ΑΛΓΕΒΡΙΚΕΣ ΔΟΜΕΣ Ι

Ακαδημαϊκο Ετος 2023-2024

Επιλυση Ασκησεων - Φυλλαδιο 2

Διδασκων: Α. Μπεληγιάννης

ΙΣΤΟΣΕΛΙΔΑ ΜΑΘΗΜΑΤΟΣ

http://users.uoi.gr/abeligia/AlgebraicStructuresI/ASI2024/ASI2024.html

Πέμπτη 21 Μαρτίου 2024

Αν $(G,\star)$ είναι μια ομάδα, τότε θα συμβολίζουμε με a^{-1} το αντίστροφο στοιχείο του a στην ομάδα G.

Άσκηση 1. Έστω ότι το ζεύγος $(G,\star)$ είναι ομάδα με ουδέτερο στοιχείο e και θεωρούμε στοιχεία $a,b,c\in G$. Να δειχθεί ότι τα ακόλουθα είναι ισοδύναμα:

(1) $a\star b\star c=e$.
(2) $b\star c\star a=e$.
(3) $c\star a\star b=e$.

Αν ικανοποιείται μια από τις παραπάνω σχέσεις, να δειχθεί με ένα αντιπαράδειγμα ότι γενικά $a\star c\star b\neq e$.

Λύση. (α) $(1)\Longrightarrow(2)$ Έχουμε:

$$\begin{aligned} a\star b\star c=e &\Longrightarrow a^{-1}\star(a\star b\star c)=a^{-1}\star e\\ &\Longrightarrow (a^{-1}\star a)\star(b\star c)=a^{-1}\\ &\Longrightarrow e\star(b\star c)=a^{-1}\\ &\Longrightarrow b\star c=a^{-1}\\ &\Longrightarrow b\star c\star a=a^{-1}\star a\\ &\Longrightarrow b\star c\star a=e \end{aligned}$$

(β) $(2)\Longrightarrow(3)$ Έχουμε:

$$\begin{aligned} b\star c\star a=e &\Longrightarrow b^{-1}\star(b\star c\star a)=b^{-1}\star e\\ &\Longrightarrow (b^{-1}\star b)\star(c\star a)=b^{-1}\\ &\Longrightarrow e\star(c\star a)=b^{-1}\\ &\Longrightarrow c\star a=b^{-1}\\ &\Longrightarrow c\star a\star b=b^{-1}\star b\\ &\Longrightarrow c\star a\star b=e \end{aligned}$$

(γ) $(3)\Longrightarrow(1)$ Έχουμε:

$$\begin{aligned} c\star a\star b=e &\Longrightarrow c^{-1}\star(c\star a\star b)=c^{-1}\star e\\ &\Longrightarrow (c^{-1}\star c)\star(a\star b)=c^{-1}\\ &\Longrightarrow e\star(a\star b)=c^{-1}\\ &\Longrightarrow a\star b=c^{-1}\\ &\Longrightarrow a\star b\star c=c^{-1}\star c\\ &\Longrightarrow a\star b\star c=e \end{aligned}$$

Θεωρούμε την συμμετρική ομάδα $(\mathsf{S}_3, \circ)$ επί του συνόλου $X = \{1,2,3\}$:

$$\mathsf{S}_3 = \{f \colon X \longrightarrow X \mid \text{η } f \text{ είναι «1-1» και «επί»}\}$$

όπου «$\circ$» είναι η σύνθεση απεικονίσεων. Θεωρούμε τις μεταθέσεις

$$f = \begin{cases} 1 \longmapsto 2 \\ 2 \longmapsto 1 \\ 3 \longmapsto 3 \end{cases}, \qquad g = \begin{cases} 1 \longmapsto 2 \\ 2 \longmapsto 3 \\ 3 \longmapsto 1 \end{cases}, \qquad h = \begin{cases} 1 \longmapsto 1 \\ 2 \longmapsto 3 \\ 3 \longmapsto 2 \end{cases}$$

Τότε εύκολα υπολογίζουμε ότι $f \circ g \circ h = \mathrm{Id}_X$ και $f \circ h \circ g = \begin{cases} 1 \longmapsto 3 \\ 2 \longmapsto 1 \\ 3 \longmapsto 2 \end{cases} \neq \mathrm{Id}_X$. ■

Άσκηση 2. Έστω ότι $(G, \star)$ είναι μια ομάδα με ουδέτερο στοιχείο e. Αν το σύνολο G έχει άρτιο πλήθος στοιχείων, να δειχθεί ότι υπάρχει ένα στοιχείο $a \neq e$ στην G τέτοιο ώστε $a \star a = e$.

Λύση. Επειδή η G έχει άρτιο πλήθος στοιχείων τότε $|G| = 2\lambda$, με $\lambda \geq 1$, και άρα το σύνολο $G \setminus \{e\}$ έχει $2\lambda - 1$ στοιχεία. Θεωρούμε το σύνολο

$$X = \{x \in G \setminus \{e\} \mid x \neq x^{-1}\}$$

Αν $x \in X$ τότε $x \neq e$ και $x^{-1} \in X$ (διότι αν $x^{-1} \notin X$ τότε θα είχαμε $x^{-1} = (x^{-1})^{-1}$ και άρα $x^{-1} = x$ το οποίο είναι άτοπο) και προφανώς $x \neq x^{-1}$, δηλαδή τα στοιχεία του συνόλου X εμφανίζονται κατά ζεύγη (x, x^{-1}) με $x \neq x^{-1}$. Αυτό σημαίνει ότι το πλήθος των στοιχείων του X είναι άρτιο.

Από την άλλη πλευρά το X είναι γνήσιο υποσύνολο του $G \setminus \{e\}$, δηλαδή $X \subseteq G \setminus \{e\}$ και $X \neq G \setminus \{e\}$, διότι το X έχει άρτιο πλήθος στοιχείων και το $G \setminus \{e\}$ έχει περιττό πλήθος στοιχείων. Άρα υπάρχει στοιχείο $a \in G \setminus \{e\}$ και $a \notin X$. Αυτό όμως σημαίνει ότι $a \neq e$ και $a = a^{-1}$, δηλαδή $a \star a = e$. ■

Υποθέτουμε ότι

$$\star \colon G \times G \longrightarrow G, \quad (a, b) \longmapsto a \star b$$

είναι μια προσεταιριστική πράξη ορισμένη επί του μη-κενού συνόλου G.

Ένα στοιχείο $e \in G$ καλείται **αριστερό ουδέτερο στοιχείο** για την πράξη «$\star$» αν: $e \star a = a$, $\forall a \in G$. Το στοιχείο $e \in G$ καλείται **δεξιό ουδέτερο στοιχείο** για την πράξη «$\star$» αν: $a \star e = a$, $\forall a \in G$.

Άσκηση 3. Θεωρούμε το σύνολο $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$ των μη-μηδενικών πραγματικών αριθμών. Ορίζουμε μια διμελή πράξη $\star : \mathbb{R}^* \times \mathbb{R}^* \longrightarrow \mathbb{R}^*$ επί του $\mathbb{R}^*$, ως εξής:

$$a \star b := |a|b$$

(1) Να δειχθεί ότι η πράξη «$\star$» προσεταιριστική.
(2) Να δειχθεί ότι υπάρχει ένα αριστερό ουδέτερο στοιχείο και ένα δεξιό αντίστροφο στοιχείο για την πράξη «$\star$».
(3) Είναι το ζεύγος $(\mathbb{R}^*, \star)$ ομάδα;
(4) Ποιά είναι η σημασία της άσκησης;

Λύση. (1) Έστω $a, b, c \in G$. Θα δείξουμε ότι $(a \star b) \star c = a \star (b \star c)$. Έχουμε:

$$(a \star b) \star c = (|a|b) \star c = ||a|b|\, c = |ab|c$$

και

$$a \star (b \star c) = a \star (|b|c) = |a||b|c = |ab|c$$

Συνεπώς η «$\star$» είναι μια προσεταιριστική διμελής πράξη επί του $\mathbb{R}^*$.

(2) Για κάθε $a \in \mathbb{R}^*$ έχουμε:

$$1 \star a = |1| \cdot a = 1 \cdot a = a$$

και άρα το $e = 1$ είναι αριστερό ουδέτερο στοιχείο για την πράξη «$\star$». Όμως, το $e = 1$ δεν είναι ουδέτερο στοιχείο διότι δεν είναι δεξιό ουδέτερο στοιχείο. Για παράδειγμα για $a = -1$ έχουμε:

$$(-1) \star 1 = |-1| \cdot 1 = 1 \neq -1 = |1| \cdot (-1) = 1 \star (-1)$$

Επίσης για κάθε $a \in \mathbb{R}^*$ υπάρχει το στοιχείο $b = \frac{1}{|a|} \in \mathbb{R}^*$ έτσι ώστε

$$a \star b = |a| \cdot b = |a| \cdot \frac{1}{|a|} = 1$$

Επομένως για κάθε $a \in \mathbb{R}^*$ το στοιχείο $b = \frac{1}{|a|} \in \mathbb{R}^*$ είναι ένα δεξιό αντίστροφο για την πράξη «$\star$».

(3) Το ζεύγος $(\mathbb{R}^*, \star)$ δεν είναι ομάδα διότι δεν υπάρχει ουδέτερο στοιχείο.

(4) Η σημασία αυτής της άσκησης είναι ότι μπορεί ένα ζεύγος $(G, \star)$ να μην είναι ομάδα, αλλά όπως είδαμε αυτό δεν σημαίνει ότι δεν μπορεί να διαθέτει αριστερό (αντίστοιχα δεξιό) ουδέτερο στοιχείο και δεξιό (αντίστοιχα αριστερό) αντίστροφο στοιχείο για τυχόν στοιχείο του συνόλου G. Επομένως αν έχουμε μια προσεταιριστική πράξη «$\star$» ορισμένη επί ενός συνόλου G, αν υπάρχει ένα αριστερό ουδέτερο στοιχείο e για την πράξη «$\star$» επί του G, και αν κάθε στοιχείο του συνόλου G έχει δεξιό αντίστροφο, τότε δεν συνεπάγεται ότι το ζεύγος $(G, \star)$ είναι ομάδα.

Από την άλλη πλευρά, στην Άσκηση 13 αυτού του φυλλαδίου δείχνουμε ότι αν έχουμε μια προσεταιριστική πράξη «$\star$» ορισμένη επί ενός συνόλου G, αν υπάρχει ένα αριστερό (αντίστοιχα δεξιό) ουδέτερο στοιχείο $e \in G$ για την πράξη «$\star$», και αν κάθε στοιχείο του G έχει αριστερό (αντίστοιχα δεξιό) αντίστροφο τότε το ζεύγος $(G, \star)$ είναι ομάδα. ■

Άσκηση 4. Έστω ότι το ζεύγος $(G, \star)$ είναι ομάδα με ουδέτερο στοιχείο e. Αν ισχύει

$$x \star x = e, \ \ \forall x \in G$$

να δειχθεί ότι η ομάδα $(G, \star)$ είναι αβελιανή. Να δοθεί παράδειγμα αβελιανής ομάδας $(G, \star)$ η οποία περιέχει στοιχείο x έτσι ώστε $x \star x \neq e$.

Λύση. Επειδή $x \star x = e$, $\forall x \in G$, έχουμε:

$$x \star x = e \implies x \star x \star x^{-1} = e \star x^{-1} \implies x \star e = x^{-1} \implies x = x^{-1} \qquad (*)$$

δηλαδή το αντίστροφο κάθε στοιχείου $x \in G$ είναι το ίδιο το στοιχείο. Τότε για $x = a \star b$ έχουμε:

$$(a \star b)^{-1} = a \star b \iff b^{-1} \star a^{-1} = a \star b \iff b \star a = a \star b \qquad (**)$$

αφού γνωρίζουμε ότι γενικά ισχύει $(a \star b)^{-1} = b^{-1} \star a^{-1}$ και αφού εδώ, λόγω της υπόθεσης, είναι $a = a^{-1}$ και $b = b^{-1}$. Η σχέση $(**)$ ισχύει $\forall a, b \in G$, και επομένως η ομάδα G είναι αβελιανή.

Για την αβελιανή ομάδα $(\mathbb{Z}_4, +)$, έχουμε $[3]_4 + [3]_4 = [6]_4 = [2]_4 \neq [0]_4$. ■

Άσκηση 5. Να δειχθεί ότι το ανοιχτό διάστημα $(-1, 1) = \{x \in \mathbb{R} \mid -1 < x < 1\}$ της πραγματικής ευθείας αποτελεί αβελιανή ομάδα με πράξη:

$$x \star y = \frac{x + y}{1 + xy}$$

Λύση. Παρατηρούμε ότι: $x \in (-1, 1) \iff |x| < 1$.

Έστω ότι $x, y \in (-1, 1)$. Θα δείξουμε πρώτα ότι το $x \star y \in (-1, 1)$, δηλαδή ότι η «$\star$» είναι διμελής πράξη επί του $(-1, 1)$.

Καταρχήν, επειδή $|x| < 1$ και $|y| < 1$, έπεται ότι $|xy| < 1$ και γι' αυτό $1 + xy \neq 0$. Συνεπώς, έχει νόημα το κλάσμα $x \star y = \frac{x+y}{1+xy}$.

