χολή Ηλεκτρολόγων Μηχανικών και Μηχανικών Υπολογιστών
Εθνικό Μετσόβιο Πολυτεχνείο
Ροή Μ, 7ο εξάμηνο

Άλγεβρα και Εφαρμογές

Δεύτερη σειρά ασκήσεων

Σπουδαστής
Παπασκαρλάτος Αλέξανδρος (Α.Μ.: 03111097)

Ημερομηνία Παράδοσης: 22 Ιανουαρίου 2020

Άσκηση 1

(α).

$\sigma = \binom{1\,2\,3\,4\,5\,6\,7}{6\,5\,a\,3\,7\,4\,b}$

Καθώς η σ είναι μετάθεση της S_7 , υπάρχουν ακριβώς δύο ενδεχόμενα για τις τιμές των a, b :

- a = 1, b = 2
  $\sigma = \binom{1\,2\,3\,4\,5\,6\,7}{6\,5\,1\,3\,7\,4\,2}$ = (1,6,4,3) (2,5,7) = (1,3) (1,4) (1,6) (2,7) (2,5)
  Συνεπώς η σ είναι περιττή, καθώς γράφεται ως γινόμενο περιττού πλήθους αντιμεταθέσεων.

- a = 2, b = 1
  $\sigma = \binom{1\,2\,3\,4\,5\,6\,7}{6\,5\,2\,3\,7\,4\,1}$ = (1,6,4,3,2,5,7) = (1,7) (1,5) (1,2) (1,3) (1,4) (1,6)
  Συνεπώς η σ είναι άρτια, καθώς γράφεται ως γινόμενο άρτιου πλήθους αντιμεταθέσεων.

Τελικά, η σ είναι άρτια ανν a = 2 και b=1 .

(β)

τ = (1,2) (4,5,6,3) (3,7) (5,6,3,4) = $\binom{1\,2\,3\,4\,5\,6\,7}{2\,1\,5\,6\,3\,7\,4}$

(i).

- Γινόμενο ξένων κύκλων
  τ = (1,2) (3,5) (4,6,7)

- Γινόμενο αντιμεταθέσεων
  τ = (1,2) (3,5) (4,7) (4,6)

(ii).

ord(τ) = ΕΚΠ (ord((1,2)), ord((3,5)), ord((4,6,7))) = ΕΚΠ (2, 2, 3) = 6

$\tau^2 = \binom{1\,2\,3\,4\,5\,6\,7}{2\,1\,5\,6\,3\,7\,4} \binom{1\,2\,3\,4\,5\,6\,7}{2\,1\,5\,6\,3\,7\,4} = \binom{1\,2\,3\,4\,5\,6\,7}{1\,2\,3\,7\,5\,4\,6}$ = (4,7,6)

$\text{ord}(\tau^2)$ = ord((4,7,6)) = 3

(iii).

τ^{-1} = ((1,2) (3,5) (4,7) (4,6))$^{-1}$ = (4,6) (4,7) (3,5) (1,2)

$\tau^{-1} = \binom{1\,2\,3\,4\,5\,6\,7}{2\,1\,5\,7\,3\,4\,6}$

τ^{-1} = (1,2) (3,5) (4,7,6)

<u>Άσκηση 2</u>

Εφαρμόζω το Θεώρημα Cayley για τις ομάδες $\mathbb{Z}_8$, $\mathbb{Z}_2$ x $\mathbb{Z}_4$, D_4 , Q_8 .

Θα δείξουμε τον ισομορφισμό της εκάστοτε ομάδας G με κάποια ομάδα μεταθέσεων, υποομάδα της αντίστοιχης S_G.

Στα κάτωθι θα ισχύουν οι εξής θεωρήσεις :

- Το α θα είναι το πολλαπλασιαστικό στοιχείο από αριστερά και σ_α η αντίστοιχη μετάθεση, σύμφωνα με τη μεθοδολογία του θεωρήματος Cayley
- Ο ισομορφισμός που θα υπολογίζουμε θα ισχύει στοιχείο προς στοιχείο, σύμφωνα με τη διάταξη που έχουμε γράψει τα αντίστοιχα σύνολα.

