12/3/2018

ΠΑΡΑΔΕΙΓΜΑ $(S_3, \circ)$ $S_3 = \{ \sigma_0 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix},$

$\sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \sigma_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \sigma_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \sigma_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \}$

Θεωρούμε το $H = \{\sigma_1, \sigma_2\}$. Το H δεν είναι υποομάδα, γιατί $\sigma_1 \circ \sigma_2 = \begin{vmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{vmatrix} = \sigma_4 \in H$, άρα

H όχι κλειστό ως προς $*$.

Αλλά $H_0 = \{\sigma_0\}$ είναι υποομάδα

Επίσης, $H_1 = \{\sigma_0, \sigma_1\}$ είναι υποομάδα, γιατί $\sigma_0 \circ \sigma_1 = \sigma_1 = \sigma_1 \circ \sigma_0$.

$\sigma_1 \circ \sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = \sigma_0 \in H_1$, επίσης $\sigma_0 \circ \sigma_0 = \sigma_0 \in H_1$

Άρα H_1 κλειστή ως προς $\circ$. Εύκολα βλέπουμε H_1 με περιορισμό της πράξης $\circ$ ομάδα

α) $\sigma_0 =$ ταυτοτικό β) πράξη προσεταιριστική και
c) $(\sigma_1)^{-1} = \sigma_1 \in H_1$, $\sigma_0^{-1} = \sigma_0 \in H_1$

Ομοίως, $H_2 = \{\sigma_0, \sigma_2\}$, $H_3 = \{\sigma_0, \sigma_3\}$ $H_4 = \{\sigma_0, \sigma_4, \sigma_5\}$ υποομάδες της G, ενώ το $H_5 = \{\sigma_0, \sigma_4\}$ ΔΕΝ είναι υποομάδα, γιατί $\sigma_4 \circ \sigma_4 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \sigma_5 \in H_5$

άρα H_5 όχι κλειστό.

ΛΗΜΜΑ Έστω $(G, *)$ ομάδα και $H \subseteq G$ υποομάδα

Τότε: i) Έχουμε $e_H = e_G$, όπου $e_G =$ ουδέτερο της ομάδος G και $e_H =$ ουδέτερο της ομάδος H

ii) Έστω $a \in H$. Τότε $a_H^{-1} = a_G^{-1}$, όπου a_G^{-1} το αντίστροφο του a στην G και a_H^{-1} το αντίστροφο του a στην H

ΑΠΟΔΕΙΞΗ

i) Αφού e_H ταυτοτικό της H, $e_H \cdot e_H = e_H$ (1)
Αφού e_G ταυτοτικό της G, $e_G \cdot e_H = e_H$ (2)
Άρα αφού από πρόταση η εξίσωση $x \cdot e_H = e_H$ στην G έχει μοναδική λύση, έχουμε $e_H = e_G$

ii) Τώρα ξέρω $e_H = e_G$. Έχουμε $a \cdot a_H^{-1} = e_G$
$a \cdot a_G^{-1} = e_G$
Αφού η εξίσωση $ax = e_G$ έχει G μοναδική λύση, έχουμε $a_H^{-1} = a_G^{-1}$

ΠΟΡΙΣΜΑ Αν $(G, *)$ ομάδα και $H \subseteq G$ υποομάδα, τότε το ταυτοτικό στοιχείο της G ανήκει στην H. Επιπλέον, αν $a \in H$, τότε το αντίστροφο του a στην G ανήκει στην H.

ΠΑΡΑΔΕΙΓΜΑ: Το $(0, \infty) \subseteq \mathbb{R}$ με πράξη την πρόσθεση δεν είναι υποομάδα του $(\mathbb{R}, +)$ γιατί $0_{\mathbb{R}} \notin (0, \infty)$

ΛΗΜΜΑ Έστω $(G, *)$ ομάδα και $H \neq \emptyset$ υποσύνολο της G Τ.Α.Ε.Ι.:
i) H υποομάδα της G.
ii) Αν $a, b \in H$ τότε $a * b \in H$ και $a^{-1} \in H$
iii) Αν $a, b \in H$ τότε $a * b^{-1} \in H$.

