Θεμέλια Άλγεβρας και Γεωμετρίας

Πρόχειρες Σημειώσεις Παραδόσεων Από Απόσταση

Οκτώβριος 2020
ΜΜ

Περιεχόμενα

Ομάδες

Η θεωρία ομάδων αφορά τη μελέτη της έννοιας της συμμετρίας, για παράδειγμα ενός υποσυνόλου του $\mathbb{R}^n$, των ριζών ενός πολυωνύμου, μιας αλγεβρικής δομής, των λύσεων ενός συστήματος διαφορικών εξισώσεων.

Στο κεφάλαιο αυτό δίνουμε τον ορισμό της ομάδας, εξετάζουμε μερικά σημαντικά παραδείγματα με μελετάμε την έννοια της τάξης στοιχείου. Ο σκοπός μας δεν είναι η εισαγωγή στη θεωρία ομάδων, αλλά η ανάδειξη της χρησιμότητας της αξιωματικής ανάπτυξης μέσω του παραδείγματος των ομάδων.

6.1. Ισομετρίες

Σκοπός μας σε αυτή την παράγραφο είναι να δώσουμε μερικά γεωμετρικά - εποπτικά παραδείγματα αυτών που θα ονομάσουμε *ομάδες* παρακάτω.

Ορισμός 6.1. (1) *Μια απεικόνιση $f : \mathbb{R}^n \to \mathbb{R}^n$ λέγεται* ***ισομετρία*** *αν*

$$d(x, y) = d(f(x), f(y))$$

για κάθε $x, y \in \mathbb{R}^n$, όπου $d(x, y)$ η συνήθης Ευκλείδεια απόσταση των x, y .

(2) *Έστω $M \neq \emptyset$, $M \subseteq \mathbb{R}^n$. Μια ισομετρία $f : \mathbb{R}^n \to \mathbb{R}^n$, ώστε $f(M) = M$ λέγεται* ***συμμετρία*** *του M. Το σύνολο των συμμετριών του M συμβολίζεται με $S(M)$.*

Η σύνθεση δύο συμμετριών του M είναι συμμετρία του M καθώς για κάθε $f, g \in S(M)$ και για κάθε $x, y \in \mathbb{R}^n$,

$$d(f \circ g(x), f \circ g(y)) = d(f(g(x)), f(g(y))) = d(g(x), g(y)) = d(x, y).$$

Στα παρακάτω θα συμβολίζουμε τη σύνθεση $f \circ g$ με fg. Ειδικά $f \circ f$ θα συμβολίζεται με f^2.

Παραδείγματα 6.2.

(1) Έστω $a \in \mathbb{R}$. Η απεικόνιση

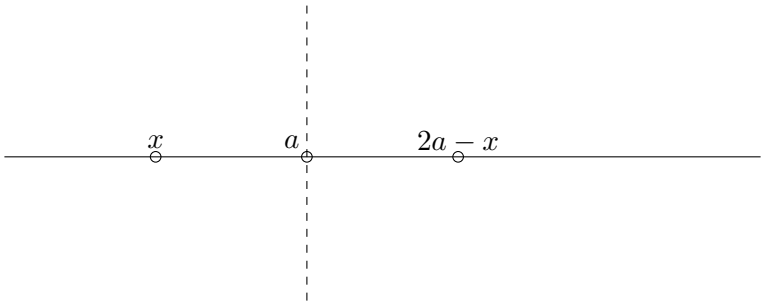
$$t_a : \mathbb{R} \to \mathbb{R}, t_a(x) = a + x$$

είναι ισομετρία. Παρατηρούμε ότι $t_a t_b = t_{a+b}$ για κάθε $a, b \in \mathbb{R}$. Επίσης η απεικόνιση

$$s_a : \mathbb{R} \to \mathbb{R}, s_a(x) = 2a - x$$

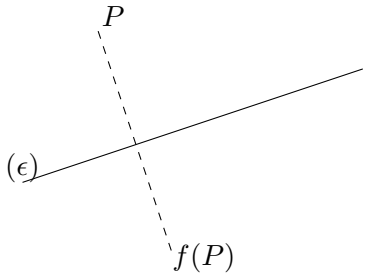
είναι ισομετρία. Εύκολα επαληθεύεται ότι s_a^2 είναι η ταυτοτική απεικόνιση $\mathbb{R} \to \mathbb{R}$ και ότι $s_a t_b = s_{b-\frac{a}{2}}$ για κάθε $a, b \in \mathbb{R}$.

Εποπτικά η t_a παριστάνει τη *μετατόπιση* της πραγματικής ευθείας κατά a και s_a παριστάνει την *ανάκλαση* της πραγματικής ευθείας ως προς την κάθετο στο σημείο a.



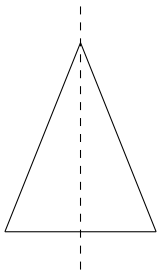
ανάκλαση s_a

Μια άλλη οικογένεια ισομετριών του επιπέδου $\mathbb{R}^2$ είναι οι ανακλάσεις ως προς τυχαία ευθεία (ϵ) του επιπέδου, όπως δείχνει το σχήμα



(2) Στη συνέχεια θα δώσουμε μερικά διαισθητικά παραδείγματα συμμετριών συνόλου M. Δεν δικαιολογούμε γιατί οι αναγραφόμενες συμμετρίες του M είναι όλες οι συμμετρίες του M.

Οι συμμετρίες ισοσκελούς τριγώνου που δεν είναι ισόπλευρο,



$$S(M) = \{1, s\},$$

όπου

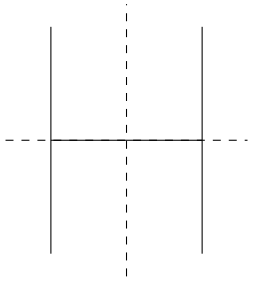
$$1 : \mathbb{R}^2 \to \mathbb{R}^2, \;\; 1(x) = x,$$

είναι η ταυτοτική απεικόνιση του επιπέδου και

$$s : \mathbb{R}^2 \to \mathbb{R}^2$$

είναι η ανάκλαση ως προς τον κατακόρυφο άξονα. Είναι σαφές ότι $s^2 = 1$.

(3) Οι συμμετρίες του γράμματος Η,



$$S(M) = \{1, s_1, s_2, r\},$$

όπου s_1 η ανάκλαση ως προς τον κατακόρυφο άξονα, s_2 η ανάκλαση ως προς τον οριζόντιο άξονα και r η περιστροφή κατά γωνία 180^o με κέντρο το κέντρο συμμετρίας και φορά $\circlearrowleft$.

Παρατηρούμε ότι

$$s_1^2 = s_2^2 = r^2 = 1.$$

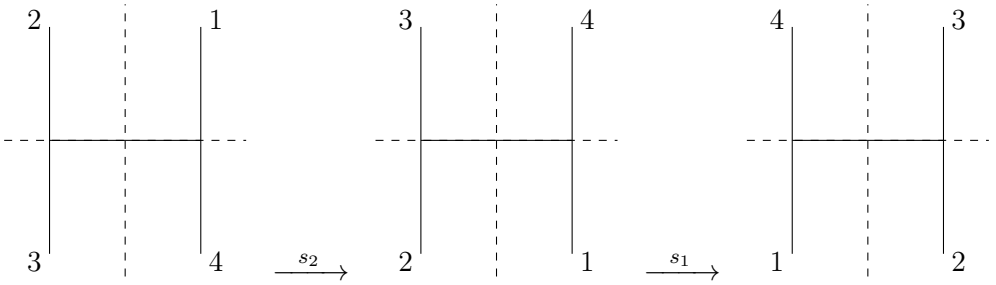
Επίσης, εύκολα επαληθεύονται οι σχέσεις

$$s_1 s_2 = s_2 s_1 = r,$$

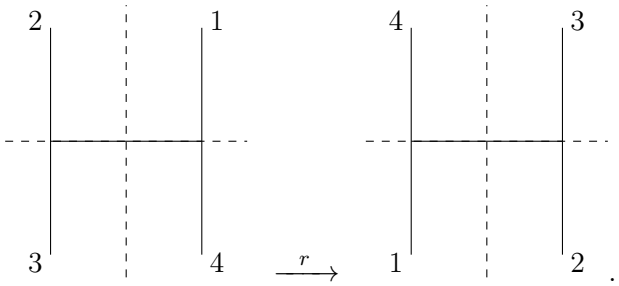
$$s_1 r = r s_1 = s_2,$$

$$s_2 r = r s_2 = s_1.$$

Πράγματι, ας συμβολίσουμε τα επίμαχα σημεία του σχήματος Η με 1,2,3,4. Σχηματικά για τη σύνθεση $s_1 s_2$ έχουμε

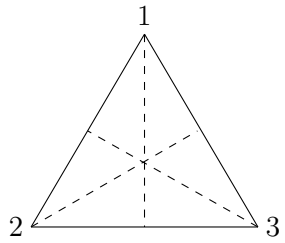


και για την απεικόνιση r έχουμε



Άρα $s_1 s_2 = r$.