G = $\mathbb{Z}_8$ = {0,1,2,3,4,5,6,7}

α	**σ_α**
0	$\binom{0\ 1\ 2\ 3\ 4\ 5\ 6\ 7}{0\ 1\ 2\ 3\ 4\ 5\ 6\ 7}$ = id
1	$\binom{0\ 1\ 2\ 3\ 4\ 5\ 6\ 7}{1\ 2\ 3\ 4\ 5\ 6\ 7\ 0}$ = (0,1,2,3,4,5,6,7)
2	$\binom{0\ 1\ 2\ 3\ 4\ 5\ 6\ 7}{2\ 3\ 4\ 5\ 6\ 7\ 0\ 1}$ = (0,2,4,6)(1,3,5,7)
3	$\binom{0\ 1\ 2\ 3\ 4\ 5\ 6\ 7}{3\ 4\ 5\ 6\ 7\ 0\ 1\ 2}$ = (0,3,6,1,4,7,2,5)
4	$\binom{0\ 1\ 2\ 3\ 4\ 5\ 6\ 7}{4\ 5\ 6\ 7\ 0\ 1\ 2\ 3}$ = (0,4)(1,5)(2,6)(3,7)
5	$\binom{0\ 1\ 2\ 3\ 4\ 5\ 6\ 7}{5\ 6\ 7\ 0\ 1\ 2\ 3\ 4}$ = (0,5,2,7,4,1,6,3)
6	$\binom{0\ 1\ 2\ 3\ 4\ 5\ 6\ 7}{6\ 7\ 0\ 1\ 2\ 3\ 4\ 5}$ = (0,6,4,2)(1,7,5,3)
7	$\binom{0\ 1\ 2\ 3\ 4\ 5\ 6\ 7}{7\ 0\ 1\ 2\ 3\ 4\ 5\ 6}$ = (0,7,6,5,4,3,2,1)

Επομένως, $\mathbb{Z}_8$ = {0,1,2,3,4,5,6,7} ≃

≃ { id, (0,1,2,3,4,5,6,7), (0,2,4,6)(1,3,5,7), (0,3,6,1,4,7,2,5), (0,4)(1,5)(2,6)(3,7), (0,5,2,7,4,1,6,3), (0,6,4,2)(1,7,5,3), (0,7,6,5,4,3,2,1) }

G = $\mathbb{Z}_2 \times \mathbb{Z}_4$ = {(0,0), (0,1), (0,2), (0,3), (1,0), (1,1), (1,2), (1,3)}

α	**σ_α**
(0,0)	$\begin{pmatrix} (0,0) & (0,1) & (0,2) & (0,3) & (1,0) & (1,1) & (1,2) & (1,3) \\ (0,0) & (0,1) & (0,2) & (0,3) & (1,0) & (1,1) & (1,2) & (1,3) \end{pmatrix}$ = id
(0,1)	$\begin{pmatrix} (0,0) & (0,1) & (0,2) & (0,3) & (1,0) & (1,1) & (1,2) & (1,3) \\ (0,1) & (0,2) & (0,3) & (0,0) & (1,1) & (1,2) & (1,3) & (1,0) \end{pmatrix}$ = ((0,0),(0,1),(0,2),(0,3))((1,0),(1,1),(1,2),(1,3))
(0,2)	$\begin{pmatrix} (0,0) & (0,1) & (0,2) & (0,3) & (1,0) & (1,1) & (1,2) & (1,3) \\ (0,2) & (0,3) & (0,1) & (0,0) & (1,2) & (1,3) & (1,0) & (1,1) \end{pmatrix}$ = ((0,0),(0,2))((0,1),(0,3))((1,0),(1,2))((1,1),(1,3))
(0,3)	$\begin{pmatrix} (0,0) & (0,1) & (0,2) & (0,3) & (1,0) & (1,1) & (1,2) & (1,3) \\ (0,3) & (0,0) & (0,1) & (0,2) & (1,3) & (1,0) & (1,1) & (1,2) \end{pmatrix}$ = ((0,0),(0,3),(0,2),(0,1))((1,3),(1,2),(1,1),(1,0))
(1,0)	$\begin{pmatrix} (0,0) & (0,1) & (0,2) & (0,3) & (1,0) & (1,1) & (1,2) & (1,3) \\ (1,0) & (1,1) & (1,2) & (1,3) & (0,0) & (0,1) & (0,2) & (0,3) \end{pmatrix}$ = ((0,0),(1,0))((0,1),(1,1))((0,2),(1,2))((0,3),(1,3))
(1,1)	$\begin{pmatrix} (0,0) & (0,1) & (0,2) & (0,3) & (1,0) & (1,1) & (1,2) & (1,3) \\ (1,1) & (1,2) & (1,3) & (1,0) & (0,1) & (0,2) & (0,3) & (0,0) \end{pmatrix}$ = ((0,0),(1,1),(0,2),(1,3))((1,0),(0,1),(1,2),(0,3))
(1,2)	$\begin{pmatrix} (0,0) & (0,1) & (0,2) & (0,3) & (1,0) & (1,1) & (1,2) & (1,3) \\ (1,2) & (1,3) & (1,1) & (1,0) & (0,2) & (0,3) & (0,0) & (0,1) \end{pmatrix}$ = ((0,0),(1,2))((0,1),(1,3))((0,2),(1,1))((0,3),(1,0))
(1,3)	$\begin{pmatrix} (0,0) & (0,1) & (0,2) & (0,3) & (1,0) & (1,1) & (1,2) & (1,3) \\ (1,3) & (1,0) & (1,1) & (1,2) & (0,3) & (0,0) & (0,1) & (0,2) \end{pmatrix}$ = ((0,0),(1,3),(0,2),(1,1))((1,0),(0,3),(1,2),(0,1))

