Άλγεβρα Ι - Λύσεις Εργασίας 2

ΚΥΚΛΙΚΕΣ ΟΜΑΔΕΣ

Ασκήσεις βιβλίου Fraleigh σελ. 71

Άσκηση 13 Κατάρχήν κάθε ομάδα είναι υποομάδα του εαυτού της, δηλαδή $G_i \leq G_i$, $i = 1, \dots 9$. Επιπλέον ισχύουν οι παρακάτω σχέσεις μεταξύ των ομάδων του καταλόγου: $G_2 = (12\mathbb{Z}, +) < G_8 = (6\mathbb{Z}, +) < G_7 = (3\mathbb{Z}, +) < G_1 = (\mathbb{Z}, +) < G_4 = (\mathbb{R}, +)$, $G_6 = (\{\pi^n | n \in \mathbb{Z}\}, \cdot) < G_5 = (\mathbb{R}^+, \cdot)$ και $G_9 = (\{6^n | n \in \mathbb{Z}\}, \cdot) < G_3 = (\mathbb{Q}^+, \cdot) < G_5 = (\mathbb{R}^+, \cdot)$.

Άσκηση 14

α) Η ομάδα $(25\mathbb{Z}, +)$ αποτελείται από όλα τα πολλαπλάσια του 25, θετικά, αρνητικά και μηδέν, δηλαδή $(25\mathbb{Z}, +) = \{\dots, -50, -25, 0, 25, 50, \dots\}$.

β) $(\{(\frac{1}{2})^n | n \in \mathbb{Z}\}, \cdot) = \{\dots, \frac{1}{4} = (\frac{1}{2})^2, \frac{1}{2} = (\frac{1}{2})^1, 1 = (\frac{1}{2})^0, 2 = (\frac{1}{2})^{-1}, 4 = (\frac{1}{2})^{-2}, \dots\}$

γ) $(\{\pi^n | n \in \mathbb{Z}\}, \cdot)\{\dots, \frac{1}{\pi^2} = \pi^{-2}, \frac{1}{\pi} = \pi^{-1}, 1 = \pi^0, \pi = \pi^1, \pi^2, \dots\}$.

Άσκηση 16 Κάνοντας τις πράξεις παρατηρούμε ότι: $< 3 >= \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\} = \mathbb{Z}_4$, δηλαδή η υποομάδα της $\mathbb{Z}_4$ που παράγεται από το 3 ταυτίζεται με την $\mathbb{Z}_4$, άρα θα έχει τάξη $|\mathbb{Z}_4| = 4$.(Ένας άλλος τρόπος είναι να σκεφτούμε ότι $(4, 3) = 1$ άρα 3 επίσης γεννήτορας του $\mathbb{Z}_4$, άρα $| < 3 > | = |\mathbb{Z}_4| = 4$ ή χρησιμοποιώντας το Θεώρημα Lagrange έχουμε $| < 3 > | = \frac{|\mathbb{Z}_4|}{(4,3)} = 4$.)

Άσκηση 20 Για την ομάδα $(U_8, \cdot)$ έχουμε $U_8 = \langle \cos\frac{2\pi}{8} + i\sin\frac{2\pi}{8} \rangle$. Επίσης $\cos\frac{3\pi}{2} + i\sin\frac{3\pi}{2} = (\cos\frac{2\pi}{8} + i\sin\frac{2\pi}{8})^6 \in U_8$, και έχουμε $(\cos\frac{3\pi}{2} + i\sin\frac{3\pi}{2})^2 = \cos\pi + i\sin\pi$, $(\cos\frac{3\pi}{2} + i\sin\frac{3\pi}{2})^3 = \cos\frac{\pi}{2} + i\sin\frac{\pi}{2}$, και $(\cos\frac{3\pi}{2} + i\sin\frac{3\pi}{2})^4 = \cos 2\pi + i\sin 2\pi$. Άρα η τάξη της υποομάδας είναι $|\langle \cos\frac{3\pi}{2} + i\sin\frac{3\pi}{2} \rangle| = 4$. Ένας άλλος τρόπος είναι να παρατηρήσουμε ότι $\langle \cos\frac{3\pi}{2} + i\sin\frac{3\pi}{2} \rangle = \langle (\cos\frac{2\pi}{8} + i\sin\frac{2\pi}{8})^6 \rangle$ και τότε από γνωστή Πρόταση έχουμε ότι για την τάξη της υποομάδας ισχύει $|\langle \cos\frac{3\pi}{2} + i\sin\frac{3\pi}{2} \rangle| = \frac{|U_8|}{(8,6)} = 4$

Άσκηση 22 Έστω

$$A = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix} \tag{1}$$

τότε $A^2 = I_4$. Άρα $\langle A \rangle = \{I_4, A\}$ και $|\langle A \rangle| = 2$.

