ΟΜΑΔΕΣ

Σημείωση. Χρήσιμο είναι ο αναγνώστης να έχει υπόψη του τα παρατιθέμενα στην ενότητα "Σύνολα", §7.

Βασικό παράδειγμα ομάδας με πεπερασμένο πλήθος στοιχεία, αποτελεί το σύνολο S_p των μεταθέσεων n στοιχείων. Ο ορισμός και οι ιδιότητες του συνόλου αυτού, έχουν ως εξής:

1. Μία ***μετάθεση*** (permutation) (ή ισοδύναμα, μετασχηματισμός (transformation)) είναι μία απεικόνιση ένα-ένα και επί $p : N \to N$, N τυχόν πεπερασμένο σύνολο.

Μία ***διάταξη,*** είναι η εικόνα μιάς μεταθέσεως. Θεωρούμε το σύνολο S_p των μεταθέσεων επί του N. Ορίζουμε το γινόμενο δύο διατάξεων από την παρακάτω σχέση. $\forall p_1, p_2 \in S_p$, $p_2 p_1 = p$, όπου p η μετάθεση επί του N, που ορίζεται από την σχέση, $\forall x \in N$, $p(x) = p_1(p_2(x))$. Η πράξη "γινόμενο" που ορίσαμε, συμπίπτει, βέβαια, με την σύνθεση των απεικονίσεων p_1 και p_2. Η δομή $(S_p, \cdot)$ αποτελεί χαρακτηριστικό παράδειγμα δομής που καλείται ***Ομάδα.***

Ουδέτερο στοιχείο της ομάδας αυτής, είναι η ταυτοτική μετάθεση $p_i \in S_p$, για την οποία ισχύει ότι $\forall x \in N$, $p_i(x) = x$.

Αν το σύνολο N έχει n το πλήθος στοιχεία $x_1, x_2, \cdots x_n$, όταν αυτό χρησιμοποιείται ως πεδίον ορισμού της p, το θέτουμε πάντα στην μορφή N = {1, 2, . . . , n}. Το σύνολο τιμών είναι τότε, το σύνολο p(N) = {p(1), p(2), . . . , p(n)} όπου το p(i) = j, με i, j∈N. Για να δηλώσουμε την μετάθεση p, χρησιμοποιούμε και τον συμβολισμό

$$p = \begin{pmatrix} 1 & 2 & \cdots & n \\ p(1) & p(2) & \cdots & p(n) \end{pmatrix}.$$

Το σύνολο p(N) είναι μία διάταξη του N. Φανερά, το σύνολο των διατάξεων, βρίσκεται σε αντιστοιχία ένα-ένα και επί, με το σύνολο των μεταθέσεων. Το σύνολο συνεπώς S_p έχει τόσα στοιχεία, όσες είναι οι διατάξεις των n αντικειμένων 1, 2, . . . , n. Το πλήθος αυτό, βρίσκεται ως εξής: Μία διάταξη προκύπτει, αν θεωρήσουμε ότι έχουμε n θέσεις, οι οποίες γεμίζονται μία προς μία από τα στοιχεία 1, 2, κλπ, ένα στοιχείο σε κάθε θέση. Η πρώτη θέση πληρούται κατά n διαφορετικούς τρόπους, η δεύτερη κατά n−1, κοκ, η n-στη κατά ένα τρόπο. Το πλήθος, λοιπόν, των διαφορετικών τρόπων με τους οποίους γεμίζουν οι n θέσεις είναι n(n−1) … 1 και συμβολίζεται με n!.

Κάνοντας χρήση του παραπάνω συμβολισμού για την μετάθεση p, μπορούμε πολύ εύκολα να βρούμε το γινόμενο δύο μεταθέσεων. για παράδειγμα, αν έχουμε να βρούμε το $p_1 p_2$, όπου

$$p_1 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \quad p_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad \text{γράφουμε,}$$

$$p_1 p_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \begin{pmatrix} 3 & 1 & 2 \\ 1 & 2 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}.$$

Στην γραφή αυτή $S_p \ni p_i = \begin{pmatrix} 1 & \cdots & n \\ 1 & \cdots & n \end{pmatrix}$, (ταυτοτική απεικόνιση = ουδέτερο ή μοναδιαίο στοιχείο) ενώ το αντίστροφο στοιχείο του $S_p \ni s = \begin{pmatrix} 1 & \cdots & n \\ s(1) & \cdots & s(n) \end{pmatrix}$ είναι το $\begin{pmatrix} s(1) & \cdots & s(n) \\ 1 & \cdots & n \end{pmatrix} = s^{-1}$.

Μία μετάθεση της μορφής $\begin{pmatrix} 1 & \cdots & n-1 & n \\ 2 & \cdots & n & 1 \end{pmatrix}$ καλείται ***κυκλική*** μετάθεση. Την κυκλική μετάθεση την συμβολίζουν $(1 \ \ldots \ n)$. Μία κυκλική μετάθεση, που ορίζεται σε ένα σύνολο δύο αντικειμένων, καλείται ***αντιμετάθεσις*** (transposition).

Με (k) συμβολίζουμε την απεικόνιση του k στον εαυτό του. Παράγοντες αυτής της μορφής, παραλείπονται.

Παράδειγμα. $(1 \ 2 \ 3 \ 4 \ 5)(2 \ 3 \ 5 \ 4) =$

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix}\begin{pmatrix} 2 & 3 & 5 & 4 \\ 3 & 5 & 4 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix}\begin{pmatrix} 2 & 3 & 4 & 5 & 1 \\ 3 & 5 & 2 & 4 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 2 & 4 & 1 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2 & 3 & 5 \\ 3 & 5 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 3 & 2 & 5 \\ 3 & 2 & 5 & 1 \end{pmatrix} = (1 \ 3 \ 2 \ 5)$$

Στις προτάσεις που ακολουθούν, αντί γενικής αποδείξεως, θα δίδουμε ένα παράδειγμα, μέσα από το οποίο θα γίνεται φανερός ο γενικός αλγόριθμος, που αποδεικνύει την πρόταση.

Πρόταση 1. Μία μετάθεση παρίσταται ως γινόμενο ***ανεξαρτήτων*** κυκλικών μεταθέσεων. (Ανεξαρτήτων σημαίνει ότι δεν έχουν κοινά στοιχεία).

Παράδειγμα. Είναι,

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 5 & 4 & 3 & 6 & 1 & 7 & 8 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 5 & 6 \\ 2 & 5 & 6 & 1 \end{pmatrix}\begin{pmatrix} 3 & 4 \\ 4 & 3 \end{pmatrix}\begin{pmatrix} 7 \\ 7 \end{pmatrix}\begin{pmatrix} 8 \\ 8 \end{pmatrix} = (1 \ 2 \ 5 \ 6)(3 \ 4)$$

Πρόταση 2. Δύο αντιμεταθέσεις, που δεν έχουν κοινό στοιχείο αντιμετατίθενται.

Παράδειγμα. Είναι $(1 \ 2)(3 \ 4) = (3 \ 4)(1 \ 2)$, μιά και

$$(1 \ 2)(3 \ 4) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix}\begin{pmatrix} 3 & 4 & 1 & 2 \\ 4 & 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix}\begin{pmatrix} 2 & 1 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$$

$$(3 \ 4)(1 \ 2) = \begin{pmatrix} 3 & 4 & 1 & 2 \\ 4 & 3 & 1 & 2 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{pmatrix}\begin{pmatrix} 1 & 2 & 4 & 3 \\ 2 & 1 & 4 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$$

Πρόταση 3. Κάθε κυκλική μετάθεση, παρίσταται ως γινόμενο ενός ελαχίστου αριθμού $n-1$ αντιμεταθέσεων.

Παράδειγμα. Είναι, $(1\ \ 2\ \ 3\ \ 4)=(4\ \ 3)(3\ \ 2)(2\ \ 1)$.

Επίσης, $(1\ \ 2\ \ 3\ \ 4)=(1\ \ 2)(1\ \ 3)(1\ \ 4)$. Βλέπουμε ότι, η παράσταση μιάς μεταθέσεως ως γινόμενο αντιμεταθέσεων, δεν είναι μοναδική. Το πλήθος όμως των παραγόντων στους οποίους αυτή αναλύεται, είναι το ολιγότερο n−1. Πράγματι, το πλήθος αυτό μπορεί να αυξηθεί, αν πολλαπλασιάσουμε το γινόμενο των n−1 παραγόντων από το ζεύγος των κυκλικών μεταθέσεων $(\nu\ \ \mu)(\nu\ \ \mu)$.

Πορίσματα. 1) Κάθε μετάθεση παρίσταται ως γινόμενο k−r αντιμεταθέσεων, κατ' ελάχιστον, όπου r είναι το πλήθος των ταυτοτικών κύκλων που περιέχει, και k το πλήθος των στοιχείων που μεταβάλλει. Π.χ. στην μετάθεση της προτάσεως 1, έχουμε, n = 8, r = 2 και k = 6.
Είναι πράγματι, $(1\ \ 2\ \ 5\ \ 6)(3\ \ 4)=(1\ \ 2)(1\ \ 5)(1\ \ 6)(3\ \ 4)$, 4 αντιμεταθέσεις σύμφωνα με τον κανόνα k−r = 6−2.

