1. Δακτύλιοι, Ακέραιες Περιοχές, Σώματα : Βασικές γνώσεις

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

α) Το R με την πράξη $+$ είναι αβελιανή 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 το 0 και ονομάζεται μηδέν. Η πράξη $\cdot$ δεν έχει, εν γένει, ουδέτερο στοιχείο (δηλ. $e \in R$ τ.ώ. $e \cdot a = a \cdot e = a \ \forall a \in R$). Αν έχει, συμβολίζεται (συνήθως) με 1 και ονομάζεται μονάδα του δακτυλίου R. Στην περίπτωση αυτή λέμε ότι ο R είναι <u>δακτύλιος με μονάδα</u>. Η πράξη $\cdot$ δεν είναι, κατ' ανάγκη, αντιμεταθετική. Αν είναι, ο R λέγεται <u>αντιμεταθετικός δακτύλιος</u>. Συνηθέστατα, αντί $a \cdot b$ γράφουμε ab.

<u>Παραδείγματα</u>:

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

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

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

Και αυτός ο δακτύλιος είναι αντιμεταθετικός με μονάδα.

γ) Έστω $K = \mathbb{Q}$ ή $\mathbb{R}$ ή $\mathbb{C}$ και $\mathcal{M}(n;K)$ το σύνολο των $n \times n$ πινάκων με στοιχεία από το K. Το σύνολο αυτό εφοδιασμένο με τις συνήθεις πράξεις πρόσθεσης και πολλαπλασιασμού πινάκων καθίσταται δακτύλιος με μονάδα, όχι όμως αντιμεταθετικός (αντιπαράδειγμα: 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 $\mathbb{Z}[\sqrt{d}] \stackrel{\text{ορ}}{=} \{x + y\sqrt{d} ;\ x, y \in \mathbb{Z}\}$ εφοδιασμένο με τις πράξεις του $\mathbb{C}$ γίνεται δακτύλιος (αντιμεταθετικός με μονάδα).

ε) Έστω $\mathcal{F}$ το σύνολο όλων των συναρτήσεων $f : A \longrightarrow \mathbb{R}$, 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 $(f+g)(x) \stackrel{\text{ορ}}{=} f(x) + g(x)$, $\forall\, x \in A$.

Και αναλογίαν 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. Εδώ, 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:

$$(r_1, s_1) + (r_2, s_2) \stackrel{\text{ορ}}{=} (r_1 + r_2,\ s_1 + s_2)$$

($+$ του R, $+$ του S)

$$(r_1, s_1) \cdot (r_2, s_2) \stackrel{\text{ορ}}{=} (r_1 \cdot r_2,\ s_1 \cdot s_2)$$

($\cdot$ του R, $\cdot$ του S)

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

γίνεται δακτύλιος, ὁ δποῖος, ἐξ ὁρισμοῦ, λέγεται εὐθύ ἄθροισμα τῶν R καὶ S.

Συμβολισμοί: Ἄν R εἶναι δακτύλιος, γιά κάθε $a \in R$ τό $-a$ συμβολίζει τό συμμετρικό (ἀντίθετο) στοιχεῖο τοῦ a στήν ὁμάδα $(R,+)$. Ἄν n εἶναι μή ἀρνητικός ἀκέραιος καί $a \in R$, ὁρίζουμε $n \cdot a$ νά σημαίνει $\underbrace{a+a+\dots+a}_{n \text{ φορές}}$ (ἄρα $0 \cdot a = 0$). ($\uparrow \in \mathbb{Z}$, $\downarrow \in R$)

Ἄν ὁ n εἶναι ἀρνητικός ἀκέραιος καί $a \in R$, ὁρίζουμε

$$n \cdot a = -((-n) \cdot a),$$

καί στή συνέχεια βλέπουμε ὅτι αὐτή ἡ σχέση ἰσχύει καί γιά $n \geq 0$.

Ἡ ἑπομένη πρόταση δίνει ὅλες τίς στοιχειώδεις ἰδιότητες τῶν πράξεων ἑνός δακτυλίου.

Πρόταση 1 Ἔστω R δακτύλιος καί $a, b, c \in R$.

α) Τό 0 τοῦ R εἶναι μοναδικό. Τό $1 \in R$, ἄν ὑπάρχει, εἶναι μοναδικό.

β) Κάθε $a \in R$ ἔχει ἕνα ἀκριβῶς ἀντίθετο $-a$.

γ) Ἄν $a+b = a+c$ τότε $b = c$, καθώς ἐπίσης καί ἄν $b+a = c+a$ τότε $b = c$.

δ) Κάθε ἐξίσωση (ὡς πρός x) $a+x = b$ καί $x+a = b$ ἔχει ἀκριβῶς μία λύση.

ε) $-(-a) = a$ καί $-(a+b) = (-a)+(-b) \overset{\text{συμβ.}}{=} -a-b$

ς) $0 \cdot a = a \cdot 0 = 0$ (ἐδῶ 0 εἶναι τό μηδέν τοῦ R)

ζ) Γιά ὁποιουσδήποτε ἀκεραίους m, n:

$m(a+b) = m \cdot a + m \cdot b$, $(m+n) \cdot a = m \cdot a + n \cdot a$

$m(n a) = (mn) \cdot a$, $m \cdot (ab) = (m \cdot a) b = a (m \cdot b)$, $(ma)(n \cdot b) = (mn) \cdot (ab)$.

η) $a(-b) = (-a) b = -(ab) \overset{\text{συμβ.}}{=} -ab$

θ) $(-a)(-b) = ab$

ι) $a(b-c) = ab - ac$, $(b-c)a = ba - ca$

Η απόδειξη αφήνεται ως άσκηση.

Συμβολισμός. Αν R είναι δακτύλιος, $a \in R$ και n θετικός ακέραιος, τότε a^n ορίζουμε να σημαίνει $\underbrace{a \cdot a \cdots a}_{n}$ φορές (άρα $a^1 = a$).
Για n αρνητικό ακέραιο, το σύμβολο a^n έχει νόημα μόνο αν R έχει μονάδα και υπάρχει το συμμετρικό (αντίστροφο) του a ως προς την πράξη $\cdot$ (δηλ. υπάρχει $b \in R$ τ.ώ. $b \cdot a = a \cdot b = 1$). 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 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,
α) $a^m \cdot a^n = a^{m+n}$,
β) Αν υπάρχει το a^{-1}, τότε $a^{-m} = (a^{-1})^m$
γ) $(a^m)^n = a^{mn} = (a^n)^m$

Η απόδειξη αφήνεται ως άσκηση.

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

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

Απόδειξη. $ab=ac \Rightarrow ab-ac=0 \Rightarrow$ (βλ. 1, 2) $a(b-c)=0$. Η τελευταία ισότητα, αφού δεν υπάρχουν μηδενοδιαιρέτες στον R και $a\neq 0$, συνεπάγεται $b=c$. Ομοίως αν $ba=ca$. Ο.Ε.Δ.

Ορισμός. Ένας αντιμεταθετικός δακτύλιος με μονάδα, στον οποίο $1\neq 0$ και δεν υπάρχουν μηδενοδιαιρέτες λέγεται ακέραια περιοχή.

Παρατηρήστε ότι ο σχολαστικός περιορισμός $1\neq 0$ σημαίνει, απλούστατα, ότι $R\neq\{0\}$. Πράγματι, αν $R\neq\{0\}$ και $a\in R-\{0\}$, τότε (υπουθέται ότι ο R έχει μονάδα) $1\cdot a=a\neq 0=$ (βλ. 1, 5) $0\cdot a$, άρα απομένει να είναι $1=0$.

Ορισμός. Έστω S ένα μη κενό υποσύνολο του δακτυλίου R. Αν το S με τις πράξεις $+$ και $\cdot$ του R είναι δακτύλιος (ειδικώτερα, συνεπώς, το αποτέλεσμα των πράξεων μεταξύ οποιωνδήποτε στοιχείων του S πρέπει ν' 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, $a\in S \Rightarrow -a\in S$).

Η απόδειξη είναι απλή και αφήνεται ως άσκηση.

Σῶμα εἶναι ἕνας ἀντιμεταθετικὸς δακτύλιος $^{\neq\{0\}}$, τοῦ ὁποίου τὰ μὴ μηδενικὰ στοιχεῖα, ἐφωδιασμένα μὲ τὸν πολλαπλασιασμό, ἀποτελοῦν ὁμάδα.

Πρόταση 5. Ἕνας δακτύλιος εἶναι σῶμα ἂν καὶ μόνο ἂν εἶναι ἀπέραντα περιοχή, τῆς ὁποίας κάθε μὴ μηδενικὸ στοιχεῖο ἔχει ἀντίστροφο.

Ἡ ἀπόδειξη ἀφήνεται ὡς ἄσκηση.

Πρόταση 6. Κάθε πεπερασμένη ἀπέραντα περιοχή εἶναι σῶμα.

Ἀπόδειξη. Σύμφωνα μὲ τὴν πρόταση 5, ἀρκεῖ ν' ἀποδείξουμε ὅτι κάθε μὴ μηδενικὸ στοιχεῖο τῆς ἀπέραντας περιοχῆς, τὴν ὁποία ἂς συμβολίσουμε μὲ R, ἔχει ἀντίστροφο. Ἔστω λοιπὸν $a \in R-\{0\}$. Γιὰ κάθε $x \in R-\{0\}$ εἶναι $a \cdot x \neq 0$. (R εἶναι ἀπέραντα περιοχή), ἄρα ἔχουμε μιὰ ἀπεικόνιση $\phi : R-\{0\} \longrightarrow R-\{0\}$, $\phi(x) = ax$. Εὔκολα φαίνεται ὅτι ἡ ϕ εἶναι ἀμφιμονοσήμαντη. (λόγῳ τοῦ ὅτι R εἶναι ἀπέραντα περιοχή). Ἄρα, τὸ πλῆθος τῶν στοιχείων τοῦ $R-\{0\}$ εἶναι τὸ ἴδιο μὲ τὸ πλῆθος τῶν στοιχείων τοῦ $\phi(R-\{0\})$ (ἐδῶ ἐπαιξε ρόλο τὸ ὅτι τὸ R εἶναι πεπερασμένο). Ὅμως, $\phi(R-\{0\}) \subseteq R-\{0\}$, ἄρα (ἀφοῦ ἔχουν τὸ ἴδιο πληθάριθμο) $\phi(R-\{0\}) = R-\{0\}$. Τώρα, ἐπειδὴ $1 \in R-\{0\}$, θὰ ὑπάρχει $x \in R-\{0\}$ τέτοιο ὥστε $\phi(x) = 1$. Δηλαδὴ $a \cdot x = 1$, ποὺ σημαίνει ὅτι τὸ a ἔχει ἀντίστροφο τὸ x, ὁ.ἐ.δ.

Πόρισμα. Ὁ δακτύλιος $\mathbb{Z}_n$ εἶναι σῶμα ἂν καὶ μόνο ἂν ὁ n εἶναι πρῶτος.

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

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

Πρόταση 7. Έστω F σώμα και $\phi \neq K \subseteq F$. 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 $\phi : R \longrightarrow S$ μια απεικόνιση τέτοια ώστε, για κάθε ζευγάρι $a, b \in R$,

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

($+$: πρόσθεση του R; $+$: πρόσθεση του S; $\cdot$: πολλαπλασιασμός του R; $\cdot$: πολλαπλασιασμός του S)

λέγεται ομομορφισμός του R στον S.

Αν, επιπλέον, η ϕ είναι αμφιμονοσήμαντη, τότε έχομε ένα μονομορφισμό του R στον S, αν η ϕ είναι "επί", έναν επιμορφισμό

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

Εξ ορισμού, αν η ϕ είναι ομομορφισμός του R στον S, θα είναι ομομορφισμός της ομάδας $(R,+)$ στην ομάδα $(S,+)$. Αντιστρόφως, όμως, αν μια απεικόνιση $\phi: R \longrightarrow S$ 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 $\phi: \mathbb{Z} \longrightarrow 2\mathbb{Z}$, $\phi(a)=2a$, 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 ορισμοί ισχύουν αν οι R, S είναι ακέραιες περιοχές ή σώματα.

Παραδείγματα

α) Έστω ακέραιος $n>1$. Η απεικόνιση $\phi: \mathbb{Z} \longrightarrow \mathbb{Z}_n$ (βλ. παράδειγμα β στην §1), η οποία ορίζεται απ' τη σχέση $\phi(a)=\hat{a}$ είναι επιμορφισμός δακτυλίων.

β) Έστω ότι R, S είναι δακτύλιοι και $R\times S$ το ευθύ τους άθροισμα (παράδειγμα ε, §1). Καθεμιά απ' τις απεικονίσεις

$$\pi_1: R\times S \longrightarrow R, \quad \pi_1(r,s)=r$$

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

είναι επιμορφισμοί.

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

$\mathbb{Z}[\sqrt{d}]$ (βλ. παράδειγμα δ, §1) καὶ τὴν ἀπεικόνιση
$\phi : \mathbb{Z}[\sqrt{d}] \longrightarrow \mathbb{Z}[\sqrt{d}]$, $\phi(x+y\sqrt{d}) = x-y\sqrt{d}$.
Ἡ ϕ εἶναι ἰσομορφισμὸς τοῦ δακτυλίου $\mathbb{Z}[\sqrt{d}]$ στὸν ἑαυτό του.

Γενικά, ἕνας ἰσομορφισμὸς δακτυλίου (ἀντιστ. ἀκεραίας περιοχῆς, σώματος) σὲ ἑαυτό του λέγεται <u>αὐτομορφισμὸς</u> τοῦ δακτυλίου (ἀντιστ. τῆς ἀκεραίας περιοχῆς, τοῦ σώματος).

δ) Ἕνας πολὺ γνωστὸς αὐτομορφισμὸς τοῦ σώματος $\mathbb{C}$ τῶν μιγαδικῶν ἀριθμῶν εἶναι ἡ ἀπεικόνιση $\bar{} : \mathbb{C} \longrightarrow \mathbb{C}$, ἡ ὁποία ὁρίζεται ἀπὸ τὴ σχέση $\overline{x+iy} = x-iy$.

ε) Στὸ παράδειγμα αὐτὸ θὰ χρησιμοποιήσουμε συχνὰ τοὺς τρεῖς δακτυλίους $\mathbb{Z}_2$, $\mathbb{Z}_3$, $\mathbb{Z}_6$. Γιὰ νὰ μὴ γίνει σύγχυση στὸ συμβολισμό, τὶς κλάσεις τοῦ τυχόντος $a \in \mathbb{Z}$ modulo 2, 3 καὶ 6, ἀντιστοίχως, θὰ συμβολίζουμε μὲ $[a]_2$, $[a]_3$, $[a]_6$. Θεωρῶ τώρα τὴν ἀπεικόνιση
$\phi : \mathbb{Z}_6 \longrightarrow \mathbb{Z}_2 \times \mathbb{Z}_3$, $\phi([a]_6) = ([a]_2, [a]_3)$
Ἡ ϕ εἶναι ἰσομορφισμός.
Γενικώτερα, ἂν οἱ m, n εἶναι ἀκέραιοι > 1, πρῶτοι μεταξύ τους, τότε ἡ ἀπεικόνιση $\phi : \mathbb{Z}_{mn} \longrightarrow \mathbb{Z}_m \times \mathbb{Z}_n$,
$\phi([a]_{mn}) = ([a]_m, [a]_n)$
εἶναι ἰσομορφισμός. Ἐδῶ, τὸ δυσκολώτερο εἶναι ν' ἀποδείξει κανεὶς ὅτι ἡ ϕ εἶναι ἀμφιμονοσήμαντη καὶ στὸ σημεῖο αὐτὸ σημαντικὸ ρόλο παίζει ἡ ὑπόθεση ὅτι οἱ m, n εἶναι πρῶτοι μεταξύ τους.

<u>Πρόταση 1</u>. Ἔστω ὅτι R, S εἶναι δακτύλιοι καὶ $\phi : R \longrightarrow S$ ὁμομορφισμός. Τότε
α) $\phi(\underset{\uparrow}{0}) = 0 \in S$
$\quad\quad 0 \in R$

β) $\phi(-r) = -\phi(r)$ $\forall\, r \in R$.

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

δ) Με τις υποθέσεις του (γ), έστω επιπλέον ότι για το $r \in R$ υπάρχει το αντίστροφό 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 ακέραια περιοχή ή σώμα, τότε και ο S είναι αντιμεταθετικός δακτύλιος ή ακέραια περιοχή ή σώμα, αντιστοίχως.

ζ) Έστω ότι ο ϕ είναι ισομορφισμός. Τότε και η απεικόνιση $\phi^{-1}: S \longrightarrow R$ (η οποία είναι καλά ορισμένη, αφού η ϕ είναι αμφιμονοσήμαντη και "επί") είναι ισομορφισμός. Επιπλέον, αν T είναι δακτύλιος και $\psi: S \longrightarrow T$ ισομορφισμός, τότε η απεικόνιση $\psi \circ \phi : R \longrightarrow T$ είναι ισομορφισμός.

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

Απόδειξη. Δίνεται ως άσκηση.

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

Στην περίπτωση δακτυλίων 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 $n \cdot 1 = 0$. Ισχυριζόμαι ότι δεν υπάρχει μη αρνητικός ακέραιος $m < n$ με $m \cdot 1 = 0$. Πράγματι, αν υπήρχε, τότε για κάθε $r \in R$ θα είχαμε

$$m \cdot r = m \cdot (1 \cdot r) \quad (\text{το } 1 \text{ είναι η μονάδα του } R)$$
$$= (m \cdot 1) \cdot r \quad (\text{Πρόταση 15, §1})$$
$$= 0 \cdot r = 0 \quad (\text{Πρόταση 15, §1}),$$

και θα έρχόμαστε σε αντίφαση με τον ορισμό του n, δ.έ.δ.

Παράδειγμα: Άν ο n είναι ακέραιος > 1, τότε η χαρακτηριστική του δακτυλίου $\mathbb{Z}_n$ 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 θετικός $m < n$ τέτοιος ώστε $m \cdot \hat{1} = \hat{0}$, αυτό θα σήμαινε ότι $\hat{m} = \hat{0}$, δηλαδή, ότι $n \mid m$, 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 ακέραια 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. πόρισμα 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
$0=p\cdot 1=(qr)1=(qr)(1\cdot 1)=(q\cdot 1)\cdot(r\cdot 1)$. Επειδή η D είναι ακέραια 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 από το q είτε από το r άρα, οπωσδήποτε, μικρότερη από το p. Άτοπο.
Στην περίπτωση που η χαρακτηριστική είναι 0, θεωρώ την απεικόνιση $\phi:\mathbb{Z}\longrightarrow D$, $\phi(m)=m\cdot 1$. 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 $\psi:\mathbb{Z}_p\longrightarrow D$, $\psi(\hat{m})=m\cdot 1$ 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 ακέραια περιοχή D υπάρχει ένα σώμα F_D με τις εξής ιδιότητες (i) Το F_D περιέχει μια ακέραια περιοχή Δ ισόμορφη προς την D και (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 ισομορφισμό. Δηλαδή, αν

, τό F είναι ένα σῶμα, πού πληροῖ τίς συνθῆκες (i) καί (ii), τότε $F \cong F_D$.

Απόδειξη. Συμβολίζομε $D^* = D - \{0\}$. Στό σύνολο $D \times D^*$ ὁρίζομε τή σχέση $\sim$ ὡς ἑξῆς:

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

Εὔκολα ἀποδεικνύεται ὅτι ἡ $\sim$ εἶναι σχέση ἰσοδυναμίας. Τήν κλάση ἰσοδυναμίας τοῦ τυχόντος $(a,b) \in D \times D^*$ συμβολίζομε μέ $\frac{a}{b}$. (Παρατηρῆστε ὅτι, μέχρι στιγμῆς, δέν ἔχομε ξαναχρησιμοποιήσει τό σύμβολο $\frac{a}{b}$). Συνεπῶς,

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

Τό σύνολο τῶν κλάσεων ἰσοδυναμίας συμβολίζομε μέ F_D. Δηλαδή, $F_D = \left\{ \frac{a}{b} : (a,b) \in D \times D^* \right\}$.

Στό F_D ὁρίζομε πρόσθεση καί πολλ/σιασμό ὡς ἑξῆς:

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

Οἱ πράξεις αὐτές εἶναι καλά ὁρισμένες. Δηλαδή, ἄν $\frac{a_1}{b_1} = \frac{c_1}{d_1}$ καί $\frac{a_2}{b_2} = \frac{c_2}{d_2}$ τότε $\frac{a_1 b_2 + a_2 b_1}{b_1 b_2} = \frac{c_1 d_2 + c_2 d_1}{d_1 d_2}$ καί

$\frac{a_1 a_2}{b_1 b_2} = \frac{c_1 c_2}{d_1 d_2}$ (ἡ ἀπόδειξη ἀφήνεται ὡς ἄσκηση).