ΑΠΟΔΕΙΞΗ i) ⇒ ii) Φανερά $a * b \in H$ αφού H κλειστή ως προς $*$ σαν υποομάδα. Αφού $a_H^{-1} = a_G^{-1}$ από πρόταση, έχουμε $a^{-1} \in H$.
ii) ⇒ iii) Έστω $a, b \in H$. Από ii) $b^{-1} \in H$ άρα ξανά από ii) $a * b^{-1} \in H$
iii) ⇒ i) **ΙΣΧΥΡΙΣΜΟΣ 1** $e_G \in H$
ΑΠΟΔΕΙΞΗ Αφού H $H \neq \emptyset$ υπάρχει $a \in H$. Άρα από iii) $a * a^{-1} \in H$, άρα $e_G \in H$

ΙΣΧΥΡΙΣΜΟΣ 2 Αν $b \in H$ τότε $b^{-1} \in H$

ΑΠΟΔΕΙΞΗ Για $a = e_G$ που είναι στοιχείο της H από τον ισχυρισμό 1 και για $b \in H$, έχουμε από iii) $a * b^{-1} \in H$, άρα $e_G * b^{-1} \in H$, άρα $b^{-1} \in H$.

ΙΣΧΥΡΙΣΜΟΣ 3 Αν $a, b \in H$ τότε $a * b \in H$

ΑΠΟΔΕΙΞΗ Αφού $b \in H$ από ισχυρισμό 2 $b^{-1} \in H$. Άρα από iii) $a * (b^{-1})^{-1} \in H$, αλλά $(b^{-1})^{-1} = b^{(-1)\cdot(-1)} = b^1 = b$. Άρα $a * b \in H$.

ΙΣΧΥΡΙΣΜΟΣ 4 Το H με τον περιορισμό της $*$ είναι ομάδα.

ΑΠΟΔΕΙΞΗ Προσεταιριστικότητα: Άμεση, γιατί $*$ στην G προσεταιριστικός.

Ουδέτερο Στοιχείο: Από ισχυρισμό 1 $e_G \in H$

Ύπαρξη αντιστρόφου: Από ισχ. 2.

Άρα H υποομάδα της G.

ΕΦΑΡΜΟΓΗ Έστω $n \geq 2$ και $G = GL_n(\mathbb{R}) =$ η ομάδα των αντιστρέψιμων $n \times n$ πινάκων με πράξη τον πολλαπλασιασμό. Θέτουμε

$H_1 = SL_n(\mathbb{R}) = \{A : A$ $n \times n$ πίνακας με στοιχεία στο $\mathbb{R}$ και $\det A = 1\}$

$H_2 = \{A : A$ $n \times n$ πίνακας με στοιχεία στο $\mathbb{R}$ και $\det A \in \{1, -1\}\}$

$H_3 = \{A : A$ $n \times n$ πίνακας με στοιχεία στο $\mathbb{R}$ και υπάρχει $k \in \mathbb{Z}$ ώστε $\det A = 5^k\}$

Θα δείξουμε ότι H_1, H_2, H_3 υποομάδες της G

Φανερά $H_1 \neq \emptyset$, $H_2 \neq \emptyset$, $H_3 \neq \emptyset$, γιατί ο ταυτοτικός $n \times n$ πίνακας είναι στοιχείο και του H_1 και του H_2 και του H_3.

ΑΠΟΔΕΙΞΗ H_1 υποομάδα της G: Δείξαμε $H_1 \neq \emptyset$

Έστω $A, B \in H_1$. Τότε $\det A = 1 = \det B$. Επομένως, αφού $B \cdot B^{-1} = I_n \Rightarrow \det(BB^{-1}) = 1 = \det(B)\cdot\det(B^{-1}) = 1$

$\Rightarrow \det(B^{-1}) = 1$

Άρα $\det(AB^{-1}) = \det A \cdot \det B^{-1} = 1 \cdot 1 = 1$

Άρα $AB^{-1} \in H_1$. Από Λήμμα H_1 υποομάδα της G.