(4) Οι συμμετρίες του ισόπλευρου τριγώνου,



$$S(M) = \{1, s_1, s_2, s_3, r_1, r_2\},$$

όπου

s_i η ανάκλαση ως προς άξονα το ύψος που διέρχεται από την κορυφή i $(i = 1, 2, 3)$

και

r_j η περιστροφή κατά γωνία $\frac{2\pi}{3} j$ στη φορά $\circlearrowleft, j = 1, 2.$

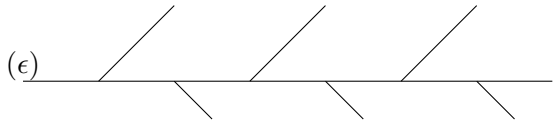
Όπως στο προηγούμενο παράδειγμα, εύκολα επαληθεύεται ότι

$$s_2 \circ s_1 = r_2, \ s_1 \circ s_2 = r_1.$$

Επίσης,

$$s_i^2 = r_j^3 = 1, \ i = 1, 2, 3, j = 1, 2.$$

(5) Άπειρο κλαδί.



Εδώ έχουμε την πραγματική ευθεία (ε) και δύο οικογένειες παράλληλων ευθυγράμμων τμημάτων που τέμνουν την (ε) στα σημεία $a \in \mathbb{Z}$ και που τα δύο μήκη των ευθυγράμμων τμημάτων είναι διαφορετικά. Οι συμμετρίες του M είναι

$$S(M) = \{t_{2a} : a \in \mathbb{Z}\},$$

όπου t_{2a} ορίστηκε στο πρώτο παράδειγμα.

6.2. Ομάδες

Ορισμός 6.3. *Μια πράξη σε ένα μη κενό σύνολο A είναι μια απεικόνιση της μορφής*

$$A \times A \to A.$$

Δηλαδή σε κάθε διατεταγμένο ζεύγος (a, b) στοιχείων το A αντιστοιχίζουμε μοναδικό στοιχείο του A. Μερικοί συνήθεις συμβολισμοί για την εικόνα του (a, b) είναι

$$a \circ b,\ a \cdot b,\ a \star b.$$

Παραδείγματα 6.4.

(1) Η συνήθης πρόσθεση ακεραίων

$$+ : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}, (a, b) \mapsto a + b$$

και ο συνήθης πολλαπλασιασμός ακεραίων

$$\cdot : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}, (a, b) \mapsto a \cdot b$$

είναι πράξεις στο $\mathbb{Z}$.

(2) Έστω M υποσύνολο του $\mathbb{R}^n$. Στην Παράγραφο 6.1 είδαμε ότι η σύνθεση συναρτήσεων ορίζει πράξη στο σύνολο των συμμετριών $S(M)$ του M.

(3) Στο Κεφάλαιο 5 είδαμε ότι έχουμε τις πράξεις της πρόσθεσης και του πολλαπλασιασμού πολυωνύμων

$$+ : F[x] \times F[x] \to F[x], (a(x), b(x)) \mapsto a(x) + b(x)$$

και

$$\cdot : F[x] \times F[x] \to F[x], (a(x), b(x)) \mapsto a(x) \cdot b(x).$$

(4) Έστω S σύνολο και A το σύνολο των υποσυνόλων του S. Στο Κεφάλαιο 5 είδαμε ότι έχουμε τις πράξεις της ένωσης και της τομής συνόλων

$$\cup : A \times A \to A, (X, Y)) \mapsto X \cup Y$$

και

$$\cap : A \times A \to A, (X, Y) \mapsto X \cap Y.$$

Ορισμός 6.5. *Έστω G σύνολο με $G \times G \to G,\ (a, b) \mapsto a \cdot b$ πράξη στο G. Το ζεύγος $(G, \cdot)$ λέγεται **ομάδα** αν ισχύουν τα ακόλουθα.*

(1) *$(a \cdot b) \cdot c = a \cdot (b \cdot c)$, για κάθε $a, b, c \in G$ (προσεταιριστική ιδιότητα).*
(2) *Υπάρχει $e \in G$ ώστε $a \cdot e = e \cdot a = a$, για κάθε $a \in G$ (ύπαρξη ουδέτερου στοιχείου).*
(3) *Για κάθε $a \in G$, υπάρχει $a' \in G$ ώστε $a \cdot a' = a' \cdot a = e$ (ύπαρξη αντιστρόφου στοιχείου).*

Αν επιπλέον ισχύει $a \cdot b = b \cdot a$, για κάθε $a, b \in G$ θα λέμε ότι η ομάδα G είναι αβελιανή.

Παρατηρήσεις. Έστω $(G, \cdot)$ ομάδα.

(1) Το e του παραπάνω ορισμού είναι μοναδικό. Πράγματι, αν $e_1, e_2 \in G$ με

$$e_i \cdot a = a \cdot e_i = a,$$

για κάθε $a \in G$, τότε

$$e_1 = e_1 \cdot e_2 = e_2.$$

Το e καλείται το ουδέτερο στοιχείο της ομάδας. Συχνά θα το συμβολίζουμε 1_G. Δεν πρέπει να δημιουργείται σύγχυση με τον αριθμό 1.

(2) Για κάθε $a \in G$, το $a' \in G$ του ορισμού είναι μοναδικό. Πράγματι, αν

$$a \cdot a' = a' \cdot a = e \quad \text{και} \quad a \cdot a'' = a'' \cdot a = e,$$

τότε

$$\begin{aligned} a'' &= e \cdot a'' \\ &= (a' \cdot a) \cdot a'' \\ &= a' \cdot (a \cdot a'') \\ &= a' \cdot e \\ &= a'. \end{aligned}$$

Θα συμβολίζουμε το στοιχείο a' με a^{-1}.

(3) Αν $a, b \in G$ και $a \cdot b = e$, τότε $b = a^{-1}$ και $a = b^{-1}$.

(4) Για κάθε $a, b \in G$ ισχύει, $(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$. Πράγματι,

$$\begin{aligned} (a \cdot b) \cdot (b^{-1} \cdot a^{-1}) &= a \cdot ((b \cdot b^{-1}) \cdot a^{-1}) \\ &= a \cdot (e \cdot a^{-1}) \\ &= a \cdot a^{-1} \\ &= e. \end{aligned}$$

Παραδείγματα 6.6.

(1) Τα σύνολα $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ είναι αβελιανές ομάδες με πράξη την πρόσθεση αριθμών (ουδέτερο στοιχείο το 0).

Τα σύνολα $\{1, -1\}$, $\mathbb{Q} \setminus \{0\}$, $\mathbb{R} \setminus \{0\}$, $\mathbb{C} \setminus \{0\}$ είναι αβελιανές ομάδες με πράξη τον πολλαπλασιασμό αριθμών (ουδέτερο στοιχείο το 1).

(2) **Σημαντικό παράδειγμα, μεταθέσεις του X** Έστω X μη κενό σύνολο και

$$S(X) = \{f : X \to X : f \ \ 1-1 \ \text{και επί}\}.$$

Με πράξη την σύνθεση συναρτήσεων, το $S(X)$ είναι ομάδα. Πράγματι έχουμε,

i)
$$(f \circ g) \circ h = f \circ (g \circ h),$$
για κάθε $f, g, h \in S(X)$.

ii) Αν $1_X : X \to X$ είναι η ταυτοτική συνάρτηση $1_x(x) = x$ για κάθε $x \in X$, τότε
$$f \circ 1_X = 1_X \circ f = f,$$
για κάθε $f \in S(X)$.

iii) Αν $f \in S(X)$, τότε η f ως 1-1 και επί συνάρτηση, έχει αντίστροφη συνάρτηση $f^{-1} : X \to X$. Ξέρουμε ότι η f^{-1} είναι 1-1 και επί, δηλαδή $f^{-1} \in S(X)$ και
$$f^{-1} \circ f = f \circ f^{-1} = 1_X.$$

(3) **Ο κύκλος** Έστω $E = \{z \in \mathbb{C} : |z| = 1\}$ ο μοναδιαίος κύκλος. Τότε ως προς τον πολλαπλασιασμό μιγαδικών το E είναι ομάδα. Πράγματι,

i) αν $z_1, z_2 \in E$, τότε $|z_1 z_2| = |z_1||z_2| = 1$. Άρα $z_1 z_2 \in E$.
ii) Προφανώς ισχύει $z_1(z_2 z_3) = (z_1 z_2) z_3$, για κάθε $z_i \in E$.
iii) $1 \cdot z = z \cdot 1 = z$, για κάθε $z \in E$.
iv) Αν $z \in E$ τότε $z \neq 0$ και το $\frac{1}{z} \in \mathbb{C}$ ικανοποιεί τη $|\frac{1}{z}| = \frac{1}{|z|} = 1$. Άρα $\frac{1}{z} \in E$. Επίσης έχουμε $z \cdot \frac{1}{z} = 1$.

