) \cdot (1 \cdot 1) = (q \cdot 1) \cdot (r \cdot 1)$. Έπειδή η D είναι ακεραία περιοχή, πρέπει $q \cdot 1 = 0$ είτε $r \cdot 1 = 0$, άρα, λόγω της πρότασης 2, η χαρακτηριστική της D θα είναι μικρότερη ή ίση απ' το q είτε απ' το r άρα, όπωςδήποτε, μικρότερη απ' το p άτοπο.

Στην περίπτωση που η χαρακτηριστική είναι 0 , θεωρώ την απεικόνιση $\phi: \mathbb{Z} \rightarrow D$, $\phi(m) = m \cdot 1$. Εύκολα διαπιστώνεται ότι η ϕ είναι μονομορφισμός δακτυλίων, συνεπώς το $\phi(\mathbb{Z})$ είναι ισόμορφο προς το \mathbb{Z} και, προφανώς, υποδακτύλιος του D .

Τέλος, αν η χαρακτηριστική είναι p (πρώτος), τότε η απεικόνιση $\psi: \mathbb{Z}_p \rightarrow D$, $\psi(\bar{m}) = m \cdot 1$ είναι μονομορφισμός και το $\psi(\mathbb{Z}_p)$ είναι σώμα ισόμορφο προς το \mathbb{Z}_p , υπόσωμα της ακεραίας περιοχής D .

Πρόταση 4. Για κάθε ακεραία περιοχή D υπάρχει ένα σώμα F_D με τις εξής ιδιότητες (i) Το F_D περιέχει μια ακεραία περιοχή Δ ισόμορφη προς την D (ii) Κάθε στοιχείο του F_D γράφεται υπό την μορφή

$$\delta_1 \delta_2^{-1}, \text{ όπου } \delta_1, \delta_2 \in \Delta \text{ και } \delta_2 \neq 0.$$

Το F_D είναι μοναδικό μέχρι ισομορφισμού. Δηλαδή, αν

ώ F είναι ένα σώμα, που πληροί τις συνθήκες (i) και (ii), τότε $F \cong F_D$.

Απόδειξη. Συμβολίζουμε $D^* = D - \{0\}$. Στο σύνολο $D \times D^*$ ορίζουμε τη σχέση \sim ως εξής:

$$(a_1, b_1) \sim (a_2, b_2) \iff a_1 b_2 = a_2 b_1.$$

Εύκολα αποδεικνύεται ότι η \sim είναι σχέση ισοδυναμίας. Την κλάση ισοδυναμίας του τυχόντος $(a, b) \in D \times D^*$ συμβολίζουμε με $\frac{a}{b}$. (Παρατηρήστε ότι, μέχρι στιγμής, δεν έχουμε ξαναχρησιμοποιήσει το σύμβολο $\frac{a}{b}$). Συνεπώς,

$$\frac{a_1}{b_1} = \frac{a_2}{b_2} \iff a_1 b_2 = a_2 b_1.$$

Το σύνολο των κλάσεων ισοδυναμίας συμβολίζουμε με F_D . Δηλαδή, $F_D = \{ \frac{a}{b} : (a, b) \in D \times D^* \}$.

Στο F_D ορίζουμε πρόσθεση και πολλαπλασιασμό ως εξής:

$$\frac{a_1}{b_1} + \frac{a_2}{b_2} = \frac{a_1 b_2 + a_2 b_1}{b_1 b_2}, \quad \frac{a_1}{b_1} \cdot \frac{a_2}{b_2} = \frac{a_1 a_2}{b_1 b_2}$$

Οι πράξεις αυτές είναι καλά ορισμένες. Δηλαδή, αν

$$\frac{a_1}{b_1} = \frac{c_1}{d_1} \quad \text{κ} \quad \frac{a_2}{b_2} = \frac{c_2}{d_2} \quad \text{τότε} \quad \frac{a_1 b_2 + a_2 b_1}{b_1 b_2} = \frac{c_1 d_2 + c_2 d_1}{d_1 d_2} \quad \text{και}$$

$$\frac{a_1 a_2}{b_1 b_2} = \frac{c_1 c_2}{d_1 d_2} \quad (\text{η απόδειξη αφήνεται ως άσκηση}).$$

Άρσως διαπιστώνεται ότι το $\frac{0}{1}$ είναι το ουδέτερο στοιχείο της πρόσθεσης (μηδέν) και το $\frac{1}{1}$ το ουδέτερο στοιχείο του πολλαπλασιασμού (μονάδα). Το αντίθετο του $\frac{a}{b}$ είναι το $-\frac{a}{b}$ και το αντίστροφο του $\frac{a}{b} \neq \frac{0}{1}$ είναι το $\frac{b}{a}$.

Ύστερα από αυτές τις παρατηρήσεις, είναι εύκολο ν' αποδείξει κανείς ότι το F_D με τις ορισθείσες πράξεις γίνεται σώμα. Εύκολα, επίσης, με τη βοήθεια της Πρότασης 4, §1, αποδεικνύ-

εσται ότι τό $\Delta = \left\{ \frac{a}{1} : a \in D \right\} \subseteq F_D$ είναι άκέραια περιοχή και ένας προφανής ισμορφισμός μεταξύ της D και της Δ είναι

$$D \ni a \longmapsto \frac{a}{1} \in \Delta.$$

Συνεπώς, ικανοποιείται η συνθήκη (i).

Η συνθήκη (ii) ικανοποιείται προφανώς. Δείξτε τό τυχόν στοιχείο του F είναι της μορφής $\frac{a}{b}$, όπου $a, b \in D$, $b \neq 0$.

Άρα, $\frac{a}{b} = \left(\frac{a}{1}\right) \cdot \left(\frac{b}{1}\right)^{-1}$ με τό $\frac{a}{1}, \frac{b}{1} \in \Delta$.

Μένει να αποδειχθεί η μοναδικότης, μέχρι ισμορφισμού, του F_D . Έστω λοιπόν σώμα F , A άκέραια περιοχή $\subseteq F$,

$A \cong D$ και κάθε στοιχείο του F είναι της μορφής $\alpha_1 \alpha_2^{-1}$, όπου $\alpha_1, \alpha_2 \in A$ και $\alpha_2 \neq 0$. Θα δείξουμε ότι $F \cong F_D$.

Πράγματι, έστω $\psi: D \rightarrow A$ ισμορφισμός. Τότε θεωρώ την άπεικόνιση

$$\phi: F_D \rightarrow F, \quad \phi\left(\frac{a}{b}\right) = \psi(a) \cdot \psi(b)^{-1}$$

Η ϕ είναι καλά ορισμένη: Αν $\frac{a_1}{b_1} = \frac{a_2}{b_2}$ τότε $a_1 b_2 = a_2 b_1$.

Λόγω του ισμορφισμού ψ , $\psi(a_1) \psi(b_2) = \psi(a_2) \psi(b_1)$ και $\psi(b_1), \psi(b_2) \neq 0$. Άρα, $\psi(a_1) \psi(b_1)^{-1} = \psi(a_2) \psi(b_2)^{-1}$, δηλ.

$$\phi\left(\frac{a_1}{b_1}\right) = \phi\left(\frac{a_2}{b_2}\right).$$

Με ανάλογο τρόπο αποδεικνύεται ότι η ϕ είναι άμφιμονοσήρακτη.

Η ϕ είναι "έπι": Έστω $f \in F$. Τότε $f = \alpha_1 \alpha_2^{-1}$, $\alpha_1, \alpha_2 \in A$, $\alpha_2 \neq 0$.

Άρα υπάρχουν $b, c \in D$, $c \neq 0$ τέτοια ώστε $\psi(b) = \alpha_1$, $\psi(c) = \alpha_2$,

$$\text{συνεπώς } f = \alpha_1 \alpha_2^{-1} = \psi(b) \psi(c)^{-1} = \phi\left(\frac{b}{c}\right)$$

Τέλος, τό ότι η ϕ είναι ισμορφισμός, αποδεικνύεται εύκολα αν ληφθεί υπ' όψη ότι η ψ είναι ισμορφισμός, ο.έ.δ.

Όρισμός. Έστω D άκέραια περιοχή. Το μοναδικό, μέχρι ισομορφισμού, σώμα F_D , του οποίου η ύπαρξη εξασφαλίζεται απ' την τελευταία πρόταση, λέγεται σώμα πηλίκων της D .

3. Πυρήνας όμομορφισμού • Ίδεώδη • Δακτύλιος-πηλίκο.

Όρισμός. Έστω R δακτύλιος. Ο υποδακτύλιος I του R λέγεται ιδεώδες του R αν για κάθε $r \in R$ και για κάθε $i \in I$ ισχύει $ir \in I$ και $ri \in I$. Ο μηδενικός δακτύλιος $\{0\}$ καθώς και ο ίδιος ο R είναι ιδεώδη, τα λεγόμενα τετριμμένα ιδεώδη του R .

Πρόταση 1. Έστω $\phi: R \rightarrow S$ όμομορφισμός δακτυλίων.

α) Η εικόνα του ϕ (που συμβολίζεται $\text{Im } \phi$ ή $\phi(R)$) είναι υποδακτύλιος του S .

β) Ο πυρήνας του ϕ , $\text{Ker } \phi \stackrel{\text{def}}{=} \{r \in R : \phi(r) = 0 \in S\}$ είναι ιδεώδες του R .

γ) Ο ϕ είναι μονομορφισμός αν και μόνο αν $\text{Ker } \phi = \{0\}$.

Απόδειξη. α) Άμεση συνέπεια της Πρότασης 4, § 1.

β) Το ότι ο $\text{Ker } \phi$ είναι υποδακτύλιος του R , είναι άμεση συνέπεια της Πρότασης 4, § 1. Αν τώρα $r \in \text{Ker } \phi$ και $a \in R$, τυχόν, τότε $\phi(ar) = \phi(a)\phi(r) = \phi(a) \cdot 0 = 0$ και, ανάλογα, $\phi(ra) = 0$. Άρα $ar \in \text{Ker } \phi$ και $ra \in \text{Ker } \phi$.

γ) Έστω ότι ο ϕ είναι μονομορφισμός. Έπειδη $\phi(0) = 0$, έπεται ότι δεν μπορεί να υπάρχει $r \neq 0$ με $\phi(r) = 0$, άρα $\text{Ker } \phi = \{0\}$.

Αντιστρόφως, έστω $\text{Ker } \phi = 0$. Θα δείξω ότι η ϕ είναι άμφιμοσημαντη. Πράγματι, αν $\phi(r_1) = \phi(r_2)$, τότε $\phi(r_1 - r_2) = 0$, δηλ.

$r_1, r_2 \in \text{Ker } \phi = \{0\}$, οπότε $r_1 = r_2$, άί έί δ.

Όρισμός. Έστω R αντιμεταθετικός δακτύλιος με μονάδα. Τό ιδεώδες I του R λέγεται κύριο ιδεώδες, αν υπάρχει $a \in R$ τέτοια ώστε $I = aR = Ra \stackrel{\text{ή}}{=} \{ra : r \in R\}$.

Έστω R αντιμεταθετικός δακτύλιος με μονάδα. Τό κύριο ιδεώδες $aR = Ra$ τό συμβολίζουμε, επίσης, με $\langle a \rangle$ ή (a) . προφανώς, είναι τό ελάχιστο ιδεώδες του R , τό οποίο περιέχει τό a . Τό $\langle a \rangle$ λέγεται κύριο ιδεώδες που παράγεται άπ' τό a . Άς τονίσαμε σ' αυτό τό σημείο ότι ο R , αν γενεί, περιέχει και ιδεώδη, τά οποία δέν είναι κύρια * βλ. π.χ. τό παράδειγμα δ, παρακάτω.

Παραδείγματα I

α) Ο επιμορφισμός $\phi: \mathbb{Z} \rightarrow \mathbb{Z}_n$, $\phi(a) = \bar{a}$ (βλ. παράδειγμα (α), §2) έχει πυρήνα $\text{Ker } \phi = n\mathbb{Z}$ (κύριο ιδεώδες).

β) Έστω R αντιμεταθετικός δακτύλιος με μονάδα και $a_1, \dots, a_n \in R$ (σταθερά). Τό σύνολο

$$\{r_1 a_1 + \dots + r_n a_n : r_1, \dots, r_n \in R\}$$

συμβολίζεται με $Ra_1 + \dots + Ra_n$ ή $\langle a_1, \dots, a_n \rangle$ ή

(a_1, \dots, a_n) . Είναι ιδεώδες και, μάλλον, τό ελάχιστο ιδεώδες του R , τό οποίο περιέχει τά a_1, \dots, a_n (ή άπιδείδη είναι άπλη).

Όνομάζεται ιδεώδες (του R) παραγόμενο άπ' τά a_1, \dots, a_n . Για $n=1$ έχουμε κτηεϊδική περίπτωση του κυρίου ιδεώδους, που παράγεται άπ' τό a_1 .

γ) Όλα τά ιδεώδη του \mathbb{Z} είναι κύρια. Πράγματι, έστω I ιδεώδες του \mathbb{Z} . Αν $I = \{0\}$, τότε $I = 0\mathbb{Z}$. Αν $I \neq \{0\}$, θεωρώ $a \in I$, $a \neq 0$. Επειδή τό I είναι δακτύλιος, θα είναι και $-a \in I$,

Άρα το I περιέχει θετικό στοιχείο, άρα μπορούμε να θεωρήσουμε το ελάχιστο θετικό στοιχείο του I , έστω n . Αφού $n \in I$, θα είναι και $n\mathbb{Z} \subseteq I$. Ίσχύει όμως και το αντίστροφο:

Έστω $m \in I$. Από την ταυτότητα της διαίρεσης, $m = n \cdot q + r$ και $0 \leq r < n$, άρα $r = m - q \cdot n \in I$ (δίδει $m \in I$ και $n \in I$).

Αν ήταν $r \neq 0$, τότε το I θα περιείχε θετικό στοιχείο $< n$, και θα έρχόμαστε σε αντίφαση με την εκλογή του n . Άρα, $r = 0$ και $m = n \cdot q \in n\mathbb{Z}$. Συμπέρασμα: $I = n\mathbb{Z}$, ο.έ.δ.

δ) Παράδειγμα μη κύριου ιδεώδους: Έστω ο δακτύλιος

$$R = \{x + y\sqrt{-5} : x, y \in \mathbb{Z}\} \quad (\text{βλ. παράδειγμα } \delta, \S 1)$$

και το ιδεώδες, που παράγεται από τα στοιχεία 2 και $1 + \sqrt{-5}$ του R , $I = \langle 2, 1 + \sqrt{-5} \rangle$ (βλ. παράδειγμα β, παρασενω).

Το I δεν είναι κύριο. Πράγματι, ως υποθέσουμε τα αντίθετα θέτοντας $I = R \cdot (A + B\sqrt{-5})$ ($A, B \in \mathbb{Z}$).

Επειδή $1 + \sqrt{-5} \in I$, θα έχουμε μία ισότητα της μορφής

$$\begin{aligned} 1 + \sqrt{-5} &= (x + y\sqrt{-5})(A + B\sqrt{-5}) \quad \text{με } x, y \in \mathbb{Z} \\ &= (Ax - 5By) + (Bx + Ay)\sqrt{-5} \end{aligned}$$

Λύνοντας το σύστημα $\begin{cases} Ax - 5By = 1 \\ Bx + Ay = 1 \end{cases}$, βρίσκουμε

$$x = \frac{A + 5B}{A^2 + 5B^2}, \quad y = \frac{A - B}{A^2 + 5B^2} \quad \text{και διακρίνουμε δύο περιπτώσεις:}$$

(i) $A = B$. Τότε $x = \frac{1}{A}$ και επειδή $x \in \mathbb{Z}$ πρέπει $A = \pm 1$. Άρα, σ' αυτή την περίπτωση $A + B\sqrt{-5} = \pm(1 + \sqrt{-5})$. Τώρα, επειδή και $2 \in I$, πρέπει $2 = (1 + \sqrt{-5})(u + v\sqrt{-5})$ για κάποια $u, v \in \mathbb{Z}$.

Παίρνοντας συζυγείς μιγαδικούς: $2 = (1 - \sqrt{-5})(u - v\sqrt{-5})$ και πολλαπλασιάζοντας τις δύο συζυγείς σχέσεις: $4 = 6(u^2 + 5v^2)$, δηλ. οδηγούμαστε σε αδύνατη ισότητα.

(ii) $A \neq B$. Τότε $1 \leq |A - B| \leq |A| + |B| < A^2 + B^2 < A^2 + 5B^2$ αν $B \neq 0$. Συνεπώς, αν $B \neq 0$, τότε $0 < |y| = \frac{|A - B|}{A^2 + 5B^2} < 1$, άτοπο, αφού $y \in \mathbb{Z}$.

Και ανάλυση, λοιπόν, $B=0$, οπότε $x=y=\frac{1}{A}$. Άρα $A=\pm 1$ (αφού $x, y \in \mathbb{Z}$) και, συνεπώς, $A+B\sqrt{-5}=\pm 1$, που σημαίνει ότι $I=R(A+B\sqrt{-5})=R$. Αυτό είναι άρα το ίδιο $1 \in R$ ενώ $1 \notin I$. Πράγματι, αν ήταν $1 \in I$, τότε

$$1 = 2(a+b\sqrt{-5}) + (1+\sqrt{-5})(c+d\sqrt{-5}),$$

για κατάλληλους άκεραίους a, b, c, d . Τότε

$2a+c-5d=1$ και $2b+c+d=0$. Λύνοντας τη δεύτερη ως προς d και αντικαθιστώντας στην πρώτη, βρίσκω $2a+10b+5c=1$, άρα, αφού το αριστερό μέλος είναι άρτιος άκεραίος.

ε) Τα μόνα ιδεώδη ενός οποιουδήποτε σώματος είναι τα τετριμμένα. Διότι, έστω I ιδεώδες του σώματος F . Αν $I \neq \{0\}$, θεωρώ $a \in I, a \neq 0$. Επειδή $a^{-1} \in F$ και $a \in I$, πρέπει $a^{-1}a \in I$, δηλ. $1 \in I$. Τότε, για κάθε $f \in F$ πρέπει $f \cdot 1 \in I$, δηλ. $F \subseteq I$, άρα $F=I$.

Έστω R δακτύλιος και I ιδεώδες του R . Το I είναι κανονική υποομάδα της ομάδας $(R, +)$, άρα ορίζεται η άβραδα-πηλίκο R/I , της οποίας η πράξη, όπως είναι γνωστό, συμβολίζεται με $+$ και ορίζεται: $(r_1 + I) + (r_2 + I) = (r_1 + r_2) + I$

\uparrow πράξη του R/I \uparrow πράξη του R

Μπορούμε να εφοδιάσουμε, έντελως φυσικά, το R/I με ένα πολλαπλασιασμό ως εξής:

$$(r_1 + I) \cdot (r_2 + I) = r_1 \cdot r_2 + I$$

\uparrow πράξη του R/I \uparrow πράξη του R

Είναι εύκολο να διαπιστώσει κανείς ότι η πράξη αυτή είναι καλά ορισμένη και το R/I με ως παραπάνω ορισθείσες πράξεις είναι δακτύλιος. Επιπλέον, αν ο R έχει μονάδα 1 τότε και ο R/I έχει μονάδα την $1+I$. Αν ο R είναι αντιμεταθετικός, τότε το ίδιο ισχύει και για το R/I .

Ο δακτύλιος-πηλίκο που ορίσθηκε έχει ως στοιχεία άριστερες κλάσεις· αυτά δεν είναι ουσιαστές, αφού $r+I = I+r \quad \forall r \in R$ (η ομάδα $(R,+)$ είναι αβελιανή). Συνεπώς, θα μπορούσε κανείς, αδιακρίτως, να κάνει χρήση άριστερών είτε δεξιών κλάσεων.

Παρατηρήστε ότι, ενώ οι ιδιότητες της ύπαρξης μονάδας και της ανυμεταθετικότητας μεταφέρονται απ' τον R στον R/I , η ιδιότητα της μη ύπαρξης μηδενοδιακριτών δεν μεταφέρεται απ' τον R στον R/I . (βλ. παράδειγμα (α) παρακάτω). Συνεπώς, αν ο R είναι ακέραια περιοχή, δεν έπεται κατ' ανάγκη ότι και ο R/I είναι ακέραια περιοχή.

Πρόταση 2 Έστω R δακτύλιος και I ιδεώδες του R .

Η απεικόνιση $\pi: R \rightarrow R/I$, $\pi(r) = r+I$ είναι δμορφισμός δακτυλίων με $\ker \pi = I$.

Η απόδειξη αφήνεται ως άκλη άσκηση.

Θεμελιώδες Θεώρημα δμορφισμού δακτυλίων.

Έστω $\phi: R \rightarrow S$ δμορφισμός δακτυλίων. Τότε

$$\text{Im } \phi \cong R/\ker \phi$$

Απόδειξη. Η πρόταση 1 λέει $\text{Im } \phi$ είναι υποδακτύλιος, έστω S' του S και $\ker \phi$ είναι ιδεώδες, έστω I , του R . Έχω να δείξω ότι $S' \cong R/I$. Θεωρώ την απεικόνιση

$$\psi: R/I \rightarrow S', \quad \psi(r+I) = \phi(r)$$

Η ψ είναι ο ζητούμενος ισομορφισμός. Πράγματι, πρώτα απ' όλα είναι καλά ορισμένη: Έστω $r_1+I = r_2+I$. Τότε $r_1 - r_2 \in I = \ker \phi$, άρα $\phi(r_1 - r_2) = 0$, συνεπώς $\phi(r_1) = \phi(r_2)$.

έτσι, $\psi(r_1 + I) = \psi(r_2 + I)$. Η ψ είναι αμφιμονοσήμαντη διότι, έστω $\psi(r_1 + I) = \psi(r_2 + I)$. Τότε $\phi(r_1) = \phi(r_2)$, $\phi(r_1 - r_2) = 0$, άρα $r_1 - r_2 \in \text{Ker } \phi = I$ και αυτό σημαίνει ότι $r_1 + I = r_2 + I$. Η ψ είναι "έπί": προφανώς, διότι κάθε $s \in S'$ είναι της μορφής $\phi(r)$ (αφού $S' = \text{Im } \phi$), άρα $s = \phi(r) = \psi(r + I)$. Τέλος, η ψ είναι ομομορφισμός, διότι $\psi[(r_1 + I) + (r_2 + I)] = \psi[(r_1 + r_2) + I] = \phi(r_1 + r_2) = \phi(r_1) + \phi(r_2) = \psi(r_1 + I) + \psi(r_2 + I)$.

§ 2.5

Παραδείγματα II

α) Θεωρώ τον έπιμορφισμό $\phi: \mathbb{Z} \rightarrow \mathbb{Z}_n$ του παραδείγματος 1, α, ο οποίος, όπως είδαμε, έχει πυρήνα $n\mathbb{Z}$. Συνεπώς, από το θεώρημα, $\mathbb{Z}_n \cong \mathbb{Z}/n\mathbb{Z}$. Αν ο n είναι σύνθετος, ο \mathbb{Z}_n έχει μηδενοδιαίρετες ($n = n_1 n_2$ με $1 < n_1, n_2 < n \Rightarrow \hat{n}_1 \cdot \hat{n}_2 = \hat{n} = \hat{0}$), άρα και ο $\mathbb{Z}/n\mathbb{Z}$ έχει μηδενοδιαίρετες, παρά το γεγονός ότι ο \mathbb{Z} δεν έχει.

β) Θεωρώ τους έπιμορφισμούς του παραδείγματος β, § 2.

Για τον έπιμορφισμό $\pi_1: R \times S \rightarrow R$ είναι προφανές ότι $\text{Ker } \pi_1 = \{(0, s) : s \in S\}$. Λόγω του θεωρήματος, $R \cong \frac{R \times S}{\text{Ker } \pi_1}$. Αφ' έτέρου είναι εύκολο να δεί κανείς ότι ο $\text{Ker } \pi_1$ είναι υποδακτύλιος του $R \times S$ και, μάλιστα, ισόμορφος του S . Άρα $\frac{R \times S}{\text{Ker } \pi_1} \cong \frac{R \times S}{S}$, άρα, σύμφωνα και με την παρα-

πάνω σχέση ισομορφίας, $R \cong \frac{R \times S}{S}$ (σχέση που θυμίζει άπλοποίηση με αριθμούς!)