Ασκήσεις βιβλίου Fraleigh σελ. 107-109

<u>Άσκηση 15</u> Έστω $G = \langle a \rangle$ με $G = 60$. Τότε, από γνωστό Θεώρημα, κάθε στοιχείο $a^r \in G$ παράγει μία υποομάδα $\langle a^r \rangle$ της G με τάξη $|\langle a^r \rangle| = \frac{|G|}{(|G|, r)}$. Αν $(|G|, r) = 1$ τότε $|\langle a^r \rangle| = |G|$ και άρα $\langle a^r \rangle = G$, δηλαδή το a^r είναι γεννήτορας της G. Άρα οι δυνατές τιμές για το r είναι όσες και το πλήθος των αριθμών πρώτων προς το 60 που είναι μικρότεροι από το 60. Αυτοί είναι οι: $1, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 49, 53, 59$, δηλαδή αντιστοιχούν σε συνολικά 16 γεννήτορες.

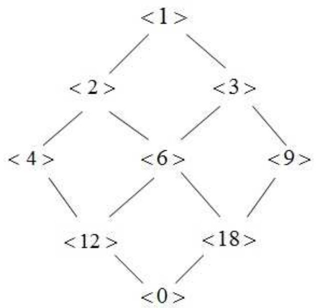
<u>Άσκηση 18</u> Είναι $\langle i \rangle = \{1, -1, i, -i\}$, δηλαδή $|\langle i \rangle| = 4$.

<u>Άσκηση 19</u> Είναι $\frac{1+i}{\sqrt{2}} = \frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2} i = \cos\frac{\pi}{4} + i \sin\frac{\pi}{4} = e^{i\frac{\pi}{4}} = e^{i\frac{2\pi}{8}}$. Άρα $(\frac{1+i}{\sqrt{2}})^8 = (e^{i\frac{2\pi}{8}})^8 = e^{i8(\frac{2\pi}{8})} = e^{i2\pi} = 1$, ενώ $k\frac{2\pi}{8} < 2\pi$, $\forall k < 8$, δηλαδή $|\langle \frac{1+i}{2} \rangle| = 8$.

<u>Άσκηση 20</u> Παρατηρούμε ότι $1 + i = \sqrt{2}(\frac{1+i}{\sqrt{2}}) = \sqrt{2}(\cos\frac{\pi}{4} + i \sin\frac{\pi}{4}) = \sqrt{2}e^{i\frac{\pi}{4}} = \sqrt{2}e^{i\frac{2\pi}{8}}$. Αν είχε πεπερασμένη τάξη, τότε θα υπήρχε $n \neq 0 \in \mathbb{N}$ τέτοιο ώστε $(1+i)^n = 1 \Leftrightarrow (\sqrt{2}e^{i\frac{2\pi}{8}})^n = 1 \Leftrightarrow (\sqrt{2})^n e^{i\frac{2n\pi}{8}} = 1$. Όμως τότε για το μέτρο του θα ισχύει $|(1+i)^n| = |1| \Leftrightarrow \sqrt{2}^n = 1$, άτοπο.

<u>Άσκηση 22</u> Κατ' αρχήν έχουμε ότι τα στοιχεία $\bar{1}, \bar{5}, \bar{7}, \bar{11}, \bar{13}, \bar{17}, \bar{19}, \bar{23}, \bar{25}, \bar{29}, \bar{31}, \bar{35}$ είναι όλα γεννήτορες της $\mathbb{Z}_{36}$, αφού είναι όλα πρώτοι ως προς 36. Εξετάζουμε τα υπόλοιπα στοιχεία:

• Για το $\bar{2}$ έχουμε ότι $| < \bar{2} > | = 18$ και έχει ως γεννήτορες τα στοιχεία της μορφής $h\bar{2}$ όπου h πρώτος ως προς 18, δηλαδή $h = 1, 5, 7, 11, 13, 17$ άρα τα $h\bar{2} = \bar{2}, \bar{10}, \bar{14}, \bar{22}, \bar{26}, \bar{34}$. Εξετάζουμε τα υπόλοιπα στοιχεία που ανήκουν στην $< \bar{2} >$ αλλά δεν είναι γεννήτορές της (δηλαδή θα είναι γεννήτορες μίας υποομάδας της $< \bar{2} >$):