2) Μία μετάθεσις αναλύεται σε γινόμενο είτε αρτίου είτε περιττού πλήθους αντιμεταθέσεων.

3) Το πλήθος των αντιμεταθέσεων εις το οποίον αναλύεται μία μετάθεσις κατά την παραγοντοποίησή της, είναι k−r+2s, όπου s τυχόν φυσικός. Ακριβώς το ίδιο πλήθος παραγόντων έχει και η αντίστροφος αυτής μετάθεσις.

Ορισμός. ***Αρτία*** καλείται εκείνη η μετάθεσις (ή διάταξις), η οποία αναλύεται σε γινόμενο αρτίου πλήθους παραγόντων. ***Περιττή***, εκείνη η οποία αναλύεται σε γινόμενο περιττού πλήθους παραγόντων. Εξ' ορισμού, η ταυτοτική είναι πάντοτε αρτία.

4) Το σύνολο S_n περιέχει $\frac{n!}{2}$ άρτιες και $\frac{n!}{2}$ περιττές μεταθέσεις.

5) Μία κυκλική μετάθεση είναι αρτία ή περιττή ανάλογα με το αν το πλήθος των στοιχείων στα οποία αυτή δρα είναι περιττό ή άρτιο. Είναι π.χ. η $(1\ \ 2\ \ 3)=(1\ \ 2)(1\ \ 3)$ είναι αρτία μετάθεση. Αν μία μετάθεση είναι αρτία, τότε και η αντίστροφός της είναι αρτία. Επίσης, η ταυτοτική μετάθεσις, η οποία δεν δρα επί ουδενός στοιχείου, είναι αρτία.

Παράδειγμα. Να βρεθεί το είδος της διατάξεως $(2\ \ 1\ \ 3\ \ 5\ \ 6\ \ 4)$.

Λύση. Στη διάταξη αυτή, αντιστοιχεί η μετάθεση $\begin{pmatrix}1&2&3&4&5&6\\2&1&3&5&6&4\end{pmatrix}$. Την γράφουμε ως γινόμενο παραγόντων κυκλικών μεταθέσεων:

$$(1\ \ 2)(4\ \ 5\ \ 6)=(1\ \ 2)(4\ \ 5)(4\ \ 6).$$

Άρα είναι περιττή μετάθεση.

Το είδος μιάς μεταθέσεως, ευρίσκεται και από το πόσες φορές η μετάθεσή μας αλλάζει το πρόσημο του πολυωνύμου

$$\prod_{i<j}(x_i - x_j)=(x_1 - x_n)(x_2 - x_n)\ \cdots\ (x_{n-1} - x_n)$$
$$(x_1 - x_{n-1})\ \cdots\ (x_{n-2} - x_{n-1})$$
$$\ddots$$
$$(x_1 - x_2).$$

που έχει 1+2+ . . . +n = $\frac{n(n+1)}{2}$ παράγοντες.

Ετσι, π.χ. για την μετάθεση $(1\ \ 2\ \ 3)$, όταν αυτή δράση πάνω στους δείκτες του αρχικού πολυώνυμου $(x_1 - x_3)(x_2 - x_3)(x_1 - x_2)$ δίδει το
$(x_2 - x_1)(x_3 - x_1)(x_2 - x_3)$. Το πολυώνυμο που προκύπτει, ισούται με το αρχικό, μιά και αλλάζει δύο φορές πρόσημο. Συνεπώς η σημειούμενη μετάθεση, είναι αρτία.

2. Ορισμός ομάδος. ***Ομάδα*** G, καλείται μία ημιομάδα με μονάδα μέσα στην οποία, για δοσμένα $\alpha, \beta \in G$ οι εξισώσεις $\alpha x = \beta$ και $y\alpha = \beta$, έχουν μοναδική λύση $x, y \in G$.

Πορίσματα. i) $\alpha\beta_1 = \alpha\beta_2 \rightarrow \beta_1 = \beta_2$ και $\beta_1\alpha = \beta_2\alpha \rightarrow \beta_1 = \beta_2$. Τούτο έπεται από την μοναδικότητα των λύσεων $x, y \in G$. ii) Αν στις εξισώσεις $\alpha x = \beta$ και $y\alpha = \beta$ λάβουμε $\beta = e$, συμπεραίνουμε ότι, κάθε $\alpha \in G$ έχει αριστερά και δεξιά αντίστροφο στοιχείο.

Πρόταση. Η μονάδα μιάς ομάδας είναι μοναδική.
Απόδειξη. Από τον ορισμό της ομάδας έχουμε ότι, η εξίσωση $\alpha e_\alpha = \alpha$ έχει την μοναδική λύση e_α. Θα δείξουμε κατ' αρχήν, ότι το στοιχείο e_α δεν εξαρτάται από το συγκεκριμένο $\alpha \in G$. Προς τούτο, αν $\beta \in G$ και y το μοναδικό στοιχείο της G για το οποίο είναι $y\alpha = \beta$, τότε έχουμε και ότι, $\beta e_\alpha = (y\alpha)\, e_\alpha = y(\alpha e_\alpha) = y\alpha = \beta$. Αν το e_α είναι, λοιπόν, δεξιά μοναδιαίο στοιχείο για το $\alpha \in G$, είναι τότε και δεξιά μοναδιαίο στοιχείο για το $\beta \in G$. (Ίδια ισχύουν και για ένα αριστερά μοναδιαίο στοιχείο). Έστω, τώρα, τα μοναδικά e_1 και e_2, για τα οποία ισχύει για όλα τα $\alpha \in G$ ότι, $\alpha e_1 = \alpha$ και $e_2\alpha = \alpha$. Λαβαίνουμε ως α το γινόμενο $e_1 e_2$.
Είναι, τότε, $(e_1 e_2)e_1 = e_1 e_2$ και $e_2(e_1 e_2) = e_1 e_2$. Άρα και, $(e_1 e_2)e_1 = e_2(e_1 e_2)$.
Ή $(e_1 e_2)e_2 = e_1(e_1 e_2)$. Ή $e_2 e_2 = e_1$, e_1 ή $e_1 = e_2$.

Πρόταση. Κάθε στοιχείο $\alpha \in G$ έχει ένα και μόνον αντίστροφο στοιχείο α^{-1}.
Απόδειξη. Θα δείξουμε ότι, $\forall \alpha \in G, \exists!\ \alpha^{-1} \in G$: $\alpha\alpha^{-1} = \alpha^{-1}\alpha = e$. Από τον ορισμό της ομάδας, γνωρίζουμε ότι υπάρχουν μοναδικά α' και $\alpha'' \in G$ τέτοια ώστε, $\alpha\alpha' = e$ και $\alpha''\alpha = e$. Είναι, όμως, $\alpha''\alpha\alpha' = \alpha''(\alpha\alpha') = \alpha''e = \alpha''$ και $\alpha''\alpha\alpha' = (\alpha''\alpha)\alpha' = e\alpha' = \alpha'$.
Άρα $\alpha' = \alpha''$.

Πόρισμα. α) $\left(\alpha^{-1}\right)^{-1} = \alpha$. β) $e^{-1} = e$. γ) $(\alpha_1\alpha_2 \cdots \alpha_n)^{-1} = \alpha^{-1} \cdots \alpha_n^{-1}$ δ) Η αντιστοιχία $\alpha \mapsto \alpha^{-1}$ είναι ένα-ένα και επί.

Παράδειγμα. Θεωρούμε το σύνολο των αυτομορφισμών ενός συνόλου U. Φανερά, η σύνθεση δύο αυτομορφισμών του U είναι πάντοτε δυνατή. Ορίζεται λοιπόν μέσα στο σύνολο αυτό, μία εσωτερική πράξη, ο πολλαπλασιασμός δύο στοιχείων του. Μέσα στο σύνολο των αυτομορφισμών του U, συγκαταλέγεται και η ταυτοτική απεικόνιση $1_U : U \rightarrow U$, που ορίζεται από την σχέση, $\forall x \in U, 1_U(x) = x$. Στην περίπτωση, που ο αυτομορφισμός είναι μετάθεση f, υπάρχει και η αντίστροφή της f^{-1}. Το σύνολο συνεπώς των μεταθέσεων του U, με πράξη την σύνθεση, αποτελεί ομάδα.

Υποομάδα Η της G, είναι ένα υποσύνολο της G, τέτοιο ώστε, $\forall \alpha, \beta \in H$, $\alpha\beta \in H$ και $\forall \alpha \in H$, $\alpha^{-1} \in H$. ***Αντιμεταθετική*** ή ***Αβελιανή*** λέγεται η ομάς G, αν και μόνον αν, οι μοναδικές λύσεις $x, y \in G$ είναι και ίσες. Στην περίπτωση αυτή, $\forall \alpha, \beta \in G$, ισχύει ότι, $\alpha\beta = \beta\alpha$.