Σε αντιμεταθετικούς δακτυλίους με μονάδα, οι έννοιες του πρώτου και του maximal ιδεώδους είναι πολύ χρήσιμες (κυρίως λόγω της πρότασης 3 παραπάνω). Ένα

ιδεώδες I του δακτυλίου R λέγεται πρώτο αν $I \neq R$ και το I έχει την ιδιότητα: αν $ab \in I$ & $ab \notin I$ τότε $a \in I$ είτε $b \in I$. Παρατηρήστε ότι το $\{0\}$ είναι πρώτο ιδεώδες αν και μόνο αν ο R είναι άκεραια περιοχή.

Το ιδεώδες I του R λέγεται maximal αν $I \neq R$ και δεν υπάρχει ιδεώδες J του R με $I \subsetneq J \subsetneq R$. Μ' άλλα λόγια, η χαρακτηριστική ιδιότητα του maximal ιδεώδους είναι η έξης: αν το I είναι maximal και J είναι ένα ιδεώδες του R , τέτοιο ώστε $I \subseteq J \subseteq R$, τότε ή $J = I$ ή $J = R$. Παρατηρήστε ότι, το $\{0\}$ είναι maximal αν και μόνο αν ο R είναι σώμα. Πράγματι, αν ο R είναι σώμα, τότε κάθε ιδεώδες $J \neq \{0\}$ περιέχει στοιχείο $r \neq 0$. Επειδή υπάρχει το $r^{-1} \in R$, θα πρέπει $r^{-1} \cdot r \in J$, δηλ. $1 \in J$. Τότε όρως, για κάθε $a \in R$ θα είναι $a \cdot 1 \in J$, άρα $R \subseteq J$, δηλ. $R = J$, οπότε αποκλείεται μια σχέση $\{0\} \subsetneq J \subsetneq R$. Άρα το $\{0\}$ είναι maximal. Αντιστρόφως, αν το R δεν είναι σώμα, θα υπάρχει $r \in R$, $r \neq 0$, μη αντιστρέψιμο. Αυτό συνεπάγεται ότι το ιδεώδες $R \cdot r$ είναι $\neq R$ (π.χ. $1 \notin R \cdot r$), άρα $\{0\} \subsetneq R \cdot r \subsetneq R$, δηλ. το $\{0\}$ δεν είναι maximal.

Πρόταση 3. Έστω R αντιμεταθετικός δακτύλιος με μονάδα ($\neq 0$) και I ιδεώδες του R . (α) Το I είναι πρώτο ιδεώδες αν και μόνο αν ο δακτύλιος R/I είναι άκεραια περιοχή. (β) Το I είναι maximal ιδεώδες αν και μόνο αν ο δακτύλιος R/I είναι σώμα. (γ) Αν το I είναι maximal, τότε είναι και πρώτο.

Απόδειξη. (α) Έστω ότι το I είναι πρώτο ιδεώδες. Έχω να δείξω ότι, αν $a+I, b+I \in R/I$ και δεν είναι μηδενικά

(δηλ. $a+I, b+I \neq 0+I=I$) τότε $(a+I)(b+I) \neq I$.

Πράγματι, $(a+I)(b+I) = ab+I$. Αν ήταν $ab+I=I$, τότε $ab \in I$: όμως το I έχει υποτεθεί πρώτο, άρα $a \in I$ είτε $b \in I$, που σημαίνει $a+I=I$ είτε $b+I=I$, σε αντίθεση με την υπόθεση. Άρα ο R/I δεν έχει μηδενοδιαίρετες. Μένει ακόμη και σχολαστικό! Να δείξω ότι $0+I \neq 1+I$. Πράγματι, αν είχα ισότητα, $1 \in I$, δηλαδή $R=I$, και που αντίκειται στον όρισμό του πρώτου ιδεώδους.

Αντιστρόφως, έστω R/I ανέραια περιοχή. Τότε $0+I \neq 1+I$, άρα $1 \notin I$, άρα $I \neq R$. Επίσης, αν $a, b \in R$ και $a, b \in I$, τότε $ab+I=0+I$, δηλ. $(a+I)(b+I)=0+I$, άρα (λόγω της υπόθεσης) $a+I=I$ είτε $b+I=I$, δηλ. $a \in I$ είτε $b \in I$. Συνεπώς το I είναι πρώτο ιδεώδες.

(β) Έστω ότι το I είναι maximal ιδεώδες του R . Τότε $I \neq R$ άρα, όπως στο (α), βλέπουμε ότι $1+I \neq 0+I$. Μένει να δείξω ότι κάθε $a+I \in R/I$, μη μηδενικό, έχει αντίστροφο. Πράγματι, από την υπόθεση $a+I \neq I$ έπεται $a \notin I$, άρα το ιδεώδες $J \stackrel{\text{def}}{=} I + aR \stackrel{\text{def}}{=} \{i + a \cdot r : i \in I, r \in R\}$ περιέχει γνησίως το I συνεπώς $J=R$ (αφού το I είναι maximal). Άρα $1 \in J$, που σημαίνει ότι υπάρχουν $i \in I$ και $r \in R$ τ.ώ. $1 = i + a \cdot r$. Τότε $(a+I)(r+I) = ar+I = 1-i+I = 1+I$ (μονάδα του R/I , άρα $r+I = (a+I)^{-1}$).

Αντιστρόφως, αν το R/I είναι σώμα τότε, όπως στο (α), $I \neq R$. Μένει να δείξω ότι αν το J είναι ιδεώδες του R , που περιέχει γνησίως το I , τότε $J=R$. Πράγματι, έστω $a \in J - I$. Τότε $a+I$ είναι μη μηδενικό στοιχείο του σώματος R/I , άρα υπάρχει $b+I \in R/I$ τ.ώ. $(a+I)(b+I) = 1+I$, δηλ. $ab+I = 1+I$, άρα $1-ab \in I$. Συνεπώς, υπάρχει $i \in I$ ο.ώ. $1 = ab+i$. Όμως $a \in J$ ή $i \in I \subseteq J$, άρα $1 \in J$, που συνεπάγεται $J=R$.

(γ) Αν \mathcal{I} είναι maximal ιδεώδες του R τότε, λόγω του (β), ο δακτύλιος R/\mathcal{I} είναι σώμα. Ειδικότερα, είναι άκεραία περιοχή άρα, λόγω του (α) \mathcal{I} είναι πρώτο ιδεώδες του R .
 ο.ε.δ.

Τονίζω εδώ ότι \mathcal{I} αντίστροφο του (γ) δεν ισχύει. Δηλαδή, υπάρχουν πρώτα ιδεώδη σε κάποιο δακτύλιο, τα οποία δεν είναι maximal. Ένα τέτοιο παράδειγμα θα δοθεί αργότερα.

4. Πολυώνυμα.

Έστω R αντιμεταθετικός δακτύλιος. Κάθε τυπικό άθροισμα της μορφής $a_n t^n + a_{n-1} t^{n-1} + \dots + a_1 t + a_0$, όπου $a_0, a_1, \dots, a_n \in R$, $n \geq 0$ (για $n=0$, $a_n t^n$ σημαίνει a_0) λέγεται πολυώνυμο με συντελεστές απ' τον R . Τυπικό άθροισμα, σημαίνει ότι το γράμμα t (που ονομάζεται μεταβλητή και θα μπορούσε, επίσης να συμβολιστεί και με άλλο γράμμα) δεν έχει κάποια σημασία (ειδικότερα, το t δεν είναι στοιχείο του R) και, αλόγη, ότι γράφοντας π.χ. $a_k t^k$ δεν εννοούμε κάποιο πολλαπλασιασμό, ούτε το $+$, που εμφανίζονται στο πολυώνυμο, υποδηλώνουν κάποια πρόσθεση.

Κάνουμε την έξης σύμβαση: Τα πολυώνυμα $a_n t^n + \dots + a_1 t + a_0$ και $a_k t^k + \dots + a_1 t + a_0$ θεωρούνται ίσα για οποιοδήποτε φυσικό αριθμό k .

Συνήθως, φροντίζουμε όταν γράφουμε ένα πολυώνυμο, π.χ. $a_n t^n + \dots + a_1 t + a_0$, να υποθέτουμε $a_n \neq 0$. Στην περίπτωση αυτή το $a_n t^n$ λέγεται μεγιστοβάθμιος όρος του πολυωνύμου.

και ο n βαθμός του πολυωνύμου. Το σύνολο των πολυωνύμων με συντελεστές απ' τον R συμβολίζεται $R[t]$ και τα στοιχεία του $R[t]$ (δηλ. τα πολυώνυμα) συμβολίζονται συνήθως $f(t), g(t), h(t)$ κ.λ.π. Ο βαθμός του πολυωνύμου $f(t) \in R[t]$ συμβολίζεται με $\deg f$.

Ίσότητα μεταξύ δύο πολυωνύμων $f(t), g(t) \in R[t]$:

Τα $f(t)$ και $g(t)$ είναι ίσα ($f(t) = g(t)$), εἰς ὄρισμόν, ἂν

i) $\deg f = \deg g = (ἔστω) n$, και

ii) ἂν $f(t) = a_n t^n + \dots + a_1 t + a_0$, $g(t) = b_n t^n + \dots + b_1 t + b_0$

τότε $b_0 = a_0, b_1 = a_1, \dots, b_n = a_n$.

Ίσοδύναμα, ὁ ὄρισμός της ἰσότητας των $f(t), g(t) \in R[t]$

μπορεῖ νὰ διατυπωθεῖ και ὡς ἑξῆς, ἀποφεύγοντας νὰ

κάνουμε μινεία στους βαθμούς: Ἐστω $f(t) = a_n t^n + \dots + a_1 t + a_0$,

$g(t) = b_m t^m + \dots + b_1 t + b_0$ (δὲν ὑποθέτω ὅτι $a_n \neq 0$ ἢ $b_m \neq 0$)

και ἂς ὑποθέσουμε δίχως βλάβη της γενικότητας $n \geq m$.

Τότε, $f(t) = g(t)$ ἂν και μόνο ἂν $b_0 = a_0, b_1 = a_1, \dots, b_m = a_m$

και $a_{m+1} = \dots = a_n = 0$.

Εἰδικώτερα, τὸ πολυώνυμο $f(t)$ εἶναι τὸ μηδενικό πολυώνυμο

(συμβολικά, $f(t) = 0$ και, σπανιώτερα, $f(t) = 0(t)$ ἂν θέ-

λομε ν' ἀντιδιαστείλομε τὸ μηδενικό πολυώνυμο ἀπ' τὸ $0 \in R$),

ἂν και μόνο ἂν $a_0 = a_1 = \dots = a_n = 0$.

Ὅρίζω $\deg 0 = -\infty$. Κάθε πολυώνυμο της μορφῆς a_0

(ἢ, ἰσοδύναμα, της μορφῆς $0 \cdot t^n + 0 \cdot t^{n-1} + \dots + 0 \cdot t + a_0$)

λέγεται σταθερό πολυώνυμο. Τα σταθερά, μη μηδενικά,

πολυώνυμα ἔχουν βαθμό 0. Συνεπῶς, τὸ νὰ γράψαι κανεὶς

$\deg f = 0$, ἰσοδυναμεῖ με τὸ ὅτι τὸ $f(t)$ εἶναι σταθερό, μη μηδενικό,

πολυώνυμο, ἐνῶ γράφοντας $\deg f = -\infty$ ἐννοεῖ ὅτι τὸ $f(t)$ εἶναι μηδενικό.

⊛

ἐκτός ἂν $n=0$ και $a_0=0$ (μηδενικό πολυώνυμο - βλ. παρακάτω).

Στο σύνολο $R[t]$ ορίζουμε πρόσθεση και πολλαπλασιασμό ως εξής: Έστω $f(t), g(t) \in R[t]$. Προκειμένου να ορίσω $f(t) + g(t)$, θεωρώ ότι τα δύο πολυώνυμα ξεκινούν από όρο του ίδιου βαθμού (αν π.χ. $f(t) = at^2 + bt + c$ και $g(t) = d \cdot t + e$, τότε γράφω $g(t) = 0t^2 + dt + e$, έτσι ώστε και τα δύο πολυώνυμα ν' αρχίζουν με όρο βαθμού 2. Θα μπορούσα, επίσης, να έγραφα $f(t) = 0t^3 + at^2 + bt + c$ και $g(t) = 0t^3 + 0t^2 + dt + e$).

Έστω, λοιπόν,
 $f(t) = a_n t^n + \dots + a_1 t + a_0$, $g(t) = b_n t^n + \dots + b_1 t + b_0$.
 Τότε, $f(t) + g(t) \stackrel{\text{ορσ}}{=} (a_n + b_n)t^n + \dots + (a_1 + b_1)t + (a_0 + b_0)$.

Προκειμένου να ορίσω $f(t) \cdot g(t)$, δεν είναι ανάγκη να γράψω τα $f(t), g(t)$ έτσι ώστε ν' αρχίζουν από όρο του ίδιου βαθμού. Έστω $f(t) = a_n t^n + \dots + a_1 t + a_0$,
 $g(t) = b_m t^m + \dots + b_1 t + b_0$. Τότε

$$f(t) \cdot g(t) = c_{m+n} t^{m+n} + \dots + c_1 t + c_0,$$

όπου, για $k = 0, 1, \dots, m+n$ είναι $c_k = \sum_{i+j=k} a_i b_j$
 $(1 \leq i \leq n, 1 \leq j \leq m)$.

Είναι άπλο ν' αποδείξει κανείς ότι το $R[t]$, εφοδιασμένο με τις παραπάνω πράξεις $+$, \cdot γίνεται δακτύλιος (κάποια μικρή δυσκολία παρουσιάζει η προσεταιριστικότητα του πολλαπλασιασμού). Ο δακτύλιος $R[t]$ είναι, προφανώς, αντιμεταθετικός, αφού ο R έχει υποτεθεί αντιμεταθετικός. Επιπλέον, αν ο R έχει μονάδα, έστω 1 , τότε το σταθερό πολυώνυμο 1 είναι, μονάδα του $R[t]$. Στην περίπτωση που ο R έχει μονάδα, όροι της μορφής $t^k, -t^k$ ($k \geq 1$) γράφονται και απλώς $t^k, -t^k$, αντίστοιχως. Ένα πολυώνυμο, του οποίου ο μεγαλύτερος όρος είναι της μορφής t^n λέγεται μονικό.

Δύο βασικές παρατηρήσεις: (α) Η απεικόνιση $j: R \rightarrow R[t]$, $j(a) = a \in R[t]$, δηλ. η απεικόνιση που σε κάθε $a \in R$ αντιστοιχεί το σταθερό πολυώνυμο $a \in R[t]$, είναι μονομορφισμός δακτυλίων. Γενικά, κάθε μονομορφισμός δακτυλίων $j: R \rightarrow S$ λέμε ότι εμφυτεύει το δακτύλιο R μέσα στον S και, κατά τη συνήθη τακτική στα γεωτέρα μαθηματικά, θεωρούμε ότι ο R είναι υποσύνολο του S (άρα, υποδακτύλιος του S) ταυτίζοντας κάθε $a \in R$ με το $j(a)$. Έτσι και στην περίπτωση μας από δω και στο έξης, ο δακτύλιος R θα θεωρείται ως υποδακτύλιος του $R[t]$.

(β) Σε κάθε $f(t) \in R[t]$ αντιστοιχεί κατά προφανή τρόπο μια συνάρτηση $R \rightarrow R$, την οποία συμβολίζουμε με το ίδιο γράμμα f . Η συνάρτηση $f: R \rightarrow R$ ορίζεται ως έξης: Αν $f(t) = a_n t^n + \dots + a_1 t + a_0$, τότε,

$$f(r) = a_n r^n + \dots + a_1 r + a_0 \quad \forall r \in R.$$

Η συνάρτηση $f: R \rightarrow R$ χαρακτηρίζεται ως πολυωνυμική συνάρτηση f , αλλά (προσοχή!) δεν πρέπει να ταυτίζεται με το πολυώνυμο $f(t)$ διότι, απλούστατα η απεικόνιση που στο $f(t) \in R[t]$ αντιστοιχεί την πολυωνυμική συνάρτηση $f: R \rightarrow R$ δεν είναι αμφιμονοσήμαντη. Για παράδειγμα, θεωρήστε τα πολυώνυμα $f(t) = t^3 + t$, $g(t) = -t \in \mathbb{Z}_3[t]$. Αυτά, έξ ορισμού, είναι διαφορετικά ενώ, όπως διαπιστώνεται αμέσως, οι αντίστοιχες πολυωνυμικές συναρτήσεις $f: \mathbb{Z}_3 \rightarrow \mathbb{Z}_3$ και $g: \mathbb{Z}_3 \rightarrow \mathbb{Z}_3$ είναι ίδιες, αφού παίρνουν ως ίδιες τιμές στα $0, 1, 2 \in \mathbb{Z}_3$.

Πολλές φορές, αντί να λέμε "η τιμή της (πολυωνυμικής) συνάρτησης f στη θέση $r \in R$ ", να λέμε "η τιμή του πολυωνύμου $f(t)$ για $t = r$ ".

Το σύνολο των συναρτήσεων από το R στο R , έστω $\mathcal{F}(R, R)$,

αν εφοδιαστεί με τις προφανείς πράξεις (για $\phi, \psi \in \mathcal{F}(R, R)$, $(\phi + \psi)(r) \stackrel{\text{def}}{=} \phi(r) + \psi(r)$, $(\phi \cdot \psi)(r) = \phi(r) \cdot \psi(r)$) γίνεται δακτύλιος. (σύμφωνα με το παράδειγμα ε της § 1), υποδακτύλιος του οποίου είναι το σύνολο των πολυωνυμικών συναρτήσεων. Η απεικόνιση, που προαναφέραμε, έστω ν

$$R[t] \ni f(t) \xrightarrow{\nu} f \in \mathcal{F}(R, R)$$

είναι, προφανώς, δμορφισμός δακτυλίων* αλλά, όπως είδαμε πριν, δεν είναι αμφιμονοσήμαντη (άρα δεν είναι μονομορφισμός).

Πρόταση 1. Αν ο δακτύλιος R δεν έχει μηδενοδιαίρετες και $f(t), g(t) \in R[t]$, τότε $\deg(f \cdot g) = \deg f + \deg g$ (έννοείται ότι $-\infty + \text{οποιοδήποτε βαθμ} = -\infty$).

Απόδειξη. Προφανής αν ένα απ' τα $f(t), g(t)$ είναι μηδενικό πολυώνυμο. Έστω τώρα $f(t) = a_n t^n + \dots$, $g(t) = b_m t^m + \dots$, όπου $a_n \neq 0$, $b_m \neq 0$ και $m, n \geq 1$. Τότε, έσ' ορισμού του $f(t) \cdot g(t)$, είναι $f(t) \cdot g(t) = a_n b_m t^{m+n} + \text{όροι βαθμού} < m+n$. Επειδή ο R δεν έχει μηδενοδιαίρετες, είναι $a_n b_m \neq 0$, άρα $\deg(f \cdot g) = m+n$.

Σημείωση. Απ' την παραπάνω απόδειξη γίνεται φανερό ότι, εν γένει, $\deg(f \cdot g) \leq \deg f + \deg g$.

Το επόμενο θεώρημα είναι θεμελιώδες για τα πολυώνυμα:

(*)

Στο σημείο αυτό, προκειμένου ν' αποδειχθεί ότι $\nu(f(t) \cdot g(t)) = \nu(f(t)) \cdot \nu(g(t))$, γίνεται για πρώτη φορά ουσιαστική χρήση της αντιμεταθετικότητας του R .

Θεώρημα 1. Έστω D ακέραια περιοχή, $f(t), g(t) \in D[t]$, $g(t) \neq 0$ και δ συντελεστής του μεγαλύτερου βαθμού όρου του $g(t)$ είναι αντιστρέψιμο στοιχείο του D . Τότε υπάρχει ένα άρριβως ζεύγος πολυωνύμων $q(t)$ (πηλίκο) & $r(t)$ (υπόλοιπο), έτσι ώστε

$$f(t) = g(t) \cdot q(t) + r(t) \quad \text{&} \quad \deg r < \deg g. \quad (1)$$

Απόδειξη. Πρώτα θ' αποδειχθεί η ύπαρξη των $q(t), r(t)$.

"Αν $\deg f < \deg g$, τότε παίρνω $q(t) = 0$ και $r(t) = f(t)$.

Υποθέτω λοιπόν ότι $\deg f \geq \deg g$. Ειδικότερα, $f(t) \neq 0$.

"Έστω $f(t) = a_n t^n + \dots + a_1 t + a_0$ ($a_n \neq 0$) και $g(t) = b_m t^m + \dots + b_1 t + b_0$ ($b_m \neq 0$, αντιστρέψιμο στην D). Θα αποδείξω την ύπαρξη των $q(t), r(t)$ επαγωγικά επί του n : Για $n=0$ είναι και $m \neq 0$, άρα $f(t) = a_0$, $g(t) = b_0$ οπότε παίρνω $q(t) = a_0 b_0^{-1}$, $r(t) = 0$.

Έστω τώρα ότι k είναι θετικός ακέραιος και ότι η ύπαρξη των $q(t), r(t)$ έχει εδασοφαλιωθεί για όλα τα πολυώνυμα $f(t)$ με $\deg f = n < k$ (έδασοκολουθεί η υπόθεση $n \geq m$).

Υποθέτω τώρα ότι $n = k$. Τότε θεωρώ το πολυώνυμο

$$\begin{aligned} f(t) - (a_k b_m^{-1}) t^{k-m} \cdot g(t) &= (a_k t^k + \dots + a_1 t + a_0) - (a_k b_m^{-1}) t^{k-m} (b_m t^m + \dots + b_1 t + b_0) \\ &= (a_k t^k + \dots + a_1 t + a_0) - (a_k t^k + \text{όροι βαθμού} \leq k-1) = \\ &= \text{πολυώνυμο βαθμού} < k. \end{aligned}$$

Συνεπώς για το πολυώνυμο αυτό ισχύει η επαγωγική υπόθεση

άρα υπάρχουν $q_1(t), r_1(t) \in D[t]$ με $\deg r_1 < \deg g$ και

$$f(t) - (a_k b_m^{-1}) t^{k-m} \cdot g(t) = q_1(t) \cdot g(t) + r_1(t).$$

Θέτω λοιπόν $q(t) = q_1(t) + (a_k b_m^{-1}) t^{k-m}$, οπότε τα $q(t), r(t)$ ικανοποιούν τις (1).

Τώρα αποδεικνύω τη μοναδικότητα: Έστω ότι, εκτός από την (1),

ισχύει και $f(t) = g(t) \cdot q_1(t) + r_1(t)$ με $\deg r_1 < \deg g$.

Αφαιρώντας αυτή τη σχέση από την (1) έχω

$$g(t) \cdot (q(t) - q_1(t)) = r_1(t) - r(t). \quad (2)$$

Λόγω της πρότασης 1, $\deg(r_1(t) - r(t)) = \deg(q_1(t) - q(t)) + \deg g$.
 Αν ήταν $q_1(t) \neq q(t)$, τότε το δεξιό μέλος θα ήταν $\geq \deg g$,
 ενώ το αριστερό είναι $< \deg g$ άωπο. Συνεπώς $q_1(t) = q(t)$
 και τότε, απ' τη (2), $r_1(t) = r(t)$. (εδώ γίνεται χρήση του
 ότι στο $D[t]$ δεν υπάρχουν μηδενοδιαίρετες * άμεση συνέ-
 πεια της πρότασης 1.), δ. ε. δ.

