Φυλλάδιο Α

A1. Έστω $\alpha \in G$. Τότε:

$$\alpha^2 = e \Rightarrow \alpha \cdot \alpha = \alpha \cdot \alpha^{-1} \xRightarrow[\text{διαγραφής}]{\text{νόμος}} \alpha = \alpha^{-1}$$

άρα: $\boxed{\forall \alpha \in G, \ \alpha = \alpha^{-1}}$ $(*)$

Για κάθε $x, y \in G$, από την $(*)$ έχουμε:

$$(xy) = (xy)^{-1} \Rightarrow xy = y^{-1}x^{-1} \xRightarrow{(*)} xy = yx.$$

Άρα η $(G, \cdot)$ είναι αβελιανή ∎

A2. Έστω $A = \begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix} \in H$. Τότε $\det(A) = 1 \neq 0$,

οπότε $A \in GL(2, \mathbb{Q})$. Συνεπώς, $H \subseteq GL(2, \mathbb{Q})$.

Ισχύει: $I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in H$ (με $\alpha = 0 \in \mathbb{Q}$).

Επίσης, για κάθε $A = \begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix}$, $B = \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \in H$

έχουμε: $B^{-1} = \begin{pmatrix} 1 & -b \\ 0 & 1 \end{pmatrix}$ και

$$AB^{-1} = \begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & -b \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & \alpha - b \\ 0 & 1 \end{pmatrix} \in H \quad (\alpha - b \in \mathbb{Q})$$

Ώστε, $H \leq GL(2, \mathbb{Q})$. ∎

A3. (i) Έχει γίνει στη θεωρία.

(ii) "$\Leftarrow$" Αν $H \subseteq K$ ή $K \subseteq H$ τότε:

$H \cup K = K \leq G$ ή $H \cup K = H \leq G$

"$\Rightarrow$" Υποθέτουμε ότι $H \cup K \leq G$. Έστω $H \nsubseteq K$ και δδο $K \subseteq H$. Επειδή $H \nsubseteq K$, υπάρχει $h \in H$ ώστε $h \notin K$. Έστω $\underline{\underline{x \in K}}$.

Τότε: $xh \notin K$ (διότι αν $xh \in K$ τότε $\exists\, y \in K: xh = y$, άρα $h = x^{-1}y \in K$ $\left(\begin{array}{l}\text{αφού } x, y \in K \\ \text{και } K \leq G\end{array}\right)$)

Άρα: $\left.\begin{array}{l} x \in K \subseteq H \cup K \\ h \in H \subseteq H \cup K \end{array}\right\} \xRightarrow{H \cup K \leq G} xh \in H \cup K$

$\xRightarrow{xh \notin K} xh \in H \Rightarrow \exists\, r \in H: xh = r$

$\Rightarrow \underline{\underline{x = rh^{-1} \in H}}.$

Ώστε, $K \subseteq H$.

■

A4. Θεωρούμε την ομάδα $V_4 = \{e, a, b, c\}$ του Klein. Τότε οι $H_1 = \{e, a\}$, $H_2 = \{e, b\}$ και $H_3 = \{e, c\}$ είναι γνήσιες υποομάδες της V_4 με $V_4 = H_1 \cup H_2 \cup H_3$. ∎

A5. Έχει γίνει στη θεωρία. Αφού $H \leq G$ και $g \in H$, έπεται $\langle g \rangle \subseteq H \leq G$. Άρα, $\langle g \rangle \leq H$. ∎

A6. $(\mathbb{Z}_{30}, +)$, $[25]_{30} \in \mathbb{Z}_{30} = \langle [1]_{30} \rangle$

$|\langle [25]_{30} \rangle| = o([25]_{30})$, όπου ισχύει:

$$o([25]_{30}) = o(25[1]_{30}) = \frac{o([1]_{30})}{(o([1]_{30}), 25)} =$$

$$= \frac{30}{(30, 25)} = \frac{30}{5} = 6.$$

• $(\mathbb{Z}_{42}, +)$, $[30]_{42} \in \mathbb{Z}_{42} = \langle [1]_{42} \rangle$