Θα δείξουμε ότι $x \star y \in (-1, 1)$, δηλαδή με άλλα λόγια ότι $\left|\frac{x+y}{1+xy}\right| < 1$ ή ισοδύναμα ότι: $-1 < x \star y = \frac{x+y}{1+xy} < 1$. Είναι:

$$\left|\frac{x + y}{1 + xy}\right| < 1 \iff |x + y| < |1 + xy| \iff (x + y)^2 < (1 + xy)^2 \iff$$
$$x^2 + y^2 < 1 + x^2y^2 \iff x^2 - 1 < y^2(x^2 - 1)$$

και επειδή $x^2 - 1 < 0$, αφού $|\ x\ | < 1$, έχουμε:

$$x^2 - 1 < y^2(x^2 - 1) \iff 1 > y^2$$

Αλλά η $1 > y^2$ είναι αληθής, αφού $\mid y \mid < 1$. Συνεπώς, η πράξη «$\star$» είναι καλά ορισμένη επί του συνόλου $(-1,1)$.

Έστω $x, y, z \in (-1,1)$. Έχουμε:

- Η πράξη «$\star$» είναι προσεταιριστική:

$$x \star (y \star z) = x \star \big(\frac{y+z}{1+yz}\big) = \frac{x + \frac{y+z}{1+yz}}{1 + x \cdot \frac{y+z}{1+yz}} = \frac{x+y+z+xyz}{1+xy+yz+xz}$$

και

$$(x \star y) \star z = \big(\frac{x+y}{1+xy}\big) \star z = \frac{\frac{x+y}{1+xy} + z}{1 + \frac{x+y}{1+xy} \cdot z} = \frac{x+y+z+xyz}{1+xy+yz+xz}$$

Άρα η πράξη «$\star$» είναι προσεταιριστική.

- Ουδέτερο στοιχείο: Έστω στοιχείο $e \in (-1,1)$ έτσι ώστε $x \star e = x = e \star x$, $\forall x \in (-1,1)$. Τότε

$$\frac{x+e}{1+xe} = x \implies x + e = x + x^2 e \implies e \cdot (1 - x^2) = 0 \implies e = 0 \quad \text{ή} \quad x = \pm 1$$

και άρα $e = 0$ διότι $x \in (-1,1)$. Το στοιχείο $e = 0 \in (-1,1)$ και

$$x \star 0 = \frac{x+0}{1+x\cdot 0} = \frac{x}{1} = x = \frac{x}{1} = \frac{0+x}{1+0\cdot x} = 0 \star x$$

για κάθε $x \in (-1,1)$. Συνεπώς το $e = 0$ είναι το ουδέτερο στοιχείο της πράξης «$\star$».

- Αντίστροφο στοιχείο: Έστω $x \in (-1,1)$ και υποθέτουμε ότι υπάρχει ένα $y \in (-1,1)$ έτσι ώστε $x \star y = 0$. Τότε

$$\frac{x+y}{1+xy} = 0 \implies x + y = 0 \implies y = -x$$

και άρα έχουμε

$$x \star (-x) = \frac{x + (-x)}{1 + x(-x)} = \frac{0}{1-x^2} = 0 = \frac{0}{1-x^2} = \frac{-x+x}{1+(-x)x} = (-x) \star x$$

Επομένως, επειδή $-x \in (-1,1)$, $\forall x \in (-1,1)$, έπεται ότι για κάθε $x \in (-1,1)$ το αντίστροφο στοιχείο του x ως προς την πράξη «$\star$» είναι το $x' = -x \in (-1,1)$.

Άρα το ζεύγος $\big((-1,1), \star\big)$ είναι ομάδα, η οποία είναι αβελιανή διότι, $\forall x, y \in (-1,1)$:

$$x \star y = \frac{x+y}{1+xy} = \frac{y+x}{1+yx} = y \star x \qquad \blacksquare$$

Άσκηση 6. Έστω ότι το ζεύγος $(G, \star)$ είναι ομάδα με ουδέτερο στοιχείο e. Αν το σύνολο G έχει πεπερασμένο πλήθος στοιχείων, να δειχθεί ότι για κάθε $a \in G$, υπάρχει ακέραιος $n \in \mathbb{N}$, ο οποίος γενικά εξαρτάται από το a, έτσι ώστε: $a^n := a \star a \star \cdots \star a = e$ (το a εμφανίζεται σαν παράγοντας n φορές). Επιπλέον να δειχθεί ότι:

$$\exists\, N \in \mathbb{N}: \quad a^N = e, \quad \forall a \in G$$

Λύση. Έστω $a \in G$. Θεωρούμε το σύνολο:

$$H = \big\{a^n \mid n \in \mathbb{Z}\big\} = \big\{ \cdots, a^{-2}, a^{-1}, e, a, a^2, \cdots \big\} \subseteq G$$

το οποίο είναι πεπερασμένο σύνολο αφού είναι υποσύνολο της ομάδας G και $|G| < \infty$. Επομένως τα στοιχεία του H δεν μπορεί να είναι όλα διαφορετικά μεταξύ τους. Αυτό σημαίνει ότι δηλαδή υπάρχουν $i, j \in \mathbb{Z}$ με $i \neq j$ έτσι ώστε $a^i = a^j$. Τότε

$$a^i = a^j \implies a^i \star (a^j)^{-1} = a^j \star (a^j)^{-1} \implies a^i \star (a^j)^{-1} = e$$

και

$$a^j \star a^{-j} = a^{j-j} = a^0 = e \implies (a^j)^{-1} = a^{-j}$$

Συνδυάζοντας τις δυο παραπάνω σχέσεις έχουμε:

$$a^i \star a^{-j} = e \implies a^{i-j} = e \tag{$*$}$$

Διακρίνουμε δυο περιπτώσεις:

(1) Αν $i > j$ τότε θέτοντας $n = i - j \in \mathbb{N}$, από τη σχέση $(*)$ έπεται ότι $a^n = e$.
(2) Αν $i < j$ τότε θέτοντας $n = j - i \in \mathbb{N}$ και χρησιμοποιώντας τη σχέση $(*)$ έχουμε:

$$a^{-n} = e \implies a^n \star a^{-n} = a^n \star e = a^n \implies a^n = a^{n-n} = a^0 = e$$

Άρα πράγματι για κάθε $a \in G$ υπάρχει $n \in \mathbb{N}$, το οποίο γενικά εξαρτάται από το a, έτσι ώστε $a^n = e$.

Επειδή η ομάδα G είναι πεπερασμένη μπορούμε να γράψουμε

$$G = \big\{e = a_1, a_2, a_3, \cdots, a_m\big\}$$

Αποδείξαμε παραπάνω ότι για κάθε $i = 1, \cdots, m$ υπάρχει $n_i \in \mathbb{N}$ έτσι ώστε $a_i^{n_i} = e$. Θέτουμε

$$N = n_1 n_2 \cdots n_m$$

Τότε για κάθε $a_i \in G$ έχουμε:

$$a_i^N = a_i^{n_1 n_2 \cdots n_m} = a_i^{n_i n_1 n_2 \cdots n_{i-1} n_{i+1} \cdots n_m} = (a_i^{n_i})^{n_1 n_2 \cdots n_{i-1} n_{i+1} \cdots n_m} = e^{n_1 n_2 \cdots n_{i-1} n_{i+1} \cdots n_m} = e$$

και άρα έχουμε το ζητούμενο: $a^N = e$, $\forall a \in G$. ■

Άσκηση 7. Έστω ότι το ζεύγος $(G, \star)$ είναι ομάδα και $a, b \in G$. Να δειχθεί ότι:

$$(a \star b)^{-1} = a^{-1} \star b^{-1} \iff a \star b = b \star a$$

Να συμπεράνετε ότι η ομάδα $(G, \star)$ είναι αβελιανή αν και μόνον αν, $\forall a, b \in G$: $(a \star b)^{-1} = a^{-1} \star b^{-1}$.

Λύση. Είναι:

$$\begin{aligned} &(a \star b)^{-1} = a^{-1} \star b^{-1} \iff \big((a \star b)^{-1}\big)^{-1} = \big(a^{-1} \star b^{-1}\big)^{-1} \iff \\ &a \star b = (b^{-1})^{-1} \star (a^{-1})^{-1} \iff a \star b = b \star a \end{aligned}$$

Αν λοιπόν η ομάδα G είναι αβελιανή, τότε $\forall a, b \in G$ είναι $a \star b = b \star a$, άρα $\forall a, b \in G$ είναι $(a \star b)^{-1} = a^{-1} \star b^{-1}$.
Αντίστροφα, αν $\forall a, b \in G$ είναι $(a \star b)^{-1} = a^{-1} \star b^{-1}$, τότε $\forall a, b \in G$ είναι $a \star b = b \star a$ και η G είναι μια αβελιανή ομάδα. ■

Έστω ότι M ένα σύνολο και $\star : M \times M \longrightarrow M$, $(a, b) \longmapsto a \star b$, μια διμελής πράξη ορισμένη επί του M. Υπενθυμίζουμε ότι το ζεύγος $(M, \star)$ καλείται **μονοειδές**, αν:

(1) Η πράξη «$\star$» είναι προσεταιριστική.
(2) Υπάρχει ουδέτερο στοιχείο $e \in G$ για την πράξη «$\star$».

Το μονοειδές $(M, \star)$ καλείται **μεταθετικό μονοειδές** αν η πράξη «$\star$» είναι μεταθετική.

Άσκηση 8. Έστω ότι το ζεύγος $(M, \star)$ είναι ένα μονοειδές με ουδέτερο στοιχείο e.

(1) Να δειχθεί ότι το ζεύγος $(\mathsf{U}(M), \star)$, όπου

$$\mathsf{U}(M) = \big\{x \in M \mid \exists\, x' \in M : \; x \star x' = e = x' \star x\big\}$$

είναι το σύνολο των αντιστρέψιμων στοιχείων του μονοειδούς $(M, \star)$, είναι ομάδα η οποία καλείται η **ομάδα των αντιστρέψιμων στοιχείων** του μονοειδούς $(M, \star)$.
Επιπλέον να δειχθεί ότι αν το μονοειδές $(M, \star)$ είναι μεταθετικό, τότε η ομάδα $(\mathsf{U}(M), \star)$ είναι αβελιανή.
(2) Να βρεθούν οι ομάδες $(\mathsf{U}(\mathbb{N}), \cdot)$, $(\mathsf{U}(\mathbb{Z}), \cdot)$ και $(\mathsf{U}(\mathbb{Z}_n), \cdot)$ των μονοειδών $(\mathbb{N}, \cdot)$, $(\mathbb{Z}, \cdot)$, και $(\mathbb{Z}_n, \cdot)$, όπου «$\cdot$» είναι ο συνήθης πολλαπλασιασμός.

(3) Να δειχθεί ότι το ζεύγος $(\mathbb{Z} \times \mathbb{Z}, \star)$, όπου

$$(x_1, x_2) \star (y_1, y_2) = (x_1 y_1, x_2 y_2)$$

ένα ένα μεταθετικό μονοειδές και να προσδιορισθεί η αβελιανή ομάδα $(\mathsf{U}(\mathbb{Z} \times \mathbb{Z}), \star)$.

Λύση. (1) Παρατηρούμε ότι το σύνολο $\mathsf{U}(M)$ δεν είναι το κενό σύνολο. Πράγματι επειδή προφανώς το αντίστροφο του ουδετέρου στοιχείου e συμπίπτει με το e, έπεται ότι $e \in \mathsf{U}(M)$.

Θα δείξουμε πρώτα ότι το υποσύνολο $\mathsf{U}(M)$ είναι κλειστό στην πράξη «$\star$».

Έστω $x, y \in \mathsf{U}(M)$. Τότε:

$$\exists\, x' \in M \ \ \& \ \ y' \in M : \quad x \star x' = e = x' \star x \quad \& \quad y \star y' = e = y' \star y$$

Επομένως χρησιμοποιώντας την προσεταιριστική ιδιότητα θα έχουμε:

$$(x \star y) \star (y' \star x') = x \star (y \star y') \star x = x \star e \star x' = x \star x' = e$$

$$(y' \star x') \star (x \star y) = y' \star (x' \star x) \star y = y' \star e \star y = y' \star y = e$$

Αυτό σημαίνει ότι θα έχουμε $x \star y \in \mathsf{U}(M)$. Έτσι το σύνολο $\mathsf{U}(M)$ είναι εφοδιασμένο με την πράξη «$\star$» και η προφανώς η πράξη «$\star$» είναι προσεταιριστική επί του $\mathsf{U}(M)$ διότι είναι προσεταιριστική επί του M, και το στοιχείο e είναι ουδέτερο στοιχείο της πράξης «$\star$» επί του $\mathsf{U}(M)$. Έτσι έχουμε το μονοειδές $(\mathsf{U}(M), \star)$, το οποίο είναι ομάδα, αν κάθε στοιχείο του είναι αντιστρέψιμο. Αυτό όμως ισχύει από τον ορισμό του υποσυνόλου $\mathsf{U}(M)$: αν $x \in \mathsf{U}(M)$, τότε υπάρχει $x' \in M$ έτσι ώστε: $x \star x' = e = x' \star x$, και τότε $x' \in \mathsf{U}(M)$ και το στοιχείο x' είναι το αντίστροφο του x. Άρα το ζεύγος $(\mathsf{U}(M), \star)$ είναι ομάδα.

Προφανώς αν το μονοειδές $(M, \star)$ είναι μεταθετικό, τότε η ομάδα $(\mathsf{U}(M), \star)$ είναι αβελιανή.

(2) Υπολογίζουμε εύκολα ότι:

(α') $\mathsf{U}(\mathbb{N}) = \{1\}$.
Διότι αν $n \in \mathbb{N}$ και υπάρχει $n' \in \mathbb{N}$ έτσι ώστε $n \cdot n' = 1 = n' \cdot n$, τότε αναγκαστικά $n = 1$.