Ορισμός α) Έστω D απέρανα περιοχή και $f(t), g(t) \in D[t]$
 με $g(t) \neq 0$. Λέμε ότι το $g(t)$ διαίρει (στο $D[t]$) το $f(t)$, ή
 ότι το $f(t)$ διαίρεται (ή είναι διαίρετό) απ' το $g(t)$ (στο $D[t]$), ή ότι το $g(t)$ είναι διαιρέτης του $f(t)$ *, συμβολικά $g(t) | f(t)$,
 αν υπάρχει $q(t) \in D[t]$, έτσι ώστε $f(t) = g(t) \cdot q(t)$.

β) Έστω K σώμα $\gg f(t) \in K[t]$. Το $p \in K$ λέγεται ρίζα του
 $f(t)$, αν $f(p) = 0$.

Άμεση συνέπεια του θεωρήματος 1 είναι η επόμενη πρόταση:

Πρόταση 2. Έστω K σώμα, $p \in K$ και $f(t) \in K[t]$. Το p είναι
 ρίζα του $f(t)$ αν και μόνο αν $t-p | f(t)$.

Απόδειξη. Γράψτε τη σχέση (1) του θεωρήματος 1, στην περί-
 πτωση που $g(t) = t-p$, δ. ε. δ.

Αν λοιπόν το $p \in K$ είναι ρίζα του $f(t) \in K[t]$, τότε το σύνολο
 $\{v \in \mathbb{Z}_{>0} : (t-p)^v | f(t)\}$ είναι μη κενό (αφού το 1 ανήκει
 σ' αυτό). Αφ' έτερου, είναι πεπερασμένο, αφού στη σχέση
 $(t-p)^v | f(t)$ το v δεν μπορεί να είναι όσοδήποτε μεγάλο
 (θεωρήστε τους βαθμούς στη σχέση $f(t) = (t-p)^v \cdot q(t)$).

Το μέγιστο στοιχείο αυτού του συνόλου λέγεται πλλαπλότητα

* ή ότι το $f(t)$ είναι πολλαπλάσιο του $g(t)$.

της ρίζας ρ του $f(t)$. Έχουμε, λοιπόν, εάν έσής, προφανώς
ισοδυναμία, όρισμό:

Όρισμός. Έστω K σώμα, $f(t) \in K[t]$ και $\rho \in K$ ρίζα του
 $f(t)$. Ο άκεραιος $\nu \geq 1$ για τον οποίο ισχύει
 $(t-\rho)^\nu \mid f(t) \not\asymp (t-\rho)^{\nu+1} \mid f(t)$ († σημαίνει "δεν διαί-
ρει) λέγεται πολλαπλότητα της ρίζας ρ του $f(t)$.

Όρισμός. Έστω D άκεραία περιοχή. Το μη σταθερό πολυώ-
νυμο $f(t) \in D[t]$ λέγεται ανάγωγο στο $D[t]$ (ή ανάγωγο
πάνω απ' το D) αν δεν υπάρχει πολυώνυμο $g(t) \in D[t]$
μέ $0 < \deg g < \deg f \not\asymp g(t) \mid f(t)$.

Παρατηρήσεις

α) Άμεσες συνέπειες του όρισμού: α) Τα πολυώνυμα
πρώτου βαθμού, είναι ανάγωγα. Για $f(t) \in K[t]$, K σώμα,
μέ $\deg f = 2, 3$, τ' να πούμε ότι τ' $f(t)$ είναι ανάγωγο στο
 $K[t]$ ισοδυναμεί μέ τ' να πούμε ότι κάποιο στοιχείο του K
είναι ρίζα του $f(t)$.

β) Ένα πολυώνυμο μέ ουτελειότες από μία άκεραία περιοχή
μπορεί να είναι ανάγωγο, αλλά, τ' ίδιο θεωρούμενο ως πο-
λυώνυμο μιας μεγαλύτερης άκεραίας περιοχής, μπορεί να
μη έξ ακολουθεί να είναι ανάγωγο. Απλά παραδείγματα:
Το $t^2 - 2$ είναι ανάγωγο αν θεωρηθεί ως πολυώνυμο του
 $\mathbb{Q}[t]$, δεν είναι όμως ανάγωγο αν θεωρηθεί ως στοιχείο
του $\mathbb{R}[t]$. Ανάλογα για τ' $t^2 + 1$ αν τ' δοσμε στο $\mathbb{R}[t]$
ή στο $\mathbb{C}[t]$.

Πρόταση 3. Έστω D άκεραία περιοχή. Κάθε μη σταθερό

πολυώνυμο του $D[t]$ έχει ένα, τουλάχιστον, ανάμμοιο
διαίρετη.

Απόδειξη. Μό επαρκή πάνω στο βαθμό του θεωρούμενου
πολυώνυμου (άπλη άσκηση).

Όρισμός. Έστω K σώμα και $f(t), g(t) \in K[t]$, όχι και τα
δύο μηδενικά. Ένα πολυώνυμο $d(t) \in K[t]$ θα λέγεται
κοινός διαίρετης των $f(t)$ και $g(t)$ αν $d(t) | f(t)$ ή $d(t) | g(t)$
(στο $K[t]$). Ο κοινός διαίρετης $d(t)$ των $f(t)$ και $g(t)$
θα χαρακτηρίζεται μέγιστος αν έχει την επιπλέον ιδιότητα
να διαιρείται (στο $K[t]$) από κάθε άλλο κοινό διαίρετη
των $f(t)$ και $g(t)$. Ο όρισμός αυτός γενικεύεται κατά προφανή
τρόπο και για περισσότερα από δύο πολυώνυμα. Πρέπει να
δείξουμε όμως ότι η έννοια του μέγιστου κοινού διαίρετη
(δύο ή περισσότερων πολυωνύμων) δεν είναι κενή περιεχο-
μένου. Αυτό επιτυγχάνεται στην επόμενη πρόταση.

Πρόταση 4. Έστω K σώμα. (α) Κάθε ιδεώδες του $K[t]$
είναι κύριο (βλ. §3).

β) Αν $f_1(t), \dots, f_n(t) \in K[t]$, όχι όλα μηδενικά, και
 $I = \langle f_1(t), \dots, f_n(t) \rangle$ το ιδεώδες του $K[t]$, που παράγεται
από αυτά τα πολυώνυμα (βλ. §3, παράδειγμα I(β)) τότε, κάθε
πολυώνυμο $d(t) \in K[t]$, που παράγει (μόνο του) το I (τέτοιο
πολυώνυμο $d(t)$ υπάρχει, λόγω του (α)) είναι μέγιστος κοινός
διαίρετης των $f_1(t), \dots, f_n(t)$.

Απόδειξη. α) Δες στο παράδειγμα I(γ), §3, πώς αποδείχθηκε
ότι κάθε ιδεώδες του \mathbb{Z} είναι κύριο και μεταφέρει εκείνη την

απόδειξη στην περίπτωση του $K[t]$ (ή πλήρης αναλογία των δύο αποδείξεων οφείλεται στο θεώρημα 1).

β) Έστω ότι το $d(t) \in K[t]$ παράγει το I . Αυτό σημαίνει ότι κάθε $h(t) \in I$ είναι πολλαπλάσιο του $d(t)$. Αφ' ετέρου, εξ' ορισμού του I ,

$$I = \{ g_1(t) \cdot f_1(t) + \dots + g_n(t) \cdot f_n(t) : g_1(t), \dots, g_n(t) \in K[t] \}.$$

Συνεπώς, κάθε $f_i(t)$ ανήκει στο I (βάλτε $g_i(t) = 1$ και όλα τα υπόλοιπα $g_j(t) = 0$), άρα είναι πολ/σιο του $d(t)$.

Δηλαδή, το $d(t)$ είναι κοινός διαιρέτης των $f_1(t), \dots, f_n(t)$.

Έστω τώρα $\delta(t) \in K[t]$ τυχών κοινός διαιρέτης των $f_1(t), \dots, f_n(t)$. Έπειδή $d(t) \in I$, θα υπάρχουν $g_1(t), \dots, g_n(t) \in K[t]$,

τέτοια ώστε $d(t) = g_1(t) \cdot f_1(t) + \dots + g_n(t) \cdot f_n(t)$. Όμως το $\delta(t)$

διαίρει όλα τα $f_1(t), \dots, f_n(t)$, άρα και το δεξιό μέλος της τελευταίας ισότητας, άρα $\delta(t) \mid d(t)$, ή $\delta \in I$.

Πρόταση 5 - Ορισμός. Έστω K σώμα και $f_1(t), \dots, f_n(t) \in K[t]$

($n \geq 2$) όχι όλα μηδενικά. Δύο οποιοδήποτε μέγιστοι κοινοί διαιρέτες των $f_1(t), \dots, f_n(t)$ διαφέρουν κατά (μη μηδενική)

πολλαπλασιαστική σταθερά. Συνεπώς, υπάρχει ένας, ακριβώς, μέγιστος κοινός διαιρέτης των $f_1(t), \dots, f_n(t)$, ο οποίος είναι μο-

νικό πολυώνυμο. αυτός χαρακτηρίζεται ως ο μέγιστος κοινός

διαιρέτης των $f_1(t), \dots, f_n(t)$. Αν αυτός ισούται με το σταθερό

πολυώνυμο 1, τότε τα $f_1(t), \dots, f_n(t)$ λέγονται πρώτα μεταξύ

τους. Ίσοδύναμα, τα $f_1(t), \dots, f_n(t)$ είναι πρώτα μεταξύ τους

αν και μόνο αν οι μόνοι κοινοί διαιρέτες τους είναι τα σταθερά

πολυώνυμα.

Απόδειξη. Μόνο ο πρώτος ισχυρισμός δεν είναι εντελώς προ-

φανής. αθετών και δ' αποδείξομε: Αν $d_1(t), d_2(t) \in K[t]$ είναι

μέγιστοι κοινοί διαιρέτες των $f_1(t), \dots, f_n(t)$ τότε, εκ του ορισμού του μέγιστου κοινού διαιρέτη, θα πρέπει $d_2(t) | d_1(t)$ και $d_1(t) | d_2(t)$. Γράφοντας $d_2(t) = g(t)d_1(t)$ και $d_1(t) = h(t)d_2(t)$ με $g(t), h(t) \in K[t]$, έχουμε $d_2(t) = g(t)h(t)d_2(t)$, άρα $1 = g(t) \cdot h(t)$, που συνεπάγεται ότι τα $g(t), h(t)$ είναι σταθερά και τα δύο, ο.έ.δ.

Προσοχή! Για $n > 2$, η συνθήκη "τα $f_1(t), \dots, f_n(t)$ είναι ανά δύο πρώτα μεταξύ τους" είναι πολύ ισχυρότερη από τη συνθήκη "τα $f_1(t), \dots, f_n(t)$ είναι πρώτα μεταξύ τους".

Πρόταση 6. Έστω K σώμα.

α) Έστω $f(t) \in K[t]$ ανάγωγο και $g(t) \in K[t]$. Τότε, η $f(t) | g(t)$ ή τα $f(t)$ και $g(t)$ είναι πρώτα μεταξύ τους.

β) Αν $f(t), g(t), h(t) \in K[t]$, το $f(t)$ είναι ανάγωγο και $f(t) | g(t) \cdot h(t)$, τότε $f(t) | g(t)$ είτε $f(t) | h(t)$.

γ) Αν τα $f(t), g(t) \in K[t]$ είναι πρώτα μεταξύ τους και καθένα διαιρεί το $h(t) \in K[t]$, τότε και $f(t) \cdot g(t) | h(t)$.

δ) Αν το $f(t) \in K[t]$ είναι πρώτο προς καθένα απ' τα $g(t), h(t) \in K[t]$, τότε είναι πρώτο και προς το $g(t) \cdot h(t)$.

Απόδειξη. α) Έστω $f(t) \nmid g(t)$. Θα δείξω ότι οι μόνοι κοινοί διαιρέτες των $f(t)$ και $g(t)$ είναι τα σταθερά πολυώνυμα. Έστω $d(t) \in K[t]$ κοινός διαιρέτης των $f(t), g(t)$. Επειδή το $f(t)$ είναι ανάγωγο, θα πρέπει, εφ' ορισμού, η $d(t) = \text{σταθερά}$ ή $d(t) = c \cdot f(t)$ με $c \in K - \{0\}$. Η δεύτερη περίπτωση αποκλείεται, αφού θα συνεπαγόταν ότι $c \cdot f(t) | g(t)$, άρα και $f(t) | g(t)$ (κάτι που αντιβαίνει στην υπόθεση), άρα μένει η πρώτη περίπτωση.

β) Έστω ότι $f(t) \nmid g(t)$. Τότε, απ' το (α), τα $f(t), g(t)$ είναι πρώτα μεταξύ τους. Άρα, απ' την πρόταση 4 (β), το ίδιο θα ισχύει και για $f(t), h(t)$.

$\langle f(t), g(t) \rangle$ παράγεται απ' τὸ 1, ἄρα ταυτίζεται μετ' τὸ $K[t]$.
 Μ' ἄλλα λόγια, ὑπάρχουν $f_1(t), g_1(t) \in K[t]$ ἔτσι ὥστε
 $f_1(t) \cdot f(t) + g_1(t) \cdot g(t) = 1$. Ἄρα, $h(t)h_1(t)f(t) + g_1(t)g(t)h(t) = h(t)$
 καὶ βλέπομε ὅτι τὸ $f(t)$ διαιρεῖ τὸν προσθετέον τοῦ ἀριστε-
 ροῦ μέλους, ὅποτε τὸ $f(t)$ διαιρεῖ καὶ τὸ δεξιὸ μέλος, δηλ. τὸ $h(t)$.

γ) Εἶναι $h(t) = f(t) \cdot F(t)$ καὶ $h(t) = g(t) \cdot G(t)$ γιὰ κάποια
 πολυώνυμα $F(t), G(t) \in K[t]$. Ἐπειδὴ τὰ $f(t), g(t)$ εἶναι πρῶτα
 μεταξύ τους, θὰ ὑπάρχουν $f_1(t), g_1(t) \in K[t]$ ἔτσι ὥστε
 $f_1(t) \cdot f(t) + g_1(t) \cdot g(t) = 1$ (βλ. ἀπόδειξη τοῦ (β)). Ἄρα,
 $f_1(t)G(t) \cdot f(t) + g_1(t) \cdot g(t) \cdot G(t) = G(t)$. Ἀντικοθιστῶ στὸ ἀριστε-
 ρὸ μέλος τὸ $g(t) \cdot G(t)$ απ' τὸ $f(t) \cdot F(t)$, ὅποτε βλέπω ὅτι
 $f(t) | G(t)$. Συνεπῶς $G(t) = f(t) \cdot H(t)$ καὶ τώρα,
 $h(t) = g(t)G(t) = g(t) \cdot f(t) \cdot H(t)$, πού εἶναι τὸ ἀποδεικτέο.

δ) Ἐπειδὴ τὰ $f(t), g(t)$ εἶναι πρῶτα μεταξύ τους, ὑπάρχουν
 $f_1(t), g_1(t) \in K[t]$, ἔτσι ὥστε $f_1(t) \cdot f(t) + g_1(t) \cdot g(t) = 1$. Πολλοὶ δὲ
 ἐπὶ $h(t)$, ὅποτε $f_1(t)h(t)f(t) + g_1(t)g(t)h(t) = h(t)$. Ἄρα, ἂν
 $d(t)$ εἶναι κοινὸς διαιρέτης τῶν $f(t)$ καὶ $g(t) \cdot h(t)$, αὐτὸς θὰ
 διαιρεῖ (λόγω τῆς τελευταίας ἰσότητος) καὶ τὸ $h(t)$, ἄρα θὰ εἶναι
 κοινὸς διαιρέτης τῶν $f(t), h(t)$, ὅποτε θὰ διαιρεῖ τὸν μέγιστο κοινὸ δι-
 αιρέτη τους, πού εἶναι 1. Συνεπῶς $d(t)$ εἶναι σταθερὸ, ὁ.έ.δ.
Γενικεύσεις. Μὲ ἀπλή χρήση ἐπαγωγῆς, τὰ (β), (γ) καὶ (δ)
 τῆς πρότασης 6 γενικεύονται ὡς ἑξῆς:

Γενίκευση τοῦ (β): Ἄν τὸ $f(t)$ εἶναι ἀνάγωγο καὶ $f(t) | g_1(t) \dots g_n(t)$,
 ὥτε τὸ $f(t)$ διαιρεῖ ἕνα τοῦλάχιστον ἀπ' τὰ $g_1(t), \dots, g_n(t)$.

Γενίκευση τοῦ (γ): Ἄν τὰ $f_1(t), \dots, f_n(t)$ εἶναι ἀνά δύο πρῶτα
 μεταξύ τους καὶ καθένα διαιρεῖ τὸ $h(t)$, τότε καὶ τὸ γινόμε-
 νό τους διαιρεῖ τὸ $h(t)$.

Γενίκευση τοῦ (δ): Ἄν τὸ $f(t)$ εἶναι πρῶτο πρὸς καθὲ $g_i(t), i=1, \dots, n$,
 τότε εἶναι πρῶτο καὶ πρὸς τὸ $g_1(t) \dots g_n(t)$.

Σημαντική παρατήρηση: Κατά την απόδειξη του (β) της πρότασης 6 δείχθηκε, επίσης, ότι αν τα $f(t), g(t)$ είναι πρώτα μεταξύ τους, τότε υπάρχουν $f_1(t), g_1(t)$ έτσι ώστε $f_1(t) \cdot f(t) + g_1(t) \cdot g(t) = 1$. Αυτό είναι ένα πολύ χρήσιμο αποτέλεσμα (ήδη ξαναχρησιμοποιήθηκε στο (γ)), του οποίου η γενίκευση (μέ ετελεώς ανάλογη απόδειξη) είναι η έξης: Αν ο μέγιστος κοινός διαιρέτης των $f_1(t), \dots, f_n(t)$ είναι $d(t)$, τότε υπάρχουν $g_1(t), \dots, g_n(t)$, τέτοια ώστε $g_1(t) \cdot f_1(t) + \dots + g_n(t) \cdot f_n(t) = d(t)$.

Πρόταση 7. Έστω K σώμα, $f(t) \in K[t]$ όχι μηδενικό. Τότε, το πολύ $\deg f$ (διαφορετικά) στοιχεία του K μπορεί να είναι ρίζες του $f(t)$. Αν ρ_1, \dots, ρ_m ($m \leq \deg f$) είναι αυτά (και μόνο αυτά) τα στοιχεία του K , που είναι ρίζες του $f(t)$, με αντίστοιχες πολλαπλότητες ν_1, \dots, ν_m , τότε

$$f(t) = (t - \rho_1)^{\nu_1} \dots (t - \rho_m)^{\nu_m} \cdot g(t),$$

όπου το $g(t) \in K[t]$ δεν έχει ρίζες στο K και $\deg f = \nu_1 + \dots + \nu_m + \deg g$.

Απόδειξη. Έστω ότι τα ρ_1, \dots, ρ_m είναι τυχόντα, διαφορετικά στοιχεία του K . Είναι άπλη άσκηση να δείξει κανείς ότι τα $t - \rho_1, \dots, t - \rho_m$ είναι πολυώνυμα ανά δύο πρώτα μεταξύ τους. Συνεπώς, αν είναι τα ρ_1, \dots, ρ_m ρίζες του $f(t)$, τότε, από την πρόταση 2 και τη γενίκευση του (γ) της πρότασης 6, $(t - \rho_1) \dots (t - \rho_m) \mid f(t)$. Συγκρίνοντας τους βαθμούς στην τελευταία σχέση, συμπεραίνω ότι $m \leq \deg f$.

Αν τώρα ρ_1, \dots, ρ_m είναι όλες-όλες οι ρίζες του $f(t)$ στο K και ν_1, \dots, ν_m είναι οι αντίστοιχες πολλαπλότητές τους, τότε και τα $(t - \rho_1)^{\nu_1}, \dots, (t - \rho_m)^{\nu_m}$ είναι ανά δύο πρώτα μεταξύ τους (άσκηση) άρα το γινόμενο τους διαιρεί το $f(t)$.

Θέω $f(t) = (t-r_1)^{v_1} \cdots (t-r_m)^{v_m} g(t)$. Είναι φανερό ότι $g(t)$ δεν έχει ρίζα στο K γιατί, αν είχε ρίζα ρ , τότε, ή $\rho = r_i$ για κάποιο $i \in \{1, \dots, m\}$, οπότε η πολλαπλότητα του r_i θα ήταν $\geq v_i + 1$, ή $\rho \neq r_i \forall i \in \{1, \dots, m\}$, οπότε $g(t)$ θα είχε κι άλλη ρίζα πλην των r_1, \dots, r_m .

Τέλος, συμπίνοντας τους βαθμούς στην τελευταία ισότητα πολυωνύμων έχουμε $\deg f = v_1 + \dots + v_m + \deg g$, ο.έ.δ.

Θεώρημα 2 (Θεμελιώδες θεώρημα της ανάλυσης πολυωνύμων).

Έστω K σώμα. Κάθε μη σταθερό πολυώνυμο $f(t) \in K[t]$ αναλύεται μονότροπα σε γινόμενο ανάγωγων πολυωνύμων του $K[t]$. Το "μονότροπα" της ανάλυσης εννοείται υπό τον όρο ότι πολυώνυμα που διαφέρουν κατά πολλαπλασιαστική σταθερά θεωρούνται, ομοιαστικά, τα ίδια, καθώς επίσης και ότι η διάταξη με την οποία γράφονται οι παράγοντες του γινομένου δεν λαμβάνεται υπ' όψη.

Απόδειξη. Έστω $\deg f = d \geq 1$. Αποδεικνύω πρώτα την ύπαρξη της ανάλυσης σε γινόμενο ανάγωγων πολυωνύμων, επαγωγικά επί του d . Για απλοποίηση στους συμβολισμούς θα παραλείπω το (t) στη γραφή των πολυωνύμων.

Αν $d=1$, το f είναι ανάγωγο και δεν έχω τίποτα να αποδείξω. Έστω ότι η ύπαρξη της ανάλυσης έχει εξασφαλισθεί για όλα τα πολυώνυμα βαθμού $< d$, όπου $d \geq 2$. Αν το f είναι ανάγωγο, τότε δεν έχω τίποτα να αποδείξω, ενώ αν $f = f_1 \cdot f_2$ με $\deg f_1, \deg f_2 < \deg f = d$, τότε η επαγωγική υπόθεση μου εξασφαλίζει την ύπαρξη ανάλυσης για τα f_1 και f_2 , άρα και για το f .

Τώρα αποδεικνύω τη μοναδικότητα. Από το που έχω να απο-

Δείξω είναι ότι αν $f = p_1 \cdots p_n$ και $f = q_1 \cdots q_m$, όπου τα $p_1, \dots, p_n, q_1, \dots, q_m \in K[t]$ είναι ανάγωγα, όχι σταθερά, τότε $n=m$ και υπάρχει μία 1-1 αντιστοιχία

$\phi: \{p_1, \dots, p_n\} \rightarrow \{q_1, \dots, q_m\}$, τέτοια ώστε το $\phi(p_i)$ να είναι κάποιο q_j , που διαφέρει απ' το p_i κατά πολλαπλασιαστική σταθερά. Πράγματι, έστω $m \geq n$. Έπειδή

$p_1 \cdots p_n = q_1 \cdots q_m$, το p_1 διαιρεί το δεξιό μέλος, άρα διαιρεί ένα τουλάχιστον απ' τα q_1, \dots, q_m , έστω το q_{j_1} . Έπειδή το q_{j_1} είναι ανάγωγο και διαιρείται απ' το p_1 , θα πρέπει το p_1 και το q_{j_1} να διαφέρουν κατά πολλαπλασιαστική σταθερά, άρα, απλοποιώντας τη σχέση

$$p_1 \cdots p_n = q_1 \cdots q_m, \text{ με διαίρεση δια } p_1, \text{ βρίσκω}$$

$$p_2 \cdots p_n = c_1 \prod_{j \neq j_1} q_j, \quad c_1 \in K^*. \text{ Προχωρώντας όμοια,}$$

απλοποιώ διαιρώντας δια' p_2 κ.δ.κ. μέχρις ότου φτάσω σε' μια σχέση *

$$L = c_1 \cdots c_n \prod_{j \neq j_1, \dots, j_n} q_j, \quad c_1, \dots, c_n \in K^*$$

Αυτή η σχέση είναι αδύνατη, εκτός αν δεν υπάρχουν q_j με $j \neq j_1, \dots, j_n$, δηλ. εκτός αν $m=n$.