Ἀμέσως διαπιστώνεται ὅτι τό $\frac{0}{1}$ εἶναι τό οὐδέτερο στοιχεῖο τῆς πρόσθεσης (μηδέν) καί τό $\frac{1}{1}$ τό οὐδέτερο στοιχεῖο τοῦ πολλ/σιασμοῦ (μονάδα). Τό ἀντίθετο τοῦ $\frac{a}{b}$ εἶναι τό $\frac{-a}{b}$. καί τό ἀντίστροφο τοῦ $\frac{a}{b} \neq \frac{0}{1}$ εἶναι τό $\frac{b}{a}$.

Ὕστερα ἀπό αὐτές τίς παρατηρήσεις, εἶναι εὔκολο ν' ἀποδείξει κανείς ὅτι τό F_D μέ τίς ὁριοθετοῦσες πράξεις γίνεται σῶμα. Εὔκολα, ἐπίσης, μέ τή βοήθεια τῆς Πρότασης 4, §1, ἀποδεικνύ-

εται ότι το $\Delta = \{\frac{a}{1} : a \in D\} \subseteq F_D$ είναι ακέραια περιοχή και ένας προφανής ισομορφισμός 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. Δίδεται το 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 τα $\frac{a}{1}, \frac{b}{1} \in \Delta$.

Μένει να αποδειχθεί η μοναδικότης, μέχρις ισομορφισμού, του F_D. Έστω λοιπόν σώμα F, A ακέραια 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 δείξωμε ότι $F \cong F_D$. Πράγματι, έστω $\psi : D \longrightarrow A$ ισομορφισμός. Τότε θεωρώ την απεικόνιση

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

Η ϕ είναι καλά ορισμένη: Άν $\frac{a_1}{b_1} = \frac{a_2}{b_2}$ τότε $a_1b_2 = a_2b_1$.

Λόγω του ισομορφισμού ψ, $\psi(a_1)\cdot\psi(b_2) = \psi(a_2)\psi(b_1)$ 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 αμφιμονοσήμαντη.

Η ϕ είναι "επί": 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 $\psi(b) = \alpha_1$, $\psi(c) = \alpha_2$, συνεπώς $f = \alpha_1\alpha_2^{-1} = \psi(b)\psi(c)^{-1} = \phi\left(\frac{b}{c}\right)$

Τέλος, το ότι η ϕ είναι δμομορφισμός, αποδεικνύεται εύκολα. Άν ληφθεί υπ' όψη ότι η ψ είναι δμομορφισμός, δ.έ.δ.

Ορισμός. Έστω D ακέραια περιοχή. Το μοναδικό, μέχρις ισομορφισμού, σώμα F_D, του οποίου η ύπαρξη εξασφαλίζεται από την τελευταία πρόταση, λέγεται σώμα πηλίκων της D.

3. Πυρήνας ομομορφισμού - Ιδεώδη - Δακτύλιος-πηλίκο.

Ορισμός. 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 $i \cdot r \in I$ και $r \cdot i \in I$. Ο μηδενικός δακτύλιος $\{0\}$ καθώς και ο ίδιος ο R είναι ιδεώδη, τα λεγόμενα τετριμμένα ιδεώδη του R.

Πρόταση 1. Έστω $\phi : R \longrightarrow S$ ομομορφισμός δακτυλίων.
α) Η εικόνα του ϕ (που συμβολίζεται $\mathrm{Im}\phi$ ή $\phi(R)$) είναι υποδακτύλιος του S.
β) Ο πυρήνας του ϕ, $\ker\phi \stackrel{\text{ορ}}{=} \{r \in R : \phi(r) = 0 \in S\}$ είναι ιδεώδες του R.
γ) Ο ϕ είναι μονομορφισμός αν και μόνο αν $\ker\phi = \{0\}$.

Απόδειξη. α) Άμεση συνέπεια της Πρότασης 4, § 1.
β) Το ότι ο $\ker\phi$ είναι υποδακτύλιος του R, είναι άμεση συνέπεια της Πρότασης 4, § 1. Αν τώρα $r \in \ker\phi$ και $a \in R$, τυχόν, τότε $\phi(ar) = \phi(a)\phi(r) = \phi(a) \cdot 0 = 0$ και, αναλόγως, $\phi(r \cdot a) = 0$. Άρα $ar \in \ker\phi$ και $ra \in \ker\phi$.
γ) Έστω ότι ο ϕ είναι μονομορφισμός. Επειδή $\phi(0) = 0$, έπεται ότι δεν μπορεί να υπάρχει $r \neq 0$ με $\phi(r) = 0$, άρα $\ker\phi = \{0\}$. Αντιστρόφως, έστω $\ker\phi = 0$. Θα δείξω ότι η ϕ είναι αμφιμονοσήμαντη. Πράγματι, αν $\phi(r_1) = \phi(r_2)$, τότε $\phi(r_1 - r_2) = 0$, δηλ.

$r_1 - r_2 \in \mathrm{Ker}\,\phi = \{0\}$, ὁπότε $r_1 = r_2$, ἀλλ' ἐλ. δ.

Ὁρισμός. Ἔστω R ἀντιμεταθετικὸς δακτύλιος μὲ μονάδα. Τὸ ἰδεώδες I τοῦ R λέγεται κύριο ἰδεώδες, ἂν ὑπάρχει $a \in R$ τέτοιο ὥστε $I = aR = Ra \overset{\text{ορ}}{=} \{ra : r \in R\}$.

Ἔστω R ἀντιμεταθετικὸς δακτύλιος μὲ μονάδα. Τὸ κύριο ἰδεώδες $aR = Ra$ τὸ συμβολίζομε, ἐπίσης, μὲ $\langle a \rangle$ ἢ (a). προφανῶς, εἶναι τὸ ἐλάχιστο ἰδεώδες τοῦ R, τὸ ὁποῖο περιέχει τὸ a. Τὸ $\langle a \rangle$ λέγεται κύριο ἰδεώδες, πού παράγεται ἀπὸ τὸ a. Ἂς τονίσαμε σ' αὐτὸ τὸ σημεῖο ὅτι ὁ R, ἐν γένει, περιέχει καὶ ἰδεώδη, τὰ ὁποῖα δὲν εἶναι κύρια· βλ. π.χ. τὸ παράδειγμα δ, παρακάτω.

Παραδείγματα I

α) Ὁ ἐπιμορφισμὸς $\phi : \mathbb{Z} \to \mathbb{Z}_n$, $\phi(a) = \hat{a}$ (βλ. παράδειγμα (α), §2) ἔχει πυρήνα $\mathrm{Ker}\,\phi = n\mathbb{Z}$ (κύριο ἰδεώδες).

β) Ἔστω R ἀντιμεταθετικὸς δακτύλιος μὲ μονάδα καὶ $a_1, \ldots, a_n \in R$ (σταθερά). Τὸ σύνολο

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

συμβολίζεται μὲ $Ra_1 + \cdots + Ra_n$ ἢ $\langle a_1, \ldots, a_n \rangle$ ἢ $(a_1, \ldots, a_n)$. Εἶναι ἰδεώδες καὶ, μάλιστα, τὸ ἐλάχιστο ἰδεώδες τοῦ R, τὸ ὁποῖο περιέχει τὰ $a_1, \ldots, a_n$ (ἡ ἀπόδειξη εἶναι ἁπλῆ). Ὀνομάζεται ἰδεώδες (τοῦ R) παραγόμενο ἀπὸ τὰ $a_1, \ldots, a_n$. Γιὰ $n = 1$ ἔχομε τὴν εἰδικὴ περίπτωση τοῦ κυρίου ἰδεώδους, πού παράγεται ἀπὸ τὸ a_1.

γ) Ὅλα τὰ ἰδεώδη τοῦ $\mathbb{Z}$ εἶναι κύρια. Πράγματι, ἔστω I ἰδεώδες τοῦ $\mathbb{Z}$. Ἂν $I = \{0\}$, τότε $I = 0\mathbb{Z}$. Ἂν $I \neq \{0\}$, θεωρῶ $a \in I$, $a \neq 0$. Ἐπειδὴ τὸ I εἶναι δακτύλιος, θὰ εἶναι καὶ $-a \in I$,

Άρα το I περιέχει θετικά στοιχεία, οπότε μπορούμε να θεωρήσουμε το ελάχιστο θετικό στοιχείο του I, έστω n. Αφού $n \in I$, θα είναι και $n\mathbb{Z} \subseteq I$. Ισχύει όμως και το αντίστροφο: Έστω $m \in I$. Από την ταυτότητα της διαίρεσης, $m = n\cdot q + r$ και $0 \le r < n$, άρα $r = m - q\cdot n \in I$ (διότι $m \in I$ 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: $I = n\mathbb{Z}$, δηλ. Κ.Δ.

δ) Παράδειγμα μη κυρίου ιδεώδους: Έστω ο δακτύλιος

$$R = \{ x + y\sqrt{-5} \,:\, x, y \in \mathbb{Z} \}$$ (βλ. παράδειγμα δ, §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, παραπάνω). Το I δεν είναι κύριο. Πράγματι, ας δοκιμάσουμε το αντίθετο θέτοντας $I = R\cdot(A + B\sqrt{-5})$ $(A, B \in \mathbb{Z})$.

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

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

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

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

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

Και' ανάγκη, 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 άτοπο διότι $1\in R$ 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 ακεραίους a,b,c,d. Τότε

$2a+c-5d=1$ και $2b+c+d=0$. Λύνοντας την δεύτερη ως προς d και αντικαθιστώντας στην πρώτη, βρίσκω $2a+10b+6c=1$, άτοπο, αφού το αριστερό μέλος είναι άρτιος ακέραιος.

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 ομάδα-πηλίκο R/I, της οποίας η πράξη, όπως είναι γνωστό, συμβολίζεται με $+$ και ορίζεται: $(r_1+I)+(r_2+I)=(r_1+r_2)+I$, όπου η πράξη του R/I και η πράξη του R.

Μπορούμε να εφοδιάσουμε, επιπλέον φυσικά, το R/I με έναν πολλαπλασιασμό ως εξής:

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

όπου η πράξη του R/I και η πράξη του R.

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

Ο δακτύλιος-πηλίκο που ορίσθηκε έχει ως στοιχεία αριστερές κλάσεις· αυτό δεν είναι ουσιώδες, αφού $r+I = I+r$ $\forall r \in R$ (ή ομάδα $(R,+)$ είναι αβελιανή). Συνεπώς, θα μπορούσε κανείς, αδιακρίτως, να κάνει χρήση αριστερών είτε δεξιών κλάσεων.

Παρατηρήστε ότι, ενώ οι ιδιότητες της ύπαρξης μονάδας και της αντιμεταθετικότητας μεταφέρονται από τον R στον R/I, η ιδιότης της μη υπάρξεως μηδενοδιαιρετών δεν μεταφέρεται από τον R στον R/I. (βλ. παράδειγμα (α) παρακάτω). Συνεπώς, άν 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 $\pi : R \longrightarrow R/I$, $\pi(r) = r+I$ είναι ομομορφισμός δακτυλίων με $\ker \pi = I$.

Η απόδειξη αφήνεται ως απλή άσκηση.

Θεμελιώδες Θεώρημα ομομορφισμού δακτυλίων.
Έστω $\phi : R \longrightarrow S$ ομομορφισμός δακτυλίων. Τότε
$$\mathrm{Im}\,\phi \cong R/\ker\phi$$

Απόδειξη. Η πρόταση 1 λέει $\mathrm{Im}\,\phi$ 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
$$\psi : R/I \longrightarrow S', \quad \psi(r+I) = \phi(r)$$
Η ψ είναι ο ζητούμενος ισομορφισμός. Πράγματι, πρώτ' 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 $\phi(r_1)=\phi(r_2)$.

ἔτσι, $\psi(r_1+I)=\psi(r_2+I)$. Ἡ ψ εἶναι ἀμφιμονοσήμαντη διότι, ἔστω $\psi(r_1+I)=\psi(r_2+I)$. Τότε $\phi(r_1)=\phi(r_2)$, $\phi(r_1-r_2)=0$, ἄρα $r_1-r_2\in\operatorname{Ker}\phi=I$ καὶ αὐτὸ σημαίνει ὅτι $r_1+I=r_2+I$. Ἡ ψ εἶναι "ἐπί" προφανῶς, διότι κάθε $s\in S'$ εἶναι τῆς μορφῆς $\phi(r)$ (ἀφοῦ $S'=\operatorname{Im}\phi$), ἄρα $s=\phi(r)=\psi(r+I)$. Τέλος, ἡ ψ εἶναι ὁμομορφισμός, διότι

$$\psi[(r_1+I)+(r_2+I)]=\psi[(r_1+r_2)+I]=\phi(r_1+r_2)=\phi(r_1)+\phi(r_2)$$
$$=\psi(r_1+I)+\psi(r_2+I).$$

ὅ.ἐ.δ.

Παραδείγματα II

α) Θεωρῶ τὸν ἐπιμορφισμὸ $\phi:\mathbb{Z}\longrightarrow\mathbb{Z}_n$ τοῦ παραδείγματος I, α, ὁ ὁποῖος, ὅπως εἴδαμε, ἔχει πυρήνα $n\mathbb{Z}$. Συνεπῶς, ἀπ' τὸ Θεώρημα, $\mathbb{Z}_n\cong\mathbb{Z}/n\mathbb{Z}$. Ἂν ὁ n εἶναι σύνθετος, ὁ $\mathbb{Z}_n$ ἔχει μηδενοδιαιρέτες ($n=n_1n_2$ μὲ $1\in n_1,n_2<n\Rightarrow$ $\Rightarrow\hat{n}_1\cdot\hat{n}_2=\hat{n}=\hat{0}$), ἄρα καὶ ὁ $\mathbb{Z}/n\mathbb{Z}$ ἔχει μηδενοδιαιρέτες, παρὰ τὸ γεγονὸς ὅτι ὁ $\mathbb{Z}$ δὲν ἔχει.

β) Θεωρῶ τοὺς ἐπιμορφισμοὺς τοῦ παραδείγματος β, §2. Γιὰ τὸν ἐπιμορφισμὸ $\pi_1:R\times S\longrightarrow R$ εἶναι προφανὲς ὅτι $\operatorname{Ker}\pi_1=\{(0,s):s\in S\}$. Λόγῳ τοῦ θεωρήματος, $R\cong\frac{R\times S}{\operatorname{Ker}\pi_1}$. Ἀφ' ἑτέρου εἶναι εὔκολο νὰ 'δεῖ κανεὶς ὅτι ὁ $\operatorname{Ker}\pi_1$ εἶναι ὑποδακτύλιος τοῦ $R\times S$ καὶ, μάλιστα, ἰσόμορφος τοῦ S. Ἄρα $\frac{R\times S}{\operatorname{Ker}\pi_1}\cong\frac{R\times S}{S}$, ὅποτε, σύμφωνα καὶ μὲ τὴν παραπάνω σχέση ἰσομορφίας, $R\cong\frac{R\times S}{S}$ (σχέση ποὺ θυμίζει ἁπλοποίηση μὲ ἀριθμούς!)

Σὲ ἀντιμεταθετικοὺς δακτυλίους μὲ μονάδα, οἱ ἔννοιες τοῦ πρώτου καὶ τοῦ maximal ἰδεώδους εἶναι πολὺ χρήσιμες (κυρίως λόγῳ τῆς πρότασης 3 παρακάτω). Ἕνα

ἰδεώδες I τοῦ δακτυλίου R λέγεται <u>πρῶτο</u> ἂν $I \neq R$ καὶ τὸ I ἔχει τὴν ἰδιότητα: ἂν $a,b \in R$ καὶ $ab \in I$ τότε $a \in I$ εἴτε $b \in I$. Παρατηρῆστε ὅτι τὸ $\{0\}$ εἶναι πρῶτο ἰδεώδες ἂν καὶ μόνο ἂν ὁ R εἶναι ἀκέραια περιοχή.

Τὸ ἰδεώδες I τοῦ R λέγεται <u>maximal</u> ἂν $I \neq R$ καὶ δὲν ὑπάρχει ἰδεώδες J τοῦ R μὲ $I \subsetneq J \subsetneq R$. Μ' ἄλλα λόγια, ἡ χαρακτηριστικὴ ἰδιότητα τοῦ maximal ἰδεώδους εἶναι ἡ ἑξῆς: ἂν τὸ I εἶναι maximal καὶ J εἶναι ἕνα ἰδεώδες τοῦ R, τέτοια ὥστε $I \subseteq J \subseteq R$, τότε ἢ $J = I$ ἢ $J = R$. Παρατηρῆστε ὅτι, τὸ $\{0\}$ εἶναι maximal ἂν καὶ μόνο ἂν ὁ R εἶναι σῶμα. Πράγματι, ἂν ὁ R εἶναι σῶμα, τότε κάθε ἰδεώδες $J \neq \{0\}$ περιέχει στοιχεῖο $r \neq 0$. Ἐπειδὴ ὑπάρχει τὸ $r^{-1} \in R$, θὰ πρέπει $r^{-1} \cdot r \in J$, δηλ. $1 \in J$. Τότε ὅμως, γιὰ κάθε $a \in R$ θὰ εἶναι $a \cdot 1 \in J$, ἄρα $R \subseteq J$, δηλ. $R = J$, ὁπότε ἀποκλείεται μιὰ σχέση $\{0\} \subsetneq J \subsetneq R$. ἄρα τὸ $\{0\}$ εἶναι maximal. Ἀντιστρόφως, ἂν τὸ R δὲν εἶναι σῶμα, θὰ ὑπάρχει $r \in R$, $r \neq 0$, μὴ ἀντιστρέψιμο. Αὐτὸ συνεπάγεται ὅτι τὸ ἰδεώδες $R \cdot r$ εἶναι $\neq R$ (π.χ. $1 \notin R \cdot r$), ἄρα $\{0\} \subsetneq R \cdot r \subsetneq R$, δηλ. τὸ $\{0\}$ δὲν εἶναι maximal.

<u>Πρόταση 3.</u> Ἔστω R ἀντιμεταθετικὸς δακτύλιος μὲ μονάδα ($1 \neq 0$) καὶ I ἰδεώδες τοῦ R. (α) Τὸ I εἶναι πρῶτο ἰδεώδες ἂν καὶ μόνο ἂν ὁ δακτύλιος R/I εἶναι ἀκέραια περιοχή. (β) Τὸ I εἶναι maximal ἰδεώδες ἂν καὶ μόνο ἂν ὁ δακτύλιος R/I εἶναι σῶμα. (γ) Ἂν τὸ I εἶναι maximal, τότε εἶναι καὶ πρῶτο.

<u>Ἀπόδειξη.</u> (α) Ἔστω ὅτι τὸ I εἶναι πρῶτο ἰδεώδες. Ἔχω νὰ δείξω ὅτι, ἂν $a+I, b+I \in R/I$ καὶ δὲν εἶναι μηδενικά,

$(\delta\eta\lambda.\ a+I,\ b+I \neq 0+I = I)$ τότε $(a+I)(b+I) \neq I$.
Πράγματι, $(a+I)(b+I) = ab + I$. Άν 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 μηδενοδιαιρέτες. Μένει απόμη κάτι σχολαστικό! Να δείξω ότι $0+I \neq 1+I$. Πράγματι, άν είχα ίσότητα, $1 \in I$, οπότε $R = I$, κάτι που αντίκειται στον ορισμό του πρώτου ιδεώδους.
Αντιστρόφως, έστω R/I ακέραια περιοχή. Τότε $0+I \neq 1+I$, άρα $1 \notin I$, άρα $I \neq R$. Επίσης, άν $a, b \in R$ και $a \cdot b \in I$, 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), βλέπομε 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 $J \overset{\text{ορ}}{=} I + aR \overset{\text{ορ}}{=} \{ \iota + a \cdot r : \iota \in I \text{ και } r \in R \}$ περιέχει γνησίως το I συνεπώς $J = R$ (αφού το I είναι maximal). Άρα $1 \in J$, που σημαίνει ότι υπάρχουν $\iota \in I$ και $r \in R$ τ.ώ. $1 = \iota + a \cdot r$. Τότε $(a+I)(r+I) = ar + I = 1 - \iota + I = 1 + I$ (μονάδα του R/I), άρα $r + I = (a+I)^{-1}$.
Αντιστρόφως, άν το R/I είναι σώμα τότε, όπως στο (α), $I \neq R$. Μένει να δείξω ότι άν 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 $\iota \in I$ τ.ώ. $1 = ab + \iota$. Όμως $a \in J$ και $\iota \in I \subseteq J$, άρα $1 \in J$, που συνεπάγεται $J = R$.

(γ) Ἂν τό I εἶναι maximal ἰδεώδες τοῦ R τότε, λόγῳ τοῦ (β), ὁ δακτύλιος R/I εἶναι σῶμα· εἰδικώτερα, εἶναι ἀκέραια περιοχή ἄρα, λόγῳ τοῦ (α) τό I εἶναι πρῶτο ἰδεώδες τοῦ R.
ὅ.ἐ.δ.

Τονίζω ἐδῶ ὅτι τό ἀντίστροφο τοῦ (γ) δέν ἰσχύει. Δηλαδή, ὑπάρχουν πρῶτα ἰδεώδη σέ κάποιο δακτύλιο, τά ὁποῖα δέν εἶναι maximal. Ἕνα τέτοιο παράδειγμα θά δοθεῖ ἀργότερα.