(β') $\mathsf{U}(\mathbb{Z}) = \{1, -1\}$.
Διότι αν $n \in \mathbb{Z}$ και υπάρχει $n' \in \mathbb{Z}$ έτσι ώστε $n \cdot n' = 1 = n' \cdot n$, τότε αναγκαστικά $n = 1$ ή $n = -1$.

(γ') $\mathsf{U}(\mathbb{Z}_n) = \{[k]_n \in \mathbb{Z}_n \mid 1 \leq k \leq n \ \ \& \ \ (k, n) = 1\}$.
Πράγματι: $\mathbb{Z}_n = \{[0]_n, [1]_n, \cdots, [n-1]_n\}$ και αν $[k]_n \in \mathsf{U}(\mathbb{Z}_n)$, τότε υπάρχει $[k']_n \in \mathbb{Z}_n$ έτσι ώστε:

$$[k]_n \cdot [k']_n = [1]_n \implies [k \cdot k']_n = [1]_n \implies n \mid 1 - k \cdot k' \implies 1 = k \cdot k' + n \cdot n' \text{ για κάποιο } n' \in \mathbb{Z}$$

Τότε όμως, όπως γνωρίζουμε από την Θεωρία Αριθμών: $(k, n) = 1$.
Αντίστροφα αν $(k, n) = 1$, τότε υπάρχουν ακέραιοι $k', n' \in \mathbb{Z}$ έτσι ώστε:

$$1 = k \cdot k' + n \cdot n' \implies [1]_n = [k \cdot k']_n + [n \cdot n']_n \implies [1]_n = [k]_n \cdot [k']_n + [n]_n \cdot [n']_n \implies [1]_n = [k]_n \cdot [k']_n$$

Επειδή η πράξη του πολλαπλασιασμού «$\cdot$» επί του συνόλου $\mathbb{Z}_n$ είναι μεταθετική, η τελευταία σχέση δείχνει ότι $[k]_n \in \mathsf{U}(\mathbb{Z}_n)$. Σημειώνουμε ότι $|\mathsf{U}(\mathbb{Z}_n)| = \varphi(n)$, όπου φ είναι η συνάρτηση του Euler.

(3) Χρησιμοποιώντας ότι η συνήθης πράξη πολλαπλασιασμού ακεραίων είναι προσετιαριστική και μεταθετική πράξη, εύκολα βλέπουμε ότι η πράξη «$\star$» επί του $\mathbb{Z} \times \mathbb{Z}$ είναι μεταθετική και προσεταιριστική. Επίσης:

$$\forall (x, y) \in \mathbb{Z} \times \mathbb{Z} : \ (x, y) \star (1, 1) = (x, y) = (1, 1) \star (x, y)$$

Δηλαδή το στοιχείο $(1, 1)$ είναι ουδέτερο στοιχείο για την πράξη «$\star$» επί του συνόλου $\mathbb{Z} \times \mathbb{Z}$. Επομένως το ζεύγος $(\mathsf{U}(\mathbb{Z} \times \mathbb{Z}), \star)$ είναι ένα μεταθετικό μονοειδές.

Έστω $(x, y) \in \mathsf{U}(\mathbb{Z} \times \mathbb{Z})$. Τότε υπάρχει στοιχείο $(z, w) \in \mathbb{Z} \times \mathbb{Z}$ έτσι ώστε $(x, y) \star (z, w) = (1, 1)$. Ισοδύναμα, επειδή οι αριθμοί x, y, z, w είναι ακέραιοι, θα έχουμε:

$$(xz, yw) = (1, 1) \implies xz = 1 \quad \& \quad yw = 1 \implies x = \pm 1 \quad \& \quad z = \pm 1$$

Επομένως

$$\mathsf{U}(\mathbb{Z} \times \mathbb{Z}) = \big\{(1, 1), (1, -1), (-1, 1), (-1, -1)\big\}$$

και ο πίνακας Cayley της ομάδας είναι ο ακόλουθος:

$\star$	$(\mathbf{1},\mathbf{1})$	$(\mathbf{1},-\mathbf{1})$	$(-\mathbf{1},\mathbf{1})$	$(-\mathbf{1},-\mathbf{1})$
$(\mathbf{1},\mathbf{1})$	$(1,1)$	$(1,-1)$	$(-1,1)$	$(-1,-1)$
$(\mathbf{1},-\mathbf{1})$	$(1,-1)$	$(1,1)$	$(-1,-1)$	$(-1,1)$
$(-\mathbf{1},\mathbf{1})$	$(-1,1)$	$(-1,-1)$	$(1,1)$	$(1,-1)$
$(-\mathbf{1},-\mathbf{1})$	$(-1,-1)$	$(-1,1)$	$(1,-1)$	$(1,1)$

$\blacksquare$

Παρατήρηση. *Αν $(M,\star)$ είναι ένα μονοειδές, τότε προφανώς το ζεύγος $(M,\star)$ είναι ομάδα αν και μόνον αν $\mathsf{U}(M)=M$.*

Άσκηση 9. Βρείτε όλους τους πιθανούς πίνακες Cayley ομάδων με πλήθος στοιχείων ίσο με 4.

Λύση. Έστω $(G,\star)$ μια ομάδα με 4 στοιχεία. Χωρίς βλάβη της γενικότητας μπορούμε να υποθέσουμε ότι $G=\{e,a,b,c\}$, όπου e είναι το ουδέτερο στοιχείο της G. Θέλουμε να συμπληρώσουμε τον παρακάτω πίνακα:

$\star$	**e**	**a**	**b**	**c**
e	e	a	b	c
a	a			
b	b			
c	c			

Παρατηρούμε ότι επειδή η G έχει άρτιο πλήθος στοιχείων οφείλει, λόγω της Άσκησης 2, να έχει ένα στοιχείο $x\neq e$, για το οποίο ισχύει ότι $x^2=x\star x=e$.

Χωρίς περιορισμό της γενικότητας[1] μπορούμε να υποθέσουμε ότι αυτό το στοιχείο είναι το a, δηλαδή $a\star a=e$. Έτσι τώρα ο πίνακας Cayley της ομάδας παίρνει τη μορφή:

$\star$	**e**	**a**	**b**	**c**
e	e	a	b	c
a	a	e		
b	b			
c	c			

Επειδή, γενικώς γνωρίζουμε ότι όταν η G είναι (πεπερασμένη) ομάδα, τότε κάθε στήλη και κάθε γραμμή του αντίστοιχου πίνακα Cayley, οφείλει να περιέχει κάθε στοιχείο της G ακριβώς μία φορά, ο πίνακας Cayley παίρνει τη μορφή:

$\star$	**e**	**a**	**b**	**c**
e	e	a	b	c
a	a	e	c	b
b	b	c		
c	c	b		

Τώρα για το γινόμενο $b\star b$ υπάρχουν δύο επιλογές:

$$b\star b=\begin{cases} e \\ \text{ή} \\ a \end{cases}$$

Η πρώτη περίπτωση δίνει τον πίνακα

$\star$	**e**	**a**	**b**	**c**
e	e	a	b	c
a	a	e	c	b
b	b	c	e	
c	c	b		

και η δεύτερη τον

$\star$	**e**	**a**	**b**	**c**
e	e	a	b	c
a	a	e	c	b
b	b	c	a	
c	c	b		

[1] Καταλήγουμε σε παρόμοιους πίνακες, αν επιλέξουμε $b\star b=e$ ή $c\star c=e$.

Τώρα όμως, χρησιμοποιώντας ότι κάθε στήλη και κάθε γραμμή του πίνακα Cayley μιας ομάδας G, οφείλει να περιέχει κάθε στοιχείο της G ακριβώς μία φορά, οι δύο παραπάνω πίνακες συμπληρώνονται κατά μοναδικό τρόπο και παίρνουμε:

Πίνακας Α′ :

$\star$	**e**	**a**	**b**	**c**
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Πίνακας Β′:

$\star$	**e**	**a**	**b**	**c**
e	e	a	b	c
a	a	e	c	b
b	b	c	a	e
c	c	b	e	a

Η ομάδα που έχει ως πίνακα πράξης τον Πίνακα Α′ ονομάζεται **η ομάδα $\mathcal{V}_4$ των τεσσάρων στοιχείων του Klein**.

• Μια ομάδα που είναι «ισόμορφη», δηλαδή δομικά ίδια, με την ομάδα $\mathcal{V}_4$ του Klein είναι το ευθύ γινόμενο της $(\mathbb{Z}_2, +)$ με τον εαυτό της, δηλαδή η $\mathbb{Z}_2 \times \mathbb{Z}_2$ με την επαγόμενη πράξη.

$$\mathbb{Z}_2 \times \mathbb{Z}_2 = \big\{([0]_2, [0]_2), ([0]_2, [1]_2), ([1]_2, [0]_2), ([1]_2, [1]_2)\big\}$$

$$([a]_2, [b]_2) + ([c]_2, [d]_2) = ([a]_2 + [c]_2, [b]_2 + [d]_2) = ([a + c]_2, [b + d]_2)$$

που έχει πίνακα Cayley:

$+$	$([\mathbf{0}], [\mathbf{0}])$	$([\mathbf{1}], [\mathbf{0}])$	$([\mathbf{0}], [\mathbf{1}])$	$([\mathbf{1}], [\mathbf{1}])$
$([\mathbf{0}], [\mathbf{0}])$	$([0], [0])$	$([1], [0])$	$([0], [1])$	$([1], [1])$
$([\mathbf{1}], [\mathbf{0}])$	$([1], [0])$	$([0], [0])$	$([1], [1])$	$([0], [1])$
$([\mathbf{0}], [\mathbf{1}])$	$([0], [1])$	$([1], [1])$	$([0], [0])$	$([1], [0])$
$([\mathbf{1}], [\mathbf{1}])$	$([1], [1])$	$([0], [1])$	$([1], [0])$	$([0], [0])$

όπου για ευκολία συμβολίσαμε με $[a]$ το στοιχείο $[a]_2 \in \mathbb{Z}_2$, $a = 0, 1$.

– Προσέξτε ότι η αντιστοιχία

$$e \longleftrightarrow ([0], [0]), \quad a \longleftrightarrow ([1], [0]), \quad b \longleftrightarrow ([0], [1]), \quad c \longleftrightarrow ([1], [1])$$

μεταξύ των στοιχείων της G και των στοιχείων της $\mathbb{Z}_2 \times \mathbb{Z}_2$ μεταφέρεται και σε αντιστοιχία μεταξύ των στοιχείων του Πίνακα Α′ και των στοιχείων του πίνακα Cayley της $\mathbb{Z}_2 \times \mathbb{Z}_2$.

• Μια ομάδα που είναι «ισόμορφη», δηλαδή δομικά ίδια, με την ομάδα που έχει ως πίνακα Cayley τον Πίνακα Β′ είναι η $(\mathbb{Z}_4, +)$. Ο πίνακας Cayley της $(\mathbb{Z}_4, +)$ είναι ο:

$+$	$[\mathbf{0}]$	$[\mathbf{1}]$	$[\mathbf{2}]$	$[\mathbf{3}]$
$[\mathbf{0}]$	$[0]$	$[1]$	$[2]$	$[3]$
$[\mathbf{1}]$	$[1]$	$[2]$	$[3]$	$[0]$
$[\mathbf{2}]$	$[2]$	$[3]$	$[0]$	$[1]$
$[\mathbf{3}]$	$[3]$	$[0]$	$[1]$	$[2]$

όπου για ευκολία συμβολίσαμε με $[a]$ το στοιχείο $[a]_4 \in \mathbb{Z}_4$, $a = 0, 1, 2, 3$.

– Προσέξτε ότι η αντιστοιχία

$$e \longleftrightarrow [0], \quad a \longleftrightarrow [1], \quad b \longleftrightarrow [2], \quad c \longleftrightarrow [3]$$

μεταξύ των στοιχείων της G και των στοιχείων της $\mathbb{Z}_4$ μεταφέρεται και μεταξύ των στοιχείων του Πίνακα Β′ και των στοιχείων του πίνακα Cayley της $\mathbb{Z}_4$. ■

Παρατήρηση. *Οι πίνακες Cayley Α′ και Β′ είναι διαφορετικοί: ο Πίνακας Α′ είναι ο πίνακας Cayley μιας ομάδας G κάθε στοιχείο a της οποίας ικανοποιεί τη σχέση $a^2 = a \star a = e$. Ο Πίνακας Β′ είναι ο πίνακας Cayley μιας ομάδας G στην οποία υπάρχει στοιχείο x έτσι ώστε $x^2 = x \star x \neq e$.*

Η ομάδα G με πίνακα Cayley τον Πίνακα Α′ μπορεί να περιγραφεί ως

$$G = \big\{e, a, b, a \star b\big\}$$

Η ομάδα G με πίνακα Cayley τον Πίνακα Β΄ μπορεί να περιγραφεί ως

$$G = \{e, b, b^2, b^3\}$$

Παρατηρούμε ότι και στις δύο δυνατές περιπτώσεις ομάδας με πλήθος στοιχείων ίσο με 4, η ομάδα είναι αβελιανή. Κάθε ομάδα με πλήθος στοιχείων ίσο με 4, πιθανόν μετά από κάποια αναδιάταξη των στοιχείων της, έχει πίνακα Cayley είτε το πίνακα Α΄ είτε τον πίνακα Β΄. ▲

Άσκηση 10. Να δειχθεί με ένα παράδειγμα, ότι είναι δυνατόν η εξίσωση $x \star x = e$ να έχει περισσότερες από δύο λύσεις, σε μια ομάδα $(G, \star)$ με ταυτοτικό στοιχείο e.