Η προηγούμενη διαδικασία, κατά την οποία στο p_1 αντιστοιχίσαμε το q_{j_1} , στο p_2 το q_{j_2} κ.δ.κ. μας δίνει

και την 1-1 αντιστοιχία ϕ για την οποία έγινε λόγος παραπάνω, δ.ε.δ.

Άμεση συνέπεια του θεωρήματος 2 είναι το έξης σημαντικό



Στην παραπάνω σχέση τα j_1, \dots, j_m είναι διαφορετικοί δείκτες.

Πόρισμα Έστω K σώμα. Κάθε μη σταθερό πολυώνυμο $f(t) \in K[t]$ αναλύεται σε γινόμενο ανάγωγων πολυωνύμων ως έξης:

$$f(t) = p_1(t)^{\nu_1} \cdots p_m(t)^{\nu_m}, \quad m \geq 1, \nu_1, \dots, \nu_m \geq 1,$$

όπου τα $p_1(t), \dots, p_m(t)$ είναι ανά δύο πρώτα μεταξύ τους.

Το πλήθος m είναι μονότροπα όρισμένο απ' το $f(t)$ · το ανάγωγο πολυώνυμο $p_1(t), \dots, p_m(t)$ είναι μονότροπα, μέχρι πολλαπλασιασμού επί (μη μηδενική) σταθερά, καθορισμένα.

Όρισμός. Έστω σώμα K . Μια ανάλυση του μη σταθερού $f(t) \in K[t]$ όπως αυτή του παραπάνω πορίσματος λέγεται κανονική ανάλυση του $f(t)$ στο $K[t]$.

5. Διαιρετότητα - Περιοχές κυρίων ιδεωδών - Εὐκλείδειες περιοχές.

Σε άλλη τήν §5 το D θα συμβολίζει απέραια περιοχή $\neq D^* = D - \{0\}$.

Όρισμός. α) Το $\varepsilon \in D^*$ λέγεται μονάδα αν είναι αντιστρέψιμο στο D^* . Το $1 \in D^*$ είναι μονάδα και, επιπλέον, είναι η μονάδα του D . Το όριστικό άρθρο "η" ξεχωρίζει την μονάδα από τις υπόλοιπες (αν υπάρχουν · βλ. στα παραδείγματα, παρακάτω) μονάδες.

β) Δύο στοιχεία $\alpha, \beta \in D^*$ λέγονται συνεταιρικά αν $\beta = \varepsilon \cdot \alpha$, με ε μονάδα του D^* . Η σχέση συνεταιρικότητας είναι, προφανώς, ισοδυναμία.

γ) Έστω ότι $\alpha, \beta \in D$, $\beta \neq 0$. Λέμε ότι το β διαίρει το α ή, ισοδύναμα, το α διαίρεται (ή είναι διαιρετό) απ' το β , ή, το β είναι διαίρετης του α , ή, το α είναι πολ/σιο του β .

και συμβολιζουμε $\beta | \alpha$ (ἀρτησή του: $\beta | \alpha$), αν υπάρχει $\gamma \in D$ έτσι ώστε $\alpha = \beta \cdot \gamma$.

δ) Ο διαιρέτης β του α χαρακτηρίζεται μη-μονο αν ούτε μονάδα είναι, ούτε συνεταυρικό στοιχείο του α . Οι μονάδες και τα συνεταυρικά στοιχεία του α , χαρακτηρίζονται τετριμμένοι διαιρέτες του α .

ε) Το $p \in D^*$ λέγεται ἀνάγωγο, αν δεν είναι μονάδα και οι μόνοι διαιρέτες του είναι οι τετριμμένοι.

ς) Το $\pi \in D^*$ λέγεται πρώτο, αν δεν είναι μονάδα και έχει την ἑξῆς ιδιότητα: κάθε σχέση της μορφῆς $\pi | \alpha \cdot \beta$, με $\alpha, \beta \in D$, να συνεπάγεται, και ἀνάγκη, ότι το π διαιρεί ένα, τουλάχιστον από τα α και β .

Παραδείγματα. α) Οι μονάδες του \mathbb{Z} είναι μόνο τα ± 1 . Οι μονάδες του $K[t]$ (K σώμα) είναι τα μη μηδενικά σταθερά πολυώνυμα.

β) Έστω $d \in \mathbb{Z}$, $d > 0$, όχι τέλειο κῆνο. Θεωρώ την ἀκέραια περιοχή $\mathbb{Z}[\sqrt{d}] = \{x + y\sqrt{d} : x, y \in \mathbb{Z}\}$. Το $\varepsilon = x + y\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$ είναι μονάδα του $\mathbb{Z}[\sqrt{d}]$ αν και μόνο αν $\varepsilon^{-1} \in \mathbb{Z}[\sqrt{d}]$.

Αλλά $\varepsilon^{-1} = \frac{x - y\sqrt{d}}{x^2 - dy^2}$, ἄρα $\varepsilon^{-1} \in \mathbb{Z}[\sqrt{d}]$ αν και μόνο αν

$\frac{x}{x^2 - dy^2} \in \mathbb{Z}$ και $\frac{y}{x^2 - dy^2} \in \mathbb{Z}$. Αυτό το τελευταίο ισχύει

αν και μόνο αν $x^2 - dy^2 = \pm 1$. Συνεπώς το $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ πρέπει και αρκεί να είναι λύση της Διοφαντευκῆς ἑξίσωσης

$$x^2 - d \cdot y^2 = \pm 1. \quad (1)$$

Ἡ ἑξίσωση (1) λέγεται ἑξίσωση του Pell (ἢ των Pell-Fermat) και ισχύουν τα ἑξῆς. Για την ἑξίσωση (1) με τό $+1$ σὺ δεξιοῦ μέλος: Πάντασε ἔχει λύση. Ἡ λύση με τό

ελάχιστο θετικό x (άρα και το ελάχιστο θετικό y) λέγεται θεμελιώδης λύση, την οποία συμβολίζουμε (x_1, y_1) , $x_1, y_1 > 0$. Τότε, απ' τη θεωρία Αριθμών είναι γνωστό ότι όλες οι λύσεις της (1) είναι οι $\pm(x_n, y_n)$, όπου

$$x_n + y_n \sqrt{d} = (x_1 + y_1 \sqrt{d})^n, \quad n \in \mathbb{Z} \quad (2)$$

Για την εξίσωση (1) με -1 στο δεξιά μέλος: Δεν έχει πάντοτε λύση· αν έχει, την ελάχιστη λύση της (με την έννοια που δόθηκε παραπάνω) συμβολίζουμε (x_1, y_1) , $x_1, y_1 > 0$. Τότε, όλες οι λύσεις της (1), με -1 στο δεξιά μέλος, είναι οι $\pm(x_{2k+1}, y_{2k+1})$, $k \in \mathbb{Z}$, ενώ όλες οι λύσεις της (1) με $+1$ στο δεξιά μέλος, είναι οι $\pm(x_{2k}, y_{2k})$, $k \in \mathbb{Z}$. Και στις δύο περιπτώσεις, η (2) δίνει τα x_n, y_n συναρτησει των x_1, y_1 .

Συμπέρασμα: Αν (x_1, y_1) είναι η ελάχιστη θετική λύση της (1), τότε όλες οι μονάδες της ακεραίας περιοχής $\mathbb{Z}[\sqrt{d}]$ είναι οι $\pm(x_1 + y_1 \sqrt{d})^n$, $n \in \mathbb{Z}$.

Για παράδειγμα, αν $d=2$, η ελάχιστη θετική λύση της (1) είναι η $(1, 1)$ (δίνει -1 στο δεξιά μέλος), άρα το σύνολο των μονάδων της $\mathbb{Z}[\sqrt{2}]$ είναι το $\{\pm(1 + \sqrt{2})^n; n \in \mathbb{Z}\}$.

Αν $d=3$, τότε η (1) δεν έχει λύση με -1 στο δεξιά μέλος (αυτό φαίνεται αν δουλέψει κανείς modulo 4) και η ελάχιστη θετική λύση της (1) είναι η $(2, 1)$. Άρα, το σύνολο όλων των μονάδων της $\mathbb{Z}[\sqrt{3}]$ είναι το $\{\pm(2 + \sqrt{3})^n; n \in \mathbb{Z}\}$.

γ) Έστω $d \in \mathbb{Z}$, $d < 0$, όχι τέλει άγνωστο. Όπως στην αρχή του (β), καταλήγει κανείς στο συμπέρασμα ότι οι μονάδες της ακεραίας περιοχής $\mathbb{Z}[\sqrt{d}]$ είναι εκείνα, ακριβώς, τα $x + y\sqrt{d}$, $x, y \in \mathbb{Z}$, τα οποία επαληθεύουν την (1). Όμως, άρα $-d > 0$, άρα οι μόνες λύσεις, για $d < -1$, είναι $\pm(1, 0)$, ενώ για $d = -1$ οι μόνες λύσεις είναι $\pm(1, 0)$, $\pm(0, 1)$. Συνεπώς,

οι μόνες μονάδες του $\mathbb{Z}[\sqrt{d}]$ είναι οι ± 1 , αν $d \leq -1$, ενώ οι μόνες μονάδες του $\mathbb{Z}[i]$ ($i = \sqrt{-1}$) είναι οι $\pm 1, \pm i$.

δ) Στην αθέριστα περιοχή \mathbb{Z} , οι μόνες μονάδες είναι οι ± 1 , ενώ τα άναρμα και τα πρῶτα στοιχεία συμπίπτουν: τα σύνολά τους είναι $\omega = \{\pm p : p \text{ πρῶτος ἀριθμὸς}\}$.

ε) Ἐστω K σῶμα. Στην ἀθέριστα περιοχή $K[t]$, τα σταθερά πολυώνυμα, και μόνον αὐτά, εἶναι μονάδες. Τα άναρμα στοιχεία του $K[t]$ εἶναι, ἀκριβῶς, τα άναρμα πολυώνυμα του $K[t]$. Δυναίμει της πρότασης 6(β), κάθε άναρμα πολυώνυμο εἶναι και πρῶτο στοιχείο της $K[t]$. Ἄρα, στην ἀθέριστα περιοχή $K[t]$, ὅπως και στην \mathbb{Z} (βλ. (δ)), οι έννοιες "άναρμα" και "πρῶτο" ταυτίζονται.

ς.) Στην ἀθέριστα περιοχή $\mathbb{Z}[\sqrt{-5}]$ οι μόνες μονάδες εἶναι ± 1 (βλ. (γ)). Το 2 εἶναι άναρμα. Πράγματι, ἔστω $2 = (a + b\sqrt{-5})(x + y\sqrt{-5})$, $a, b, x, y \in \mathbb{Z}$. Τότε θα ἀληθεύει και η συζυγής σχέση και πολ/σιάζοντας κατά μέλη τις δύο σχέσεις παίρνουμε $4 = (a^2 + 5b^2)(x^2 + 5y^2)$. Αν ἦταν $b \neq 0$ εἴτε $y \neq 0$, τὸ δεξιὸ μέλος θα ἦταν ≥ 5 , ἄτοπο. Ἄρα $b = y = 0$ και $2 = a \cdot x$, που σημαίνει ὅτι ένα ἀπ' τα $a + b\sqrt{-5}$ και $x + y\sqrt{-5}$ ἴσούται με ± 1 , δηλ. τὸ ἀποδεικτέο.

Τὸ 2 δὲν εἶναι πρῶτο. Πράγματι, $2 \mid 6 = (1 + \sqrt{-5})(1 - \sqrt{-5})$, ἔνω $2 \nmid 1 + \sqrt{-5}$ και $2 \nmid 1 - \sqrt{-5}$, και πάλι ἀποδεικνύεται πολὺ εύκολα. Τὸ συμπέρασμα εἶναι ὅτι στην ἀθέριστα περιοχή $\mathbb{Z}[\sqrt{-5}]$ οι έννοιες του άναρμου και του πρῶτου στοιχείου δὲν εἶναι ταυτόσημες. Ἐν γένει, κάθε πρῶτο στοιχείο εἶναι και άναρμα, δυναίμει της παρακάτω πρότασης.

Πρόταση 1. Σε κάθε ἀθέριστα περιοχή, τα πρῶτα στοιχεία εἶναι άναρμα, ἔνω τὸ ἀντίστροφο δὲν ἀληθεύει (παράδειγμα (ς)).

Απόδειξη. Έστω D αλγεαία περιοχή και $\pi \in D$ πρώτο. Θα δείξω ότι το π έχει μόνο τετριμμένους διαιρέτες. Έστω $\rho | \pi$. Γράφω $\pi = \rho \cdot \rho'$, $\rho, \rho' \in D$. Προφανώς $\pi | \rho \cdot \rho'$, άρα (αφού το π είναι πρώτο) $\pi | \rho$ είτε $\pi | \rho'$. Αν $\pi | \rho$, τότε οι σχέσεις $\rho | \pi$ και $\pi | \rho$ συνεπάγονται (πολύ εύκολα) ότι το π, ρ είναι συνεταιρικά. Αν $\pi | \rho'$, τότε θέτω $\rho' = \pi \cdot \rho''$, άρα, απ' την $\pi = \rho \cdot \rho' = \rho \cdot \pi \cdot \rho''$, έχω $\rho \cdot \rho'' = 1$, που σημαίνει ότι το ρ είναι μονάδα, ο.έ.δ.

Όρισμός. Μια αλγεαία περιοχή λέγεται περιοχή ανάλυσης (σε ανάγωγα στοιχεία) αν κάθε ^{μη μηδενικό} στοιχείο της, που δεν είναι μονάδα, μπορεί να γραφεί ως γινόμενο (πεπερασμένου πλήθους) αναγώνων παραγόντων. Μια περιοχή ανάλυσης θα λέγεται περιοχή μονότροπης ανάλυσης, αν η προαναφερθείσα ανάλυση μπορεί να γίνει, αυθαίρετα, με ένα μόνο τρόπο. Το επίρρημα "αυθαίρετα", αναφέρεται εδώ υπό την έννοιαν ότι συνεταιρικά στοιχεία δεν θεωρούνται διαφορετικά, καθώς επίσης και ότι η σειρά, με την οποία γράφονται οι ανάγωγοι παράγοντες στο γινόμενο, δεν παίζει ρόλο.

Το θεώρημα 2, §4, λέει ότι η αλγεαία περιοχή $K[t]$ (Κ σώμα) είναι περιοχή μονότροπης ανάλυσης. Επίσης, από το λεγόμενο "θεμελιώδες θεώρημα της Αριθμητικής", ξέραμε ότι και η \mathbb{Z} είναι περιοχή μονότροπης ανάλυσης. Το γεγονός ότι όλα τα ιδεώδη του $K[t]$ είναι κύρια (§4, Πρόταση 4(α)) καθώς επίσης και όλα τα ιδεώδη του \mathbb{Z} (§3, Παράδειγμα I(γ)), δεν είναι τυχαίο: Οι περιοχές κυρίων ιδεωδών (δηλ. οι αλγεαίες περιοχές των οποίων όλα τα ιδεώδη είναι κύρια)

είναι πολύ σημαντικές, λόγω του θεωρήματος 1, που θα δούμε λίγο παρακάτω. Δεν είναι, επίσης, τυχαίο ότι και στην $K[t]$ και στην \mathbb{Z} , πρώτα και ανάμεσα στοιχεία τυτίζονται.

Πρόταση 2. Αν η D είναι περιοχή ανάλυσης, στην οποία κάθε άνομο στοιχείο είναι πρώτο, τότε η D είναι περιοχή μοναδικότητας ανάλυσης.

Απόδειξη. Η απόδειξη δεν διαφέρει, ουσιαστικά, σε τίποτα από την απόδειξη της μοναδικότητας στο Θεώρημα 2, §4: μόνο που το f και τα διαφορά p και q , αντί για πολυώνυμα, τα φανταζόμαστε τώρα ως στοιχεία της D , και ως διαφορές μη μηδενικές σταθερές c ως μονάδες της D , ό.έ.δ.

Η σημασία των περιοχών κυρίων ιδεωδών θα φανεί στα αμέσως παρακάτω: Έστω D περιοχή κυρίων ιδεωδών και $\alpha_1, \dots, \alpha_n \in D$, όχι όλα μηδέν. Λόγω της υπόθεσης για την D , το ιδεώδες $\langle \alpha_1, \dots, \alpha_n \rangle$ είναι κύριο, συνεπώς υπάρχει $d \in D$, έτσι ώστε $\langle \alpha_1, \dots, \alpha_n \rangle = D \cdot d$. Έπειδή κάθε α_i ανήκει στο $\langle \alpha_1, \dots, \alpha_n \rangle$, έπεται ότι το d είναι κοινός διαιρέτης των $\alpha_1, \dots, \alpha_n$. Έπειδή $d \in D \cdot d$, έπεται ότι υπάρχουν $\lambda_1, \dots, \lambda_n \in D$ έτσι ώστε

$$\lambda_1 \alpha_1 + \dots + \lambda_n \alpha_n = d. \quad (1)$$

Η (1) συνεπάγεται, ειδικότερα, ότι κάθε κοινός διαιρέτης των $\alpha_1, \dots, \alpha_n$ είναι, επίσης, διαιρέτης του d . Ο d έχει δηλαδή τις έντελώς ανάλογες των ιδιοτήτων, που συναντήσαμε στον ορισμό του μέγιστου κοινού διαιρέτη πολυωνύμων (σελ. 31), και χαρακτηρίζεται ως μέγιστος κοινός διαιρέτης των $\alpha_1, \dots, \alpha_n$.

Τώρα, είναι φανερό ότι δύο οποιοδήποτε μέγιστοι κοινοί διαιρέτες των a_1, \dots, a_n είναι συνεταίρικοί καθώς επίσης και ότι (λόγω της (1)) 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). Τα a_1, \dots, a_n θα λέγονται πρώτα μεταξύ τους αν ή μονάδα είναι μέγιστος κοινός διαιρέτης τους. Η επόμενη πρόταση είναι έντελως ανάλογη με την πρόταση 6, § 4 και η απόδειξή της είναι, ουσιαστικά, η ίδια με εκείνη της πρότασης 6, αρκεί στη θέση του $K[E]$ να βάλουμε τη D , αντί για πολυώνυμα να φανταζόμαστε, φυσικά, στοιχεία της D και αντί για μη μηδενικές σταθερές, μονάδες της D .

Πρόταση 3. Έστω D περιοχή κυρίων ιδεωδών.

- Αν τὸ $\pi \in D$ είναι ἀνάγωγο και $\alpha \in D$ εὐχόν, τότε, ἢ $\pi | \alpha$ ἢ τὰ π και α εἶναι πρῶτα μεταξύ τους.
- Κάθε ἀνάγωγο στοιχείο τοῦ D εἶναι πρῶτο.
- Αν τὰ $\alpha, \beta \in D$ εἶναι πρῶτα μεταξύ τους και καθένα διαιρεῖ τὸ $\gamma \in D$ τότε και τὸ $\alpha\beta$ διαιρεῖ τὸ γ .
- Αν τὸ $\alpha \in D$ εἶναι πρῶτο πρὸς τὸ β και πρὸς τὸ γ ($\beta, \gamma \in D$), τότε τὸ α εἶναι πρῶτο και πρὸς τὸ $\beta\gamma$.

Θεώρημα 1. Αν μιὰ περιοχή κυρίων ιδεωδῶν εἶναι περιοχή ἀνάλυσης, τότε εἶναι και περιοχή μονότροπης ἀνάλυσης.

Απόδειξη. Άμεση συνέπεια τῶν προτάσεων 3(β) και 2.

Χάρη στο Θεώρημα 1 και στην πρόταση 3, μπορούμε να μεταφέρουμε ὅλη, ουσιαστικά, τὴ θεωρία διαιρετότητας τῶν ἀκεραίων σὲ κάθε περιοχή ἀνάλυσης, ἡ ὁποία εἶναι και

περιοχή κυρίων ιδεωδών. Η απόδειξη της πρότασης 3 στηρίζεται στην ύπαρξη μεγίστου κοινού διαιρέτου, για οποιαδήποτε στοιχεία a_1, \dots, a_n της θεωρούμενης περιοχής και στη δυνατότητα γραφής του μεγίστου κοινού διαιρέτου ως γραμμικού συνδυασμού των a_1, \dots, a_n (βλ. (1), σελ. 43). Οι ιδιότητες αυτές, με τη σειρά τους, στηρίζονται κατά ουσιαστικό τρόπο στο γεγονός ότι κάθε ιδεώδες της θεωρούμενης περιοχής είναι κύριο. Αυτό μπορεί να κάνει κάποιον να υποθέσει ότι σε περιοχές όπου δεν είναι όλα τα ιδεώδη κύρια, η δυνατότητα να έχουμε μια καλή θεωρία διαιρετότητας δεν υπάρχει. Για τις απέραντες περιοχές, εν γένει, ακόμη και για τις περιοχές ανάλυσης, αυτό αληθεύει. Για τις περιοχές μονότροπης ανάλυσης όμως, όλη η βασική θεωρία διαιρετότητας των απεράντων σώζεται. Έπειδή, υπάρχουν περιοχές μονότροπης ανάλυσης, οι οποίες δεν είναι περιοχές κυρίων ιδεωδών (αργότερα θα δούμε τέτοια παράδειγμα) και όμως είναι πολύ σημαντικές στα Μαθηματικά, αξίζει να δούμε πώς σώζεται η διαιρετότητα στις περιοχές μονότροπης ανάλυσης.

Έστω D περιοχή μονότροπης ανάλυσης. Η έννοια του μεγίστου κοινού διαιρέτου στοιχείων $a_1, \dots, a_n \in D$, τα οποία δεν είναι όλα 0, είναι αυτή που ήδη έχουμε δανα συναντήσει: Το $d \in D$ είναι μεγίστος κοινός διαιρέτης (μ.κ.δ.) των a_1, \dots, a_n αν είναι κοινός διαιρέτης τους και αν διαιρείται από κάθε άλλο κοινό διαιρέτη των a_1, \dots, a_n . Είναι εντελώς τετριμμένο να δείξει κανείς ότι δύο οποιαδήποτε μεγίστοι κοινοί διαιρέτες των a_1, \dots, a_n είναι συνεταρτικοί.

"Αν η μονάδα είναι μ.κ.δ. των a_1, \dots, a_n τότε οι a_1, \dots, a_n λέγονται πρώτοι μεταξύ τους" ή ισοδύναμη συνθήκη είναι ότι οι μόνοι κοινοί διαιρέτες των a_1, \dots, a_n είναι οι μονάδες.

Πρόταση 4. Σε περιοχή μονότροπης ανάλυσης, κάθε ανάγωγο στοιχείο είναι πρώτο. (πρβλ. πρόταση 3(β)).