άρα $|\langle [30]_{42} \rangle| = o([30]_{42})$, όπου

$$o([30]_{42}) = o(30[1]_{42}) = \frac{o([1]_{42})}{(o([1]_{42}), 30)} =$$

$$= \frac{42}{(42, 30)} = \frac{42}{6} = 7.$$

A7. Έχουμε αποδείξει ότι το σύνολο των γεννητόρων μιας πεπερασμένης κυκλικής ομάδας $G = \langle a \rangle$, τάξης $n \in \mathbb{N}$ είναι το

$$\{ a^k \in G \mid 1 \leq k \leq n-1, (k,n) = 1 \}.$$

$(\mathbb{Z}_{10}, +)$: $\mathbb{Z}_{10} = \langle [1]_{10} \rangle$

• $(1, 10) = 1$, $(3, 10) = 1$, $(7, 10) = 1$, $(9, 10) = 1$

Γεννήτορες της $\mathbb{Z}_{10}$: $[1]_{10}, [3]_{10}, [7]_{10}, [9]_{10}$

Με ίδιο σκεπτικό:

Γεννήτορες της $\mathbb{Z}_{12}$: $[1]_{12}$, $[5]_{12}$, $[7]_{12}$, $[11]_{12}$

Γεννήτορες της $\mathbb{Z}_{15}$: $[1]_{15}$, $[2]_{15}$, $[4]_{15}$, $[7]_{15}$

$[8]_{15}$, $[11]_{15}$, $[13]_{15}$, $[14]_{15}$.

A8. Εφ' όσον $(G,\cdot)$ αβελιανή έχουμε:

$x^n = y^n \Rightarrow (xy^{-1})^n = e$. Θέτω $xy^{-1} = z$.

Επειδή $z^n = e$, έπεται $\boxed{o(z) \mid n}$ και

$xy^{-1} = z \iff \boxed{x = zy = yz}$

A9. $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 6 & 7 & 1 & 9 & 2 & 3 & 8 & 5 & 4 \end{pmatrix} \in S_9$

Έχουμε: $\sigma = (1\ 6\ 3) \circ (2\ 7\ 8\ 5) \circ (4\ 9)$

γινόμενο ξένων κύκλων

$o(\sigma) = [3,4,2] = 12$

Γράφουμε $\sigma = \underbrace{(1\ 3)\circ(1\ 6)\circ(2\ 5)\circ(2\ 8)\circ(2\ 7)\circ(4\ 9)}_{6 \text{ αντιμεταθέσεις}}$

άρα σ: άρτια.

Ισχύει $100.000 = 8.333 \cdot 12 + 4$, οπότε

$$\sigma^{100.000} = \sigma^{8.333\cdot 12+4} = (\sigma^{12})^{8.333} \circ \sigma^4 =$$

$$= Id^{8.333} \circ \sigma^4 = Id \circ \sigma^4 = \sigma^4,$$ άρα

$$\sigma^{100.000}(1) = \sigma^4(1) = \sigma(\sigma(\sigma(\sigma(1)))) = \sigma(\sigma(\sigma(6)))$$

$$= \sigma(\sigma(3)) = \sigma(1) = 6.$$

A10. i) Γράφουμε

$$\sigma = (1\ 3\ 6) \circ (2\ 4\ 8) \circ (5\ 7)$$

$$\tau = (1\ 2) \circ (3\ 4\ 5) \circ (6\ 7\ 8)$$

με $o(\sigma) = [3, 3, 2] = 6$

$o(\tau) = [2, 3, 3] = 6$

ii) Ισχύουν: $2013 = 6 \cdot 335 + 3$, οπότε:

$2015 = 6 \cdot 335 + 5$

$$\sigma^{2013} = \sigma^{6 \cdot 335 + 3} = \sigma^{6 \cdot 335} \circ \sigma^3 = (\sigma^6)^{335} \circ \sigma^3$$

$$\xlongequal[\sigma^6 = Id]{o(\sigma) = 6} Id^{335} \circ \sigma^3 = Id \circ \sigma^3 = \sigma^3$$

Ομοίως, $\tau^{2015} = \tau^5$

Άρα, $\sigma^2 = \sigma \circ \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 6 & 8 & 1 & 2 & 5 & 3 & 7 & 4 \end{pmatrix}$

$$\sigma^3 = \sigma^2 \circ \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 2 & 3 & 4 & 7 & 6 & 5 & 8 \end{pmatrix}$$

$$\tau^2 = \tau \circ \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 2 & 5 & 3 & 4 & 8 & 6 & 7 \end{pmatrix}$$

$$\tau^3 = \tau^2 \circ \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 1 & 3 & 4 & 5 & 6 & 7 & 8 \end{pmatrix}$$