Λύση. Η ομάδα των τεσσάρων στοιχείων $\mathcal{V}_4 = \{e, a, b, c\}$ του Klein είναι ένα τέτοιο παράδειγμα, αφού έχουμε ότι

$$a \star a = e, \qquad b \star b = e, \qquad c \star c = e$$

Ιδιαίτερα αν ταυτίσουμε την ομάδα $\mathcal{V}_4$ του Klein με την ομάδα $(\mathbb{Z}_2 \times \mathbb{Z}_2, +)$, όπως στην προηγούμενη Άσκηση 9, τότε (εδώ $[a]$ σημαίνει $[a]_2$):

$$\begin{cases} a = ([1],[0]) \implies ([1],[0]) + ([1],[0]) = ([0],[0]) \\[2ex] b = ([0],[1]) \implies ([0],[1]) + ([0],[1]) = ([0],[0]) \\[2ex] c = ([1],[1]) \implies ([1],[1]) + ([1],[1]) = ([0],[0]) \end{cases}$$

Για ένα άλλο ενδιαφέρον παράδειγμα δείτε την Άσκηση 13. ■

Άσκηση 11. Θεωρούμε τους ακόλουθους αντιστρέψιμους πίνακες πραγματικών αριθμών:

$$A = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} \in \mathsf{GL}_4(\mathbb{R}) \quad \text{και} \quad B = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} \in \mathsf{GL}_4(\mathbb{R})$$

και έστω

$$G = \{A^n \in \mathsf{GL}_4(\mathbb{R}) \mid n \in \mathbb{Z}\} \qquad \text{και} \qquad G' = \{B^n \in \mathsf{GL}_4(\mathbb{R}) \mid n \in \mathbb{Z}\}$$

Να δείξετε ότι τα ζεύγη $(G, \cdot)$ και $(G', \cdot)$, όπου «$\cdot$» είναι ο συνήθης πολλαπλασιασμός πινάκων, είναι αβελιανές ομάδες. Πόσα στοιχεία έχουν οι ομάδες G και G';

Λύση. Υπολογίζοντας τις δυνάμεις A^n και B^n βρίσκουμε ότι

$$A^2 = I_4, \qquad B^2 = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \qquad B^3 = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}, \qquad B^4 = I_4$$

Άρα τα σύνολα G και G' είναι τα ακόλουθα:

$$G = \{I_4, A\} \quad \text{και} \quad G' = \{I_4, B, B^2, B^3\}$$

Είναι φανερό ότι τα σύνολα G και G' είναι ομάδες με $A^{-1} = A$ και $B^{-1} = B^3$. Η ομάδα G είναι προφανώς αβελιανή και αφού

$$B^i \cdot B^j = B^{i+j} = B^{j+i} = B^j \cdot B^i$$

έπεται ότι η ομάδα G' είναι αβελιανή. Τέλος έχουμε $|G| = 2$ και $|G'| = 4$. ■

Αν $(G, \star)$ είναι μια ομάδα και $a \in G$, τότε η **κυκλική υποομάδα η οποία παράγεται από το στοιχείο** a είναι το σύνολο

$$\langle a \rangle = \{a^n \in G \mid n\mathbb{Z}\}$$

και το ζεύγος $(\langle a\rangle, \star)$ είναι μια αβελιανή ομάδα. Αν η ομάδα έχει δοθεί με προσθετικό συμβολισμό $(G, +)$, τότε

$$\langle a\rangle = \{na \in G \mid n\mathbb{Z}\}$$

Το στοιχείο a καλείται **γεννήτορας** της G αν: $\langle a\rangle = G$.

Άσκηση 12. Μελετήστε τη δομή της ομάδας $(\mathbb{Z}_6, +)$, και συμπληρώστε τον πίνακα Cayley

$+$	$[\mathbf{0}]_\mathbf{6}$	$[\mathbf{1}]_\mathbf{6}$	$[\mathbf{2}]_\mathbf{6}$	$[\mathbf{3}]_\mathbf{6}$	$[\mathbf{4}]_\mathbf{6}$	$[\mathbf{5}]_\mathbf{6}$
$[\mathbf{0}]_\mathbf{6}$						
$[\mathbf{1}]_\mathbf{6}$						
$[\mathbf{2}]_\mathbf{6}$						
$[\mathbf{3}]_\mathbf{6}$						
$[\mathbf{4}]_\mathbf{6}$						
$[\mathbf{5}]_\mathbf{6}$						

Λύση. Ο πίνακας Cayley της $(\mathbb{Z}_6, +)$ είναι ο ακόλουθος (εδώ $[a]$ σημαίνει $[a]_6$):

$+$	$[\mathbf{0}]$	$[\mathbf{1}]$	$[\mathbf{2}]$	$[\mathbf{3}]$	$[\mathbf{4}]$	$[\mathbf{5}]$
$[\mathbf{0}]$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$	$[5]$
$[\mathbf{1}]$	$[1]$	$[2]$	$[3]$	$[4]$	$[5]$	$[0]$
$[\mathbf{2}]$	$[2]$	$[3]$	$[4]$	$[5]$	$[0]$	$[1]$
$[\mathbf{3}]$	$[3]$	$[4]$	$[5]$	$[0]$	$[1]$	$[2]$
$[\mathbf{4}]$	$[4]$	$[5]$	$[0]$	$[1]$	$[2]$	$[3]$
$[\mathbf{5}]$	$[5]$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$

Στη συνέχεια υπολογίζουμε τις κυκλικές υποομάδες που παράγονται από τα στοιχεία της $\mathbb{Z}_6$. Έχουμε:

- $\langle[0]\rangle = \{[0]\}$
- $\langle[1]\rangle = \{[0], [1], [2], [3], [4], [5]\} = \langle[5]\rangle$
- $\langle[2]\rangle = \{[0], [2], [4]\} = \langle[4]\rangle$
- $\langle[3]\rangle = \{[0], [3]\}$

Παρατηρούμε ότι

$$\mathbb{Z}_6 = \langle[1]\rangle = \langle[5]\rangle$$

και επομένως τα στοιχεία $[1]$ και $[5]$ είναι οι γεννήτορες της ομάδας $(\mathbb{Z}_6, +)$. ■

Άσκηση 13. Θεωρούμε το σύνολο απεικονίσεων

$$G = \Big\{\alpha_0, \alpha_1, \alpha_2, \beta_1, \beta_2, \beta_3 \,:\, \mathbb{Q}\setminus\{0,1\} \longrightarrow \mathbb{Q}\setminus\{0,1\}\Big\}$$

όπου:

$$\alpha_0(x) = x, \qquad \alpha_1(x) = \frac{1}{1-x}, \qquad \alpha_2(x) = \frac{x-1}{x}$$
$$\beta_1(x) = \frac{1}{x}, \qquad \beta_2(x) = 1-x, \qquad \beta_3(x) = \frac{x}{x-1}$$

Να δειχθεί ότι το ζεύγος $(G, \circ)$, όπου «$\circ$» είναι πράξη της σύνθεσης απεικονίσεων, αποτελεί μια μη-αβελιανή ομάδα. Να συμπληρωθεί ο αντίστοιχος πίνακας Cayley της ομάδας $(G, \circ)$.

Λύση. Ο πίνακας Cayley της G είναι ο ακόλουθος:

$\circ$	$\alpha_\mathbf{0}$	α_1	α_2	β_1	β_2	β_3
α_0	α_0	α_1	α_2	β_1	β_2	β_3
α_1	α_1	α_2	α_0	β_3	β_1	β_2
α_2	α_2	α_0	α_1	β_2	β_3	β_1
β_1	β_1	β_2	β_3	α_0	α_1	α_2
β_2	β_2	β_3	β_1	α_2	α_0	α_1
β_3	β_3	β_1	β_2	α_1	α_2	α_0

Οι υπολογισμοί στον πίνακα δείχνουν ότι το σύνολο G είναι κλειστό στη πράξη της σύνθεσης, και επομένως η σύνθεση είναι μια καλά ορισμένη πράξη επί του συνόλου G:

$$\circ : G \times G \longrightarrow G$$

Γνωρίζουμε ότι η σύνθεση απεικονίσεων είναι προσεταιριστική. Επίσης η απεικόνιση $\alpha_0 = \mathrm{Id}_{\mathbb{Q}\setminus\{0,1\}}$ είναι το ουδέτερο στοιχείο και τα αντίστροφα στοιχεία των απεικονίσεων $\alpha_0, \alpha_1, \alpha_2, \beta_1, \beta_2, \beta_3$ είναι τα εξής:

$$\alpha_1^{-1} = \alpha_2, \quad \alpha_2^{-1} = \alpha_1, \quad \beta_1^{-1} = \beta_1, \quad \beta_2^{-1} = \beta_2, \quad \beta_3^{-1} = \beta_3$$

Άρα το ζεύγος $(G, \circ)$ είναι ομάδα. Να σημειώσουμε ότι τα στοιχεία $\beta_1, \beta_2, \beta_3$ έχουν την ιδιότητα:

$$\beta_1^2 = \mathrm{Id}_{\mathbb{Q}\setminus\{0,1\}} = \alpha_0, \quad \beta_2^2 = \mathrm{Id}_{\mathbb{Q}\setminus\{0,1\}} = \alpha_0, \quad \beta_3^2 = \mathrm{Id}_{\mathbb{Q}\setminus\{0,1\}} = \alpha_0$$

δηλαδή τα στοιχεία $\beta_1, \beta_2, \beta_3$ είναι λύσεις της εξίσωσης $x^2 = \mathrm{Id}_{\mathbb{Q}\setminus\{0,1\}}$ στη G (βλέπε την Άσκηση 10). Όμως η ομάδα $(G, \circ)$ δεν είναι αβελιανή, διότι για παράδειγμα:

$$(\beta_1 \circ \alpha_2)(x) = \beta_1(\alpha_2(x)) = \beta_1\big(\frac{x-1}{x}\big) = \frac{1}{\frac{x-1}{x}} = \frac{x}{x-1} = \beta_3(x)$$

$$(\alpha_2 \circ \beta_1)(x) = \alpha_2(\beta_1(x)) = \alpha_2\big(\frac{1}{x}\big) = \frac{\frac{1}{x} - 1}{\frac{1}{x}} = \frac{\frac{1-x}{x}}{\frac{1}{x}} = 1 - x = \beta_2(x)$$

και άρα $\beta_1 \circ \alpha_2 = \beta_3 \neq \beta_2 = \alpha_2 \circ \beta_1$. ■

Άσκηση 14. Έστω ότι «$\star$» είναι μια προσεταιριστική πράξη επί ενός συνόλου G. Υποθέτουμε ότι:

(1) Υπάρχει ένα στοιχείο[2] $e \in G$: $e \star x = x, \ \forall x \in G$.
(2) Για κάθε $x \in G$, υπάρχει ένα στοιχείο[3] $x' \in G$: $x' \star x = e$.

Να δειχθεί ότι το ζεύγος $(G, \star)$ είναι ομάδα.

Λύση. Επειδή $e \star x = x, \ \forall x \in G$, τότε επιλέγοντας $x = e$ έχουμε

$$e \star e = e \tag{3}$$

Επίσης επειδή για κάθε $x \in G$ υπάρχει ένα στοιχείο $x' \in G$ έτσι ώστε $x' \star x = e$, τότε έπεται ότι

$$(x')' \star x' = e \tag{4}$$

Έστω $x \in G$. Τότε από την υπόθεση (2) και τη σχέση (3) έχουμε:

$$\begin{aligned}
(x' \star x) \star e = e \star e = e = x' \star x \quad &\Longrightarrow \quad (x' \star x) \star e = x' \star x \\
&\Longrightarrow \quad (x')' \star \big[(x' \star x) \star e\big] = (x')' \star (x' \star x) \\
&\Longrightarrow \quad \big[(x')' \star (x' \star x)\big] \star e = \big[(x')' \star x'\big] \star x \\
&\overset{(4)}{\Longrightarrow} \quad \big([(x')' \star x'] \star x\big) \star e = e \star x \\
&\overset{(4)}{\Longrightarrow} \quad (e \star x) \star e = e \star x \\
&\overset{(1)}{\Longrightarrow} \quad x \star e = e \star x
\end{aligned}$$

Επομένως δείξαμε ότι

$$\boxed{e \star x = x = x \star e, \quad \forall x \in G} \tag{5}$$

---

[2]Ένα στοιχείο $e \in G$ έτσι ώστε $e \star x = x, \ \forall x \in G$, καλείται **αριστερό ουδέτερο στοιχείο** για την πράξη «$\star$».

[3]Αν για την προσεταιριστική πράξη «$\star$» επί του συνόλου G υπάρχει αριστερό ουδέτερο στοιχείο e, τότε ένα στοιχείο $x' \in G$ έτσι ώστε $x' \star x = e$, καλείται **αριστερό αντίστροφο στοιχείο** του x για την πράξη «$\star$».

Έστω $x \in G$. Από την υπόθεση (2) έχουμε:

$$\begin{aligned} x' \star x = e \quad &\Longrightarrow \quad (x' \star x) \star x' = e \star x' = x' \\ &\Longrightarrow \quad (x')' \star \big[(x' \star x) \star x'\big] = (x')' \star x' \\ &\overset{(4)}{\Longrightarrow} \quad \big[(x')' \star x'\big] \star (x \star x') = e \\ &\overset{(4)}{\Longrightarrow} \quad e \star (x \star x') = e \\ &\overset{(1)}{\Longrightarrow} \quad x \star x' = e \end{aligned}$$

Άρα έχουμε ότι

$$\boxed{\forall x \in G,\ \exists\ x' \in G\colon \quad x' \star x = e = x \star x'} \tag{6}$$

Συνεπώς από τις σχέσεις (5) και (6) συμπεραίνουμε ότι το ζεύγος $(G, \star)$ είναι ομάδα. ■

Άσκηση 15. Γνωρίζουμε ότι αν $(G, \star)$ είναι μια ομάδα, τότε οι εξισώσεις

$$a \star x = b \qquad \text{και} \qquad x \star a = b$$

έχουν (μοναδική) λύση για κάθε $a, b \in G$.