Απόδειξη. Έστω π ανάγωγο στοιχείο και $\pi \mid \alpha \cdot \beta$. Τότε $\alpha \cdot \beta = \pi \cdot \rho$. Αναλύω τὰ α, β, ρ σε γινόμενο αναγωγών: $\alpha = \pi_1 \dots \pi_\lambda, \beta = \pi'_1 \dots \pi'_\mu, \rho = \rho_1 \dots \rho_\nu$, οπότε $\pi_1 \dots \pi_\lambda \pi'_1 \dots \pi'_\mu = \pi \rho_1 \dots \rho_\nu$. Δηλαδή τὸ ἴδιο στοιχείο τῆς περιοχῆς (τὸ $\alpha \cdot \beta$) ἀναλύεται σὲ ἀνάγωγα μὲ δύο τρόπους. Λόγω τῆς μονότροπης ἀνάλυσης, οἱ ἀναλύσεις στὰ δύο μέλη δὲν εἶναι οὐσιαστικῶς διαφορετικῆς, ἀρα τὸ π , πού ἐμφανίζεται στὸ δεξιὸ μέλος, πρέπει νὰ εἶναι συνεταίρικό μὲ ἓνα, τοῦλάχιστον, ἀπ' τὰ $\pi_1, \dots, \pi_\lambda$ ἢ π'_1, \dots, π'_μ καί, συνεπῶς, τὸ π διαιρεῖ τὸ α εἴτε τὸ β , ὅ. εἶ.δ.

Συχνὰ ἐξυπηρετεῖ νὰ κάνομε τὸ ἐξῆς (ὑποθέτω ὅτι βρισκόμαστε στὴν περιοχή μονότροπης ἀνάλυσης \mathcal{D}). Έστω

\mathcal{P} ἓνα πλήρες σύστημα πρώτων (= ἀναγωγών) στοιχείων τοῦ \mathcal{D} . Αὐτὸ σημαίνει ὅτι καθε ἀνάγωγο στοιχείο τῆς \mathcal{D} εἶναι συνεταίρικό μὲ κάποιο στοιχείο τοῦ \mathcal{P} καὶ ἀνά δύο τὰ στοιχεῖα τοῦ \mathcal{P} δὲν εἶναι συνεταίρικά. Τότε, κάθε $\alpha \in \mathcal{D}^*$ γράφεται μονότροπα ὑπὸ τῆ μορφῆ

$$\alpha = \mu \cdot \prod_{p \in \mathcal{P}} p^{e_p(\alpha)}, \quad e_p(\alpha) \geq 0 \quad \forall p, \quad \mu \text{ μονάδα} \quad (1)$$

καὶ στὸ δεξιὸ μέλος "σχεδὸν ὅλοι" οἱ ἐκθέτες $e_p(\alpha)$ εἶναι 0

"σχεδόν όλοι" σημαίνει "όλοι εκτός από πεπερασμένο, τόπολύ, πλήθος". Η ανάλυση (1) λέγεται κανονική ανάλυση σε γινόμενο αναζώμων (ή πρώτων) παραγόντων. Για παράδειγμα, αν $D = \mathbb{Z}$ τότε παίρνουμε \mathcal{P} να είναι το σύνολο των θετικών πρώτων αριθμών * αν $D = K[t]$ (K σώμα) μια συνηθισμένη επιλογή για το \mathcal{P} είναι το σύνολο των αναζώμων μονικών πολυωνύμων του $K[t]$. Έν γενει κάνουμε την έξης σύμβαση: $e_p(0) = \infty \forall p$, όπου έννοείται ότι $\infty + n = \infty \forall n \in \mathbb{Z}$. * έτσι μπορούμε να μιλούμε και για την κανονική ανάλυση του 0.

Πρόταση 5. Έστω D περιοχή μονότροπης ανάλυσης και $\alpha, \beta \in D$, $\beta \neq 0$. Τότε (έχοντας υπ' όψη τις κανονικές αναλύσεις των α, β) $\beta | \alpha$ αν και μόνο αν

$$e_p(\beta) \leq e_p(\alpha) \quad \forall p \in \mathcal{P}.$$

Απόδειξη. Για απλούστευση του συμβολισμού θα παραλείπω απ' το σύμβολο $\prod_{p \in \mathcal{P}}$ το $p \in \mathcal{P}$.

Έστω $\beta | \alpha$. Θέω $\alpha = \beta \cdot \gamma$ και θεωρώ τις κανονικές αναλύσεις των α, β, γ :

$$\prod_p e_p(\alpha) = \left\{ \prod_p e_p(\beta) \right\} \left\{ \prod_p e_p(\gamma) \right\} = \prod_p e_p(\beta) + e_p(\gamma)$$

Λόγω της μονότροπης ανάλυσης πρέπει $e_p(\alpha) = e_p(\beta) + e_p(\gamma)$ $\forall p \in \mathcal{P}$ και, επειδή $e_p(\gamma) \geq 0$, είναι $e_p(\alpha) \geq e_p(\beta) \forall p$. Αντιστρόφως, έστω $e_p(\alpha) \geq e_p(\beta) \forall p \in \mathcal{P}$.

Θέω $v_p = e_p(\alpha) - e_p(\beta) \geq 0 \forall p \in \mathcal{P}$ και $\gamma = \prod_p p^{v_p}$. Επειδή όλα σχεδόν τα v_p είναι 0, έχει νόημα το γ ως

στοιχείο της D και είναι προφανές ότι $\beta \mid \alpha$, άρα $\beta \mid \alpha$.

Παρατήρηση: Κατά την απόδειξη δείξαμε ότι, αν $\alpha = \beta \cdot \gamma$, τότε $e_p(\alpha) = e_p(\beta) + e_p(\gamma) \quad \forall p \in \mathcal{P}$.

Τώρα είμαστε σε θέση να δούμε γιατί, για τυχόντα $\alpha_1, \dots, \alpha_n \in D$, που δεν είναι όλα 0, υπάρχει ο μ.κ.δ τους.

Πρόταση 6: Έστω D περιοχή μονότροπης ανάλυσης και $\alpha_1, \dots, \alpha_n \in D$, όχι όλα 0. Τότε το $\delta \in D$, που ορίζεται

$$\delta = \prod_{p \in \mathcal{P}} p^{\nu_p}, \quad \nu_p = \min\{e_p(\alpha_1), \dots, e_p(\alpha_n)\},$$

είναι μέγιστος κοινός διαιρέτης των $\alpha_1, \dots, \alpha_n$.

Απόδειξη: Είναι $e_p(\delta) = \nu_p \leq e_p(\alpha_i) \quad \forall p \in \mathcal{P}$ και $\forall i=1, \dots, n$. Συνεπώς, από την πρόταση 5, $\delta \mid \alpha_i \quad \forall i=1, \dots, n$.

Έστω τώρα d κοινός διαιρέτης των $\alpha_1, \dots, \alpha_n$. Τότε (πρόταση 5) $e_p(d) \leq e_p(\alpha_i) \quad \forall p \in \mathcal{P}$ και $\forall i=1, \dots, n$.

Άρα $e_p(d) \leq \nu_p = e_p(\delta) \quad \forall p \in \mathcal{P}$, οπότε (πρόταση 5), $d \mid \delta$, δηλ. δ .

Πρόταση 7: Έστω D περιοχή μονότροπης ανάλυσης.

α) Αν το $\pi \in D$ είναι ανάγωγο και $\alpha \in D$ τυχόν, τότε ή $\pi \mid \alpha$ ή το π είναι πρώτο προς το α (πρβλ. πρόταση 3(α)).

β) Αν τα $\alpha, \beta \in D$ είναι πρώτα μεταξύ τους και καθένα διαιρεί το γ , τότε $\alpha \cdot \beta$ διαιρεί το γ (πρβλ. πρόταση 3(β)).

γ) Αν το $\alpha \in D$ είναι πρώτο προς καθένα από τα $\beta, \gamma \in D$, τότε το α είναι πρώτο και προς το $\beta \cdot \gamma$ (πρβλ. πρόταση 3(δ)).

Απόδειξη α) Έστω ότι $p \nmid \alpha$. Θεωρώ $p \in \mathcal{P}$ συνεταίρικό προς το π . Τότε $e_p(\pi) = 1$ και από την πρόταση 5, $e_p(\alpha) < e_p(\pi) = 1$, άρα $e_p(\alpha) = 0$. Για κάθε $p \in \mathcal{P}$, $p \neq p_0$ είναι, προφανώς $e_p(\pi) = 0$, αφού το π είναι ανάγωγο. Άρα, στην πρόταση 6, για $n=2$, $\alpha_1 = \alpha$, $\alpha_2 = \pi$, είναι $v_p = 0$ για κάθε $p \in \mathcal{P}$, που σημαίνει ότι τα α, π είναι πρώτα μεταξύ τους.

β) Λόγω της πρότασης 5, αρκεί να δείξω ότι $e_p(\gamma) \geq e_p(\alpha\beta)$ για κάθε $p \in \mathcal{P}$. Έστω $p \in \mathcal{P}$ τυχόν. Αν $p \nmid \alpha$ και $p \nmid \beta$ τότε $e_p(\alpha) = e_p(\beta) = 0$, άρα $e_p(\alpha\beta) = e_p(\alpha) + e_p(\beta) = 0$, οπότε ισχύει το αποδεικτέο. Αν $p \mid \alpha$ τότε $p \nmid \beta$, αφού τα α, β είναι πρώτα μεταξύ τους. Άρα $e_p(\alpha\beta) = e_p(\alpha) + e_p(\beta) = e_p(\alpha)$. Όμως $\alpha \mid \gamma$, άρα $e_p(\gamma) \geq e_p(\alpha)$, άρα έχουμε ξανά το αποδεικτέο. Η περίπτωση $p \mid \beta$ είναι όμοια.

γ) Έστω $p \in \mathcal{P}$ τυχόν. Έχω να δείξω, λόγω της πρότασης 6, ότι $\min\{e_p(\alpha), e_p(\beta\gamma)\} = 0$, δηλ. ότι ένα τουλάχιστον από τα $e_p(\alpha)$ και $e_p(\beta\gamma)$ είναι μηδέν. Πράγματι, αν $p \nmid \alpha$, τότε τέλειωσα. Αν $p \mid \alpha$ τότε $p \nmid \beta$ και $p \nmid \gamma$, αφού έχει υποτεθεί ότι το α είναι πρώτο και προς το β και προς το γ . Άρα, αν $p \mid \alpha$, τότε $e_p(\beta) = e_p(\gamma) = 0$, οπότε και $e_p(\beta\gamma) = e_p(\beta) + e_p(\gamma) = 0$.

Τώρα θα εξετάσουμε το δακτύλιο των πολυωνύμων με συντελεστές από μια περιοχή μονότροπης ανάλυσης D . Παρατηρήστε ότι στην ειδική περίπτωση που $D = K$, σώμα, ούτε καν μιλάμε για μονότροπη ανάλυση, διότι, κάθε μη μηδενικό στοιχείο του K , ως αντιστρέψιμο, είναι μονάδα του K και, συνεπώς, ανάγωγα στοιχεία δεν υπάρχουν στο K . Ξέραμε όμως ήδη (Θεώρημα 2, §4) ότι το $K[t]$ είναι

περιοχή μονότροπης ανάλυσης. Τό 'ίδιο θ' αποδείξομε και για τὸ $D[t]$, στην περίπτωση που ἡ D εἶναι περιοχή μονότροπης ανάλυσης. Αυτό τὸ γεγονός ἔχει πολὺ ἐνδιαφέρουσες συνέπειες: ἡ πιὸ ἀρεστή, ἴσως, εἶναι ὅτι στα πολυώνυμα πολλῶν μεταβλητῶν (θὰ ὀρισθοῦν αὐστέρᾳ παρακάτω) με' συντελεστὲς ἀπ' τῆ D , ἰσχύει ἡ μονότροπη ἀνάλυση. Χρειαζόμαστε μιὰ μικρὴ προεργασία. Σημειώστε ὅτι, μέχρι τέλους τῆς §5, τὸ D θὰ συμβολίζει περιοχή μονότροπης ἀνάλυσης.

Ὁρισμός. Τὸ μὴ σταθερὸ $f(t) \in D[t]$ λέγεται πρωταρχικό, ἀν οἱ συντελεστὲς του εἶναι πρῶτοι μετὰδὺ τους. Ἄν τὸ $f(t)$ εἶναι σταθερὸ, τότε, θὰ λέγεται πρωταρχικό ἀν ἴσοῦται με' μονάδα τοῦ D .

Πρόταση 8 (Λήμμα τοῦ Gauss). Ἐστω F_D τὸ σώμα πηλίκων τῆς περιοχῆς μονότροπης ἀνάλυσης D καὶ $f(t) \in D[t]$. Τότε, τὸ $f(t)$ εἶναι ἀνάγωγο στοιχείο τῆς περιοχῆς $D[t]$, ἀν καὶ μόνο ἀν τὸ $f(t)$ εἶναι ἢ ἀνάγωγο στοιχείο τῆς D ἢ πρωταρχικό πολυώνυμο, τὸ ὁποῖο, θεωρούμενο ὡς πολυώνυμο τοῦ $F_D[t]$, εἶναι ἀνάγωγο.

Ἀπόδειξη. Ἐστω ὅτι τὸ $f(t)$ εἶναι ἀνάγωγο στοιχείο τῆς $D[t]$. Ἄν εἶναι σταθερὸ, τότε πρέπει νὰ εἶναι ἀνάγωγο στοιχείο τῆς D . Ἄν δὲν εἶναι σταθερὸ, τότε πρέπει νὰ εἶναι πρωταρχικό, διαφορετικὰ θὰ εἶχε μιὰ ἀνάλυση $f(t) = d \cdot g(t)$, με' $g(t) \in D[t]$ καὶ $d \in D$ ὄχι μονάδα τῆς D . Μέτρη αὐρὰ νὰ δεῖσομε τὸ πιὸ δύσκολο: ὅτι τὸ πρωταρχικό πολυώνυμο $f(t) \in D[t]$, θεωρούμενο ὡς πολυώνυμο τοῦ $F_D[t]$, εἶναι ἀνάγωγο. Ἐστω ὅτι

δεν ήταν. Τότε θα είχαμε μια σχέση $f(t) = f_1(t) \cdot f_2(t)$ με τὰ $f_1(t), f_2(t)$ μη σταθερά πολυώνυμα του $F_D[t]$.

Οι συντελεστές των $f_1(t), f_2(t)$ ανήκουν στο F_D άρα είναι πηλίκα στοιχείων της D . Συνεπώς, πολλαπλαζόντας με κατάλληλο στοιχείο $d \in D$ (π.χ. $d =$ μινόμενο των παρανομαστών, που εμφανίζονται στους συντελεστές των $f_1(t), f_2(t)$), παίρνουμε σε μια σχέση της μορφής

$$d \cdot f(t) = (a_m t^m + \dots + a_1 t + a_0)(b_n t^n + \dots + b_1 t + b_0), \quad (1)$$

$$a_0, \dots, a_m, b_0, \dots, b_n \in D, \quad m, n \geq 1, \quad a_m, b_n \neq 0.$$

Έστω $f(t) = c_N t^N + \dots + c_1 t + c_0$ ($N = m+n$), $c_N \neq 0$.

Ήσχυρίζομαι ότι στην (1) μπορώ να υποθέσω τὰ a_0, \dots, a_m πρώτα μεταξύ τους και τὰ b_0, \dots, b_n πρώτα μεταξύ τους.

Ας πούμε ότι τὰ a_0, \dots, a_m δεν ήταν πρώτα μεταξύ τους. Τότε* θα υπήρχε πρώτο στοιχείο p της D , τὸ ὅποιο να διαιρεί ὅλα τὰ a_0, \dots, a_m , άρα και ὅλους τους συντελεστές του μινόμενου στο δεξιό μέλος της (1). Αυτό συνεπάγεται ότι ὅλα τὰ

$d \cdot a_0, d \cdot a_1, \dots, d \cdot a_m$ είναι πολλαπλασιασμοί του p . Ὅμως τὸ p δεν είναι δυνατόν να διαιρεί ὅλα τὰ c_0, c_1, \dots, c_N , αφού

αὐτὰ είναι πρώτα μεταξύ τους, άρα υπάρχει c_i τέτοιο ὥστε $p \nmid c_i$. Ἐπειδή $p \mid d \cdot c_i$, έπεται τότε ότι $p \mid d$. Άρα,

σ' αὐτή τήν περίπτωση, θα μπορούσαμε να ἀπλοποιήσουμε την (1) διαιρώντας και τὰ δύο μέλη διαί p . Αν ἐξακολουθοῦν τὰ

"νέα" a_0, \dots, a_m , που θα προκύψουν μετά τήν ἀπλοποίηση, να μην είναι πρώτα μεταξύ τους, επαναλαμβάνομε τήν παραπάνω διαδικασία.

Αὐτό μπορεί να ἐπαναληφθεῖ πεπερασμένες (τὸ πολύ) φορές, λόγω τοῦ ότι κάθε a_i έχει πεπερασμένο, τὸ πολύ, πλήθος πρώτων διαιρετῶν. Τελικά, ἡ (1) μᾶς

* λόγω τῆς Πρότασης 6.

* λόγω τῆς Πρότασης 6.

όδηγει σε μια αχάλη της μορφής

$$d \cdot f(t) = (a_m t^m + \dots + a_1 t + a_0)(b_n t^n + \dots + b_1 t + b_0), \quad (2)$$

με $d \in D^*$, $a_0, \dots, a_m \in D$ πρώτα μεταξύ τους ($a_m \neq 0, m \geq 1$)
 $b_0, \dots, b_n \in D$ " " " " ($b_n \neq 0, n \geq 1$).

Αν το d στην (2) είναι μονάδα της D , τότε η (2) λέει ότι το $f(t)$ δεν είναι ανάγωγο στοιχείο της $D[t]$, εν αντιθέσει προς την υπόθεση. Αν το d δεν είναι μονάδα, τότε θα έχει κάποια πρώτη διαίρεση $p \neq 0$ που δεν είναι δυνατόν να διαιρεί όλα τα a_i ούτε όλα τα b_i . Άρα υπάρχει ένας δείκτης k , $0 \leq k \leq m$, τέτοιος ώστε

$$p \nmid a_k, \text{ ενώ } p \mid a_0, \dots, a_{k-1},$$

(αν $k=0$, η παραπάνω συνθήκη απλώς λέει ότι $p \nmid a_0$).

Επιπλέον ανάλογα, υπάρχει δείκτης l , $0 \leq l \leq n$, τέτοιος ώστε

$$p \nmid b_l, \text{ ενώ } p \mid b_0, \dots, b_{l-1}.$$

Συγκρίνω τώρα συντελεστές του t^{k+l} στα δύο μέλη της (2) και έχω:

$$d \cdot c_{k+l} = a_0 b_{k+l} + \dots + a_{k-1} b_{l+1} + a_k b_l + a_{k+1} b_{l-1} + \dots + a_{k+l} b_0.$$

Στο δεξιό μέλος: Το αριστερό κομμάτι, πριν από το $a_k b_l$, είναι διαίρετο δια p (αφού το p διαιρεί τα a_0, \dots, a_{k-1}) και το δεξιό κομμάτι, μετά το $a_k b_l$ είναι, επίσης, διαίρετο δια p . Άρα, όλο το δεξιό μέλος διαιρείται δια p (αφού αυτό ισχύει για το αριστερό μέλος)· συνεπώς $p \mid a_k b_l$, και θάρηπε τότε $p \mid a_k$ είτε $p \mid b_l$, και που αντικρούεται στην υπόθεσή μας.

Αντιστροφώς: Αν το $f(t)$ είναι σταθερό, ανάγωγο στοιχείο της D , τότε, προφανώς είναι ανάγωγο στοιχείο της $D[t]$. Έστω τώρα ότι το $f(t)$ είναι (μη σταθερό) πρωταρχικό

και ανάλυση στο $F_D[t]$. Τότε αποδεικνύεται να είναι μινόμενο δυο μη σταθερών πολυωνύμων του $D[t] \subseteq F_D[t]$. Άν, πάλι, $f(t) = c \cdot g(t)$ με $c \in D^*$, τότε το c πρέπει να είναι μονάδα της D , διότι το $f(t)$ έχει υποτεθεί πρωταρχικό. Συνεπώς, το $f(t)$ είναι ανάλυση στοιχείο της περιοχής $D[t]$, ό.ε.δ.

Σημαντική παρατήρηση: Η σχέση (2) (υπό τις συνθήκες, που γράφονται πάνω από αυτή) οδηγεί σε άτοπο, αν το δ δεν είναι μονάδα της D . Αυτό αποδεικνύει ότι, το μινόμενο δυο πρωταρχικών πολυωνύμων της $D[t]$ είναι πρωταρχικό πολυώνυμο της $D[t]$. Η γενίκευση για περισσότερα από δυο πολυώνυμα, είναι προφανής.

Ένας τεχνικός ορισμός, που θα χρειαστούμε είναι ο έξης: Άν $f(t) \in D[t]$, όχι σταθερό, με "περιεχόμενο του $f(t)$ ", εννοούμε ένα άπαιδο ή ποτε μέγιστο κοινό διαιρέτη των συντελεστών του $f(t)$. Εύδικότερα, το $f(t)$ είναι πρωταρχικό, αν και μόνο αν, το περιεχόμενό του είναι μονάδα.

Λήμμα. Έστω D περιοχή μονόστασης ανάλυσης και F_D το σώμα κλάσμων της. Τότε, κάθε $f(t) \in F_D[t]$, όχι σταθερό, μπορεί να γραφτεί ως $f(t) = \alpha \cdot g(t)$, όπου $\alpha \in F_D$ και το $g(t) \in D[t]$ είναι πρωταρχικό. Άν $f(t) = \alpha_1 \cdot g_1(t)$ είναι μια άλλη ανάλογη γραφή του $f(t)$, τότε $g_1(t) = \varepsilon \cdot g(t)$, με ε μονάδα της D .

Απόδειξη. Έστω β το μινόμενο των παρανομοιασίων των συντελεστών του $f(t)$. Προφανώς $\beta \cdot f(t) = h(t) \in D[t]$. Άν g

είναι τὸ περιεχόμενο τοῦ $h(t)$, ὥστε $h(t) = \gamma \cdot g(t)$, ὅπου τὸ $g(t) \in D[t]$ εἶναι πρωταρχικό. Συνεπῶς, $\beta \cdot f(t) = \gamma \cdot g(t)$ καί, θέτοντας $\gamma \cdot \beta^{-1} = \alpha \in F_D$ ἔχομε $f(t) = \alpha \cdot g(t)$, σύμφωνα μὲ τὸν ἰσχυρισμό. Ἐστω τώρα $f(t) = \alpha_1 \cdot g_1(t)$. Θεωρῶ $\delta \in D$, τέτοιον ὥστε $\delta \alpha, \delta \alpha_1 \in D$. Τότε $\delta f(t) = (\delta \alpha) \cdot g(t)$ καὶ $\delta f(t) = (\delta \alpha_1) \cdot g_1(t)$. Ἐπειδὴ τὸ $g(t)$ εἶναι πρωταρχικό, εἶναι φανερό ὅτι τὸ $\delta \alpha$ εἶναι περιεχόμενο τοῦ $\delta \cdot f(t)$. Ὁμοίως, τὸ $\delta \alpha_1$ εἶναι περιεχόμενο τοῦ $\delta \cdot f(t)$. Ἀφοῦ τὰ $\delta \alpha$ καὶ $\delta \alpha_1$ εἶναι μέγιστοι κοινὸί διαιρέτες τῶν αὐτῶν στοιχείων (ὅσων τῶν συντελεστῶν τοῦ $\delta \cdot f(t)$), θα συνδέονται μὲ μιὰ σχέση $\delta \alpha = \varepsilon \cdot \delta \alpha_1$, ὅπου ε εἶναι μονάδα τῆς D . Λόγω καὶ τῆς σχέσης $\alpha \cdot g(t) = f(t) = \alpha_1 \cdot g_1(t)$, ἔχομε $g(t) = \varepsilon \cdot g_1(t)$, ὅ.ε.δ.

Θεώρημα 2. Ἄν D εἶναι περιοχή μονότροπης ἀνάλυσης, τότε καὶ $\eta D[t]$ εἶναι περιοχή μονότροπης ἀνάλυσης.