4. Πολυώνυμα.

Ἔστω R ἀντιμεταθετικός δακτύλιος. Κάθε τυπικό ἄθροισμα τῆς μορφῆς $a_n t^n + a_{n-1} t^{n-1} + \cdots + a_1 t + a_0$, ὅπου $a_0, a_1, \ldots, a_n \in R$, $n \geq 0$ (γιά $n=0$, $a_n t^n$ σημαίνει a_0) λέγεται <u>πολυώνυμο μέ συντελεστές ἀπ' τόν R</u>. "Τυπικό ἄθροισμα" σημαίνει ὅτι τό γράμμα t (πού ὀνομάζεται <u>μεταβλητή</u> καί θά μποροῦσε, ἐπίσης νά συμβολιστεῖ καί μέ ἄλλο γράμμα) δέν ἔχει κάποια σημασία (εἰδικώτερα, τό t δέν εἶναι στοιχεῖο τοῦ R) καί, ἀκόμη, ὅτι γράφοντας π.χ. $a_k t^k$ δέν ἐννοοῦμε κάποιο πολλαπλασιασμό, οὔτε τά $+$, πού ἐμφανίζονται στό πολυώνυμο, ὑποδηλώνουν κάποια πρόσθεση.
Κάνουμε τήν ἑξῆς σύμβαση: Τά πολυώνυμα $a_n t^n + \cdots + a_1 t + a_0$ καί $0 t^{n+k} + \cdots + 0 t^{n+1} + a_n t^n + \cdots + a_1 t + a_0$ θεωροῦνται ἴσα γιά ὁποιονδήποτε φυσικό ἀριθμό k.
Συνήθως, φροντίζουμε ὅταν γράφουμε ἕνα πολυώνυμο, π.χ. $a_n t^n + \cdots + a_1 t + a_0$, νά ὑποθέτουμε $a_n \neq 0$. Στήν περίπτωση αὐτή τό $a_n t^n$ λέγεται <u>μεγιστοβάθμιος ὅρος τοῦ πολυωνύμου</u>.

καὶ ὁ n <u>βαθμὸς τοῦ πολυωνύμου</u>. (*) Τὸ σύνολο τῶν πολυωνύμων μὲ συντελεστὲς ἀπ' τὸν R συμβολίζεται $R[t]$ καὶ τὰ στοιχεῖα τοῦ $R[t]$ (δηλ. τὰ πολυώνυμα) συμβολίζονται συνήθως $f(t)$, $g(t)$, $h(t)$ κ.λ.π. Ὁ βαθμὸς τοῦ πολυωνύμου $f(t) \in R[t]$ συμβολίζεται μὲ $\deg f$.

<u>Ἰσότητα μεταξὺ δύο πολυωνύμων</u> $f(t), g(t) \in R[t]$:
Τὰ $f(t)$ καὶ $g(t)$ εἶναι ἴσα ($f(t)=g(t)$), ἐξ ὁρισμοῦ, ἂν
i) $\deg f = \deg g = (\text{ἔστω}) \, n$, καὶ
ii) ἂν $f(t) = a_n t^n + \cdots + a_1 t + a_0$, $g(t) = b_n t^n + \cdots + b_1 t + b_0$ τότε $b_0 = a_0$, $b_1 = a_1$, ..., $b_n = a_n$.

Ἰσοδύναμα, ὁ ὁρισμὸς τῆς ἰσότητας τῶν $f(t), g(t) \in R[t]$ μπορεῖ νὰ διατυπωθεῖ καὶ ὡς ἑξῆς ; ἀποφεύγοντας νὰ κάνομε λόγια στοὺς βαθμούς : Ἔστω $f(t) = a_n t^n + \cdots + a_1 t + a_0$, $g(t) = b_m t^m + \cdots + b_1 t + b_0$ (δὲν ὑποθέτω ὅτι $a_n \neq 0$ ἢ $b_m \neq 0$) καὶ ἂς ὑποθέσομε δίχως βλάβη τῆς γενικότητος $n \geq m$. Τότε, $f(t) = g(t)$ ἂν καὶ μόνο ἂν $b_0 = a_0, b_1 = a_1, \ldots, b_m = a_m$ καὶ $a_{m+1} = \cdots = a_n = 0$.

Εἰδικώτερα, τὸ πολυώνυμο $f(t)$ εἶναι τὸ <u>μηδενικὸ πολυώνυμο</u> (συμβολικά, $f(t) = 0$ καὶ, σπανιώτερα, $f(t) = 0(t)$ ἂν θέλομε ν' ἀντιδιαστείλομε τὸ μηδενικὸ πολυώνυμο ἀπ' τὸ $0 \in R$), ἂν καὶ μόνο ἂν $a_0 = a_1 = \cdots = a_n = 0$.

Ὁρίζω $\deg 0 = -\infty$. Κάθε πολυώνυμο τῆς μορφῆς a_0 (ἢ, ἰσοδύναμα, τῆς μορφῆς $0 \cdot t^n + 0 \cdot t^{n-1} + \cdots + 0 \cdot t + a_0$) λέγεται <u>σταθερὸ πολυώνυμο</u>. Τὰ σταθερά, μὴ μηδενικά, πολυώνυμα ἔχουν βαθμὸ 0. Συνεπῶς, τὸ νὰ γράψω κανεὶς $\deg f = 0$, ἰσοδυναμεῖ μὲ τὸ ὅτι τὸ $f(t)$ εἶναι σταθερό, μὴ μηδενικό, πολυώνυμο, ἐνῶ γράφοντας $\deg f = -\infty$ ἐννοεῖ ὅτι τὸ $f(t)$ εἶναι μηδενικό.

(*) ἐκτὸς ἂν $n=0$ καὶ $a_0 = 0$ (μηδενικὸ πολυώνυμο · βλ. παρακάτω).

Στό σύνολο $R[t]$ ὁρίζομε πρόσθεση καί πολ/σιασμό ὡς ἑξῆς: Ἔστω $f(t), g(t) \in R[t]$. Προκειμένου νά ὁρίσω $f(t)+g(t)$, θεωρῶ ὅτι τά δύο πολυώνυμα ξεκινοῦν ἀπό ὅρο τοῦ ἴδιου βαθμοῦ (ἄν π.χ. $f(t) = at^2+bt+c$ καί $g(t) = dt+e$, τότε γράφω $g(t) = 0t^2+dt+e$, ἔτσι ὥστε καί τά δύο πολυώνυμα ν' ἀρχίζουν μέ ὅρο βαθμοῦ 2· θά μποροῦσα, ἐπίσης, νά' ἔγραφα $f(t) = 0t^3+at^2+bt+c$ καί $g(t) = 0t^3+0t^2+dt+e$). Ἔστω, λοιπόν, $f(t) = a_n t^n + \cdots + a_1 t + a_0$, $g(t) = b_n t^n + \cdots + b_1 t + b_0$. Τότε, $f(t)+g(t) \overset{\text{ορσ}}{=} (a_n+b_n)t^n + \cdots + (a_1+b_1)t + (a_0+b_0)$.

Προκειμένου νά' ὁρίσω $f(t)\cdot g(t)$, δέν εἶναι ἀνάγκη νά γράψω τά $f(t), g(t)$ ἔτσι ὥστε ν' ἀρχίζουν ἀπό ὅρο τοῦ ἴδιου βαθμοῦ. Ἔστω $f(t) = a_n t^n + \cdots + a_1 t + a_0$, $g(t) = b_m t^m + \cdots + b_1 t + b_0$. Τότε

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

ὅπου, γιά $k = 0, 1, \ldots, m+n$ εἶναι $c_k = \sum_{\substack{i+j=k \\ 1\le i\le n,\ 1\le j\le m}} a_i b_j$.

Εἶναι ἁπλό ν' ἀποδείξει κανείς ὅτι τό $R[t]$, ἐφοδιασμένο μέ τίς παραπάνω πράξεις $+,\cdot$ γίνεται δακτύλιος (κάποια μικρή δυσκολία παρουσιάζει ἡ προσεταιριστικότης τοῦ πολ/σιασμοῦ). Ὁ δακτύλιος $R[t]$ εἶναι, προφανῶς, ἀντιμεταθετικός, ἀφοῦ ὁ R ἔχει ὑποτεθεῖ ἀντιμεταθετικός. Ἐπιπλέον, ἄν ὁ R ἔχει μονάδα, ἔστω 1, τότε τό σταθερό πολυώνυμο 1 εἶναι μονάδα τοῦ $R[t]$. Στήν περίπτωση πού ὁ R ἔχει μονάδα, ὅροι τῆς μορφῆς $1t^k, -1t^k$ $(k\ge 1)$ γράφονται ἁπλῶς $t^k, -t^k$, ἀντιστοίχως. Ἕνα πολυώνυμο, τοῦ ὁποίου ὁ μεγιστοβάθμιος ὅρος εἶναι τῆς μορφῆς t^n λέγεται <u>μονικό</u>.

Δύο βασικές παρατηρήσεις: (α) Η απεικόνιση $j: R \to R[t]$, $j(a) = a \in R[t]$, δηλ. η απεικόνιση που σε κάθε $a \in R$ αντιστοιχεί το σταθερό πολυώνυμο $a \in R[t]$, είναι μονομορφισμός δακτυλίων. Γενικά, κάθε μονομορφισμός δακτυλίων $j: R \to S$ λέμε ότι εμφυτεύει το δακτύλιο R μέσα στον S και, κατά την συνήθη ταχτική στα νεώτερα 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 περίπτωσή μας· από 'δω και στο εξής, ο δακτύλιος R θα θεωρείται ως υποδακτύλιος του $R[t]$.

(β) Σε κάθε $f(t) \in R[t]$ αντιστοιχεί κατά προφανή τρόπο μιά συνάρτηση $R \longrightarrow R$, την οποία συμβολίζομε με το ίδιο γράμμα f. Η συνάρτηση $f: R \longrightarrow R$ ορίζεται ως εξής: Αν $f(t) = a_n t^n + \cdots + a_1 t + a_0$, τότε,

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

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

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 $\mathcal{F}(R,R)$,

ἂν ἐφοδιαστεῖ μὲ τὶς προφανεῖς πράξεις (γιὰ $\phi, \psi \in \mathcal{F}(R,R)$, $(\phi+\psi)(r) \stackrel{\text{def}}{=} \phi(r)+\psi(r)$, $(\phi\cdot\psi)(r) = \phi(r)\cdot\psi(r)$) γίνεται δακτύλιος (σύμφωνα μὲ τὸ παράδειγμα ε τῆς § 1), ὑποδακτύλιος τοῦ ὁποίου εἶναι τὸ σύνολο τῶν πολυωνυμικῶν συναρτήσεων. Ἡ ἀπεικόνιση, ποὺ προαναφέραμε, ἔστω ν

$$R[t] \ni f(t) \longmapsto f \in \mathcal{F}(R;R)$$

εἶναι, προφανῶς, ὁμομορφισμὸς δακτυλίων(*) ἀλλά, ὅπως εἴδαμε πρίν, δὲν εἶναι ἀμφιμονοσήμαντη (ἄρα δὲν εἶναι μονομορφισμός).

Πρόταση 1. Ἂν ὁ δακτύλιος R δὲν ἔχει μηδενοδιαιρέτες καὶ $f(t), g(t) \in R[t]$, τότε $\deg(f\cdot g) = \deg f + \deg g$ (ἐννοεῖται ὅτι $-\infty +$ ὁποιοδήποτε βαθμὸ $= -\infty$).

Ἀπόδειξη. Προφανὴς ἂν ἕνα ἀπ' τὰ $f(t), g(t)$ εἶναι μηδενικὸ πολυώνυμο. Ἔστω τώρα $f(t) = a_n t^n + \cdots$, $g(t) = b_m t^m + \cdots$, ὅπου $a_n \neq 0$, $b_m \neq 0$ καὶ $m, n \geq 1$. Τότε, ἐξ ὁρισμοῦ τοῦ $f(t)\cdot g(t)$, εἶναι $f(t)\cdot g(t) = a_n b_m t^{m+n} +$ ὅροι βαθμοῦ $< m+n$. Ἐπειδὴ ὁ R δὲν ἔχει μηδενοδιαιρέτες, εἶναι $a_n b_m \neq 0$, ἄρα $\deg(f\cdot g) = m+n$.

Σημείωση. Ἀπ' τὴν παραπάνω ἀπόδειξη γίνεται φανερὸ ὅτι, ἐν γένει, $\deg(f\cdot g) \leq \deg f + \deg g$.

Τὸ ἑπόμενο θεώρημα εἶναι θεμελιώδες γιὰ τὰ πολυώνυμα:

(*) Στὸ σημεῖο αὐτό, προκειμένου ν' ἀποδειχθεῖ ὅτι $\nu(f(t)\cdot g(t)) = \nu(f(t))\cdot\nu(g(t))$, γίνεται γιὰ πρώτη φορὰ οὐσιαστικὴ χρήση τῆς ἀντιμεταθετικότητας τοῦ R.

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

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

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 $\deg f \geq \deg g$. Ειδικώτερα, $f(t)\neq 0$.
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 $f(t)=a_0$, $g(t)=b_0$ όπότε 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 εξασφαλισθεί για όλα τα πολυώνυμα $f(t)$ με $\deg f = n < k$ (εξακολουθεί η υπόθεση $n \geq m$).
Υποθέτω τώρα ότι $n=k$. Τότε θεωρώ το πολυώνυμο

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

Συνεπώς για το πολυώνυμο αυτό ισχύει η επαγωγική υπόθεση, άρα υπάρχουν $q_1(t)$, $r(t) \in D[t]$ με $\deg r < \deg g$ και

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

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

$$g(t)\cdot(q(t) - q_1(t)) = r_1(t) - r(t). \tag{2}$$

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 $< \deg g$ ᾽άτοπο. Συνεπώς $q_1(t)=q(t)$ και κατ', απ' τη (2), $r_1(t)=r(t)$ (εδώ γίνεται χρήση του ότι στο $D[t]$ δεν υπάρχουν μηδενοδιαιρέτες ᾽άμεση συνέπεια της πρότασης 1.), ὅ.ἐ.δ.

Ορισμός α) Έστω D ακέραια περιοχή και $f(t), g(t)\in D[t]$ με $g(t)\neq 0$. Λέμε ότι το $g(t)$ διαιρεῖ (στο $D[t]$) το $f(t)$, ἢ ότι το $f(t)$ διαιρεῖται (ἢ είναι διαιρετό) ἀπ' το $g(t)$ (στο $D[t]$), ἢ ότι το $g(t)$ είναι διαιρέτης του $f(t)$ (*), συμβολικά $g(t)\mid f(t)$, ἂν υπάρχει $q(t)\in D[t]$, ἔτσι ὥστε $f(t)=g(t)\cdot q(t)$.
β) Έστω K σῶμα ἢ $f(t)\in K[t]$. Το $\rho\in K$ λέγεται ρίζα του $f(t)$ ἂν $f(\rho)=0$.

Άμεση συνέπεια του Θεωρήματος 1 είναι ἡ επόμενη πρόταση:

Πρόταση 2. Έστω K σῶμα, $\rho\in K$ και $f(t)\in K[t]$. Το ρ είναι ρίζα του $f(t)$ ἂν και μόνο ἂν $t-\rho \mid f(t)$.

Απόδειξη. Γράψτε τη σχέση (1) του Θεωρήματος 1, στην περίπτωση που $g(t)=t-\rho$, ὅ.ἐ.δ.

Αν λοιπόν το $\rho\in K$ είναι ρίζα του $f(t)\in K[t]$, τότε το σύνολο $\{\nu\in\mathbb{Z}_{>0} : (t-\rho)^\nu \mid f(t)\}$ είναι μη κενό (αφοῦ το 1 ανήκει σ' αὐτό). Αφ' ἑτέρου, είναι πεπερασμένο, αφοῦ στη σχέση $(t-\rho)^\nu \mid f(t)$ το ν δεν μπορεῖ να είναι ὁσοδήποτε μεγάλο (θεωρῆστε τους βαθμούς στη σχέση $f(t)=(t-\rho)^\nu\cdot q(t)$).
Το μέγιστο στοιχεῖο αὐτοῦ του συνόλου λέγεται πολλαπλότητα

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

της ρίζας ρ του $f(t)$. Έχομε, λοιπόν, τον έξης, προφανώς ισοδύναμο, ορισμό:

Ορισμός. Έστω Κ σώμα, $f(t) \in K[t]$ και $\rho \in K$ ρίζα του $f(t)$. Ο ακέραιος $\nu \geq 1$ για τον οποίο ισχύει $(t-\rho)^\nu \mid f(t)$ $\not\mid (t-\rho)^{\nu+1} \dagger f(t)$ ($\dagger$ σημαίνει "δεν διαιρεί") λέγεται πολλαπλότητα της ρίζας ρ του $f(t)$.

Ορισμός Έστω D ακέραια περιοχή. Το μη σταθερό πολυώνυμο $f(t) \in D[t]$ λέγεται αναγωγο στο $D[t]$ (ή αναγωγο πάνω απ' το D) αν δεν υπάρχει πολυώνυμο $g(t) \in D[t]$ με $0 < \deg g < \deg f$ ώ $g(t) \mid f(t)$.

Παρατηρήσεις

α) Άμεσες συνέπειες του ορισμού: α) Τα πολυώνυμα πρώτου βαθμού, είναι αναγωγα. Για $f(t) \in K[t]$, Κ σώμα, με $\deg f = 2, 3$, το να πούμε ότι το $f(t)$ είναι αναγωγο στο $K[t]$ ισοδυναμεί με το να πούμε ότι κανένα στοιχείο του Κ είναι ρίζα του $f(t)$.

β) Ένα πολυώνυμο με συντελεστές από μια ακέραια περιοχή μπορεί να είναι αναγωγο, αλλά, το ίδιο θεωρούμενο ως πολυώνυμο μιας μεγαλύτερης ακέραιας περιοχής, μπορεί να μην εξακολουθεί να είναι αναγωγο. Απλά παραδείγματα: Το t^2-2 είναι αναγωγο αν θεωρηθεί ως πολυώνυμο του $\mathbb{Q}[t]$, δεν είναι όμως αναγωγο αν θεωρηθεί ως στοιχείο του $\mathbb{R}[t]$. Ανάλογα για το t^2+1 αν το δούμε στο $\mathbb{R}[t]$ ή στο $\mathbb{C}[t]$.

Πρόταση 3. Έστω D ακέραια περιοχή. Κάθε μη σταθερό

πολυωνύμο τοῦ $D[t]$ ἔχει ἕνα, τοὐλάχιστον, ἀνάγωγο διαιρέτη.

Ἀπόδειξη. Μό ἐπαγωγή πάνω στό βαθμό τοῦ θεωρουμένου πολυωνύμου (ἁπλῆ ἄσκηση).

Ὁρισμός. Ἔστω K σῶμα καί $f(t), g(t) \in K[t]$, ὄχι καί τά δύο μηδενικά. Ἕνα πολυώνυμο $d(t) \in K[t]$ θά λέγεται κοινός διαιρέτης τῶν $f(t)$ καί $g(t)$ ἄν $d(t) \mid f(t)$ καί $d(t) \mid g(t)$ (στό $K[t]$). Ὁ κοινός διαιρέτης $d(t)$ τῶν $f(t)$ καί $g(t)$ θά χαρακτηρίζεται μέγιστος ἄν ἔχει τήν ἐπιπλέον ἰδιότητα νά διαιρεῖται (στό $K[t]$) ἀπό κάθε ἄλλο κοινό διαιρέτη τῶν $f(t)$ καί $g(t)$. Ὁ ὁρισμός αὐτός γενικεύεται κατά προφανῆ τρόπο καί γιά περισσότερα ἀπό δύο πολυώνυμα. Πρέπει νά δείξουμε ὅμως ὅτι ἡ ἔννοια τοῦ μεγίστου κοινοῦ διαιρέτη (δύο ἤ περισσοτέρων πολυωνύμων) δέν εἶναι κενή περιεχομένου. Αὐτό ἐπιτυγχάνεται στήν ἑπόμενη πρόταση.

Πρόταση 4. Ἔστω K σῶμα. (α) Κάθε ἰδεώδες τοῦ $K[t]$ εἶναι κύριο (βλ. §3).
(β) Ἄν $f_1(t), \ldots, f_n(t) \in K[t]$, ὄχι ὅλα μηδενικά, καί $I = \langle f_1(t), \ldots, f_n(t) \rangle$ τό ἰδεώδες τοῦ $K[t]$, πού παράγεται ἀπ' αὐτά τά πολυώνυμα (βλ. §3, παράδειγμα I(β)) τότε, κάθε πολυώνυμο $d(t) \in K[t]$, πού παράγει (μόνο του) τό I (τέτοιο πολυώνυμο $d(t)$ ὑπάρχει, λόγῳ τοῦ (α)) εἶναι μέγιστος κοινός διαιρέτης τῶν $f_1(t), \ldots, f_n(t)$.