Σχήμα 1: Το δικτυωτό διάγραμμα της $\mathbb{Z}_{36}$

$i)$ Για το $\bar{4}$ έχουμε ότι η $<\bar{4}>=\{\bar{0},\bar{4},\bar{8},\bar{12},\bar{16},\bar{20},\bar{24},\bar{28},\bar{32}\}$ έχει τάξη 9 και έχει ως γεννήτορες τα στοιχεία της μορφής $h'\bar{4}$ όπου h' πρώτος ως προς 9, δηλαδή $h'=1,2,4,5,7,8$ άρα τα $h'\bar{4}=\bar{4},\bar{8},\bar{16},\bar{20},\bar{28},\bar{32}$. Εξετάζουμε τα υπόλοιπα στοιχεία που ανήκουν στην $<4>$ αλλά δεν είναι γεννήτορές της (δηλαδή θα είναι γεννήτορες μίας υποομάδας της $<4>$):

$ia)$ Για το $\bar{12}$ είναι $<\bar{12}>=\{\bar{0},\bar{12},\bar{24}\}$ έχει τάξη 3 και έχει ως γεννήτορες τα στοιχεία της μορφής $h''\bar{12}$ όπου h'' πρώτος ως προς 3, δηλαδή $h''=1,2$ άρα τα $h''\bar{12}=\bar{12},\bar{24}$.

$ii)$ Για το $\bar{6}$ η $<\bar{6}>=\{\bar{0},\bar{6},\bar{12},\bar{18},\bar{24},\bar{30}\}$ έχει τάξη 6 και έχει ως γεννήτορες τα στοιχεία της μορφής $h''\bar{6}$ όπου h'' πρώτος ως προς 6, δηλαδή $h''=1,5$ άρα τα $h''\bar{6}=\bar{6},\bar{30}$. Εξετάζουμε τα υπόλοιπα στοιχεία που ανήκουν στην $<\bar{6}>$ αλλά δεν είναι γεννήτορές της (δηλαδή θα είναι γεννήτορες μίας υποομάδας της $<\bar{6}>$):

$iia)$ Για το $\bar{18}$ είναι $<\bar{18}>=\{\bar{0},\bar{18}\}$.

• Για το $\bar{3}$ είναι $<\bar{3}>=\{\bar{0},\bar{3},\bar{6},\bar{9},\bar{12},\bar{15},\bar{18},\bar{21},\bar{24},\bar{27},\bar{30},\bar{33}\}$ που έχει τάξη 12 και έχει ως γεννήτορες τα στοιχεία της μορφής $u\bar{3}$ όπου u πρώτα ως προς 12, δηλαδή $u=1,5,7,11$, άρα τα $u\bar{3}=\bar{3},\bar{15},\bar{21},\bar{33}$.Εξετάζουμε τα υπόλοιπα στοιχεία που ανήκουν στην $<\bar{3}>$ αλλά δεν είναι γεννήτορές της (δηλαδή θα είναι γεννήτορες μίας υποομάδας της $<3>$):

$i)$ Για το $\bar{9}$ είναι $<\bar{9}>=\{\bar{0},\bar{9},\bar{18},\bar{27}\}$ τάξης 4 και έχει ως γεννήτορες τα στοιχεία της μορφής $h'''\bar{9}$ όπου h''' πρώτος ως προς 9, δηλαδή $h'''=1,3$, άρα τα $h'''\bar{9}=\bar{9},\bar{27}$.

<u>Άσκηση 37</u> Η ομάδα U_8 είναι κυκλική με γεννήτορα το $\rho=\cos\frac{\pi}{4}+i\sin\frac{\pi}{4}=e^{i\frac{\pi}{4}}=$

$e^{i\frac{2\pi}{8}}$ με $\rho^8 = 1$ $|U_8| = |<\rho>| = 8$. Κάθε άλλο στοιχείο v της U_8 θα είναι της μορφής $v = \rho^k = e^{i\frac{2k\pi}{8}}$, $k < 8, k \in \mathbb{N}$ αφού $v \in <\rho>$ και για να είναι γεννήτορας θα πρέπει να έχει τάξη m τέτοια ώστε $(m, 8) = 1$. Άρα οι δυνατές τιμές είναι $m = 1, 3, 5, 7$, δηλαδή τα στοιχεία $\rho = \frac{1+i}{\sqrt{2}}$, $\rho^3 = \frac{-1+i}{\sqrt{2}}$, $\rho^5 = \frac{-1-i}{\sqrt{2}}$ και $\rho^7 = \frac{1-i}{\sqrt{2}}$.