H_2 υποομάδα της G. Δείξαμε $H_2 \neq \emptyset$. Έστω $A, B \in H_1$. Άρα $\det A \in \{1, 9\}$ και $\det B \in \{-1, 1\}$.
Από $BB^{-1} = I_n \Rightarrow \det(BB^{-1}) = \det(I_n) = 1 \Rightarrow$

$\det(B)\cdot\det(B^{-1}) = 1 \Rightarrow \det(B^{-1}) = \dfrac{1}{\det(B)}$.

Έχουμε $\det B^{-1} \in \{-1, 1\}$. Άρα $\det(AB^{-1}) \Rightarrow$

$\det(A)\cdot\det(B^{-1}) \in \{-1, 1\}$, γιατί $\det(A) \in \{1, 1\}$

$\det(B^{-1}) \in \{1, -1\}$

Άρα $AB^{-1} \in H_2$. Από Λήμμα H_2 υποομάδα της G.
- H_3 υποομάδα της G. Παρόμοια Επιχειρήματα (Άσκηση).

ΕΡΩΤΗΜΑ 1 Είναι η τομή υποομάδων υποομάδα;

ΕΡΩΤΗΜΑ 2 Είναι η ένωση υποομάδων υποομάδα;

ΠΡΟΤΑΣΗ Έστω $(G, *)$ ομάδα, I μη κενό σύνολο και H_i, για $i \in I$ υποομάδα της G. Τότε το υποσύνολο $\bigcap_{i \in I} H_i$ είναι υποομάδα της G.

Απόδειξη Θέτουμε $H = \bigcap_{i \in I} H_i$

ΙΣΧΥΡΙΣΜΟΣ 1 $H \neq \emptyset$

ΑΠΟΔΕΙΞΗ Από πρόταση $e_G \in H_i$ για κάθε $i \in I$. Άρα

$e_G \in H$.

ΙΣΧΥΡΙΣΜΟΣ 2 H υποομάδα της G.

ΑΠΟΔΕΙΞΗ Έστω $a, b \in H$. Τότε $a, b \in H_i$ για κάθε $i \in I$. Άρα $a * b^{-1} \in H_i$ για $i \in I$. Άρα $a * b^{-1} \in H$. Συνεπώς αφού από ισχυρ. 1 $H \neq \emptyset$ από το Λήμμα H υποομάδα της G.

ΠΑΡΑΔΕΙΓΜΑ Έστω $G = (\mathbb{Z}, +)$

$H_1 = \{a \in \mathbb{Z} : 2|a\}$ $H_2 = \{a \in \mathbb{Z} : 3|a\}$

ΙΣΧΥΡΙΣΜΟΣ 1 H_1, H_2 υποομάδες της G.

ΑΠΟΔΕΙΞΗ Φανερά $H_1, H_2 \neq \emptyset$

Θ.δ.ο. H_1 υποομάδα. Έστω $a, b \in H_1$. Τότε $2|a$ και $2|b$ άρα $2|a-b$ άρα $a-b \in H_1$. Αφού $H_1 \neq \emptyset$ από Λήμμα H_1 υποομάδα της G. Θ.δ.ο. H_2 υποομάδα. Έστω $a, b \in H_2$. Τότε $3|a$ και $3|b$ άρα $3|a-b$ άρα $a-b \in H_2$. Αφού $H_2 \neq \emptyset$ από Λήμμα H_2 υποομάδα της G.

ΙΣΧΥΡΙΣΜΟΣ 2 $H_1 \cup H_2$ ΟΧΙ υποομάδα της G

ΑΠΟΔΕΙΞΗ Το $2 \in H_1 \cup H_2$, το $3 \in H_1 \cup H_2$. Αλλά $5 \notin H_1 \cup H_2$

γιατί $2 \nmid 5$ και $3 \nmid 5$. Άρα $H_1 \cup H_2$ όχι κλειστό

ως προς +, άρα $H_1 \cup H_2$ ΟΧΙ υποομάδα της G.

ΠΡΟΣΟΧΗ. Έστω $(G, *)$ ομάδα και H μη κενό υποσύνολο της G. Μπορεί να τύχει η H να μην είναι υποομάδα της G, αλλά το H να είναι ομάδα ως προς άλλη πράξη.