Ἀπόδειξη. Ἐστω $f(t) \in D[t]$. Θα ἀποδείξω πρῶτα ὅτι τὸ $f(t)$ ἀναλύεται σὲ ἀνάγωγα στοιχεία τῆς $D[t]$. Ἄν τὸ $f(t)$ εἶναι σταθερό, ὁ ἰσχυρισμὸς μου ἔξασφαλίζεται ἀμέσως, ἀπὸ τὸ γεγονός ὅτι ηD εἶναι περιοχή μονότροπης ἀνάλυσης. Ἐστω τώρα ὅτι τὸ $f(t)$ δὲν εἶναι σταθερό. Τράφω $f(t) = \alpha \cdot g(t)$, ὅπου α εἶναι τὸ περιεχόμενο τοῦ $f(t)$ καὶ τὸ $g(t) \in D[t]$ εἶναι πρωταρχικό. Ἀρκεῖ, λοιπόν, ν' ἀποδείξω ὅτι τὸ $g(t)$ ἀναλύεται σὲ ἀνάγωγα στοιχεία τῆς $D[t]$. Βλέπω τὸ $g(t)$ ὡς πολυώνυμο τοῦ $F_D[t]$, ὁποῦ, ἀπὸ τὸ Θεώρημα 2 τῆς §4, ἐξασφαλίσω τὴν ἀνάλυση $g(t) = p_1(t) \cdots p_n(t)$ σὲ ἀνάγωγα πολυώνυμα τοῦ $F_D[t]$. Λόγω τοῦ προηγουμένου λήμματος, γιὰ καθὲν $i = 1, \dots, n$, μπορῶ νὰ γράψω $p_i(t) = \beta_i \cdot q_i(t)$, ὅπου $\beta_i \in F_D$ καὶ τὸ $q_i(t) \in D[t]$ εἶναι πρωταρχικό καὶ ἀνάγ.

γωγο πολυώνυμο του $D[t]$ (άρα ανάγωγο στοιχεία της $D[t]$).
 Συνεπώς, $g(t) = \beta_1 \cdots \beta_n \cdot q_1(t) \cdots q_n(t) = \beta \cdot q_1(t) \cdots q_n(t)$, όπου
 $\beta_1 \cdots \beta_n = \beta \in F_D$. Η παρατήρηση της σελ. 53 λέει ότι το
 $q(t) = q_1(t) \cdots q_n(t)$ είναι πρωταρχικό πολυώνυμο, άρα έχουμε
 $g(t) = \beta \cdot q(t)$ με τὰ $g(t), q(t) \in D[t]$, πρωταρχικά
 και $\beta \in F_D$. Το μονότροπο, με τὸ ὁποῖο μιλεῖ τὸ λήμμα,
 συνεπάγεται ὅτι τὸ β εἶναι μονάδα τῆς D , ἄρα στή
 σχέση $g(t) = \beta \cdot q_1(t) \cdots q_n(t)$ μπορῶ νὰ ὑποθέσω, χωρὶς
 βλάβη τῆς γενικότητος, ὅτι $\beta = 1$ κ. ἔχω ἀποδείξει τὸν ἰσχυ-
 ρισμό μου. Ἐστω τῶρα ὅτι ἔχω δύο ἀναλύσεις

$$g(t) = \alpha_1 \cdots \alpha_m \cdot p_1(t) \cdots p_m(t), \quad g(t) = \beta_1 \cdots \beta_n \cdot q_1(t) \cdots q_n(t) \quad (1)$$

(οἱ συμβολισμοὶ αὗτοὶ δὲν ἔχουν σχέση μετὰ ἐπεινους τοῦ πρώ-
 του μέρους τῆς ἀπόδειξης), ὅπου $\alpha_1, \dots, \alpha_m, \beta_1, \dots, \beta_n \in D$
 εἶναι ἀνάγωγα στοιχεία τῆς D καὶ τὰ $p_1(t), \dots, p_m(t), q_1(t),$
 $\dots, q_n(t)$ εἶναι ἀνάγωγα καὶ πρωταρχικά πολυώνυμα τοῦ
 $D[t]$. Τὰ $p(t) = p_1(t) \cdots p_m(t)$ καὶ $q(t) = q_1(t) \cdots q_n(t)$ εἶναι
 πρωταρχικά (παρατήρηση σελ. 53) καὶ ἰσχύει $\alpha \cdot p(t) = \beta \cdot q(t)$,
 ὅπου $\alpha = \alpha_1 \cdots \alpha_m$ καὶ $\beta = \beta_1 \cdots \beta_n$. Ἀπὸ τὸ λήμμα ἔπεται ὅτι
 τὰ α, β εἶναι συνεταίρικα, ἄρα, λόγω τοῦ μοδοτρόπου τῆς
 ἀνάλυσης στήν D , οἱ ἀναλύσεις $\alpha_1, \dots, \alpha_m$ καὶ β_1, \dots, β_n εἶναι
 ἀντιστοιχῶς οἱ ἴδιες (δηλ. $m = n$ καὶ τὰ $\alpha_1, \dots, \alpha_m$ μετὰ
 β_1, \dots, β_m εἶναι συνεταίρικα, ἕνα πρὸς ἕνα). Λόγω τῆς (1)
 τῶρα ἔχομε

$$p_1(t) \cdots p_m(t) = \varepsilon \cdot q_1(t) \cdots q_m(t) \quad (2)$$

Τὰ πολυώνυμα στή (2) εἶναι ἀνάγωγα στοιχεία τῆς $D[t]$, ἄρα
 (Πρόταση 8) εἶναι ἀνάγωγα πολυώνυμα τοῦ $F_D[t]$ καὶ τῶρα, τὸ
 θεώρημα 2, § 4, συνεπάγεται ὅτι οἱ ἀναλύσεις στα δύο μέλη
 τῆς (2) εἶναι ἀντιστοιχῶς οἱ ἴδιες, ὅ. ἔ. ὁ.

Πολυώνυμα δύο ή περισσότερων μεταβλητών Έστω D αέραια περιοχή και $D[t_1]$ δ δακτύλιος (αέραια περιοχή) των πολυωνύμων με συντελεστές απ' την D και μεταβλητής t_1 . Μπορώ τώρα να θεωρήσω τον δακτύλιο των πολυωνύμων με συντελεστές απ' την $D[t_2]$ και μεταβλητής t_2 , δηλ. τον δακτύλιο $(D[t_1])[t_2]$. Αυτό συμβολίζεται με $D[t_1, t_2]$. Τα στοιχεία του είναι, έξ' ορισμού, της μορφής $f(t_1, t_2) = f_n(t_1) \cdot t_2^n + \dots + f_1(t_1) \cdot t_2 + f_0(t_1)$, όπου $f_i(t_1) \in D[t_1]$, για κάθε $i = 1, \dots, n$. Άρα, το τυπικό στοιχείο του $D[t_1, t_2]$ είναι της μορφής

$$f(t_1, t_2) = \sum_{\substack{0 \leq j_1 \leq n_1 \\ 0 \leq j_2 \leq n_2}} a_{j_1, j_2} t_1^{j_1} t_2^{j_2}, \quad a_{j_1, j_2} \in D. \quad (2)$$

Στη συνέχεια μπορούμε να ορίσουμε τον δακτύλιο των πολυωνύμων $D[t_1, t_2, t_3] \stackrel{\text{def}}{=} (D[t_1, t_2])[t_3]$ και, επαγωγικά, τον δακτύλιο των πολυωνύμων $D[t_1, t_2, \dots, t_n]$.

Δεν θα μπορούμε σε πολλές λεπτομέρειες, αλλά θα κάνουμε κάποιες βασικές παρατηρήσεις:

- α) Ο δακτύλιος $D[t_1, \dots, t_n]$ είναι αέραια περιοχή.
 β) Οι δακτύλιοι $D[t_1, t_2]$ και $D[t_2, t_1]$ είναι ισόμορφοι, μέσω του ισομορφισμού, ο οποίος απεικονίζει κάθε $t_1^{j_1} t_2^{j_2}$ με το $t_2^{j_2} t_1^{j_1}$. Στην πράξη, αντιστοιχεί το $t_1^{j_1} t_2^{j_2}$ και $t_2^{j_2} t_1^{j_1}$ και τους δακτυλίους $D[t_1, t_2]$ και $D[t_2, t_1]$.

Γενικότερα, τον δακτύλιο $D[t_1, \dots, t_n]$ τον αντιστοιχεί με τον δακτύλιο $D[t_{i_1}, \dots, t_{i_n}]$, για οποιαδήποτε μετάθεση (i_1, \dots, i_n) των $(1, \dots, n)$.

- γ) Το $f(t_1, t_2)$ στην (1), είναι το μηδενικό στοιχείο του $D[t_1, t_2]$, δηλ. το μηδενικό στοιχείο του $(D[t_1])[t_2]$ αν και μόνο αν $f_n(t_1) = \dots = f_1(t_1) = f_0(t_1) = 0 \in D[t_1]$. Αυτό, με τη

σειρά του, ισοδυναμεί με το ότι όλα οι συντελεστές των $f_n(t_1), \dots, f_1(t_1), f_0(t_1)$ είναι μηδέν, και που είναι ισοδύναμο με το ότι όλα τα a_{j_1, j_2} στην (2) είναι μηδέν (κάθε a_{j_1, j_2} προκύπτει από άθροισμα κάποιων συντελεστών των $f_n(t_1), \dots, f_1(t_1), f_0(t_1)$). Έτσι όμως ανάλογα γενικεύεται αυτή η παρατήρηση και για περισσότερες μεταβλητές.

Θεώρημα 3 (α) Αν η D είναι περιοχή μονότροπης ανάλυσης τότε και η $D[t_1, \dots, t_n]$ είναι περιοχή μονότροπης ανάλυσης. (β) Αν το K είναι σώμα, τότε το $K[t_1, \dots, t_n]$ είναι περιοχή μονότροπης ανάλυσης.

Απόδειξη. (α) Λόγω του θεωρήματος 2, η απόδειξη συνίσταται σε μία απλούστατη επαγωγή (έπί του πλήθους n των μεταβλητών).

(β) Λόγω του θεωρήματος 2, § 4, το $K[t_1]$ είναι περιοχή μονότροπης ανάλυσης. Λόγω τώρα του θεωρήματος 2 (§ 5) το $(K[t_1])[t_2] (= K[t_1, t_2])$ είναι, επίσης, περιοχή μονότροπης ανάλυσης. Τώρα, επαγωγικά, με χρήση του ίδιου θεωρήματος, καταλήγουμε στο αποδεικτέο.

Δύο σημαντικά παραδείγματα. Ας θεωρήσουμε τα πολυώνυμα δύο μεταβλητών με παραγματικούς συντελεστές. Τις μεταβλητές, αντί t_1, t_2 , ας τις γράφομε (για απλούστευση) x, y .

α) Στο τέλος της § 3 (σελ. 23) είχα ισχυριστεί ότι κάθε πρώτο ιδεώδες δεν είναι, κατ' ανάγκη, *maximal*: Έστω το ιδεώδες $\langle x \rangle$ στο δακτύλιο $\mathbb{R}[x, y]$. Τα στοιχεία του $\langle x \rangle$ είναι της μορφής $x \cdot h(x, y)$ με

$h(x, y) \in \mathbb{R}[x, y]$. Ισχυρίζομαι ότι το $\langle x \rangle$ είναι πρώτο ιδεώδες. Πράγματι, έστω $f(x, y) \cdot g(x, y) \in \langle x \rangle$. Έχω να δείξω ότι $f(x, y) \in \langle x \rangle$ είτε $g(x, y) \in \langle x \rangle$. Ας γράψω $f(x, y) = f_m(y) \cdot x^m + \dots + f_1(y) \cdot x + f_0(y)$ και $g(x, y) = g_m(y) \cdot x^m + \dots + g_1(y) \cdot x + g_0(y)$.

Από το γεγονός ότι το $f(x, y) \cdot g(x, y)$ είναι της μορφής $x \cdot h(x, y)$, συμπεραίνω ότι $f_0(y) \cdot g_0(y) = 0$, άρα $f_0(y) = 0$ είτε $g_0(y) = 0$. Αυτό σημαίνει ότι το x βγαίνει κοινός παράγων στο $f(x, y)$ είτε στο $g(x, y)$, δηλ. $f(x, y) \in \langle x \rangle$ είτε $g(x, y) \in \langle x \rangle$. Τώρα ισχυρίζομαι ότι το $\langle x \rangle$ δεν είναι maximal.

Πράγματι, $\langle x \rangle \subsetneq \langle x, y \rangle \subsetneq \mathbb{R}[x, y]$, ό. έ. δ.

β) Σύμφωνα με το θεώρημα 3(β), το $\mathbb{R}[x, y]$ είναι περιοχή μονότροπης ανάλυσης και παρακάτω θα δείξω ότι δεν είναι περιοχή κύριων ιδεωδών. Αυτό θα δικαιολογήσει τον ισχυρισμό μου στη σελ. 45 ότι υπάρχουν περιοχές μονότροπης ανάλυσης, που δεν είναι περιοχές κύριων ιδεωδών.

Συγκεκριμένα, θα δείξω ότι το ιδεώδες $\langle x, y \rangle$ του $\mathbb{R}[x, y]$ δεν είναι κύριο. Πράγματι: έστω ότι $\langle x, y \rangle = f(x, y) \cdot \mathbb{R}[x, y]$.

Από τη σχέση $x \in \langle x, y \rangle$ έπεται τότε ότι $x = f(x, y) \cdot g(x, y)$,

για κάποιο $g(x, y) \in \mathbb{R}[x, y]$. Βλέποντας το $g(x, y)$ ως πολυώνυμο του $(\mathbb{R}[y])[x]$, συμπεραίνω ότι έχω δύο περιπτώσεις:

$$\eta' \text{ (i)} \quad f(x, y) = A_1(y) \cdot x + A_0(y) \quad \& \quad g(x, y) = B_0(y) \quad , \quad \eta'$$

$$\text{(ii)} \quad f(x, y) = A_0(y) \quad \& \quad g(x, y) = B_1(y) \cdot x + B_0(y)$$

$$(A_0(y), A_1(y), B_0(y), B_1(y) \in \mathbb{R}[y]).$$

Στην περίπτωση (i) έχουμε $x = A_1(y) \cdot B_0(y) \cdot x + A_0(y) \cdot B_0(y)$, άρα $A_0(y) \cdot B_0(y) = 0$ και $A_1(y) \cdot B_0(y) = 1$. Οι δύο τελευταίες σχέσεις συνεπάγονται $A_0(y) = 0$ και $A_1(y), B_0(y)$ σταθερά.

Άρα $f(x, y) = A_1 \cdot x$, $A_1 \in \mathbb{R}$ και λόγω της $y \in \langle x, y \rangle$,

$Y = A_1 \cdot X \cdot H(X, Y)$, $H(X, Y) \in \mathbb{R}[X, Y]$. Άλλα αυτή, ως σχέση στο $(\mathbb{R}[Y])[X]$ είναι, προφανώς, αδύνατη.

Στην περίπτωση (ii) συμπεραίνω, ανάλογα, ότι $A_0(Y) \cdot B_0(Y) = 0$ και $A_0(Y) \cdot B_1(Y) = 1$, άρα $B_0(Y) = 0$ και $A_0(Y), B_1(Y)$ σταθερά. Τότε, $f(X, Y) = A_0 \in \mathbb{R}$, συνεπώς $\langle X, Y \rangle = f(X, Y) \cdot \mathbb{R}[X, Y] = \mathbb{R}[X, Y]$, άτοπο διότι, σε τέτοια περίπτωση, τα σταθερά πολυώνυμα θα έπρεπε να ανήκουν στο $\langle X, Y \rangle$, κάτι προφανώς αδύνατο.

Ευκλείδειες περιοχές: Μια πολύ ενδιαφέρουσα, ειδική περίπτωση περιοχών μονότροπης ανάλυσης είναι οι ευκλείδειες περιοχές. Μια άκεραία περιοχή E λέγεται ευκλείδεια, αν υπάρχει συνάρτηση $v: E \rightarrow \mathbb{Z}_{\geq 0}$, με τις εξής ιδιότητες: (i) Αν $a, b \in E^*$ και $a|b$, τότε $v(a) \leq v(b)$. (ii) Αν $a, b \in E$ και $b \neq 0$, υπάρχουν $q, r \in E$, τέτοια ώστε $a = q \cdot b + r$ και είτε $r = 0$, είτε $v(r) < v(b)$.

Η v λέγεται στάθμη της E . Μέχρι τέλους της §5, E θα παριστάνει ευκλείδεια περιοχή.

Παραδείγματα ευκλείδειων περιοχών είναι η \mathbb{Z} με στάθμη την απόλυτη τιμή και η $K[t]$ (K σώμα) με στάθμη το βαθμό των πολυωνύμων.

Πρόταση 9. Έστω E είναι ευκλείδεια περιοχή στάθμης v .

α) Αν $a, b \in E^*$, $a|b$ και $v(a) = v(b)$, τότε τα a, b είναι συνεταίρια.

β) Η E είναι περιοχή ανάλυσης.

Απόδειξη. α) Λόγω της συνθήκης (ii) των ευκλείδειων περιοχών, υπάρχουν $q, r \in E$, τέτοια ώστε $a = bq + r$

και $r=0$ ή $v(r) < v(b)$. Αν $r=0$, τότε $b|a$ και αυτή η σχέση, σε συνδυασμό με την $a|b$ συνεπάγονται ότι τα a, b είναι συνεταίρικα. Αν $r \neq 0$ τότε $v(r) < v(b)$. αφ' ετέρου, γράφοντας $b=ac$, $c \in E$, έχω $a=acq+r$ και $r=a(1-cq)$. Τότε (συνθήκη (i)) $v(r) \geq v(a) = v(b) > v(r)$, άτοπο.

β) Έστω $\min v(E) = n_0 \in \mathbb{Z}_{\geq 0}$. Θα αποδείξω επαγωγικά τον ισχυρισμό: Αν $v(a) = n_0$, τότε τα a είναι μονάδα του E ή ανάγωγο στοιχείο του E (άρα ο ισχυρισμός αληθεύει). Πράγματι, αν δεν ήταν έτσι, τότε θα μπορούσα να γράψω $a=b \cdot c$ με $b, c \in E$ και τα b, c ούτε μονάδες, ούτε συνεταίρικα του a . Θα είχα τότε $v(b), v(c) \leq v(a) = n_0$, άρα, κατ' ανάγκη, $v(b) = v(c) = n_0$ (λόγω της επιλογής του n_0). Αυτό, λόγω του (α) θα συνεπαγόταν ότι τα b, c είναι συνεταίρικα του a , άτοπο.

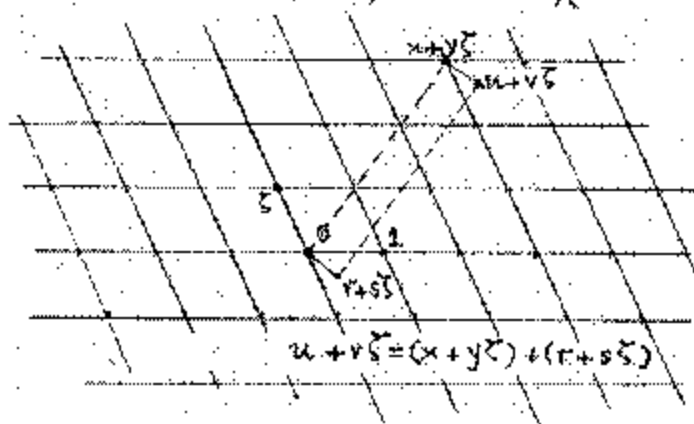
Έστω τώρα ότι έχω αποδείξει τον ισχυρισμό (β) για όλα τα $a \in E$ με $n_0 \leq v(a) \leq n-1$ για κάποιο $n > n_0$, και έστω a με $v(a) = n$. Αν τα a είναι ανάγωγα, έχω τελειώσει. Αν όχι γράψω $a=b \cdot c$ με b, c γνήσιους διαιρέτες του a . Συνεπώς, λόγω του (α), θα είναι $v(b), v(c) < v(a) = n$, άρα, απ' την επαγωγική υπόθεση, τα b, c αναλύονται σε γινόμενο ανάγωγων στοιχείων της E . Τότε και τα $a=b \cdot c$ αναλύεται, δ.έ.δ.

Θεώρημα 4 Κάθε ευκλείδια περιοχή είναι περιοχή κύριων ιδεωδών και περιοχή μονότροπης ανάλυσης.

Απόδειξη. Η απόδειξη του ότι κάθε ιδεώδες της ευκλείδιας περιοχής είναι κύριο, είναι πανομοιότυπη με εκείνη του

παραδείγματος $I(\gamma)$, § 3. Αντί για άκεραίους θα έχουμε τώρα στοιχεία κάποιας ευκλείδειας περιοχής E και αντί για σχέσεις της μορφής $a \leq b$, με $a, b \in \mathbb{Z}$, θα έχουμε σχέσεις $v(a) \leq v(b)$, με $a, b \in E$. Αφού η E είναι περιοχή κυρίων ιδεωδών και περιοχή ανάλυσης (πρόταση 9(β)), έπεται (Θεώρημα 1) ότι είναι και περιοχή μονότροπης ανάλυσης, δι.ε.δ.

Παράδειγμα. Έστω ζ ένας από τους μιγαδικούς αριθμούς $i, i\sqrt{2}$, $\omega = \frac{-1+i\sqrt{3}}{2}$ ($\omega^3=1, \omega^2+\omega+1=0$). Θεωρώ την άκεραία περιοχή $E = \{x+y\zeta : x, y \in \mathbb{Z}\}$. Στο μιγαδικό επίπεδο, τα στοιχεία της E είναι οι κόμβοι του



δικτυωτού στο διπλανό σχήμα (Σημείωση: Αν $\zeta = i$ ή $i\sqrt{2}$ τα παραλληλόγραμμα είναι ορθογώνια και, για $\zeta = i$, είναι τετράγωνα). Στην E ορίζω την απεικόνιση $v: E^* \rightarrow \mathbb{Z}_{\geq 0}$,

$v(x+y\zeta) = |x+y\zeta|^2$. Τοχυρίζομαι ότι η v είναι σταθμη της E : Η συνθήκη (i) της σταθμής (σελ. 59), προφανώς ικανοποιείται. Θ' αποδείξω τώρα ότι ικανοποιείται και η (ii).

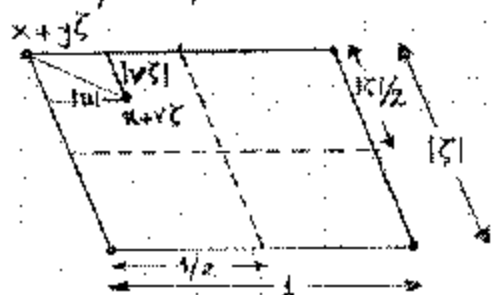
Έστω ότι $c+d\zeta, a+b\zeta \in E$, $a+b\zeta \neq 0$. Έχω να δείξω ότι υπάρχουν $x+y\zeta, r+q\zeta \in E$, τέτοια ώστε

$$c+d\zeta = (a+b\zeta)(x+y\zeta) + (r+q\zeta)$$

$$\leq \{ r+q\zeta = 0 \text{ ή } v(r+q\zeta) < v(a+b\zeta) \}$$

Έστω $\frac{c+d\zeta}{a+b\zeta} = u+v\zeta$ (προσοχή! τα u, v δεν είναι,

κατ' ανάγκη, ακέραιοι). Το $u+v\zeta$ ανήκει σ' ένα απ' τα παραλληλόγραμμα (στο εσωτερικό του, εν γένει), τα οποία καλύπτουν το μοναδικό επίπεδο. Έστω $x+y\zeta$ το πλησιέστερο προς το $u+v\zeta$ κομβικό σημείο (βλ. σχήμα της



σελ. 61, καθώς και τη "μεγέθυνση" του παραλληλογράμμου, στο οποίο ανήκει το $u+v\zeta$, δίπλα).

Τότε $u+v\zeta = (x+y\zeta) + (r+s\zeta)$, όπου $|r| \leq \frac{1}{2}$ και $|s| \leq \frac{1}{2}|\zeta|$.

Θέτω $p+q\zeta = (a+b\zeta)(r+s\zeta) = (c+d\zeta) - (a+b\zeta)(x+y\zeta) \in E$.