<u>Άσκηση 41</u> Τέτοια παραδείγματα είναι τα:

• Η S_3, η οποία δεν είναι κυκλική, όμως κάθε υποομάδα της είναι. Πιο, συγκεκριμένα, οι μή τετριμμένες υποομάδες της είναι οι $\{\rho_0, \rho_1, \rho_2\} =<\rho_1>=<\rho_2>$, $\{\rho_0, \mu_1\} =<\mu_1>$, $\{\rho_0, \mu_2\} =<\mu_2>$, $\{\rho_0, \mu_3\} =<\mu_3>$.

• Η ομάδα του Klein, $V_4 = \mathbb{Z}_2 \times \mathbb{Z}_2$.

• Η ομάδα στρέψης $T = \{z \in U : ord(z) < \infty\} = \{z = e^{i2\pi q} | q \in \mathbb{Q}\}$.

<u>Άσκηση 46</u> Αφού $m|n$, θα είναι $n = a \cdot m$ για κάποιον $a \in \mathbb{N}$. Προφανώς το e είναι μία λύση της $x^m = e$. Έστω g ο γεννήτορας της G, δηλαδή $G =<g>$ οπότε είναι $g^n = e \Leftrightarrow g^{ma} = e \Leftrightarrow (g^a)^m = e$, άρα το g^a είναι μία λύση της $x^m = e$. Παρατηρούμε ότι κάθε στοιχείο της μορφής $(g^a)^k$ με $k \in \mathbb{N}$ θα είναι επίσης λύση της $x^m = e$, αφού $((g^a)^k)^m = (g^{am})^k = e^k = e$. Μάλιστα, κάθε λύση της $x^m = e$ πρέπει να είναι αυτής της μορφής, δηλαδή πρέπει να είναι μία δύναμη του g^a διότι εάν ήταν ένα στοιχείο $g^b \in G =<g>, b \neq ka$ λύση της $x^m = e$ τότε θα είχαμε $(g^b)^m = e = (g^a)^m \Leftrightarrow g^{bm} = g^{am} \Leftrightarrow g^{bm} = g^n \Rightarrow bm \equiv n \mod n \Leftrightarrow bm \equiv 0 \mod n \Leftrightarrow bm \equiv 0 \mod am \Leftrightarrow b \equiv 0 \mod a \Leftrightarrow b = \lambda a$ $\lambda \in \mathbb{N}$, άτοπο. Όλες οι διαφορετικές λύσεις της $x^m = e$ είναι τα στοιχεία $g^a, (g^a)^2 = g^{2a}, g^{3a}, \ldots, g^{(m-1)a}, g^{ma} = g^n = e$, αφού για κάθε $k > m$, το στοιχείο $(g^a)^k = g^{ak} = g^{ak \mod n} = g^{a(k \mod m)}$ θα είναι ένα από τα m στοιχεία $g^a, g^{2a}, g^{3a}, \ldots, g^{(m-1)a}, e$.

ΣΥΜΠΛΟΚΑ – ΤΟ ΘΕΩΡΗΜΑ LAGRANGE

<u>Άσκηση 3</u>

α) Σύμφωνα με τον συμβολισμό του βιβλίου του Fraleigh $H = \langle e, \mu_1 \rangle$. Τα αριστερά και δεξιά σύμπλοκα της H στην D_4 είναι τα:

$\rho_0 H = H\rho_0 = \mu_1 H = H\mu_1 = H$

$\rho_1 H = \{\rho_1, \delta_1\} \neq H\rho_1 = \{\rho_1, \delta_2\}$

$\rho_2 H = \{\rho_2, \mu_2\} = H\rho_2$

$\rho_3 H = \{\rho_3, \delta_2\} \neq H\rho_3 = \{\rho_3, \delta_1\}$, άρα η H δεν είναι κανονική υποομάδα.

$\mu_2 H = \{\mu_2, \rho_2\} = H\mu_2$

$\delta_1 H = \{\delta_1, \rho_1\} \neq H\delta_1 = \{\delta_1, \rho_3\}$

$\delta_2 H = \{\delta_2, \rho_3\} \neq H\delta_2 = \{\delta_2, \rho_1\}$.

β) Η D_n εκτός από τις n στροφές έχει άλλα n στοιχεία, έστω $\delta_i, i = 1, \ldots, n$, τα οποία αντιστοιχούν σε ανακλάσεις ως προς τις μεσοκαθέτους των πλευρών του κανονικού n-γώνου για n περιττό και σε ανακλάσεις ως προς τις μεσοκαθέτους και ως προς τις διαγωνίους για n άρτιο. Επιπλέον, παρατηρούμε ότι $\delta_i r_j = \delta_j$, δηλαδή η σύνθεση ανάκλασης με στροφή μας δίνει πάλι ανάκλαση. Άρα αφού κάθε σύμπλοκο $\delta_i N$ θα έχει n στοιχεία, και αφού αυτά τα στοιχεία ανήκουν στο σύνολο των ανακλάσεων, οι οποίες έχουν πλήθος n, τα στοιχεία του συμπλόκου $\delta_i N$ θα είναι ακριβώς τα στοιχεία του συνόλου των ανακλάσεων. Ομοίως, έχουμε ότι η σύνθεση στροφής με ανάκλαση μας δίνει πάλι ανάκλαση, άρα τα στοιχεία του συμπλόκου $N\delta_i$ θα είναι ακριβώς το σύνολο των ανακλάσεων, άρα $\delta_i N = N\delta_i \ \forall i = 1, \ldots, n$.