Σημειώσεις επί του συμβολισμού. Στην περίπτωση Αβελιανής ομάδας, σημειώνουμε πάντα την πράξη με το "+", το ουδέτερο στοιχείο με το "0" (μηδέν), και το αντίστροφο στοιχείο του α με το "−α" (αντίθετο). Γράφουμε α−β αντί του (σωστού) α+(−β). Αυτό είναι η μοναδική λύση $x \in R$ της εξίσωσης α+x = β. Φανερά, λόγω της αντιμεταθετικότητας της προσθέσεως, ισχύει ότι, $\alpha - (\beta_1 + \beta_2) = \alpha - \beta_1 - \beta_2$.
Αν η ομάς G είναι ισόμορφος (βλέπε ενότητα "Σύνολα" §6-7) της ομάδος H, θα γράφουμε $G \cong H$. Η σχέση $"\cong"$ είναι, φανερά, μία σχέση ισοδυναμίας (βλέπε ενότητα "Σύνολα" §5).

Θεώρημα του Cayley. Έστω a τυχόν στοιχείο της ομάδας G. Ορίζουμε την $\varphi_a : G \to G$ από την σχέση $\forall x \in G, \varphi_a(x) = ax \in G$. Η φ_a είναι ένα – ένα και επί
Απόδειξη. 1) Η φ_a είναι ένα – ένα. Πράγματι, αν για $x_1 \neq x_2, \varphi_a(x_1) = \varphi_a(x_2)$, τότε και $ax_1 = ax_2$, άτοπο. 2) $\forall g \in G, \exists x \in G : \varphi_a(x) = g$. Αρκεί να λάβουμε $x = a^{-1}g$. Στην πραγματικότητα η φ_a αποτελεί μία μετάθεση του G.
Το γεγονός ότι το σύνολο των μεταθέσεων αποτελεί ομάδα με ουδέτερο στοιχείο την ταυτοτική μετάθεση $\forall x \in G, \varphi_e(x) = ex = x \in G$ το γνωρίζουμε από ότι είπαμε στην προηγούμενη παράγραφο. Αν την ομάδα αυτή την καλέσουμε S_φ, τότε, θα δείξουμε ότι, $S_\varphi \cong G$. Πράγματι είναι,

$$\begin{array}{ccc} G \times G \ni (a,b) & \mapsto & ab \\ \varphi \downarrow & & \varphi \downarrow \\ S_\varphi \times S_\varphi \ni (\varphi_a, \varphi_b) & \mapsto & \forall x \in G,\ \varphi_a(\varphi_b) = abx = \varphi_{ab}(x) \end{array}$$

Έχουμε, λοιπόν, την σχέση $\varphi_a \varphi_b = \varphi_{ab}$ η οποία και αποδεικνύει τον σημειούμενο ισομορφισμό.

Υποομάδα Η μιάς ομάδας G, είναι ένα υποσύνολο $H \subseteq G$, το οποίο αποτελεί ομάδα με πράξη αυτήν, που καθιστά την G ομάδα. Αναγκαία και ικανή συνθήκη για να είναι το H υποομάδα της G, είναι αυτό να είναι κλειστό ως προς την εσωτερική του πράξη που το καθιστά ομάδα. Δηλαδή $\forall x_1, x_2 \in H, x_1 x_2 \in H$.
Για την υποομάδα H της G, έχουμε, φανερά, τις προτάσεις:
1) Οι ομάδες G και H έχουν το ίδιο μοναδιαίο στοιχείο e.
2) Αν $a \in H \subseteq G$, τότε και $a^{-1} \in H \subseteq G$.

3. Πράξεις με υποομάδες. Επειδή οι υποομάδες της ομάδας G είναι υποσύνολα της G, μπορούμε να θεωρούμε την τομή και την ένωσή τους. Σχετικά με τα σύνολα αυτά, έχουμε ότι: α) Φανερά, η τομή όλων των υποομάδων της G, είναι υποομάς της G. β) Η ένωση δύο υποομάδων της G δεν είναι πάντα υποομάς της G. Για παράδειγμα, έστω G η ομάς των ακεραίων $\mathbb{Z}$, με πράξη την "+". Τα σύνολα $H_\kappa = \{\kappa x \mid x \in \mathbb{Z}\}$, είναι υποομάδες της $\mathbb{Z}$. Η τομή $H_\kappa \cap H_\lambda$ είναι το σύνολο των ακεραίων H_μ, όπου $\mu = \kappa\lambda$, και είναι βέβαια και αυτό υποομάδα της $\mathbb{Z}$. Η ένωση όμως $H_\kappa \cup H_\lambda$ δεν είναι πάντα υποομάς της $\mathbb{Z}$, μιά και το στοιχείο $\kappa x + \lambda y \notin H_\kappa \cup H_\lambda$, στην περίπτωση, που $(\kappa, \lambda) = 1$.

Εκτός της ενώσεως και της τομής δύο συνόλων, έχουμε και το καρτεσιανό τους γινόμενο. Στην περίπτωση, που τα σύνολά μας είναι δύο ομάδες Α, Β, το ***εξωτερικό γινόμενό*** τους $A \times B$ είναι η ομάδα, που έχει πράξη την

$$(a_1, b_1)(a_2, b_2) = (a_1 a_2, b_1 b_2)\text{, όπου } a_1, a_2 \in A \text{ και } b_1, b_2 \in B .$$

Ισχύουν οι προτάσεις:

1) Το $A \times B$ περιέχει μν το πλήθος στοιχεία, αν το Α έχει μ και το Β ν στοιχεία.

2) Οι ομάδες $A \times B$ και $B \times A$ είναι ισόμορφες.

3) Το σύνολο των στοιχείων της μορφής (a, e) όπου $a \in A$ και $e \in B$ αποτελούν υποομάδα της $A \times B$. Το σύνολο των στοιχείων της μορφής (e, b) όπου $b \in B$ και $e \in A$ αποτελούν υποομάδα της $B \times A$.

4) Αν $A_1 \subseteq A$ και $B_1 \subseteq B$ υποομάδες των Α και Β, τότε και η $A_1 \times B_1$ υποομάς της $A \times B$.

Το ***γινόμενο*** (ή ***άθροισμα,*** ανάλογα με την πράξη της ομάδας), δύο υποομάδων Η και Κ της ομάδας G, ορίζεται ως το σύνολο $HK = \{hk \mid h \in H \text{ και } k \in K\}$. (Ανάλογα ορίζουμε το $H + K$).

Πρόταση. Το γινόμενο δύο υποομάδων Η και Κ της ομάδας G είναι ομάς, αν και μόνον αν $HK = KH$.

Απόδειξη. α) Έστω ότι ΗΚ ομάς. Θα πρέπει να δείξουμε ότι

$\forall h \in H$ και $\forall k \in K$, $hk = kh$. Πράγματι, $h^{-1}k^{-1} \in HK$, άρα και $\left(h^{-1}k^{-1}\right)^{-1} \in HK$, δηλαδή, $kh \in HK$, απ' όπου $KH \subseteq HK$. Ανάλογα έχουμε και την $KH \supseteq HK$.

β) Έστω ότι, $HK = KH$. Θα δείξουμε, τότε, ότι το γινόμενο ΗΚ είναι ομάς. Πράγματι, το γινόμενο δύο στοιχείων h_1k_1 και h_2k_2 του ΗΚ είναι και πάλι εν ΗΚ, μιά και $(h_1k_1)(h_2k_2) = (h_1h_2)(k_1k_2)$. Εξ' άλλου, αν $hk \in HK$, τότε είναι και

$$(hk)^{-1} = k^{-1}h^{-1} \in KH = HK .$$

Παρατήρηση. Το $H + K$ είναι πάντα υποομάδα της G.

Με $o(H)$ συμβολίζουν το πλήθος των στοιχείων ενός συνόλου Η. Στην περίπτωση, που το σύνολο αυτό είναι ομάδα, ο φυσικός αυτός αριθμός, καλείται ***τάξις*** της ομάδος.

Θα ασχοληθούμε με ομάδες πεπερασμένης τάξεως.

Πρόταση. Για το σύνολο ΗΚ, ισχύει ότι, $o(HK) = \dfrac{o(H)o(K)}{o(H \cap K)}$.

Απόδειξη. Κατ' αρχήν παρατηρούμε ότι, αν $H \cap K = \{e\}$ τότε όλα τα στοιχεία του συνόλου ΗΚ είναι μεταξύ τους διαφορετικά. Πράγματι, αν $h_1k_1 = h_2k_2$, όπου τα στοιχεία h και k δεν είναι το e, τότε, και, $h_2^{-1}h_1 = k_2k_1^{-1}$, πράγμα άτοπο. Στην περίπτωση, λοιπόν, αυτή, η προς απόδειξη ισότητα ισχύει, υπό την μορφή $o(HK) = o(H)o(K)$.

Έστω, τώρα, $H \cap K \neq \{e\}$. Τότε, $h_2^{-1}h_1 = k_2k_1^{-1}$ ανν $h_1k_1 = h_2k_2 = z \in H \cap K$. Κάθε, λοιπόν, $z \in H \cap K$, συμβάλει στην καταμέτρηση του πλήθους $o(H)o(K)$ με στοιχεία της μορφής zk, όλα ίδια, αν και μόνον αν, $k \in H \cap K$, δηλαδή, με $o(H \cap K)$ το πλήθος. Κάθε ένα συνεπώς $z \in H \cap K$ συμβάλει στον υπολογισμό του αριθμού

$o(H)o(K)$ με $o(H\cap K)$ ίδια στοιχεία. Τα διαφορετικά, λοιπόν, στοιχεία του HK είναι, $o(H)o(K)/o(H\cap K)$.

