Άρα για το ισόπλευρο μας:

$$\Sigma_3 = \{ f:\{1,2,3\} \xrightarrow[\text{επι}]{1-1} \{1,2,3\}\} = \{1, f, f^2, g, g\circ f, g\circ f^2\}$$

όχι αβελιανή ομάδα. Με f, g: γεννήτορες ώστε $f^3=1$ και $g^2=1$ αλλά είναι ομάδα

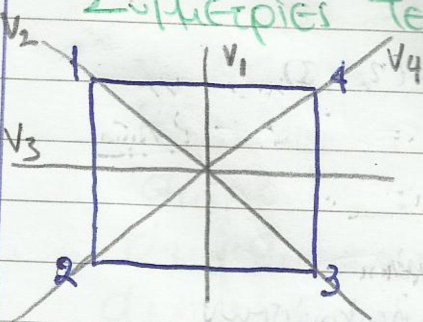
Πόσα στοιχεία έχει το Σ_ν;

Έχει $|\Sigma_\nu| = \nu!$

αφού το

$$\left.\begin{array}{cccccc} 1 & 2 & 3 & \cdots & \nu \\ \downarrow & \downarrow & \downarrow & & \downarrow \\ \nu \text{ φορές} & \nu-1 \text{ φορές} & \nu-2 \text{ φορές} & & 1 \text{ φορές} \end{array}\right\} \nu!$$

Συμμετρίες Τετραγώνου



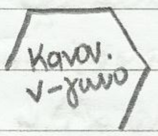
$$D_4 = \{R, R^2, R^3, 1=R^4, V_1, V_2, V_3, V_4\}$$

$V_i^2 = 1$

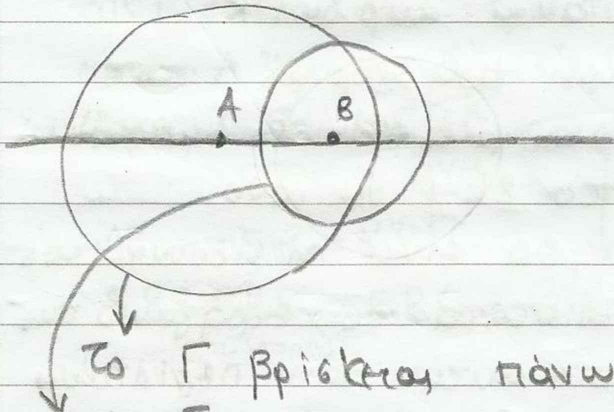
$|D_4| = 8$ και $|\Sigma_4| = 4! = 24$ $\quad D_4 \subset \Sigma_4$

ΛΗΜΜΑ: Κάθε σημείο ενός κανονικού ν-γωνου καθορίζεται από την απόσταση δύο διαδοχικών κορυφών.

Απόδειξη:



Κυρτό $\Leftrightarrow$ { το ευθύγραμμο τμήμα που ενώνει δύο τυχαία σημεία του βρίσκεται στο εσωτερικό του



Γνωρίζουμε την απόσταση του Γ απο το Α και απο το Β. Αυτές είναι δεδομένες.

το Γ βρίσκεται πάνω στην περιφέρεια
" Γ " " " "

Επειδή το κανονικό ν-γωνο είναι κυρτό το Γ, θα βρίσκεται ή απο τη μία ή απο την άλλη πλευρά που ορίζεται απο τα Α και Β.

ΘΕΩΡΗΜΑ: Η D_ν έχει 2ν στοιχεία

Απόδειξη:

α) Η D_ν έχει το πολύ 2ν στοιχεία. Επειδή κάθε σημείο του καθορίζεται πλήρως απο την απόσταση δύο διαδοχικών κορυφών, αρκεί να βρούμε πόσες διαδοχικές κορυφές έχουμε.

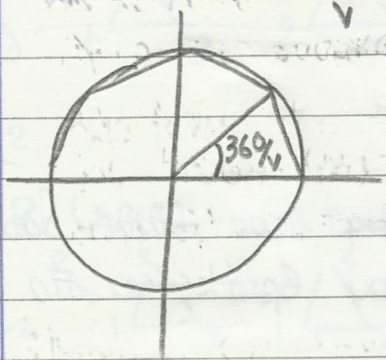
Έχουμε, το $(A,B) \xrightarrow{f} (f(A), f(B))$

$\Gamma \longrightarrow f(\Gamma)$
$A \xrightarrow{f} \nu$ περιπτώσεις
$B \xrightarrow{f} 2$ περιπτώσεις

} τελικά 2ν το πολύ περιπτ.