ΠΑΡΑΔΕΙΓΜΑ Έστω $G = (\mathbb{R}, +)$ $H = \mathbb{R} \setminus \{0\} \subseteq G$

ΙΣΧΥΡΙΣΜΟΣ 1 H όχι υποομάδα της G

ΑΠΟΔΕΙΞΗ Έχουμε το ουδέτερο της G, δηλ. το $0_{\mathbb{R}}$ δεν ανήκει στην H. Άρα H όχι υποομάδα

ΙΣΧΥΡΙΣΜΟΣ 2. Το H είναι ομάδα ως προς άλλη πράξη του πολλαπλασιασμό.

ΑΠΟΔΕΙΞΗ Το έχουμε δει.

ΚΥΚΛΙΚΕΣ ΥΠΟΟΜΑΔΕΣ ΜΙΑΣ ΟΜΑΔΟΣ

ΟΡΙΣΜΟΣ: Έστω $(G, *)$ ομάδα και $a \in G$ Θέτουμε $\langle a \rangle = \{a^k : k \in \mathbb{Z}\} =$
$\{\ldots, a^{-3}, a^{-2}, a^{-1}, a, a^1, a^2, a^3, \ldots\}$

ΠΡΟΤΑΣΗ a) Το $\langle a \rangle$ είναι υποομάδα της G

b) $a \in \langle a \rangle$

c) Αν H υποομάδα της G με $a \in H$, τότε $\langle a \rangle \subseteq H$. Με άλλα λόγια, $\langle a \rangle$ είναι η μικρότερη υποομάδα της G που περιέχει το a.

Η $\langle a \rangle$ λέγεται ΚΥΚΛΙΚΗ ΥΠΟΟΜΑΔΑ της G που παράγεται από το στοιχείο a. Το a καλείται ΓΕΝΝΗΤΟΡΑΣ της $\langle a \rangle$.

ΑΠΟΔΕΙΞΗ a) Το έχουμε κάνει.

b) Για $n=1$ $a = a^1 \in \langle a \rangle$

c) Έστω H υποομάδα της G με $a \in H$. Αφού

Η υποομάδα $a^{-1} \in H$. Τότε για $n \in \mathbb{Z}$ με $n>0$
$a^n = \underbrace{a * a * \dots * a}_{n\text{-φορές}} \in H$, γιατί Η υποομάδα.

Επίσης, $a^{-n} = (a^{-1})^n = \underbrace{a^{-1} * a^{-1} * \dots * a^{-1}}_{n\text{-φορές}} \in H$, γιατί

Η υποομάδα. Φανερά $a^0 = e \in H$ γιατί Η υποομάδα. Άρα $\langle a \rangle \subseteq H$.

<u>Ορισμός</u>: Έστω G ομάδα. Η G λέγεται ΚΥΚΛΙΚΗ ΟΜΑΔΑ αν υπάρχει $a \in G$ ώστε $G = \langle a \rangle$
(Δηλ. αν υπάρχει $a \in G$ ώστε G είναι ακριβώς οι δυνάμεις του a)

(ΠΡΟΣΟΧΗ)
<u>ΣΥΜΒΟΛΙΣΜΟΣ</u>: Έστω $(G, +)$ αβελιανή ομάδα.

Τότε συμβολίζουμε $na = \begin{cases} \underbrace{a+a+\dots+a}_{n\text{-φορές}}, & \text{αν } n>0 \\ 0_G, & \text{αν } n=0 \\ \underbrace{(-a)+(-a)+(-a)+\dots+(-a)}_{|n|\text{-φορές}}, & n<0 \end{cases}$

(όπου 0_G = ουδέτερο στοιχείο της G)

Με άλλα λόγια: Η ύψωση σε ακέραια δύναμη, όταν η G αβελιανή ομάδα και η πράξη είναι η πρόσθεση συμβολίζεται na (και όχι a^n)

