ΜΑΘΗΜΑ 07

10 Ο δακτύλιος $\mathbb{Z}_m$

Θεωρούμε ένα $m \in \mathbb{N}$, σταθερό, και ορίζουμε την διμελή σχέση $R \subseteq \mathbb{Z} \times \mathbb{Z}$ με

$$\begin{aligned} xRy &\iff x - y \text{ είναι ακέραιο πολλαπλάσιο του } m \\ &\iff \exists\, k \in \mathbb{Z} \ : \ x - y = km \end{aligned}$$

Η σχέση R συνήθως συμβολίζεται με $\equiv (\mathrm{mod} m)$, δηλ.

$$x \equiv y (\mathrm{mod} m) \iff \exists\, k \in \mathbb{Z} \ : \ x - y = km.$$

10.1 Λήμμα. *Η ανωτέρω σχέση R είναι σχέση ισοδυναμίας.*

Απόδειξη. (i) Για κάθε $x \in \mathbb{Z}$, υπάρχει $k = 0 \in \mathbb{Z}$ με

$$x - x = 0 = 0m,$$

άρα xRx και η R είναι ανακλαστική.

(ii) Ισχύουν οι συνεπαγωγές

$$\begin{aligned} xRy &\implies \exists\, k \in \mathbb{Z} \ : \ x - y = km \\ &\implies \exists (-k) \in \mathbb{Z} \ : \ y - x = (-k)m \\ &\implies yRx \end{aligned}$$

και η R είναι συμμετρική.

(iii) Έστω xRy και yRz. Τότε υπάρχουν $k, \lambda \in \mathbb{Z}$ με

$$x - y = km \quad \text{και} \quad y - z = \lambda m.$$

Προσθέτοντας τις ισότητες κατά μέλη παίρνουμε

$$x - z = (k + \lambda)m$$

με $k + \lambda \in \mathbb{Z}$, άρα η R είναι μεταβατική. □

Θα μελετήσουμε τώρα πώς η δεδομένη σχέση ισοδυναμίας διαμερίζει το $\mathbb{Z}$ σε κλάσεις ισοδυναμίας. Έστω $x_1, x_2 \in \mathbb{Z}$ με $x_1 R x_2$. Θεωρώντας την διαίρεση των x, y με m, γνωρίζουμε ότι υπάρχουν μονοσήμαντα ορισμένοι $k_1, k_2, \upsilon_1, \upsilon_2 \in \mathbb{Z}$ με

$$x_i = k_i m + \upsilon_i, i = 1, 2$$

και

$$0 \leq \upsilon_1, \upsilon_2 \leq m - 1.$$

Η σχέση $x_1 R x_2$ σημαίνει ότι η διαφορά

$$x_1 - x_2 = (k_1 - k_2)m + (\upsilon_1 - \upsilon_2)$$

είναι ακέραιο πολλαπλάσιο του m. Άρα και η διαφορά $\upsilon_1 - \upsilon_2$ είναι ακέραιο πολλαπλάσιο του m. Όμως οι ανισότητες $0 \leq \upsilon_1, \upsilon_2 \leq m - 1$ μας δίνουν

$$\left.\begin{array}{rcccl} 0 & \leq & \upsilon_1 & \leq & m-1 \\ -(m-1) & \leq & -\upsilon_2 & \leq & 0 \end{array}\right\} \Rightarrow -(m-1) \leq \upsilon_1 - \upsilon_2 \leq m-1$$

και το μοναδικό ακέραιο πολλαπλάσιο του m μέσα στο ανωτέρω διάστημα είναι το 0. Άρα $\upsilon_1 = \upsilon_2$. Αποδείξαμε λοιπόν το επόμενο:

10.2 Λήμμα. *Έστω $x_1, x_2 \in \mathbb{Z}$. Τότε*

$$x_1 \equiv x_2 (\mathrm{mod} m) \iff x_1, x_2 \textit{ διαιρούμενοι με } m \textit{ δίνουν το ίδιο υπόλοιπο.}$$