β) Θα πρέπει νδο ακριβώς 2ν περιπτώσεις
Έχουμε ν-διαδοχικές στροφές οπου δίνονται απο τη βασική

σχέση $R = \frac{360}{v}$.

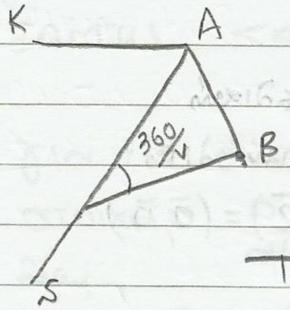


• Εαν $v = 2k+1$ τότε μια συμμετρία οπου διατηρεί την τυχαία κορυφή A σταθερή δεν μπορεί να κρατάει και την άλλη, $v-1=2k$ και θα πρέπει να έχουμε k κορυφές απο τη μία και k από την άλλη. Αυτές είναι ακριβώς k.

• Εάν $v=2k$: (α) Αν διατηρεί μια κορυφή A τότε υποχρεωτικά θα διατηρεί και μία άλλη B διότι αλλιώς θα είχαμε να διαιρέσουμε το $2k-1$ διά δύο.
(β) Αν δε διατηρεί καμία, θα είναι η μεσοκάθετος κάποιας πλευράς με την ιδιότητα το τετράγωνό της να είναι η ταυτοτική, και σε αυτήν την περίπτωση έχουμε $\frac{v}{2} + \frac{v}{2} = v$ συμμετρίες. Επειδή οι συμμετρίες έχουν την ιδιότητα το τετράγωνό τους να είναι την ταυτοτική και οι στροφές δεν την έχουν, θα είναι διαφορετικές.

ΠΡΟΤΑΣΗ: Αν R είναι η βασική στροφή ενός κανονικού v-γώνου και S μία συμμετρία, τότε ισχύει:
$SRS^{-1} = R^{v-1}$

Απόδειξη
$D_v = \{1, R, \ldots, R^{v-1}, S, RS, R^2S, \ldots, R^{v-1}S\}$
Αν είχαμε $R=R^i \Rightarrow R^{i-1} = 1!$ $2 \leq i \leq n-1$
Αν είχαμε $R^i = R^k S \Rightarrow R^{i-k} = S$ Αδύνατο
Αν είχαμε $R^i S = R^k S \Rightarrow R^i SS = R^k SS \Rightarrow R^i = R^k$
$SRS = R^{v-1} \Leftrightarrow RS = SR^{v-1}$
Ας πάρουμε την S να είναι μία συμμετρία με μία κορυφή σταθερή.



$RS(A) = R(A) = B$

$SR^{\nu-1}(A) = S(K) = B$

$RS(B) = R(K) = A$

$SR^{\nu-1}(B) = S(A) = A$

Αφού και οι 2 απεικονίζουν δύο σημεία στα ίδια αντίστοιχα σημεία, ταυτίζονται

Το ίδιο ισχύει αν η S στέλνει το A στο B και δεν διατηρεί σημεία

Ισχυρισμός: D_ν γεννάται - παράγεται (δηλ. κάθε στοιχείο της) δίνεται σαν γινόμενο των R και S για τα οποία ισχύει $R^\nu = 1 = S^2$ και $SRS = R^{\nu-1}$

Άρα $SR^i = SR^k$ πρέπει $SR^iS = R^{-i}$

$SRS = R^{\nu-1}$ $\quad\big\downarrow$ απόδ. $\quad SRS = R^{\nu-1} = R^{-1}$

$SR = R^{\nu-1}S$

$\underbrace{SR\cancel{SS}RS \dots \cancel{S}RS}_{i \text{ φορές}} = \underbrace{R^{\nu-1}R^{\nu-1}\dots R^{\nu-1}}_{i \text{ φορές}} \Rightarrow SR^iS = R^{i(\nu-1)} = R^k = R^{-i}$

ΚΥΚΛΙΚΕΣ ΟΜΑΔΕΣ:

Ορισμός: Μια ομάδα Ο καλείται κυκλική, αν όλα τα στοιχεία της δίνονται σαν δυνάμεις ή αθροίσματα ενός μόνο στοιχείου της, ο οποίος είναι γεννήτορας.

