Πρόοδος στη Θεωρία Δακτυλίων
Απρίλιος 2003

1. *Να δείξετε ότι:*
(α) *Κάθε ιδεώδες του δακτύλιου $\mathbb{Z}$ είναι κύριο.*
(β) *Αν $a_1, \ldots a_n$ είναι μη μηδενικοί ακέραιοι τότε $(a_1, \ldots, a_n) = (d)$ αν και μόνο αν ο $|d|$ είναι ο μέγιστος κοινός διαιρέτης τους, και ότι $(a_1) \cap \cdots \cap (a_n) = (m)$ αν και μόνο αν ο $|m|$ είναι το ελάχιστο κοινό πολλαπλάσιό τους.*
(γ) *Να γράψετε σαν κύρια ιδεώδη τα $(17, 15 \cdot 10^{10})$, $(3003, 3289)$, $\big(\,19, (18!)^{18} - 1\,\big)$.*

ΛΥΣΗ:(α) Θεωρούμε ένα οποιοδήποτε ιδεώδες $I \subseteq \mathbb{Z}$. Αν $I = (0)$ τότε είναι κύριο. Αν $I \neq (0)$ τότε θα περιέχει μη μηδενικά στοιχεία. Έστω $M = \{|a| : a \in I, a \neq 0\}$. Τότε $M \neq \emptyset$, και σαν σύνολο φυσικών αριθμών θα έχει ένα μικρότερο στοιχείο $|a| \in M$. Θα δείξουμε ότι $(a) = I$. Αφού, $a \in I$ τότε $(a) \subseteq I$. Αρκεί συνεπώς να δείξουμε ότι $I \subseteq (a)$. Έστω $x \in I$. Από την ταυτότητα της διαίρεσης στο $\mathbb{Z}$ θα υπάρχουν $b, c \in \mathbb{Z}$ με

$$x = ab + c, \qquad |c| < |a| \tag{1}$$

Αλλά $x \in I, a \in I$ οπότε $ab \in I$ και τελικά $c = x - ab \in I$. Πρέπει $c = 0$ γιατί διαφορετικά θα βρίσκαμε ένα στοιχείο του ιδεώδους διαφορετικό από 0 με απόλυτη τιμή μικρότερη από αυτήν του a και αυτό δεν μπορεί να συμβαίνει λόγω της εκλογής του a. Συνεπώς $x = ab$ δηλαδή $x \in (a)$.

(β) Έστω $(a_1, \ldots, a_n) = (d)$. Αλλά $(d) = (|d|)$ συνεπώς $(a_1, \ldots, a_n) = (|d|)$. Επειδή $a_1, \ldots, a_n \in (a_1, \ldots, a_n)$ θα έχουμε $a_1, \ldots, a_n \in (|d|)$ που σημαίνει ότι ο $|d|$ είναι κοινός διαιρέτης των $a_1, \ldots . a_n$. Μένει να δείξουμε ότι είναι ο μέγιστος κοινός διαιρέτης. Ας θεωρήσουμε έναν οποιοδήποτε άλλο κοινό διαιρέτη d' των $a_1, \ldots . a_n$. Επειδή $|d| \in (a_1, \ldots . a_n)$ ο $|d| = x_1 a_1 + \cdots + x_n a_n$ για κάποια $x_1, \ldots, x_n \in \mathbb{Z}$. Αλλά τότε $d' | d$ και τελειώσαμε.
Όμοια αν $(a_1) \cap \cdots \cap (a_n) = (m) = (|m|)$ τότε ο $|m| \in (a_1), \ldots, |m| \in (a_n)$ δηλαδή ο $|m|$ είναι κοινό πολλαπλάσιο των $a_1, \ldots, a_n$. Μένει να δείξουμε ότι είναι ελάχιστο κοινό πολλαπλάσιο τους. Ας πάρουμε οποιοδήποτε άλλο κοινό πολλαπλάσιο τους m' τότε $m' \in (a_1) \cap \cdots \cap (a_n) = (m)$ άρα $m' \in (m)$ άρα ο $m | m'$ και τελειώσαμε.

