Δευτέρα 1/04/2019

ΘΕΩΡΗΜΑ Έστω $G=\langle a\rangle$ κυκλική ομάδα τάξης n και H υποομάδα της G. Η τάξη της H διαιρεί την τάξη της ομάδας G. Αν d διαιρέτης του $n=|G|$ τότε υπάρχει μοναδική υποομάδα της G που να έχει τάξη d, η $H=\langle a^{n/d}\rangle$.

Απόδειξη

- Έστω $|H|=d \Rightarrow H$ υποομάδα κυκλικής ομάδας $\Rightarrow H$ κυκλική
$H=\langle b\rangle$ $\quad o(b)=k\,b>1=|H|=d$
$b\in G=\langle a\rangle \Rightarrow b=a^m \quad d=o(b)=o(a^m)=\frac{o(a)}{\mu\kappa\delta(m,o(a))}=\frac{n}{\mu\kappa\delta(m,n)} \Rightarrow n=d\,\mu\kappa\delta(m,n) \Rightarrow d\mid n$
$|H|\mid|G|$.

- Έστω $d\mid n$. Τότε η τάξη της υποομάδας $\langle a^{n/d}\rangle$ είναι:

$$|\langle a^{n/d}\rangle|=o(a^{n/d})=\frac{o(a)}{\mu\kappa\delta(n/d,o(a))}=\frac{n}{\mu\kappa\delta(n/d,n)}=\frac{n}{\frac{n}{d}}=d$$

Άρα υπάρχει μια υποομάδα της G που έχει τάξη d, η $H=\langle a^{n/d}\rangle$.
Έστω H_1 υποομάδα της $G=\langle a\rangle$ τάξης d.
$H_1\le G=\langle a\rangle \Rightarrow H_1$ κυκλική $\Rightarrow H_1=\langle a^s\rangle$ για κάποιο $s\in\mathbb{Z}$
$d=|H_1|=|\langle a^s\rangle|=o(a^s)=\frac{o(a)}{\mu\kappa\delta(s,o(a))}=\frac{n}{\mu\kappa\delta(s,n)} \Rightarrow \mu\kappa\delta(s,n)=\frac{n}{d} \Rightarrow \frac{n}{d}\mid s \Rightarrow s=\lambda\frac{n}{d}$

$H_1=\langle a^s\rangle=\langle a^{\lambda\frac{n}{d}}\rangle=\langle (a^{n/d})^\lambda\rangle\le\langle a^{n/d}\rangle=H$
$\{a^{\frac{n}{n/d}}, a^{n/d}, a^{(n/d)^2}, \dots a^{(d-1)n/d}\}$ Άρα $H_1\le H$.
Το H_1 έχει d στοιχεία κι το H έχει d-στοιχεία. Άρα $H_1=H$.
(Το $H_1\le H$ και έχουν το ίδιο πλήθος στοιχείων d άρα $H_1=H$)
Άρα η H είναι μοναδική.

Παράδειγμα Έστω $G=\langle a\rangle$ κυκλική ομάδα τάξης 12. Βρείτε όλες τις υποομάδες της G.

Έστω $H\leq G=\langle a\rangle$ τότε $|H|$ είναι διαιρέτης της τάξης της G
Άρα $|H|\in\{1,2,3,4,6,12\}$.

1η περίπτωση $|H|=12$, $\langle a^{12/12}\rangle=\langle a^1\rangle$

2η περίπτωση $|H|=6$, $\langle a^{12/6}\rangle=\langle a^2\rangle$

3η περίπτωση $|H|=4$, $\langle a^{12/4}\rangle=\langle a^3\rangle$

4η περίπτωση $|H|=3$, $\langle a^{12/3}\rangle=\langle a^4\rangle$

5η περίπτωση $|H|=2$, $\langle a^{12/2}\rangle=\langle a^6\rangle$

6η περίπτωση $|H|=1$, $\langle a^{12/1}\rangle=\langle a^{12}\rangle=\langle 1\rangle$.