<u>ΠΑΡΑΔΕΙΓΜΑ</u> Αν $G = (\mathbb{Z}, +)$ και $a = b \in \mathbb{Z}$, τότε

για $n \in \mathbb{Z}$ η ύψωση του 6 στην δύναμη n ως προς + συμβολίζεται με $n \cdot 6$ (και όχι 6^n)

<u>ΠΡΟΣΟΧΗ</u> Έστω $(G, *)$ ομάδα και Η μη κενό υποσύνολο του G κλειστό ως προς την $*$. Έπεται ότι Η υποομάδα της G;

Όχι, για παράδειγμα αν $G = (\mathbb{Z}, +)$ και

$H = \{a \in \mathbb{Z} : a > 0\}$ $H \neq \emptyset$ και αν $a, b \in H$ τότε

$a+b \in H$. Αλλά H <u>όχι</u> υποομάδα της G, γιατί $0_{\mathbb{Z}} \notin H$.

<u>ΠΡΟΤΑΣΗ</u> Έστω $(G,*)$ ομάδα και H μη κενό υποσύνολο της G κλειστό ως προς την $*$. Αν το H είναι πεπερασμένο σύνολο, τότε H υποομάδα της G.

<u>ΑΠΟΔΕΙΞΗ</u> <u>ΙΣΧΥΡΙΣΜΟΣ 1</u> $e_G \in H$

<u>ΑΠΟΔΕΙΞΗ</u> Αφού $H \neq \emptyset$ υπάρχει $a \in H$.

Ορίζουμε την απεικόνιση $l_a : H \to H$ με $l_a(h) = a*h$.
Αφού H κλειστό η l_a είναι καλά ορισμένη.
Η l_a είναι 1-1 γιατί $l_a(h) = l_a(h') \Rightarrow$
$a*h = a*h' \Rightarrow h = h'$ από πρόταση.
Αφού H πεπερασμένο και l_a 1-1 έχουμε l_a ΕΠΙ. Άρα υπάρχει $h \in H$ με $l_a(h) = a$, δηλ.
$a*h = a$. Αλλά και $a*e_G = a$.
Αφού G ομάδα $\Rightarrow h = e_G$. Άρα $e_G \in H$

<u>ΙΣΧΥΡΙΣΜΟΣ 2</u> Αν $b \in H$ τότε $b^{-1} \in H$

<u>ΑΠΟΔΕΙΞΗ</u> Από Ισχυρ. 1 $e_G \in H$ και $l_b : H \to H$

ΕΠΙ. Άρα υπάρχει $h \in H$ με $l_b(h) = e_G \Rightarrow b*h = e_G$ (1)
$b*b^{-1} = e_G$ (2)

Αφού G ομάδα (1) κ' (2) $\Rightarrow b^{-1} = h \in H$

<u>ΙΣΧΥΡΙΣΜΟΣ 3</u> H υποομάδα της G
<u>ΑΠΟΔΕΙΞΗ</u> Φανερό από H κλειστό ως προς $(*)$ και Ισχυρ 1 και 2

<u>ΕΦΑΡΜΟΓΗ</u> Έστω $(S_3, \circ)$ με $S_3 = \{\sigma_0, \sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5\}$

Για $i = 0,1,2,3,4,5$ υπολόγισε τις κυκλικές υποομάδες $\langle \sigma_i \rangle$ της S_3.

$\sigma_0 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = e_{S_3}$. Αφού σ_0 ουδέτερο στοιχείο της G, $\langle \sigma_0 \rangle = \{\sigma_0\}$

$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$ Βλέπουμε $\sigma_1^2 = \sigma_1 \circ \sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$

$= \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = \sigma_0$.