Επομένως, $\mathbb{Z}_2 \times \mathbb{Z}_4$ = {(0,0), (0,1), (0,2), (0,3), (1,0), (1,1), (1,2), (1,3)} ≃
≃ { id, ((0,0),(0,1),(0,2),(0,3)) ((1,0),(1,1),(1,2),(1,3)),
((0,0),(0,2)) ((0,1),(0,3)) ((1,0),(1,2)) ((1,1),(1,3)), ((0,0),(0,3),(0,2),(0,1)) ((1,3),(1,2),(1,1),(1,0)),
((0,0),(1,0)) ((0,1),(1,1)) ((0,2),(1,2)) ((0,3),(1,3)), ((0,0),(1,1),(0,2),(1,3)) ((1,0),(0,1),(1,2),(0,3)),
((0,0),(1,2)) ((0,1),(1,3)) ((0,2),(1,1)) ((0,3),(1,0)), ((0,0),(1,3),(0,2),(1,1)) ((1,0),(0,3),(1,2),(0,1)) }

$G = D_4 = \{e, r, r^2, r^3, a, b, d_1, d_2\}$

α	σ_α
e	$\begin{pmatrix} e & r & r^2 & r^3 & a & b & d_1 & d_2 \\ e & r & r^2 & r^3 & a & b & d_1 & d_2 \end{pmatrix} = id$
r	$\begin{pmatrix} e & r & r^2 & r^3 & a & b & d_1 & d_2 \\ r & r^2 & r^3 & e & d_1 & d_2 & b & a \end{pmatrix} = (e, r, r^2, r^3)\ (a, d_1, b, d_2)$
r^2	$\begin{pmatrix} e & r & r^2 & r^3 & a & b & d_1 & d_2 \\ r^2 & r^3 & e & r & b & a & d_2 & d_1 \end{pmatrix} = (e, r^2)\ (r, r^3)\ (a, b)\ (d_1, d_2)$
r^3	$\begin{pmatrix} e & r & r^2 & r^3 & a & b & d_1 & d_2 \\ r^3 & e & r & r^2 & d_2 & d_1 & a & b \end{pmatrix} = (e, r^3, r^2, r)\ (a, d_2, b, d_1)$
a	$\begin{pmatrix} e & r & r^2 & r^3 & a & b & d_1 & d_2 \\ a & d_2 & b & d_1 & e & r^2 & r^3 & r \end{pmatrix} = (e, a)\ (r, d_2)\ (r^2, b)\ (r^3, d_1)$
b	$\begin{pmatrix} e & r & r^2 & r^3 & a & b & d_1 & d_2 \\ b & d_1 & a & d_2 & r^2 & e & r & r^3 \end{pmatrix} = (e, b)\ (r, d_1)\ (r^2, a)\ (r^3, d_2)$
d_1	$\begin{pmatrix} e & r & r^2 & r^3 & a & b & d_1 & d_2 \\ d_1 & a & d_2 & b & r & r^3 & e & r^2 \end{pmatrix} = (e, d_1)\ (r, a)\ (r^2, d_2)\ (r^3, b)$
d_2	$\begin{pmatrix} e & r & r^2 & r^3 & a & b & d_1 & d_2 \\ d_2 & b & d_1 & a & r^3 & r & r^2 & e \end{pmatrix} = (e, d_2)\ (r, b)\ (r^2, d_1)\ (r^3, a)$