$\langle a\rangle=\{a^0=1, a, a^2, a^3, a^4, a^5, a^6, a^7, a^8, a^9, a^{10}, a^{11}\}=\langle a^1\rangle=\langle a^5\rangle=\langle a^7\rangle=\langle a^{11}\rangle$
(a γεννήτορας)
$=\varphi(12)=4$

γεννήτορας $a^r \iff 0\leq r\leq o(a)$, $\mu.κ.δ(r,o(a))=1$.

$\langle a^2\rangle=\{a^0=1, a^2, a^4, a^6, a^8, a^{10}\}=\langle(a^2)^1\rangle=\langle(a^2)^5\rangle=\langle a^{10}\rangle=\{\varphi(6)=2\}$

$(a^2)^r$: $0\leq r\leq 6$, $\mu.κ.δ(r,o(a^2))=\mu.κ.δ(r,6)=1$

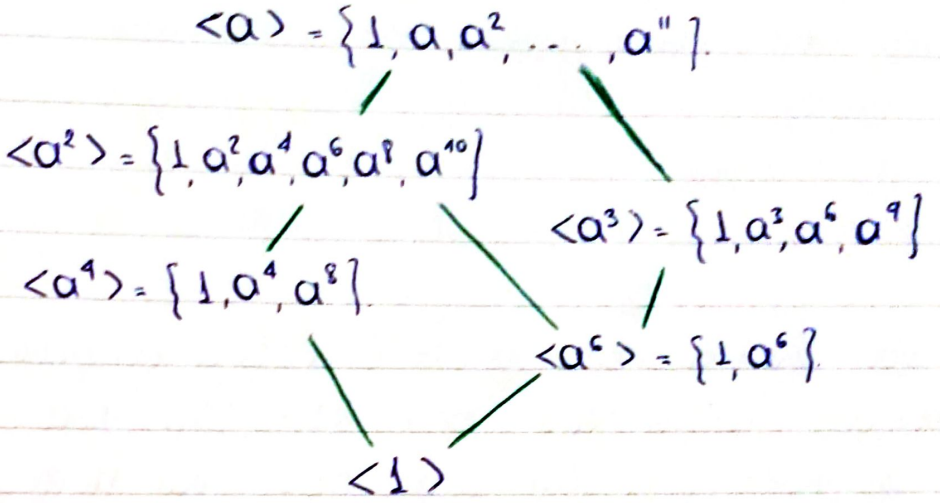
$\langle a^3\rangle=\{a^0=1, a^3, a^6, a^9\}=\langle a^3\rangle=\langle a^9\rangle$

$(a^3)^r$: $0\leq r\leq 4$, $\mu.κ.δ(r,4)=1$

$\langle a^4\rangle=\{a^0=1, a^4, a^8\}=\langle a^1\rangle=\langle a^8\rangle$ ← $\varphi(3)$
$\langle a^6\rangle=\{a^0=1, a^6\}$ ← $\varphi(2)$.
$\langle a^{12}\rangle=\langle 1\rangle$ ← $\varphi(1)$

$$\sum_{d \mid u} \varphi(d) = u$$

Διάγραμμα Hasse



Διάγραμμα Hasse της $Z_{12} = \{[0]_{12}, [1]_{12}, [2]_{12}, \ldots, [11]_{12}\}$

$$Z_{12} = \langle [1]_{12} \rangle$$

$\langle \frac{12}{6} [1]_{12} \rangle$

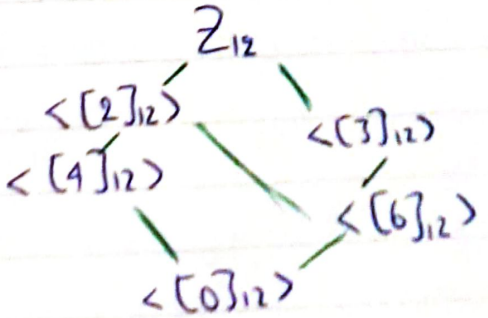
$= \langle [2]_{12} \rangle = \{[0]_{12}, [2]_{12}, [4]_{12}, [6]_{12}, [8]_{12}, [10]_{12}\}$