Εφαρμογή. Έστω οι υποομάδες H και K της ομάδας G με $o(H)>\sqrt{o(G)}$, $o(K)>\sqrt{o(G)}$. Εξ΄ άλλου, επειδή $HK\subseteq G$, $o(HK)\le o(G)$. Είναι, τότε,

$$o(G)\ge o(HK)=\frac{o(H)o(K)}{o(H\cap K)}>\frac{\sqrt{o(G)}\sqrt{o(G)}}{o(H\cap K)}=\frac{o(G)}{o(H\cap K)}.$$

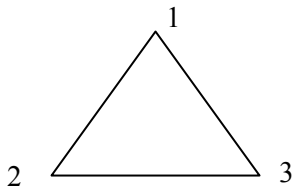
Άρα και $o(H\cap K)>1$, δηλαδή, $H\cap K\neq\{e\}$.

4. Οι συμμετρικές ομάδες S_i, $1\le i\le 4$**.** Κατά τον Herman Weyl, συμμετρία είναι εκείνη η πράξις, η οποία ενεργουμένη επί ενός αντικειμένου, αφίνει αυτό, κατά κάποια έννοια, αναλλοίωτο.

Η S_1 περιέχει όλες τις διατάξεις, που μπορούμε να επιτύχουμε διατάσοντας ένα αντικείμενο. Από την διάταξη {1}, ουδεμία άλλη προκείπτει. Η S_1 περιέχει συνεπώς, μόνον την ταυτοτική μετάθεση.

Η S_2 περιέχει τις διατάξεις {1, 2} και {2, 1}. Η πρώτη, προέρχεται από την ταυτοτική μετάθεση $\begin{pmatrix}1&2\\1&2\end{pmatrix}$, και η δεύτερη, από την $\begin{pmatrix}1&2\\2&1\end{pmatrix}$, που είναι η αντιμετάθεση $(1\quad 2)$. Ισχύει ότι, $\begin{pmatrix}1&2\\2&1\end{pmatrix}\begin{pmatrix}1&2\\2&1\end{pmatrix}=\begin{pmatrix}1&2\\2&1\end{pmatrix}\begin{pmatrix}2&1\\1&2\end{pmatrix}=\begin{pmatrix}1&2\\1&2\end{pmatrix}$, και συνεπώς, αντίστροφο στοιχείο του $(1\quad 2)$ είναι το $(1\quad 2)$. Η $(1\quad 2)$ είναι περιττή μετάθεσις. Η υποομάδα A_2 των αρτίων μεταθέσεων της S_2, περιέχει μόνον την ταυτοτική μετάθεση. Αν τα αντικείμενα 1 και 2 ήταν τα άκρα ενός ευθυγράμμου τμήματος, η δράση της S_2 πάνω σ' αυτό, συνίσταται σε μία συμμετρία του ευθυγράμμου αυτού τμήματος, ως προς το μέσον του.
Τα στοιχειώδη συμμετρικά πολυώνυμα $\sigma(x_1,x_2)$ είναι τα $\sigma_1=x_1+x_2$, $\sigma_2=x_1x_2$. Η S_2, όταν ενεργεί πάνω στους δείκτες των x, αφίνει αυτά αναλλοίωτα.

Η S_3 περιέχει τις 3! διατάξεις τριών αντικειμένων. Οι 6 αυτές διατάξεις, αποτελούνται από τις: α) Την ταυτοτική (δεν έχουμε δράση επί ουδενός αντικειμένου). β) Αυτές που δεν έχουμε δράση επί ενός αντικειμένου. γ) Αυτές που δρούν επί όλων των αντικειμένων.
Αν τα αντικείμενά μου ήταν κορυφές ισοπλεύρου τριγώνου, η κατηγορία β), θα άφηνε μία κορυφή στην θέση της, και θα άλλαζε τις άλλες δύο. Περιλαμβάνει συνεπώς, τις συμμετρίες (= κατοπτρισμοί) ως προς την μεσοκάθετο. Η κατηγορία γ), περιλαμβάνει τις στροφές του τριγώνου κατά 120^o και 240^o. Έχουμε, συνεπώς, τις μεταθέσεις:



α) $\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}$, β) $\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}$ $\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}$ $\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}$,

και γ) $\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$ $\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$.

Άρτιες είναι, η α) και οι γ). Αυτές και αποτελούν την υποομάδα A_3 της S_3. Πράγματι, παρατηρούμε ότι, $\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}\begin{pmatrix}2&3&1\\1&2&3\end{pmatrix}=\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}$. Η υποομάδα αυτή, είναι και Αβελιανή. Αν καλέσουμε p_0 την ταυτοτική και p_1, p_2 τις άλλες δύο, όπου $p_0 \neq p_1 \neq p_2$ και $p_2 = p_1^{-1}$, που αντιστοιχούν στις στροφές του τριγώνου κατά 120^o και 240^o, μπορούμε να σχηματίσουμε των πολλαπλασιαστικό πίνακα της υποομάδας αυτής, που είναι ο παρακάτω.

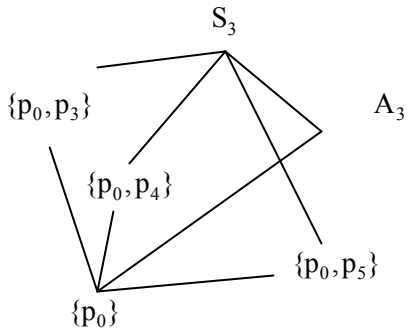
	$\mathbf{p_0}$	$\mathbf{p_1}$	$\mathbf{p_2}$
$\mathbf{p_0}$	p_0	p_1	p_2
$\mathbf{p_1}$	p_1	p_2	p_0
$\mathbf{p_2}$	p_2	p_0	p_1

Από τον πίνακα αυτόν, έχουμε και τις εξισώσεις που ορίζουν την ομάδα αυτήν (και αντίστροφα):
$p_0p_i = p_ip_0 = p_i$ $(i = 1, 2)$ και
$p_1p_2 = p_2p_1 = p_0$, $p_ip_i = p_j$ $(i, j = 1, 2, i \neq j)$. Ή ακόμα,
$p_ip_j = p_k$, όπου $k = (i + j)(\mathrm{mod}\,3)$, με $0 \leq i, j \leq 2$.

Ο πίνακας αυτός, αποτελεί μέρος του πολλαπλασιαστικού πίνακα της ομάδας S_3, που είναι:

	$\mathbf{p_0}$	$\mathbf{p_1}$	$\mathbf{p_2}$	$\mathbf{p_3}$	$\mathbf{p_4}$	$\mathbf{p_5}$
$\mathbf{p_0}$	p_0	p_1	p_2	p_3	p_4	p_5
$\mathbf{p_1}$	p_1	p_2	p_0	p_4	p_5	p_3
$\mathbf{p_2}$	p_2	p_0	p_1	p_5	p_3	p_4
$\mathbf{p_3}$	p_3	p_5	p_4	p_0	p_2	p_1
$\mathbf{p_4}$	p_4	p_3	p_5	p_1	p_0	p_2
$\mathbf{p_5}$	p_5	p_4	p_3	p_2	p_1	p_0

Εδώ, η p_3 διατειρεί την κορυφή 1, η p_4 την κορυφή 2, και η p_5 την κορυφή 3.
Από μία επισκόπιση του πίνακα αυτού, έχουμε τα συμπεράσματα.
α) Η S_3 δεν είναι Αβελιανή. Π.χ., $p_2p_3 \neq p_3p_2$.
β) Εκτός από τις υποομάδες $\{p_0\}$ και $A_3 = \{p_0, p_1, p_2\}$, που είναι και αντιμεταθετική (Αβελιανή) έχουμε και τις υποομάδες $\{p_0, p_3\}$, $\{p_0, p_4\}$, $\{p_0, p_5\}$. Αν διατάξουμε ως προς "$\subseteq$" το σύνολο των υποομάδων της S_3, θα έχουμε το παρακάτω διάγραμμα του Hasse (βλέπε §6):



Τα στοιχειώδη συμμετρικά πολυώνυμα $\sigma(x_1, x_2, x_3)$ είναι τα
$\sigma_1 = x_1 + x_2 + x_3$,
$\sigma_2 = x_1x_2 + x_1x_3 + x_2x_3$ και $\sigma_3 = x_1x_2x_3$.
Η δράση της S_3 πάνω στους δείκτες των x, αφίνει αυτά αναλλοίωτα.
Αναλλοίωτο αφίνει επίσης το πολυώνυμο

$$\prod_{i<j}(x_i - x_j) = (x_1 - x_2)(x_1 - x_3)(x_2 - x_3)$$

η δράση της A_3, ενώ οι άλλες τρείς υποομάδες, που προκαλούν κάποια δράση στους δείκτες, αλλάζουν το πρόσημο του πολυωνύμου. Αν θεωρήσουμε τις τρείς ρίζες της