Ἀπόδειξη. α) Δές στό παράδειγμα I(γ), §3, πῶς ἀποδείχθηκε ὅτι κάθε ἰδεώδες τοῦ $\mathbb{Z}$ εἶναι κύριο καί μετάφερε ἐκείνη τήν

απόδειξη στην περίπτωση του $K[t]$· η 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,

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

Συνεπώς, κάθε $f_i(t)$ ανήκει στο I (βάλε $g_i(t) = 1$ και όλα τα υπόλοιπα $g_j(t) = 0$), άρα είναι πολ/σιο του $d(t)$. Δηλαδή, το $d(t)$ είναι κοινός διαιρέτης των $f_1(t), \ldots, f_n(t)$. Έστω τώρα $\delta(t) \in K[t]$ τυχών κοινός διαιρέτης των $f_1(t), \ldots, f_n(t)$. Επειδή $d(t) \in I$, θα υπάρχουν $g_1(t), \ldots, g_n(t) \in K[t]$, τέτοια ώστε $d(t) = g_1(t) \cdot f_1(t) + \cdots + g_n(t) \cdot f_n(t)$. Όμως το $\delta(t)$ διαιρεί όλα τα $f_1(t), \ldots, f_n(t)$, άρα και το δεξιό μέλος της τελευταίας ισότητας, όπότε $\delta(t) \mid d(t)$, δ.ε.δ.

<u>Πρόταση 5 – Ορισμός</u>. Έστω K σώμα και $f_1(t), \ldots, f_n(t) \in K[t]$ ($n \geq 2$) όχι όλα μηδενικά. Δύο οποιοιδήποτε μέγιστοι κοινοί διαιρέτες των $f_1(t), \ldots, f_n(t)$ διαφέρουν κατά (μη μηδενική) πολλαπλασιαστική σταθερά. Συνεπώς, υπάρχει ένας, ακριβώς, μέγιστος κοινός διαιρέτης των $f_1(t), \ldots, f_n(t)$, ο οποίος είναι μονικό πολυώνυμο· αυτός χαρακτηρίζεται ως <u>ο μέγιστος κοινός διαιρέτης των $f_1(t), \ldots, f_n(t)$</u>. Αν αυτός ισούται με το σταθερό πολυώνυμο 1, τότε τα $f_1(t), \ldots, f_n(t)$ λέγονται <u>πρώτα μεταξύ τους</u>. Ισοδύναμα, τα $f_1(t), \ldots, f_n(t)$ είναι πρώτα μεταξύ τους αν και μόνο αν οι μόνοι κοινοί διαιρέτες τους είναι τα σταθερά πολυώνυμα.

<u>Απόδειξη</u>. Μόνο ο πρώτος ισχυρισμός δεν είναι εντελώς προφανής· αυτόν και θ' αποδείξουμε: 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 μεγίστου κοινού διαιρέτη, θα πρέπει $d_2(t)\mid d_1(t)$ και $d_1(t)\mid d_2(t)$. Γράφοντας $d_2(t)=g(t)d_1(t)$ και $d_1(t)=h(t)d_2(t)$ με $g(t),h(t)\in K[t]$, έχομε $d_2(t)=g(t)h(t)d_2(t)$, άρα $1=g(t)\cdot h(t)$, που συνεπάγεται ότι τα $g(t),h(t)$ είναι σταθερά και τα δύο, ό.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 την 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, ή $f(t)\mid g(t)$ 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 $f(t)\mid g(t)\cdot h(t)$, τότε $f(t)\mid g(t)$ είτε $f(t)\mid h(t)$.
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 $f(t)\cdot g(t)\mid h(t)$.
δ) Αν το $f(t)\in K[t]$ είναι πρώτο προς καθένα από 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, εξ ορισμού, ή $d(t)=$σταθερό ή $d(t)=c\cdot f(t)$ με $c\in K-\{0\}$. Η δεύτερη περίπτωση αποκλείεται, αφού θα συνεπαγόταν ότι $c\cdot f(t)\mid g(t)$, άρα και $f(t)\mid g(t)$ (πάτα που αντιβαίνει στην υπόθεση), άρα μένει η πρώτη περίπτωση.
β) Έστω ότι $f(t)\nmid g(t)$. Τότε, από το (α), τα $f(t),g(t)$ είναι πρώτα μεταξύ τους. Άρα, από την πρόταση 4(β), το ζητούμενο

$\langle f(t), g(t)\rangle$ παράγεται απ' το 1, άρα ταυτίζεται με το $K[t]$. Μ' άλλα λόγια, υπάρχουν $f_1(t), g_1(t) \in K[t]$ έτσι ώστε $f_1(t)\cdot f(t) + g_1(t)\cdot g(t) = 1$. Άρα, $h(t)h_1(t)f(t) + g_1(t)g(t)h(t) = h(t)$ και βλέπουμε ότι το $f(t)$ διαιρεί τους προσθετέους του αριστερού μέλους, οπότε το $f(t)$ διαιρεί και το δεξιό μέλος, δηλ. το $h(t)$.

γ) Είναι $h(t) = f(t)\cdot F(t)$ και $h(t) = g(t)\cdot G(t)$ για κάποια πολυώνυμα $F(t), G(t) \in K[t]$. Επειδή τα $f(t), g(t)$ είναι πρώτα μεταξύ τους, θα υπάρχουν $f_1(t), g_1(t) \in K[t]$ έτσι ώστε $f_1(t)\cdot f(t) + g_1(t)\cdot g(t) = 1$ (βλ. απόδειξη του (β)). Άρα, $f_1(t)G(t)\cdot f(t) + g_1(t)\cdot g(t)\cdot G(t) = G(t)$. Αντικαθιστώ στο αριστερό μέλος το $g(t)\cdot G(t)$ απ' το $f(t)\cdot F(t)$, οπότε βλέπω ότι $f(t) \mid G(t)$. Συνεπώς $G(t) = f(t)\cdot H(t)$ και τώρα, $h(t) = g(t)G(t) = g(t)\cdot f(t)\cdot H(t)$, που είναι το αποδεικτέο.

δ) Επειδή τα $f(t), g(t)$ είναι πρώτα μεταξύ τους, υπάρχουν $f_1(t), g_1(t) \in K[t]$, έτσι ώστε $f_1(t)\cdot f(t) + g_1(t)g(t) = 1$. Πολ/σιάζω επί $h(t)$, οπότε $f_1(t)h(t)f(t) + g_1(t)g(t)h(t) = h(t)$. Άρα, αν $d(t)$ είναι κοινός διαιρέτης των $f(t)$ και $g(t)\cdot h(t)$, αυτός θα διαιρεί (λόγω της τελευταίας ισότητας) και το $h(t)$, άρα θα είναι κοινός διαιρέτης των $f(t), h(t)$, οπότε θα διαιρεί τον μέγιστο κοινό διαιρέτη τους, που είναι 1. Συνεπώς $d(t)$ είναι σταθερό, δ.ε.δ.

<u>Γενικεύσεις</u>. Με απλή χρήση επαγωγής, τα (β), (γ) και (δ) της πρότασης 6 γενικεύονται ως εξής:

Γενίκευση του (β): Αν το $f(t)$ είναι ανάγωγο και $f(t) \mid g_1(t)\cdots g_n(t)$, τότε το $f(t)$ διαιρεί ένα τουλάχιστον απ' τα $g_1(t), \ldots, g_n(t)$.

Γενίκευση του (γ): Αν τα $f_1(t), \ldots, f_n(t)$ είναι ανά δύο πρώτα μεταξύ τους και καθένα διαιρεί το $h(t)$, τότε και το γινόμενό τους διαιρεί το $h(t)$.

Γενίκευση του (δ): Αν το $f(t)$ είναι πρώτο προς καθέ $g_i(t)$, $i=1,\ldots,n$, τότε είναι πρώτο και προς το $g_1(t)\ldots g_n(t)$.

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 $f_1(t)\cdot f(t)+g_1(t)g(t)=1$. Αυτό είναι ένα πολύ χρήσιμο αποτέλεσμα (ήδη ξαναχρησιμοποιήθηκε στο (γ)), του οποίου η γενίκευση (με εντελώς ανάλογη απόδειξη) είναι η εξής: 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 $\rho_1,\dots,\rho_m$ ($m\leq\deg f$) είναι αυτά (και μόνο αυτά) τα στοιχεία του K, που είναι ρίζες του $f(t)$, με αντίστοιχες πολλαπλότητες $\nu_1,\dots,\nu_m$, 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 $\rho_1,\dots,\rho_m$ είναι τυχόντα, διαφορετικά στοιχεία του K. Είναι απλή άσκηση να δείξει κανείς ότι τα $t-\rho_1,\dots,t-\rho_m$ είναι πολυώνυμα ανά δύο πρώτα μεταξύ τους. Συνεπώς, αν είναι τα $\rho_1,\dots,\rho_m$ 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 $\rho_1,\dots,\rho_m$ είναι όλες-όλες οι ρίζες του $f(t)$ στο K και $\nu_1,\dots,\nu_m$ 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 γινόμενό τους διαιρεί το $f(t)$,

Θέτω $f(t) = (t-\rho_1)^{\nu_1} \cdots (t-\rho_m)^{\nu_m} g(t)$. Είναι φανερό ότι το $g(t)$ δεν έχει ρίζα στο K· γιατί, αν είχε ρίζα ρ, τότε, ή $\rho = \rho_i$ για κάποιο $i \in \{1,\dots,m\}$, οπότε η πολλαπλότητα του ρ_i θα ήταν $\geq \nu_i + 1$, ή $\rho \neq \rho_i$ $\forall i \in \{1,\dots,m\}$, οπότε το $f(t)$ θα είχε και άλλη ρίζα πλην των $\rho_1,\dots,\rho_m$.
Τέλος, συμπίπτοντας των βαθμών στην τελευταία ισότητα πολυωνύμων έχομε $\deg f = \nu_1 + \cdots + \nu_m + \deg g$, ό.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 αναγώγων πολυωνύμων του $K[t]$. Το "μονότροπα" της ανάλυσης εννοείται υπό τον όρον ότι πολυώνυμα που διαφέρουν κατά πολ/σιαστική σταθερά θεωρούνται, ουσιαστικά, 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 αναγώγων 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 ν' 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 τίποτε ν' 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. Αυτό που έχω ν' απο-

δείξω είναι ότι αν $f = p_1 \cdots p_n$ και $f = q_1 \cdots q_m$, όπου τα $p_1, \ldots, p_n, q_1, \ldots, q_m \in K[t]$ είναι ανάγωγα, όχι σταθερά, τότε $n = m$ και υπάρχει μιά 1-1 αντιστοιχία $\phi : \{p_1, \ldots, p_n\} \longrightarrow \{q_1, \ldots, q_n\}$, τέτοια ώστε το $\phi(p_i)$ να είναι κάπου q_j, που διαφέρει απ' το p_i κατά πολ/σιαστική σταθερά. Πράγματι, έστω $m \geq n$. Επειδή $p_1 \cdots p_n = q_1 \cdots q_m$, το p_1 διαιρεί το δεξιό μέλος, άρα διαιρεί ένα τουλάχιστον απ' τα $q_1, \ldots, q_m$, έστω το q_{j_1}. Επειδή 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 πολ/σιαστική σταθερά, άρα, απλοποιώντας τη σχέση $p_1 \cdots p_n = q_1 \cdots q_m$, με διαίρεση διά p_1, βρίσκω $p_2 \cdots p_n = c_1 \prod_{j \neq j_1} q_j$, $c_1 \in K^*$. Προχωρώντας όμοιως, απλοποιώ διαιρώντας διά p_2 κ.ο.κ. μέχρις ότου φτάσω σε μιά σχέση ⊛

$$1 = c_1 \cdots c_n \prod_{j \neq j_1, \ldots, j_m} q_j \quad , \quad c_1, \ldots, c_n \in K^*$$

Αυτή η σχέση είναι αδύνατη, εκτός αν δεν υπάρχουν q_j με $j \neq j_1, \ldots, j_m$, 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.ο.κ. μας δίνει και την 1-1 αντιστοιχία ϕ για την οποία είχε λόγος παραπάνω, ό.ε.δ.

Άμεση συνέπεια του Θεωρήματος 2 είναι το εξής σημαντικό:

⊛ Στην παραπάνω σχέση τα $j_1, \ldots, j_m$ είναι διαφορετικοί δείκτες.

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

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

όπου τα $p_1(t), \ldots, p_m(t)$ είναι ανά δύο πρώτα μεταξύ τους. Το πλήθος m είναι μονότροπα ορισμένο απ' το $f(t)$ · τα ανάγωγα πολυωνυμα $p_1(t), \ldots, p_m(t)$ είναι μονότροπα, μέχρι πολλαπλασιασμού επί (μη μηδενική) σταθερά, καθορισμένα.

Ορισμός. 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 - Ευκλείδιες περιοχές.

Σε όλη την §5 το D θα συμβολίζει άκεραια περιοχή $\neq D^* = D - \{0\}$.

Ορισμός 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 οριστικό άρθρο "η" ξεχωρίζει την μονάδα από τις υπόλοιπες (αν υπάρχουν · βλ. στα παραδείγματα, παρακάτω) μονάδες.

β) Δυό 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 διαιρεί το α ή, ισοδύναμα, το α διαιρείται (ή είναι διαιρετό) απ' το β, ή, το β είναι διαιρέτης του α, ή, το α είναι πολλαπλάσιο του β

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

δ) Ο διαιρέτης β του α χαρακτηρίζεται <u>γνήσιος</u> αν ούτε μονάδα είναι, ούτε συνεταιρικό στοιχείο του α. Οι μονάδες και τα συνεταιρικά στοιχεία του α, χαρακτηρίζονται <u>τετριμμένοι διαιρέτες</u> του α.

ε) Το $p \in D^*$ λέγεται <u>ανάγωγο</u>, αν δεν είναι μονάδα και οι μόνοι διαιρέτες του είναι οι τετριμμένοι.

ς) Το $\pi \in D^*$ λέγεται <u>πρώτο</u>, αν δεν είναι μονάδα και έχει την εξής ιδιότητα: κάθε σχέση της μορφής $\pi|\alpha\cdot\beta$, με $\alpha, \beta \in D$, να συνεπάγεται, κατ' ανάγκη ότι το π διαιρεί ένα, τουλάχιστον από τα α και β.

<u>Παραδείγματα</u>. 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 τετράγωνο. Θεωρώ την ακέραια 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 $\varepsilon^{-1} = \frac{x-y\sqrt{d}}{x^2-dy^2}$, άρα $\varepsilon^{-1} \in \mathbb{Z}[\sqrt{d}]$ 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 διοφαντικής εξίσωσης

$$X^2 - d\cdot Y^2 = \pm 1. \qquad (1)$$

Η εξίσωση (1) λέγεται εξίσωση του Pell (ή των Pell-Fermat) και ισχύουν τα εξής: Για την εξίσωση (1) με το $+1$ στο δεξιό μέλος: Πάντοτε έχει λύση. Η λύση με το

ἐλάχιστο θετικό x (ἄρα καὶ τὸ ἐλάχιστο θετικό y) λέγεται θεμελιώδης λύση, τὴν ὁποία συμβολίζομε (x_1, y_1), $x_1, y_1 > 0$. Τότε, ἀπ' τὴ Θεωρία Ἀριθμῶν εἶναι γνωστὸ ὅτι ὅλες οἱ λύσεις τῆς (1) εἶναι οἱ $\pm(x_n, y_n)$, ὅπου

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

Γιὰ τὴν ἐξίσωση (1) μὲ -1 στὸ δεξιὸ μέλος: Δὲν ἔχει πάντοτε λύση· ἂν ἔχει, τὴν ἐλάχιστη λύση της (μὲ τὴν ἔννοια ποὺ δόθηκε παραπάνω) συμβολίζομε (x_1, y_1), $x_1, y_1 > 0$. Τότε, ὅλες οἱ λύσεις τῆς (1), μὲ -1 στὸ δεξιὸ μέλος, εἶναι οἱ $\pm(x_{2k+1}, y_{2k+1})$, $k \in \mathbb{Z}$, ἐνῶ ὅλες οἱ λύσεις τῆς (1) μὲ $+1$ στὸ δεξιὸ μέλος, εἶναι οἱ $\pm(x_{2k}, y_{2k})$, $k \in \mathbb{Z}$. Καὶ στὶς δύο περιπτώσεις, ἡ (2) δίνει τὰ x_n, y_n συναρτήσει τῶν x_1, y_1.

Συμπέρασμα: Ἂν (x_1, y_1) εἶναι ἡ ἐλάχιστη θετικὴ λύση τῆς (1), τότε ὅλες οἱ μονάδες τῆς ἀκεραίας περιοχῆς $\mathbb{Z}[\sqrt{d}]$ εἶναι οἱ $\pm(x_1 + y_1\sqrt{d})^n$, $n \in \mathbb{Z}$.

Γιὰ παράδειγμα, ἂν $d = 2$, ἡ ἐλάχιστη θετικὴ λύση τῆς (1) εἶναι ἡ $(1, 1)$ (δίνει -1 στὸ δεξιὸ μέλος), ἄρα τὸ σύνολο τῶν μονάδων τῆς $\mathbb{Z}[\sqrt{d}]$ εἶναι τὸ $\{\pm(1+\sqrt{2})^n ; n \in \mathbb{Z}\}$.

Ἂν $d = 3$, τότε ἡ (1) δὲν ἔχει λύση μὲ -1 στὸ δεξιὸ μέλος (αὐτὸ φαίνεται ἂν δουλέψει κανεὶς modulo 4) καὶ ἡ ἐλάχιστη θετικὴ λύση τῆς (1) εἶναι ἡ $(2, 1)$. Ἄρα, τὸ σύνολο ὅλων τῶν μονάδων τῆς $\mathbb{Z}[\sqrt{3}]$ εἶναι τὸ $\{\pm(2+\sqrt{3})^n : n \in \mathbb{Z}\}$.

γ) Ἔστω $d \in \mathbb{Z}$, $d < 0$, ὄχι τέλειο ἀμφιλ. Ὅπως στὴν ἀρχὴ τοῦ (β), καταλήγει κανεὶς στὸ συμπέρασμα ὅτι οἱ μονάδες τῆς ἀκεραίας περιοχῆς $\mathbb{Z}[\sqrt{d}]$ εἶναι ἐκεῖνα, ἀκριβῶς, τὰ $x + y\sqrt{d}$, $x, y \in \mathbb{Z}$, τὰ ὁποῖα ἐπαληθεύουν τὴν (1). Ὅμως, ὡρα $-d > 0$, ἄρα οἱ μόνες λύσεις, γιὰ $d < -1$, εἶναι $\pm(1, 0)$, ἐνῶ γιὰ $d = -1$ οἱ μόνες λύσεις εἶναι $\pm(1, 0)$, $\pm(0, 1)$. Συνεπῶς,

οἱ μόνες μοναδες τοῦ $\mathbb{Z}[\sqrt{d}]$ εἶναι οἱ ± 1, ἂν $d<-1$, ἐνῶ οἱ μόνες μοναδες τοῦ $\mathbb{Z}[i]$ $(i=\sqrt{-1})$ εἶναι οἱ $\pm 1, \pm i$.

δ) Στην ἀκέραια περιοχή $\mathbb{Z}$, οἱ μόνες μοναδες εἶναι οἱ ± 1, ἐνῶ τά ἀνάγωγα καί τά πρῶτα στοιχεῖα συμπίπτουν· τό σύνολό τους εἶναι τό $\{\pm p : p \text{ πρῶτος ἀριθμός}\}$.

ε) Ἔστω K σῶμα. Στην ἀκέραια περιοχή $K[t]$, τά σταθερά πολυώνυμα, καί μόνον αὐτά, εἶναι μοναδες. Τά ἀνάγωγα στοιχεῖα τοῦ $K[t]$ εἶναι, ἀκριβῶς, τά ἀνάγωγα πολυώνυμα τοῦ $K[t]$. Δυνάμει τῆς πρότασης 6(β), κάθε ἀνάγωγο πολυώνυμο εἶναι καί πρῶτο στοιχεῖο τῆς $K[t]$. Ἄρα, στην ἀκέραια περιοχή $K[t]$, ὅπως καί στην $\mathbb{Z}$ (βλ. (δ)), οἱ ἔννοιες "ἀνάγωγο" καί "πρῶτο" ταυτίζονται.

ε) Στην ἀκέραια περιοχή $\mathbb{Z}[\sqrt{-5}]$ οἱ μόνες μοναδες εἶναι ± 1 (βλ. (γ)). Τό 2 εἶναι ἀνάγωγο. Πράγματι, ἔστω $2=(a+b\sqrt{-5})(x+y\sqrt{-5})$, $a,b,x,y\in\mathbb{Z}$. Τότε θά ἀληθεύει καί ἡ συζυγής σχέση καί πολ/σιάζοντας κατά μέλη τίς δύο σχέσεις παίρνομε $4=(a^2+5b^2)(x^2+5y^2)$. Ἂν ἦταν $b\neq 0$ εἶχε $y\neq 0$, τό δεξιό μέλος θά ἦταν ≥ 5, ἄτοπο. Ἄρα $b=y=0$ καί $2=a\cdot x$, πού σημαίνει ὅτι ἕνα ἀπ' τά $a+b\sqrt{-5}$ καί $x+y\sqrt{-5}$ ἰσοῦται μέ ± 1, δηλ. τό ἀποδεικτέο.