<u>ΙΣΧΥΡΙΣΜΟΣ</u> Θέτουμε $H_1 = \{\sigma_0, \sigma_1\}$. Τότε H_1 υποομάδα της G και μάλιστα $H_1 = \langle \sigma_1 \rangle$

<u>ΑΠΟΔΕΙΞΗ</u> Το H_1 είναι υποομάδα της G από το Λήμμα, γιατί είναι μη κενό, πεπερασμένο και κλειστό ως προς την πράξη γιατί $\sigma_0 \circ \sigma_0 = \sigma_0$, $\sigma_0 \circ \sigma_1 = \sigma_1 \circ \sigma_0 = \sigma_1$
$\sigma_1 \circ \sigma_1 = \sigma_0$

<u>ΙΣΧΥΡΙΣΜΟΣ</u> $\langle \sigma_1 \rangle \subseteq H_1$

ΙΣΧΥΡ. 1 $\langle \sigma_1 \rangle \subseteq H_1$

ΑΠΟΔ. Αφού H_1 υποομάδα της G, $\sigma_1 \in H_1$ από πρόταση $\langle \sigma_1 \rangle \subseteq H$.

ΙΣΧΥΡ. 2 $H_1 \subseteq \langle \sigma_1 \rangle$

Πράγματι, $H_1 = \{\sigma_0, \sigma_1\}$ και $\sigma_0 \in \langle \sigma_1 \rangle$ αφού είναι το ουδέτερο και $\sigma_1 \in \langle \sigma_1 \rangle$

Από Ισχυρ. 1 και 2 έπεται $H_1 = \langle \sigma_1 \rangle$, δηλ. $\langle \sigma_1 \rangle = \{\sigma_0, \sigma_1\}$. Έχουμε $\sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$. Παρατηρούμε

$\sigma_2 \circ \sigma_2 = \sigma_0$. Όπως προηγουμένως έπεται $\langle \sigma_2 \rangle = \{\sigma_0, \sigma_2\}$

Έχουμε $\sigma_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$ Παρατηρούμε $\sigma_3 \circ \sigma_3 = \sigma_0$

Όπως προηγουμένως έπεται $\langle \sigma_3 \rangle = \{\sigma_0, \sigma_3\}$

Έχουμε $\sigma_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ $\sigma_4 \circ \sigma_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} =$

$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \sigma_5$

ΙΣΧΥΡΙΣΜΟΣ. Θέτουμε $H_4 = \{\sigma_0, \sigma_4, \sigma_5\}$. Τότε H_4 υποομάδα της G και $H_4 = \langle \sigma_4 \rangle$

ΑΠΟΔΕΙΞΗ Αφού H_4 μη κενό πεπερασμένο υποσύνολο της G, από την πρόταση για να δείξουμε ότι H_4 υποομάδα της G αρκεί να δείξουμε H_4 κλειστό ως προς την πράξη. Πράγματι, $\sigma_0 \circ \sigma_0 = \sigma_0$,

$\sigma_0 \circ \sigma_4 = \sigma_4 \circ \sigma_0 = \sigma_4$, $\sigma_0 \circ \sigma_5 = \sigma_5 \circ \sigma_0 = \sigma_5$

$\sigma_4 \circ \sigma_4 = \sigma_5$

$\sigma_4 \circ \sigma_5 = \sigma_0$ $\sigma_5 \circ \sigma_4 = \sigma_0$

$\sigma_5 \circ \sigma_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \sigma_4$, άρα H_4 κλειστό

άρα H_4 υποομάδα της G.

ΙΣΧΥΡΙΣΜΟΣ 3 $H_4 = \{\sigma_0, \sigma_4, \sigma_5\} \subseteq \langle \sigma_4 \rangle$

Πράγματι $\sigma_0 = \sigma_4^0$, $\sigma_4 = \sigma_4^1$, $\sigma_5 = \sigma_4^2 = \sigma_4 \circ \sigma_4$

ΙΣΧΥΡΙΣΜΟΣ 4 $\langle \sigma_4 \rangle \subseteq H_4$

Πράγματι, αφού H_4 υποομάδα της G και $\sigma_4 \in H_4$ έχουμε $\langle \sigma_4 \rangle \subseteq H_4$

Από ισχυρ. 1 και 2 έχουμε $H_4 = \langle \sigma_4 \rangle$

ΤΕΛΟΣ με παρόμοια απόδειξη $\langle \sigma_5 \rangle = H_4 = \{\sigma_0, \sigma_4, \sigma_5\}$

Έτσι υπολογίσαμε όλες τις κυκλικές υποομάδες της S_3.