Σαν αποτέλεσμα του προηγούμενου λήμματος, έχουμε ότι υπάρχουν ακριβώς τόσες κλάσεις ισοδυναμίας, όσα είναι τα δυνατά υπόλοιπα. Δηλ. το $\mathbb{Z}$ διαμερίζεται στις εξής (m το πλήθος) κλάσεις ισοδυναμίας:

$$\begin{aligned} [0]_m &= \{km : k \in \mathbb{Z}\} \\ [1]_m &= \{km + 1 : k \in \mathbb{Z}\} \\ [2]_m &= \{km + 2 : k \in \mathbb{Z}\} \\ &\vdots \\ [m-1]_m &= \{km + (m-1) : k \in \mathbb{Z}\} \end{aligned}$$

10.3 Ορισμός. Στο $\mathbb{Z}_m$ ορίζουμε μια πράξη που ονομάζουμε ***πρόσθεση*** του $\mathbb{Z}_m$, ως εξής:

$$+ : \mathbb{Z}_m \times \mathbb{Z}_m \longrightarrow \mathbb{Z}_m : ([x]_m, [y]_m) \longmapsto [x]_m + [y]_m := [x + y]_m.$$

Παρατηρούμε ότι η πρόσθεση του $\mathbb{Z}_m$ είναι *καλά ορισμένη*, δηλ. αν $[x]_m = [x']_m$ και $[y]_m = [y']_m$, τότε $[x+y]_m = [x'+y']_m$. Πράγματι:

$$\left.\begin{array}{rcl} [x]_m = [x']_m & \Rightarrow & xRx' \\ [y]_m = [y']_m & \Rightarrow & yRy' \end{array}\right\} \Rightarrow \begin{array}{c} \Rightarrow \exists k \in \mathbb{Z} : x - x' = km \\ \Rightarrow \exists \lambda \in \mathbb{Z} : y - y' = \lambda m \end{array}$$
$$(x+y) - (x'-y') = (k+\lambda)m,\ k+\lambda \in \mathbb{Z} \Rightarrow$$
$$[x+y]_m = [x'+y']_m$$

Ακόμη, η πρόσθεση έχει τις παρακάτω ιδιότητες:
(A1) Είναι *μεταθετική*: Πράγματι, για κάθε $[x]_m, [y]_m \in \mathbb{Z}_m$, έχουμε

$$[x]_m + [y]_m = [x+y]_m = [y+x]_m = [y]_m + [x]_m.$$

(A2) Είναι *προσεταιριστική*: Για κάθε $[x]_m, [y]_m, [z]_m \in \mathbb{Z}_m$ ισχύει

$$\begin{aligned} [x]_m + ([y]_m + [z]_m) &= [x]_m + [y+z]_m = [x+(y+z)]_m = [(x+y)+z]_m \\ &= [x+y]_m + [z]_m = ([x]_m + [y]_m) + [z]_m. \end{aligned}$$

(A3) *Υπάρχει ουδέτερο στοιχείο*, η κλάση $[0]_m \in \mathbb{Z}_m$:

$$[x]_m + [0]_m = [x+0]_m = [x]_m, \qquad \forall\ [x]_m \in \mathbb{Z}_m.$$

(A4) Κάθε $[x]_m \in \mathbb{Z}_m$ *έχει αντίθετο*, την κλάση $[-x]_m$:

$$[x]_m + [-x]_m = [x+(-x)]_m = [0]_m.$$

Οι ιδιότητες (A1)-(A4) καθιστούν το ζεύγος $(\mathbb{Z}_m, +)$ *αβελιανή/μεταθετική ομάδα*.