(γ) $15 \cdot 10^{10} = 3 \cdot 2^{10} \cdot 5^{11}$ συνεπώς ο μέγιστος κοινός διαιρέτης των $17, 15 \cdot 10^{10}$ είναι 1 και άρα (από **(β)**) $(17, 15 \cdot 10^{10}) = (1) = \mathbb{Z}$.
Για να βρούμε τον μέγιστο κοινό διαιρέτη των $3003, 3289$ μάλλον συμφέρει ο αλγόριθμος του Ευκλείδη:

$$\mathbf{3289} = 1 \cdot \mathbf{3003} + \mathbf{286}$$
$$3003 = 10 \cdot \mathbf{286} + \mathbf{143}$$
$$286 = 2 \cdot \mathbf{143} + 0$$

άρα (3289, 3003)=(143).
Τέλος, Ο 19 δεν διαιρεί τον 18! και από το θεώρημα του Fermat θα διαιρεί τον $(18!)^{18} - 1$ άρα $(19, (18!)^{18} - 1) = (19)$. ■

2. *Ας υποθέσουμε ότι σε ένα δακτύλιο R έχει οριστεί μία σχέση ισοδυναμίας $\sim$ τέτοια ώστε: Αν $x \sim x'$, $y \sim y'$ τότε $x + y \sim x' + y'$ και $xy \sim x'y'$. Να δείξετε ότι:*
(α) *$x \sim y$ αν και μόνο αν $x - y \sim 0$.*
(β) *Υπάρχει ένα μοναδικό ιδεώδες $I \subset R$ ώστε $R/I = R/\sim$.*

ΛΥΣΗ: (α) Οι υποθέσεις μου για την $\sim$ είναι ότι εκτός από σχέση ισοδυναμίας θα έχω ότι μπορώ να προσθέτω και να πολλαπλασιάζω κατά μέλη ισοδυναμίες:

$$\begin{array}{l} x \sim y \\ \underline{x' \sim y'\qquad\quad} \\ x + x' \sim y + y' \end{array} \qquad\qquad \begin{array}{l} x \sim y \\ \underline{x' \sim y'\quad\ } \\ xx' \sim yy' \end{array}$$

Αν $x \sim y$ επειδή[1] $-y \sim -y$ θα έχουμε $x + (-y) \sim y + (-y)$ δηλαδή $x - y \sim 0$. Αν $x - y \sim 0$ αφού $y \sim y$ προσθέτοντας κατά μέλη $x \sim y$.

(β) Θέτω $I = \{x : x \sim 0\}$. Αρκεί να δείξω ότι το I είναι ιδεώδες. Αν $x \in I$ τότε $x \sim 0$ άρα $0 \sim x$, $-x \sim -x$ και αφού από υπόθεση μπορώ να προσθέτω κατά μέλη, προσθέτω κατά μέλη και έχω ότι $-x \sim 0$ δηλαδή ότι $-x \in I$. Άρα αν $x, y \in I$ τότε $x, -y \in I$ και προσθέτοντας πάλι κατά μέλη $x - y \sim 0$ δηλαδή $x - y \in I$.
Επίσης, αν $a \in I$ και $r \in R$ τότε $a \sim 0$ και $r \sim r$ και αφού από υπόθεση μπορώ και πολλαπλασιάζω κατά μέλη $ar \sim 0$ δηλαδή $ar \in I$.
Τέλος από (α), $x \sim y$ ισοδυναμεί $x - y \sim 0$ που ισοδυναμεί με $x - y \in I$ που ισοδυναμεί $x \in y + I$. Άρα, $R/_\sim = R/I$. Αν υπήρχαν δύο ιδεώδη I, J με $R/I = R/_\sim = R/J$ τότε το R/I ταυτίζεται με το R/J άρα αυτά τα σύνολα έχουν το ίδιο 0, άρα $I = J$. ■

[1] κάθε στοιχείο είναι ισοδύναμο με τον εαυτό του

3. *Έστω R, R' δακτύλιοι, $f : R \to R'$ επιμορφισμός και I, J ιδεώδη του R. Να δείξετε ότι:*

(α) Το $f(I)$ είναι ιδεώδες και $f(I+J) = f(I) + f(J)$

(β) $f(I \cap J) \subseteq f(I) \cap f(J)$ και αν συμβαίνει $I \supseteq \mathrm{Ker} f$ είτε $J \supseteq \mathrm{Ker} f$ θα ισχύει η ισότητα.

(γ) Αν $I \supseteq \mathrm{Ker} f$ τότε $I = f^{-1}(f(I))$.