Αντίστροφα: να δειχθεί ότι αν «$\star$» είναι μια προσεταιριστική πράξη επί του μη-κενού συνόλου G και οι παραπάνω εξισώσεις έχουν λύση για κάθε $a, b \in G$, τότε υπάρχει ουδέτερο στοιχείο $e \in G$ για την πράξη «$\star$» και το ζεύγος $(G, \star)$ είναι μια ομάδα.

Λύση. Υποθέτουμε ότι οι εξισώσεις $a \star x = b$ και $x \star a = b$ έχουν λύση για κάθε $a, b \in G$. Έστω a ένα στοιχείο της G και έστω e μια λύση της εξίσωσης $x \star a = a$, δηλαδή $e \star a = a$. Θα δείξουμε ότι $e \star b = b$ για κάθε $b \in G$. Έστω c μια λύση της εξίσωσης $a \star x = b$, δηλαδή $a \star c = b$. Τότε για κάθε $b \in G$ έχουμε:

$$e \star b = e \star (a \star c) = (e \star a) \star c = a \star c = b \implies \boxed{e \star b = e, \quad \forall b \in G} \tag{1}$$

Έστω $a \in G$ και θεωρούμε την εξίσωση $x \star a = e$. Τότε έχουμε ότι υπάρχει $a' \in G$ έτσι ώστε $a' \star a = e$. Επομένως δείξαμε ότι

$$\boxed{\forall a \in G,\ \exists\ a' \in G \quad \text{έτσι ώστε:} \quad a' \star a = e} \tag{2}$$

Από την Άσκηση 13 και τις σχέσεις (1) και (2) έπεται ότι το ζεύγος $(G, \star)$ είναι μια ομάδα. ■

Άσκηση 16. **1.** Στο σύνολο $G = \mathbb{R}^* \times \mathbb{R}$ ορίζουμε μια πράξη «$\star$» ως εξής:

$$\star\colon\ G \times G \longrightarrow G, \qquad (a, b) \star (c, d) = (ac, ad + b)$$

Να δειχθεί ότι το ζεύγος $(G, \star)$ είναι ομάδα.

2. Να δειχθεί ότι το σύνολο

$$G' = \big\{ f\colon \mathbb{R} \longrightarrow \mathbb{R} \mid f(x) = ax + b, \quad a, b \in \mathbb{R},\ a \neq 0 \big\}$$

εφοδιασμένο με την πράξη της σύνθεσης απεικονίσεων είναι ομάδα.

3. Παρατηρείτε κάποια σχέση μεταξύ των ομάδων, G και G';

Λύση. **1.** Έστω $(a_1, b_1), (a_2, b_2), (a_3, b_3) \in G = \mathbb{R}^* \times \mathbb{R}$. Έχουμε:

- Η πράξη «$\star$» είναι προσεταιριστική:

$$(a_1, b_1) \star \big[(a_2, b_2) \star (a_3, b_3)\big] = (a_1, b_1) \star (a_2 a_3, a_2 b_3 + b_2) = (a_1 a_2 a_3, a_1 a_2 b_3 + a_1 b_2 + b_1)$$

και

$$\big[(a_1, b_1) \star (a_2, b_2)\big] \star (a_3, b_3) = (a_1 a_2, a_1 b_2 + b_1) \star (a_3, b_3) = (a_1 a_2 a_3, a_1 a_2 b_3 + a_1 b_2 + b_1)$$

Άρα η πράξη «$\star$» είναι προσεταιριστική.

• Ουδέτερο στοιχείο: Έστω στοιχείο $(e_1, e_2) \in G$ έτσι ώστε $(a,b)\star(e_1,e_2) = (a,b) = (e_1,e_2)\star(a,b)$ για κάθε $(a,b) \in G$. Τότε

$$(ae_1, ae_2 + b) = (a,b) \implies \begin{cases} ae_1 = a \\ \\ ae_2 + b = b \end{cases} \stackrel{a\neq 0}{\Longrightarrow} \begin{cases} e_1 = 1 \\ \\ e_2 = 0 \end{cases}$$

Το στοιχείο $e = (e_1, e_2) = (1,0) \in G = \mathbb{R}^* \times \mathbb{R}$ και

$$(a,b) \star (1,0) = (a\cdot 1, a\cdot 0 + b) = (a,b) = (1\cdot a, 1\cdot b + 0) = (1,0) \star (a,b)$$

για κάθε $(a,b) \in G$. Συνεπώς το $e = (1,0)$ είναι το ουδέτερο στοιχείο της πράξης «$\star$».

• Αντίστροφο στοιχείο: Έστω $(a,b) \in G$ και υποθέτουμε ότι υπάρχει ένα $(x,y) \in G$ έτσι ώστε $(a,b) \star (x,y) = (1,0)$. Τότε

$$(ax, ay + b) = (1,0) \implies \begin{cases} ax = 1 \\ \\ ay + b = 0 \end{cases} \stackrel{a\neq 0}{\Longrightarrow} \begin{cases} x = \frac{1}{a} \\ \\ y = -\frac{b}{a} \end{cases}$$

και άρα έχουμε

$$(a,b) \star (\frac{1}{a}, -\frac{b}{a}) = (a\frac{1}{a}, -\frac{ba}{a} + b) = (1,0) = (\frac{1}{a}a, \frac{b}{a} - \frac{b}{a}) = (\frac{1}{a}, -\frac{b}{a}) \star (a,b)$$

Επομένως για κάθε $(a,b) \in G$ το αντίστροφο στοιχείο της πράξης «$\star$» είναι $(a,b)' = (\frac{1}{a}, -\frac{b}{a}) \in G$.

Άρα το ζεύγος $(G, \star)$ είναι ομάδα. Παρατηρούμε ότι η ομάδα G δεν είναι αβελιανή διότι για παράδειγμα

$$(1,2) \star (2,3) = (2,5) \neq (2,7) = (2,3) \star (1,2)$$

2. Για κάθε $f \in G'$ θα γράφουμε $f := f_{a,b} \colon \mathbb{R} \longrightarrow \mathbb{R}$, όπου $f_{a,b}(x) = ax + b$ με $a \neq 0$. Έχουμε:

• Η πράξη «$\circ$» είναι προσεταιριστική: Είναι γνωστό ότι η σύνθεση απεικονίσεων «$\circ$» είναι προσεταιριστική.

• Ουδέτερο στοιχείο: Η ταυτοτική απεικόνιση $f_{1,0} = \mathrm{Id}_{\mathbb{R}} \colon \mathbb{R} \longrightarrow \mathbb{R}$, $\mathrm{Id}_{\mathbb{R}}(x) = x = 1\cdot x + 0 \in G'$, είναι προφανώς το ουδέτερο στοιχείο της G'.

• Αντίστροφο στοιχείο: Έστω $f_{a,b} \in G'$ και υποθέτουμε ότι υπάρχει μια συνάρτηση $f_{c,d} \in G'$ έτσι ώστε $f_{a,b} \circ f_{c,d} = f_{1,0}$. Τότε για κάθε $x \in \mathbb{R}$ έχουμε:

$$f_{a,b}\big(f_{c,d}(x)\big) = x \implies f_{a,b}(cx + d) = x \implies a\cdot(cx + d) + b = x \implies acx + ad + b = x$$

$$\implies \begin{cases} ad + b = 0 \\ \\ ac = 1 \end{cases} \stackrel{a\neq 0}{\Longrightarrow} \begin{cases} d = -\frac{b}{a} \\ \\ c = \frac{1}{a} \end{cases}$$

Άρα έχουμε

$$f_{a,b}\big(f_{\frac{1}{a},-\frac{b}{a}}(x)\big) = f_{a,b}(\frac{1}{a}x - \frac{b}{a}) = a\frac{1}{a}x - a\frac{b}{a} + b = x \implies f_{a,b} \circ f_{\frac{1}{a},-\frac{b}{a}} = f_{1,0}$$

και όμοια δείχνουμε ότι

$$f_{\frac{1}{a},-\frac{b}{a}} \circ f_{a,b} = f_{1,0}$$

Επομένως για κάθε $f_{a,b} \in G'$ το αντίστροφο στοιχείο είναι η συνάρτηση

$$(f_{a,b})' = (f_{a,b})^{-1} = f_{\frac{1}{a},-\frac{b}{a}} \in G'$$

Άρα το σύνολο $(G', \circ)$ είναι ομάδα, η οποία δεν είναι αβελιανή διότι γενικά η σύνθεση συναρτήσεων δεν είναι μεταθετική:

$$f_{a,b} \circ f_{c,d} = f_{ac,ad+b} \quad \text{και} \quad f_{c,d} \circ f_{a,b} = f_{ca,cb+d}$$

Έτσι για παράδειγμα:

$$f_{1,1} \circ f_{-1,1} = f_{-1,2} \neq f_{-1,0} = f_{-1,1} \circ f_{1,1}$$

3. Παρατηρούμε ότι υπάρχει μια αντιστοιχία μεταξύ των στοιχείων, των πράξεων, των ουδέτερων στοιχείων και των αντίστροφων στοιχείων της G και G' αντίστοιχα:

$$\begin{array}{rcl} G & \longleftrightarrow & G' \\ \\ (a,b) & \longleftrightarrow & f_{a,b}(x) = ax + b \\ \\ (a,b) \star (c,d) = (ac, ad+b) & \longleftrightarrow & f_{a,b} \circ f_{c,d} = f_{ac,ad+b} \\ \\ (1,0) & \longleftrightarrow & f_{1,0} = \mathrm{Id}_{\mathbb{R}} \\ \\ (a,b)' = (\dfrac{1}{a}, -\dfrac{b}{a}) & \longleftrightarrow & (f_{a,b})' = f_{\frac{1}{a},-\frac{b}{a}} \end{array}$$

Αργότερα θα δείξουμε ότι αυτές οι ομάδες είναι «ισόμορφες» μεταξύ τους, δηλαδή ότι υπάρχει μια απεικόνιση από τη G στη G' η οποία διατηρεί τις πράξεις των ομάδων και είναι «1-1» και «επί». ■

Άσκηση 17. Έστω $(M, \star_1)$ και $(M_2, \star_2)$ δύο μονοειδή. Να δειχθεί ότι ορίζοντας:

$$(m_1, m_2) \star (n_1, n_2) = (m_1 \star_1 n_1, m_2 \star_2 n_2)$$

το ζεύγος $(M_1 \times M_2, \star)$ είναι ένα μονοειδές, το οποίο καλείται **μονοειδές ευθύ γινόμενο** των $(M, \star_1)$ και $(M, \star_2)$. Επιπλέον να δειχθούν τα εξής:

(1) Το μονοειδές $(M_1 \times M_2, \star)$ είναι μεταθετικό αν και μόνον αν τα μονοειδή $(M_1, \star_1)$ και $(M_2, \star_2)$ είναι μεταθετικά.

(2) Για τις αντίστοιχες ομάδες των αντιστρέψιμων στοιχείων έχουμε:

$$\mathsf{U}(M_1 \times M_2, \star) = \mathsf{U}(M_1, \star_1) \times \mathsf{U}(M_2, \star_2)$$

(3) Το μονοειδές $(M_1 \times M_2, \star)$ είναι ομάδα αν και μόνον αν τα μονοειδή $(M_1, \star_1)$ και $(M_2, \star_2)$ είναι ομάδες.

Λύση. Προφανώς η πράξη «$\star$» είναι καλά ορισμένη επί του συνόλου $M_1 \times M_2$.

Έστω (x_1, x_2), (y_1, y_2) και (z_1, z_2) τυχόντα στοιχεία του συνόλου $M_1 \times M_2$. Τότε χρησιμοποιώντας την προσεταιριστικότητα των πράξεων «$\star_1$» και «$\star_2$» στα μονοειδή $(M_1, \star_1)$ και $(M_2, \star_2)$ αντίστοιχα, θα έχουμε:

$$(x_1, x_2) \star \big((y_1, y_2 \star (z_1, z_2)\big) = (x_1, x_2) \star (y_1 \star_1 z_1, y_2 \star_2 z_2) = \big(x_1 \star_1 (y_1 \star z_1), x_2 \star_2 (y_2 \star_2 z_2)\big) =$$

$$= \big((x_1 \star_1 y_1) \star_1 z_1, (x_2 \star_2 y_2) \star_2 z_2\big) = (x_1 \star_1 y_1, x_2 \star_2 y_2) \star (z_1, z_2) = \big((x_1, x_2) \star (y_1, y_2)\big) \star (z_1, z_2)$$

Επομένως η πράξη «$\star$» επί του συνόλου $M_1 \times M_2$ είναι προσεταιριστική.

Έστω e_1 το ουδέτερο στοιχείο του μονοειδούς $(M_1, \star_1)$ και e_1 το ουδέτερο στοιχείο του μονοειδούς $(M_2, \star_2)$. Ισχυριζόμαστε ότι το στοιχείο (e_1, e_2) είναι το ουδέτερο στοιχείο του $M_1 \times M_2$ ως προς την πράξη «$\star$». Πράγματι, για κάθε στοιχείο $(x_1, x_2) \in M_1 \times M_2$ θα έχουμε:

$$(x_1, x_2) \star (e_1, e_2) = (x_1 \star_1 e_1, x_2 \star_2 e_2) = (x_1, x_2) = (e_1 \star_1 x_1, e_2 \star_2 x_2) = (e_1, e_2) \star (x_1, x_2)$$

Επομένως το ζεύγος $(M_1 \times M_2, \star)$ είναι ένα μονοειδές.