Άρα, μένει να δείξω ότι $|p+q\zeta|^2 < |a+b\zeta|^2$.

Για $\zeta = i$ ή $i\sqrt{2}$ έχω:

$$\begin{aligned} |p+q\zeta|^2 &= |a+b\zeta|^2 |r+s\zeta|^2 = |a+b\zeta|^2 (r^2 + s^2 |\zeta|^2) \\ &\leq |a+b\zeta|^2 \left(\frac{1}{4} + \frac{1}{4} \cdot 2 \right) = \frac{3}{4} |a+b\zeta|^2 < |a+b\zeta|^2. \end{aligned}$$

Για $\zeta = \omega$ έχω:

$$\begin{aligned} |p+q\zeta|^2 &= |a+b\zeta|^2 |r+s\zeta|^2 = |a+b\zeta|^2 (r+s\omega)(r+s\bar{\omega}) \\ &= |a+b\zeta|^2 (r^2 - rs + s^2) = |a+b\zeta|^2 \left\{ \left(r + \frac{s}{2}\right)^2 + \frac{3}{4}s^2 \right\} \\ &\leq |a+b\zeta|^2 \left\{ \left(\frac{1}{2} + \frac{1}{4}\right)^2 + \frac{3}{4} \cdot \frac{1}{4} \right\} = \frac{3}{4} |a+b\zeta|^2 < |a+b\zeta|^2. \end{aligned}$$

Το συμπέρασμα, λοιπόν, είναι ότι η ακέραια περιοχή E είναι εὐκλείδεια περιοχή και, συνεπώς (Θεώρημα 4), ἔχομε μονότροπη ἀνάλυση.

Ἐφαρμογές 1) "Αποδείξε ότι το μόνο τετράγωνο, το οποίο, αὐξανόμενο κατά 2 γίνεται κύβος, είναι το 25" (ἀπό γραμμα του Fermat, προς τὸν Wallis). Μ' ἄλλα λόγια, γὰ λυθεῖ ἡ Διοφαντική (σὲ ἀκεραῖους) ἐξίσωση

$$x^2 + 2 = y^3 \quad (1)$$

καί, μάλιστα, γὰ δειχθεῖ ὅτι μοναδικὴ λύση τῆς εἶναι ἡ

$$x=1, y=3.$$

Γράφω την (1) από τη μορφή

$$(x+\zeta)(x-\zeta)=y^3, \quad \zeta=i\sqrt{2} \quad (2)$$

και δουλεύω στην ανέριαια περιοχή $\mathbb{Z}[\zeta]$. Επειδή η περιοχή αυτή είναι ευκλείδεια, έχω τη μονότροπη ανάλυση (θεώρημα 4), συνεπώς μπορούμε να κάνουμε "Αριθμητική".

Το χριζόφορμα, πρώτα-πρώτα, ότι οι παράγοντες στο αριστερό μέλος της (2) είναι πρώτοι μεταξύ τους. Πράγματι, αν δεν ήταν, τότε θα είχαν κάποιο κοινό πρώτο διαιρέτη π (υπενθύμιση: πρώτα και ανάγνωμα στοιχεία ταυτίζονται, σύμφωνα με την πρόταση 4). Άρα $\pi | (x+\zeta) - (x-\zeta) = 2\zeta = -\zeta^3$, οπότε $\pi | \zeta$ (επειδή ο π είναι πρώτος). Όμως το ζ είναι ανάγνωμο (άσκηση ρουτίνας), οπότε η $\pi | \zeta$ συνεπάγεται ότι τα π, ζ είναι συνεταρικό, δηλ. $\pi = \pm i\sqrt{2}$ (έχομε 'δει, από άσκηση, ότι οι μονάδες της $\mathbb{Z}[\zeta]$ είναι μόνο οι ± 1). Επιστρέφω στην (2): Επειδή το π διαιρεί το αριστερό μέλος, θα διαιρεί το y^3 , άρα και το y , συνεπώς το y θα έχει τη μορφή $y = i\sqrt{2}(a+bi\sqrt{2})$, $a, b \in \mathbb{Z}$. Παίρνοντας τη συζυγή μιγαδική σχέση και πολλαπλαζοντας κατά μέλη βρίσκω $y^2 = 2(a^2 + 2b^2)$, άρα ο y είναι άρτιος. Τότε, από την (1), και ο x είναι άρτιος οπότε $y^3 - x^2 \equiv 0 \pmod{4}$.

Αυτό είναι άτοπο, διότι $y^3 - x^2 = 2$. Άρα, οι παράγοντες στο αριστερό μέλος της (2) είναι, όπως, πρώτοι μεταξύ τους. Το γινόμενο τους είναι κύβος, άρα (σύμφωνα με άσκηση που έχω κάνει) κάθε παράγοντας είναι συνεταρικό στοιχείο κάποιου κύβου. Τότε (επειδή οι μονάδες ± 1 είναι κύβοι) θα έχω μια σχέση της μορφής

$$x+\zeta = (m+n\zeta)^3, \quad m, n \in \mathbb{Z}$$

Το δεξιά μέλος είναι $(m^3 - 6mn^2) + n(3m^2 - 2n^2)\zeta$, άρα

$$x = m^3 - 6mn^2 \quad \text{και} \quad 1 = n(3m^2 - 2n^2) \quad (3)$$

Από τη δεύτερη σχέση έπεται ότι $n = 3m^2 - 2n^2 = \pm 1$, άρα $|n| = |m| = 1$ και τότε, η πρώτη σχέση συνεπάγεται ότι $x = \pm 5$, που είναι το άποδεικτέο.

2) Με έντελως ανάλογο τρόπο μπορούμε να χειριστούμε και τη λύση της διαφαντικής εξίσωσης

$$x^2 + 5 = 2y^3 \quad (4)$$

οι σχέσεις, όμως, οι ανάλογες των (3) δεν θα έχουν λύση (σε ακέραιους m, n) και, συνεπώς, θα συμπεράνουμε ότι η (4) δεν έχει ακέραιες λύσεις. Κάνετε σάν άσκηση όλη αυτή τη διαδικασία. Όπως... η (4) έχει λύση π.χ. την $(x, y) = (7, 3)$! Τι πήγε στραβά; (Άσκηση)

3) Τώρα θ' αποδείξω το έξης κλασικό αποτέλεσμα της Θεωρίας Αριθμών: Ένας περιττός πρώτος p γράφεται ως άθροισμα δύο τελειών τετραγώνων αν και μόνο αν είναι $\equiv 1 \pmod{4}$.

Απόδειξη: Είναι $p \equiv 1$ ή $3 \pmod{4}$. Αν $p \equiv 3 \pmod{4}$, αποδεικνύεται να έχω μια σχέση της μορφής $p = a^2 + b^2$.

Πράγματι, αυτή η σχέση συνεπάγεται ότι ο ένας από τους a, b είναι άρτιος και ο άλλος περιττός. Όμως, τότε,

$$a^2 + b^2 \equiv 1 \pmod{4},$$

που αντίκειται στην $p \equiv 3 \pmod{4}$.

Το αντίστροφο είναι το δύσκολο: Αν $p \equiv 1 \pmod{4}$ να δείξω ότι ο p γράφεται ως άθροισμα δύο τετραγώνων.

Θα χρησιμοποιήσω το έξης αποτέλεσμα από τη στοιχειώδη Θεωρία Αριθμών: Αν $p \equiv 1 \pmod{4}$, τότε υπάρχει $x \in \mathbb{Z}$, τ.ώ. $x^2 \equiv -1 \pmod{p}$.

Το αποτέλεσμα αυτό μπορούμε να το θεωρήσουμε γνωστό για πληρότητα, όμως, θα δώσω στο τέλος μια απόδειξη, η οποία θα είναι και μια ενδιαφέρουσα άσκηση λίγο παραλίστερης θεωρίας.

Θεωρώ λοιπόν $x \in \mathbb{Z}$ τ.ώ. $x^2 \equiv -1 \pmod{p}$. Τότε $x^2 + 1 = p \cdot y$ για κάποιο $y \in \mathbb{Z}$. Δουλεύω στην ευκλείδεια περιοχή $\mathbb{Z}[i]$, όπου έχω, λόγω της τελευταίας ισότητας, $p \mid (x+i)(x-i)$. Αν ο p ήταν πρῶτος στην $\mathbb{Z}[i]$, θα έπρεπε $p \mid x+i$ είτε $p \mid x-i$. Δηλαδή, θα είχα κάποια σχέση

$$x+i = p(u+vi) \quad \text{είτε} \quad x-i = p(u+vi), \quad \text{μὲ } u, v \in \mathbb{Z}.$$

Τότε όμως (έξισώνοντας τους συντελεστές του i) $1 = \pm p \cdot v$, προφανώς άτοπο. Άφου ο p δεν είναι πρῶτος, δεν είναι και ανάμικτο στοιχείο της $\mathbb{Z}[i]$ (πρῶτα και ανάμικτα συγκρίπτονται γιατί είμαστε σε περιοχή μονότροπης ἀνάλυσης), ἄρα υπάρχουν $\gamma, \delta \in \mathbb{Z}[i]$, ὄχι μονάδες, τέτοια ὥστε

$$p = \gamma \cdot \delta. \quad \text{Τότε (παίρνοντας συζυγείς μιγαδικούς)} \quad p = \bar{\gamma} \cdot \bar{\delta} \quad \text{καὶ, πολλαπλασιάζοντας κατὰ μέλη,} \quad p^2 = |\gamma|^2 |\delta|^2.$$

Ἐπειδὴ τὰ γ, δ δὲν εἶναι μονάδες, εἶναι $|\gamma|, |\delta| > 1$, συνεπῶς, $|\gamma|^2 = |\delta|^2 = p$. Ἄν θέσω $\gamma = a+bi$, $a, b \in \mathbb{Z}$, τότε $a^2 + b^2 = p$, ὁ.έ.δ.

Μένει τώρα νὰ ἀποδείξω ὅτι (για $p \equiv 1 \pmod{4}$) ὑπάρχει $x \in \mathbb{Z}$ τ.ώ. $x^2 \equiv -1 \pmod{p}$.

Για νὰ τ' ἀποδείξω δουλεύω στὸ σῶμα \mathbb{Z}_p . Ἐχω $t^{p-1} - 1 = (t^{\frac{p-1}{2}} - 1)(t^{\frac{p-1}{2}} + 1)$ καὶ τὸ πολυώνυμο (τοῦ $\mathbb{Z}_p[t]$) στὸ ἀριστερὸ μέλος ἔχει ὡς ρίζες τοῦ ὅλα τὰ μὴ μηδενικά στοιχεία τοῦ \mathbb{Z}_p ("μικρὸ θεώρημα τοῦ Fermat", τὸ ὁποῖο εἶδαμε παλιότερα σὴν ἀσκηση).

Ἄρα κάθε στοιχείο τοῦ \mathbb{Z}_p^* εἶναι ρίζα ἢ τοῦ $t^{\frac{p-1}{2}} - 1$, ἢ τοῦ $t^{\frac{p-1}{2}} + 1$. Ὅμως, δεῖ εἶναι δυνατόν ὅλα τὰ στοιχεία τοῦ \mathbb{Z}_p^* (πλήθους $p-1$) νὰ εἶναι ρίζες τοῦ $t^{\frac{p-1}{2}} - 1$ (τοῦ ὁποίου ὁ βαθμὸς εἶναι $< p-1$), ἄρα ὑπάρχει $\tilde{n} \in \mathbb{Z}_p^*$, ρίζα τοῦ $t^{\frac{p-1}{2}} + 1$. Τότε $\tilde{n}^{\frac{p-1}{2}} + 1 = 0$ ἄρα $\tilde{n}^{\frac{p-1}{2}} \equiv -1 \pmod{p}$ καὶ, θέτοντας $x = \tilde{n}^{\frac{p-1}{4}}$ ($\frac{p-1}{4} \in \mathbb{Z}$), ἔχω $x^2 \equiv -1 \pmod{p}$, ὁ.έ.δ.

Άλγεβρικές επεκτάσεις

Όρισμός Αν R είναι δακτύλιος και K υπόσπρω του R , τώ $\alpha \in R$ λέγεται άλγεβρικό πάνω σ' K αν υπάρχει μη μηδενικό πολυώνυμο $f(t) \in K[t]$, τέτοιω ώστε $f(\alpha) = 0$.

Τώ $L \supseteq K$ λέγεται άλγεβρική επέκταση του K αν είναι σώμα που περιέχει τώ K σαν υπόσπρωμα και κάθε $\alpha \in L$ είναι αλγεβρικό πάνω σ' K .

Είναι φανερό ότι κάθε $\alpha \in K$ είναι αλγεβρικό πάνω σ' K , αφού $f(\alpha) = 0$, όπου $f(t) = t - \alpha$. Έστω K, R όπως παραπάνω.

Ο R μπορεί να θεωρηθεί και ως προφανή πρότυπο ενός K -διανυσματικού χώρου. Αν τώ R είναι υπόσπρω του σώματος L και τώ L είναι πεπερασμένης διάστασης θεωρούμε σαν K -διανυσματικό χώρο, τότε τώ L χαρακτηρίζεται πεπερασμένη επέκταση του K , και η διάσταση τού L λέγεται βαθμός επέκτασης L του K .

Τώ παραπάνω K είναι υπόσπρω του L .

Συμβολίζομε με $K[x]$, όπου $x \in L$, τώ δισκύνολο του L , που αποτελείται απ' τώ στοιχεία της μορφής $a_0 + a_1x + \dots + a_nx^n$, $a_i \in K$. Είναι φανερό ότι τώ $K[x]$, εφοδιασμένο με τήν πρόσθεση και τόν πολλαπλασιασμό του L είναι δακτύλιος αντιμεταθετικός με μονάδα.

Ίσχυει τώ έδής θεμελιώδες.

Θεώρημα 1 Αν τώ $\alpha \in L$ είναι αλγεβρικό πάνω σ' K , τότε ο δακτύλιος $K[x]$ είναι σώμα. Υπάρχει ένα μοναδικό ανάγωγο μονικό πολυώνυμο (μονικό σημαίνει "με συντελεστή μεγιστουβάθμου όρου τώ 1") $q(t) \in K[t]$, τέτοιω ώστε $q(\alpha) = 0$. Τώ $K[x]$ είναι πεπερασμένη επέκταση του K , βαθμού του με $n = \deg q$, και τώ στοιχεία $1, x, \dots, x^{n-1}$ παράγουν τώ διανυσματικό χώρο $K[x]$ πάνω σ' K .

Απόδειξη. Πρώτα θα δείξομε ότι κάθε μη μηδενικό στοιχείο τού $K[x]$ έχει αντίστροφο. Πραγματικά έστω $0 \neq y = g(x) \in K[x]$, όπου $g(t) \in K[t]$. Εξ υπόθεσης υπάρχει μη μηδενικό $f(t) \in K[t]$, τέτοιω ώστε $f(\alpha) = 0$. Αναλύομε τώ f σε γινόμενο ανάγωγων πολυωνύμων τού $K[t]$ (Θ2, §4), $f = q_1 \dots q_r$, έποτε θα πρέπει $q_i(\alpha) = 0$ για κάποιο $i \in \{1, \dots, r\}$. Πολλώτερον με κατάλληλο στοιχείο τού K τώ $q_i(t)$ μπορούμε να πεινάχομε ανάγωγο μονικό πολυώνυμο $q(t) \in K[t]$ με $q(\alpha) = 0$.

Τώρα μπορούμε να δείξομε ότι τώ πολυώνυμα g και q είναι πρώτα μεταξύ τους. Πραγματικά, αν δεν ήσαν, τώ q θα διαιρούσε τώ g (Π6, §4), έποτε $g(\alpha) = 0$, άτοπο.

Άρα, λοιπόν, ο μ.κ.δ. των g, q είναι 1, θα υπάρξουν $g', q' \in K[t]$, έτσι ώστε $g \cdot g' + q \cdot q' = 1$ (βλ. σελ. 35). Έτσι $g(x)g'(x) + q(x)q'(x) = 1$, άρα $y \cdot g'(x) = 1$. Έτσι το y έχει αντίστροφο το $g'(x) \in K[x]$, άρα ο δ.α.κ.δ. $K[x]$ είναι σώμα.

Το $q(t)$ είναι το μοναδικό μορικό ανάγωγο πολυώνυμο του $K[t]$ που μηδενίζεται αν το t αντικατασταθεί απ' το x . Πραγματικά, έστω ένα τέτοιο πολυώνυμο $p(t)$. Αν ήταν το q και p πρώτα μεταξύ τους, τότε $q \cdot q' + p \cdot p' = 1$ για κάποια $q', p' \in K[t]$, άρα $q(x)q'(x) + p(x)p'(x) = 1$ και $0 = 1$, άτονω. Άρα, αφού δεν είναι πρώτα μεταξύ τους και είναι και ανάγωγα, θα πρέπει $p|q$ και $q|p$, άρα θα πρέπει $q = a \cdot p$, $a \in K$. Έπειδή όμως οι συντελεστές των μεγιστοβαθμίων όρων στα q, p είναι 1, θα πρέπει $a = 1$, άρα $p = q$.

Μένει τώρα να δείξουμε ότι αν $q(t) = a_0 + a_1 t + \dots + a_{n-1} t^{n-1} + t^n$, τότε τα $1, x, \dots, x^{n-1}$ αποτελούν βάση του διανυσματικού χώρου $K[x]$ πάνω στο K : Πρώτα παρατηρούμε ότι τα $1, x, \dots, x^{n-1}$ είναι K -γραμμικώς ανεξάρτητα. Γιατί αν δεν ήταν θα είχαμε $b_{n-1} x^{n-1} + \dots + b_1 x + b_0 = 0$ για κάποια $b_0, \dots, b_{n-1} \in K$, που δεν είναι όλα 0. Άρα θα υπήρχε $h(t) \in K[t]$ με $h(x) = 0$. Έτσι όμως θα υπήρχε κάποιο ανάγωγο μορικό πολυώνυμο $p(t) \in K[t]$ με $p(x) = 0$, (p παράγοντας του h), άρα $\partial p \leq \partial h \leq n-1$. Ειδικότερα, $p \neq q$ κι αυτό αντικρούει στη μοναδικότητα του q . Μένει να δείξουμε ότι τα $1, x, \dots, x^{n-1}$ παράγουν το $K[x]$. Γι' αυτό αρκεί να δείξουμε ότι παράγουν κάθε x^m με $m \geq n$: Για $m = n$ έχουμε $x^n = -a_{n-1} x^{n-1} - \dots - a_1 x - a_0$ και το x^n παράγεται απ' τα $1, x, \dots, x^{n-1}$. Έπαγωγικά τώρα, έστω ότι τα x^r , $r \geq n$ παράγονται απ' τα $1, x, \dots, x^{n-1}$ και $x^r = b_{n-1} x^{n-1} + \dots + b_1 x + b_0$, $b_i \in K$. Έτσι $x^{r+1} = b_{n-1} x^n + b_{n-2} x^{n-1} + \dots + b_1 x^2 + b_0 x = b_{n-1} (-a_{n-1} x^{n-1} - \dots - a_1 x - a_0) + b_{n-2} x^{n-1} + \dots + b_1 x^2 + b_0 x$ άρα και το x^{r+1} παράγεται απ' τα $1, x, \dots, x^{n-1}$. ■

Το $q(t) \in K[t]$ που περιγράφεται στην έκφραση του θεωρήματος 1 λέγεται ελάχιστο πολυώνυμο του x πάνω στο K .

Έστω τώρα ότι $x_1, \dots, x_r \in L$. Με $K[x_1, \dots, x_r]$ θα συμβολίζουμε το δ.α.κ.δ. του L που αποτελείται απ' όλα τα πεπερασμένα αλγεβρικά στοιχεία του L ως προς τις $a_1^{n_1} \dots x_r^{n_r}$, $a \in K$, $n_i \geq 0$ για κάθε $i = 1, \dots, r$. Το $K[x_1, \dots, x_r]$ με τις πράξεις του L γίνεται αντιμεταθετικός δ.α.κ.δ. με μονάδα.

Θεώρημα 2 Αν L είναι πεπερασμένη επέκταση του K και M πεπερασμένη επέκταση του L , τότε M είναι πεπερασμένη επέκταση του K και μάλιστα

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

($[L:K]$ είναι ο βαθμός της επέκτασης L του K , κ.θ.κ.)

Απόδειξη: Έστω $\{y_1, \dots, y_n\}$ μια K -βάση του L και $\{z_1, \dots, z_m\}$ μια L -βάση του M . Αρκεί να δείξουμε ότι τα $y_i z_j$, $1 \leq i \leq n$, $1 \leq j \leq m$ είναι μια K -βάση του M .

Πραγματικά, πρώτα δείχνουμε ότι το σύνολο των $y_i z_j$ παράγει τον M πάνω απ' το K : Έστω $u \in M$. Τότε $u = \alpha_1 z_1 + \alpha_2 z_2 + \dots + \alpha_m z_m$, $\alpha_i \in L$. Άλλα για κάθε $i \in \{1, \dots, m\}$

$$\alpha_i = \beta_{i1} y_1 + \beta_{i2} y_2 + \dots + \beta_{in} y_n, \quad \beta_{ij} \in K$$

Αντικαθιστώντας αυτές τις εκφράσεις των α_i στην παραπάνω έκφραση του u βλέπουμε ότι το u γράφεται ως γραμμικός συνδυασμός των $y_i z_j$, $1 \leq i \leq n$, $1 \leq j \leq m$ με συντελεστές απ' το K .

Τώρα δείχνουμε την ανεξαρτησία του συνόλου των $y_i z_j$ πάνω απ' το K : Έστω

$$\beta_{11} y_1 z_1 + \beta_{12} y_1 z_2 + \dots + \beta_{1m} y_1 z_m + \beta_{21} y_2 z_1 + \beta_{22} y_2 z_2 + \dots + \beta_{2m} y_2 z_m + \dots + \beta_{n1} y_n z_1 + \beta_{n2} y_n z_2 + \dots + \beta_{nm} y_n z_m = 0, \quad \beta_{ij} \in K. \quad \text{Τότε,}$$

$$\sum_{i=1}^n (\beta_{i1} y_i + \beta_{i2} y_i + \dots + \beta_{im} y_i) z_i = 0$$

και ο συντελεστής του z_i ανήκει στο L . Έπειδή τα z_i είναι L -ανεξάρτητα,

$$\beta_{i1} y_1 + \beta_{i2} y_2 + \dots + \beta_{in} y_n = 0, \quad \text{για κάθε } i = 1, \dots, m.$$

Έπειδή τα y_j είναι K -ανεξάρτητα, $\beta_{i1} = \beta_{i2} = \dots = \beta_{in} = 0$. Έτσι, όλα τα β_{ij} είναι 0, άρα τα $y_i z_j$, $1 \leq i \leq n$, $1 \leq j \leq m$ είναι K -ανεξάρτητα. ■

Θεώρημα 3 Αν $x_1, \dots, x_r \in L$, έστωι ώστε το x_i είναι αλγεβρικό πάνω στο K και για $1 \leq i \leq r$ το x_i είναι αλγεβρικό πάνω στο $K[x_1, \dots, x_{i-1}]$, (ειδικώτερα, αν όλα τα x_1, \dots, x_r είναι αλγεβρικά πάνω στο K), τότε ο $K[x_1, \dots, x_r]$ είναι πεπερασμένη επέκταση του K (ειδικώτερα, είναι σώμα).

Απόδειξη. Σύμφωνα με το θεώρημα 3.2, $K[x_1]$ είναι πεπερασμένη επέκταση του K .

Εύκολα διαπιστώνεται ότι $K[x_1, x_2] = (K[x_1])[x_2]$, κι επειδή το x_2 είναι αλγεβρικό πάνω στο σώμα $K[x_1]$, το $K[x_1, x_2]$ είναι πεπερασμένη επέκταση του $K[x_1]$, άρα (θεώρ. 2)

πεπερασμένη επέκταση του K . Τώρα, $K[x_1, x_2, x_3] = (K[x_1, x_2])[x_3]$ και το x_3 είναι

αλγεβρικό πάνω στο $K[x_1, x_2]$, άρα $K[x_1, x_2, x_3]$ πεπερασμένη επέκταση του $K[x_1, x_2]$.