ΛΥΣΗ:(α) Αν $x, y \in f(I)$ τότε $x = f(a), y = f(b)$ για κάποια $a, b \in I$ άρα $x - y = f(a) - f(b) = f(a-b)$ και αφού $a - b \in I$ έχω ότι $x - y \in I$.
Επίσης αν $x \in f(I)$ και $y \in R'$ τότε θα υπάρχει $a \in I$ με $x = f(a)$ και αφού ο f είναι επί θα υπάρχει και ένα $r \in R$ με $f(r) = y$ άρα $xy = f(a)f(r) = f(ar)$. Επειδή $a \in I$ θα έχω ότι $ar \in I$ και συνεπώς $xy \in f(I)$.

$$\begin{aligned}
& x \in f(I+J) && \Leftrightarrow \\
& \exists c \in I+J \ \text{ ώστε } \ x = f(c) && \Leftrightarrow \\
& \exists a \in I, \exists b \in J \ \text{ ώστε } \ x = f(a+b) && \Leftrightarrow \\
& \exists a \in I, \exists b \in J \ \text{ ώστε } \ x = f(a) + f(b) && \Leftrightarrow \\
& x \in f(I) + f(J)
\end{aligned}$$

(β) Αφού $I \cap J \subset I, I \cap J \subset J$ θα έχουμε $f(I \cap J) \subseteq f(I)$, $f(I \cap J) \subseteq f(J)$ και άρα $f(I \cap J) \subseteq f(I) \cap f(J)$. (δεν χρειάζεται να υποθέσετε τίποτα για την f και τα I, J !!!!). Αν τυχαίνει πχ

$$I \supseteq \mathrm{Ker} f \tag{2}$$

και πάρουμε $x \in f(I) \cap f(J)$ τότε

$$\exists a \in I, \exists b \in J \ \text{ ώστε } \ x = f(a) = f(b) \tag{3}$$

Από την (3) θα έχουμε $f(a) - f(b) = 0$ και αφού η f είναι ομομορφισμός $f(a-b) = 0$ δηλαδή $a - b \in \mathrm{Ker} f$, άρα $a - b \in I$ (Λόγω της (2)). Αλλά $a - b \in I, a \in I$ συνεπώς και $b \in I$, οπότε $b \in I \cap J$, άρα $x = f(b) \in f(I \cap J)$.

(γ) ■

4. *Ένα στοιχείο a ενός δακτυλίου R λέγεται* ***μηδενοδύναμο*** *αν υπάρχει κάποιος φυσικός n με $a^n = 0$. Έστω M το σύνολο όλων των μηδενοδύναμων στοιχείων ενός αντιμεταθετικού δακτύλιου.*
(α) *Το M είναι ιδεώδες του R. (Υπόδειξη: Αν $a^3 = 0, b^2 = 0$ τότε $(a-b)^5 = 0$, γενικά να χρησιμοποιήσετε το διώνυμο του Νεύτωνα.)*
(β) *Το R/M δεν έχει μηδενοδύναμα στοιχεία εκτός από το μηδέν του.*
(γ) *Αν p_1, p_2, p_3 είναι πρώτοι διαφορετικοί ανά δύο δείξτε ότι οι $\mathbb{Z}_{p_1}$, $\mathbb{Z}_{p_1p_2}$, $\mathbb{Z}_{p_1p_2p_3}$ δεν έχουν μηδενοδύναμα στοιχεία εκτός από το μηδενικό στοιχείο τους. Μπορείτε να διατυπώσετε μία ικανή και αναγκαία συνθήκη για το πότε ο $\mathbb{Z}_n$ έχει μηδενοδύναμα στοιχεία $\neq 0$;*
(δ) *Να βρείτε το σύνολο M των μηδενοδύναμων στοιχείων του $\mathbb{Z}_{16}$ και να δείξετε ότι $\mathbb{Z}_{16}/M \cong \mathbb{Z}_2$.*

ΛΥΣΗ:(α) Πρέπει να δείξουμε πως αν a, b είναι μηδενοδύναμα τότε τα $a - b$ και ra είναι μηδενοδύναμα. Για το ra είναι εύκολο, αφού αν το a είναι μηδενοδύναμο τότε για κάποιο n θα έχουμε $a^n = 0$ άρα και $(ra)^n = r^n a^n = r^n 0 = 0$. Ας υποθέσουμε ότι $a^n = 0, b^m = 0$. Θα δείξουμε ότι $(a-b)^{n+m} = 0$. Το διώνυμο του Νεύτωνα μας λέει ότι

$$(a-b)^{n+m} = (a+(-b))^{n+m} = \sum_{k=0}^{n+m} (-1)^k \binom{n+m}{n+m-k} a^{n+m-k} b^k = \sum_{k=0}^{n+m} n_k a^{n+m-k} b^k$$

Αλλά για κάθε k , θα έχουμε $a^{n+m-k}b^k = 0$ αφού αν $k < m$ τότε $m - k \geq 0$ οπότε $a^{n+m-k}b^k = a^n a^{m-k} b^k = 0$ ενώ αν $k \geq m$ τότε $a^{n+m-k}b^k = a^{n+m-k}b^{k-m}b^m = 0$. Με άλλα λόγια κάθε όρος στο ανάπτυγμα θα είναι 0, άρα $(a-b)^{n+m} = 0$ δηλαδή το $a - b$ είναι μηδενοδύναμο.