(4) **n-στες ρίζες της μονάδας** Έστω $n \in \mathbb{Z}_{>0}$. Θέτουμε $E_n = \{z \in \mathbb{C} : z^n = 1\}$. Είναι σαφές ότι το E_n είναι μια ομάδα ως προς τον πολλαπλασιασμό μιγαδικών (όπως πριν). Εδώ έχουμε $|E_n| = n$. Πράγματι, έστω

$$\omega_n = cos(\frac{2\pi}{n}) + isin(\frac{2\pi}{n}).$$

Τότε

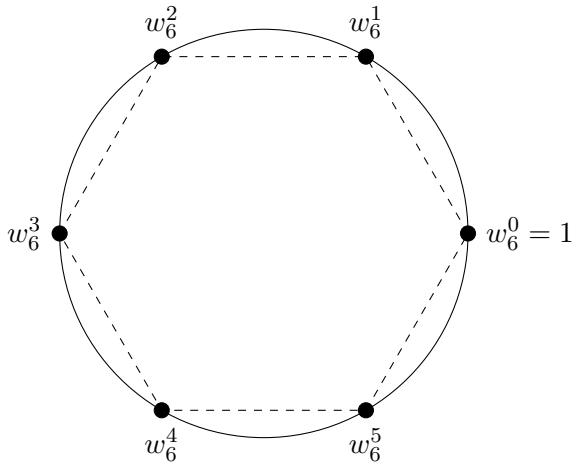
$$1, \omega_n, \omega_n^2, ..., \omega_n^{n-1} \in E_n$$

σύμφωνα με το θεώρημα De Moivre που λέει ότι

$$(\cos\theta + i\sin\theta)^n = \cos(n\theta) + i\sin(n\theta).$$

Από την ισότητα μιγαδικών εύκολα προκύπτει ότι τα παραπάνω στοιχεία είναι διάφορα ανά δύο, οπότε $|E_n| \geq n$. Επειδή το πολυώνυμο $x^n - 1 \in \mathbb{C}[x]$ είναι βαθμού n, παίρνουμε $|E_n| \leq n$. Άρα $|E_n| = n$.

Εποπτικά μπορούμε να σκεφτόμαστε τις n-στές ρίζες της μονάδας ως τις κορυφές του κανονικού κυρτού n-γώνου. Για $n = 6$ έχουμε το ακόλουθο σχήμα.



(5) **Αφφινικοί μετασχηματισμοί της ευθείας** Έστω $a, b \in \mathbb{R},\ a \neq 0$. Ορίζουμε

$$T_{a,b} : \mathbb{R} \to \mathbb{R},\ \ T_{a,b}(x) = ax + b.$$

Έστω

$$G = \{T_{a,b} : a, b \in \mathbb{R},\ a \neq 0\}.$$

Θα δείξουμε ότι ως προς την σύνθεση συναρτήσεων η G είναι ομάδα.

Έστω $T_{a,b}$ και $T_{c,d} \in G$. Τότε

$$\begin{aligned} T_{a,b} \circ T_{c,d}(x) &= T_{a,b}\left(T_{c,d}(x)\right) = T_{a,b}(cx + d) \\ &= a(cx + d) + b = acx + ad + b. \end{aligned}$$

Επειδή $a \neq 0,\ c \neq 0$, έχουμε $ac \neq 0$. Τότε

$$T_{a,b} \circ T_{c,d}(x) = T_{ac,ad+b} \in G.$$

Παρατηρούμε ότι

$$(T_{a,b} \circ T_{c,d}) \circ T_{e,f} = T_{ac,ad+b} \circ T_{e,f} = T_{ace,acf+ad+b}, \text{ και}$$

$$(T_{a,b} \circ (T_{c,d} \circ T_{e,f}) = T_{a,b} \circ T_{ce,cf+d} = T_{ace,acf+ad+b}$$

Άρα ισχύει η προσεταιριστική ιδιότητα.

Για την $T_{1,0}$ ισχύει $T_{1,0}(x) = x$ για κάθε $x \in \mathbb{R}$, άρα

$$T_{1,0} \cdot T_{a,b} = T_{a,b} \cdot T_{1,0} = T_{a,b}$$

για κάθε $T_{a,b} \in G$. Το ουδέτερο στοιχείο είναι η απεικόνιση $T_{1,0}$, που είναι η ταυτοτική απεικόνιση στο σύνολο $\mathbb{R}$.

Το στοιχείο $T_{a,b}$ έχει αντίστροφο το $T_{a^{-1},-ba^{-1}}$. Πράγματι,

$$T_{a,b} \circ T_{a^{-1},-ba^{-1}} = T_{a^{-1},-ba^{-1}} \circ T_{a,b} = T_{1,0}.$$

(6) Έστω $G = \mathbb{R} \setminus \{-1\}$ με πράξη

$$a \star b = a + b + ab.$$

Θα δείξουμε ότι $(G, \star)$ είναι αβελιανή ομάδα.

Παρατηρούμε ότι αν $a, b \in \mathbb{R} \setminus \{-1\}$ και $a \star b = -1$, τότε

$$a + b + ab = -1 \Rightarrow (a+1)(b+1) = 0 \Rightarrow a = -1 \ \text{ή} \ b = -1.$$

Άρα πράγματι η $\star$ είναι πράξη στο G.

Έστω $a, b, c \in G$. Τότε

$$(a \star b) \star c = (a + b + ab) \star c = a + b + ab + c + ac + bc + abc$$

και

$$a \star (b \star c) = a \star (b + c + bc) = a + b + c + bc + ab + ac + abc.$$

Άρα $(a \star b) \star c = a \star (b \star c)$.

Για $e = 0$, έχουμε $a \star e = e \star a = a$, για κάθε $a \in G$.

Έστω $a \in G$. Θεωρούμε το $a' = -\frac{a}{1+a}$. Τότε $a' \in \mathbb{R} \setminus \{-1\}$ και $a \star a' = a' \star a = 0$.

Σημειώνουμε ότι το σύνολο $\mathbb{R}$ με πράξη $a \star b = a + b + ab$ δεν είναι ομάδα γιατί το -1 δεν έχει αντίστροφο.

(7) **Ομάδα συμμετριών** Έστω $M \subseteq \mathbb{R}^n$, $M \neq \emptyset$. Έστω

$$S(M) = \{f : \mathbb{R}^n \to \mathbb{R}^n : f \ \text{ συμμετρία του M}\}.$$

Ως προς την σύνθεση συναρτήσεων το $S(M)$ είναι ομάδα. Πράγματι εύκολα ελέγχουμε ότι αν $f, g \in S(M)$, τότε $f \circ g \in S(M)$. Επίσης η ταυτοτική απεικόνιση $1 : \mathbb{R}^n \to \mathbb{R}^n$ ανήκει στον $S(M)$ και $f \circ 1 = 1 \circ f = f$, για κάθε $f \in S(M)$. Τέλος εύκολα ελέγχουμε ότι αν $f \in S(M)$, τότε η f είναι 1-1. Αποδεικνύεται ότι η f είναι και επί, αλλά δεν θα δώσουμε απόδειξη εδώ καθώς απαιτούνται μέσα που δεν έχουμε αναπτύξει. Άρα η αντίστροφη απεικόνιση μιας συμμετρίας του M είναι συμμετρία του M.

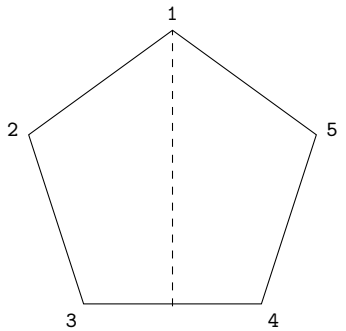
(8) **Διεδρικές ομάδας** D_n Με D_n συμβολίζουμε την ομάδα συμμετριών του κανονικού κυρτού n-γώνου. Θα δείξουμε εδώ ότι

$$|D_n| = 2n$$

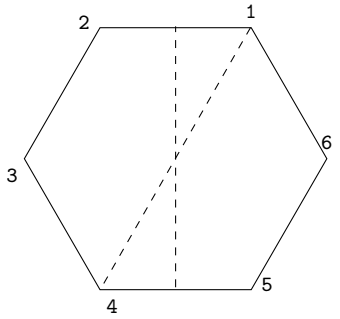
και θα βρούμε χρήσιμες παραστάσεις των στοιχείων της D_n.

Ας συμβολίσουμε με $r_i, i = 0, 1, ..., n-1$ την περιστροφή κατά γωνία $\frac{2\pi}{n} i$ στη θετική φορά, που δεχόμαστε ότι είναι η $\circlearrowleft$. Τότε $r_i \in D_n$ και οι συμμετρίες αυτές είναι διακεκριμένες. Θα θεωρήσουμε τώρα ανακλάσεις και για το σκοπό αυτό θα διακρίνουμε περιπτώσεις.

Αν το n είναι περιττός, θεωρούμε για κάθε κορυφή τον άξονα συμμετρίας που διέρχεται από αυτή. Έχουμε n το πλήθος τέτοιους άξονες και θεωρούμε τις ανακλάσεις $s_j, j = 1, ..., n$ ως προς αυτούς. Είναι σαφές ότι τα s_j είναι διακεκριμένες συμμετρίες (για παράδειγμα έχουν διαφορετικά σταθερά σημεία) και ότι συνολικά τα r_i, s_j για $i = 0, 1, ..., n-1$ και $j = 1, 2, ..., n$ είναι διακεκριμένα. Συνεπώς έχουμε $|D_n| \geq 2n$ όταν n είναι περιττός.