(1) Αν τα μονοειδή $(M,\star_1)$ και $(M,\star_2)$ είναι μεταθετικά, τότε για τυχόντα στοιχεία (x_1,x_2) και (y_1,y_2) του μονοειδούς $(M_1\times M_2,\star)$, θα έχουμε:

$$(x_1,x_2)\star(y_1,y_2)=(x_1\star_1 y_1,x_2\star_2 y_2)=(y_1\star_1 x_1,y_2\star_2 x_2)=(y_1,y_2)\star(x_1,x_2)$$

και επομένως το μονοειδές $(M_1\times M_2,\star)$ είναι μεταθετικό.

Αντίστροφα, έστω ότι το μονοειδές $(M_1\times M_2,\star)$ είναι μεταθετικό, και έστω $x_1,y_1\in M_1$ και $x_2,y_2\in M_2$. Τότε θα έχουμε:

$$(x_1,e_2)\star(y_1,e_2)=(y_1,e_2)\star(x_1,e_2)\implies(x_1\star_1 y_1,e_2\star_2 e_2)=(y_1\star_1 x_1,e_2\star_2 e_2)\implies$$
$$\implies x_1\star_1 y_1=y_1\star_1 x_1$$

και παρόμοια

$$(e_1,x_2)\star(e_1,y_2)=(e_1,y_2)\star(e_1,x_2)\implies(e_1\star_1 e_1,x_2\star_2 y_2)=(e_1\star_1 e_1,y_2\star_2 x_2)\implies$$
$$\implies x_2\star_2 y_2=y_2\star_2 x_2$$

Επομένως τα μονοειδή $(M_1,\star_1)$ και $(M_2,\star_2)$ είναι μεταθετικά.

(2) Έστω $(x_1,x_2)\in\mathsf{U}(M_1\times M_2,\star)$. Τότε υπάρχει στοιχείο $(y_1,y_2)\in M_1\times M_2$ έτσι ώστε:

$$(x_1,x_2)\star(y_1,y_2)=(e_1,e_2)=(y_1,y_2)\star(x_1,x_2)\implies(x_1\star_1 y1,x_2\star_2 y_2)=(e_1,e_2)=(y_1\star_1 x_1,y_2\star_2 x_2)$$
$$\implies x_1\star_1 y_1=e_1=y_1\star_1 x_1\quad\text{και}\quad x_2\star_2 y_2=e_2=y_2\star_2 x_2\implies y_1=x_1'\implies y_2=x_2'$$

δηλαδή τα στοιχεία $x_1\in M_1$ και $x_2\in M_2$ είναι αντιστρέψιμα και $y_1=x_1'$ και $y_2=x_2'$. Άρα $(x_1,x_2)\in\mathsf{U}(M_1,\star_1)\times\mathsf{U}(M_2,\star_2)$ και επομένως $\mathsf{U}(M_1\times M_2,\star)\subseteq\mathsf{U}(M_1,\star_1)\times\mathsf{U}(M_2,\star_2)$.

Αντίστροφα, έστω $(x_1,x_2\in\mathsf{U}(M_1,\star_1)\times\mathsf{U}(M_2,\star_2)$. Τότε το x_1 είναι αντιστρέψιμο στοιχείο του μονοειδούς $(M_1,\star_1)$, με αντίστροφο έστω το στοιχείο x_1', και το x_2 είναι αντιστρέψιμο στοιχείο του μονοειδούς $(M_2,\star_2)$, με αντίστροφο έστω το στοιχείο x_1'. Τότε θα έχουμε:

$$(x_1,x_2)\star(x_1',x_2')=(x_1\star_1 x_1',x_2\star_2 x_2')=(e_1,e_2)\quad\text{και}\quad(x_1',x_2')\star(x_1,x_2)=(x_1'\star_1 x_1,x_2'\star_2 x_2)=(e_1,e_2)$$

δηλαδή το στοιχείο (x_1,x_2) του μονοειδούς $(M_1\times M_2,\star)$ είναι αντιστρέψιμο και το αντίστροφό του είναι το $(x_1,x_2)'=(x_1',x_2')$. Άρα $(x_1,x_2)\in\mathsf{U}(M_1\times M_2,\star)$ και επομένως $\mathsf{U}(M_1,\star_1)\times\mathsf{U}(M_2,\star_2)\subseteq\mathsf{U}(M_1\times M_2,\star)$.

Έτσι δείξαμε ότι $\mathsf{U}(M_1,\star_1)\times\mathsf{U}(M_2,\star_2)=\mathsf{U}(M_1\times M_2,\star)$.

(3) Αν το μονοειδή $(M,\star_1)$ και $(M,\star_2)$ είναι ομάδες, τότε χρησιμοποιώντας το μέρος (3), θα έχουμε

$$\mathsf{U}(M_1,\star_1)=(M_1,\star_1)\quad\text{και}\quad\mathsf{U}(M_2,\star_2)=(M_2,\star_2)\implies\mathsf{U}(M_1\times M_2,\star)=(M_1,\star_1)\times(M_2,\star_2)$$

Η παραπάνω ισότητα δείχνει ότι κάθε στοιχείο του μονοειδούς $(M_1\times M_2,\star)$ είναι αντιστρέψιμο και άρα το μονοειδές $(M_1\times M_2,\star)$ είναι ομάδα. Αντίστροφα αν το μονοειδές $(M_1\times M_2,\star)$ είναι ομάδα, τότε θα έχουμε μια ισότητα $\mathsf{U}(M_1\times M_2,\star)=(M_1,\star_1)\times(M_2,\star_2)$ και άρα από το μέρος (3) έπεται ότι Η ισότητα αυτή δείχνει ότι $\mathsf{U}(M_1,\star_1)\times\mathsf{U}(M_2,\star_2)=(M_1,\star_1)\times(M_2,\star_2)$ και επομένως άμεσα θα έχουμε $\mathsf{U}(M_1,\star_1)=(M_1,\star_1)$ και $\mathsf{U}(M_2,\star_2)=(M_2,\star_2)$, δηλαδή τα μονοειδή $(M_1,\star_1)$ και $(M_2,\star_2)$ είναι ομάδες. ■

Η παραπανω άσκηση 17 δείχνει ιδιαίτερα ότι αν $(G_1,\star_1)$ και $(G_2,\star_2)$ είναι ομάδες, τότε το ζεύγος $(G_1\times G_2,\star)$ είναι ομάδα, η **ομάδα ευθύ γινόμενο** των $(G_1,\star_1)$ και $(G_2,\star_2)$, όπου $(x_1,x_2)\star(y_1,y_2)=(x_1\star_1 y_1,x_2\star_2 y_2)$.

Οι επόμενες τρεις Ασκήσεις, οι οποίες δείχνουν ότι κάθε μεταθετικό μονοειδές μπορεί να «εμφυτευθεί» σε μια αβελιανή ομάδα με έναν ιδιαίτερο τρόπο, έχουν πολλές σημαντικές εφαρμογές.

Άσκηση 18. Έστω $(M,\star)$ ένα μεταθετικό μονοειδές με ουδέτερο στοιχείο e. Στο μονοειδές ευθύ γινόμενο $(M\times M,\star)$ ορίζουμε την ακόλουθη σχέση $\mathcal{R}$:

$$(m_1,n_1)\sim_{\mathcal{R}}(m_2,n_2)\iff\exists x\in M:\quad m_1\star n_2\star x=n_1\star m_2\star x$$

(1) Να δειχθεί ότι η σχέση $\mathcal{R}$ είναι μια σχέση ισοδυναμίας επί του $M\times M$.

(2) Αν $G(M) = (M \times M)/\mathcal{R}$ είναι το επαγόμενο σύνολο πηλίκο του $M \times M$ ως προς τη σχέση ισοδυναμίας $\mathcal{R}$, να δειχθεί ότι ορίζοντας

$$[(m_1, n_1)]_{\mathcal{R}} * [(m_2, n_2)]_{\mathcal{R}} = [(m_1 \star m_2, n_1 \star n_2)]_{\mathcal{R}}$$

αποκτούμε μια αβελιανή ομάδα $(G(M), *)$, με ουδέτερο στοιχείο $[(e, e)]_{\mathcal{R}}$ η οποία καλείται η **ομάδα Grothendieck** του μεταθετικού μονοειδούς $(M, \star)$.

Λύση. (1) • Για κάθε ζεύγος στοιχείων $(m, n) \in M \times M$ θα έχουμε $(m, n) \sim_{\mathcal{R}} (m, n)$. Πράγματι επειδή το μονοειδές $(M, \star)$ είναι μεταθετικό, θα έχουμε $m \star n \star e = n \star m \star e$. Άρα η σχέση $\mathcal{R}$ είναι ανακλαστική.

• Έστω (m_1, n_1) και (m_2, n_2) τυχόντα στοιχεία του $M \times M$, και υποθέτουμε ότι $(m_1, n_1) \sim_{\mathcal{R}} (m_2, n_2)$. Τότε υπάρχει $x \in M$ έτσι ώστε $m_1 \star n_2 \star x = n_1 \star m_2 \star x$. Λόγω μεταθετικότητας του μονοειδούς $(M, \star)$ θα έχουμε τότε $m_2 \star n_1 \star x = n_2 \star m_1 \star x$ και επομένως $(m_2, n_2) \sim_{\mathcal{R}} (m_1, n_1)$. Άρα η σχέση $\mathcal{R}$ είναι συμμετρική.

• Έστω (m_1, n_1), (m_2, n_2) (m_3, n_3) τρία τυχόντα στοιχεία του $M \times M$, και υποθέτουμε ότι $(m_1, n_1) \sim_{\mathcal{R}} (m_2, n_2)$ και $(m_2, n_2) \sim_{\mathcal{R}} (m_3, n_3)$. Τότε υπάρχουν στοιχεία $x, y \in M$ έτσι ώστε $m_1 \star n_2 \star x = n_1 \star m_2 \star x$ και $m_2 \star n_3 \star y = n_2 \star m_3 \star y$. Χρησιμοποιώντας τη μεταθετικότητα του μονοειδούς $(M, \star)$ Θα έχουμε:

$$m_1 \star n_2 \star x = n_1 \star m_2 \star x \implies m_1 \star n_2 \star x \star n_3 \star y = n_1 \star m_2 \star x \star n_3 \star y \implies m_1 \star n_3 \star (x \star y \star n_2) = (m_2 \star n_3 \star y) \star n_1 \star x$$

και τότε, επειδή $m_2 \star n_3 \star y = n_2 \star m_3 \star y$, θα έχουμε:

$$m_1 \star n_3 \star (x \star y \star n_2) = (n_2 \star m_3 \star y) \star n_1 \star x \implies m_1 \star n_3 \star (x \star y \star n_2) = n_1 \star m_3 \star (x \star y \star n_2)$$

Έτσι θέτοντας $z = x \star y \star n_2$, θα έχουμε $m_1 \star n_3 \star z = n_1 \star m_3 \star z$ και επομένως $(m_1, n_1) \sim_{\mathcal{R}} (m_3, n_3)$. Άρα η σχέση $\mathcal{R}$ είναι μεταβατική.

Συνοψίζοντας, δείξαμε ότι η σχέση $\mathcal{R}$ επί του $M \times M$ είναι μια σχέση ισοδυναμίας.

(2) Θέτουμε $G(M) = (M \times M)/\mathcal{R}$. Στην παρούσα Άσκηση το αντίστροφο ενός στοιχείου a σε ένα μονοειδές, αν αυτό υπάρχει, θα συμβολίζεται με a^{-1} και όχι με a'. Για να είναι η πράξη

$$[(m_1, n_1)]_{\mathcal{R}} * [(m_2, n_2)]_{\mathcal{R}} = [(m_1 \star m_2, n_1 \star n_2)]_{\mathcal{R}}$$

καλά ορισμένη, θα πρέπει να ισχύει το εξής:

$$[(m_1, n_1)]_{\mathcal{R}} = [(m_1', n_1')]_{\mathcal{R}} \text{ και } [(m_2, n_2)]_{\mathcal{R}} = [(m_2', n_2')]_{\mathcal{R}} \implies [(m_1, n_1)]_{\mathcal{R}} * [(m_2, n_2)]_{\mathcal{R}} = [(m_1', n_1')]_{\mathcal{R}} * [(m_2', n_2')]_{\mathcal{R}}$$

Ισοδύναμα, από το ορισμό της πράξης, θα πρέπει να ισχύει η εξής συνεπαγωγή:

$$(m_1, n_1) \sim_{\mathcal{R}} (m_1', n_1') \quad \text{και} \quad (m_2, n_2) \sim_{\mathcal{R}} (m_2', n_2') \implies (m_1 \star m_2, n_1 \star n_2) \sim_{\mathcal{R}} (m_1' \star m_2', n_1' \star n_2')$$

Από τις σχέσεις $(m_1, n_1) \sim_{\mathcal{R}} (m_1', n_1')$ και $(m_2, n_2) \sim_{\mathcal{R}} (m_2', n_2')$, έπεται ότι υπάρχουν στοιχεία $x, y \in M$ έτσι ώστε: $m_1 \star n_1' \star x = n_1 \star m_1' \star x$ και $m_2 \star n_2' \star y = n_2 \star m_2' \star y$. Τότε από τη σχέση $m_1 \star n_1' \star x = n_1 \star m_1' \star x$, και λαμβάνοντας υπόψη τη μεταθετικότητα του μονοειδούς $(M, \star)$, θα έχουμε

$$m_1 \star n_1' \star x = n_1 \star m_1' \star x \implies m_1 \star n_1' \star x \star m_1 \star n_2' \star y = n_1 \star m_1' \star x \star m_1 \star n_2' \star y \implies$$

$$m_1 \star m_2 \star n_1' \star n_2' \star x \star y = n_1 \star m_1' \star x \star (n_2' \star m_2 \star y)$$

Από τη σχέση $m_2 \star n_2' \star y = n_2 \star m_2' \star y$, και λαμβάνοντας υπόψη τη μεταθετικότητα του μονοειδούς $(M, \star)$, θα έχουμε:

$$m_1 \star m_2 \star n_1' \star n_2' \star x \star y = n_1 \star n_2 \star m_1' \star m_2' \star x \star y$$

Θέτοντας $z = x \star y$, θα έχουμε:

$$m_1 \star m_2 \star n_1' \star n_2' \star z = n_1 \star n_2 \star m_1' \star m_2' \star z \implies (m_1 \star m_2, n_1 \star n_2) \sim_{\mathcal{R}} (m_1' \star m_2', n_1' \star n_2')$$

Επομένως η πράξη «$*$» επί του $G(M)$ είναι καλά ορισμένη.