(β) Αν $x + M \in R/M$ είναι μηδενοδύναμο τότε αυτό σημαίνει ότι για κάποιο n θα έχουμε $(x+M)^n = M$ αλλά

$$\begin{aligned}(x+M)^n = M \;&\Leftrightarrow\; x^n + M = M \;\Leftrightarrow\\ x^n \in M \;&\Leftrightarrow\; x \in M \;\Leftrightarrow\; x + M = M = 0_{R/M}\end{aligned}$$

(γ) Αν $n = p_1^{n_1} \cdots p_i^{n_i} \cdots p_k^{n_k}$ είναι το ανάπτυγμα του n σε γινόμενο πρώτων και κάποιος από τους εκθέτες $n_i 1$ είναι > 1 τότε ο ο $a = p_1^{n_1} \cdots p_i^{n_i - 1} \cdots p_k^{n_k} \in \mathbb{Z}_n$ και $a^2 = p_1^{2n_1} \cdots p_i^{2n_i-2} \cdots p_k^{2n_k} = n p_1^{2n_1-1} \cdots p_i^{2n_i-3} \cdots p_k^{2n_k-1}$. Δηλαδή $n|a^2$ άρα $a^2 \equiv 0 \pmod n$ και ο $\mathbb{Z}_n$ έχει μηδενοδύναμα. Αντίστροφα τώρα, αν κανείς εκθέτης στο ανάπτυγμα του n σε γινόμενο πρώτων δεν είναι μεγαλύτερος του 1, με άλλα λόγια είναι όλοι ίσοι με με άλλα λόγια $n = p_1 \ldots p_n$, τότε ο $\mathbb{Z}_n$ δεν μπορεί να έχει μη μηδενικά μηδενοδύναμα στοιχεία. Πράγματι, ας υποθέσουμε ότι για κάποιο $a \in \{1, \ldots, n-1\}$, και κάποιο $m \geq 1$ είχαμε $a^m \equiv 0 \pmod n$ δηλαδή $n = p_1 \ldots p_n | a^n$ αλλά τότε $p_1 | a, \ldots, p_n | a$ και αφού οι $p_1, \ldots, p_n$ είναι πρώτοι διαφορετικοί μεταξύ τους θα έχουμε ότι $n = p_1 \ldots p_n | a$ που είναι αδύνατον αφού $0 < a < n$.
(δ) Κάθε πολλαπλάσιο του 2 είναι μηδενοδύναμο στοιχείο του $\mathbb{Z}_{16}$ (και γενικά του $\mathbb{Z}_{2^n}$), άρα το ιδεώδες M έχει 8 στοιχεία άρα ο $\mathbb{Z}_{16}/M$ έχει δύο ακριβώς στοιχεία άρα είναι ισόμορφος με τον $\mathbb{Z}_2$.

■

5. *Έστω R, R' δακτύλιοι και $f : R \to R'$ επιμορφισμός. Δείξτε ότι:*
(α) *Αν I' ιδεώδες του R' τότε $I' = f(f^{-1}(I'))$.*
(β) *Αν $a \in R$ τότε $f\,(\,(a)\,) = (\,f(a)\,)$. Με άλλα λόγια η εικόνα ενός κύριου ιδεώδους μέσω επιμορφισμού είναι κύριο ιδεώδες.*
(γ) *Αν I είναι ιδεώδες ενός δακτύλιου R, η απεικόνιση $\pi : R \to R/I$ με $\pi(x) = x + I$ είναι επιμορφισμός.*
(δ) *Κάθε ιδεώδες ενός δακτύλιου της μορφής $\mathbb{Z}_n$ είναι κύριο.*

ΛΥΣΗ:(α) Αν R, R' σύνολα και $f : R \to R'$ είναι μία απεικόνιση που είναι επί του R' και πάρετε ένα οποιοδήποτε υποσύνολο I' του R' τότε $I' = f(f^{-1}(I'))$.
(β) Ας υποθέσουμε ότι R είναι αντιμεταθετικός, δηλαδή τα κύρια ιδεώδη είναι τα $(a) = \{ra : r \in R\}$.

$$\begin{aligned}
& y \in f((a)) && \Leftrightarrow \\
& \exists x \in (a) \text{ ώστε } y = f(x) && \Leftrightarrow \\
& \exists r \in R \text{ ώστε } y = f(ar) && \Leftrightarrow \\
& \exists r \in R \text{ ώστε } y = rf(a) && \Leftrightarrow \\
& y \in (f(a))
\end{aligned}$$

(γ) Τετριμμένο.