μονάδος, 1, ω, ω^2 (βλέπε §20), παρατηρούμε ότι, η αντιστοιχία $p_0 \to 1$, $p_1 \to \omega$, $p_2 \to \omega^2$, είναι ισομορφισμός.
Επίσης, σε κάθε στοιχείο της ομάδας S_3, είναι δυνατόν να αντιστοιχίσουμε έναν 2×2 πίνακα, έτσι ώστε, το σύνολο των 6 αυτών πινάκων με πράξη τον πολλαπλασιασμό τους, να αποτελεί ομάδα ισόμορφο της S_3. Η αντιστοιχία αυτή, δίδεται παρακάτω:

$$p_0 \to \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},\ p_1 \to \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix},\ p_2 \to \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix},$$
$$p_3 \to \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},\ p_4 \to \begin{pmatrix} -1 & 0 \\ -1 & 1 \end{pmatrix},\ p_5 \to \begin{pmatrix} 1 & -1 \\ 0 & -1 \end{pmatrix}.$$

Ο ισομορφισμός αυτός, δεν επάγεται από τον ισομορφισμό που έχουμε ανάμεσα στους 2×2 πίνακες και στους μιγαδικούς αριθμούς (βλέπε §22).
Παρατηρούμε εξ' άλλου, ότι και οι 6 πίνακες

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},\ \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix},\ \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix},\ \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix},\ \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix},\ \begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix}$$

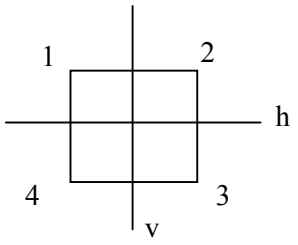
αποτελούν και αυτοί πολλαπλασιαστική ομάδα G_6, πλην όμως, αυτοί δεν είναι ισόμορφος με την προηγούμενη. Είναι όμως ισόμορφη, με την ομάδα των εξ ριζών της μονάδος.

Ερχόμαστε, τέλος στην S_4. Η S_4 περιέχει τις 4! διατάξεις τεσσάρων αντικειμένων. Οι 24 αυτές διατάξεις, προκύπτουν από τις 6 διατάξεις του S_3, αν σε από κάθε μία διάταξη του S_3, λάβουμε 4 διατάξεις του S_4, κατά τον ακόλουθο τρόπο: Από την ταυτοτική π.χ. διάταξη $(1\ 2\ 3)$, λαβαίνουμε 4 διατάξεις $(1\ 2\ 3\ 4)$, $(1\ 2\ 4\ 3)$, $(1\ 4\ 2\ 3)$, και $(4\ 1\ 2\ 3)$, και συνεπώς τις μεταθέσεις, που αντιστοιχούν σ' αυτές, που είναι, αντίστοιχα,

οι $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$. Από όλες αυτές τις 24 μεταθέσεις του S_4, ξεχορίζουμε αυτές, που συνδέονται με τις συμμετρίες του τετραγώνου, και οι οποίες είναι οι εξής 8, και οι οποίες αποτελούν την ομάδα G: α) Την ταυτοτική (δεν έχουμε δράση επί ουδεμιάς κορυφής του τετραγώνου). Η κατηγορία β), που περιλαμβάνει τις συμμετρίες ως προς τις μεσοκαθέτους (2) και τις διαγώνιες (2) του τετραγώνου, και περιλαμβάνει, 4 το πλήθος μεταθέσεις. Τέλος, η κατηγορία γ) περιλαμβάνει τις στροφές του τετραγώνου κατά $k90^o$, k = 1, 2, 3 και συνεπώς, έχουμε 3 ακόμα διατάξεις. Αν συμβολίσουμε με p_0 την ταυτοτική, p_h, p_v, την συμμετρία ως προς την οριζόντιο, και την κατακόρυφο μεσοκάθετο αντίστοιχα, που είναι οι

$$p_h = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} \text{ και } p_v = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$$

και με p_a, p_b τους κατοπτρισμούς ως προς τις διαγώνιες 1, 3 και 2, 4, αντίστοιχα, που αναλυτικά είναι οι



$$p_a = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix} \text{ και } p_b = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix},$$

και, τέλος, αν συμβολίσουμε με p_1, p_2, p_3 τις στροφές κατά 90^o, 180^o, και 270^o, και, που αναλυτικά είναι οι $p_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$, $p_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$ και $p_3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$, και, τέλος, με $p_0 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$ την στροφή κατά 0^0, μπορούμε να κατασκευάσουμε τον πολλαπλασιαστικό πίνακα της ομάδος των συμμετριών του τετραγώνου:

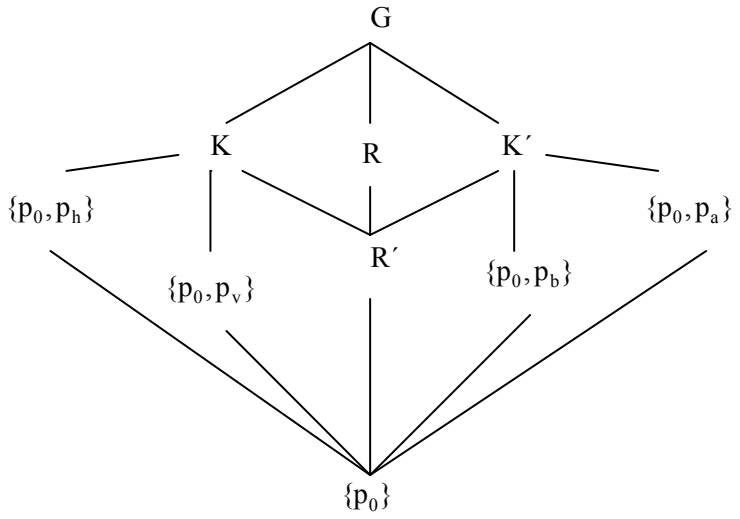
	$\mathbf{p_0}$	$\mathbf{p_1}$	$\mathbf{p_2}$	$\mathbf{p_3}$	$\mathbf{p_h}$	$\mathbf{p_v}$	$\mathbf{p_a}$	$\mathbf{p_b}$
$\mathbf{p_0}$	p_0	p_1	p_2	p_3	p_h	p_v	p_a	p_b
$\mathbf{p_1}$	p_1	p_2	p_3	p_0	p_a	p_b	p_v	p_h
$\mathbf{p_2}$	p_2	p_3	p_0	p_1	p_v	p_h	p_b	p_a
$\mathbf{p_3}$	p_3	p_0	p_1	p_2	p_b	p_a	p_h	p_v
$\mathbf{p_h}$	p_h	p_b	p_v	p_a	p_0	p_2	p_3	p_1
$\mathbf{p_v}$	p_v	p_a	p_h	p_b	p_2	p_0	p_1	p_3
$\mathbf{p_a}$	p_a	p_h	p_b	p_v	p_1	p_3	p_0	p_2
$\mathbf{p_b}$	p_b	p_v	p_a	p_h	p_3	p_1	p_2	p_0

Από μία επισκόπιση του δίπλα πίνακα, προκύπτει ότι έχουμε τις εξής υποομάδες (εκτός της $\{p_0\}$):

α) Η ομάδα

$R = \{p_0, p_1, p_2, p_3\}$

των περιστροφών του τετραγώνου κατά γωνία π/2. Η R είναι Αβελιανή, και ορίζεται από τις εξισώσεις $p_i p_j = p_k$, όπου $k = (i + j)(\mathrm{mod}\, 4)$, $0 \le i, j \le 3$ Η R περιέχει ως υποομάδα την $R' = \{p_0, p_2\}$ που είναι η ομάδα των περιστροφών του τετραγώνου, κατά γωνία π. Η R′ είναι Αβελιανή, και ορίζεται από τις εξισώσεις $p_i p_j = p_k$, όπου $k = (i + j)(\mathrm{mod}\, 2)$, i, j = 0,2. β) Οι υποομάδες $K = \{p_0, p_h, p_v, p_2\}$ (κατοπτρισμοί ως προς τις μεσοκαθέτους, περιστροφή κατά γωνία π) και $K' = \{p_0, p_a, p_b, p_2\}$ (κατοπτρισμοί ως προς τις διαγώνιες, περιστροφή κατά γωνία π). Η K περιέχει τις υποομάδες $\{p_0, p_h\}$, $\{p_0, p_v\}$ και η K′ τις $\{p_0, p_a\}$ και $\{p_0, p_b\}$. Αν διατάξουμε ως προς "$\subseteq$" το σύνολο των υποομάδων της G, λαβαίνουμε το σημειούμενο παρακάτω διάγραμμα.