Από τον τρόπο ορισμού της, εύκολα βλέπουμε ότι η πράξη «$\star$» είναι προσεταιριστική. Έστω e το ουδέτερο στοιχείο του μονοειδούς M. Για κάθε κλάση ισοδυναμίας $[(m,n)]_{\mathfrak{R}} \in G(M)$ θα έχουμε

$$[(m,n)]_{\mathfrak{R}} * [(e,e)]_{\mathfrak{R}} = [(m \star e, n \star e)]_{\mathfrak{R}} = [(m,n)]_{\mathfrak{R}} \quad \text{και} \quad [(e,e)]_{\mathfrak{R}} * [(m,n)]_{\mathfrak{R}} = [(e \star m, e \star n)]_{\mathfrak{R}} = [(m,n)]_{\mathfrak{R}}$$

και επομένως η κλάση ισοδυναμίας $[(e,e)]_{\mathfrak{R}}$ είναι ουδέτερο στοιχείο για την πράξη «$*$» επί του $G(M)$.

Έτσι το ζεύγος $(G(M), *)$ είναι ένα μονοειδές, το οποίο είναι μεταθετικό διότι:

$$[(m_1,n_1)]_{\mathfrak{R}} * [(m_2,n_2)]_{\mathfrak{R}} = [(m_1 \star m_2, n_1 \star n_2)]_{\mathfrak{R}} = [(m_2 \star m_1, n_2 \star n_1)]_{\mathfrak{R}} = [(m_2,n_2)]_{\mathfrak{R}} * [(m_1,n_1)]_{\mathfrak{R}}$$

Τέλος για κάθε κλάση ισοδυναμίας $[(m,n)]_{\mathfrak{R}} \in G(M)$ θα έχουμε

$$[(m,n)]_{\mathfrak{R}} * [(n,m)]_{\mathfrak{R}} = [(m \star n, n \star m)]_{\mathfrak{R}}$$

Επειδή, λόγω μεταθετικότητας τησε πράξης «$\star$», έχουμε $m \star n \star e = n \star m \star e$, έπεται ότι $(m \star n, n \star m) \sim_{\mathfrak{R}} (e,e)$ και επομένως $[(m \star n, n \star m)]_{\mathfrak{R}} = [(e,e)]_{\mathfrak{R}}$. Άρα λόγω μεταθετικότητας της πράξης «$*$», θα έχουμε

$$[(m,n)]_{\mathfrak{R}} * [(n,m)]_{\mathfrak{R}} == [(e,e)]_{\mathfrak{R}} = [(n,m)]_{\mathfrak{R}} * [(m,n)]_{\mathfrak{R}}$$

δηλαδή το στοιχείο το τυχόν στοιχείο $[(m,n)]_{\mathfrak{R}}$ είναι αντιστρέψιμο στοιχείο του μονοειδούς $(G(M), *)$ με αντίστροφο στοιχείο το

$$[(m,n)]_{\mathfrak{R}}^{-1} = [(n,m)]_{\mathfrak{R}}$$ ■

Μια απεικόνιση $f\colon (M_1, \star_1) \longrightarrow (M_2, \star_2)$ μεταξύ μονοειδών $(M_1, \star_1)$ και $(M_2, \star_2)$ με ουδέτερα στοιχεία e_1 και e_2 αντίστοιχα, καλείται **ομομορφισμός μονοειδών**, αν, $\forall x, y \in M_1$:

$$f(e_1) = e_2 \qquad \text{και} \qquad f(x \star_1 y) = f(x) \star_2 f(y)$$

Ένας ομομορφισμός μονοειδών ο οποίος είναι απεικόνιση «1-1», αντίστοιχα «επί», αντίστοιχα «1-1» και «επί», καλείται **μονομορφισμός**, αντίστοιχα **επιμορφισμός**, αντίστοιχα **ισομορφισμός μονοειδών**.

Παρόμοια μια απεικόνιση $f\colon (G_1, \star_1) \longrightarrow (G_2, \star_2)$ μεταξύ ομάδων $(G_1, \star_1)$ και $(G_2, \star_2)$, καλείται **ομομορφισμός ομάδων**, αν, $\forall x, y \in G_1$:

$$f(x \star_1 y) = f(x) \star_2 f(y)$$

Ένας ομομορφισμός ομάδων ο οποίος είναι απεικόνιση «1-1», αντίστοιχα «επί», αντίστοιχα «1-1» και «επί», καλείται **μονομορφισμός**, αντίστοιχα **επιμορφισμός**, αντίστοιχα **ισομορφισμός ομάδων**.

Αν υπάρχει ένας ισομορφισμός $f\colon (G_1, \star_1) \longrightarrow (G_2, \star_2)$ μεταξύ μονοειδών ή ομάδων $(G_1, \star_1)$ και $(G_2, \star_2)$, τότε θα λέμε ότι τα μονοειδή ή ομάδες $(G_1, \star_1)$ και $(G_2, \star_2)$ είναι ισόμορφα και θα γράφουμε

$$(G_1, \star_1) \ \cong \ (G_2, \star_2)$$

Άσκηση 19. Έστω $f\colon : (G_1, \star_1) \longrightarrow (G_2, \star_2)$ μεταξύ μονοειδών με ουδέτερα στοιχεία e_1 και e_2, για την οποία ισχύει ότι $f(x \star_1 y) = f(x) \star_2 f(y)$, $\forall x, y \in G_1$.

(1) Να δειχθεί, με ένα αντιπαράδειγμα, ότι γενικά η απεικόνιση f δεν είναι ομομορφισμός μονοειδών.
(2) Αν η απεικόνιση f είναι «επί», να δειχθεί ότι η απεικόνιση f είναι ομομορφισμός μονοειδών.
(3) Αν το μονοειδές $(G, \star_2)$ είναι ομάδα, να δειχθεί ότι η απεικόνιση f είναι ομομορφισμός μονοειδών.

Λύση. Για να είναι η απεικόνιση f ομομορφισμός μονοειδών, θα πρέπει να ισχύει ότι: $f(e_1) = e_2$.

(1) Θεωρούμε το μονοειδές $(\mathbb{N}_0, \cdot)$, όπου «$\cdot$» είναι ο συνήθης πολλαπλασιασμός μη-αρνητικών ακεραίων, το ουδέτερο στοιχείο του οποίου είναι ο αριθμός 1. Τότε η απεικόνιση $f\colon (\mathbb{N}_0, \cdot) \longrightarrow (\mathbb{N}_0, \cdot)$, $f(n) = 0$, ικανοποιεί προφανώς τη συνθήκη $f(n \cdot m) = f(n) \cdot f(m)$, αλλά $f(1) = 0 \neq 1$. Επομένως η απεικόνιση f δεν είναι ομομορφισμός μονοειδών.

(2) Υποθέτουμε ότι η απεικόνιση f είναι «επί». Τότε υπάρχει ένα στοιχείο $x \in G_1$ έτσι ώστε $f(x) = e_2$ και θα έχουμε:

$$e_2 = f(x) = f(x \star_1 e_1) = f(x) \star_2 f(e_1) = e_2 \star f(e_2) = f(e_1)$$

(3) Έστω $f(e_1) = x$. Τότε $f(e_1) = f(e_1 \star_1 e_1) = f(e_1) \star_2 f(e_1)$ και επομένως $x = x \star_2 x$, δηλαδή $x \star_2 e_2 = x \star_2 x$. Επειδή ισχύει το ζεύγος $(G_2, \star_2)$ είναι ομάδα και σε κάθε ομάδα ισχύει ο νόμος διαγραφής, έπεται ότι $x = e_2$ και επομένως $f(e_1) = e_2$. ■

Άσκηση 20. Θεωρούμε ένα μεταθετικό μονοειδές $(M, \star)$ και έστω $(G(M), *)$ η ομάδα Grothendieck του $(M, \star)$, βλέπε την Άσκηση 18. Να δειχθούν τα εξής:

(1) Η απεικόνιση

$$\iota \colon M \longrightarrow G(M), \quad \iota(m) = [(m, e)]_{\mathfrak{R}}$$

είναι ομομορφισμός μονοειδών, ο οποίος είναι μονομορφισμός μονοειδών αν και μόνον αν, $\forall m, n, x \in M$:

$$m \star x = n \star x \quad \Longrightarrow \quad m = n$$

(2) Αν $(G, \star')$ είναι μια αβελιανή ομάδα με ουδέτερο στοιχείο ϵ και $f \colon M \longrightarrow G$ είναι ένας ομομορφισμός μονοειδών, να δειχθεί ότι υπάρχει μοναδικός ομομορφισμός ομάδων $f^* \colon G(M) \longrightarrow G$ έτσι ώστε $f^* \circ \iota = f$:

Λύση. (1) Για την απεικόνιση $\iota \colon M \longrightarrow G(M)$, $\iota(m) = [(m, e)]_{\mathfrak{R}}$ θα έχουμε προφανώς $\iota(e) = [(e, e)]_{\mathfrak{R}}$ και

$$\iota(m_1 \star m_2) = [(m_1 \star m_2, e)]_{\mathfrak{R}} = [(m_1 \star m_2, e \star e)]_{\mathfrak{R}} = [(m_1, e)]_{\mathfrak{R}} * [(m_2, e)]_{\mathfrak{R}} = \iota(m_1) * \iota(m_2)$$

δηλαδή η απεικόνιση ι είναι ένας ομομορφισμός μονοειδών.

Αν $\iota(m) = [(e, e)]_{\mathfrak{R}}$, τότε θα έχουμε $[(m, e)]_{\mathfrak{R}} = [(e, e)]_{\mathfrak{R}}$ και επομένως $(m, e) \sim_{\mathfrak{R}} (e, e)$. Τότε υπάρχει στοιχείο $x \in M$ έτσι ώστε $m \star e \star x = e \star e \star x$. Επειδή το x είναι ουδέτερο στοιχείο του M, θα έχουμε $m \star x = x$. Αντίστροφα, αν $m \star x = x$, τότε όπως και παραπάνω θα έχουμε $m \star e \star x = e \star e \star x$, δηλαδή $(m, e) \sim_{\mathfrak{R}} (e, e)$ και επομένως $\iota(m) = [(m, e)]_{\mathfrak{R}} = [(e, e)]_{\mathfrak{R}} = \iota(e)$.

(2) Έστω ότι $(G, \star')$ είναι μια αβελιανή ομάδα με ουδέτερο στοιχείο ϵ και έστω $f \colon M \longrightarrow G$ ένας ομομορφισμός μονοειδών, δηλαδή, $\forall m_1, m_2 \in M$:

$$f(e) = \epsilon \quad \text{και} \quad f(m_1 \star m_2) = f(m_1) \star' f(m_2)$$

Ορίζουμε απεικόνιση

$$f^* \colon G(M) \longrightarrow G', \quad f^*([(m, n)]_{\mathfrak{R}}) = f(m) \star f(n)^{-1}$$

Δείχνουμε ότι η απεικόνιση f^* είναι καλά ορισμένη. Έστω ότι $[(m_1, n_1)]_{\mathfrak{R}} = [(m_2, n_2)]_{\mathfrak{R}}$ και επομένως θα έχουμε $(m_1, n_1) \sim_{\mathfrak{R}} (m_1', n_1')$. Τότε υπάρχει στοιχείο $x \in M$ έτσι ώστε $m_1 \star n_1' \star x = n_1 \star m_1' \star x$. Εφαρμόζωντας την απεικόνιση f, θα έχουμε στην ομάδα G':

$$f(m_1 \star n_1' \star x) = f(n_1 \star m_1' \star x) \quad \Longrightarrow \quad f(m_1) \star' f(n_1') \star' f(x) = f(n_1) \star' f(m_1') \star' f(x)$$

Από το Νόμο διαγραφής στην ομάδα G', χρησιμοποιώντας επιπρόσθετα ότι η ομάδα G' είναι αβελιανή και πολλαπλασιάζοντας από την τελευταία ισότητα πρώτα με το $f(n_1)^{-1}$ και ακολούθως με το $f(n_1')^{-1}$, έπεται ότι:

$$f(m_1) \star' f(n_1') = f(n_1) \star' f(m_1') \quad \Longrightarrow \quad f(m_1) \star' f(n_1)^{-1} = f(m_1') \star' f(n_1')^{-1} \quad \Longrightarrow$$
$$f^*([(m, n)]_{\mathfrak{R}}) = f^*([(m_1', n_1')]_{\mathfrak{R}}$$

Άρα η f^* είναι καλά ορισμένη απεικόνιση και επιπλέον $f^*([(e, e)]_{\mathfrak{R}}) = f(e) \star' f(e)^{-1} = \epsilon \star' \epsilon^{-1} = \epsilon \star' \epsilon = \epsilon$, και $\forall m \in M$:

$$(f^* \circ \iota)(m) = f^*([(m, e)]_{\mathfrak{R}}) = f(m) \star' f(e)^{-1} = f(m) \star' \epsilon^{-1} = f(m) \star' \epsilon = f(m) \quad \Longrightarrow \quad f^* \circ \iota = f$$

Επιπρόσθετα, χρησιμοποιώντας ότι η πράξη «$\star'$» είναι μεταθετική, θα έχουμε:

$$f^*\big([(m_1, n_1)]_{\mathfrak{R}} * [(m_2, n_2)]_{\mathfrak{R}}\big) = f^*\big([(m_1 \star m_2, n_1 \star n_2)]_{\mathfrak{R}}\big) = f(m_1 \star m_2) \star' f(n_1 \star n_2)^{-1} =$$

$$= f(m_1) \star' f(m_2) \star' \big(f(n_1) \star' f(n_2)\big)^{-1} = f(m_1) \star' f(m_2) \star' f(n_2)^{-1} \star' f(n_1)^{-1} =$$

$$= f(m_1) \star' f(n_1)^{-1} \star' f(m_2) \star' f(n_2)^{-1} = f^*[(m_1, n_1)]_{\mathcal{R}}) \star' f^*([(m_2, n_2)]_{\mathcal{R}})$$

Επομέμνως η απεικόνιση f^* είναι ένας ομομορφισμός ομάδων.