<u>Άσκηση 4</u> Το πλήθος των αριστερών συμπλόκων της H στην G είναι ίσο με $\frac{|G|}{|H|} = \frac{n}{n/2} = 2$. Το ένα σύμπλοκο είναι το $H = eH = He = hH = Hh, \forall h \in H$. Αφού τα αριστερά (αντίστοιχα δεξιά) σύμπλοκα διαμερίζουν την G, το άλλο αριστερό (αντίστοιχα δεξιό) σύμπλοκο θα είναι το $G \setminus H$. Επίσης για κάθε $g \in G \setminus H$ θα είναι $gH \neq H \Rightarrow gH = G \setminus H$ (διαφορετικά θα υπήρχαν $h, h' \in H$ τέτοια ώστε $gh = h' \Leftrightarrow g = h'' \in H$, άτοπο). Ομοίως, για κάθε $g \in G \setminus H$ θα είναι $Hg \neq H \Rightarrow Hg = G \setminus H$. Άρα δείξαμε ότι $gH = Hg$ για κάθε $g \in G$.

Ασκήσεις βιβλίου Fraleigh σελ. 117-119

<u>Άσκηση 2</u> Οι ομάδες $2\mathbb{Z}$ και $4\mathbb{Z}$ αποτελούνται από όλα τα ακέραια πολλαπλάσια του 2 και του 4 αντίστοιχα. Αν $x \in 4\mathbb{Z}$, τότε $x + 4\mathbb{Z} = 4\mathbb{Z}$. Επίσης $2 \notin 4\mathbb{Z}$ και έχουμε $2 + 4\mathbb{Z} = \{\ldots, -6, -2, 2, 6, 10, \ldots\}$. Τέλος παρατηρούμε ότι $4\mathbb{Z} \cup (2 + 4\mathbb{Z}) = 2\mathbb{Z}$. Δηλαδή το μόνο μή τετριμμένο σύμπλοκο είναι το $2 + 4\mathbb{Z}$.

<u>Άσκηση 4</u> Είναι $< 4 >= \{0, 4, 8\}$. Το πλήθος των συμπλόκων της $< 4 >$ στην $\mathbb{Z}_{12}$ είναι $\frac{|\mathbb{Z}_{12}|}{|<4>|} = 4$. Τα 4 σύμπλοκα $0+ < 4 >=< 4 >$, $1 + \langle 4 \rangle = \{1, 5, 9\}$,

$2+\langle 4\rangle=\{2,6,10\}$, $3+\langle 4\rangle=\{3,7,11\}$ είναι όλα διαφορετικά μεταξύ τους και άρα αυτά είναι όλα τα σύμπλοκα της $<4>$ στην $\mathbb{Z}_{12}$.

Άσκηση 15

α) Σωστό, αφού αριστερά και δεξιά σύμπλοκα ορίζονται για οποιαδήποτε υποομάδα H μίας ομάδας G.

β) Σωστό, αφού κάθε αριστερό σύμπλοκο της H στην G έχει $|H|$ στοιχεία και η αντιστοίχιση των στοιχείων της G σε σύμπλοκα διαμερίζει την G. Δηλαδή ισχύει ότι $[G:H]=\frac{|G|}{|H|}\Leftrightarrow\frac{|H|}{[G:H]}=|H|$ όπου $[G:H]$ το πλήθος των συμπλόκων της H στην G.

γ) Σωστό, αφού κάθε ομάδα με τάξη πρώτο αριθμό είναι κυκλική, και κάθε κυκλική ομάδα είναι και αβελιανή.

δ) Λάθος, π.χ. η ομάδα U όλων των σημείων πάνω στον τριγωνομετρικό κύκλο με πράξη τον πολλαπλασιασμό μιγαδικών αριθμών που έχει άπειρη τάξη, έχει υποομάδα την U_n που αποτελείται από τις n-οστές ρίζες της μονάδας, που έχει τάξη n και αντιστοιχεί στις κορυφές ενός κανονικού n-γώνου εγγεγραμμένου στον μοναδιαίο κύκλο. Τότε για κάθε στοιχείο $z\in U\setminus U_n$ ορίζεται το σύμπλοκο zU_n που αντιστοιχεί στην στροφή του εγγεγραμμένου n-γώνου κατά γωνία $Arg(z)$.