πχ

$\mathbb{Z}$ γεννάται από το 1

$\mathbb{Z}_5$ γεννάται από τα $\bar{1}, \bar{2}, \bar{3}, \bar{4}$ δηλαδή έχουμε 5-1 γεννήτορες

Ορισμός: Η τάξη μιας ομάδας Ο συμβολίζεται με $|O|$ και δείχνει το πλήθος των στοιχείων της Ο

1) $|O| < \infty$ και 2) $|O| = \infty$

πχ: το $\mathbb{Z}_p$, p πρώτος

πχ: $D_3 = \{1, R, R^2, S, RS, R^2S\}$

$\{1, f, f^2, g, fg, f^2g\}$

πχ 1

Μια πεπερασμένη, όχι κυκλική αλλά αβελιανή

$\mathbb{Z}_2\times\mathbb{Z}_2=\{(\bar0,\bar0),(\bar0,\bar1),(\bar1,\bar0),(\bar1,\bar1)\}$ όχι κυκλική

Αν ήταν θα είχαμε $(\bar0,\bar1)+(\bar0,\bar1)=(\bar0,\bar2)=(\bar0,\bar0)$

ομοια και το $(\bar1,\bar0)+(\bar1,\bar0)=(\bar0,\bar0)$

$(\bar1,\bar1)+(\bar1,\bar1)=(\bar1+\bar1,\bar1+\bar1)=(\bar0,\bar0)$

πχ 2

Μια άπειρη κυκλική είναι το $\mathbb{Z}$

Μια άπειρη μη κυκλική αβελιανή ή όχι αβελιανή

$\downarrow \mathbb{Z}\times\mathbb{Z}$ $\downarrow \Sigma_\infty$

Βασικές Ιδιότητες:

Αν $(G,\cdot)$ ομάδα και a στοιχείο. Τότε ισχύει:

1) $a^k\cdot a^v=a^{k+v}$, $k\in\mathbb{Z}$ & $v\in\mathbb{Z}$

2) $(a^{-1})^k=(a^{-1})^k$, $k\in\mathbb{Z}$

3) $(a^k)^v=a^{kv}=(a^v)^k$, $k,v\in\mathbb{Z}$

Αποδ:

Για $k,v\in\mathbb{N}$ προφανώς ισχύουν

Για $k,v\in\mathbb{Z}$

$$a^k\cdot a^v=\underbrace{a\cdots a}_{k}\cdot\underbrace{a\cdots a}_{v}=a^{k+v}$$

$$(a^{-1})^k\to(a^{-1})^k\cdot a^k=\underbrace{a^{-1}\cdots a^{-1}}_{k\ \varphi o\rho.}\cdot\underbrace{a\cdots a}_{k\ \varphi o\rho}=1$$

$(a^k)^{-1}=(a^{-1})^k=a^{-k}=$ αντίστροφος του a^k

Θεωρούμε ότι ο k είναι ακέραιος

πχ

Κυκλική $\mathbb{Z}=\langle 1\rangle=\langle -1\rangle$

$\mathbb{Q}=\{p/q\ /\ (p,q)=1\ \ q\in\mathbb{N}^*\}$

όπου $\langle a\rangle$ η ομάδα που γεννάται από το a

$\langle a\rangle=\{a^k\ /\ k\in\mathbb{Z}\}$

Επίσης $<a,b> = \{ab \neq ba$ όπου $a^{k_1} \cdot b^{m_1} \cdot a^{k_2} \cdot b^{m_2} \cdots a^{k_v} \cdot b^{m_v}$
ώστε $v > 1$ και $k_i, m_i \in \mathbb{Z}\}$.

Για το σύνολο $\mathbb{Q}$ προφανώς $p<q$. Θέλαμε ένα στοιχείο $\frac{p'}{q'} \neq k\frac{p}{q}$ $k \in \mathbb{Z}$

άρα,

$$\frac{3}{2}\cancel{\frac{p}{q}} = k\cancel{\frac{q}{q}} \Rightarrow k = \frac{3}{2} \quad k \notin \mathbb{Z}$$

Άρα, το $\frac{3}{2}\frac{p}{q} \notin <\frac{p}{q}>$ αλλά $\frac{3}{2}\frac{p}{q} \in \mathbb{Q}$