Επομένως, $D_4 = \{e, r, r^2, r^3, a, b, d_1, d_2\} \simeq$

$\simeq \{$ id,

$(e, r, r^2, r^3)\ (a, d_1, b, d_2)$, $(e, r^2)\ (r, r^3)\ (a, b)\ (d_1, d_2)$, $(e, r^3, r^2, r)\ (a, d_2, b, d_1)$,

$(e, a)\ (r, d_2)\ (r^2, b)\ (r^3, d_1)$, $(e, b)\ (r, d_1)\ (r^2, a)\ (r^3, d_2)$,

$(e, d_1)\ (r, a)\ (r^2, d_2)\ (r^3, b)$, $(e, d_2)\ (r, b)\ (r^2, d_1)\ (r^3, a)\ \}$

$G = Q_8 = \{1,-1,i,-i,j,-j,k,-k\}$

α	**σ_α**
1	$\begin{pmatrix} 1 & -1 & i & -i & j & -j & k & -k \\ 1 & -1 & i & -i & j & -j & k & -k \end{pmatrix}$ = id
-1	$\begin{pmatrix} 1 & -1 & i & -i & j & -j & k & -k \\ -1 & 1 & -i & i & -j & j & -k & k \end{pmatrix}$ = (1, -1)(i,-i)(j,-j)(k,-k)
i	$\begin{pmatrix} 1 & -1 & i & -i & j & -j & k & -k \\ i & -i & -1 & 1 & k & -k & -j & j \end{pmatrix}$ = (1,i,-1,-i)(j,k,-j,-k)
-i	$\begin{pmatrix} 1 & -1 & i & -i & j & -j & k & -k \\ -i & i & 1 & -1 & -k & k & j & -j \end{pmatrix}$ = (1,-i,-1,i)(j,-k,-j,k)
j	$\begin{pmatrix} 1 & -1 & i & -i & j & -j & k & -k \\ j & -j & -k & k & -1 & 1 & i & -i \end{pmatrix}$ = (1,j,-1,-j)(i,-k,-i,k)
-j	$\begin{pmatrix} 1 & -1 & i & -i & j & -j & k & -k \\ -j & j & k & -k & 1 & -1 & -i & i \end{pmatrix}$ = (1,-j,-1,j)(i,k,-i,-k)
k	$\begin{pmatrix} 1 & -1 & i & -i & j & -j & k & -k \\ k & -k & j & -j & -i & i & -1 & 1 \end{pmatrix}$ = (1,k,-1,-k)(i,j,-i,-j)
-k	$\begin{pmatrix} 1 & -1 & i & -i & j & -j & k & -k \\ -k & k & -j & j & i & -i & 1 & -1 \end{pmatrix}$ = (1,-k,-1,k)(i,-j,-i,j)

Επομένως, $Q_8 = \{1,-1,i,-i,j,-j,k,-k\} \simeq$
≃ { id, (1,-1) (i,-i) (j,-j) (k,-k), (1,i,-1,-i) (j,k,-j,-k), (1,-i,-1,i) (j,-k,-j,k),
(1,j,-1,-j) (i,-k,-i,k), (1,-j,-1,j) (i,k,-i,-k), (1,k,-1,-k) (i,j,-i,-j), (1,-k,-1,k) (i,-j,-i,j) }

<u>Άσκηση 3</u>

(α).
Είναι 20 = ΕΚΠ(4,5)

Θεωρώ σ = (1,2,3,4) (5,6,7,8,9) = $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 3 & 4 & 1 & 6 & 7 & 8 & 9 & 5 \end{pmatrix} \in S_9$

ord(σ) = ΕΚΠ(ord((1,2,3,4)), ord((5,6,7,8,9))) = ΕΚΠ(4, 5) = 20

Δηλαδή η σ είναι ένα στοιχείο του S_9 τάξης 20.