Τελικά, $\tau^5 = \tau^3 \circ \tau^2 =$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 1 & 5 & 3 & 4 & 8 & 6 & 7 \end{pmatrix}$$

(iii) Θεωρία: Δύο μεταθέσεις $\sigma, \tau \in S_n$ λέγονται **συζυγείς**, αν υπάρχει $\rho \in S_n$ ώστε $\rho \circ \tau \circ \rho^{-1} = \sigma$.

Έχουμε αποδείξει ότι συζυγείς μεταθέσεις έχουν ίδια τάξη και ίδιο πρόσημο (δηλαδή ή και οι δύο άρτιες ή και οι δύο περιττές).

Πίσω στην άσκηση:

<u>Βήμα 1</u>: Ελέγχουμε αν οι σ, τ έχουν ίδια τάξη. Αν $o(\sigma) \neq o(\tau)$ τότε οι σ, τ δεν είναι συζυγείς ($\nexists\, \rho \in S_8 : \rho \circ \tau \circ \rho^{-1} = \sigma$).

Αν $o(\sigma) = o(\tau)$, βλέπε Βήμα 2.

<u>Βήμα 2</u>: Ελέγχουμε τις σ, τ ως προς την αρτιότητα. Αν σ: άρτια (αντ. περιττή) και τ: περιττή (αντ. άρτια) τότε οι σ, τ δεν είναι συζυγείς. Αν οι σ, τ είναι ταυτόχρονα άρτιες ή ταυτόχρονα περιττές, βλέπε Βήμα 3.

Από (i)

$$\sigma = (1\ 3\ 6)\circ(2\ 4\ 8)\circ(5\ 7)$$
$$= (1\ 6)\circ(1\ 3)\circ(2\ 8)\circ(2\ 4)\circ(5\ 7)$$

$$\tau = (1\ 2)\circ(3\ 4\ 5)\circ(6\ 7\ 8)$$
$$= (1\ 2)\circ(3\ 5)\circ(3\ 4)\circ(6\ 8)\circ(6\ 7)$$

Συνεπώς οι σ, τ είναι περιττές.

<u>Βήμα 3</u>: Για $\rho \in S_8$ έχουμε:

$\rho \circ \tau \circ \rho^{-1} = \rho \circ ((1\ 2) \circ (3\ 4\ 5) \circ (6\ 7\ 8)) \circ \rho^{-1} =$

$= (\rho \circ (1\ 2) \circ \rho^{-1}) \circ (\rho \circ (3\ 4\ 5) \circ \rho^{-1}) \circ (\rho \circ (6\ 7\ 8) \circ \rho^{-1})$

$= (\rho(1)\ \rho(2)) \circ (\rho(3)\ \rho(4)\ \rho(5)) \circ (\rho(6)\ \rho(7)\ \rho(8))$

Για να ισχύει $\rho \circ \tau \circ \rho^{-1} = \sigma$, θα πρέπει:

$(\rho(1)\ \rho(2)) \circ (\rho(3)\ \rho(4)\ \rho(5)) \circ (\rho(6)\ \rho(7)\ \rho(8)) = \sigma$

ή ισοδύναμα:

επειδή ξένοι κύκλοι μετατίθενται:

$(\rho(3)\ \rho(4)\ \rho(5)) \circ (\rho(6)\ \rho(7)\ \rho(8)) \circ (\rho(1)\ \rho(2)) =$

$(1\ 3\ 6) \circ (2\ 4\ 8) \circ (5\ 7) = \sigma$

Λόγω μοναδικότητας της ανάλυσης της σ σε ξένους κύκλους επιλέγουμε:

$$\rho = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 7 & 1 & 3 & 6 & 2 & 4 & 8 \end{pmatrix}.$$

∎

A11. $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 1 & 2 & i & j & 7 & 8 & 9 & 6 \end{pmatrix}$

Υπάρχουν δύο επιλογές:

1) $i=4,\ j=5,$ οπότε:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 1 & 2 & 4 & 5 & 7 & 8 & 9 & 6 \end{pmatrix}$$

$$= (1\ 3\ 2) \circ (6\ 7\ 8\ 9)$$

$$= (1\ 2) \circ (1\ 3) \circ (6\ 9) \circ (6\ 8) \circ (6\ 7) : \text{περιττή}$$

2) $i=5,\ j=4,$ οπότε:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 1 & 2 & 5 & 4 & 7 & 8 & 9 & 6 \end{pmatrix}$$

$$= (1\ 3\ 2) \circ (4\ 5) \circ (6\ 7\ 8\ 9)$$

$$= (1\ 2) \circ (1\ 3) \circ (4\ 5) \circ (6\ 9) \circ (6\ 8) \circ (6\ 7) : \text{άρτια.}$$

Τελικά, $i=5,\ j=4$

Α12. Επειδή η τ είναι 8-κύκλος

έπεται: $o(\tau) = 8 \Rightarrow \tau^8 = Id$.

$\langle \tau \rangle = \{ Id, \tau, \tau^2, \tau^3, \tau^4, \tau^5, \tau^6, \tau^7 \}$

$= \langle \tau^{-1} \rangle = \langle \tau^7 \rangle$ (διότι: $\tau \circ \tau^7 = Id = \tau^7 \circ \tau$)

Για $n \geq 9$ έχουμε: $n = 8q + r$, όπου $0 \leq r \leq 7$.

άρα: $\tau^n = \tau^r$, $0 \leq r \leq 7$.

Για $n \leq -2$: $\tau^n = \tau^r$, $0 \leq r \leq 7$.

. $o(\tau^2) = \dfrac{o(\tau)}{(o(\tau), 2)} = \dfrac{8}{(8,2)} = \dfrac{8}{2} = 4$

$\langle \tau^2 \rangle = \{ Id, \tau^2, \tau^4, \tau^6 \}$

. $o(\tau^3) = 8 \Rightarrow \langle \tau^3 \rangle = \langle \tau \rangle$

. $o(\tau^4) = 2 \Rightarrow \langle \tau^4 \rangle = \{ Id, \tau^4 \}$

. $o(\tau^5) = o(\tau^7) = 8 \Rightarrow \langle \tau^5 \rangle = \langle \tau^7 \rangle = \langle \tau \rangle$

. $o(\tau^6) = \dfrac{8}{(8,6)} = \dfrac{8}{2} = 4$

$\langle \tau^6 \rangle = \{ Id, \tau^6, \underset{\tau^4}{\tau^{12}}, \underset{\tau^2}{\tau^{18}} \} = \langle \tau^2 \rangle$

A13. Στα ακόλουθα $f: G \to H$ ισομορφισμός ομάδων.

P_1 | <u>G: αβελιανή</u>: Θδο H: αβελιανή

Έστω $x, y \in H$. Αφού f: επί του H, υπάρχουν $a, b \in G$ με $f(a) = x$ και $f(b) = y$. Τότε

$$xy = f(a) f(b) = f(ab) \xrightarrow[\text{αβελιανή}]{G:} f(ba) = f(b) f(a) = yx.$$

Άρα H: αβελιανή. ∎

P_2 | <u>G: κυκλική</u>: Θδο H: κυκλική

Έστω $G = \langle a \rangle$ και θδο $H = \langle f(a) \rangle$.

Εφ' όσον $\langle f(a) \rangle \subseteq H$ αρκεί νδο $H \subseteq \langle f(a) \rangle$.

Έστω λοιπόν $x \in H$. Αφού f επί του H, υπάρχει $g \in G$ ώστε $f(g) =$ Όμως,

$g \in G \Rightarrow g \in \langle a \rangle \Rightarrow \exists k \in \mathbb{Z}: g = a^k$, άρα:

$$x = f(g) = f(a^k) = (f(a))^k \in \langle f(a) \rangle.$$

∎

P3 : <u>G: άπειρη</u> : Θδο H: άπειρη.

Πράγματι, εφ' όσον f: 1-1 και επί έχουμε $|H| = |G| = \infty$. ∎

P4 : $|G| = m$ και Θδο $|H| = m$

Πράγματι, f: 1-1 και επί $\Rightarrow |H| = |G| = m$ ∎

P5 $Z(G) = \{e_G\}$, Θδο $Z(H) = \{e_H\}$

Επειδή $\{e_H\} \subseteq Z(H)$, αρκεί $Z(H) \subseteq \{e_H\}$.