ε) Σωστό, αφού για κάθε υποομάδα H μίας ομάδας G, ο πολλαπλασιασμός κάθε στοιχείου της H με το e παράγει το σύμπλοκο $eH=H$.

στ) Λάθος, για παράδειγμα δείτε το α).

ζ) Σωστό, αφού $[S_n:A_n]=\frac{|S_n|}{|A_n|}=\frac{n!}{n!/2}=2$.

η) Σωστό, αφού μας δίνει την δυνατότητα να ελέγξουμε εάν μία ομάδα H είναι υποομάδα μίας ομάδας G γνωρίζοντας τις τάξεις τους και μετρά το πλήθος των συμπλόκων της H στην G. Επίσης από το Θεώρημα Lagrange προκύπτει ότι κάθε ομάδα με τάξη πρώτο αριθμό είναι κυκλική και ότι η τάξη ενός στοιχείου μίας πεπερασμένης ομάδας διαιρεί την τάξη της ομάδας.

θ) Λάθος, π.χ. η ομάδα V_4 δέν έχει στοιχείο τάξης 4.

ι) Σωστό, διότι αν $G=<g>$ και $|<g>|=n$. Τότε για κάθε $m|n$ θα υπάρχει a τέτοιο ώστε $n=ma$ και θα είναι $g^n=e\Leftrightarrow g^{ma}=e\Leftrightarrow(g^a)^m=e$, δηλαδή $|<g^a>|=m$.

Άσκηση 16 Αδύνατον, αφού η ομάδα είναι αβελιανή και άρα για κάθε υποομάδα H της G και κάθε $g \in G$ θα είναι $gH = \{gh|h \in H\} = \{hg|h \in H\} = Hg$, δηλαδή κάθε αρισερό σύμπλοκο ταυτίζεται με το δεξί.

Άσκηση 17 Η υποομάδα $G \leq G$ διαμερίζει την G σε ένα μόνο σύμπλοκο το G.

Άσκηση 18 Αν $|G| = 6$ και για μία υποομάδα $H \leq G$ είναι $[G : H] = 6$, τότε $[G : H] = \frac{|G|}{|H|} \Leftrightarrow |H| = 1$. Αφού H υποομάδα, $e \in H$ και άρα $H = \{e\}$, δηλαδή είναι τετριμμένη υποομάδα.

Άσκηση 20 Αν $|G| = 6$ και για μία $H \leq G$ είναι $[G : H] = 4$, τότε θα είναι $[G : H] = \frac{|G|}{|H|} \Leftrightarrow |H| = \frac{|G|}{[G:H]} = \frac{6}{4}$, το οποίο είναι αδύνατον.

Άσκηση 25 Έστω $G = S_3$ και $H = \{\rho_0, \mu_1\}$ μία υποομάδα της. Τότε για $a = \mu_1, b = \mu_3$ είναι $aH = bH$, αλλά $Ha \neq Hb$.

Άσκηση 26 Αν $Ha = Hb$, τότε υπάρχουν $h \in H$ και $h' \in H$ τέτοια ώστε $ha = h'b \Leftrightarrow h'^{-1}ha = b$, δηλαδή υπάρχει $h'' \in H$ τέτοιο ώστε $h''a = b \Leftrightarrow b \in Ha$. (Ένας άλλος τρόπος είναι να παρατηρήσουμε ότι αφού H υποομάδα της G και $e \in H$ άρα $b = e \cdot b \in Hb = Ha \Rightarrow b \in Ha$.)