Τό 2 δέν εἶναι πρῶτο. Πράγματι, $2\mid 6=(1+\sqrt{-5})(1-\sqrt{-5})$, ἐνῶ $2\nmid 1+\sqrt{-5}$ καί $2\nmid 1-\sqrt{-5}$, κάτι πού ἀποδεικνύεται πολύ εὔκολα. Τό συμπέρασμα εἶναι ὅτι στην ἀκέραια περιοχή $\mathbb{Z}[\sqrt{-5}]$ οἱ ἔννοιες τοῦ ἀναγώγου καί τοῦ πρώτου στοιχείου δέν εἶναι ταυτόσημες. Ἐν γένει, κάθε πρῶτο στοιχεῖο εἶναι καί ἀνάγωγο, δυνάμει τῆς παρακάτω πρότασης.

Πρόταση 1. Σέ κάθε ἀκέραια περιοχή, τά πρῶτα στοιχεῖα εἶναι ἀνάγωγα, ἐνῶ τό ἀντίστροφο δέν ἀληθεύει (παράδειγμα (ε)).

Απόδειξη. Έστω D ακέραια περιοχή και $\pi \in D$ πρώτο. Θά δείξω ότι τό π έχει μόνο τετριμμένους διαιρέτες. Έστω $\rho \mid \pi$. Γράφω $\pi = \rho \cdot \rho'$, $\rho, \rho' \in D$. Προφανώς $\pi \mid \rho \cdot \rho'$, άρα (αφού τό π είναι πρώτο) $\pi \mid \rho$ είτε $\pi \mid \rho'$. Άν $\pi \mid \rho$, τότε οί σχέσεις $\rho \mid \pi$ και $\pi \mid \rho$ συνεπάγονται (πολύ εύκολα) ότι τά π, ρ είναι συνεταιρικά. Άν $\pi \mid \rho'$, τότε θέτω $\rho' = \pi \cdot \rho''$, άρα, άπ' τήν $\pi = \rho \cdot \rho' = \rho \cdot \pi \cdot \rho''$, έχω $\rho \cdot \rho'' = 1$, πού σημαίνει ότι τό ρ είναι μονάδα, ό.έ.δ.

Ορισμός. Μιά ακέραια περιοχή λέγεται περιοχή ανάλυσης (σέ ανάγωγα στοιχεία) άν κάθε μή μηδενικό στοιχείο της, πού δέν είναι μονάδα, μπορεί νά γραφεί ώς γινόμενο (πεπερασμένου πλήθους) ανάγωγων παραγόντων. Μιά περιοχή ανάλυσης θά λέγεται περιοχή μονότροπης ανάλυσης, άν ή προαναφερθείσα ανάλυση μπορεί νά γίνει, αναιρετικά, μέ ένα μόνο τρόπο. Τό επίρρημα "αναιρετικά" αναφέρεται έδώ στήν έννοια ότι συνεταιρικά στοιχεία δέν θεωρούνται διαφορετικά, καθώς επίσης και ότι ή σειρά, μέ τήν οποία γράφονται οί ανάγωγοι παράγοντες στό γινόμενο, δέν παίζει ρόλο.

Τό θεώρημα 2, §4, λέει ότι ή ακέραια περιοχή $K[t]$ (Κωμα) είναι περιοχή μονότροπης ανάλυσης. Επίσης, άπ' τό λεγόμενο "Θεμελιώδες Θεώρημα τής Αριθμητικής", ξέρομε ότι και ή $\mathbb{Z}$ είναι περιοχή μονότροπης ανάλυσης. Τό γεγονός ότι όλα τά ιδεώδη τού $K[t]$ είναι κύρια (§4, Πρόταση 4(α)) καθώς επίσης και όλα τά ιδεώδη τού $\mathbb{Z}$ (§3, Παράδειγμα I(γ)), δέν είναι τυχαίο: Οί περιοχές κυρίων ιδεωδών (δηλ. οί ακέραιες περιοχές τών οποίων όλα τά 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 ανάγωγα στοιχεία ταυτίζονται.

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

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

Η σημασία των περιοχών κυρίων ιδεωδών θα φανεί σαφέστατα παρακάτω: Έστω D περιοχή κυρίων ιδεωδών και $a_1, \dots, a_n \in D$, όχι όλα μηδέν. Λόγω της υπόθεσης για την D, το ιδεώδες $\langle a_1, \dots, a_n \rangle$ είναι κύριο, συνεπώς υπάρχει $d \in D$, έτσι ώστε $\langle a_1, \dots, a_n \rangle = D \cdot d$. Επειδή κάθε a_i ανήκει στο $\langle a_1, \dots, a_n \rangle$, έπεται ότι το d είναι κοινός διαιρέτης των $a_1, \dots, a_n$. Επειδή $d \in D \cdot d$, έπεται ότι υπάρχουν $\lambda_1, \dots, \lambda_n \in D$ έτσι ώστε

$$\lambda_1 a_1 + \dots + \lambda_n a_n = d. \qquad (1)$$

Η (1) συνεπάγεται, ειδικώτερα, ότι κάθε κοινός διαιρέτης των $a_1, \dots, a_n$ είναι, επίσης, διαιρέτης του d. Το d έχει δηλαδή τις εντελώς ανάλογες των ιδιοτήτων, που συναντήσαμε στον ορισμό του μεγίστου κοινού διαιρέτη πολυωνύμων (σελ. 31), και χαρακτηρίζεται ως μέγιστος κοινός διαιρέτης των $a_1, \dots, a_n$.

Τώρα, είναι φανερό ότι δύο οποιοιδήποτε μέγιστοι κοινοί διαιρέτες των $\alpha_1, \ldots, \alpha_n$ είναι συνεταιρικοί καθώς επίσης και ότι (λόγω της (1)) κάθε μέγιστος κοινός διαιρέτης των $\alpha_1, \ldots, \alpha_n$ γράφεται ως γραμμικός συνδυασμός των $\alpha_1, \ldots, \alpha_n$ (με συντελεστές από την D). Τα $\alpha_1, \ldots, \alpha_n$ θα λέγονται <u>πρώτα μεταξύ τους</u> αν η μονάδα είναι μέγιστος κοινός διαιρέτης τους. Η επομένη 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 $K[t]$ να βάλομε τη D, αντί για πολυώνυμα να φανταζόμαστε, φυσικά, στοιχεία της D και αντί για μη μηδενικές σταθερές, μονάδες της D.

<u>Πρόταση 3.</u> Έστω D περιοχή κυρίων ιδεωδών.
α) Αν το $\pi \in D$ είναι ανάγωγο και $\alpha \in D$ εχόν, τότε, ή $\pi | \alpha$ ή τα π και α είναι πρώτα μεταξύ τους.
β) Κάθε ανάγωγο στοιχείο του D είναι πρώτο.
γ) Αν τα $\alpha, \beta \in D$ είναι πρώτα μεταξύ τους και καθένα διαιρεί το $\gamma \in D$ τότε και το $\alpha\beta$ διαιρεί το γ.
δ) Αν το $\alpha \in D$ είναι πρώτο προς το β και προς το γ $(\beta, \gamma \in D)$, τότε το α είναι πρώτο και προς το $\beta\gamma$.

<u>Θεώρημα 1.</u> Αν μια περιοχή κυρίων ιδεωδών είναι περιοχή ανάλυσης, τότε είναι και περιοχή μονότροπης ανάλυσης.

<u>Απόδειξη.</u> Άμεση συνέπεια των προτάσεων 3(β) και 2.

Χάρη στο Θεώρημα 1 και στην πρόταση 3, μπορούμε να μεταφέρομε όλη, ουσιαστικά, τη θεωρία διαιρετότητας των ακεραίων σε κάθε περιοχή ανάλυσης, η οποία είναι και

περιοχή κυρίων ιδεωδών. Η απόδειξη της πρότασης 3 στηρίζεται στην ύπαρξη μεγίστου κοινού διαιρέτου, για όποιαδήποτε στοιχεία $\alpha_1, \dots, \alpha_n$ της θεωρουμένης περιοχής και στη δυνατότητα γραφής του μεγίστου κοινού διαιρέτου ως γραμμικού συνδυασμού των $\alpha_1, \dots, \alpha_n$ (βλ. (1), σελ. 43). Οι ιδιότητες αυτές, με τη σειρά τους, στηρίζονται κατ' ουσίαν στο γεγονός ότι κάθε ιδεώδες της θεωρουμένης περιοχής είναι κύριο. Αυτό μπορεί να κάνει κάποιον να υποθέσει ότι σε περιοχές όπου δεν είναι όλα τα ιδεώδη κύρια, η δυνατότητα να έχομε μιά καλή θεωρία διαιρετότητας δεν υπάρχει. Για τις άπειρες περιοχές, εν μέρει, αλήθεια και για τις περιοχές ανάλυσης, αυτό αληθεύει. Για τις περιοχές μονότροπης ανάλυσης όμως, όλη η βασική θεωρία διαιρετότητας των ακεραίων σώζεται. Επειδή, υπάρχουν περιοχές μονότροπης ανάλυσης, οι οποίες δεν είναι περιοχές κυρίων ιδεωδών (αργότερα θα δούμε τέτοιο 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 $\alpha_1, \dots, \alpha_n \in D$, τα οποία δεν είναι όλα 0, είναι αυτή που ήδη έχομε συναντήσει: Το $d \in D$ είναι μέγιστος κοινός διαιρέτης (μ.κ.δ.) των $\alpha_1, \dots, \alpha_n$ αν είναι κοινός διαιρέτης τους και αν διαιρείται από κάθε άλλο κοινό διαιρέτη των $\alpha_1, \dots, \alpha_n$. Είναι εντελώς τετριμμένο να δείξει κανείς ότι δύο οποιοιδήποτε μέγιστοι κοινοί διαιρέτες των $\alpha_1, \dots, \alpha_n$ είναι συνεταιρικοί.

Ἂν ἡ μονάδα εἶναι μ.κ.δ. τῶν $\alpha_1, \dots, \alpha_n$ τότε οἱ $\alpha_1, \dots, \alpha_n$ λέγονται πρῶτοι μεταξύ τους. Ἡ ἰσοδύναμη συνθήκη εἶναι ὅτι οἱ μόνοι κοινοὶ διαιρέτες τῶν $\alpha_1, \dots, \alpha_n$ εἶναι οἱ μονάδες.

Πρόταση 4. Σὲ περιοχὴ μονοτροπης ἀνάλυσης, κάθε ἀναγωγο στοιχεῖο εἶναι πρῶτο. (πρβλ. Πρόταση 3(β)).

Ἀπόδειξη. Ἔστω π ἀνάγωγο στοιχεῖο καὶ $\pi | \alpha\cdot\beta$. Τότε $\alpha\cdot\beta = \pi\cdot\rho$. Ἀναλύω τὰ α, β, ρ σὲ γινόμενο ἀναγώγων: $\alpha = \pi_1 \cdots \pi_\lambda$, $\beta = \pi'_1 \cdots \pi'_\mu$, $\rho = \rho_1 \cdots \rho_\nu$, ὁπότε $\pi_1 \cdots \pi_\lambda \pi'_1 \cdots \pi'_\mu = \pi\rho_1 \cdots \rho_\nu$. Δηλαδὴ τὸ ἴδιο στοιχεῖο τῆς περιοχῆς (τὸ $\alpha\cdot\beta$) ἀναλύεται σὲ ἀνάγωγα μὲ δύο τρόπους. Λόγῳ τῆς μονοτροπης ἀνάλυσης, οἱ ἀναλύσεις στὰ δύο μέλη δὲν εἶναι οὐσιωδῶς διαφορετικές, ἄρα τὸ π, ποὺ ἐμφανίζεται στὸ δεξιὸ μέλος, πρέπει νὰ εἶναι συνεταιρικὸ μὲ ἕνα, τοὐλάχιστον, ἀπὸ τὰ $\pi_1, \dots, \pi_\lambda, \pi'_1, \dots, \pi'_\mu$ καὶ, συνεπῶς, τὸ π διαιρεῖ τὸ α εἴτε τὸ β, δ' ἐ.δ.

Συχνὰ ἐξυπηρετεῖ νὰ κάνομε τὸ ἑξῆς (ὑποθέτω ὅτι βρισκόμαστε στὴν περιοχὴ μονοτροπης ἀνάλυσης D). Ἔστω $\mathcal{P}$ ἕνα πλῆρες σύστημα πρώτων (= ἀναγώγων) στοιχείων τοῦ D. Αὐτὸ σημαίνει ὅτι κάθε ἀνάγωγο στοιχεῖο τῆς D εἶναι συνεταιρικὸ μὲ κάποιο στοιχεῖο τοῦ $\mathcal{P}$ καὶ ἀνὰ δύο τὰ στοιχεῖα τοῦ $\mathcal{P}$ δὲν εἶναι συνεταιρικά. Τότε, κάθε $\alpha \in D^*$ γράφεται μονοτροπα ὑπὸ τὴ μορφὴ

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

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

("σχεδόν ὅλοι" σημαίνει "ὅλοι ἐκτὸς ἀπὸ πεπερασμένο, τό πολύ, πλῆθος"). Ἡ ἀνάλυση (1) λέγεται κανονική ἀνάλυση σέ γινόμενο ἀναγώγων (ἢ πρώτων) παραγόντων. Γιά παράδειγμα, ἄν $D = \mathbb{Z}$ τότε παίρνομε $\mathcal{P}$ νά εἶναι τό σύνολο τῶν θετικῶν πρώτων ἀριθμῶν· ἄν $D = K[t]$ (Κ σῶμα) μιά συνηθισμένη ἐπιλογή γιά τό $\mathcal{P}$ εἶναι τό σύνολο τῶν ἀναγώγων μονικῶν πολυωνύμων τοῦ $K[t]$. Ἐν γένει κάνομε τήν ἑξῆς σύμβαση: $\varepsilon_p(0) = \infty$ $\forall p$, ὅπου ἐννοεῖται ὅτι $\infty + n = \infty$ $\forall n \in \mathbb{Z}$. Ἔτσι μποροῦμε νά μιλοῦμε καί γιά τήν κανονική ἀνάλυση τοῦ 0.

Πρόταση 5. Ἔστω D περιοχή μοναδικῆς ἀναλύσεως καί $\alpha, \beta \in D$, $\beta \neq 0$. Τότε (ἔχοντας ὑπ' ὄψη τίς κανονικές ἀναλύσεις τῶν α, β) $\beta \mid \alpha$ ἄν καί μόνο ἄν

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

Ἀπόδειξη. Γιά ἁπλούστευση τοῦ συμβολισμοῦ θά παραλείπω ἀπ' τό σύμβολο $\prod_{p \in \mathcal{P}}$ τό $p \in \mathcal{P}$.

Ἔστω $\beta \mid \alpha$. Θέτω $\alpha = \beta \cdot \gamma$ καί θεωρῶ τίς κανονικές ἀναλύσεις τῶν α, β, γ:

$$\prod p^{\varepsilon_p(\alpha)} = \left\{\prod p^{\varepsilon_p(\beta)}\right\}\left\{\prod p^{\varepsilon_p(\gamma)}\right\} = \prod p^{\varepsilon_p(\beta)+\varepsilon_p(\gamma)}$$

Λόγῳ τῆς μοναδικῆς ἀναλύσεως πρέπει $\varepsilon_p(\alpha) = \varepsilon_p(\beta) + \varepsilon_p(\gamma)$ $\forall p \in \mathcal{P}$ καί, ἐπειδή $\varepsilon_p(\gamma) \geq 0$, εἶναι $\varepsilon_p(\alpha) \geq \varepsilon_p(\gamma)$ $\forall p$. Ἀντιστρόφως, ἔστω $\varepsilon_p(\alpha) \geq \varepsilon_p(\beta)$ $\forall p \in \mathcal{P}$. Θέτω $\nu_p = \varepsilon_p(\alpha) - \varepsilon_p(\beta) \geq 0$ $\forall p \in \mathcal{P}$ καί $\gamma = \prod p^{\nu_p}$. Ἐπειδή ὅλα σχεδόν τά ν_p εἶναι 0, ἔχει νόημα τό γ ὡς

στοιχείο της D και είναι προφανές ότι $\gamma \cdot \beta = \alpha$, άρα $\beta | \alpha$.

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

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 μονοσήμαντης ανάλυσης και $\alpha_1, \dots, \alpha_n \in D$, όχι όλα 0. Τότε το $\delta \in D$, που ορίζεται

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

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

Απόδειξη Είναι $\varepsilon_p(\delta) = \nu_p \leq \varepsilon_p(\alpha_i) \quad \forall p \in \mathcal{P}$ και $\forall i = 1, \dots, n$.
Συνεπώς, από την πρόταση 5, $\delta | \alpha_i \quad \forall i = 1, \dots, n$.
Έστω τώρα d κοινός διαιρέτης των $\alpha_1, \dots, \alpha_n$. Τότε (πρόταση 5) $\varepsilon_p(d) \leq \varepsilon_p(\alpha_i) \quad \forall p \in \mathcal{P}$ και $\forall i = 1, \dots, n$.
Άρα $\varepsilon_p(d) \leq \nu_p = \varepsilon_p(\delta) \quad \forall p \in \mathcal{P}$, δηλαδή (πρόταση 5), $d | \delta$, δηλ. δ.

Πρόταση 7. Έστω D περιοχή μονοσήμαντης ανάλυσης.
α) Αν το $\pi \in D$ είναι ανάγωγο και $\alpha \in D$ τυχόν, τότε ή $\pi | \alpha$ 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(γ)).
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 $\pi \nmid \alpha$. Θεωρώ $p_0 \in \mathcal{P}$ συνεταιρικό προς τό π. Τότε $\varepsilon_{p_0}(\pi) = 1$ και από την πρόταση 5, $\varepsilon_{p_0}(\alpha) < \varepsilon_{p_0}(\pi) = 1$, άρα $\varepsilon_{p_0}(\alpha) = 0$. Για κάθε $p \in \mathcal{P}$, $p \neq p_0$ είναι, προφανώς $\varepsilon_p(\pi) = 0$, αφού τό π είναι ανάγωγο. Άρα, στην πρόταση 6, για $n = 2$, $\alpha_1 = \alpha$, $\alpha_2 = \pi$, είναι $\nu_p = 0$ για κάθε $p \in \mathcal{P}$, που σημαίνει ότι τά α, π είναι πρώτα μεταξύ τους.

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

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

Τώρα θά εξετάσομε τό δακτύλιο των πολυωνύμων με συντελεστές από μιά περιοχή μονότροπης ανάλυσης D. Παρατηρήστε ότι στην ειδική περίπτωση που $D = K$, σώμα, ούτε κάν μιλάμε για μονότροπη ανάλυση, διότι, κάθε μή μηδενικό στοιχείο του K, ως αντιστρέψιμο, είναι μονάδα του K και, συνεπώς, άνάγωγα στοιχεία δέν υπάρχουν στό K. Έχομε όμως ήδη (Θεώρημα 2, §4) ότι τό $K[t]$ είναι

περιοχή μονότροπης ανάλυσης. Το ίδιο θ' αποδείξομε και για το $D[t]$, στην περίπτωση που η D είναι περιοχή μονότροπης ανάλυσης. Αυτό το γεγονός έχει πολύ ενδιαφέρουσες συνέπειες· η πιό άμεση, ίσως, είναι ότι στα πολυώνυμα πολλών μεταβλητών (θα ορισθούν αυστηρά παρακάτω) με συντελεστές από τη D, ισχύει η μονότροπη ανάλυση. Χρειαζόμαστε μιά μικρή προεργασία. Σημειώστε ότι, μέχρι τέλους της §5, το D θα συμβολίζει περιοχή μονότροπης ανάλυσης.

Ορισμός. Το μη σταθερό $f(t) \in D[t]$ λέγεται πρωταρχικό, άν οι συντελεστές του είναι πρώτοι μεταξύ τους. Άν το $f(t)$ είναι σταθερό, τότε, θα λέγεται πρωταρχικό άν ισούται με μονάδα του D.

Πρόταση 8 (Λήμμα του Gauss). Έστω F_D το σώμα πηλίκων της περιοχής μονότροπης ανάλυσης D και $f(t) \in D[t]$. Τότε, το $f(t)$ είναι ανάγωγο στοιχείο της περιοχής $D[t]$, άν και μόνο άν το $f(t)$ είναι ή ανάγωγο στοιχείο της D ή πρωταρχικό πολυώνυμο, το οποίο, θεωρούμενο ως πολυώνυμο του $F_D[t]$, είναι ανάγωγο.

