Παραδείγματα Κυκλικών Ομάδων

(I) Η τετριμμένη ομάδα $G = \{e\} = \langle e \rangle$ είναι κυκλική.

(II) Η $G = \{e, a\}$ όπου γνωρίζουμε ότι $a^2 = e$ είναι κυκλική με γεννήτορα το a, $G = \langle a \rangle$.

(III) Η $G = \{e, a, b\}$ με

$\cdot$	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

είναι κυκλική διότι:

$$G = \{e, a, b\} = \{e, a, a^2\} = \langle a \rangle$$

(IV) Η ομάδα V_4 του Klein δεν είναι κυκλική διότι $a^2 = b^2 = c^2 = e$, άρα κανένα στοιχείο της δεν είναι γεννήτοράς της.

Αντιθέτως η ομάδα G με τέσσερα στοιχεία e, a, b, c και πίνακα πολ/μου

$\cdot$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	a	e
c	c	b	e	a

είναι κυκλική διότι:

$$G = \{e, a, b, c\} = \{e, b^2, b, b^3\} = \langle b \rangle$$

(V) Η ομάδα $(\mathbb{Z}, +)$ είναι κυκλική με γεννήτορα το $1 \in \mathbb{Z}$ διότι:

$$\langle 1 \rangle = \{n \cdot 1 \in \mathbb{Z} \mid n \in \mathbb{Z}\} = \{n \in \mathbb{Z} \mid n \in \mathbb{Z}\} = \mathbb{Z}$$

<u>Άσκηση</u> (H/W): Να αποδείξετε ότι κάθε κυκλική ομάδα είναι αβελιανή. Ισχύει το αντίστροφο; (Έγινε στην παράδοση)

<u>Άσκηση</u> (H/W): Να δώσετε παράδειγμα ομάδας $(G, \cdot)$ και στοιχείου $g \in G$ με $|G| = \infty$ αλλά $|\langle g \rangle| < \infty$.

<u>Άσκηση</u> (H/W): Έστω $(G, \cdot)$ ομάδα, $H \leq G$ και $g \in H$. Να δείξετε ότι $\langle g \rangle \leq H$

<u>Άσκηση</u> (H/W): Να δείξετε ότι η $(\mathbb{Q}, +)$ δεν είναι κυκλική ομάδα.

Το κέντρο μιας Ομάδας

Ορισμός: Έστω $(G,\cdot)$ μια ομάδα. Το **κέντρο** $Z(G)$ της G ορίζεται να είναι το σύνολο $Z(G)=\{x\in G \mid xg=gx,\ \forall g\in G\}\subseteq G$.

! Το κέντρο μιας ομάδας μετράει "πόσο απέχει" η ομάδα απ' το να είναι αβελιανή.

Βασική Πρόταση

Έστω $(G,\cdot)$ μια ομάδα. Τότε:

(i) $Z(G)\leq G$ και $Z(G)$: αβελιανή

(ii) $Z(G)=G \iff G$: αβελιανή

(iii) $\forall a\in G,\ \forall x\in Z(G),\ axa^{-1}\in Z(G)$

Απόδειξη

(i) $\forall g\in G$: $eg=ge=g$, άρα: $e\in Z(G)$.

Έστω τώρα $x,y\in Z(G)$. Τότε:

$$\begin{cases} xg=gx,\ \forall g\in G & (*) \\ yg=gy,\ \forall g\in G & (**) \end{cases}$$

Τότε για κάθε $g \in G$ έχουμε: $xy^{-1}g =$

$x(g^{-1}y)^{-1} \overset{**}{=} x(yg^{-1})^{-1} = xgy^{-1} \overset{(*)}{=} gxy^{-1}$, άρα $xy^{-1} \in Z(G)$.

Συνεπώς, $Z(G) \leq G$. Επιπλέον, $Z(G)$: αβελιανή

διότι αν $x, y \in Z(G)$ τότε: $xg = gx$, $\forall g \in G$.

Για $g = y$ έχουμε: $xy = yx$.