(β).
Είναι 18 = 3 · 3 · 2

<u>Block άτοπο: Έστω τ $\in S_9$ με ord(τ) = 18</u>

- Η τ αναλύεται σε γινόμενο ξένων κύκλων, έστω τ_1 , τ_2 , …, τ_κ , δηλαδή $\tau = \tau_1 \tau_2 \dots \tau_\kappa$
- Έστω $r_1 = ord(\tau_1)$, $r_2 = ord(\tau_2)$, …, $r_\kappa = ord(\tau_\kappa)$
- Είναι ord(τ) = ΕΚΠ(ord(τ_1), ord(τ_2), …, ord(τ_κ)) ⇔ 18 = ΕΚΠ (r_1 , r_2 , …, r_κ)
- Επίσης, καθώς τ $\in S_9$ και οι τ_1, τ_2, …, τ_κ είναι ξένοι κύκλοι, ισχύει $r_1 + r_2 + \dots + r_3 \leq 9$

<u>Άτοπο</u>, καθώς δεν υπάρχουν αριθμοί r_i τ.ω. $r_1 + r_2 + \dots + r_3 \leq 9$ και ΕΚΠ (r_1 , r_2 , …, r_κ) = 18
Επομένως, δεν υπάρχει στοιχείο της S_9 τάξης 18

Άσκηση 4

(i).

Κάθε ζεύγος αντιμεταθέσεων ορίζει μια μετάθεση.
Κάθε γινόμενο (οσοδήποτε πλήθους) ζευγών αντιμεταθέσεων ορίζει μια μετάθεση.
Καθώς τα στοιχεία των επιμέρους αντιμεταθέσεων είναι φραγμένα από το n, ισχύει πως κάθε τέτοια μετάθεση είναι μια έγκυρη μετάθεση στο S_n .

Κάθε ζεύγος από αντιμεταθέσεις είναι ένα γινόμενο δύο αντιμεταθέσεων.
Κάθε γινόμενο (οσοδήποτε πλήθους) ζευγών αντιμεταθέσεων είναι ένα γινόμενο άρτιου πλήθους αντιμεταθέσεων. Συνεπώς, είναι μια άρτια μετάθεση.
Καμία άρτια μετάθεση δεν μπορεί να είναι και περιττή.

Από όλα τα παραπάνω προκύπτει πως όλα τα στοιχεία που παράγονται από ζεύγη αντιμεταθέσεων ανήκουν στην εναλλάσσουσα υποομάδα A_n .

Μένει να αποδείξω ότι τα ζεύγη αντιμεταθέσεων είναι ικανά να παράγουν όλα τα στοιχεία της A_n.

- Έστω τυχαία άρτια μετάθεση $\sigma \in S_n$.
- Η σ μπορεί να γραφεί ως γινόμενο άρτιου πλήθους αντιμεταθέσεων.
- Είναι $\sigma = (a_1 , a_1') (a_2 , a_2') \dots (a_{2k} , a_{2k}')$, $k \in \mathbb{N}$
  όπου $\forall$ i, $a_i \neq a_i'$
- Επειδή $\forall$ i, $(a_i , a_i') \equiv (a_i', a_i)$,
  μπορούμε να θεωρήσουμε χωρίς βλάβη της γενικότητας πως $\forall$ i, $a_i < a_i'$
  Αυτό δεν είναι ουσιαστική παρατήρηση, απλά το γράφουμε για να συμφωνει τυπικά με την εκφώνηση, καθώς σε μια αντιμετάθεση (i, j) θεωρείται πως $1 \leq i < j \leq n$, σύμφωνα με τον ορισμό της εκφώνησης.
- Επομένως, η σ παράγεται από τα ζεύγη αντιμεταθέσεων:
  $\{(a_1 , a_1') (a_2 , a_2')\}$, $\{(a_3 , a_3') (a_4 , a_4')\}$, ... , $\{(a_{2k-1} , a_{2k-1}') (a_{2k} , a_{2k}')\}$

Επομένως, κάθε άρτια μετάθεση, δηλαδή κάθε στοιχείο της A_n μπορεί να παραχθεί από ζεύγη αντιμεταθέσεων.