Απόδειξη. Έστω ότι το $f(t)$ είναι ανάγωγο στοιχείο της $D[t]$. Άν είναι σταθερό, τότε πρέπει να είναι ανάγωγο στοιχείο της D. Άν δέν είναι σταθερό, τότε πρέπει να είναι πρωταρχικό, διαφορετικά θα είχε μιά ανάλυση $f(t) = d \cdot g(t)$, με $g(t) \in D[t]$ και $d \in D$ όχι μονάδα της D. Μένει τώρα να δείξομε το πιό δύσκολο: ότι το πρωταρχικό πολυώνυμο $f(t) \in D[t]$, θεωρούμενο ως πολυώνυμο του $F_D[t]$, είναι ανάγωγο. Έστω ότι

δέν ἦταν. Τότε θά εἴχαμε μιά σχέση $f(t) = f_1(t) \cdot f_2(t)$ μέ τά $f_1(t)$, $f_2(t)$ μή σταθερά πολυώνυμα τοῦ $F_D[t]$. Οἱ συντελεστές τῶν $f_1(t)$, $f_2(t)$ ἀνήκαν στό F_D ἄρα εἶναι πηλίκα στοιχείων τῆς D. Συνεπῶς, πολ/σιάζοντας μέ κατάλληλο στοιχεῖο $d \in D$ (π.χ. d = γινόμενο τῶν παρονομαστῶν, πού ἐμφανίζονται στούς συντελεστές τῶν $f_1(t)$, $f_2(t)$), νά τά λήγαμε σέ μιά σχέση τῆς μορφῆς

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

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

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

Ἰσχυρίζομαι ὅτι στήν (1) μπορῶ νά ὑποθέσω τά $a_0, \ldots, a_m$ πρῶτα μεταξύ τους καί τά $b_0, \ldots, b_n$ πρῶτα μεταξύ τους. Ἄς ποῦμε ὅτι τά $a_0, \ldots, a_m$ δέν ἦταν πρῶτα μεταξύ τους. Τότε* θά ὑπῆρχε πρῶτο στοιχεῖο p τῆς D, τό ὁποῖο νά διαιρεῖ ὅλα τά $a_0, \ldots, a_m$, ἄρα καί ὅλους τούς συντελεστές τοῦ γινομένου στό δεξιό μέλος τῆς (1). Αὐτό συνεπάγεται ὅτι ὅλα τά $d \cdot c_0, d \cdot c_1, \ldots, d \cdot c_N$ εἶναι πολ/σια τοῦ p. Ὅμως τό p δέν εἶναι δυνατόν νά διαιρεῖ ὅλα τά $c_0, c_1, \ldots, c_N$, ἀφοῦ αὐτά εἶναι πρῶτα μεταξύ τους, ἄρα ὑπάρχει c_i τέτοιο ὥστε $p \nmid c_i$. Ἐπειδή $p \mid d \cdot c_i$, ἕπεται τότε ὅτι $p \mid d$. Ἄρα, σ' αὐτή τήν περίπτωση, θά μπορούσαμε νά ἁπλοποιήσουμε τήν (1) διαιρώντας καί τά δύο μέλη διά p. Ἄν ἐξακολουθοῦν τά "νέα" $a_0, \ldots, a_m$, πού θά προκύψουν μετά τήν ἁπλοποίηση, νά μήν εἶναι πρῶτα μεταξύ τους, ἐπαναλαμβάνουμε τήν παραπάνω διαδικασία. Αὐτό μπορεῖ νά ἐπαναληφθεῖ πεπερασμένες (τό πολύ) φορές, λόγῳ τοῦ ὅτι κάθε a_i ἔχει πεπερασμένο, τό πολύ, πλῆθος πρώτων διαιρετῶν. Τελικά, ἡ (1) μᾶς

---

* λόγῳ τῆς Πρότασης 6

δίνεται σε μιά ακέραια της μορφής

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

με $d \in D^*$, $a_0, \ldots, a_m \in D$ πρώτα μεταξύ τους $(a_m \neq 0, m \geq 1)$

$b_0, \ldots, b_n \in D$ " " " " $(b_n \neq 0, n \geq 1)$.

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 κάποιο πρώτο διαιρέτη p. Το p 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

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

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

Εντελώς αναλόγως, υπάρχει δείκτης l, $0 \leq l \leq n$, τέτοιος ώστε

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

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

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

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

Αντιστρόφως: 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

καὶ ἀνάγωγο στὸ $F_D[t]$. Τότε ἀπαιτεῖται νὰ εἶναι γινόμενο δύο μὴ σταθερῶν πολυωνύμων τοῦ $D[t] \subseteq F_D[t]$. Ἂν, πάλι, $f(t) = c \cdot g(t)$ μὲ $c \in D^*$, τότε τὸ c πρέπει νὰ εἶναι μονάδα τῆς D, διότι τὸ $f(t)$ ἔχει ὑποτεθεῖ πρωταρχικό. Συνεπῶς, τὸ $f(t)$ εἶναι ἀνάγωγο στοιχεῖο τῆς περιοχῆς $D[t]$, ὅ.ἔ.δ.

Σημαντικὴ παρατήρηση: Ἡ σχέση (2) (ὑπὸ τὶς συνθῆκες, ποὺ γράφονται κάτω ἀπὸ αὐτὴ) δίδηται σὲ ἄτοπο, ἂν τὸ δ δὲν εἶναι μονάδα τῆς D. Αὐτὸ ἀποδεικνύει ὅτι, τὸ γινόμενο δύο πρωταρχικῶν πολυωνύμων τῆς $D[t]$ εἶναι πρωταρχικὸ πολυώνυμο τῆς $D[t]$. Ἡ γενίκευση γιὰ περισσότερα ἀπὸ δύο πολυώνυμα, εἶναι προφανής.

Ἕνας τεχνικὸς ὁρισμός, ποὺ θὰ χρειαστοῦμε εἶναι ὁ ἑξῆς: Ἂν $f(t) \in D[t]$, ὄχι σταθερό, μὲ "περιεχόμενο τοῦ $f(t)$" ἐννοοῦμε ἕνα ὁποιοδήποτε μέγιστο κοινὸ διαιρέτη τῶν συντελεστῶν τοῦ $f(t)$. Εἰδικώτερα, τὸ $f(t)$ εἶναι πρωταρχικό, ἂν καὶ μόνο ἂν, τὸ περιεχόμενό του εἶναι μονάδα.

Λῆμμα. Ἔστω D περιοχὴ μοναδιαίας ἀναλύσεως καὶ F_D τὸ σῶμα πηλίκων της. Τότε, κάθε $f(t) \in F_D[t]$, ὄχι σταθερό, μπορεῖ νὰ γραφτεῖ ὡς $f(t) = \alpha \cdot g(t)$, ὅπου $\alpha \in F_D$ καὶ τὸ $g(t) \in D[t]$ εἶναι πρωταρχικό. Ἂν $f(t) = \alpha_1 \cdot g_1(t)$ εἶναι μιὰ ἄλλη ἀνάλογη γραφὴ τοῦ $f(t)$, τότε $g_1(t) = \varepsilon \cdot g(t)$, μὲ ε μονάδα τῆς D.

Ἀπόδειξη. Ἔστω β τὸ γινόμενο τῶν παρονομαστῶν τῶν συντελεστῶν τοῦ $f(t)$. Προφανῶς $\beta \cdot f(t) = h(t) \in D[t]$. Ἂν g

είναι τό περιεχόμενο τοῦ $h(t)$, τότε $h(t) = \gamma \cdot g(t)$, ὅπου τό $g(t) \in D[t]$ 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 μέ τόν ἰσχυρισμό. Ἔστω τώρα $f(t) = \alpha_1 \cdot g_1(t)$. Θεωρῶ $\delta \in D$, τέτοιο ὥστε $\delta\alpha, \delta\alpha_1 \in D$. Τότε $\delta f(t) = (\delta\alpha) \cdot g(t)$ καί $\delta f(t) = (\delta\alpha_1) \cdot g_1(t)$. Ἐπειδή τό $g(t)$ εἶναι πρωταρχικό, εἶναι φανερό ὅτι τό $\delta\alpha$ εἶναι περιεχόμενο τοῦ $\delta \cdot f(t)$. Ὁμοίως, τό $\delta\alpha_1$ εἶναι περιεχόμενο τοῦ $\delta \cdot f(t)$. Ἀφοῦ τά $\delta\alpha$ καί $\delta\alpha_1$ εἶναι μέγιστοι κοινοί διαιρέτες τῶν αὐτῶν στοιχείων (δηλ. τῶν συντελεστῶν τοῦ $\delta \cdot f(t)$), θά συνδέονται μέ μιά σχέση $\delta\alpha = \varepsilon \cdot \delta\alpha_1$, ὅπου ε εἶναι μονάδα τῆς D. Λόγῳ καί τῆς σχέσης $\alpha \cdot g(t) = f(t) = \alpha_1 \cdot g_1(t)$, ἔχομε $g_1(t) = \varepsilon \cdot g(t)$, ὅ.ἐ.δ.

Θεώρημα 2. Ἄν D εἶναι περιοχή μοναδικῆς ἀναλύσης, τότε καί ἡ $D[t]$ εἶναι περιοχή μοναδικῆς ἀναλύσης.

Ἀπόδειξη. Ἔστω $f(t) \in D[t]$. Θά ἀποδείξω πρῶτα ὅτι τό $f(t)$ ἀναλύεται σέ ἀναγωγα στοιχεῖα τῆς $D[t]$. Ἄν τό $f(t)$ εἶναι σταθερό, ὁ ἰσχυρισμός μου ἐξασφαλίζεται ἀμέσως, ἀπ' τό γεγονός ὅτι ἡ D εἶναι περιοχή μοναδικῆς ἀναλύσης. Ἔστω τώρα ὅτι τό $f(t)$ δέν εἶναι σταθερό. Γράφω $f(t) = \alpha \cdot g(t)$, ὅπου α εἶναι τό περιεχόμενο τοῦ $f(t)$ καί τό $g(t) \in D[t]$ εἶναι πρωταρχικό. Ἀρκεῖ, λοιπόν, ν' ἀποδείξω ὅτι τό $g(t)$ ἀναλύεται σέ ἀναγωγα στοιχεῖα τῆς $D[t]$. Βλέπω τό $g(t)$ ὡς πολυώνυμο τοῦ $F_D[t]$, ὁπότε, ἀπ' τό Θεώρημα 2 τῆς §4, ἐξασφαλίζω τήν ἀνάλυση $g(t) = p_1(t) \cdots p_n(t)$ σέ ἀναγωγα πολυώνυμα τοῦ $F_D[t]$. Λόγῳ τοῦ προηγουμένου λήμματος, γιά κάθε $i = 1, \ldots, n$, μπορῶ νά γράψω $p_i(t) = \beta_i \, q_i(t)$, ὅπου $\beta_i \in F_D$ καί τό $q_i(t) \in D[t]$ εἶναι πρωταρχικό καί ἀνά-

μηδενικό πολυώνυμο τοῦ $D[t]$ (ἄρα ἀνάγωγο στοιχεῖο τῆς $D[t]$). Συνεπῶς, $g(t) = \beta_1 \cdots \beta_n \cdot q_1(t) \cdots q_n(t) = \beta \cdot q_1(t) \cdots q_n(t)$, ὅπου $\beta_1 \cdots \beta_n = \beta \in F_D$. Ἡ παρατήρηση τῆς σελ. 53 λέει ὅτι τό $q(t) = q_1(t) \cdots q_n(t)$ εἶναι πρωταρχικό πολυώνυμο, ὅπότε ἔχομε $g(t) = \beta \cdot q(t)$ μέ τά $g(t), q(t) \in D[t]$, πρωταρχικά καί $\beta \in F_D$. Τό μονάκριπο, μιά τό ὁποῖο μιλεῖ τό λῆμμα, συνεπάγεται ὅτι τό β εἶναι μονάδα τῆς D, ἄρα στή σχέση $g(t) = \beta\, q_1(t) \cdots q_n(t)$ μπορῶ καί ὑποθέτω, χωρίς βλάβη τῆς γενικότητας, ὅτι $\beta = 1$ κι ἔχω ἀποδείξει τόν ἰσχυρισμό μου. Ἔστω τώρα ὅτι ἔχω δύο ἀναλύσεις

$$g(t) = \alpha_1 \cdots \alpha_\mu \cdot p_1(t) \cdots p_m(t), \quad g(t) = \beta_1 \cdots \beta_\nu\, q_1(t) \cdots q_n(t) \qquad (1)$$

(οἱ συμβολισμοί αὐτοί δέν ἔχουν σχέση μέ ἐκείνους τοῦ πρώτου μέρους τῆς ἀπόδειξης), ὅπου $\alpha_1, \ldots, \alpha_\mu, \beta_1, \ldots, \beta_\nu \in D$ εἶναι ἀνάγωγα στοιχεῖα τῆς D καί τά $p_1(t), \ldots, p_m(t), q_1(t), \ldots, q_n(t)$ εἶναι ἀνάγωγα καί πρωταρχικά πολυώνυμα τοῦ $D[t]$. Τά $p(t) = p_1(t) \cdots p_m(t)$ καί $q(t) = q_1(t) \cdots q_n(t)$ εἶναι πρωταρχικά (παρατήρηση σελ. 53) καί ἰσχύει $\alpha \cdot p(t) = \beta \cdot q(t)$, ὅπου $\alpha = \alpha_1 \cdots \alpha_\mu$ καί $\beta = \beta_1 \cdots \beta_\nu$. Ἀπ' τό λῆμμα ἕπεται ὅτι τά α, β εἶναι συνεταιρικά, ἄρα, λόγῳ τοῦ μοναδικοῦ τῆς ἀνάλυσης στήν D, οἱ ἀναλύσεις $\alpha_1 \cdots \alpha_\mu$ καί $\beta_1 \cdots \beta_\nu$ εἶναι αὐταιωδῶς οἱ ἴδιες (δηλ. $\mu = \nu$ καί τά $\alpha_1, \ldots, \alpha_\mu$ μέ τά $\beta_1, \ldots, \beta_\mu$ εἶναι συνεταιρικά, ἕνα πρός ἕνα). Λόγῳ τῆς (1) τώρα ἔχομε

$$p_1(t) \cdots p_m(t) = \varepsilon \cdot q_1(t) \cdots q_n(t) \qquad (2)$$

Τά πολυώνυμα στή (2) εἶναι ἀνάγωγα στοιχεῖα τῆς $D[t]$, ἄρα (Πρόταση 8) εἶναι ἀνάγωγα πολυώνυμα τοῦ $F_D[t]$ καί τώρα, τό Θεώρημα 2, §4, συνεπάγεται ὅτι οἱ ἀναλύσεις στά δύο μέλη τῆς (2) εἶναι αὐταιωδῶς οἱ ἴδιες, ὅ.ἐ.δ.

Πολυώνυμα δύο ή περισσοτέρων μεταβλητών. Έστω D ακέραια περιοχή και $D[t_1]$ ο δακτύλιος (ακέραια περιοχή) των πολυωνύμων με συντελεστές από την D και μεταβλητής t_1. Μπορώ τώρα να θεωρήσω τον δακτύλιο των πολυωνύμων με συντελεστές από την $D[t_1]$ και μεταβλητής t_2, δηλ. τον δακτύλιο $(D[t_1])[t_2]$. Αυτός συμβολίζεται με $D[t_1,t_2]$. Τα στοιχεία του είναι, εξ ορισμού, της μορφής $f(t_1,t_2) = f_n(t_1)\cdot t_2^n + \cdots + f_1(t_1)\cdot t_2 + f_0(t_1)$, όπου $f_i(t_1) \in D[t_1]$, (1) για κάθε $i = 1,\dots,n$. Άρα, τα τυπικά στοιχεία του $D[t_1,t_2]$ είναι της μορφής

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

Στη συνέχεια μπορούμε να ορίσομε τον δακτύλιο των πολυωνύμων $D[t_1,t_2,t_3] \overset{\text{ορ}}{=} (D[t_1,t_2])[t_3]$ και, επαγωγικά, τον δακτύλιο των πολυωνύμων $D[t_1,t_2,\dots,t_\nu]$.

Δεν θα μπούμε σε πολλές λεπτομέρειες, αλλά θα κάνομε κάποιες βασικές παρατηρήσεις:

α) Ο δακτύλιος $D[t_1,\dots,t_\nu]$ είναι ακέραια 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, ταυτίζομε τα $t_1^{j_1}t_2^{j_2}$ και $t_2^{j_2}t_1^{j_1}$ και τους δακτυλίους $D[t_1,t_2]$ και $D[t_2,t_1]$.

Γενικώτερα, τον δακτύλιο $D[t_1,\dots,t_\nu]$ τον ταυτίζομε με τον δακτύλιο $D[t_{i_1},\dots,t_{i_\nu}]$, για οποιαδήποτε μετάθεση $(i_1,\dots,i_\nu)$ των $(1,\dots,\nu)$.

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 $f_n(t_1) = \cdots = f_1(t_1) = f_0(t_1) = 0 \in D[t_1]$. Αυτό, με τη

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

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

Απόδειξη. (α) Λόγω του Θεωρήματος 2, η απόδειξη συνίσταται σε μιά απλουστευτική επαγωγή (επί του πλήθους ν των μεταβλητών).
(β) Λόγω του Θεωρήματος 2, §4, το $K[t_1]$ είναι περιοχή μονότροπης ανάλυσης. Λόγω πάλι 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, καταλήγομε στο αποδεικτέο.

Δύο σημαντικά παραδείγματα. Ας θεωρήσομε τα πολυώνυμα δύο μεταβλητών με πραγματικούς συντελεστές. Τις μεταβλητές, αντί t_1, t_2, ας τις γράψομε (για απλούστευση) X, Y.
α) Στο τέλος της §3 (σελ. 23) είχα ισχυριστεί ότι καθένα 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 και δείξω ότι $f(X,Y) \in \langle X \rangle$ είτε $g(X,Y) \in \langle X \rangle$. Ας γράψω $f(X,Y) = f_m(Y)\cdot X^m + \cdots + f_1(Y)\cdot X + f_0(Y)$ και $g(X,Y) = g_m(Y)\cdot X^m + \cdots + g_1(Y)\cdot X + g_0(Y)$.

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, $\langle X \rangle \subsetneq \langle X, Y \rangle \subsetneq \mathbb{R}[X,Y]$, δι' ει 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 κυρίων ιδεωδών· αυτό θα δικαιολογήσει τον ισχυρισμό μου στη σελ. 45 ότι υπάρχουν περιοχές μονότροπης ανάλυσης, που δεν είναι περιοχές κυρίων 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 τα $f(X,Y)$, $g(X,Y)$ ως πολυώνυμα του $(\mathbb{R}[Y])[X]$, συμπεραίνω ότι έχω δύο περιπτώσεις: η' (i) $f(X,Y) = A_1(Y)\cdot X + A_0(Y)$ & $g(X,Y) = B_0(Y)$, η' (ii) $f(X,Y) = A_0(Y)$ & $g(X,Y) = B_1(Y)\cdot X + B_0(Y)$ $(A_0(Y), A_1(Y), B_0(Y), B_1(Y) \in \mathbb{R}[Y])$.

Στην περίπτωση (i) έχομε $X = A_1(Y)\cdot B_0(Y)\cdot X + A_0(Y)\cdot B_0(Y)$, 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 $Y \in \langle X, Y \rangle$,

$Y = A_1 \cdot X \cdot H(X,Y)$, $H(X,Y) \in \mathbb{R}[X,Y]$. Αλλά αύτή, ώς σχέση στό $(\mathbb{R}[Y])[X]$ είναι, προφανώς, αδύνατη.
Στήν περίπτωση (ii) συμπεραίνω, ανάλογα, ότι $A_0(Y) \cdot B_0(Y) = 0$ καί $A_0(Y) \cdot B_1(Y) = 1$, άρα $B_0(Y) = 0$ καί $A_0(Y), B_1(Y)$ 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, σέ τέτοια περίπτωση, τά σταθερά πολυώνυμα θά έπρεπε καί ανήκουν στό $\langle X, Y \rangle$, κάτι προφανώς αδύνατο.

Ευκλείδιες περιοχές. Μιά πολύ ενδιαφέρουσα, είδική περίπτωση περιοχών μονότροπης ανάλυσης είναι οί ευκλείδιες περιοχές. Μιά ακέραια περιοχή E λέγεται ευκλείδια, άν υπάρχει συνάρτηση $\nu : E \longrightarrow \mathbb{Z}_{\geq 0}$, μέ τίς έξής ιδιότητες: (i) Άν $a, b \in E^*$ καί $a \mid b$, τότε $\nu(a) \leq \nu(b)$.
(ii) Άν $a, b \in E$ καί $b \neq 0$, υπάρχουν $q, r \in E$, τέτοια ώστε $a = q \cdot b + r$ καί είτε $r = 0$, είτε $\nu(r) < \nu(b)$.
Ή ν λέγεται σταθμη τής E. Μέχρι τέλους τής §5, E θά παριστάνει ευκλείδια περιοχή.
Παραδείγματα ευκλειδίων περιοχών είναι ή $\mathbb{Z}$ μέ σταθμη τήν απόλυτη τιμή καί ή $K[t]$ (K σώμα) μέ σταθμη τό βαθμό τών πολυωνύμων.

Πρόταση 9. Έστω E είναι ευκλείδια περιοχή σταθμης ν.
α) Άν $a, b \in E^*$, $a \mid b$ καί $\nu(a) = \nu(b)$, τότε τά a, b είναι συνεταιρικά.
β) Ή E είναι περιοχή ανάλυσης.

Απόδειξη. α) Λόγω τής συνθήκης (ii) τών ευκλειδίων περιοχών, υπάρχουν $q, r \in E$, τέτοια ώστε $a = bq + r$.