Αν το n είναι άρτιος, τότε κάθε άξονας συμμετρίας που διέρχεται από μια κορυφή, διέρχεται και από την απέναντι κορυφή. Όμως έχουμε και τους άξονες συμμετρίας που είναι οι μεσοκάθετοι απέναντι πλευρών. Τελικά και εδώ έχουμε n άξονες συμμετρίας που ορίζουν n ανακλάσεις οι οποίες με τις n περιστροφές είναι διάφορες ανά δύο. Συνεπώς έχουμε $|D_n| \geq 2n$ όταν n είναι άρτιος.



Μέχρι στιγμής είδαμε ότι $|D_n| \geq 2n$ για κάθε n. Θα δούμε τώρα ότι $|D_n| \leq 2n$ και άρα θα έχουμε ισότητα $|D_n| = 2n$.

Πράγματι, η εικόνα της κορυφής 1 κάτω από οποιαδήποτε συμμετρία του n-γώνου μπορεί να είναι οποιαδήποτε κορυφή i_1, άρα έχουμε το πολύ n επιλογές. Η κορυφή 2 (διαδοχική της 1) μπορεί να έχει εικόνα μια από τις 2 διαδοχικές της i_1 λόγω της διατήρησης αποστάσεων. Άρα για τις $1, 2$ έχουμε το πολύ $2n$ επιλογές. Εύκολα επαληθεύεται ότι οι υπόλοιπες κορυφές της εικόνας είναι μοναδικά ορισμένες λόγω διατήρησης αποστάσεων. (Για παράδειγμα, η κορυφή 3 έχει εικόνα διαδοχική της i_2, αλλά από τις δύο διαδοχικές κορυφές της i_2 η μία, η i_1, είναι ήδη κατειλημμένη).

(9) **Μη παραδείγματα.** (α) Η συνήθης πρόσθεση ακεραίων ορίζει πράξει στο σύνολο των φυσικών αριθμών $\mathbb{N} = \{0, 1, 2, ...\}$. Ισχύει η προσεταιριστική ιδιότητα καθώς $a + (b + c) = (a + b) + c$ για κάθε $a, b, c \in \mathbb{N}$. Επίσης υπάρχει ουδέτερο στοιχείο, το $0 \in \mathbb{N}$. Όμως δεν αληθεύει το αξίωμα (iii) στον ορισμό της ομάδας καθώς, για παράδειγμα το 1 (και κάθε άλλος θετικός ακέραιος) δεν έχει αντίθετο στο $\mathbb{N}$. Έτσι το $\mathbb{N}$ με τη συνήθη πρόσθεση δεν αποτελεί ομάδα.

(β) Στο σύνολο $\mathbb{Z}$, έχουμε την πράξη που ορίζεται από $a \star b = a - b$. Η πράξη αυτή δεν είναι προσεταιριστική καθώς, για παράδειγμα, $1 \star (1 \star 1) = 1 - (1 - 1) = 1$ αλλά $(1 \star 1) \star 1 = (1 - 1) - 1 = -1$.

Έστω G ομάδα και $a, b \in G$. Συνήθως θα γράφουμε ab για την εικόνα του διατεταγμένου ζεύγους $(a, b) \in G \times G$ κάτω από την πράξη της G και επίσης θα συμβολίζουμε με 1_G ή απλά με 1 το ουδέτερο στοιχείο της G. Δεν πρέπει να υπάρχει σύγχυση με τον αριθμό 1.

Νόμοι διαγραφής σε ομάδα

Έστω G ομάδα με πράξη

$$G \times G \to G, (a, b) \mapsto ab.$$

Αν $a_1, a_2, b_1, b_2 \in G$ με $a_1 = a_2, b_1 = b_2$, τότε τα διατεταγμένα ζεύγη $(a_1, b_1), (a_2, b_2)$ είναι ίσια και επειδή η παραπάνω αντιστοιχία είναι απεικόνιση (μοναδική εικόνα κάθε διατεταγμένου ζεύγους) έχουμε

$$a_1 b_1 = a_2 b_2.$$

Μιλώντας ελεύθερα, μπορούμε να πολλαπλασιάζουμε κατά μέλη δύο ισότητες σε μια ομάδα.

Τώρα αν $a, b, c \in G$ με

$$ac = bc,$$

τότε με βάση την προηγούμενη ιδιότητα παίρνουμε

$$\begin{aligned}(ac)c^{-1} &= (bc)c^{-1} \Rightarrow\\ a(cc^{-1}) &= b(cc^{-1}) \Rightarrow\\ a1_G &= b1_G \Rightarrow\\ a &= b.\end{aligned}$$

Επομένως σε μια ομάδα ισχύει η συνεπαγωγή

$$ac = bc \Rightarrow a = b.$$

Όμοια αποδεικνύεται ότι

$$ca = cb \Rightarrow a = b.$$

Οι συνεπαγωγές αυτές ονομάζονται νόμοι της διαγραφής.

Παραλείποντας παρενθέσεις

Έστω G ομάδα με πράξη $G \times G \to G, (a, b) \mapsto ab$. Για κάθε $a, b, c \in G$ έχουμε σύμφωνα με την προσεταιριστική ιδιότητα ότι

$$(ab)c = a(bc).$$

Το στοιχείο αυτό θα το συμβολίζουμε απλά abc χωρίς αναγραφή των παρενθέσεων.

Όμοια, για κάθε $a, b, c, d \in G$ έχουμε

$$((ab)c)d = (ab)(cd) = a(b(cd)) = a((bc)d).$$

Το στοιχείο αυτό θα το συμβολίζουμε συχνά $abcd$ χωρίς αναγραφή των παρενθέσων. Γενικά σε μια παράσταση της μορφής $a_1 \cdots (a_k \cdots (a_l \cdots) \cdots a_m) \cdots a_n$ σε ομάδα μπορούμε να παραλείψουμε τις παρενθέσεις και να γράψουμε απλά $a_1 a_2 \cdots a_n$. Δεν θα δώσουμε εδώ την ακριβή διατύπωση και απόδειξη του λεγόμενου γενικευμένου προσεταιριστικού νόμου. Μπορείτε να το δείτε στο Θεώρημα 13.8 (4) του βιβλίου των Stewart and Tall.

Είδαμε στο Παράδειγμα 6.6(2) ότι αν $X \neq \emptyset$ είναι ένα σύνολο και

$$S(X) = \{f : X \to X : f \ \ 1-1 \ \ \text{και επί}\},$$

τότε ως προς την σύνθεση συναρτήσεων το $S(X)$ είναι ομάδα. Θα μελετήσουμε τώρα τη $S(X)$ όταν το σύνολο X είναι πεπερασμένο.

Ορισμός 6.7. *Έστω n θετικός ακέραιος. Το σύνολο*

$$S_n = \{f : \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\} : f \ \ 1-1 \ \ \textit{και επί}\}$$

*εφοδιασμένο με την πράξη της σύνθεσης συναρτήσεων είναι ομάδα που καλείται η **συμμετρική ομάδα βαθμού** n. Κάθε στοιχείο της S_n λέγεται **μετάθεση** του $\{1, 2, \ldots, n\}$.*

Θα χρησιμοποιούμε συχνά το συμβολισμό

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \cdots & \sigma(n) \end{pmatrix}$$

για μεταθέσεις. Για παράδειγμα, γράφοντας

$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \in S_3,$$

εννοούμε ότι σ είναι η απεικόνιση $\sigma : \{1, 2, 3\} \to \{1, 2, 3\}$ που ορίζεται από

$$\sigma(1) = 3, \ \sigma(2) = 2, \ \sigma(3) = 1.$$

Παρατηρήσεις.

(1) Για $n = 1, 2, 3$ έχουμε

$$S_1 = \left\{ \begin{pmatrix} 1 \\ 1 \end{pmatrix} \right\},$$
$$S_2 = \left\{ \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \right\},$$
$$S_3 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \right\}.$$

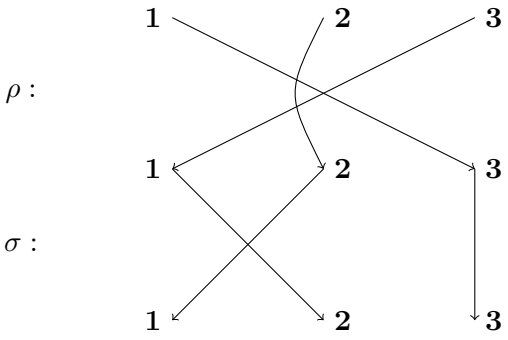
(2) Σύνθεση με τον συμβολισμό $\sigma = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \cdots & \sigma(n) \end{pmatrix}$.

Αν $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$ και $\rho = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$, τότε

$$\sigma \circ \rho = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix},$$

αφού $1 \xrightarrow{\rho} 3 \xrightarrow{\sigma} 3$, $2 \xrightarrow{\rho} 2 \xrightarrow{\sigma} 1$, $3 \xrightarrow{\rho} 1 \xrightarrow{\sigma} 2$.