Οι υπόλοιπες 16 μεταθέσεις της ομάδας S_4 είναι οι

$$\sigma_1=\begin{pmatrix}1&2&3&4\\2&3&4&1\end{pmatrix}\quad \sigma_3=\begin{pmatrix}1&2&3&4\\4&1&2&3\end{pmatrix}\quad \sigma_7=\begin{pmatrix}1&2&3&4\\3&4&2&1\end{pmatrix}\quad \sigma_9=\begin{pmatrix}1&2&3&4\\4&3&1&2\end{pmatrix}$$

$$\tau_1=\begin{pmatrix}1&2&3&4\\1&3&4&2\end{pmatrix}\quad \tau_2=\begin{pmatrix}1&2&3&4\\1&4&2&3\end{pmatrix}\quad \tau_3=\begin{pmatrix}1&2&3&4\\3&2&4&1\end{pmatrix}\quad \tau_4=\begin{pmatrix}1&2&3&4\\4&2&1&3\end{pmatrix}$$

$$\tau_5=\begin{pmatrix}1&2&3&4\\2&4&3&1\end{pmatrix}\quad \tau_6=\begin{pmatrix}1&2&3&4\\4&1&3&2\end{pmatrix}\quad \tau_7=\begin{pmatrix}1&2&3&4\\2&3&1&4\end{pmatrix}\quad \tau_8=\begin{pmatrix}1&2&3&4\\3&1&2&4\end{pmatrix}$$

$$\alpha_1=\begin{pmatrix}1&2&3&4\\2&1&3&4\end{pmatrix}\quad \alpha_2=\begin{pmatrix}1&2&3&4\\3&2&1&4\end{pmatrix}\quad \alpha_5=\begin{pmatrix}1&2&3&4\\1&4&3&2\end{pmatrix}\quad \alpha_6=\begin{pmatrix}1&2&3&4\\1&2&4&3\end{pmatrix}$$

Οι άρτιες μεταθέσεις που αποτελούν την ομάδα A_4, είναι οι p_0, p_h, p_2, p_v, τ_i, $1\le i\le 8$.
Ο πολλαπλασιαστικός πίνακας της A_4 είναι ο

	$\mathbf{p_0}$	$\mathbf{p_h}$	$\mathbf{p_2}$	$\mathbf{p_v}$	$\boldsymbol{\tau_1}$	$\boldsymbol{\tau_2}$	$\boldsymbol{\tau_3}$	$\boldsymbol{\tau_4}$	$\boldsymbol{\tau_5}$	$\boldsymbol{\tau_6}$	$\boldsymbol{\tau_7}$	$\boldsymbol{\tau_8}$
$\mathbf{p_0}$	p_0	p_h	p_2	p_v	τ_1	τ_2	τ_3	τ_4	τ_5	τ_6	τ_7	τ_8
$\mathbf{p_h}$	p_h	p_0	p_v	p_2	τ_4	τ_7	τ_6	τ_1	τ_8	τ_3	τ_2	τ_5
$\mathbf{p_2}$	p_2	p_v	p_0	p_h	τ_5	τ_3	τ_2	τ_8	τ_1	τ_7	τ_6	τ_4
$\mathbf{p_v}$	p_v	p_2	p_h	p_0	τ_8	τ_6	τ_7	τ_5	τ_4	τ_2	τ_3	τ_1
$\boldsymbol{\tau_1}$	τ_1	τ_8	τ_4	τ_5	τ_2	p_0	p_h	τ_6	τ_7	p_2	p_v	τ_3
$\boldsymbol{\tau_2}$	τ_2	τ_3	τ_6	τ_7	p_0	τ_1	τ_8	p_2	p_v	τ_4	τ_5	p_h
$\boldsymbol{\tau_3}$	τ_3	τ_2	τ_7	τ_6	p_2	τ_5	τ_4	p_0	p_h	τ_8	τ_1	p_v
$\boldsymbol{\tau_4}$	τ_4	τ_5	τ_1	τ_8	τ_7	p_h	p_0	τ_3	τ_2	p_v	p_2	τ_6
$\boldsymbol{\tau_5}$	τ_5	τ_4	τ_8	τ_1	τ_3	p_2	p_v	τ_7	τ_6	p_0	p_h	τ_2
$\boldsymbol{\tau_6}$	τ_6	τ_7	τ_2	τ_3	p_v	τ_8	τ_1	p_h	p_0	τ_5	τ_4	p_2
$\boldsymbol{\tau_7}$	τ_7	τ_6	τ_3	τ_2	p_h	τ_4	τ_5	p_v	p_2	τ_1	τ_8	p_0
$\boldsymbol{\tau_8}$	τ_8	τ_1	τ_5	τ_4	τ_6	p_v	p_2	τ_2	τ_3	p_h	p_0	τ_7

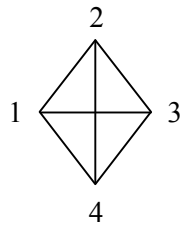
Μία επισκόπιση του παραπάνω πίνακα, μας αποκαλύπτει τις υποομάδες της ομάδας A_4:
Δύο υποομάδες τάξεως 2, οι $\{p_0,p_h\}$, $\{p_0,p_v\}$, δύο υποομάδα τάξεως 3, που είναι οι $\{p_0,p_h,p_2\}$, $\{p_0,p_v,p_2\}$, και μιά ομάδα τάξεως 4, που είναι η $\{p_0,p_v,p_2,p_h\}$.

5. Η ομάδα του Klein. Στην παράγραφο αυτή, θα δόσουμε ένα παράδειγμα ομάδος με 4 στοιχεία, και την οποία θα ορίσουμε με εξισώσεις. Αν $V=\{a_0,a_1,a_2,a_3\}$, ορίζουμε τις σχέσεις:

	$\mathbf{a_0}$	$\mathbf{a_1}$	$\mathbf{a_2}$	$\mathbf{a_3}$
$\mathbf{a_0}$	a_0	a_1	a_2	a_3
$\mathbf{a_1}$	a_1	a_0	a_3	a_2
$\mathbf{a_2}$	a_2	a_3	a_0	a_1
$\mathbf{a_3}$	a_3	a_2	a_1	a_0

$$a_0a_i=a_ia_0=a_i,\ 0\le i\le 3,$$
$a_ia_i=a_0,\ 1\le i\le 3$, και, τέλος, $a_ia_j=a_ja_i=a_k$, όπου $i\ne j\ne k,\ 1\le i,j,k\le 3$. Η ομάδα του Klein

είναι Αβελιανή, και έχει τον παραπλεύρως πολλαπλασιαστικό πίνακα.
Η ομάδα του Klein συνδέεται με τις συμμετρίες του ρόμβου.



Είναι, $a_0 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$, η ταυτοτική.

$a_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}$ και $a_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 1 \end{pmatrix}$

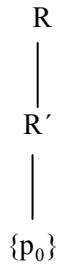
κατοπτρισμοί ως προς

την κατακόρυφο και την οριζόντιο διαγώνιο.

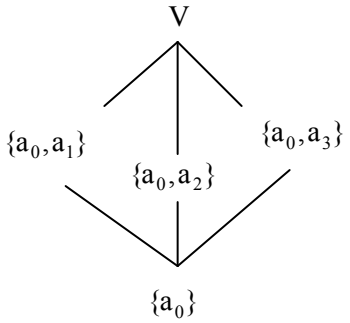
$a_3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$ περιστροφή κατά γωνία π.

Παρατηρούμε ότι, οι περιστροφές του τετραγώνου, που δίδονται από την ομάδα R της προηγούμενης παραγράφου, δεν είναι ισόμορφος με την ομάδα του Klein. Τούτο φαίνεται αμέσως, από μιά σύγκριση των διαγραμμάτων του Hasse που αντιστοιχούν στις δύο αυτές ομάδες:

Διάγραμμα υποομάδων
της ομάδος περιστροφής R
του τετραγώνου



Διάγραμμα υποομάδων
της ομάδος του Klein



Σημείωση. Αναφερόμεθα πάντοτε σε ομάδες με πεπερασμένο πλήθος στοιχείων.

6. Κυκλικές ομάδες. Θεωρούμε πάλι την ομάδα $G = \{a_1, a_2, \ldots, a_n\}$, και σχηματίζουμε τις δυνάμεις a_i^k του στοιχείου $a_i \in G$. Φανερά, $\exists a_j \in G$, με $a_j = a_i^k$. Αν τύχει να συμβεί και $a_j = a_i^m$, τότε και $a_i^k = a_i^m$ ή $a_i^{m-k} = a_i^0$. Το στοιχείο όμως αυτό, δρα ως μοναδιαίο στοιχείο e στο σύνολο H των δυνάμεων του a_i, και, επειδή, η G έχει ένα και μόνο μοναδιαίο στοιχείο, αυτό είναι το $a_i^{m-k} = a_i^0$. Ο εκθέτης εκείνος λ, για τον οποίο έχουμε $a_i^\lambda = e$, ενώ $\forall \mu < \lambda$, $a_i^\mu \neq e$, καλείται ***τάξις*** του στοιχείου $a_i = a$. Το σύνολο $(a) = \{a, a^2, \ldots, a^\lambda\}$, $a^\lambda = a^{o(a)} = e$ αποτελεί φανερά υποομάδα της G τάξεως λ. Η ομάδα αυτή, καλείται ***κυκλική υποομάδα,*** που ***παράγεται*** από το στοιχείο $a \in G$. Στην περίπτωση, που $o(a) = o(G)$, η G είναι κυκλική ομάς, παραγόμενη από το στοιχείο $a \in G$.
Συναντήσαμε τις κυκλικές ομάδες στις περιπτώσεις των n ριζών της μονάδος, βλέπε §20, και στις ομάδες περιστροφών του τριγώνου και του τετραγώνου.