Όπως είδαμε ότι $K[x_1, x_2]$ είναι πεπερασμένη επέκταση του K , άρα (θεώρημα 2) $K[x_1, x_2, x_3]$ είναι πεπερασμένη επέκταση του K . Προχωρώντας μ' αυτό τον τρόπο γρήγορα το δικό σου συμπέρασμα ότι $K[x_1, \dots, x_n]$ είναι πεπερασμένη επέκταση του K . ■

Θεώρημα 3: Κάθε πεπερασμένη επέκταση του K είναι αλγεβρική επέκταση του K .

Απόδειξη. Έστω L πεπερασμένη επέκταση του K και $\alpha \in L$. Επειδή είναι αδύνατο να υπάρχουν άπειρα στοιχεία του L που να είναι K -ανεξάρτητα, θα υπάρχει ακέραιος $n \geq 1$, τέτοιος ώστε τα $1, \alpha, \dots, \alpha^n$ να είναι K -εξαρτημένα. Άρα υπάρχουν $b_0, b_1, \dots, b_n \in K$, όχι όλα 0 με $b_0 + b_1 \alpha + \dots + b_n \alpha^n = 0$. Δηλ. υπάρχει μη μηδενικό πολυώνυμο $f(t) \in K[t]$ με $f(\alpha) = 0$, άρα α είναι αλγεβρικό πάνω στο K . ■

Θεώρημα 4: Αν K υπόσωμα του σώματος L , τότε το υποσύνολο A του L , που αποτελείται από εκείνα τα στοιχεία του L , που είναι αλγεβρικά πάνω στο K , είναι υπόσωμα του L (προφανώς $K \subseteq A$).

Απόδειξη. Άρκει να δείξουμε ότι αν $x, y \in A$, τότε $x+y, x-y, xy \in A$ καθώς επίσης και $x^{-1} \in A$ (αν $x \neq 0$).: Άρα τα x, y είναι αλγεβρικά πάνω στο K , άρα από το θεώρημα 2 ότι $K[x, y]$ είναι πεπερασμένη επέκταση του K , άρα, από το θεώρημα 3, $K[x, y]$ είναι αλγεβρική επέκταση του K . Όπως $x+y, x-y, xy$ είναι στοιχεία του $K[x, y]$, καθώς επίσης και το $x^{-1} \in K[x, y]$ (για $x \neq 0$), άρα τα $x+y, x-y, xy, x^{-1}$ είναι αλγεβρικά πάνω στο K , δηλ. ανήκουν στο A . ■

Αν πάρουμε σαν L το \mathbb{C} και σαν K το \mathbb{Q} τότε το A (του θεωρήματος 3.5) είναι το σύνολο των αλγεβρικών αριθμών. Δηλ. ένας μεγάλος αριθμός χαρακτηρίζεται αλγεβρικός αριθμός αν είναι ρίζα ενός πολυωνύμου με ρητώς συντελεστές. Στην ανείδωτη περίπτωση χαρακτηρίζεται δυσεμβατικός αριθμός.

Ο διάδοχος κείμενος για x αποδείξουμε ότι το σύνολο των δυσεμβατικών αριθμών είναι $\neq \emptyset$ (δηλ. ότι το A είναι γνήσιο υπόσωμα του \mathbb{C}) είναι συνολοθεωρητικός και έρμετος (Cantor): Αποδεικνύουμε πρώτα ότι το \mathbb{R} είναι μη αριθμησιμο σύνολο (δεν υπάρχει δηλ. αμφιμοτοφάνεια, ήτοι απεικόνιση μεταξύ του \mathbb{R} και του \mathbb{N}) και μετά

ὅτι τὸ A εἶναι ἀριθμησιμὸν. Κατὰ συνέπεια, τὸ A εἶναι ὄχι μόνον γνήσιο ὑποσύνολο τοῦ \mathbb{C} ἀλλὰ γνήσιον ὑποσύνολο καὶ τοῦ \mathbb{R} .

Τὸ μειονέκτημα τῆς παραπάνω μεθόδου εἶναι ὅτι δὲ βρίσκουμε μ' αὐτὴ ἕνα καὶ ἓνα ὑπερβατικὸ ἀριθμὸ, μόνον μὴ ἀνιχνεύουμε τὴν ὑπαρξήν τους. Ὁ Liouville μὴ πρώτη φορά, τὸ 1844, "κατασκεύασε" ὑπερβατικὸ ἀριθμὸ:

$$\xi = \sum_{n=1}^{\infty} 10^{-n!}$$

Ἀργότερα ὁ Hermite ἀπέδειξε ὅτι ὁ e εἶναι ὑπερβατικὸς καὶ ὁ Lindemann ἀπέδειξε τὴν ὑπερβατικότητα τοῦ π .

Ἀσκήσεις

Στις παρακάτω ασκήσεις, καθὼς ἐπιπλέον καὶ σ' ἄλλα τὰ ὑπόμνητα κεφάλαια, θεωροῦμε $L:K$ θὰ ἐννοεῖμε ὅτι τὸ K εἶναι ὑπόσωμα τοῦ σώματος L , ἢ, ἰσοδύναμα, τὸ L εἶναι ἐπέκταση τοῦ K . Μὲ $[L:K]$ θὰ συμβολίζουμε τὸ βαθμὸ τῆς ἐπέκτασης.

1 Να βρεθοῦν οἱ βαθμοὶ τῶν ἐπιπέδων ἐπέκτασεων: $\mathbb{C}:\mathbb{Q}$, $\mathbb{R}[\sqrt{5}]:\mathbb{R}$, $\mathbb{Q}[\sqrt[3]{2}]:\mathbb{Q}$, $\mathbb{Q}[\sqrt{3}, \sqrt{7}]:\mathbb{Q}$, $\mathbb{Q}[\sqrt[7]{3}]:\mathbb{Q}$.

2 Ἄν $[L:K]$ πρῶτος, τότε δὲν διαρρήνται σώματα M , $M:K$ καὶ $L:M$ (ταυτοχρόνως), ἐκτός ἀπ' τὸ L καὶ τὸ K .

3 Ἄν $[L:K] = 1$, τότε $L = K$.

4 Ἄν $L:K$ πεπερασμένη ἐπέκταση καὶ ἔχουμε τὴν διαδοχικὴν ἐπέκτασιν

$$L:K_1:K_2:\dots:K_r:K, \text{ τότε } [L:K] = [L:K_1][K_1:K_2]\dots[K_{r-1}:K_r][K_r:K]$$

5 Δείξτε ὅτι ἡ ἐπέκταση $L:K$ εἶναι πεπερασμένη ἂν καὶ μόνον ἂν $L = K[\alpha_1, \dots, \alpha_r]$, ὅπου r πεπερασμένο καὶ καθεὶ α_i εἶναι ἀλγεβρικό πάνω σὲ K .

6 Ἄν A εἶναι τὸ σῶμα τῶν ἀλγεβρικών ἀριθμῶν, δείξτε ὅτι ἡ ἐπέκταση $A:\mathbb{Q}$ δὲν εἶναι πεπερασμένη (κρυστήριον Eisenstein γιὰ τὴν ὑπαρξὴ ἀνιχνεύων πολυώνυμων πάνω σὲ \mathbb{Q} , ὅσοδήποτε μεγάλου βαθμοῦ).

7 Ὑποθέτουμε ὅτι καθεὶ πολυώνυμο τοῦ $\mathbb{Q}[t]$ ἔχει ρίζα σὲ \mathbb{C} , δείξτε ὅτι καθεὶ πολυώνυμο τοῦ $\mathbb{A}[t]$ ἔχει ρίζα σὲ \mathbb{A} . Δείξτε, κατὰ συνέπεια, ὅτι δὲν διαρρήνεται ἄλλ' ἐπέκταση τοῦ \mathbb{A} .

8 Δείξτε ὅτι $\mathbb{Q}[\sqrt{3}, \sqrt{5}] = \mathbb{Q}[\sqrt{3} + \sqrt{5}]$

9 Βρεῖτε μιὰ \mathbb{Q} -βάση τοῦ $\mathbb{Q}[\sqrt{1+\sqrt{3}}]$, ἀρα βρεῖτε τὸ βαθμὸ $[\mathbb{Q}[\sqrt{1+\sqrt{3}}]:\mathbb{Q}]$.

10 Ἄν $[L:K]$ πρῶτος, τότε διαρρήνεται $\alpha \in L$ τέτοιον ὥστε $L = K[\alpha]$. (Τὸ L τότε λέγεται ἀπλήρ' ἐπέκταση τοῦ K .)

Εφαρμογές

Κατασκευές με κλίμα και διαβίτη.

Έστω Σ_0 ένα σύνολο σφαιρών του \mathbb{R}^2 (επίπεδο). Λέμε ότι ένα σημείο του επιπέδου είναι άμεσα κατασκευάσιμο (με κλίμα και διαβίτη) απ' το Σ_0 αν αυτό είναι σημείο κομής δύο εὐθειών, ή μιας εὐθείας με ενός κύκλου, ή δύο κύκλων, οι όποιοι κύκλοι ή εὐθείες προκύπτουν, αντίστοιχα, απ' τις ίδιες γεωμετρικές "πράξεις".

Με κέντρο σημείο του Σ_0 και άκτινα την απόσταση δύο σημείων του Σ_0 γράφεται κύκλος.
2) Γράφεται η εὐθεία που περνά από δύο σημεία του Σ_0 .

Λέμε τώρα ότι ένα σημείο $\sigma \in \mathbb{R}^2$ κατασκευάζεται απ' το Σ_0 αν υπάρχει πεπεραμένο πλήθος σφαιρών $\sigma_1, \sigma_2, \dots, \sigma_n = \sigma$ του \mathbb{R}^2 , τέτοια ώστε το σ_i να είναι άμεσα κατασκευάσιμο απ' το Σ_0 και για $2 \leq i \leq n$, το σ_i να είναι άμεσα κατασκευάσιμο από το $\Sigma_0 \cup \{\sigma_1, \dots, \sigma_{i-1}\}$.

Συμβολίζουμε τώρα με K_0 το υποσύνολο του \mathbb{R} που παράγεται απ' τις συσκευασμένες θλων των σφαιρών του Σ_0 (K_0 είναι δηλ. το ελάχιστο υποσύνολο του \mathbb{R} που περιέχει τις συσκευασμένες θλων των σφαιρών του Σ_0 μ' άλλα λόγια, K_0 είναι η κοινή θλων των υποσυνόλων του \mathbb{R} , που περιέχουν τις συσκευασμένες θλων των σφαιρών του Σ_0).

Θεώρημα 5 Αν οι συσκευασμένες θλων των σφαιρών ενός συνόλου $\Sigma \subseteq \mathbb{R}^2$ περιέχονται σ' ένα υποσύνολο K του \mathbb{R} και το σημείο $\sigma = (x, y)$ είναι άμεσα κατασκευάσιμο, τότε τα x, y είναι άλγεβρικά πάνω στο K και η επέκταση $K[x, y] : K$ είναι βαθμού 1, 2 ή 4 (πρβλ. θεώρημα 3)

Σημείωση: Με τις ίδιες διαδικασίες μπορεί ν' αποδείξει το ακριβέστερο αποτέλεσμα, ότι δηλ. $[K[x, y] : K] = 1$ ή 2, αλλά δε μας είναι απαραίτητο αυτό.

Απόδειξη. Θ' αποδείξουμε το θεώρημα στη "δυσκολότερη" περίπτωση που το σ είναι κομμή δύο κύκλων (οι κύκλοι έγκοιούνται ότι έχουν γράψει όπως μας λέει η πράξη 1, παραπάνω): Αν $(x_1, y_1), (x_2, y_2)$ είναι τα κέντρα των δύο κύκλων τότε, βέβαια, $x_1, y_1, x_2, y_2 \in K$ (τα κέντρα είναι σημεία του Σ). Επίσης αν z_i $i=1, 2$ είναι οι άκτινες των κύκλων και z_i είναι η απόσταση των σφαιρών $(\alpha_i, \beta_i), (\alpha'_i, \beta'_i)$ του Σ (δηλ. $\alpha_i, \beta_i, \alpha'_i, \beta'_i \in K$), τότε $z_i^2 = (\alpha_i - \alpha'_i)^2 + (\beta_i - \beta'_i)^2 \in K$.

Οι συσχετισμένες (x, y) του σ θα επαληθεύουν λοιπός τις σχέσεις

$$(x-x_1)^2 + (y-y_1)^2 = z_1^2, \quad (x-x_2)^2 + (y-y_2)^2 = z_2^2$$

ή, ισοδύναμα

$$(x-x_1)^2 + (y-y_1)^2 - z_1^2, \quad 2(x_2-x_1)x + 2(y_2-y_1)y + x_1^2 - x_2^2 + y_1^2 - y_2^2 = z_1^2 - z_2^2$$

όπου οι συντελεστές και στις δύο εξισώσεις ανήκουν στο K . Απαλείφοντας το y π.χ. μεταξύ των δύο εξισώσεων βρίσκουμε μία εξίσωση, το πολύ δευτεροβάθμια ως προς x , με συντελεστές από το K . Έτσι, το x είναι αλγεβρικό πάνω στο K και $[K[x]:K] = 1$ ή 2 . Όμοια ισχύουν για το y . Τότε (θεώρημα 3) $K[x, y]$ είναι πεπερασμένη επέκταση του K και (βλ. θεώρημα 2),

$$[K[x, y]:K] = [K[x, y]:K[y]] \cdot [K[y]:K]$$

Επειδή $K[x, y]:K[y]$ είναι η επέκταση $(K[y])[x]:K[y]$ και το x είναι ρίζα ενός δευτεροβάθμιου πολυωνύμου του $K[y]$, θα είναι ρίζα ενός, το πολύ δευτεροβάθμιου πολυωνύμου του $(K[y])[t]$, άρα ο βαθμός της επέκτασης $K[x, y]:K[y]$ είναι 1 ή 2. Αντίθετα $[K[y]:K] = 1$ ή 2 , κι έχουμε έτσι το αποτέλεσμα. ■

Έστω τώρα ότι το σ είναι κατασκευασμένο από το σύνολο Σ_0 και $\sigma_1, \sigma_2, \dots, \sigma_n = \sigma$ τα σημεία που μας δόθηκαν από το Σ_0 στην κατασκευή του σ . Θέτουμε $\sigma_i = (x_i, y_i)$ κι έστω K_0 το σώμα του \mathbb{R} που δρίστηκε πριν την έκφραση του θεωρήματος 4. Τότε έχουμε τις έξης διαδοχικές επεκτάσεις:

$$K_1:K_0 \text{ όπου } K_1 = K_0[x_1, y_1], \quad K_2:K_1 \text{ όπου } K_2 = K_1[x_2, y_2] \text{ κ.λ.π. } K_n:K_{n-1}, \text{ όπου } K_n = K_{n-1}[x_n, y_n].$$

Με διαδοχική εφαρμογή του θεωρήματος 2 (βλ. άσκηση 4) και λόγω του θεωρήματος 5 θα έχουμε $[K_n:K_0] = [K_n:K_{n-1}] [K_{n-1}:K_{n-2}] \dots [K_2:K_1] [K_1:K_0] = \text{δύναμη του 2}$. Έτσι αποδεικνύεται το έξης

Θεώρημα 6 Αν το σημείο σ κατασκευάζεται από το σύνολο σημείων Σ_0 και K_0 είναι το ελάχιστο σώμα που περιέχει τις συσχετισμένες δίδων των σημείων του Σ_0 , τότε υπάρχει πεπερασμένη επέκταση K του K_0 που περιέχει τις συσχετισμένες του σ και είναι βαθμού ίσου με δύναμη του 2.

Τώρα έχουμε όλα τα απαραίτητα εφόδια για να αποδείξουμε ότι είναι αδύνατο να δοθεί λύση με κανόνα και διαβήτη στα τρία περίφημα προβλήματα της αρχαιότητας: Διπλασιασμός

του κύβου, ερχοσύνισμα της γωνίας $\frac{\pi}{3}$, τετραγωνισμός του κύβου

Θεώρημα 7 Ο διπλασιασμός του κύβου είναι αδύνατος με κανόνα και διαβήση.

Απόδειξη. Αν υποθέσουμε ότι μας δίνεται ο μοναδιαίος κύβος. Για να πετύχουμε το διπλασιασμό του πρέπει να κατασκευάσουμε ένα ευθύγραμμο τμήμα (ή άκρη του νέου κύβου) με μήκος $\sqrt[3]{2}$. Έδώ τα μόνα μας δεδομένα είναι το μοναδιαίο μήκος (ή άκρη του αρχικού κύβου). Άρα $\Sigma_0 = \{(0,0), (1,0)\}$, οπότε $K_0 = \mathbb{Q}$.

Πρέπει να κατασκευάσουμε με κανόνα και διαβήση το σημείο $\sigma = (x,0)$ όπου $x = \sqrt[3]{2}$.

Αν αυτό γίνει, τότε θα υπήρχε πεπερασμένη επέκταση K του \mathbb{Q} με $x \in K$ και $[K:\mathbb{Q}] = \delta$ δύναμη του 2. Όμως το α είναι ρίζα του $t^3 - 2 \in \mathbb{Q}[t]$, που είναι ανάγωγο (σε $\mathbb{Q}[t]$), λόγω του κριτηρίου του Eisenstein, οπότε (θεώρημα 1)

$[\mathbb{Q}[\alpha]:\mathbb{Q}] = 3$. Είναι φανερό όμως ότι $K \supseteq \mathbb{Q}[\alpha]$, άρα έχουμε τις διαδοχικές επεκτάσεις $K:\mathbb{Q}[\alpha]$ και $\mathbb{Q}[\alpha]:\mathbb{Q}$ και κατά συνέπεια,

$$\delta \text{ δύναμη του } 2 = [K:\mathbb{Q}] = [K:\mathbb{Q}[\alpha]] \cdot [\mathbb{Q}[\alpha]:\mathbb{Q}] = \text{πολλώ του } 3,$$

άτοπο. ■

Θεώρημα 8 Η γωνία $\frac{\pi}{3}$ δεν είναι δυνατή να ερχοσύνισθεί με κανόνα και διαβήση.

Απόδειξη. Έχουμε στη διάθεσή μας το μοναδιαίο (τριγωνομετρικό) κύκλο, οπότε μια γωνία είναι κατασκευάσιμη αν και μόνο αν μπορούμε να κατασκευάσουμε ευθύγραμμο τμήμα ίσο με το συνήμιτονα της γωνίας. Άρα, στο συγκεκριμένο μας πρόβλημα,

$\Sigma_0 = \{(0,0), (1,0)\}$, $K_0 = \mathbb{Q}$ και ζητούμε να κατασκευάσουμε το σημείο $\sigma = (x,0)$,

όπου $x = \cos \frac{\pi}{3}$. Αν αυτό μπορούσε να γίνει με κανόνα και διαβήση, τότε θα υπήρχε

επέκταση $K:\mathbb{Q}$ με $x \in K$ και $[K:\mathbb{Q}] = \delta$ δύναμη του 2. Όμως, λόγω της σχέσης

$$\cos 3\theta = 4\cos^3\theta - 3\cos\theta \quad \text{θα έχουμε (για } \theta = \frac{\pi}{3}\text{)} \quad \frac{1}{2} = 4x^3 - 3x \quad \eta$$

$$8x^3 - 6x - 1 = 0$$

και το x είναι, λοιπόν, ρίζα του $8t^3 - 6t - 1$, που είναι ανάγωγο σε $\mathbb{Q}[t]$. (αν

δεν ήταν, θα πρέπει να έχει τουλάχιστον ένα πρωτοβάθμιο παράγοντα, άρα τουλάχιστον

μία ρητή ρίζα. Όμως οι μονές μηδενές ρητές ρίζες του πολυωνύμου αυτού είναι οι

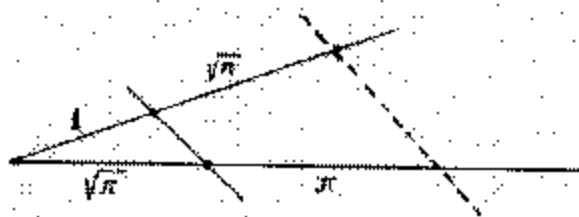
$\pm 1, \pm \frac{1}{2}, \pm \frac{1}{4}, \pm \frac{1}{8}$, κι άμεσα επαληθεύεται ότι καμία απ' αυτούς τους ρητούς δεν είναι ρίζα του). Άρα $[\mathbb{Q}[x]:\mathbb{Q}] = 3$, και όπως στο θεώρημα 7. Οδηγούμαστε

σε άτοπο. ■

Θεώρημα 9 Ο τετραγωνισμός του κύκλου είναι αδύνατος με τόν κανόνα και τή διαβήτη.

Απόδειξη. Μπορούμε να υποθέσουμε ότι μας δίνουμε τή μοναδιαία κύκλο. τή πρόβλημα του τετραγωνισμού του συνίσταται στή να κατασκευάσουμε ένα τετράγωνο μέ εμβαδόν ίσο μέ τή εμβαδόν του κύκλου, που είναι π . Άρα πρέπει να κατασκευάσουμε εδωγραφίμο τμήμα μήκους $\sqrt{\pi}$, δηλ. να κατασκευάσουμε τή σφύρα $\sigma = (x, 0)$, όπου $x = \sqrt{\pi}$.

Ξεκινούμε πάλι από τή $\Sigma_0 = \{(0, 0), (1, 0)\}$, $K_0 = \mathbb{Q}$. Αν η κατασκευή τή σφύρας σ ήταν δυνατή μέ κανόνα και διαβήτη, τότε θα ήταν δυνατή (μέ κανόνα και διαβήτη) και η κατασκευή τή σφύρας $(\pi, 0)$ (βλ. σχήμα)



Αλλά τότε (θεώρημα 6) θα υπήρχε πεπερασμένη επέκταση τή \mathbb{Q} που θα περιείχε τή π και, κατά συνέπεια (θεώρημα 3), ό π θα ήταν αλγεβρικός πάνω στή \mathbb{Q} , δηλ. αλγεβρικός αριθμός. Αυτό όμως αντίκειται στή διάσημο θεώρημα τή Lindemann ότι ό π είναι υπερβατικός αριθμός. ~~(Lindemann's theorem states that pi is transcendental over the rationals)~~ ■

Άσκησης

1. Αποδείξτε ότι είναι αδύνατη μέ κανόνα και διαβήτη η κατασκευή τή κανονικού εννεαγώνου.
2. Αποδείξτε ότι η γωνία θ μπορεί να τριχοκομίδει μέ κανόνα και διαβήτη, αν και μόνο αν τή πολυώνυμο $4t^3 - 3t - \sin\theta$ είναι σύνθετο στή $\mathbb{Q}(\sin\theta)$. (Αν L είναι επέκταση τή K και $\alpha \in L$, συμβολίζουμε μέ $K(\alpha)$ τή ελάχιστη επέκταση τή K που περιέχει τή σύνολο $K \cup \{\alpha\}$. αποδεικνύεται απ' όπλα τή συνέχεια τή L τή μορφή $(x_1 \alpha^n + \dots + x_r \alpha + x_0)(y_1 \alpha^m + \dots + y_s \alpha + y_0)^{-1}$, όπου $x_i, y_j \in K$ και η δεικνύει παράγοντας είναι $\neq 0$. Για ό αλγεβρικό πάνω στή K είναι, προφανώς, $K(\alpha) = K[\alpha]$).
3. Κάνοντας χρήση τή τύπου για τή συν5θ κατασκευάστε μέ κανόνα και διαβήτη τή κανονικό πεντάγωνο. (συν5θ = 16 συν³θ - 20 συν²θ + 5 συνθ).