Σχηματικά, έχουμε την ακόλουθη κατακόρυφη διάταξη. Για να βρούμε, για παράδειγμα, την εικόνα $\sigma \circ \rho(3)$ της σύνθεσης $\sigma \circ \rho$ στο 3, ακολουθούμε το μονοπάτι που αρχίζει από πάνω με το 3.



(3) Υπολογισμός της σ^{-1} με τον συμβολισμό $\sigma = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \cdots & \sigma(n) \end{pmatrix}$.

Αν $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 2 & 1 \end{pmatrix}$, τότε

$$\sigma^{-1} = \begin{pmatrix} 3 & 4 & 5 & 2 & 1 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 1 & 2 & 3 \end{pmatrix}.$$

(4) Αν $n \geq 3$, τότε η ομάδα S_n δεν είναι αβελιανή.
Πράγματι, αν
$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & \cdots & n \\ 2 & 1 & 3 & 4 & \cdots & n \end{pmatrix}$ και $\rho = \begin{pmatrix} 1 & 2 & 3 & 4 & \cdots & n \\ 1 & 3 & 2 & 4 & \cdots & n \end{pmatrix}$, τότε

$$\sigma \circ \rho(3) = \sigma(\rho(3)) = \sigma(2) = 1, \text{ και}$$
$$\rho \circ \sigma(3) = \rho(\sigma(3)) = \rho(3) = 2.$$

Άρα $\sigma \circ \rho(3) \neq \rho \circ \sigma(3)$, οπότε $\sigma \circ \rho \neq \rho \circ \sigma$.

Πρόταση 6.8. $|S_n| = n!$.

Απόδειξη. Κάθε μετάθεση του S_n γράφεται μοναδικά στη μορφή

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & \cdots & n-1 & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \cdots & \sigma(n-1) & \sigma(n) \end{pmatrix}.$$

Για το $\sigma(1)$ υπάρχουν n περιπτώσεις.

Για το $\sigma(2)$ υπάρχουν $n-1$ περιπτώσεις, αφού $\sigma(2) \neq \sigma(1)$ (σ είναι 1-1).

Για το $\sigma(3)$ υπάρχουν $n-2$ περιπτώσεις, αφού $\sigma(3) \neq \sigma(2), \sigma(3) \neq \sigma(1)$.

Συνεχίζοντας με τον ίδιο τρόπο βλέπουμε ότι για το $\sigma(n-1)$ υπάρχουν 2 περιπτώσεις και για το $\sigma(n)$ υπάρχει 1 περίπτωση.
Επομένως $|S_n| = n(n-1)\cdots 2 \cdot 1 = n!$. □

Κύκλοι

Ορισμός 6.9. *Μια μετάθεση $\sigma \in S_n$ λέγεται* ***κυκλική μετάθεση*** *(ή* ***κύκλος****) αν υπάρχουν $a_1, a_2, \cdots, a_m \in \{1, 2, \cdots, n\}$, ώστε*

$$\sigma(a_1) = a_2, \sigma(a_2) = a_3, \sigma(a_3) = a_4, \cdots, \sigma(a_{m-1}) = a_m, \sigma(a_m) = a_1, \text{ και}$$
$$\sigma(i) = i \quad \text{για κάθε } i \in \{1, 2, 3, \cdots, n\} \setminus \{a_1, \cdots, a_m\}.$$

Το m λέγεται το ***μήκος*** *της κυκλικής μετάθεσης. Συμβολίζουμε τον παραπάνω κύκλο με $\sigma = (a_1\ a_2\ \cdots\ a_m)$.*

Παραδείγματα 6.10.

(1) Ο κύκλος $\sigma = (4213) \in S_4$ είναι η μετάθεση $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}$.

(2) Ο κύκλος $\sigma = (4213) \in S_5$ είναι η μετάθεση $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 4 & 2 & 5 \end{pmatrix}$.

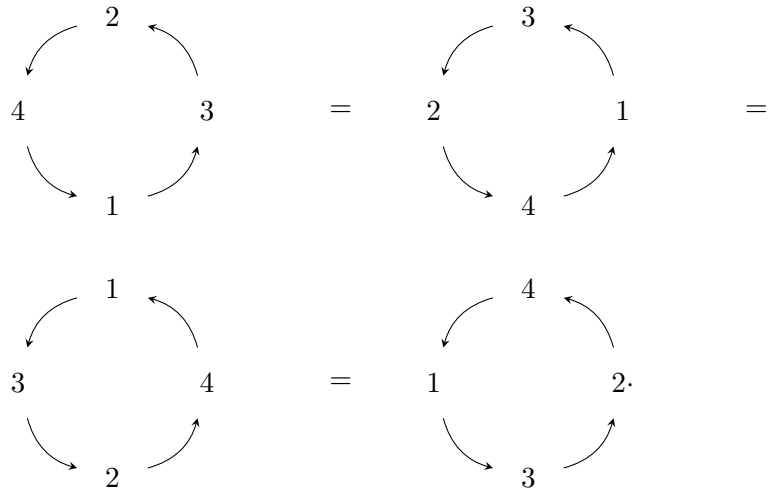
(3) Η μετάθεση $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} \in S_4$ δεν είναι κύκλος.

(4) Κάθε κύκλος μήκους 1 είναι η ταυτοτική μετάθεση, $(i) = 1$. Έτσι στο παράδειγμα (2), θα μπορούσαμε να γράψουμε $\sigma = (4213) \circ (5)$ για να το διακρίνουμε από τον κύκλο του παραδείγματος (1).

Παρατήρηση. Τα a_i στην παράσταση $(a_1\ a_2\ \cdots\ a_m)$ ενός κύκλου δεν είναι μοναδικά. Πράγματι, έχουμε

$$(2413) = (3241) = (1324) = (4132).$$

Σχηματικά οι παραπάνω ισότητες φαίνονται στο εξής διάγραμμα.



Γενικά έχουμε

$$(a_1\ a_2\ a_3 \cdots a_m) =$$

$$(a_m\ a_1\ a_2 \cdots a_{m-1}) = (a_{m-1}\ a_m\ a_1 \cdots a_{m-2}) = \cdots = (a_2\ a_3 \cdots a_m\ a_1).$$

Για τη (4213) έχουμε $4 \mapsto 2$, ενώ για τη (2413) έχουμε $4 \mapsto 1$ άρα $(4213) \neq (2134)$.

Παρατήρηση. Αν $\sigma = (a_1\ a_2 \cdots a_{m-1}\ a_m)$, τότε σ^{-1} είναι πάλι κύκλος και μάλιστα $\sigma^{-1} = (a_m\ a_{m-1} \cdots a_2\ a_1)$. Για παράδειγμα, $(4213)^{-1} = (3124)$.

Πριν διατυπώσουμε την επόμενη πρόταση, να σημειώσουμε ότι αν $\sigma \in S_n$, τότε ορίζεται η σύνθεση απεικονίσεων

$$\sigma \circ \sigma : \{1, 2, ..., n\} \xrightarrow{\sigma} \{1, 2, ..., n\} \xrightarrow{\sigma} \{1, 2, ..., n\}$$

που θα συμβολίζουμε σ^2. Δηλαδή $\sigma^2(i) = \sigma(\sigma(i))$ για κάθε $i = 1, 2, ..., n$. Όμοια τη σύνθεση $\sigma \circ \sigma \circ \sigma$ θα τη συμβολίζουμε σ^3 κοκ.

Πρόταση 6.11. *Έστω $\sigma \in S_n$ κύκλος μήκους $m \geq 2$. Τότε*
(1) *$\sigma^m = 1$ και*
(2) *$\sigma^k \neq 1$, για κάθε $k = 1, 2, \cdots, m-1$.*

Απόδειξη. Έστω $\sigma = (a_1\ a_2\ a_3 \cdots a_m)$. Τότε $\sigma(a_1) = a_2$, $\sigma^2(a_1) = \sigma(\sigma(a_1)) = \sigma(a_2) = a_3$ κλπ. Συνεχίζοντας με τον ίδιο τρόπο βλέπουμε ότι

$$\sigma^{m-1}(a_1) = \sigma(\sigma^{m-2}(a_1)) = \sigma(a_{m-1}) = a_m.$$

Άρα $\sigma,\ \sigma^2, \cdots, \sigma^{m-1} \neq 1$. Επίσης $\sigma^m(a_1) = \sigma(\sigma^{m-1}(a_1)) = \sigma(a_m) = a_1$. Ομοίως

$$\sigma^m(a_i) = a_i, \quad \text{για κάθε} \quad i = 1, 2, \cdots, m.$$

Άρα $\sigma^m = 1$ (θυμίζουμε ότι $\sigma(b) = b$, για κάθε $b \neq a_1, \cdots, a_m$). □

Η προηγούμενη πρόταση λέει ότι για έναν κύκλο σ μήκους m, ο μικρότερος θετικός ακέραιος k για τον οποίο ισχύει $\sigma^k = 1$ είναι ο m. Αυτό μας οδηγεί στην έννοια της τάξης στοιχείου που εξετάζεται στη συνέχεια.

6.3. Τάξη στοιχείου ομάδας

Έστω G ομάδα και $a, b \in G$. Συνήθως θα γράφουμε ab για την εικόνα του διατεταγμένου ζεύγους $(a, b) \in G \times G$ κάτω από την πράξη της G και επίσης θα συμβολίζουμε με 1_G ή απλά με 1 το ουδέτερο στοιχείο της G.