Πρόταση. Θεωρούμε την κυκλική ομάδα G, που παράγεται από το στοιχείο a, και έχει τάξη $o(G) = n$. Τότε $a^m = e$ αν και μόνον αν $m = \mu n$ όπου $\mu \in \mathbb{Z}$.
Απόδειξη. Έστω $m = \mu n + \upsilon$, όπου $0 \le \upsilon \le n-1$. Άρα και $a^{\mu n+\upsilon} = a^{\mu n}a^{\upsilon} = e$, αν και μόνον αν $\upsilon = 0$.

Πόρισμα. Στην περίπτωση που ο $n = p$, p πρώτος, τότε, για τον τυχόντα ακέραιο $m \in \mathbb{Z}$ ισχύει ότι είτε $a^m = e$, είτε $o(a^m) = p$.

Πρόταση. Μία κυκλική ομάς είναι πάντοτε Αβελιανή, μιά και για κάθε δύο στοιχεία της a^{μ} και a^{ν} ισχύει ότι, $a^{\mu}a^{\nu} = a^{\mu+\nu} = a^{\nu+\mu} = a^{\nu}a^{\mu}$.

Πρόταση. Η υποομάδα μιάς κυκλικής ομάδας είναι κυκλική.
Απόδειξη. Έστω $G = \{a, a^2, \ldots, a^n\}$ η κυκλική μου ομάς, και H μία υποομάς της G. Έστω το $a^m \in H$, με m τον μικρότερο θετικό εκθέτη για τον οποίο $a^m \in H$. Θα δείξουμε ότι το τυχόν $b \in H$ έχει την μορφή $a^{\mu m}$. Το b ως στοιχείο της G, έχει την μορφή $b = a^s$. Επειδή είναι και $b \in H$, $m \le s$. Άρα, $s = \mu m + \upsilon$, με $0 \le \upsilon < \mu$. Είναι, λοιπόν, $a^s = a^{\mu m}a^{\upsilon} \in H$, άρα, και $a^{\upsilon} \in H$. Αναγκαστικά είναι, λοιπόν, $\upsilon = 0$.

Παρατήρηση. Κυκλικές είναι και όλες οι προσθετικές (= Αβελιανές) ομάδες $\mathbb{Z}_n$ (βλέπε §16) μιά και, $kn = 0(\mathrm{mod}\, n)$, $\mathbb{Z}_n = \{(1)_n, (2)_n, \ldots, (n-1)_n, (0)_n\}$.
Η $\mathbb{Z}_n$ είναι ισόμορφος προς την πολλαπλασιαστική ομάδα των 2×2 πινάκων

$$\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}, \begin{pmatrix}1 & 2\\ 0 & 1\end{pmatrix}, \begin{pmatrix}1 & 3\\ 0 & 1\end{pmatrix}, \ldots, \begin{pmatrix}1 & n-1\\ 0 & 1\end{pmatrix}, \begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}$$

όπου ο πολλαπλασιασμός των πινάκων γίνεται mod n.

Πρόταση. Αν $(m,n) = 1$, τότε η $\mathbb{Z}_m \times \mathbb{Z}_n$ κυκλική ομάς, ισόμορφος της $\mathbb{Z}_{mn}$.
Απόδειξη. Είναι, $\mathbb{Z}_m \times \mathbb{Z}_n = \{((\mu)_m, (\nu)_n) \,|\, (\mu)_m \in \mathbb{Z}_m,\ (\nu)_n \in \mathbb{Z}_n\}$. Το στοιχείο $((0)_{mn}, (0)_{nm})$ είναι το μηδενικό στοιχείο της ομάδας $\mathbb{Z}_m \times \mathbb{Z}_n$, η οποία παράγεται από το $((1)_m, (1)_n)$. Η αντιστοιχία $((1)_m, (1)_n) \mapsto (1)_{mn}$ παρέχει τον ζητούμενο ισομορφισμό.

7. Θεώρημα του Lagrange. Αν H υποομάδα της ομάδας G, τότε, $o(H) \,|\, o(G)$.
Απόδειξη. Έστω η ομάδα $G = \{e, x_2, \ldots, x_n\}$, τάξεως n, όπου $x_i \ne x_j$, για $i \ne j$.
$H = \{e, h_2, \ldots, h_r\}$ υποομάδα της, τάξεως r. Θεωρούμε τα γινόμενα

ee	h_2e	h_3e	$\ldots$	h_re
ea_2	h_2a_2	h_3a_2	$\ldots$	h_ra_2
ea_3	h_2a_3	h_3a_3	$\ldots$	h_ra_3
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
ea_k	h_2a_k	h_3a_k	$\ldots$	h_ra_k

ha, όπου το στοιχείο $a \in G$, $a \notin H$, $a \ne e$, που εμφανίζεται στην i γραμμή, δεν εμφανίζεται στην $i+1$ γραμμή. Ο πίνακας αυτός, περιέχει kr διαφορετικά στοιχεία. Πράγματι, αν $h_ja_i = h_{j'}a_{i'}$, τότε και $h_j = h_{j'}a_ia_i^{-1} \in H$. Όμως, η H υποομάδα. Άρα, $a_ia_i^{-1} \in H$. Τούτο όμως είναι, άτοπο, μιά και $a \notin H$. Εξ' άλλου, στον πίνακα αυτό, αναγράφονται όλα τα στοιχεία της ομάδας G. Άρα $n = kr$, ή $r \,|\, n$, όπως θέλαμε να δείξουμε.

Παρατήρηση. Ο παραπάνω πίνακας, αποτελεί έναν μερισμό του συνόλου G. Ορίζεται συνεπώς επί του G μία σχέση ισοδυναμίας, τέτοια ώστε, οι τάξεις ισοδυναμίας αυτής, να είναι οι γραμμές του πίνακα. Να είναι, δηλαδή, $C_a = \{ea, \ \dots \ , h_r a\}$, $a \in G$. Η σχέση αυτή R, ορίζεται ως εξής:

$R = \{(a,b) \in G \times G \,|\, ab^{-1} = h \in H\}$, Η μιά υποομάδα της G. Έχουμε, τότε, ότι,

α) $(a,a) \in R$, μιά και $aa^{-1} = e \in H$.

β) $(a,b) \in R \to a = hb \to b = h^{-1}a$, όπου $h^{-1} \in H$. Άρα και, $ba^{-1} \in H$, δηλαδή, $(b,a) \in R$.

γ) $(a,b) \in R$ και $(b,c) \in R \to (a,c) \in R$, μιά και από τις σχέσεις $ab^{-1} = h_1$ και $bc^{-1} = h_2$ ή την $b^{-1} = c^{-1}h_2^{-1}$, έχουμε και την $ac^{-1}h_2^{-1} = h_1$, ή την $ac^{-1} = h_1 h_2 \in H$.

Γράφουμε και, $a = b(\mathrm{mod}\, H)$. Στην συνέχεια, θεωρούμε το σύνολο G/H. Ένα στοιχείο $C_a \in G/H$, είναι το, $C_a = \{x \in G \,|\, x = a(\mathrm{mod}\, H)\} = Ha$. Παρατηρούμε ότι, όλες οι τάξεις C_a έχουν r το πλήθος στοιχεία. Πράγματι, η αντιστοιχία $C_a \ni x \mapsto y \in C_b$, αν και μονον αν $y = hb$ με h το στοιχείο εκείνο της H, για το οποίο είναι $x = ha$, είναι μία αντιστοιχία ένα-ένα και επί ανάμεσα στις τυχούσες τάξεις C_a και C_b, ως επίσης και μία αντιστοιχία ένα-ένα και επί ανάμεσα στα στοιχεία μιάς τάξεως, και της H.

Ορισμός. Η τάξη $Ha = \{ha \,|\, h \in H\}$, καλείται ***δεξιά τάξη*** (right coset) του H. Με τον ίδιο τρόπο, ορίζουμε και την ***αριστερή τάξη*** του H, την $aH = \{ah \,|\, h \in H\}$. Ο ακέραιος που εκφράζει το πλήθος των δεηιά (ή αριστερά) τάξεων της H εν G, καλείται ***δείκτης*** (index) της H εν G. Είναι, $i_G(H) = \dfrac{o(G)}{o(H)}$, όπου $i_G(H)$ ο δείκτης της H εν G.

Παράδειγμα. Θεωρούμε την ομάδα S_3, και έστω η υποομάδα της $H = \{p_0, p_3\}$ (βλέπε §32). Είναι, $i_G(H) = \dfrac{6}{2} = 3$. Έχουμε, λοιπόν, τρείς αριστερά και τρείς δεξιά τάξεις της H εν G.