Τέλος αν $g\colon G(M) \longrightarrow G'$ είναι ένας άλλος ομομορφισμός ομάδων για τον οποίο ισχύει ότι: $g \circ \iota = f$, τότε θα έχουμε, $\forall [(m,n)]_{\mathcal{R}} \in G(M)$:

$$g([m,n]_{\mathcal{R}}) = g\big([(m,e) \star [(e,n)]_{\mathcal{R}}\big) = g([(m,e)]_{\mathcal{R}}) \star' g([(e,n)]_{\mathcal{R}}) = g(\iota(m)) \star' g([(n,e)]_{\mathcal{R}}^{-1}) =$$

$$= (g \circ \iota)(m) \star' g([(n,e)]_{\mathcal{R}}^{-1}) = f(m) \star' g([(n,e)]_{\mathcal{R}}^{-1}) \qquad (\dagger)$$

Όμως

$$g([(n,e)]_{\mathcal{R}}) \star' g([(n,e)]_{\mathcal{R}}^{-1}) = g\big((n,e)]_{\mathcal{R}} \star [(n,e)]_{\mathcal{R}}^{-1}\big) = g([(e,e)]_{\mathcal{R}}) = \epsilon$$

και επομένως επειδή η ομάδα G' είναι αβελιανή θα έχουμε:

$$g([(n,e)]_{\mathcal{R}}^{-1}) = g([(n,e)]_{\mathcal{R}})^{-1} = g(\iota(n))^{-1} = (g \circ \iota)(n)^{-1} = f(n)^{-1}$$

και επομένως από τη σχέση $(\dagger)$ έπεται ότι, $\forall [(m,n)]_{\mathcal{R}} \in G(M)$:

$$g([m,n]_{\mathcal{R}}) = f(m) \star' g([(n,e)]_{\mathcal{R}}^{-1}) = f(m) \star' f(n)^{-1} = f^*([(m,n)]_{\mathcal{R}})$$

Άρα $f^* = g$. ■

Παρατήρηση. *Ένα μονοειδές $(M, \star)$ καλείται* **αριστερά**, *αντίστοιχα* **δεξιά**, **διαγράψιμο**, *αν:*

$$x \star m = x \star n \implies m = n \quad \text{αντίστοιχα,} \quad m \star x = n \star x \implies m = n$$

Προφανώς αν το μονοειδές $(M, \star)$ είναι μεταθετικό, τότε το μονοειδές είναι αριστερά διαγράψιμο αν και μόνον αν είναι δεξιά διαγράψιμο, και τότε θα καλούμε το $(M, \star)$ απλά **διαγράψιμο**.

Η προηγούμενη Άσκηση 20 πιστοποιεί ότι κάθε διαγράψιμο μεταθετικό μονοειδές μπορεί να εμφυτευθεί σε μια αβελιανή ομάδα. Πράγματι τότε η απεικόνιση $\iota\colon (M, \star) \longrightarrow G(M, \star)$ είναι ένας μονομορφισμός μονοειδών, και επομένως μπορούμε να ταυτίσουμε το μονοειδές $(M, \star)$ με την εικόνα του $\mathsf{Im}(\iota) \subseteq G(M, \star)$ η οποία είναι «υπομονοειδές» του $G(M, \star)$, δηλαδή το υποσύνολο $\mathsf{Im}(\iota)$ είναι κλειστό στην πράξη «$*$» του $G(M, \star)$ και το ζεύγος $(\mathrm{Im}(\iota), *)$ είναι μονοειδές.

Εύκολα βλέπουμε ότι αν ένα μεταθετικό μονοειδές $(M, \star)$ μπορεί να εμφυτευθεί σε μια ομάδα, τότε είναι διαγράψιμο. Πράγματι, έστω $(G, \cdot)$ μια ομάδα και $f\colon (M, \star) \longrightarrow (G, \cdot)$ ένας μονομορφισμός μονοειδών. Αν έχουμε $x \star m = x \star n$ στο $(M, \star)$, τότε

$$x \star m = x \star n \implies f(x \star m) = f(x \star n) \implies f(x) \cdot f(m) = f(x) \cdot f(n)$$

Επειδή κάθε ομάδα είναι προφανώς διαγράψιμο μονοειδές, θα έχουμε $f(m) = f(n)$ και επειδή η απεικόνιση f είναι μονομορφισμός, έπεται ότι $m = n$. Άρα το μονοειδές $(M, \star)$ είναι διαγράψιμο. Επομένως:

Ένα μεταθετικό μονοειδές μπορεί να εμφυτεθεί σε μια ομάδα $\iff$ το μονοειδές είναι διαγράψιμο

Τίθεται φυσιολογικά τότε το ερώτημα αν διαγράψιμα, όχι κατ' ανάγκην μεταθετικά, μονοειδή μπορούν να εμφυτεθούν σε μια ομάδα. Η απάντηση, η οποία είναι αρκετά δύσκολη, είναι γενικά όχι, και δόθηκε από τον Ρώσσο Μαθηματικό Anatoly Malcev το 1936. ▲

Άσκηση 21. Θεωρούμε τα μεταθετικά μονοειδή $(\mathbb{N}_0, +)$ και $(\mathbb{N}_0, \cdot)$, και $(\mathbb{N}, \cdot)$. Να δειχθεί ότι:

$$G(\mathbb{N}_0, +) \cong (\mathbb{Z}, +) \quad \text{και} \quad G(\mathbb{N}_0, \cdot) = \big\{[(1,1)]_{\mathcal{R}}\big\}$$

Λύση. Θα δείξουμε ότι για το μεταθετικό μονοειδές $(\mathbb{N}_0, \cdot)$ η ομάδα Grothendieck $G(\mathbb{N}_0, \cdot)$ αποτελείται μόνο από το ουδέτερο στοιχείο της. Πράγματι, αν $[(m,n)]_{\mathcal{R}}$ είναι ένα τυχόν στοιχείο της ομάδας $G(\mathbb{N}_0, \cdot)$, τότε επειδή

$$n \cdot 1 \cdot 0 = 0 = m \cdot 1 \cdot 0 \quad \Longrightarrow \quad (m,n) \sim_{\mathcal{R}} (1,1) \quad \Longrightarrow \quad [(m,n)]_{\mathcal{R}} = [(1,1)]_{\mathcal{R}}$$

Άρα

$$G(\mathbb{N}_0, \cdot) = \big\{[(1,1)]_{\mathcal{R}}\big\}$$

Θεωρούμε την ομάδα $(\mathbb{Z}, +)$ και ορίζουμε απεικόνιση

$$f\colon (\mathbb{N}_0, +) \longrightarrow (\mathbb{Z}, +), \qquad f(n) = n$$

Από την Άσκηση 20 έπεται ότι υπάρχει μοναδικός ομομορφισμός ομάδων

$$f^*\colon G(\mathbb{N}_0, +) \longrightarrow (\mathbb{Z}, +), \qquad f^*([(n,m)]_{\mathcal{R}}) = f(n) - f(m) = n - m$$

έτσι ώστε $f^* \circ \iota = f$, όπου $\iota\colon (\mathbb{N}_0, +) \longrightarrow G(\mathbb{N}_0, +)$ είναι η κανονικός ομομορφισμός μονοειδών $\iota(n) = [(n,0)]_{\mathcal{R}}$. Έτσι αρκεί να δείξουμε ότι ο ομομορφισμός f^* είναι «1-1» και «επί».

- Έστω $z \in \mathbb{Z}$. Αν $z \geq 0$, τότε προφανώς θα έχουμε $f^*([(z,0)]_{\mathcal{R}}) = z - 0 = z$, και αν $z < 0$, τότε $-z > 0$ και $f^*([(0,-z)]_{\mathcal{R}}) = 0 - (-z) = z$. Επομένως η απεικόνιση f^* είναι «επί».

- Έστω $f^*([(n,m)]_{\mathcal{R}}) = f^*([(k,l)]_{\mathcal{R}})$. Τότε $n - m = k - l$ και άρα $n + l = m + k$ ή ισοδύναμα $n + l + 0 = m + k + 0$. Αυτό σημαίνει ότι $(n,m) \sim_{\mathcal{R}} (k,l)$, βλέπε την Άσκηση 18, και επομένως $[(n,m)]_{\mathcal{R}} = [(k,l)]_{\mathcal{R}}$. Άρα η απεικόνιση f^* είναι «1-1».

Συνοψίζουμε, η απεικόνιση f^* είναι ένας ισομορφισμός ομάδων. ■

Άσκηση 22. (Θεώρημα Cayley για Μονοειδή). Έστω $(M, \star)$ ένα μονοειδές με ουδέτερο στοιχείο e. Θεωρούμε το μονοειδές $(\mathsf{Map}(M), \circ)$, όπου

$$\mathsf{Map}(M) = \big\{f\colon M \longrightarrow M \mid f: \text{ απεικόνιση}\big\}$$

και «$\circ$» είναι η σύνθεση απεικονίσεων. Να δειχθεί ότι η απεικόνιση

$$\mathsf{R}: (M, \star) \longrightarrow (\mathsf{Map}(M), \circ), \quad m \longmapsto \mathsf{R}(m) := \mathsf{R}_m\colon M \longrightarrow M, \quad \mathsf{R}_m(x) = m \star x$$

είναι ένας μονομορφισμός μονοειδών.

Λύση. Υπενθυμίζουμε ότι το ουδέτερο στοιχείο του μονοειδούς $(\mathsf{Map}(M), \circ)$, είναι η ταυτοτική απεικόνιση $\mathsf{Id}_M\colon\ M \longrightarrow M$, $\mathsf{Id}_M(m) = m$. Θα έχουμε, $\forall m \in M$:

(1) $$\mathsf{R}_e(m) = e \star m = m \quad \Longrightarrow \quad \mathsf{R}_m = \mathsf{Id}_M$$

Επομένως $\mathsf{R}(e) = \mathsf{Id}_M$.

Έστω $m_1, m_2 \in M$. Τότε θα έχουμε, $\forall x \in M$:

$$\mathsf{R}_{m_1 \star m_2}(x) = (m_1 \star m_2) \star x \quad \text{και} \quad (\mathsf{R}_{m_1} \circ \mathsf{R}_{m_2})(x) = \mathsf{R}_{m_1}(\mathsf{R}_{m_2}(x)) = \mathsf{R}_{m_1}(m_2 \star x) = m_1 \star (m_2 \star x)$$

Λόγω της προσεταιριστικής ιδιότητας για την πράξη «$\star$», θα έχουμε $\mathsf{R}_{m_1 \star m_2}(x) = (\mathsf{R}_{m_1} \circ \mathsf{R}_{m_2})(x)$, $\forall x \in M$, και επομένως, $\forall m_1, m_2 \in M$:

(2) $$\mathsf{R}(m_1 \star m_2) = \mathsf{R}(m_1) \circ \mathsf{R}(m_2)$$

Οι σχέσεις (1) και (2) δείχνουν ότι η απεικόνιση R είναι ένας ομομορφισμός μονοειδών.

Έστω $\mathsf{R}(m_1) = \mathsf{R}(m_2)$, δηλαδή $\mathsf{R}_{m_1} = \mathsf{R}_{m_2}$. Τότε για κάθε $x \in M$:

$$\mathsf{R}_{m_1} = \mathsf{R}_{m_2} \quad \Longrightarrow \quad \mathsf{R}_{m_1}(x) = \mathsf{R}_{m_2}(x) \quad \Longrightarrow \quad m_1 \star x = m_2 \star x, \quad \forall x \in M$$

Τότε επιλέγοντας $x = e$, το ουδέτερο στοιχείο του μονοειδούς $(M, \star)$, θα έχουμε $m_1 \star e = m_2 \star e$ και επομένως $m_1 = m_2$. Αυτό δείχνει ότι η απεικόνιση R είναι «1-1» και άρα είναι ένας μονομορφισμός μονοειδών. ■