Άσκηση 27 Αν είναι $aH = bH$, τότε για κάθε $h \in H$ υπάρχει $h' \in H$ τέτοιο ώστε $ah = bh'$. Έχουμε ότι $e = (ah)(ah)^{-1} = (bh')(ah)^{-1}$ άρα $(ah)^{-1} = (bh')^{-1} \Leftrightarrow h^{-1}a^{-1} = h'^{-1}b^{-1}$ και αφού $H \leq G$, έπεται ότι για κάθε $h \in H \Rightarrow h^{-1} \in H$ και άρα $h'^{-1} \in H$ τέτοιο ώστε $h^{-1}a^{-1} = h'^{-1}b^{-1}$ δηλαδή $Ha^{-1} = Hb^{-1}$. Τέλος παρατηρούμε ότι όταν το h διατρέχει την H, τότε h^{-1} επίσης θα διατρέχει ολόκληρη την H. Άρα δείξαμε ότι $aH = bH \Rightarrow Ha^{-1} = Hb^{-1}$.
(Παρατηρείστε ότι αντίστροφα, αν $Ha^{-1} = Hb^{-1}$ τότε για κάθε $h \in H$ υπάρχει $h' \in H$ τέτοιο ώστε $ha^{-1} = h'b^{-1} \Leftrightarrow (ah^{-1})^{-1} = (bh'^{-1})^{-1}$, δηλαδή $ah^{-1} = bh'^{-1}$ και αφού κάθε στοιχείο της H έχει μοναδικό αντίστροφο στην H, έπεται $Ha = Hb$. Άρα συνολικά έχουμε δείξει ότι: $aH = bH \Leftrightarrow Ha^{-1} = Hb^{-1}$.)

Άσκηση 28 Λάθος, αφού στην D_4 για $H = \{\rho_0, \mu_1\}$ έχουμε $\rho_1 H = \delta_1 H = \{\rho_1, \delta_1\}$. Όμως $\rho_1^2 = \rho_2, \delta_1^2 = \rho_0$ και $\rho_1^2 H = \{\rho_2, \mu_2\} \neq \{\rho, \mu_1\} = \delta_1^2 H$ Η εκφώνηση ισχύει μόνο στην περίπτωση που $H \rhd G$. Οπότε το γινόμενο συμπλόκων είναι καλά ορισμένο.

Άσκηση 29 Θα πρέπει να ισχύει $|H| \mid |G|$ δηλαδή είτε $|H| = p$ ή $|H| = q$, δηλαδή η H έχει τάξη πρώτο αριθμό, άρα είναι κυκλική.

Άσκηση 30 Έστω η απεικόνιση ϕ από το σύνολο των αριστερών συμπλόκων στο σύνολο των δεξιών συμπλόκων, η οποία ορίζεται ως $\phi(aH) = Ha^{-1}$, $\forall a \in G$. Τότε για το δεξιό σύμπλοκο Hb, $b \in G$, υπάρχει το αριστερό σύμπλοκο $H((b^{-1})^{-1})$, τέτοιο ώστε $\phi(b^{-1}H) = Hb$. Δηλαδή η απεικόνιση ϕ είναι επί. Επίσης έχουμε $\phi(aH) = \phi(bH) \Leftrightarrow Ha^{-1} = Hb^{-1} \Leftrightarrow aH = bH$ (δείτε Άσκηση 27), δηλαδή η απεικόνιση ϕ είναι και '$1-1$'.

Άσκηση 38

α) Είναι $a \sim a \Leftrightarrow a = eae$, $e \in H$ $e \in K$ δηλαδή ισχύει η ανκλαστική ιδιότητα.

Είναι $a \sim b \Leftrightarrow a = hbk \Leftrightarrow b = h^{-1}ak^{-1} \Leftrightarrow \in HaK$, δηλαδή ισχύει η συμμετρική ιδιότητα.

Αν $a \sim b$ και $b \sim c \Leftrightarrow b = h'ck'$ είναι $a = hbk = hh'ck'k \in HaK$ δηλαδή και $a \sim c$, άρα ισχύει η μεταβατική ιδιότητα.

β) Έστω $a \in G$, τότε η κλάση ισοδυναμίας που περιέχει το a είναι το σύνολο $\{b \in G | b = hak, h \in H, k \in K\} = HaK$. Παρατηρούμε ότι $HaK = (Ha)K = H(aK)$ δηλαδή είναι το δεξιό σύμπλοκο του a ως προς την H πολλαπλασιασμένο από δεξιά με στοιχεία της K ή το αριστερό σύμπλοκο του a ως προς K πολλαπλασιασμένο από αριστερά με στοιχεία της H.

Άσκηση 40 Έστω $G = \langle a \rangle$ τότε για κάθε $d|n$ υπάρχει $k < n$ τέτοιο ώστε $n = kd$, δηλαδή υπάρχει στοιχείο a^k της G που παράγει μία υποομάδα με τάξη $| < a^k > | = d$. Άρα για κάθε διαιρέτη d της τάξης της G υπάρχει μία υποομάδα τάξης d. Έστω ότι υπάρχει και άλλη υποομάδα της G τάξης d. Αφού G κυκλική, κάθε υποομάδα της θα είναι κυκλική, άρα έστω ότι υπάρχει $a^l \in G, l \neq k, l < n$ τέτοιο ώστε $| < a^l > | = d$. Τότε θα είναι $ld = un$ για κάποιο $u \in \mathbb{N}$, δηλαδή $ld = ukd \Leftrightarrow l = uk$. Άρα $a^l = a^{uk} = (a^k)^u \in < a^k >$ άρα $< a^l > \leq < a^k >$. Υποθέσαμε όμως ότι $| < a^l > | = | < a^k > |$, άρα θα είναι $< a^l > = < a^k >$. Δηλαδή δεν υπάρχει άλλη υποομάδα της G τάξης d. Τέλος, αφού η τάξη μίας υποομάδας της G πρέπει να διαιρεί την τάξη της G, οι υποομάδες τάξης d, με $d||G|$, είναι οι μόνες υποομάδες της G.