Αν $a \in G$, ορίζουμε επαγωγικά

$$a^0 = 1 \text{ και } a^{m+1} = aa^m,$$

όπου $m \in \mathbb{N}$. Επίσης ορίζουμε

$$a^{-m} = (a^{-1})^m,$$

όπου $m \in \mathbb{N}$. Αφήνουμε την επαλήθευση των εξής ισοτήτων ως άσκηση (η τυχερή σας μέρα).

Έστω $a, b \in G$, όπου G ομάδα. Για κάθε $m, n \in \mathbb{Z}$,

- $a^m a^n = a^{m+n} = a^n a^m$,
- $(a^m)^n = a^{mn} = (a^n)^m$,
- αν $ab = ba$, τότε $(ab)^m = a^m b^m$.

Προσοχή. Τα παραπάνω έχουν γραφεί έχοντας υπόψη *πολλαπλασιαστικό* συμβολισμό, ab, για την πράξη της G. Αν είχαμε προσθετικό συμβολισμό, $a + b$, τότε στη θέση του a^m θα γράφαμε ma και οι προηγούμενες ισότητες θα γράφονταν ως εξής (βλ. Παράγραφο 3.3 στους δακτυλίους).

- $ma + na = (m + n)a = na + ma$,
- $n(ma) = (mn)a = m(na)$,
- αν $a + b = b + a$, τότε $m(a + b) = ma + mb$.

Ορισμός 6.12. *Έστω G ομάδα και $g \in G$. Αν υπάρχει $m \in \mathbb{Z}_{>0}$ με $g^m = 1$, τότε ο ελάχιστος τέτοιος m λέγεται η* ***τάξη*** *του g και συμβολίζεται με $|g|$ ή $o(g)$. Αν δεν υπάρχει τέτοιος m, θα λέμε ότι η τάξη του g είναι* ***άπειρη****.*

Παραδείγματα 6.13.

(1) Έστω $\sigma \in S_n$ κύκλος μήκους k. Τότε $\sigma^k = 1$ και $\sigma^j \neq 1$, για κάθε $j = 1, 2, \ldots, k-1$, σύμφωνα με την Πρόταση 6.11 Δηλαδή $|\sigma| = k$.

(2) Έστω $G = \mathbb{R} \setminus \{0\}$ με πράξη τον πολλαπλασιασμό. Το στοιχείο 2 έχει άπειρη τάξη αφού $2^m \neq 1$ για κάθε θετικό ακέραιο m. Το στοιχείο -1 έχει τάξη 2 αφού $-1 \neq 1$ και $(-1)^2 = 1$.

(3) Θεωρούμε το σύνολο $E_4 = 1, -1, i, -i$. Ξέρουμε ότι είναι ομάδα με πράξη τον πολλαπλασιασμό του μιγαδικών. Παρατηρούμε ότι

g	1	-1	i	$-i$
$\|g\|$	1	2	4	4

για παράδειγμα $3^2 \equiv 9 \equiv 1 \mathrm{mod} 8$, δηλαδή $[3]^2 = [1]$ ($[3] \neq [1]$).

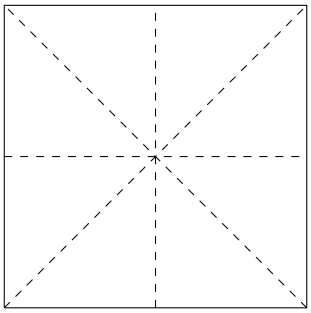
(4) Σύμφωνα με το πρώτο παράδειγμα, οι τάξεις των στοιχείων της ομάδας S_3 είναι

$g \in S_3$	1	(1 2)	(1 3)	(2 3)	(1 2 3)	(2 1 3)
$\|g\|$	1	2	2	2	3	3

(5) Θυμίζουμε ότι η διεδρική ομάδα D_4, δηλαδή η ομάδα των συμμετριών του τετραγώνου, έχει 8 στοιχεία

$$D_4 = \{1, r_1, r_2, r_3, s_1, s_2, s_3, s_4\},$$

όπου r_i είναι η περιστροφή κατά γωνία $\frac{\pi}{2} i$ και s_j είναι οι ανακλάσεις ως προς τους 4 άξονες συμμετρίας.



Είναι σαφές ότι $r_1^2 = r_2, r_1^3 = r_3$ και $r_1^4 = 1$. Άρα η τάξη του r_1 είναι ίση με 4. Με όμοιο τρόπο έχουμε ότι $|r_2| = 2$ και $|r_3| = 4$.

Για τις ανακλάσεις είναι σαφές ότι $|s_j| = 2$ για κάθε j.

(6) Σημειώνουμε ότι αν G είναι πεπερασμένη ομάδα, τότε κάθε $g \in G$ έχει πεπερασμένη τάξη. Πράγματι, θεωρώντας την ακολουθία στοιχείων της G,

$$1, g, g^2, g^3, ...$$

είναι σαφές ότι υπάρχουν φυσικοί αριθμοί $m > n$ με $g^m = g^n$. Άρα $g^{m-n} = 1$.

Θεώρημα 6.14. *Έστω G ομάδα και $g \in G$. Έστω ότι $|g| = k < \infty$. Τότε ισχύουν τα ακόλουθα.*

(1) *Έστω $m \in \mathbb{Z}_{>0}$. Τότε $g^m = 1 \Leftrightarrow k|m$.*
(2) *Έστω $m \in \mathbb{Z}_{>0}$. Τότε $|g^m| = \frac{k}{\mu\kappa\delta(k,m)}$.*

Απόδειξη. (1) Από την Ευκλείδεια διαίρεση υπάρχουν $q, r \in \mathbb{Z}$ ώστε $m = qk + r$, $0 \leq r < k$. Τότε

$$g^m = (g^k)^q g^r = 1^q g^r = g^r.$$

Αν $g^m = 1$, τότε $g^r = 1$ και επειδή $0 \leq r < k$, όπου $k = |g|$ παίρνουμε $r = 0$. Αν $k|m$, τότε $r = 0$ και $g^m = 1$.

(2) Παρατηρούμε ότι $(g^m)^{\frac{k}{\mu\kappa\delta(k,m)}} = (g^k)^{\frac{m}{\mu\kappa\delta(k,m)}} = 1$. Άρα

$$|g^m| \leq \frac{k}{\mu\kappa\delta(k,m)}.$$

Έστω $(g^m)^s = 1,\ s \in \mathbb{Z}_{>0}$. Τότε $g^{ms} = 1$, οπότε από το (1) του θεωρήματος έπεται ότι $k|ms$. Τότε

$$\frac{k}{\mu\kappa\delta(k,m)} \Bigg| \frac{m}{\mu\kappa\delta(k,m)} s.$$

Όμως $\mu\kappa\delta\left(\frac{k}{\mu\kappa\delta(k,m)}, \frac{m}{\mu\kappa\delta(k,m)}\right) = 1$, άρα $\frac{k}{\mu\kappa\delta(k,m)} \Big| s \Rightarrow \frac{k}{\mu\kappa\delta(k,m)} \leq s$. Συνεπώς $|g^m| = \frac{k}{\mu\kappa\delta(k,m)}$. □

Για παράδειγμα, αν $\sigma \in S_n$ είναι κύκλος μήκους 8, τότε $\left|\sigma^{50}\right| = \frac{8}{\mu\kappa\delta(50,8)} = \frac{8}{2} = 4$.

Σχόλιο. Είδαμε πριν ότι αν g είναι στοιχείο ομάδας, τότε η τάξη του g^m καθορίζεται από την τάξη του g και το m. Για το γινόμενο ab δυο στοιχείων μια ομάδας δεν αληθεύει ότι η τάξη του ab καθορίζεται από τις τάξεις των a, b. Για παράδειγμα, στην ομάδα S_4 καθένα από τα στοιχεία $(12), (23), (34)$ έχει τάξη 2, το γινόμενο $(12)(23) = (132)$ έχει τάξη 3 ενώ το γινόμενο $(12)(34)$ έχει τάξη 2. Επίσης, είναι δυνατό δύο στοιχεία πεπερασμένης τάξης να έχουν γινόμενο άπειρης τάξης. Συνεπώς τίθεται το ερώτημα: Ποια είναι γενικά η σχέση των τάξεων των a, b, ab; Απάντηση: Απολύτως καμία. Συγκεκριμένα αναφέρουμε χωρίς απόδειξη το εξής αποτέλεσμα. Για κάθε $l, m, n \in \mathbb{Z}_{>0}$, υπάρχουν ομάδα G και στοιχεία a, b αυτής τέτοια ώστε $|a| = l, |b| = m, |ab| = n$.

Είδαμε στο Παράδειγμα 6.13 (6) ότι κάθε στοιχείο πεπερασμένης ομάδας G έχει πεπερασμένη τάξη. Μάλιστα αποδεικνύεται στην περίπτωση αυτή ότι η τάξη του g διαιρεί την τάξη της G. Θα δώσουμε εδώ μια απόδειξη στην ειδική περίπτωση που η ομάδα είναι αβελιανή. Με το αποτέλεσμα αυτό θα ολοκληρώσουμε το κεφάλαιο περί ομάδων. Περισσότερα μπορείτε να δείτε στα μαθήματα Βασική Άλγεβρα και Θεωρία Ομάδων.