(ii) "$\Longrightarrow$" Αν $G = Z(G)$ τότε λόγω του (i) η

G είναι αβελιανή.

"$\Longleftarrow$" Έστω $(G, \cdot)$ αβελιανή. Θα δείξουμε $G = Z(G)$.

Επειδή $Z(G) \subseteq G$, αρκεί $G \subseteq Z(G)$. Έστω

$a \in G$. Αφού G: αβελιανή έχουμε $ag = ga$, $\forall g \in G$,

άρα $a \in Z(G)$.

(iii) Έστω $a \in G$, $x \in Z(G)$ και θα δείξουμε ότι

$axa^{-1} \in Z(G)$. Γνωρίζουμε $\boxed{xy = yx, \ \forall y \in G}$ (I)

Τότε για κάθε $g \in G$ έχουμε:

$$\left.\begin{aligned} axa^{-1}g &\underset{y=a^{-1}g}{\overset{(I)}{=}} aa^{-1}gx = gx \\ gaxa^{-1} &\underset{y=ga}{\overset{(I)}{=}} xgaa^{-1} = xg \overset{(I)}{=} gx \end{aligned}\right\} \Rightarrow axa^{-1}g = gaxa^{-1},$$

που σημαίνει ότι $axa^{-1} \in Z(G)$

Οι Ομάδες $(\mathbb{Z}_n, +)$, $n \in \mathbb{N}$

Πριν τις ορίσουμε είναι αναγκαίο να υπενθυμίσουμε βασικές έννοιες της Θεωρίας Αριθμών:

Ορισμός (Διαιρετότητα): Έστω $\alpha, b \in \mathbb{Z}$.
Λέμε ότι ο <u>b διαιρεί τον α</u> και γράφουμε $b|\alpha$, αν υπάρχει $c \in \mathbb{Z}$: $\alpha = bc$

Ιδιότητες

Για κάθε $\alpha, b, c, d \in \mathbb{Z}$ ισχύουν:

(i) $\alpha \neq 0 \Rightarrow \alpha|\alpha$ και $\alpha|0$

(ii) $1|\alpha$ (iii) Αν $0|\alpha$, τότε $\alpha = 0$

(iv) $c|b$ και $b|\alpha \Rightarrow c|\alpha$

(v) $c|b$ και $c|\alpha \Rightarrow c|\alpha x + by$, $\forall x, y \in \mathbb{Z}$

(vi) $b|\alpha \Rightarrow cb|c\alpha$, για $c \neq 0$

(vii) $cb | ca,\ c \neq 0 \Rightarrow b | a$

(viii) $b | a$ και $a \neq 0 \Rightarrow |b| \leq |a|$

(ix) $b | a$ και $a | b \Rightarrow a = \pm b$

(x) $c | a$ και $d | b \Rightarrow cd | ab$

• Αποδεικνύουμε ενδεικτικά τις (ix) και (x).

(ix) $b | a \Rightarrow \exists\, c_1 \in \mathbb{Z} : a = bc_1$, άρα

$a | b \Rightarrow \exists\, c_2 \in \mathbb{Z} : b = ac_2$

$a = bc_1 = ac_2c_1 \Rightarrow a(1 - c_1c_2) = 0$

$\Rightarrow a = 0$ ή $c_1c_2 = 1$

Αν $a = 0$, τότε $b = 0 = \pm a$ ✓

Αν $c_1c_2 = 1$ τότε $c_1 = c_2 = 1$ και άρα $a = b$

ή $c_1 = c_2 = -1$ και άρα $a = -b$

(x) $c | a \Rightarrow \exists\, \lambda \in \mathbb{Z} : a = \lambda c$ Τότε.

$d | b \Rightarrow \exists\, t \in \mathbb{Z} : b = td$

$ab = \lambda t cd \Rightarrow cd | ab$.

$\blacksquare$

Πόρισμα: Κάθε $a \in \mathbb{Z}^*$ έχει πεπερασμένους το πλήθος διαιρέτες.

Απόδειξη: Έστω $a \in \mathbb{Z}^*$ και $b \in \mathbb{Z}$ με $b|a$.