Άσκηση 41 Έστω G μία κυκλική ομάδα με $|G| = n$. Γνωρίζουμε ότι κάθε στοιχείο της G παράγει μία μοναδική υποομάδα της G. Επίσης γνωρίζουμε ότι μία υποομάδα $K_i \leq G$ μπορεί να έχει περισσότερους από έναν γεννήτορες. Όμως οι γεννήτορες της K_i δεν μπορούν να είναι γεννήτορες κάποιας άλλης υποομάδας K_j. Άρα η G διαμερίζεται σε υποσύνολα που το καθένα περιέχει τους γεννήτορες μίας συγκεκριμένης υποομάδας. Δηλαδή είναι

$n = \sum_{K_i \leq G} \text{nr of generators of } K_i$

Επιπλέον, από την προηγούμενη άσκηση γνωρίζουμε ότι η G έχει ακριβώς μία υποομάδα για κάθε διαιρέτη d της τάξης της n. Δηλαδή είναι

$n = \sum_{d|n} \text{nr of generators of } K_d$

Αφού G κυκλική, είναι ισομορφική με την $\mathbb{Z}_n$ και κάθε υποομάδα της τάξης d είναι επίσης κυκλική, ισομορφική με την $\mathbb{Z}_d$. Δηλαδή είναι

$n = \sum_{d|n} \text{nr of generators of } \mathbb{Z}_d = \sum_{d|n} \phi(d)$.

Άσκηση 42 Κατ' αρχήν έχουμε ότι κάθε $a \in G$, $|G| = n$ παράγει μία υποομάδα τάξης $d, d|n$, η οποία είναι ισομορφική με την $\mathbb{Z}_d$, και άρα υπάρχουν $\phi(d)$ γεννήτορες της $< a >$ στην $< a > \subseteq G$. Από την Άσκηση 46, σελ. 109, έχουμε ότι η εξίσωση $x^d = e$ έχει ακριβώς d λύσεις στην $< a > \leq G$ (αφού $d|d$). Άρα από υπόθεση έχουμε ότι αυτές είναι και οι μοναδικές λύσεις της $x^d = e$ σε ολόκληρη την G, δηλαδή όλα τα στοιχεία της $< a >$ είναι λύσεις της $x^d = e$. Θα δείξουμε ότι η $< a >$ είναι η μόνη υποομάδα τάξης d. Πράγματι, αν υπήρχε και άλλη υποομάδα της G τάξης d, έστω H, τότε θα ήταν $b^d = e, \forall b \in H$, άτοπο, αφού η εξίσωση $x^d = e$ έχει το πολύ d λύσεις που τις βρήκαμε πρίν. Άρα υπάρχουν $\phi(d)$ στοιχεία τα οποία παράγουν μία μοναδική υποομάδα τάξης d.

Έστω τώρα ότι το σύνολο $D = \{d_1, \ldots, d_k\}$ περιέχει τους διαιρέτες του n τέτοιοι ώστε η $x^{d_i} = e$ να μην έχει λύση, δηλαδή να μην υπάρχει στοιχείο a που να παράγει υποομάδα της G τάξης $d_i, \forall i = 1, \ldots, k$. Δηλαδή όλα τα στοιχεία της G παράγουν υποομάδες τάξης που ανήκει στο σύνολο $D' = \{d|n\} \setminus D$. Δηλαδή έχουμε

$n = \sum_{d \in D'} \phi(d)$

Όμως από προηγούμενη άσκηση έχουμε ότι $n = \sum_{d|n} \phi(d) > \sum_{d \in D'} \phi(d)$. Άτοπο, δηλαδή δεν υπάρχουν διαιρέτες του n τέτοιοι ώστε η $x^d = e$ να να μην έχει λύση.

Δηλαδή για κάθε διαιρέτη $d|n$, άρα και για n, η $x^d = e$ έχει λύση. Δηλαδή υπάρχει $a \in G$ τέτοιο ώστε $a^n = e$, οπότε $G = < a >$ κυκλική.