Τελικά, η εναλλάσσουσα υποομάδα A_n παράγεται από ζεύγη αντιμεταθέσεων.

(ii).
Έστω τυχαίος 3-κύκλος (a,b,c) .
Κάθε τέτοιος κύκλος μπορεί να γραφεί ως ένα ζεύγος αντιμεταθέσεων.
Πράγματι, είναι $(a,b,c) = (a,c)\ (a,b)$.

Επιπλέον, έστω τυχαίο ζεύγος αντιμεταθέσεων $(i,j)\ (k,l)$
Ισχύει $i \neq j$ και $k \neq l$
Διακρίνω τρεις περιπτώσεις:

- Τα i,j,k,l είναι όλα διαφορετικά ανά 2. Τότε ισχύει:
  $(i,j)\ (k,l) = (i,j)\ (i,k)\ (i,k)\ (k,l) = (i,j)\ (i,k)\ (k,i)\ (k,l) = (i,k,j)\ (k,l,i)$
  Δηλαδή η αντιμετάθεση μπορεί να γραφεί ως γινόμενο 3-κύκλων.

- Ακριβώς 2 εκ των i, j, k, l είναι ίδια μεταξύ τους.
  Έστω $j = l$. Τότε ισχύει:
  $(i,j)\ (k,l) = (i,j)\ (k,j) = (j,i)\ (j,k) = (j,k,i)$
  Δηλαδή η αντιμετάθεση μπορεί να γραφεί ως ένας 3-κύκλος.
  Επειδή σε οποιαδήποτε αντιμετάθεση ισχύει $(a,b) \equiv (b, a)$, το συμπέρασμα ισχύει όμοια για τις περιπτώσεις όπου αντί για $j = l$, είναι $i = k$ ή $i = l$ ή $j = k$.

- Υπάρχουν δύο ζεύγη ομοίων στα i,j,k,l
  Έστω $i = l$ και $j = k$. Τότε ισχύει:
  $(i,j)\ (k,l) = (i,j)\ (j,i) = id$, δηλαδή πρόκειται για την ταυτοτική μετάθεση.
  Όμως, μπορούμε να σχηματίσουμε την ταυτοτική και ως γινόμενο 3-κύκλων.
  Πράγματι, $(a,b,c)\ (a,c,b) = (a,c)\ (a,b)\ (a,b)\ (a,c) = (a,c)\ (a,c) = id$
  Οπότε, $(i,j)\ (k,l) = id = (a,b,c)\ (a,c,b)$
  Δηλαδή η αντιμετάθεση μπορεί να γραφεί ως γινόμενο 3-κύκλων.

Συνεπώς, για κάθε αποδεκτή περίπτωση για τις τιμές των i,j,k,l, βλέπουμε πως το τυχαίο ζεύγος αντιμεταθέσεων $(i,j)\ (k,l)$ μπορεί να γραφεί ως γινόμενο 3-κύκλων.

Τελικά, κάθε 3-κύκλος μπορεί να γραφεί ως ζεύγος αντιμεταθέσεων και κάθε ζεύγος αντιμεταθέσεων μπορεί να γραφεί ως γινόμενο 3-κύκλων.

Επομένως, καθώς η A_n παράγεται από τα ζεύγη αντιμεταθέσεων σύμφωνα με το υποερώτημα (i), προκύπτει πως η A_n παράγεται από τους 3-κύκλους.

Άσκηση 5

(α).
Είναι $|G| = 40$, $|G'| = 28$ και $f : G \to G'$ ομομορφισμός.

Από Θεμελιώδες Θεώρημα Ομομορφισμού, προκύπτουν τα εξής:

Ο πυρήνας Kerf είναι υποομάδα της G.
Συνεπώς, $|Kerf| \mid |G| \quad \Rightarrow \quad |Kerf| \mid 40$
$\Rightarrow \quad |Kerf| = 1 \lor 2 \lor 4 \lor 5 \lor 8 \lor 10 \lor 20 \lor 40$

Η εικόνα $f(G) \equiv Imf$ είναι υποομάδα της G'.
Συνεπώς, $|Imf| \mid |G'| \quad \Rightarrow \quad |Imf| \mid 28$
$\Rightarrow \quad |Imf| = 1 \lor 2 \lor 4 \lor 7 \lor 14 \lor 28$