Τότε από Ιδιότητα (viii) $|b| \leq |a|$ και

συνεπώς $b \in \underbrace{\{-|a|, -|a|+1, \dots, |a|-1, |a|\}}_{\text{πεπερασμένο σύνολο}}$

$\blacksquare$

Ορισμός: Ένας φυσικός αριθμός n λέγεται **πρώτος** αν οι μόνοι θετικοί διαιρέτες του είναι το 1 και το n

- $\mathbb{P} = \{2, 3, 5, 7, 11, 13, 17, \dots\}$

  ↳ το σύνολο των πρώτων αριθμών

Το $\mathbb{P}$ είναι άπειρο σύνολο.

Θεώρημα

Κάθε $n \in \mathbb{N}$, $n \geq 2$, γράφεται με μοναδικό τρόπο ως γινόμενο πρώτων αριθμών

Ευκλείδεια Διαίρεση

Αν $a, b \in \mathbb{Z}$ με $b > 0$, τότε υπάρχει μοναδικό ζεύγος $(q, r) \in \mathbb{Z} \times \mathbb{Z}$ τέτοιο ώστε

$$a = bq + r, \quad 0 \leq r < b$$

q: πηλίκο
r: υπόλοιπο

Ορισμός: Αν $a, b \in \mathbb{Z}^*$ τότε ο μεγαλύτερος $d \in \mathbb{N}$ ώστε $d \mid a$ και $d \mid b$ λέγεται μέγιστος κοινός διαιρέτης των a, b και συμβολίζεται με (a, b)

- Αποδεικνύεται ότι ο (a, b) όντως υπάρχει.

πχ: $(2,3) = 1$, $(5,20) = 5$, $(6,32) = 2$

Ορισμός: Δύο μη-μηδενικοί ακέραιοι a, b λέγονται σχετικά πρώτοι μεταξύ τους, αν $(a,b) = 1$.

Ορισμός: Αν $a, b \in \mathbb{Z}^*$, τότε ο ελάχιστος $m \in \mathbb{N}$ με $a|m$ και $b|m$ λέγεται ελάχιστο κοινό πολλαπλάσιο των a, b και συμβολίζεται με $[a, b]$.

Θεώρημα (Bachet ή Bezout)

Αν $a, b \in \mathbb{Z}^*$, τότε υπάρχουν $x, y \in \mathbb{Z}$ ώστε $(a, b) = ax + by$

Λήμμα Ευκλείδη

Έστω p: πρώτος και $a, b \in \mathbb{Z}^*$ με $p | ab$. Τότε $p | a$ ή $p | b$.

Αριθμητική Υπολοίπων

Ορισμός (Gauss): Έστω $n \in \mathbb{N}$. Δύο αριθμοί $a, b \in \mathbb{Z}$ λέγονται **ισοδύναμοι ή ισοϋπόλοιποι modulo n**, αν $n \mid a-b$.

Γράφουμε τότε $a \equiv b \pmod{n}$.

πχ: $8 \equiv 4 \pmod{2}$, $3 \equiv 11 \pmod{4}$
$1 \equiv 6 \pmod{5}$

Θεώρημα (Ιδιότητες)

Έστω $n \in \mathbb{N}$ και $a, b, c \in \mathbb{Z}$. Τότε:

(i) $a \equiv a \pmod{n}$ (ανακλαστική)

(ii) $a \equiv b \pmod{n} \Rightarrow b \equiv a \pmod{n}$
(συμμετρική)

(iii) $a \equiv b \pmod{n}$ και $b \equiv c \pmod{n} \Rightarrow a \equiv c \pmod{n}$
(μεταβατική)

Απόδειξη

(i) Έχουμε ότι $n \mid \alpha - \alpha = 0$, άρα $\alpha \equiv \alpha \pmod{n}$

(ii) Αν $\alpha \equiv b \pmod{n}$ τότε $n \mid \alpha - b$, άρα

$n \mid -(\alpha - b) \Rightarrow n \mid b - \alpha \Rightarrow b \equiv \alpha \pmod{n}$