Έστω λοιπόν $x \in Z(H)$, δηλαδή: $xh = hx$, $\forall h \in H$.

Άρα, $\forall h \in H$: $f^{-1}(xh) = f^{-1}(hx) \Rightarrow \forall h \in H$:

$f^{-1}(x) f^{-1}(h) = f^{-1}(h) f^{-1}(x)$ $(*)$:

Για κάθε $g \in G$, θέτω $h = f(g) \in H$ και η

$(*)$ δίνει: $f^{-1}(x) f^{-1}(f(g)) = f^{-1}(f(g)) f^{-1}(x) \Rightarrow$

$\Rightarrow f^{-1}(x) g = g f^{-1}(x)$, οπότε: $f^{-1}(x) \in Z(G)$

$\Rightarrow f^{-1}(x) = e_G \Rightarrow f(f^{-1}(x)) = f(e_G)$

$\Rightarrow x = e_H \in \{e_H\}$, όπως θέλαμε. ∎

$\underline{P6}$ $\forall x \in G$, $o(x) < \infty$. Θδο: $\forall h \in H$, $o(h) < \infty$.

Έστω $h \in H$. Τότε $h = f(x)$ για κάποιο $x \in G$ διότι f: επί. Τότε $o(x) < \infty$ και από γνωστή πρόταση: $o(f(x)) \mid o(x) \Rightarrow o(h) \mid o(x) \Rightarrow$

$o(h) \leq o(x) < \infty$.

■

A14. $\mathbb{Z}_6 \ncong S_3$ διότι $\mathbb{Z}_6$: αβελιανή

S_3: όχι αβελιανή

· $\mathbb{Z}_4 \ncong \mathbb{Z}_2 \times \mathbb{Z}_2$ διότι: $\mathbb{Z}_4$: κυκλική

$\mathbb{Z}_2 \times \mathbb{Z}_2$: όχι κυκλική

· $\mathbb{Z} \ncong \mathbb{Q}$ διότι $\mathbb{Z}$: κυκλική

$\mathbb{Q}$: όχι κυκλική

A15. Εφ' όσον $H, K \leq G$ έπεται ότι $e \in H$ και $e \in K$, άρα: $e = e \cdot e \in H \cdot K$.

Έστω τώρα τυχόντα $x, y \in H \cdot K$ και θα αποδείξουμε ότι: $xy^{-1} \in H \cdot K$.

- $x \in H \cdot K \Rightarrow \exists\, h_1 \in H, k_1 \in K : x = h_1 k_1$
- $y \in H \cdot K \Rightarrow \exists\, h_2 \in H, k_2 \in K : y = h_2 k_2$

Άρα $xy^{-1} = h_1 k_1 (h_2 k_2)^{-1} = h_1 k_1 k_2^{-1} h_2^{-1}$

$$\underset{\text{αβελιανή}}{\overset{G:}{=\!=}} h_1 h_2^{-1} k_1 k_2^{-1} \overset{(*)}{\in} H \cdot K$$

Συνεπώς, $H \cdot K \leq G$. ∎

(*) $h_1, h_2 \in H,\ H \leq G \Rightarrow h_1 h_2^{-1} \in H$

$k_1, k_2 \in K,\ K \leq G \Rightarrow k_1 k_2^{-1} \in K$

A16. (i) Έστω $d = (n,m)$. Τότε υπάρχουν $x, y \in \mathbb{Z}$ ώστε $d = nx + my$ $(*)$.

Έστω $g \in \langle a^{(n,m)} \rangle = \langle a^d \rangle$. Τότε υπάρχει $k \in \mathbb{Z}$ ώστε $g = (a^d)^k$, άρα:

$$g = a^{dk} \overset{(*)}{=} a^{nkx + mky} = a^{nkx} \cdot a^{mky} =$$

$$= (a^n)^{kx} \cdot (a^m)^{ky} \in \langle a^n \rangle \cdot \langle a^m \rangle.$$

Άρα, $\langle a^d \rangle \subseteq \langle a^n \rangle \cdot \langle a^m \rangle$ (1).