Επίσης, η G/Kerf είναι ισομορφική με την Imf, άρα $|G/Kerf| = |Imf|$

Ισχύει, $|G/Kerf| \cdot |Kerf| = |G| \quad \Leftrightarrow \quad |Imf| \cdot |Kerf| = 40$

Τελικά, προκύπτουν τρία αποδεκτά ενδεχόμενα για τα |Kerf|, |Imf|
- $|Kerf| = 10$, $|Imf| = 4$
- $|Kerf| = 20$, $|Imf| = 2$
- $|Kerf| = 40$, $|Imf| = 1$

(β).
Ορίζω $\varphi : \mathbb{Z}_{40} \rightarrow \mathbb{Z}_{28}$ ως εξής:

$$\text{Για } x \in \mathbb{Z}_{40}, \quad \varphi(x) = \begin{cases} 0 \in \mathbb{Z}_{28}, & \text{αν } x \text{ άρτιο} \\ 14 \in \mathbb{Z}_{28}, & \text{αν } x \text{ περιττό} \end{cases}$$

Προκειμένου να δείξω πως η φ είναι ομομορφισμός, αρκεί να δείξω πως
$\forall\ \alpha, \beta \in \mathbb{Z}_{40}$, ισχύει $\varphi(\alpha + \beta) = \varphi(\alpha) + \varphi(\beta)$

Θυμίζω πως στο $\mathbb{Z}_{28}$, ισχύει $14 + 14 = 0$
Επίσης, επειδή το 40 είναι άρτιος αριθμός, ισχύει :
$\forall\ a,b \in \mathbb{Z}_{40}$ με $a + b = c \in \mathbb{Z}_{40}$ ισχύει πως το c είναι άρτιο ανν τα a,b έχουν την ίδια αρτιότητα (και πως το c είναι περιττό, ανν τα a,b έχουν διαφορετική αρτιότητα) .

Έστω $\alpha, \beta \in \mathbb{Z}_{40}$. Διακρίνω 4 περιπτώσεις :

- <u>α άρτιο, β άρτιο</u>
  Είναι $\alpha \in \mathbb{Z}_{40}$ άρτιο, άρα $\varphi(\alpha) = 0 \in \mathbb{Z}_{28}$
  Είναι $\beta \in \mathbb{Z}_{40}$ άρτιο, άρα $\varphi(\beta) = 0 \in \mathbb{Z}_{28}$
  Είναι $(\alpha + \beta) \in \mathbb{Z}_{40}$ άρτιο, άρα $\varphi(\alpha + \beta) = 0 \in \mathbb{Z}_{28}$
  Επομένως, $\varphi(\alpha + \beta) = 0 = 0 + 0 = \varphi(\alpha) + \varphi(\beta)$

- <u>α άρτιο, β περιττό</u>
  Είναι $\alpha \in \mathbb{Z}_{40}$ άρτιο, άρα $\varphi(\alpha) = 0 \in \mathbb{Z}_{28}$
  Είναι $\beta \in \mathbb{Z}_{40}$ περιττό, άρα $\varphi(\beta) = 14 \in \mathbb{Z}_{28}$
  Είναι $(\alpha + \beta) \in \mathbb{Z}_{40}$ περιττό, άρα $\varphi(\alpha + \beta) = 14 \in \mathbb{Z}_{28}$
  Επομένως, $\varphi(\alpha + \beta) = 14 = 0 + 14 = \varphi(\alpha) + \varphi(\beta)$

- <u>α περιττό, β περιττό</u>
  Είναι $\alpha \in \mathbb{Z}_{40}$ περιττό, άρα $\varphi(\alpha) = 14 \in \mathbb{Z}_{28}$
  Είναι $\beta \in \mathbb{Z}_{40}$ περιττό, άρα $\varphi(\beta) = 14 \in \mathbb{Z}_{28}$
  Είναι $(\alpha + \beta) \in \mathbb{Z}_{40}$ άρτιο, άρα $\varphi(\alpha + \beta) = 0 \in \mathbb{Z}_{28}$
  Επομένως, $\varphi(\alpha + \beta) = 0 = 14 + 14 = \varphi(\alpha) + \varphi(\beta)$