Θεώρημα 6.15. *Έστω G πεπερασμένη αβελιανή ομάδα τάξης n και $g \in G$. Τότε ο ακέραιος $|g|$ διαιρεί το n και επιπλέον $g^n = 1$.*

Απόδειξη. Έστω ότι

$$G = \{g_1, g_2, ..., g_n\}.$$

Τα στοιχεία

$$gg_1, gg_2, ..., gg_n$$

ανήκουν στη G και είναι διακεκριμένα καθώς αν $gg_i = gg_j$, τότε από το νόμο διαγραφής έχουμε $g_i = g_j$. Επειδή το πλήθος τους είναι $n = |G|$ που είναι πεπερασμένος αριθμός, έχουμε

$$\{g_1, g_2, ..., g_n\} = \{gg_1, gg_2, ..., gg_n\}.$$

Σχηματίζοντας το γινόμενο όλων των στοιχείων της G, παίρνουμε

$$g_1 g_2 ... g_n = gg_1 gg_2 ... gg_n$$

και χρησιμοποιώντας ότι η ομάδα G είναι αβελιανή έχουμε,

$$g_1 g_2 ... g_n = g_1 g_2 ... g_n g^n.$$

Από το νόμο της διαγραφής παίρνουμε $g^n = 1$. Από το Θεώρημα 6.14 έπεται ότι $|g|$ διαιρεί το n. □

Ασκήσεις Κεφαλαίου 6

1. Έστω p ένας πρώτος αριθμός. Θεωρούμε το σύνολο

$$\mathbb{Q}_p = \{m/p^n \in \mathbb{Q} : m, n \in \mathbb{Z}\}.$$

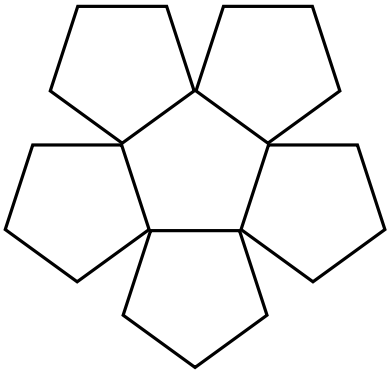
Δείξτε ότι $\mathbb{Z} \subseteq \mathbb{Q}_p \subseteq \mathbb{Q}$ και ότι με τη συνήθη πρόσθεση ρητών αριθμών το $\mathbb{Q}_p$ είναι αβελιανή ομάδα. Αληθεύει ότι $\mathbb{Q}_2 = \mathbb{Q}_3$; Ποια είναι η τομή $\mathbb{Q}_2 \cap \mathbb{Q}_3$;

2. Έστω G ομάδα και $a, b \in G$ με $ab = 1$.
   i) Αληθεύει ότι $ba = 1$;
   ii) Απλοποιείστε την παράσταση $a^{-1}bab^2a^3$.

3. Έστω G ομάδα. Δείξτε ότι για κάθε $a, b \in G$ υπάρχει μοναδικό $x \in G$ με $ax = b$. Στην απόδειξή σας, ποια αξιώματα στον ορισμό της ομάδας χρησιμοποιήσατε;

4. Δείξτε ότι η ομάδα G των συμμετριών του κύκλου περιέχει
   i) στοιχείο άπειρης τάξης, και
   ii) στοιχείο τάξης m για κάθε θετικό ακέραιο m.

5. Πόσα στοιχεία τάξης 2 και πόσα τάξης 5 έχει η ομάδα συμμετριών του παρακάτω σχήματος



6. Έστω G ομάδα και $a, b \in G$. Δείξτε ότι αν $ba = ab^n$ για κάποιο ακέραιο n τότε $b^m a = ab^{mn}$ για κάθε φυσικό αριθμό m.

7. Έστω G ομάδα και και $a \in G$. Δείξτε ότι οι παρακάτω απεικονίσεις είναι 1-1 και επί,

$$L_a : G \to G, x \mapsto ax,$$

$$R_a : G \to G, x \mapsto xa.$$

8. Έστω $G = \{a_1, ..., a_n\}$ πεπερασμένη ομάδα. Ο πίνακας πολλπλασιασμού της G είναι ένας $n \times n$ πίνακας που στην τομή της στήλης $\mathbf{a_i}$ και της στήλης $\mathbf{a_i}$ υπάρχει το στοιχείο $a_i a_j$. Δείξτε ότι κάθε γραμμή και κάθε στήλη αποτελείται από n διακεκριμένα στοιχεία. Συμπληρώστε τον παρακάτω πίνακα πολλαπλασιασμού μιας ομάδας τάξης 4.

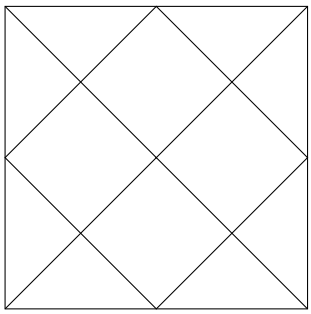
	$\mathbf{a_1}$	$\mathbf{a_2}$	$\mathbf{a_3}$	$\mathbf{a_4}$
$\mathbf{a_1}$	a_1	a_2	a_3	a_4
$\mathbf{a_2}$	a_2	a_1		a_3
$\mathbf{a_3}$	a_3	a_4		
$\mathbf{a_4}$	a_4		a_2	a_1

9. Πόσα στοιχεία έχει η ομάδα συμμετριών του σχήματος (γράμματος) Β και πόσα η ομάδα συμμετριών του σχήματος (γράμματος) Φ;

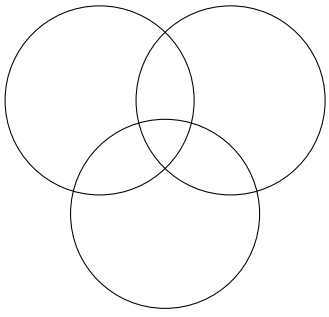
10. Έστω G ομάδα και $a, b \in G$. Τότε
    i) $|a| = |a^{-1}|$.
    ii) $|b^{-1}ab| = |a|$.
    iii) $|ab| = |ba|$.

11. Έστω G ομάδα τέτοια ώστε υπάρχει μοναδικό στοιχείο $a \in G$ με $|a| = 2$. Τότε $ab = ba$, για κάθε $b \in G$.
12. Βρείτε τις τάξης των στοιχείων της ομάδας E_6.
13. Έστω G ομάδα και $a, b, c \in G$ με $abc = 1$. Αληθεύει ότι $bca = 1$; Αληθεύει ότι $bac = 1$;
14. Δείξτε ότι αν μια ομάδα περιέχει στοιχείο τάξης 10, τότε περιέχει τουλάχιστον 4 στοιχεία τάξης 10.
15. Πόσα στοιχεία τάξης 2 έχει η διεδρική ομάδα D_n;
16. Έστω G αβελιανή ομάδα με $|G| \leq 40$. Να βρεθεί η τάξη της αν έχει στοιχείο τάξης 3 και στοιχείο τάξης 7.
17. Αν μια ομάδα G έχει στοιχείο τάξης m τότε η G έχει στοιχείο τάξης d για κάθε θετικό διαιρέτη d του m.
18. Έστω G αβελιανή ομάδα που διαθέτει στοιχεία τάξης m και n , όπου $\mu\kappa\delta(m, n) = 1$. Δείξτε ότι η G διαθέτει στοιχείο τάξης mn.
19. Έστω G αβελιανή ομάδα που διαθέτει στοιχεία τάξης m και n. Δείξτε ότι η G διαθέτει στοιχείο τάξης $\varepsilon\kappa\pi(m, n)$.
20. Έστω G αβελιανή ομάδα που διαθέτει στοιχεία τάξης 3 και 16. Αληθεύει ότι η G διαθέτει στοιχείο τάξης d για κάθε $d \in \{6, 12, 24, 48\}$;
21. Έστω G ομάδα τέτοια ώστε κάθε $g \in G \setminus \{1\}$ έχει τάξη 2. Τότε η G είναι αβελιανή.
22. Έστω G πεπερασμένη ομάδα και $A \subseteq G$ με $|A| > \frac{|G|}{2}$. Τότε για κάθε $g \in G$, υπάρχουν $a, a' \in A$ ώστε $g = aa'$.
23. Ποιες από τις ακόλουθες προτάσεις αληθεύουν; Δώστε απόδειξη ή αντιπαράδειγμα σε κάθε περίπτωση.
    i) Υπάρχει ομάδα με μοναδικό στοιχείο τάξης 3.
    ii) Αν G ομάδα, $a, b \in G$ και $a^3 = b^3$, τότε $a = b$.
    iii) Αν G ομάδα, $a, b \in G$ με $a^3 = b^3$ και $a^5 = b^5$, τότε $a = b$.
24. Ποιες είναι οι ομάδες συμμετριών των επόμενων σχημάτων;

i)