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

β) Έστω $\min\nu(E)=n_0\in\mathbb{Z}_{\geq 0}$. Θ' αποδείξω επαγωγικά τον ισχυρισμό: Αν $\nu(a)=n_0$, τότε το 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 μοναδες, ούτε συνεταιρικά του a. Θα είχα τότε $\nu(b), \nu(c)\leq\nu(a)=n_0$, άρα, κατ' ανάγκη, $\nu(b)=\nu(c)=n_0$ (λόγω της επιλογής του n_0). Αυτό, λόγω του (α) θα συνεπαγόταν ότι τα b, c είναι συνεταιρικά του a, άτοπο.

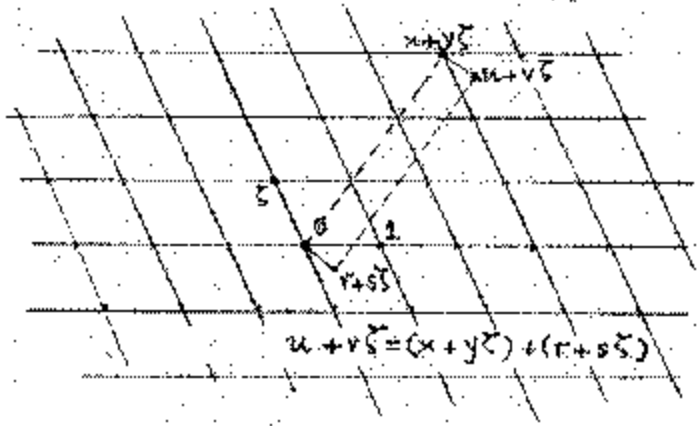
Έστω τώρα ότι έχω αποδείξει τον ισχυρισμό (β) για όλα τα $a\in E$ με $n_0\leq\nu(a)\leq n-1$ για κάποιο $n>n_0$, και έστω a με $\nu(a)=n$. Αν το a είναι άναγωγο, έχω τελειώσει· αν όχι γράφω $a=b\cdot c$ με b, c γνήσιους διαιρέτες του a. Συνεπώς, λόγω του (α), θα είναι $\nu(b), \nu(c)<\nu(a)=n$, άρα, από την επαγωγική υπόθεση, τα b, c αναλύονται σε γινόμενο αναγώγων στοιχείων της E. Τότε και το $a=b\cdot c$ αναλύεται, δηλ. ό.

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

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

παράδειγμα I(γ), §3. Αντί για ακεραίους θα έχομε τώρα στοιχεία κάποιας ευκλείδιας περιοχής E και αντί για σχέσεις της μορφής $a \leq b$, με $a, b \in \mathbb{Z}$, θα έχομε σχέσεις $\nu(a) \leq \nu(b)$, 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, δηλ.

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 ακέραια 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 $\nu : E^* \longrightarrow \mathbb{Z}_{\geq 0}$, $\nu(x + y\zeta) = |x + y\zeta|^2$. Ισχυρίζομαι ότι η ν είναι σταθμη της E: Η συνθήκη (i) της σταθμης (σελ. 59), προφανώς ικανοποιείται. Θ' αποδείξω τώρα ότι ικανοποιείται και η (ii).

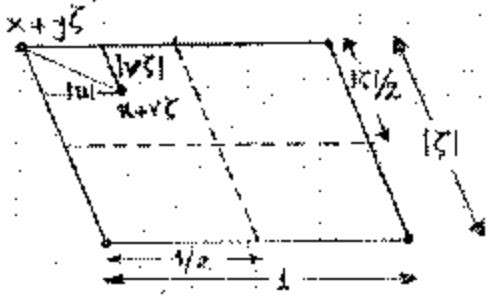
Έστω ότι $c + d\zeta$, $a + b\zeta \in E$, $a + b\zeta \neq 0$. Έχω να δείξω ότι υπάρχουν $x + y\zeta$, $p + q\zeta \in E$, τέτοια ώστε

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

$$\Leftrightarrow \{ p + q\zeta = 0 \text{ ή } \nu(p + q\zeta) < \nu(a + b\zeta).$$

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

κατ' ἀνάγκη, ἀπειραιοι). Τό $u+v\zeta$ ἀνήκει σ' ἕνα ἀπ' τά παραλληλόγραμμα (στό ἐσωτερικό του, ἐν γένει), τά ὁποῖα καλύπτουν τό μιγαδικό ἐπίπεδο. Ἔστω $x+y\zeta$ τό πλησιέστερο πρός τό $u+v\zeta$ κομβικό σημεῖο (βλ. σχῆμα τῆς σελ. 61, καθώς καί τή "μεσέθυνση" τοῦ παραλληλογράμμου, στό ὁποῖο ἀνήκει τό $u+v\zeta$, δίπλα).



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

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

Ἄρα, μένει νά δείξω ὅτι $|p+q\zeta|^2<|a+b\zeta|^2$.

Γιά $\zeta=i$ ἤ $i\sqrt{2}$ ἔχω:

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

Γιά $\zeta=\omega$ ἔχω:

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

Τό συμπέρασμα, λοιπόν, εἶναι ὅτι ἡ ἀπειραια περιοχή E εἶναι εὐκλείδια περιοχή καί, συνεπῶς (Θεώρημα 4), ἔχομε μονότροπη ἀνάλυση.

Ἐφαρμογές 1) "Ἀπόδειξε ὅτι τό μόνο τετράγωνο, τό ὁποῖο, αὐξανόμενο κατά 2 γίνεται κύβος, εἶναι τό 25" (ἀπό γράμμα τοῦ Fermat πρός τόν Wallis). Μ' ἄλλα λόγια, νά λυθεῖ ἡ διοφαντική (σέ ἀκεραίους) ἐξίσωση

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

καί, μάλιστα, νά δειχθεῖ ὅτι μοναδική λύση της εἶναι ἡ $|x|=5$, $y=3$.

§5

Γράφω την (1) υπό τη μορφή

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

και δουλεύω στην ακέραια περιοχή $\mathbb{Z}[\zeta]$. Επειδή η περιοχή αυτή είναι ευκλείδια, ισχύει η μονότροπη ανάλυση (θεώρημα 4), συνεπώς μπορούμε να κάνουμε "Αριθμητική". Θα χωρίζομαι, 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 ανάγωγα στοιχεία ταυτίζονται, σύμφωνα με την πρόταση 4). Άρα $\pi \mid (x+\zeta)-(x-\zeta)=2\zeta=-\zeta^3$, δηλαδή $\pi \mid \zeta$ (επειδή το π είναι πρώτος). Όμως το ζ είναι ανάγωγο (άσκηση ρουτίνας), δηλαδή η $\pi \mid \zeta$ συνεπάγεται ότι τα π, ζ είναι συνεταιρικά, δηλ. $\pi = \pm i\sqrt{2}$ (έχομε δει, σαν άσκηση, ότι οι μοναδίες της $\mathbb{Z}[\zeta]$ είναι μόνο οι ± 1). Επανέρχομαι 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 την ευχάριστη μιγαδική οχέση και πολλαπλασιάζοντας κατά μέλη βρίσκω $y^2 = 2(a^2+2b^2)$, άρα ο y είναι άρτιος. Τότε, από την (1), και ο x είναι άρτιος δηλαδή $y^3 - x^2 \equiv 0 \pmod 4$. Αυτό είναι άτοπο, διότι $y^3-x^2=2$. Άρα, οι παράγοντες στο αριστερό μέλος της (2) είναι, όντως, πρώτοι μεταξύ τους. Το γινόμενό τους είναι κύβος, άρα (σύμφωνα με άσκηση που έχομε κάνει) καθε παράγοντας είναι συνεταιρικό στοιχείο κάποιου κύβου. Τότε (επειδή οι μοναδες ± 1 είναι κύβοι) θα έχω μια οχέση της μορφής

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

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

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

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 αποδεικτέο.

2) Με εντελώς ανάλογο τρόπο μπορούμε να χειριστούμε και τη λύση της διοφαντικής εξίσωσης

$$x^2 + 5 = 2y^3, \tag{4}$$

οι σχέσεις, όμως, οι ανάλογες των (3) δεν θα έχουν λύση (σε ακεραίους m, n) και, συνεπώς, θα συμπεράνουμε ότι η (4) δεν έχει ακέραιες λύσεις. Κάνετε σαν άσκηση όλη αυτή τη διαδικασία. Όμως .... 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 τελείων τετραγώνων αν και μόνο αν είναι $\equiv 1 \pmod 4$.

Απόδειξη: Είναι $p \equiv 1$ ή $3 \pmod 4$. Αν $p \equiv 3 \pmod 4$, αποκλείεται 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 παλιότερης 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 ευκλείδια περιοχή $\mathbb{Z}[i]$, όπου έχω, λόγω της τελευταίας ισότητας, $p \mid (x+i)(x-i)$. Αν ο p ήταν πρώτος στην $\mathbb{Z}[i]$, θα έπρεπε $p \mid x+i$ είτε $p \mid x-i$. Δηλαδή, θα είχα κάποια σχέση $x+i = p(u+vi)$ είτε $x-i = p(u+vi)$, με $u, v \in \mathbb{Z}$. Τότε όμως (εξισώνοντας τους συντελεστές του i) $1 = \pm pv$, προφανώς άτοπο. Αφού ο p δεν είναι πρώτος, δεν είναι και ανάγωγο στοιχείο της $\mathbb{Z}[i]$ (πρώτα και ανάγωγα συμπίπτουν γιατί είμαστε σε περιοχή μονότροπης ανάλυσης), άρα υπάρχουν $\gamma, \delta \in \mathbb{Z}[i]$, όχι μονάδες, τέτοια ώστε $p = \gamma \cdot \delta$. Τότε (παίρνοντας συζυγείς μιγαδικούς) $p = \bar\gamma \cdot \bar\delta$ και, πολλαπλασιάζοντας κατά μέλη, $p^2 = |\gamma|^2 |\delta|^2$. Επειδή τα γ, δ δεν είναι μονάδες, είναι $|\gamma|, |\delta| > 1$, συνεπώς $|\gamma|^2 = |\delta|^2 = p$. Αν θέσω $\gamma = a+bi$, $a, b \in \mathbb{Z}$, τότε $a^2 + b^2 = p$, δ.ε.δ.

Μένει τώρα να αποδείξω ότι (για $p \equiv 1 \pmod 4$) υπάρχει $x \in \mathbb{Z}$ τ.ώ. $x^2 \equiv -1 \pmod p$.

Για να το αποδείξω δουλεύω στο σώμα $\mathbb{Z}_p$. Έχω $t^{p-1} - 1 = (t^{\frac{p-1}{2}} - 1)(t^{\frac{p-1}{2}} + 1)$ και το πολυώνυμο (του $\mathbb{Z}_p[t]$) στο αριστερό μέλος έχει ως ρίζες του όλα τα μη μηδενικά στοιχεία του $\mathbb{Z}_p$ ("μικρό θεώρημα του Fermat", το οποίο είδαμε παλιότερα σαν άσκηση). Άρα κάθε στοιχείο του $\mathbb{Z}_p^*$ είναι ρίζα ή του $t^{\frac{p-1}{2}} - 1$, ή του $t^{\frac{p-1}{2}} + 1$. Όμως, δεν είναι δυνατόν όλα τα στοιχεία του $\mathbb{Z}_p^*$ (πλήθους $p-1$) να είναι ρίζες του $t^{\frac{p-1}{2}} - 1$ (του οποίου ο βαθμός είναι $< p-1$), άρα υπάρχει $n \in \mathbb{Z}_p^*$, ρίζα του $t^{\frac{p-1}{2}} + 1$. Τότε $n^{\frac{p-1}{2}} + 1 = 0$ άρα $n^{\frac{p-1}{2}} \equiv -1 \pmod p$ και, θέτοντας $x = n^{\frac{p-1}{4}}$ ($\frac{p-1}{4} \in \mathbb{Z}$), έχω $x^2 \equiv -1 \pmod p$, δ.ε.δ.

§6

Αλγεβρικές επεκτάσεις

Ορισμός Αν R είναι δακτύλιος και K υπόσωμα του R, τό $x \in R$ λέγεται αλγεβρικό πάνω από K άν υπάρχει μή μηδενικό πολυώνυμο $f(t) \in K[t]$, τέτοιο ώστε $f(x)=0$.

Τό $L \supseteq K$ λέγεται αλγεβρική επέκταση του K άν είναι σώμα πού περιέχει τό K σάν υπόσωμα και κάθε $x \in L$ είναι αλγεβρικό πάνω από K.

Είναι φανερό ότι κάθε $a \in K$ είναι αλγεβρικό πάνω από K, αφού $f(a)=0$, όπου $f(t)=t-a$. Έστω K, R όπως παραπάνω. Ο R μπορεί να θεωρηθεί κατά προφανή τρόπο ένας K-διανυσματικός χώρος. Αν τό K είναι υπόσωμα του σώματος L και τό L είναι πεπερασμένης διάστασης θεωρούμενο σάν K-διανυσματικός χώρος, τότε τό L χαρακτηρίζεται πεπερασμένη επέκταση του K, και η διάσταση του L λέγεται βαθμός της επέκτασης L του K. Στα παρακάτω K είναι υπόσωμα του L.

Συμβολίζουμε με $K[x]$, όπου $x \in L$, το σύνολο του L, πού αποτελείται από τά στοιχεία της μορφής $a_0 + a_1 x + \cdots + a_n x^n$, $a_i \in K$. Είναι φανερό ότι τό $K[x]$, εφοδιασμένο με τήν πρόσθεση και τον πολλαπλασιασμό του L είναι δακτύλιος αντιμεταθετικός με μονάδα. Ισχύει τό εξής θεμελιώδες.

Θεώρημα 1 Αν τό $x \in L$ είναι αλγεβρικό πάνω από K, τότε ο δακτύλιος $K[x]$ είναι σώμα. Υπάρχει ένα μοναδικό ανάγωγο μονικό πολυώνυμο (μονικό σημαίνει "με συντελεστή μεγιστοβάθμιου όρου τό 1") $q(t) \in K[t]$, τέτοιο ώστε $q(x)=0$. Τό $K[x]$ είναι πεπερασμένη επέκταση του K, βαθμού ίσου με $n=\deg q$, και τά στοιχεία $1, x, \ldots, x^{n-1}$ παράγουν τον διανυσματικό χώρο $K[x]$ πάνω από K.

Απόδειξη. Πρώτα θά δείξουμε ότι κάθε μή μηδενικό στοιχείο του $K[x]$ έχει αντίστροφο. Πράγματι έστω $0 \neq y = g(x) \in K[x]$, όπου $g(t) \in K[t]$. Εξ υποθέσεως υπάρχει μή μηδενικό $f(t) \in K[t]$, τέτοιο ώστε $f(x)=0$. Αναλύουμε τό f σε γινόμενο ανάγωγων πολυωνύμων του $K[t]$ (Θ2, §4), $f = q_1 \cdots q_r$, όπότε θά πρέπει $q_i(x)=0$ για κάποιο $i \in \{1, \ldots, r\}$. Πολλαπλασιάζοντας με κατάλληλο στοιχείο του K τό $q_i(t)$ μπορούμε να πετύχουμε ανάγωγο μονικό πολυώνυμο $q(t) \in K[t]$ με $q(x)=0$.

Τώρα μπορούμε να δείξουμε ότι τά πολυώνυμα g και q είναι πρώτα μεταξύ τους. Πράγματι, άν δέν ήταν, τό q θά διαιρούσε τό g (ΠΘ, §4), όπότε $g(x)=0$, άτοπο.

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

Το $q(t)$ είναι το μοναδικό μονικό ανάγωγο πολυώνυμο του $K[t]$ που μηδενίζεται αν το t αντικατασταθεί απ' το x. Πράγματι, έστω ένα τέτοιο πολυώνυμο $p(t)$. Αν ήταν τα q και p πρώτα μεταξύ τους, τότε $q \cdot q' + p \cdot p' = 1$ για κάποια $q', p' \in K[t]$, δηλαδή $q(x)q'(x) + p(x)p'(x) = 1$ και $0 = 1$, άτοπο. Άρα, αφού δεν είναι πρώτα μεταξύ τους και είναι και ανάγωγα, θα πρέπει $p \mid q$ και $q \mid p$, δηλαδή θα πρέπει $q = a \cdot p$, $a \in K$. Επειδή όμως οι συντελεστές των μεγιστοβάθμιων όρων στα q, p είναι 1, θα πρέπει $a = 1$, δηλαδή $p = q$.

Μένει τώρα να δείξουμε ότι αν $q(t) = a_0 + a_1 t + \cdots + a_{n-1} t^{n-1} + t^n$, τότε τα $1, x, \ldots, x^{n-1}$ αποτελούν βάση του διανυσματικού χώρου $K[x]$ πάνω από K. Πρώτα παρατηρούμε ότι τα $1, x, \ldots, x^{n-1}$ είναι K-γραμμικώς ανεξάρτητα. Γιατί αν δεν ήταν θα είχαμε $b_{n-1} x^{n-1} + \cdots + b_1 x + b_0 = 0$ για κάποια $b_0, \ldots, b_{n-1} \in K$, που δεν είναι όλα 0. Άρα θα υπήρχε $h(t) \in K[t]$ με $h(x) = 0$. Τότε όμως θα υπήρχε και κάποιο ανάγωγο μονικό πολυώνυμο $p(t) \in K[t]$ με $p(x) = 0$, (p παράγοντας του h), δηλαδή $\partial p \leq \partial h \leq n-1$. Ειδικότερα, $p \neq q$ κι αυτό αντίκειται στη μοναδικότητα του q.

Μένει να δείξουμε ότι τα $1, x, \ldots, x^{n-1}$ παράγουν το $K[x]$. Γι' αυτό αρκεί να δείξουμε ότι παράγουν κάθε x^m με $m \geq n$. Για $m = n$ έχουμε $x^n = -a_{n-1} x^{n-1} - \cdots - a_1 x - a_0$ και το x^n παράγεται απ' τα $1, x, \ldots, x^{n-1}$. Επαγωγικά τώρα, έστω ότι το x^r, $r \geq n$ παράγεται απ' τα $1, x, \ldots, x^{n-1}$ και $x^r = b_{n-1} x^{n-1} + \cdots + b_1 x + b_0$, $b_i \in K$. Τότε

$$x^{r+1} = b_{n-1} x^n + b_{n-2} x^{n-1} + \cdots + b_1 x^2 + b_0 x = b_{n-1}(-a_{n-1} x^{n-1} - \cdots - a_1 x - a_0) + b_{n-2} x^{n-2} + \cdots + b_1 x^2 + b_0 x$$

δηλαδή και το x^{r+1} παράγεται απ' τα $1, x, \ldots, x^{n-1}$. ■

Το $q(t) \in K[t]$ που περιγράφεται στην εκφώνηση του θεωρήματος 1 λέγεται <u>ελάχιστο πολυώνυμο του x πάνω από K</u>.

Έστω τώρα ότι $x_1, \ldots, x_r \in L$. Με $K[x_1, \ldots, x_r]$ θα συμβολίζουμε το υποσύνολο του L που αποτελείται απ' όλα τα πεπερασμένα αθροίσματα στοιχείων του L της μορφής $a x_1^{n_1} \cdots x_r^{n_r}$, $a \in K$, $n_i \geq 0$ για κάθε $i = 1, \ldots, r$. Το $K[x_1, \ldots, x_r]$ με τις πράξεις του L γίνεται αντιμεταθετικός δακτύλιος 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 ισχύει*

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

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

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_iz_j, $1\le i\le n$, $1\le j\le m$ είναι μια K-βάση του M. Πραγματικά, πρώτα δείχνουμε ότι το σύνολο των y_iz_j παράγει τον M πάνω από το K: Έστω $u\in M$. Τότε $u=\alpha_1z_1+\alpha_2z_2+\dots+\alpha_mz_m$, $\alpha_i\in L$. Αλλά για κάθε $i\in\{1,\dots,m\}$

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

Αντικαθιστώντας αυτές τις εκφράσεις των α_i στην παραπάνω έκφραση του u βλέπουμε ότι το u γράφεται σαν γραμμικός συνδυασμός των y_iz_j, $1\le i\le n$, $1\le j\le m$ με συντελεστές από το K.

Τώρα δείχνουμε την ανεξαρτησία του συνόλου των y_iz_j πάνω από το K: Έστω

$$b_{11}y_1z_1+b_{12}y_1z_2+\dots+b_{1m}y_1z_m+b_{21}y_2z_1+b_{22}y_2z_2+\dots+b_{2m}y_2z_m+\dots+b_{n1}y_nz_1+b_{n2}y_nz_2+\dots+b_{nm}y_nz_m=0,\quad b_{ij}\in K.$$

Τότε,

$$\sum_{i=1}^{m}(b_{1i}y_1+b_{2i}y_2+\dots+b_{ni}y_n)z_i=0$$

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

$$b_{1i}y_1+b_{2i}y_2+\dots+b_{ni}y_n=0,\quad \text{για κάθε } i=1,\dots,m.$$

Επειδή τα y_j είναι K-ανεξάρτητα, $b_{1i}=b_{2i}=\dots=b_{ni}=0$. Έτσι, όλα τα b_{ij} είναι 0, δηλαδή τα y_iz_j $1\le i\le n$, $1\le j\le m$ είναι K-ανεξάρτητα ■

Θεώρημα 3 *Αν $x_1,\dots,x_r\in L$, έτσιοι ώστε το x_i είναι αλγεβρικό πάνω στο K και για $1\le i\le r$ το x_i είναι αλγεβρικό πάνω στο $K[x_1,\dots,x_{i-1}]$, (ειδικότερα, 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 (ειδικότερα, είναι σώμα).*

Απόδειξη. Συμφωνα 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 $K[x_1]$, θα $K[x_1,x_2]$ θα'ναι πεπερασμένη επέκταση του $K[x_1]$, άρα (θεωρ.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 $K[x_1,x_2]$.