Αντίστροφα, έστω $g \in \langle a^n \rangle \cdot \langle a^m \rangle$. Τότε $g = g_1 \cdot g_2$, όπου $g_1 \in \langle a^n \rangle$ και $g_2 \in \langle a^m \rangle$.

Δηλαδή, $g_1 = a^{nk_1}$ και $g_2 = a^{mk_2}$ για κάποια $k_1, k_2 \in \mathbb{Z}$. Επίσης: $d \mid n \Rightarrow \exists \lambda_1 \in \mathbb{Z}: n = \lambda_1 d$

$d \mid m \Rightarrow \exists \lambda_2 \in \mathbb{Z}: m = \lambda_2 d$

Ώστε, $g = g_1 \cdot g_2 = a^{nk_1} \cdot a^{mk_2} = a^{dk_1\lambda_1} \cdot a^{dk_2\lambda_2}$

$$= a^{d(k_1\lambda_1 + k_2\lambda_2)} = (a^d)^{k_1\lambda_1 + k_2\lambda_2} \in \langle a^d \rangle$$

οπότε $\langle a^n\rangle \cdot \langle a^m\rangle \subseteq \langle a^d\rangle$. (2)

Από (1), (2), $\langle a^d\rangle = \langle a^n\rangle \cdot \langle a^m\rangle$.

(ii) Θέτουμε $c = [n,m]$. Άρα:

$$n \mid c \Rightarrow \exists x \in \mathbb{Z} : c = nx$$

$$m \mid c \Rightarrow \exists y \in \mathbb{Z} : c = my$$

· Έστω $g \in \langle a^n\rangle \cap \langle a^m\rangle$. Τότε $g \in \langle a^n\rangle$ που σημαίνει ότι $g = a^{n\lambda_1}$ και $g \in \langle a^m\rangle$, που σημαίνει ότι $g = a^{n\lambda_1}$ και $g = a^{m\lambda_2}$ για κάποια $\lambda_1, \lambda_2 \in \mathbb{Z}$. Τότε:

$$a^{\lambda_1 n} = a^{\lambda_2 m} \Rightarrow a^{\lambda_1 n - \lambda_2 m} = e \xrightarrow[o(a)=\infty]{|G|=\infty}$$

$\lambda_1 n - \lambda_2 m = 0 \Rightarrow \lambda_1 n = \lambda_2 m$, οπότε:

Θέτοντας $t = \lambda_1 n = \lambda_2 m$, έχουμε:

$g = a^t \in \langle a^t\rangle$. Όμως: $\left.\begin{array}{l} n \mid t \\ m \mid t \end{array}\right\} \Rightarrow c \mid t$,

δηλαδή: $t = c \cdot r$ για κάποιο $r \in \mathbb{Z}$. Έτσι

$$g = a^t = (a^c)^r \in \langle a^c\rangle.$$

Επομένως, $\langle a^n \rangle \cap \langle a^m \rangle \subseteq \langle a^c \rangle$. (3)

Αντίστροφα, έστω $g \in \langle a^c \rangle$. Υπάρχει $s \in \mathbb{Z}$ ώστε $g = (a^c)^s = a^{cs}$. Λόγω (*):

$\cdot\ g = a^{cs} = a^{nxs} = (a^n)^{xs} \in \langle a^n \rangle$

$\cdot\ g = a^{cs} = a^{mys} = (a^m)^{ys} \in \langle a^m \rangle$

που συνεπάγεται ότι: $g \in \langle a^n \rangle \cap \langle a^m \rangle$.

Επομένως, $\langle a^c \rangle \subseteq \langle a^n \rangle \cap \langle a^m \rangle$ (4)

Από (3), (4), $\langle a^c \rangle = \langle a^n \rangle \cap \langle a^m \rangle$. ∎

<u>Σχόλιο</u>: $(\mathbb{Z}, +)$, $\mathbb{Z} = \langle 1 \rangle$: άπειρη κυκλική.

Για $n, m \in \mathbb{N}$: $\langle n \cdot 1 \rangle = \langle n \rangle = n\mathbb{Z}$

$\langle m \cdot 1 \rangle = \langle m \rangle = m\mathbb{Z}$

Α16: $n\mathbb{Z} + m\mathbb{Z} = (n, m)\mathbb{Z}$

$n\mathbb{Z} \cap m\mathbb{Z} = [n, m]\mathbb{Z}$ ∎