- <u>α περιττό, β άρτιο</u>
  Είναι $\alpha \in \mathbb{Z}_{40}$ περιττό, άρα $\varphi(\alpha) = 14 \in \mathbb{Z}_{28}$
  Είναι $\beta \in \mathbb{Z}_{40}$ άρτιο, άρα $\varphi(\beta) = 0 \in \mathbb{Z}_{28}$
  Είναι $(\alpha + \beta) \in \mathbb{Z}_{40}$ περιττό, άρα $\varphi(\alpha + \beta) = 14 \in \mathbb{Z}_{28}$
  Επομένως, $\varphi(\alpha + \beta) = 14 = 14 + 0 = \varphi(\alpha) + \varphi(\beta)$

Συνεπώς η σχέση ισχύει σε κάθε περίπτωση, δηλαδή πράγματι
$\forall\ \alpha, \beta \in \mathbb{Z}_{40}$, ισχύει $\varphi(\alpha + \beta) = \varphi(\alpha) + \varphi(\beta)$
Επομένως η φ είναι ομομορφισμός.

Άσκηση 6

Θα βρούμε όλες τις μη ισόμορφες αβελιανές ομάδες G τ.ω. $|G| \leq 30$ και $\forall\ g \in G,\ g^{12} \equiv 1$.

Είναι $\forall\ g \in G$, $ord(g) \mid 12$
Επομένως, οι ενδεχόμενες τάξεις των στοιχείων μιας τέτοιας ομάδας G είναι 1, 2, 3, 4, 6, 12 ,
δηλαδή 1, 2, 2^2, 3, $2 \cdot 3$, $2 \cdot 2 \cdot 3$.

Θυμίζουμε πως αν $G = \mathbb{Z}_{a1} \times \mathbb{Z}_{a2} \times \ldots \times \mathbb{Z}_{ak}$, τότε $|G| = a_1 \cdot a_2 \cdot \ldots \cdot a_k$
καθώς αυτό είναι το πλήθος των διακεκριμένων στοιχείων της G.

Αξιοποιούμε το Θεμελιώδες Θεώρημα των Πεπερασμένα Παραγόμενων Αβελιανών Ομάδων.

Υπάρχουν 17 τέτοιες ομάδες. Είναι οι εξής:

$\mathbb{Z}_2$, $\mathbb{Z}_2 \times \mathbb{Z}_2$, $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$, $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$,
$\mathbb{Z}_2 \times \mathbb{Z}_4$, $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_4$, $\mathbb{Z}_4$, $\mathbb{Z}_4 \times \mathbb{Z}_4$,

$\mathbb{Z}_3$, $\mathbb{Z}_3 \times \mathbb{Z}_3$, $\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3$,

$\mathbb{Z}_2 \times \mathbb{Z}_3$, $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3$, $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3$,
$\mathbb{Z}_4 \times \mathbb{Z}_3$, $\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_3$,
$\mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3$

Άσκηση 7

(α).

Θα υπολογίσω το 7^{402} (mod 12)

Είναι $\gcd(7,12) = 1$

Είναι $\varphi(12) = \varphi(2^2)\ \varphi(3) = (2^2 - 2^1)\ 2 = 2 \cdot 2 = 4$

Είναι $7^{402} = 7^{400+2} = 7^{400} \cdot 7^2 = (7^4)^{100} \cdot 49$

Είναι $7^{402} \equiv (7^4)^{100} \cdot 49 \equiv 1^{100} \cdot 49 \equiv 49 \equiv 1 \pmod{12}$

Συνεπώς, το υπόλοιπο της ακέραιας διαίρεσης του 7^{402} δια 12 είναι 1 (και όχι 0), άρα το 12 δε διαιρεί το 7^{402} .

(β).

Θα υπολογίσω το 3^{111} (mod 7)

Είναι $\gcd(3,7) = 1$

Είναι $\varphi(7) = 6$

Είναι $3^{111} = 3^{108+3} = 3^{108} \cdot 3^3 = (3^6)^{18} \cdot 27$

Είναι $3^{111} \equiv (3^6)^{18} \cdot 27 \equiv 1^{18} \cdot 27 \equiv 27 \equiv 6 \pmod 7$

Συνεπώς, το υπόλοιπο της ακέραιας διαίρεσης του 3^{111} δια 7 είναι 6 .