πχ

Για το $GL(2,\mathbb{R}) = \{2\times 2$ αντιστρέψιμοι πίνακες$\}$

τότε $|GL(2,\mathbb{R})| = \infty$ γιατί

$\{(r)_{1\times 1} \mid r \neq 0 \quad r \in \mathbb{R}^*\} = \mathbb{R}^*$, $|\mathbb{R}^*| = \infty$

$\underbrace{\{\begin{pmatrix} r & 0 \\ 0 & r \end{pmatrix} \mid r \in \mathbb{R}^*\}}_{\infty} \subset GL(2,\mathbb{R})$

$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in GL(2,\mathbb{R}) - \{\begin{pmatrix} r & 0 \\ 0 & r \end{pmatrix} \mid r \in \mathbb{R}^*\}$.

$\begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}^k = \begin{pmatrix} 2^k & 0 \\ 0 & 2^k \end{pmatrix} \neq \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad k \neq 0$

αλλά,

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Ορισμός: Τάξη ενός στοιχείου a μιας ομάδας G είναι ο μικρότερος φυσικός n ώστε $a^n = 1$. Αν δεν υπάρχει λέμε ότι το a έχει άπειρη τάξη.

$O(a) = n$ η ελάχιστος φυσικος ώστε:

$a^n = 1$

πχ

$$O\begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} = \infty \quad \text{και} \quad O\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = 2$$

ΙΔΙΟΤΗΤΕΣ

1) $O(a) = O(a^{-1})$
2) Αν $O(a) = n$ και $a^k = 1 \Rightarrow n \mid k$
3) Αν $O(a) = n$ και $d = (n,k)$ τότε
$O(a^k) = \frac{n}{(n,k)} = \frac{n}{d}$

ΑΠΟΔΕΙΞΗ

1) Εστω $O(a) = n$ $a^n = 1$ n μικρότερος
$(a^{-1})^n = a^{-n} = (a^n)^{-1} = 1^{-1} = 1$. Αρα, $O(a^{-1}) \leq n$
Εστω $O(a^{-1}) = k < n$
$(a^{-1})^k = 1 \Rightarrow a^{-k} = 1 \Rightarrow (a^{-k})^{-1} = 1^{-1} = 1 \Rightarrow a^{-(-k)} = 1 \Rightarrow a^k = 1$
$k < n$ άτοπο

2) Αν $n \nmid k \Rightarrow k = \pi n + u$ με $u < n$
$a^k = a^{\pi n + u} = 1 \Rightarrow (a^n)^{\pi} \cdot a^u = 1 \Rightarrow$
$\Rightarrow 1^{\pi} \cdot a^u = 1 \Rightarrow a^u = 1$ και $u < n \Rightarrow u = 0$
άρα $k = \pi n \Rightarrow n \mid k$

3) $O(a) = n$
τότε $O(a^k) = m$ και έτσι:
$(a^k)^{n/(n,k)} = a^{k \cdot n/(n,k)} = (a^n)^{k/(n,k)} = 1^{k/(n,k)} = 1$
Αρα, $m \mid \frac{n}{(n,k)}$ (+) Θέλουμε $\frac{n}{(n,k)}$ $(a^k)^m = 1 \Rightarrow a^{km} = 1$

Αρα $n \mid km$ ⇒ $km = n \cdot x = n'(n,k)x \Rightarrow$
$\Rightarrow k'(n,k)m = n'(n,k)x \Rightarrow$
με $(k', n') = 1$
$\Rightarrow n \mid km \Rightarrow \frac{n}{(n,k)} \Big/ \frac{k}{(n,k)} m$
$\left(\frac{n}{(n,k)}, \frac{k}{(n,k)}\right) = 1$
$\Big\}\ \frac{n}{(n,k)} \Big/ m$ (++)

Απο (+) και (++) : $m = O(a^k) = \frac{n}{(n,k)}$.

πχ

$(\mathbb{Z}_{12}, \oplus)$ Προσθεση

$O(\bar{1}) = 12$

$O(\bar{3}) = \bar{0}$, $\bar{3}+\bar{3}+\bar{3}+\bar{3}=\bar{0}$

$$O(\bar{1}+\bar{1}+\bar{1}) = \frac{O(\bar{1})}{(12,3)} = \frac{12}{3} = 4$$

ομοια,

$$O(\bar{5}) = \frac{O(\bar{1})}{(12,5)} = 12$$

$\mathbb{Z}_{12} = \langle \bar{5} \rangle$ αφου $(5,12)=1$