Όμως είδαμε ότι $K[x_1, x_2]$ είναι πεπερασμένη επέκταση του K, άρα (θεωρ. 2) $K[x_1, x_2, x_3]$ είναι πεπερασμένη επέκταση του K. Προχωρώντας μ' αυτό τον τρόπο φτάνουμε τελικά στο συμπέρασμα ότι $K[x_1, \dots, x_\nu]$ 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 $x \in L$. Επειδή είναι αδύνατο να' ναι άπειρα στοιχεία του L που να' ναι K-ανεξάρτητα, θα' ναι άπειρος $n \geq 1$, τέτοιος ώστε τα $1, x, \dots, x^n$ να' ναι K-εξαρτημένα. Άρα υπάρχουν $b_0, b_1, \dots, b_n \in K$, όχι όλα 0 με $b_0 + b_1 x + \dots + b_n x^n = 0$. Δηλ. υπάρχει μη μηδενικό πολυώνυμο $f(t) \in K[t]$ με $f(x) = 0$, δηλαδή το x 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. Αρκεί να' δείξουμε ότι αν $x, y \in A$, τότε $x+y$, $x-y$, $xy \in A$ καθώς επίσης και $x^{-1} \in A$ (αν $x \neq 0$). Αφού τα x, y είναι αλγεβρικά πάνω στο K, έπεται απ' το θεώρημα 2 ότι $K[x, y]$ είναι πεπερασμένη επέκταση του K, δηλαδή, απ' το θεώρημα 3, $K[x, y]$ είναι αλγεβρική επέκταση του K. Όμως $x+y$, $x-y$, xy είναι στοιχεία του $K[x, y]$, καθώς επίσης και το $x^{-1} \in K[x, y]$ (για $x \neq 0$), δηλαδή τα $x+y$, $x-y$, xy, x^{-1} είναι αλγεβρικά πάνω στο K, δηλ. ανήκουν στο A. ■

Αν παίρναμε σαν L το $\mathbb{C}$ και σαν K το $\mathbb{Q}$ τότε το A (του θεωρήματος 3.5) είναι το σώμα των αλγεβρικών αριθμών. Δηλ. ένας μιγαδικός αριθμός χαρακτηρίζεται αλγεβρικός αριθμός αν είναι ρίζα ενός πολυωνύμου με ρητούς συντελεστές. Στην αντίθετη περίπτωση χαρακτηρίζεται υπερβατικός αριθμός.

Ο απλούστερος τρόπος για ν' αποδείξουμε ότι το σύνολο των υπερβατικών αριθμών είναι $\neq \emptyset$ (δηλ. ότι το A είναι γνήσιο υποσώμα του $\mathbb{C}$) είναι συνολοθεωρητικός και έμμεσος (Cantor): Αποδείχνουμε πρώτα ότι το $\mathbb{R}$ είναι μη αριθμήσιμο σύνολο (δεν υπάρχει δηλ. αμφιμονοσήμαντη, επί απεικόνιση μεταξύ του $\mathbb{R}$ και του $\mathbb{N}$) και μετά

ότι το A είναι αριθμητικό. Και συνέπεια, το A είναι όχι μόνο γνήσιο υποσύνολο του $\mathbb{C}$ αλλά γνήσιο υποσύνολο και του $\mathbb{R}$.

Το μειονέκτημα της παραπάνω μεθόδου είναι ότι δε βρίσκομε μ' αυτή έστω και ένα υπερβατικό αριθμό, μόνο που αντιληφθήκαμε την ύπαρξή τους. Ο Liouville για πρώτη φορά, το 1844, "κατασκεύασε" υπερβατικό αριθμό:

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

Αργότερα ο Hermite απόδειξε ότι ο e είναι υπερβατικός και ο Lindemann απόδειξε την υπερβατικότητα του π.

Ασκήσεις

Στις παρακάτω ασκήσεις, καθώς επίσης και σ' όλα τα υπόλοιπα κεφάλαια, όταν γράφομε $L:K$ θα εννοούμε ότι το K είναι υπόσωμα του σώματος L, αλλοιώς, το L είναι επέκταση του K. Με $[L:K]$ θα συμβολίζομε το βαθμό της επέκτασης.

1 Να βρεθούν οι βαθμοί των επόμενων επεκτάσεων: $\mathbb{C}:\mathbb{Q}$, $\mathbb{R}[\sqrt{5}]:\mathbb{R}$, $\mathbb{Q}[\sqrt[3]{2}]:\mathbb{Q}$, $\mathbb{Q}[\sqrt{5},\sqrt{7}]:\mathbb{Q}$, $\mathbb{Q}[\sqrt[7]{3}]:\mathbb{Q}$.

2 Αν $[L:K]$ πρώτος, τότε δεν υπάρχουν σώματα M, $M:K$ και $L:M$ (γνησίως).

3 Αν $[L:K]=1$, τότε $L=K$.

4 Αν $L:K$ πεπερασμένη επέκταση και έχομε τις διαδοχικές επεκτάσεις $L:k_r:k_{r-1}:\cdots:k_1:K$, τότε $[L:K]=[L:k_r][k_r:k_{r-1}]\cdots[k_2:k_1][k_1:K]$.

5 Δείξτε ότι η επέκταση $L:K$ είναι πεπερασμένη αν και μόνο αν $L=K[\alpha_1,\ldots,\alpha_r]$, όπου r πεπερασμένο και κάθε α_i είναι αλγεβρικό πάνω από K.

6 Αν A είναι το σώμα των αλγεβρικών αριθμών, δείξτε ότι η επέκταση $A:\mathbb{Q}$ δεν είναι πεπερασμένη (Κριτήριο Eisenstein για την ύπαρξη ανάγωγων πολυωνύμων πάνω από $\mathbb{Q}$, οσοδήποτε μεγάλου βαθμού).

7 Υποθέτοντας ότι κάθε πολυώνυμο του $\mathbb{C}[t]$ έχει ρίζα στο $\mathbb{C}$, δείξτε ότι κάθε πολυώνυμο του $A[t]$ έχει ρίζα στο A. Δείξτε, κατά συνέπεια, ότι δεν υπάρχει γνήσια αλγ. επέκταση του A.

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

9 Βρείτε μια $\mathbb{Q}$-βάση του $\mathbb{Q}[\sqrt{1+\sqrt{3}}]$, άρα βρείτε το βαθμό $[\mathbb{Q}[\sqrt{1+\sqrt{3}}]:\mathbb{Q}]$.

10 Αν $[L:K]$ πρώτος, τότε υπάρχει $\alpha\in L$ τέτοιο ώστε $L=K[\alpha]$. (Το L τότε λέγεται απλή επέκταση του K.)

Εφαρμογές

Κατασκευές με κανόνα και διαβήτη

Έστω Σ_0 ένα σύνολο σημείων του $\mathbb{R}^2$ (επιπέδου). Λέμε ότι ένα σημείο του επιπέδου είναι <u>άμεσα κατασκευάσιμο</u> (με κανόνα και διαβήτη) από το Σ_0 αν αυτό είναι σημείο τομής δύο ευθειών, ή μιας ευθείας με ενός κύκλου, ή δύο κύκλων, οι οποίοι κύκλοι ή ευθείες προκύπτουν, αντίστοιχα, από τις εξής γεωμετρικές "πράξεις":
1) Με κέντρο σημείο του Σ_0 και άκτινα την απόσταση δύο σημείων του Σ_0 γράφεται κύκλος.
2) Γράφεται η ευθεία που περνά από δύο σημεία του Σ_0.
Λέμε τώρα ότι <u>ένα σημείο $\sigma \in \mathbb{R}^2$ κατασκευάζεται από το Σ_0</u> αν υπάρχει πεπερασμένο πλήθος σημείων $\sigma_1, \sigma_2, \dots, \sigma_n = \sigma$ του $\mathbb{R}^2$, τέτοια ώστε το σ_i να είναι άμεσα κατασκευάσιμο από το Σ_0 και για $2 \le i \le n$, το σ_i να είναι άμεσα κατασκευάσιμο από το $\Sigma_0 \cup \{\sigma_1, \dots, \sigma_{i-1}\}$.

Συμβολίζουμε τώρα με K_0 το υποσώμα του $\mathbb{R}$ που παράγεται από τις συντεταγμένες όλων των σημείων του Σ_0 (το K_0 είναι δηλ. το ελάχιστο υποσώμα του $\mathbb{R}$ που περιέχει τις συντεταγμένες όλων των σημείων του Σ_0 · με άλλα λόγια, K_0 είναι η τομή όλων των υποσωμάτων του $\mathbb{R}$, που περιέχουν τις συντεταγμένες όλων των σημείων του Σ_0).

<u>Θεώρημα 5</u> <u>Αν οι συντεταγμένες όλων των σημείων ενός συνόλου $\Sigma \subseteq \mathbb{R}^2$ περιέχονται σ' ένα υποσώμα K του $\mathbb{R}$ και το σημείο $\sigma = (x, y)$ είναι άμεσα κατασκευάσιμο, τότε τα x, y είναι αλγεβρικά πάνω από K και η επέκταση $K[x,y] : K$ είναι βαθμού 1 ή 2</u> (πρβλ. θεώρημα 3).

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

Απόδειξη. Θ' αποδείξουμε το θεώρημα στην "δυσκολότερη" περίπτωση που το σ είναι τομή δύο κύκλων (οι κύκλοι εννοείται ότι έχουν χαραχτεί όπως μάς 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 ακτίνες των κύκλων και z_i είναι η απόσταση των σημείων (α_i, β_i), (α_i', β_i') του Σ (όπότε $\alpha_i, \beta_i, \alpha_i', \beta_i' \in K$), τότε $z_i^2 = (\alpha_i - \alpha_i')^2 + (\beta_i - \beta_i')^2 \in K$.

Οἱ συντεταγμένες (x,y) τοῦ σ' δὰ ἐπαληθεύων λοιπὸν τὶς σχέσεις

$$(x-x_1)^2+(y-y_1)^2=r_1^2 \quad , \quad (x-x_2)^2+(y-y_2)^2=r_2^2$$

ἢ, ἰσοδύναμα

$$(x-x_1)^2+(y-y_1)^2=r_1^2 \quad , \quad 2(x_2-x_1)x+2(y_2-y_1)y+x_1^2-x_2^2+y_1^2-y_2^2=r_1^2-r_2^2$$

ὅπου οἱ συντελεστὲς καὶ στὶς δυὸ ἐξισώσεις ἀνήκουν στὸ K. Ἀπαλείφοντας τὸ y π.χ. μεταξὺ τῶν δύο ἐξισώσεων βρίσκομε μιὰ ἐξίσωση, τὸ πολὺ δευτεροβάθμια ὡς πρὸς x, μὲ συντελεστὲς ἀπ' τὸ K. Ἔτσι, τὸ x εἶναι ἀλγεβρικὸ πάνω στὸ K καὶ $[K[x]:K]=1$ ἢ 2. Ὅμοια ἰσχύουν γιὰ τὸ y. Τότε (θεώρημα 3) $K[x,y]$ εἶναι πεπερασμένη ἐπέκταση τοῦ K καὶ (βλ. θεώρημα 2),

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

Ἐπειδὴ $K[x,y]:K[y]$ εἶναι ἡ ἐπέκταση $(K[y])[x]:K[y]$ καὶ τὸ x εἶναι ρίζα ἑνὸς δευτεροβάθμιου ὡς πολὺ πολυωνύμου τοῦ $K[t]$, δὰ εἶναι ρίζα ἑνὸς, τὸ πολὺ δευτεροβάθμιου πολυωνύμου τοῦ $(K[y])[t]$, ἄρα ὁ βαθμὸς τῆς ἐπέκτασης $K[x,y]:K[y]$ εἶναι 1 ἢ 2. Ἀφ' ἑτέρου $[K[y]:K]=1$ ἢ 2, κι ἔχομε ἔτσι τὸ ἀποδεικτέο. ■

Ἔστω τώρα ὅτι τὸ σ εἶναι κατασκευάσιμο ἀπ' τὸ σύνολο Σ_0 καὶ $\sigma_1,\sigma_2,\dots,\sigma_n=\sigma$ τὰ σημεῖα ποὺ μᾶς δόθηκαν ἀπ' τὸ Σ_0 στὴν κατασκευὴ τοῦ σ. Θέτομε $\sigma_i=(x_i,y_i)$ κι ἔστω K_0 τὸ ὑπόσωμα τοῦ R ποὺ βρίσκεται πρὶν ἀπὸ τὴν ἐκφώνηση τοῦ θεωρήματος 4α. Τότε ἔχομε τὶς ἑξῆς διαδοχικὲς ἐπεκτάσεις:

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

Μὲ διαδοχικὴ ἐφαρμογὴ τοῦ θεωρήματος 2 (βλ. ἄσκηση 4) καὶ λόγῳ τοῦ θεωρήματος 5 δὰ ἔχομε $[K_n:K_0]=[K_n:K_{n-1}][K_{n-1}:K_{n-2}]\cdots[K_2:K_1][K_1:K_0]=$ δύναμη τοῦ 2. Ἔτσι ἀποδείξαμε τὸ ἑξῆς

<u>Θεώρημα 6</u> <u>Ἂν τὸ σημεῖο σ κατασκευάζεται ἀπ' τὸ σύνολο σημείων Σ_0 καὶ K_0 εἶναι τὸ ἐλάχιστο σῶμα ποὺ περιέχει τὶς συντεταγμένες δύο τῶν σημείων τοῦ Σ_0, τότε ὑπάρχει πεπερασμένη ἐπέκταση K τοῦ K_0 ποὺ περιέχει τὶς συν/μένες τοῦ σ καὶ εἶναι βαθμοῦ ἴσου μὲ δύναμη τοῦ 2.</u>

Τώρα ἔχομε ὅλα τ' ἀπαραίτητα ἐφόδια γιὰ ν' ἀποδείξομε ὅτι εἶναι ἀδύνατο νὰ δοθεῖ λύση μὲ κανόνα καὶ διαβήτη στὰ τρία περίφημα προβλήματα τῆς ἀρχαιότητας: Διπλασιασμὸς

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

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

Απόδειξη. Ας υποθέσουμε ότι μας δίνεται ο μοναδιαίος κύβος. Για να κατασκευάσουμε το διπλασιασμό του πρέπει να κατασκευάσουμε ένα ευθύγραμμο τμήμα (η ακμή του νέου κύβου) με μήκος $\sqrt[3]{2}$. Εδώ τα μόνα μας δεδομένα είναι το μοναδιαίο μήκος (η ακμή του αρχικού κύβου). Άρα $\Sigma_0 = \{(0,0), (1,0)\}$, δηλαδή $K_0 = \mathbb{Q}$.
Πρέπει να κατασκευάσουμε με κανόνα και διαβήτη το σημείο $\sigma = (x, 0)$ όπου $x = \sqrt[3]{2}$. Αν αυτό γινόταν, τότε θα υπήρχε πεπερασμένη επέκταση K του $\mathbb{Q}$ με $x \in K$ και $[K : \mathbb{Q}] =$ δύναμη του 2. Όμως το x είναι ρίζα του $t^3 - 2 \in \mathbb{Q}[t]$, που είναι ανάγωγο (στο $\mathbb{Q}[t]$), λόγω του κριτηρίου του Eisenstein, δηλαδή (Θεώρημα 1) $[\mathbb{Q}[x] : \mathbb{Q}] = 3$. Είναι φανερό όμως ότι $K \supseteq \mathbb{Q}[x]$, άρα έχουμε τις διαδοχικές επεκτάσεις $K : \mathbb{Q}[x]$ και $\mathbb{Q}[x] : \mathbb{Q}$ και κατά συνέπεια,

δύναμη του $2 = [K : \mathbb{Q}] = [K : \mathbb{Q}[x]] \cdot [\mathbb{Q}[x] : \mathbb{Q}] =$ πολλαπλάσιο του 3,

άτοπο. ■

Θεώρημα 8 Η γωνία $\frac{\pi}{3}$ δεν είναι δυνατό να τριχοτομηθεί με κανόνα και διαβήτη.

Απόδειξη. Έχουμε στη διάθεσή μας το μοναδιαίο (τριγωνομετρικό) κύκλο, δηλαδή μια γωνία είναι κατασκευάσιμη αν και μόνο αν μπορούμε να κατασκευάσουμε ευθύγραμμο τμήμα ίσο με το συνημίτονό 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 $x = \text{συν}\frac{\pi}{9}$. Αν αυτό μπορούσε να γίνει με κανόνα και διαβήτη, τότε θα υπήρχε επέκταση $K : \mathbb{Q}$ με $x \in K$ και $[K : \mathbb{Q}] =$ δύναμη του 2. Όμως, λόγω της σχέσης $\text{συν}3\theta = 4\text{συν}^3\theta - 3\text{συν}\theta$ θα έχουμε (για $\theta = \frac{\pi}{9}$) $\frac{1}{2} = 4x^3 - 3x$ ή

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

και το x είναι, λοιπόν, ρίζα του $8t^3 - 6t - 1$, που είναι άνωγο στο $\mathbb{Q}[t]$. (Αν δεν ήταν, θάπρεπε να έχει τουλάχιστον ένα πρωτοβάθμιο παράγοντα, άρα τουλάχιστον μια ρητή ρίζα· όμως οι μόνες πιθανές ρητές ρίζες του πολυωνύμου αυτού είναι οι ± 1, $\pm \frac{1}{2}$, $\pm \frac{1}{4}$, $\pm \frac{1}{8}$, κι άμεσα επαληθεύεται ότι κανείς απ' αυτούς τους ρητούς δεν είναι ρίζα του). Άρα $[\mathbb{Q}[x] : \mathbb{Q}] = 3$, και όπως στο Θεώρημα 7 συμπεραίνουμε άτοπο. ■

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

Απόδειξη. Μπορούμε να υποθέσουμε ότι μας δίνουν το μοναδιαίο κύκλο. Το πρόβλημα του τετραγωνισμού του συνίσταται στο να κατασκευάσουμε ένα τετράγωνο με εμβαδόν ίσο με το εμβαδόν του κύκλου, που είναι π. Άρα πρέπει να κατασκευάσουμε ευθύγραμμο τμήμα μήκους $\sqrt{\pi}$, δηλ. να κατασκευάσουμε το σημείο $\sigma = (x, 0)$, όπου $x = \sqrt{\pi}$.

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

Αλλά τότε (θεώρημα 6.) θα υπήρχε πεπερασμένη επέκταση του $\mathbb{Q}$ που θα περιείχε το π και, κατα συνέπεια (θεώρημα 3.), ο π θα ήταν αλγεβρικός πάνω στο $\mathbb{Q}$, δηλ. αλγεβρικός αριθμός. Αλλά όμως αυτό έρχεται στο διάφορο θεώρημα του Lindemann ότι ο π είναι υπερβατικός αριθμός. ■

Ασκήσεις

1. Αποδείξτε ότι είναι αδύνατη με κανόνα και διαβήτη η κατασκευή του κανονικού εννεαγώνου.

2. Αποδείξτε ότι η γωνία θ μπορεί να τριχοτομηθεί με κανόνα και διαβήτη, αν και μόνο αν το πολυώνυμο $4t^3 - 3t - \sigma\upsilon\nu\theta$ είναι σύνδετο στο $\mathbb{Q}(\sigma\upsilon\nu\theta)$. (Αν L είναι επέκταση του K και $\alpha \in L$, συμβολίζουμε με $K(\alpha)$ το ελάχιστο υποσώμα του L που περιέχει το σύνολο $K \cup \{\alpha\}$. Αποτελείται από όλα τα στοιχεία του L της μορφής $(x_n\alpha^n + \cdots + x_1\alpha + x_0)(y_m\alpha^m + \cdots + y_1\alpha + y_0)^{-1}$, όπου $x_i, y_j \in K$ και η δεύτερη παρένθεση είναι $\neq 0$. Για α αλγεβρικό πάνω στο K είναι, προφανώς, $K(\alpha) = K[\alpha]$.)

3. Κάνοντας χρήση του τύπου για το $\sigma\upsilon\nu 5\theta$ κατασκευάστε με κανόνα και διαβήτη το κανονικό πεντάγωνο. ($\sigma\upsilon\nu 5\theta = 16\sigma\upsilon\nu^5\theta - 20\sigma\upsilon\nu^3\theta + 5\sigma\upsilon\nu\theta$.)