(δ) $\mathbb{Z}_n = \mathbb{Z}/(n)$. θεωρείστε ένα οποιοδήποτε ιδεώδες I' και την κανονική απεικόνιση $\pi : \mathbb{Z} \to \mathbb{Z}_n$ που περιγράφεται στην ερώτηση (γ). Τότε η π είναι επιμορφισμός και το $\pi^{-1}(I')$ είναι ιδεώδες του $\mathbb{Z}$ και αφού κάθε ιδεώδες στο $\mathbb{Z}$ είναι κύριο θα έχουμε ότι $\pi^{-1}(I') = (a)$ για κάποιο $a \in \mathbb{Z}$. Από τα (α), (β) θα έχουμε ότι $I' = \pi(\pi^{-1}(I')) = \pi((a)) = (\pi(a)) = (a + (n))$, δηλαδή είναι κύριο.
■

6. *Έστω* $R = \mathbb{Z}(\sqrt{2}) = \{a + b\sqrt{2} : a, b \in \mathbb{Z}\}$, *θεωρούμενο σαν υπο-δακτύλιος των πραγματικών αριθμών. Ορίζουμε μία απεικόνιση* $N : R \to \mathbb{N}$ *με* $N(a + b\sqrt{2}) = |a^2 - 2b^2|$. *Να δείξετε τα παρακάτω:*

(α) *Αν* $x, y \in R$ *τότε* $N(xy) = N(x)N(y)$.

(β) $N(x) = 0$ *αν και μόνο αν* $x = 0$.

(γ) *Ένα στοιχείο* $x \in R$ *είναι αντιστρέψιμο αν και μόνο αν* $N(x) = 1$.

(δ) *Δείξτε ότι ο* $\mathbb{Z}(\sqrt{2})$ *δεν είναι σώμα.*

ΛΥΣΗ:(α) Αν $x = a + b\sqrt{2}, y = c + d\sqrt{2} \in R$ τότε

$$N(xy) = N\left(a + b\sqrt{2})(c + d\sqrt{2})\right) = N\left((ac + 2bd) + (ad + bc)\sqrt{2})\right) =$$
$$= \left|(ac + 2bd)^2 - 2(ad + bc)^2\right| = \left|(a^2c^2 + 4b^2d^2 + 4abcd - 2a^2d^2 - 2b^2c^2 - 4abcd\right| =$$
$$= \left|(a^2c^2 + 4b^2d^2 - 2a^2d^2 - 2b^2c^2\right| = \left|a^2(c^2 - 2d^2) - 2b^2(c^2 - 2d^2)\right| =$$
$$= \left|(a^2 - 2b^2)(c^2 - 2d^2)\right| = N(x)N(y)$$

(β) Αν $x = 0 = 0 + 0\sqrt{2}$ τότε $N(x) = |0^2 - 20^2| = 0$. Αν $N(x) = N\left(a + b\sqrt{2})\right) = 0$ τότε $b = 0$ οπότε και $a = 0$ και $x = 0$. Γιατί αν $b \neq 0$ τότε $\sqrt{2} = \pm\frac{a}{b}$ που είναι αδύνατον γιατί ο $\sqrt{2}$ είναι άρητος.

(γ) Αν $x \in R$ είναι αντιστρέψιμο τότε $xy = 1$ για κάποιο y αλλά τότε $N(xy) = N(x)N(y) = 1$ και επειδή οι $N(x), N(y)$ είναι θετικοί ακέραιοι θα έχουμε $N(x) = N(y) = 1$. Αντίστροφα, αν $N(x) = N\left(a + b\sqrt{2})\right) = 1$ τότε αν $x = a - b\sqrt{2}$ θα έχουμε $|xy| = 1$ άρα $xy = 1$ είτε $xy = -1$ και σε κάθε περίπτωση ο x είναι αντιστρέψιμος με αντίστροφο τον y (στην πρώτη περίπτωση) ή τον $-x$ στην δεύτερη.

(δ) Αν ο $\mathbb{Z}(\sqrt{2})$ ήταν σώμα κάθε μη μηδενικό στοιχείο του θα αντιστρεφόταν, άρα και το $5 = 5 + 0\sqrt{2}$, αλλά $N(5) = 25 \neq 1$ αντίθετα με το (γ).

■