$\langle \frac{12}{4} [1]_{12} \rangle = \langle [3]_{12} \rangle = \{[0]_{12}, [3]_{12}, [6]_{12}, [9]_{12}\}$

$\langle \frac{12}{3} [1]_{12} \rangle = \langle [4]_{12} \rangle = \{[0]_{12}, [4]_{12}, [8]_{12}\}$

$\langle \frac{12}{2} [1]_{12} \rangle = \langle [6]_{12} \rangle = \{[0]_{12}, [6]_{12}\}$

$\langle \frac{12}{1} [1]_{12} \rangle = \langle [0]_{12} \rangle = \{[0]_{12}\}$



$G=\langle a\rangle$ με $|G|=o(a)=\infty$. Η τάξη του a δεν είναι πεπερασμένη.

$\{\dots, a^{-4}, \dots, a^{-3}, a^{-2}, a^{-1}, a^0, a^1, a^2, a^3, \dots, a^4, \dots\}$.

όλες οι δυνάμεις του a είναι διαφορετικές

$G \leq G=\langle a\rangle=\langle a^{-1}\rangle$

$\{1\}=\langle 1\rangle=\langle a^0\rangle$ ← 1 μόνο στοιχείο

$\langle a^{-2}\rangle=\langle a^2\rangle=\{a^{2\mu} \mid \mu\in\mathbb{Z}\}$.

$\langle a^{-3}\rangle=\langle a^3\rangle$

$\langle a^{-4}\rangle=\langle a^4\rangle$

Έστω $G=\langle a\rangle$ και $o(a)=\infty$ τότε η G έχει μια ακριβώς υποομάδα πεπερασμένης τάξης την $\langle a^0\rangle=\langle 1\rangle=\{1\}$ και έχει άπειρες υποομάδες που κάθε μία από αυτές δεν είναι πεπερασμένης τάξης. Αυτές είναι της μορφής $\langle a^m\rangle=\{a^{\nu m} \mid \nu\in\mathbb{Z}\}$ και κάθε μια από αυτές έχουν 2 γεννήτορες τον a^m και τον a^{-m}

Άσκηση: Έστω $G=\langle a\rangle$ με $|G|=o(a)=\infty$. Η τάξη του a δεν είναι πεπερασμένη. Δείξτε ότι αν $\langle a^\kappa\rangle=\langle a^\lambda\rangle$ τότε $\kappa=\lambda$ ή $\kappa=-\lambda$, $\kappa,\lambda\in\mathbb{Z}$

$a^\kappa=(a^\kappa)^1\in\langle a^\kappa\rangle=\langle a^\lambda\rangle \Rightarrow a^\kappa=(a^\lambda)^\mu \Rightarrow a^\kappa=a^{\lambda\mu}$ $\Big\}\Rightarrow \kappa=\lambda\mu \Rightarrow \lambda\mid\kappa$ ($o(a)=\infty$)

$a^\lambda=(a^\lambda)^1\in\langle a^\lambda\rangle=\langle a^\kappa\rangle \Rightarrow a^\lambda=(a^\kappa)^m \Rightarrow a^\lambda=a^{\kappa m}$ $\Big\}\Rightarrow \lambda=\kappa m \Rightarrow \kappa\mid\lambda$ ($m\in\mathbb{Z}$, $o(a)=\infty$)

$\left.\begin{array}{l}\kappa\mid\lambda\\ \lambda\mid\kappa\\ \kappa,\lambda\in\mathbb{Z}\end{array}\right\} \Rightarrow \left.\begin{array}{l}|\kappa|\mid|\lambda|\\ |\lambda|\mid|\kappa|\\ |\lambda|,|\kappa|\in\mathbb{N}\end{array}\right\} \Rightarrow |\kappa|=|\lambda| \Rightarrow \kappa=\lambda$ ή $\kappa=-\lambda$