10.4 Ορισμός. Ονομάζουμε ***πολλαπλασιασμό*** του $\mathbb{Z}_m$ την πράξη

$$\cdot : \mathbb{Z}_m \times \mathbb{Z}_m \longrightarrow \mathbb{Z}_m : ([x]_m, [y]_m) \longmapsto [x]_m \cdot [y]_m := [xy]_m.$$

Όπως προηγουμένως, ο πολλαπλασιασμός στο $\mathbb{Z}_m$ είναι *καλά ορισμένος*, δηλ. αν $[x]_m = [x']_m$ και $[y]_m = [y']_m$, τότε $[xy]_m = [x'y']_m$. Πράγματι, από την ισότητα $[x]_m = [x']_m$ προκύπτει ότι τα x και x' διαιρούμενα με m δίνουν το ίδιο υπόλοιπο υ_x. Άρα, $x = km + \upsilon_x$ και $x' = k'm + \upsilon_x$, με $k, k' \in \mathbb{Z}$.

Παρόμοια από την ισότητα $[y]_m = [y']_m$ παίρνουμε ότι $y = \lambda m + \upsilon_y$ και $y' = \lambda' m + \upsilon_y$. Άρα

$$\begin{aligned} xy - x'y' &= (km + \upsilon_x)(\lambda m + \upsilon_y) - (k'm + \upsilon_x)(\lambda' m + \upsilon_y) \\ &= (k\lambda m^2 + km\upsilon_y + \lambda m\upsilon_x + \upsilon_x\upsilon_y) \\ &\quad - (k'\lambda' m^2 + k'm\upsilon_y + \lambda' m\upsilon_x + \upsilon_x\upsilon_y) \\ &= [(k\lambda m + k\upsilon_y + \lambda\upsilon_x) - (k'\lambda' m + k'\upsilon_y + \lambda'\upsilon_x)] \cdot m \end{aligned}$$

άρα $[xy]_m = [x'y']_m$.

Ακόμη, ο πολλαπλασιασμός έχει τις παρακάτω ιδιότητες:

(Β1) Είναι *μεταθετικός*: Για κάθε $[x]_m, [y]_m \in \mathbb{Z}_m$, έχουμε

$$[x]_m \cdot [y]_m = [xy]_m = [yx]_m = [y]_m \cdot [x]_m.$$

(Β2) Είναι *προσεταιριστικός*: Για κάθε $[x]_m, [y]_m, [z]_m \in \mathbb{Z}_m$ είναι:

$$\begin{aligned} [x]_m \cdot ([y]_m \cdot [z]_m) &= [x]_m \cdot [yz]_m = [x(yz)]_m = [(xy)z]_m \\ &= [xy]_m \cdot [z]_m = ([x]_m \cdot [y]_m) \cdot [z]_m. \end{aligned}$$

(Β3) *Υπάρχει ουδέτερο στοιχείο*, η κλάση $[1]_m \in \mathbb{Z}_m$:

$$[1]_m \cdot [x]_m = [1x]_m = [x]_m, \qquad \forall\ [x]_m \in \mathbb{Z}_m.$$

Τέλος, πρέπει να παρατηρήσουμε ότι:

(Γ1) Η πρόσθεση και ο πολλαπλασιασμός στο $\mathbb{Z}_m$ *συνδέονται με την επιμεριστική ιδιότητα*: Για κάθε $[x]_m, [y]_m, [x]_m \in \mathbb{Z}_m$, ισχύει

$$\begin{aligned} [x]_m \cdot ([y]_m + [z]_m) &= [x]_m \cdot [y + z]_m = [x(y + z)]_m = [xy + xz]_m \\ &= [xy]_m + [xz]_m = [x]_m \cdot [y]_m + [x]_m \cdot [z]_m. \end{aligned}$$

Οι ιδιότητες (Α1)-(Α4) μαζί με τις (Β1)-(Β3) και την (Γ1) καθιστούν την τριάδα $(\mathbb{Z}_m, +, \cdot)$ *μεταθετικό δακτύλιο με μονάδα.*

Αξίζει να σημειώσουμε ότι *ο δακτύλιος* $(\mathbb{Z}_m, =, \cdot)$ *είναι σώμα, αν και μόνον αν ο* m *είναι πρώτος αριθμός.*