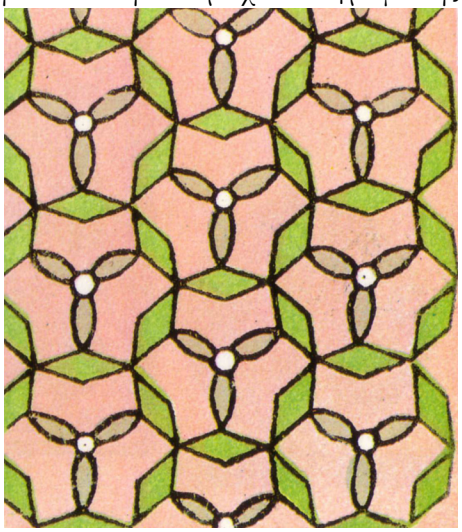
ii)



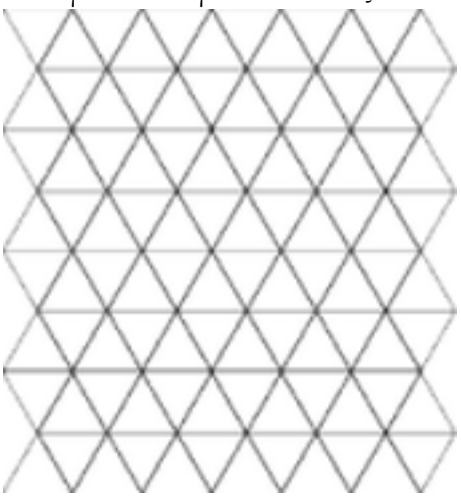
25. **Επίπεδες κρυσταλλογραφικές ομάδες** Θα δούμε εδώ δύο παραδείγματα άπειρων ομάδων συμμετριών που σχετίζονται με επικαλύψεις του επιπέδου. Θα περιορισθούμε σε διαισθητικές παρατηρήσεις.

    Φανταστείτε το επίπεδο καλυμμένο με το ακόλουθο μοτίβο και θεωρείστε την ομάδα G των ισομετριών του επιπέδου που διατηρούν την επικάλυψη αυτή. Αληθεύει ότι η G περιέχει άπειρο

το πλήθος μεταφορές και άπειρο το πλήθος ανακλάσεις και άπειρο το πλήθος περιστροφές; Αληθεύει ότι η G περιέχει αντίγραφο της ομάδας D_3; Της D_4;



Στη συνέχεια θεωρείστε την επικάλυψη του επιπέδου από ίσα ισόπλευρα τρίγωνα όπως υποδεικνύει η ακόλουθη εικόνα και εξετάστε τα ίδια ερωτήματα για την νέα ομάδα H.



Διαισθητικά, οι ομάδες G, H είναι ΄ίδιες΄; Ποια επικάλυψη είναι ΄πιο συμμετρική΄; Ποια έχει περισσότερες οικογένειες παραλλήλων αξόνων συμμετρίας;

Στο σύνδεσμο Wallpaper groups μπορείτε να δείτε μερικά πράγματα για τις επίπεδες κρυσταλλογραφικές ομάδες. Η ομάδα G είναι η $p31m$ και η ομάδα H είναι η $p6m$.

Υποδείξεις Ασκήσεων Κεφαλαίου 7

1.
2.
3.
4. *Λύση.* Έστω $r_a \in G$ η περιστροφή του επιπέδου κατά γωνία a. Είναι σαφές ότι για κάθε θετικό ακέραιο m έχουμε $(r_a)^m = r_{ma}$. Άρα $(r_a)^m = 1 \Leftrightarrow ma = 2k\pi, k \in \mathbb{Z}$. Συνεπώς επιλέγοντας $a = 2\pi x$, όπου x άρρητος, έχουμε $(r_a)^m \neq 1$ για κάθε $m \in \mathbb{Z}$, δηλαδή το r_a έχει άπειρη τάξη.

   Από τα παραπάνω έπεται ότι για κάθε θετικό ακέραιο m η περιστροφή κατά γωνία $\frac{2\pi}{m}$ έχει τάξη m.
5. Απάντηση. Έχει 5 στοιχεία τάξης 2 (ανακλάσεις) και 4 στοιχεία τάξης 5 (κάθε μη τετριμμένη περιστροφή).
6. Υπόδειξη. Επαγωγή στο m.
7.
8. Υπόδειξη. Βλ. προηγούμενη άσκηση.
9. Απάντηση. 2 και 4 αντίστοιχα.
10. *Λύση.*
    i) Παρατηρούμε ότι $a^s = 1 \Leftrightarrow (a^s)^{-1} = 1 \Leftrightarrow (a^{-1})^s = 1$. Άρα $|a| = |a^{-1}|$.
    ii) Παρατηρούμε ότι $(b^{-1}ab)^2 = b^{-1}abb^{-1}ab = b^{-1}a^2b$. Γενικά με επαγωγή παίρνουμε, $(b^{-1}ab)^s = b^{-1}a^sb$, για κάθε $s \in \mathbb{Z}_{>0}$. Επομένως $(b^{-1}ab)^s = 1 \Leftrightarrow b^{-1}a^sb = 1 \Leftrightarrow a^s = 1$. Άρα $|b^{-1}ab| = |a|$.
    iii) Χρησιμοποιώντας το ii) έχουμε $b^{-1}(ba)b = ab \Rightarrow |ba| = |ab|$.
11. *Λύση.* Έστω $b \in G$. Τότε από το δεύτερο ερώτημα της προηγούμενης άσκησης, παίρνουμε $|b^{-1}ab| = |a|$, άρα $|b^{-1}ab| = 2$. Από τη μοναδικότητα έπεται ότι $b^{-1}ab = a$, δηλαδή $ab = ba$.
12.
13. *Λύση.* Από $abc = 1$ έχουμε $bc = a^{-1}$ και επομένως $bca = 1$.

    Δεν αληθεύει ότι $bac = 1$. Ένα παράδειγμα είναι η ομάδα S_3,
    όπου $(12)(13)(123) = 1$, αλλά $(13)(12)(123) = (132) \neq 1$.
14. *Υπόδειξη.* Αν $|g| = 10$, τότε για κάθε ακέραιο m σχετικό πρώτο με το 10, ξέρουμε ότι $|g^m| = \frac{n}{\mu\kappa\delta(m,n)} = n$. Θεωρείστε τα g, g^3, g^7, g^9.
15. *Απάντηση.* Γενικά το ζητούμενο πλήθος για τη D_n είναι n αν το n είναι περιττός και $n+1$ αν το n είναι άρτιος.
16. Υπόδειξη. Η τάξη της G διαιρείται και από το 3 και από το 7 σύμφωνα με το θεώρημα 6.15. Άρα από το 21.
17.
18.
19.
20.
21. *Λύση.* Έστω $a, b \in G$. Από την υπόθεση έπεται ότι $(ab)^2 = 1$. Άρα
$$abab = 1 \Rightarrow ba = a^{-1}b^{-1} = ab,$$
    αφού $a^2 = b^2 = 1$.
22. *Λύση.* Θεωρούμε το σύνολο $B = \{a^{-1}g \in G : a \in A\}$. Έστω $g \in G$. Θα δείξουμε ότι $|B| > \frac{|G|}{2}$. Η απεικόνιση $f : A \to B$ με $f(a) = a^{-1}g$ είναι 1-1. Πράγματι, έστω $a_1, a_2 \in A$ με $f(a_1) = f(a_2)$. Τότε $a_1^{-1}g = a_2^{-1}g \Rightarrow a_1^{-1} = a_2^{-1} \Rightarrow a_1 = a_2$. Προφανώς η f είναι και επί. Άρα

$|B| = |A| > \frac{|G|}{2}$. Επομένως $A \cap B \neq \emptyset$. Δηλαδή υπάρχει $a' \in A$ και $a^{-1}g \in B$ ($a \in A$) ώστε $a^{-1}g = a' \Rightarrow g = aa'$.

23. *Λύση.*
   i) Λάθος. Αν το $a \in G$ έχει $|a| = 3$, τότε $|a^2| = \frac{3}{\mu\kappa\delta(3,2)} = 3$ και $a \neq a^2$. (Αν $a = a^2$, τότε $a = 1$ που δεν έχει τάξη 3.)
   Σημείωση. Αν η G έχει στοιχεία τάξης $m(< \infty)$, τότε η G έχει τουλάχιστον $\varphi(m)$ στοιχεία τάξης m. Αυτό έπεται από την $|a^k| = \frac{m}{\mu\kappa\delta(k,m)}$.
   ii) Λάθος. Έστω $G = S_3$ και $a = (123)$, $b = (213)$. Τότε $a \neq b$, ενώ $a^3 = b^3 = 1$.
   iii) Σωστό. Υπάρχουν $m, n \in \mathbb{Z}$ ώστε $1 = 3m + 5n$. Τότε
   $$a = a^1 = (a^3)^m(a^5)^n = (b^3)^m(b^5)^n = b^{3m+5n} = b.$$

24. *Απάντηση.* Του τετραγώνου και του ισόπλευρου τριγώνου αντίστοιχα, δηλαδή, D_4 και D_3.