Έστω G ομάδα, H υποομάδα της G και $a, b \in G$

$$a \sim_L b \quad \text{αν-ν} \quad a^{-1} \cdot b \in H$$
$$a \sim_R b \quad \text{αν-ν} \quad a \cdot b^{-1} \in H$$

Η $\sim_L$ είναι σχέση ισοδυναμίας / $\sim_R$ στο G είναι σχέση ισοδυναμίας

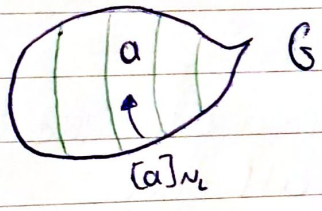
$1 \in H \Rightarrow a^{-1} a \in H \Rightarrow a \sim_L a, \forall a \in G \Rightarrow \sim_L$ είναι ανακλαστική

$a \sim_L b \Rightarrow a^{-1} \cdot b \in H \underset{H \leq G}{\Rightarrow} (a^{-1} \cdot b)^{-1} \in H \Rightarrow b^{-1} (a^{-1})^{-1} \in H \Rightarrow b^{-1} a \in H \Rightarrow b \sim_L a \Rightarrow \sim_L$ συμμετρική

$$\left.\begin{array}{l} a \sim_L b \Rightarrow a^{-1} \cdot b \in H \\ b \sim_L \gamma \Rightarrow b^{-1} \cdot \gamma \in H \end{array}\right\} \underset{H \leq G}{\Rightarrow} (a^{-1} b)(b^{-1} \gamma) \in H \to a^{-1} \cdot b \cdot b^{-1} \gamma \in H \Rightarrow a^{-1} \gamma \in H \Rightarrow a \sim_L \gamma \Rightarrow$$

$\sim_L$ μεταβατική.

Άρα η $\sim_L$ είναι σχέση ισοδυναμίας.



$a \sim_L b \Leftrightarrow a^{-1} \cdot b \in H$
$a \sim_R b \Leftrightarrow a \cdot b^{-1} \in H$

$a^{-1} \cdot b \in H$
$a^{-1} \cdot b = h, \ h \in H$
$b = ah$
$aH = \{ah \mid h \in H\}$.

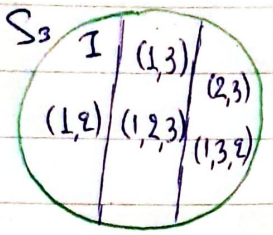
$$[a]_{\sim_L} = \{b \in G \mid a \sim_L b\} = \{b \in G \mid a^{-1} \cdot b \in H\}$$
$$= \{b \in G \mid b \in aH\} = aH$$

$$[a]_{\sim_R} = Ha$$

Ορισμός: Το σύνολο aH ονομάζεται αριστερό σύμπλοκο ή αριστερή πλευρική κλάση του a. Αντίστοιχα το σύνολο Ha ονομάζεται δεξιό σύμπλοκο ή δεξιά πλευρική κλάση που περιέχει το a.

Άσκηση: Έστω $H = \{I, (1,2)\} = \langle (1,2) \rangle$ υποομάδα της S_3. Βρείτε τα αριστερά και τα δεξιά σύμπλοκα (ή πλευρικές κλάσεις) της H.

Αριστερά

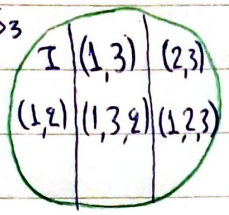


$I \cdot H = I \cdot \{I, (1,2)\} = \{I \cdot I, I \cdot (1,2)\} = \{I, (1,2)\}$.

$(1,3) \cdot H = (1,3)\{I, (1,2)\} = \{(1,3)I, (1,3)(1,2)\} = \{(1,3), (1,2,3)\}$.

$(2,3) \cdot H = (2,3)\{I, (1,2)\} = \{(2,3)I, (2,3)(1,2)\} = \{(2,3), (1,3,2)\}$

Δεξιά



$H \cdot I = \{I, (1,2)\}I = \{I \cdot I, (1,2) \cdot I\} = \{I, (1,2)\}$.