(iii) $\left.\begin{array}{l} \alpha \equiv b \pmod{n} \\ b \equiv c \pmod{n} \end{array}\right\} \Longrightarrow \begin{array}{l} n \mid \alpha - b \\ n \mid b - c \end{array}$, οπότε:

$n \mid (\alpha - b) + (b - c) \Rightarrow n \mid \alpha - c \Rightarrow \alpha \equiv c \pmod{n}$

$\blacksquare$

<u>Συμπέρασμα</u>: Έστω $n \in \mathbb{N}$. Το προηγούμενο θεώρημα μας λέει ότι η σχέση $\equiv \pmod{n}$ ορίζει μια σχέση ισοδυναμίας στο σύνολο $\mathbb{Z}$ και συνεπώς διαμερίζει το $\mathbb{Z}$ σε ξένα μεταξύ τους σύνολα, τις κλάσεις ισοδυναμίας

$$[\alpha]_n := \{ b \in \mathbb{Z} \mid \alpha \equiv b \pmod{n} \} \subseteq \mathbb{Z}.$$

Άρα, $\forall \alpha, \alpha' \in \mathbb{Z}$: $[\alpha]_n = [\alpha']_n \iff \alpha \equiv \alpha' \pmod{n}$

• Στο σύνολο $\mathbb{Z}_n$ ορίζουμε:

$+ : \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n$, $[a]_n + [c]_n := [a+c]_n$

Ισχυρισμός: Η + είναι καλά ορισμένη:

Έστω $[a]_n = [a']_n$ και $[c]_n = [c']_n$ και

Θδο $[a+c]_n = [a'+c']_n$: Πράγματι:

$\begin{cases} [a]_n = [a']_n \Rightarrow n \mid a-a' \\ [c]_n = [c']_n \Rightarrow n \mid c-c' \end{cases}$, άρα:

$n \mid a-a'+c-c' \Rightarrow n \mid (a+c)-(a'+c') \Rightarrow$

$a+c \equiv (a'+c') \pmod n \Rightarrow [a+c]_n = [a'+c']_n$.

Πχ: (i) $[7]_3 + [14]_3 = [19]_3 = [1]_3$

(ii) $[2]_5 + [2]_5 = [4]_5$

(iii) $[1]_7 + [102]_7 = [103]_7 = [5]_7$

(iv) $[0]_n + [a]_n = [a]_n$, $\forall n, \forall a$

(1) Για κάθε $[a]_n, [b]_n, [c]_n \in \mathbb{Z}_n$ ισχύει:

$$[a]_n + ([b]_n + [c]_n) = [a]_n + [b+c]_n = [a+(b+c)]_n =$$

$$[(a+b)+c]_n = [a+b]_n + [c]_n = ([a]_n + [b]_n) + [c]_n$$

(2) Υπάρχει το $[0]_n \in \mathbb{Z}_n$ ώστε:

$\forall [a]_n \in \mathbb{Z}_n$: $[a]_n + [0]_n = [a+0]_n = [a]_n = [0]_n + [a]_n$

(3) Για κάθε $[a]_n \in \mathbb{Z}_n$ ισχύει $[-a]_n \in \mathbb{Z}_n$

και $[a]_n + [-a]_n = [a+(-a)]_n = [0]_n = [-a]_n + [a]_n$

(4) $\forall [a]_n, [b]_n \in \mathbb{Z}_n$: $[a]_n + [b]_n = [a+b]_n = [b]_n + [a]_n$.

<u>Συμπέρασμα</u>: Οι ιδιότητες (1) - (4) καθιστούν το ζεύγος $(\mathbb{Z}_n, +)$ αβελιανή ομάδα με μηδενικό στοιχείο το $[0]_n$ και για κάθε $[a]_n \in \mathbb{Z}_n$ ο αντίθετος είναι: $-[a]_n = [-a]_n$.

<u>Ερώτημα</u>: Η $(\mathbb{Z}_n, +)$ είναι πεπερασμένη ή άπειρη;