$H(1,3) = \{I, (1,2)\}(1,3) = \{I(1,3), (1,2)(1,3)\} = \{(1,3), (1,3,2)\}$

$H(2,3) = \{I, (1,2)\}(2,3) = \{I(2,3), (1,2)(2,3)\} = \{(2,3), (1,2,3)\}$.

Τα αριστερά συμπλοκα δεν ταυτίζονται με τα δεξιά συμπλοκα

ΠΑΡΑΤΗΡΗΣΕΙΣ:

$HI = H(1,2)$

$H(1,3) = H(1,3,2)$

$H(2,3) = H(1,2,3)$

ΠΡΟΤΑΣΗ Έστω H υποομάδα μιας ομάδας με πεπερασμένο πλήθος στοιχείων (δηλ. $|H| = d$). Το αριστερό συμπλοκο aH έχει d-στοιχεία (δηλ. το πλήθος των στοιχείων του συνόλου aH είναι ίσο με το πλήθος των στοιχείων της H.).

$H \xrightarrow{f} aH$

$f(h) = ah$ f καλά ορισμένη αφού $f(a) = a \cdot h \in aH$

- $f(h_1) = f(h_2) \Rightarrow a \cdot h_1 = a h_2 \xrightarrow[\text{νόμος διαγρ.}]{\text{αριστερός}} h_1 = h_2 \Rightarrow$ η f "1-1"
- Έστω $x \in aH \Rightarrow x = ah \Rightarrow x = f(h) \Rightarrow f$ επί

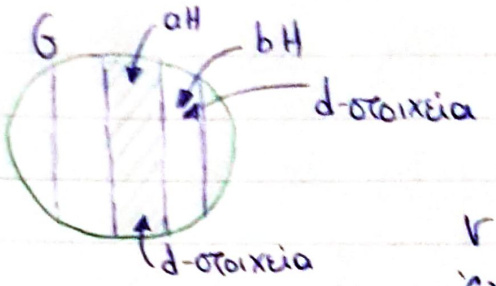
Άρα τα δυο σύνολα H, aH έχουν το ίδιο πλήθος στοιχείων.

ΘΕΩΡΗΜΑ Lagrange: Έστω H μια υποομάδα μιας πεπερασμένης ομάδας G. Τότε η τάξη της H διαιρεί την τάξη της G.

Αριστερά συμπλοκα της H στην G

Έστω r το πλήθος των αριστερών συμπλόκων

$n = |G|$ $d = |H|$.



r συμπλοκα και το καθε ενα εχει d-στοιχεια

$n=|G|$

Αρα $n=|G| = r\cdot d - r|H| \Rightarrow d|n$

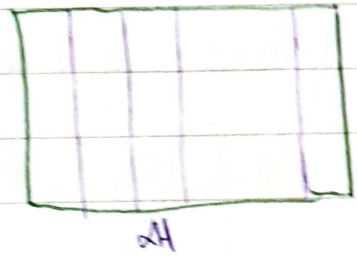
Τετάρτη 31-01-2019

ΘΕΩΡΗΜΑ LAGRANGE

Έστω H υποομάδα μιας ομάδας G πεπερασμένης τάξης. Τότε η τάξη της H είναι διαιρέτης της τάξης της G.

$|H| \,|\, |G|$ $\quad |G| = |H|\,(G:H)$

Ορισμός: Έστω H υποομάδα μιας ομάδας G τότε το πλήθος των αριστερών συμπλόκων ορίζεται δείκτης της H στην G και συμβολίζεται με $(G:H)$



$|G| = |H|\,(G:H)$.

Πόρισμα: Η τάξη ενός στοιχείου μιας πεπερασμένης ομάδας G είναι διαιρέτης της τάξης της ομάδας

$a \in G$ $\quad o(a) = |\langle a\rangle|$ Lagrange $o(a) - |\langle a\rangle| \,|\, |G|$

$\langle a\rangle \leq G$