Οι δεξιά τάξεις είναι οι: 1) $Hp_0 = H = \{p_0, p_3\}$. Λαβαίνουμε στην συνέχεια ένα στοιχείο $p \in G$ με $p \notin H$. Έστω το p_1. Σχηματίζουμε τα γινόμενα Hp_1. Είναι, 2) $Hp_1 = \{p_1, p_5\}$. Λαβαίνουμε, τέλος, ένα στοιχείο $p \in G$ με $p \notin H$ και $p \notin Hp_1$. Ένα τέτοιο στοιχείο είναι το p_2. Σχηματίζουμε τα γινόμενα Hp_2. Είναι, 3) $Hp_2 = \{p_2, p_4\}$.

Οι αριστερά τάξεις είναι οι: 1) $p_0H = H = \{p_0, p_3\}$. Λαβαίνουμε στην συνέχεια ένα στοιχείο $p \in G$ με $p \notin H$. Έστω το p_1. Σχηματίζουμε τα γινόμενα p_1H.

Είναι, 2) $p_1H = \{p_1, p_4\}$. Λαβαίνουμε, τέλος, ένα στοιχείο $p \in G$ με $p \notin H$ και $p \notin p_1H$. Ένα τέτοιο στοιχείο είναι το p_2. Σχηματίζουμε τα γινόμενα p_2H.

Είναι, 3) $p_2H = \{p_2, p_5\}$.

Παρατηρούμε ότι, οι δεξιά τάξεις του H εν G, δεν συμπίπτουν με τις αριστερά τάξεις του H εν G, αν και όλες έχουν από δύο στοιχεία του G.

Αν, τώρα, αντί για $H = \{p_0, p_3\}$, είχαμε λάβει $H = \{p_0, p_1, p_2\}$, τότε εργαζόμενοι ως και προηγουμένως, θα διαπιστώναμε ότι, οι δεξιά και οι αριστερά τάξεις συμπίπτουν. Τούτο σημβαίνει διότι έχουμε την,

Πρόταση. Η δεξιά τάξη Ha του H ταυτίζεται με την αριστερή τάξη aH του H, αν και μόνον αν ισχύει ότι $\forall h \in H,\ ha = ah$, δηλαδή, αν και μόνον αν, το στοιχείο $a \in G$, αντιμετατίθεται με όλα τα στοιχεία του H.

Παρατήρηση. Λόγω του θεωρήματος του Lagrange $o(a) \mid o(G)$.

Πόρισμα. $\forall a \in G$, ισχύει ότι, $a^{o(G)} = e$, μιά και, $a^{o(G)} = a^{ko(a)} = (a^{o(a)})^k = e^k = e$.

mod 8	**1**	**3**	**5**	**7**
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

Εφαρμογή. Θεωρούμε την συνάρτηση $\varphi(n)$ του Euler (βλέπε §20). Οι ακέραιοι και θετικοί αριθμοί a, που είναι $< n$ και για τους οποίους ισχύει ότι $(a,n) = 1$, αποτελούν πολλαπλασιαστική ομάδα Φ $\bmod n$ με $o(\Phi) = \varphi(n)$.

Για παράδειγμα, αν $n = 8$, $\varphi(n) = 4$ και $\Phi = \{1,3,5,7\}$. Ο πολλαπλασιαστικός πίνακας της Φ είναι ο δίπλα.

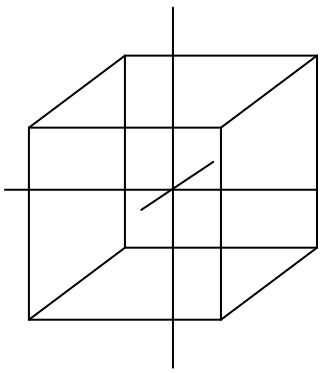
Εφαρμόζουμε το προηγούμενο πόρισμα στην ομάδα Φ, και έχουμε ότι, $a^{\varphi(n)} = 1 \bmod n$, που είναι το θεώρημα του Euler. Στην περίπτωση, που ο n είναι αριθμός πρώτος p, $\varphi(p) = p - 1$, οπότε και $a^{p-1} = 1 \bmod p$, ή $a^p = a \bmod p$. Εδείχθη συνεπώς το θεώρημα του Fermat για την περίπτωση $(a,p) = 1$ (βλέπε §16). Στην περίπτωση που, ο a και ο p έχουν διαιρέτη $\delta \neq 1$, επειδή ο p πρώτος, έπεται ότι, $p \mid a$, και άρα, $a = 0 \bmod p$, ή και $a^p = a \bmod p$. Το θεώρημα του Fermat ισχύει συνεπώς, για κάθε ακέραιο a.

Παρατηρούμε ότι, ο πίνακας αυτός, δεν διαφέρει ουσιαστικά από τον πίνακα της ομάδας του Klein. Η Φ είναι λοιπόν ισόμορφη προς την ομάδα αυτή.

Αν $o(G) = p$, αριθμός πρώτος, τότε κάθε στοιχείο της G έχει τάξη p. Συνεπώς, μία ομάδα τάξεως p, αποτελείται από τις δυνάμεις ενός μόνον στοιχείου a, και ουδεμία υποομάδα πλην της {e} περιέχει. Η G είναι, λοιπόν, κυκλική ομάδα.

8. Ομομορφισμοί. Έστω οι ομάδες G και G΄. Η $f : G \to G'$ είναι ***ομομορφισμός***, ανν $\forall a,b \in G,\ f(ab) = f(a)f(b) \in G'$.

ΠΑΡΑΔΕΙΓΜΑ. G η ομάδα των περιστροφών του κύβου. Η G αποτελείται από τις υποομάδες:



1) Ταυτοτική.
2) 9 περιστροφές γύρω από τους άξονες που διέρχονται απο τα κέντρα των εδρών του κατά 90º, 180º και 270º.
3) 6 περιστροφές κατά 180º γύρω από τους άξονες που ορίζονται από τα μέσα των απέναντι πλευρών.
4) 8 περιστροφές κατά 180º και 270º γύρω από τους άξονες που ορίζουν οι απέναντι κορυφές.

Αν συνδέσουμε τα κέντρα των εδρών, λαβαίνουμε ένα τετράεδρο. Η ομάδα των περιστροφών του τετραέδρου, αποτελεί την ομάδα G΄. Η απεικόνιση f ορίζεται από την τοποθέτηση αυτή του τετραέδρου εντός του κύβου. Σε κάθε περιστροφή του κύβου αντιστοιχεί και μία περιστροφή του τετραέδρου. Δύο διαδοχικές περιστροφές

του κύβου αντιστοιχούν σε δύο διαφορετικές περιστροφές του τετραέδρου. Η f είναι, λοιπόν, ένας ομομορφισμός.

Ορισμός. ***Πυρήνας*** (kernel) ενός ομομορφισμού $f : G \to G'$, είναι το σύνολο των στοιχείων της G, που απεικονίζονται στο ουδέτερο στοιχείο της G΄. Τον πυρήνα της f τον συμβολίζουν με K = kerf.

Ισχύουν οι προτάσεις:
1) Ο K = kerf είναι υποομάδα της G.
2) $\forall x \in G$ και $k \in \ker f$, ισχύει ότι $xkx^{-1} \in K$. Γράφουμε και $xK = Kx$.
Είναι, $f(xkx^{-1}) = f(x)f(k)f(x^{-1}) = f(x)f(x)^{-1} = e$.

Ορισμός. Το σύνολο Z των στοιχείων z της G, τα οποία αντιμετατίθεντε με όλα τα στοχεία x της G, καλείται και ***κέντρον*** της ομάδας G. Είναι, λοιπόν, $Z = \{z \in G \mid \forall x \in G,\ zx = xz\}$.
Ο πυρήνας συνεπώς του ομομορφισμού f, ταυτίζεται με το ***κέντρο*** Z της ομάδας G.

9. Αυτομορφισμοί. Με κάθε στοιχείο $g \in G$ η απεικόνιση $\varphi_g : G \to G$ που ορίζεται από την σχέση $G \ni h \mapsto \varphi_g(h) = ghg^{-1} \in G$ αποτελεί έναν ***εσωτερικό αυτομορφισμό*** της ομάδας G. Η φ_g είναι ένα – ένα και επί, μιά και η $gx_1g^{-1} \neq gx_2g^{-1}$ συνεπάγεται την $x_1 \neq x_2$. Εξ' άλλου, το τυχόν στοιχείο $x \in G$ είναι εικόνα του $g^{-1}xg \in G$. Η φ_g είναι και ισομορφισμός της G μιά και

$$\varphi_g(x_1x_2) = gx_1x_2g^{-1} = gx_1g^{-1}gx_2g^{-1} = \varphi_g(x_1)\varphi_g(x_2).$$

ΠΑΡΑΔΕΙΓΜΑ. Έστω $G = S_3 = \{p_0, p_1, p_2, p_3, p_4, p_5\}$ (βλέπε σελ. 8). Ως g λαβαίνουμε το στοιχείο p_3 (κατοπτρισμός ως προς το ύψος ισοπλεύρου τριγώνου που άγεται από την κορυφή 3). Η $\varphi_g(S_3) = \{p_3p_ip_3^{-1}, 0 \le i \le 5\}$. Χρησιμοποιούμε τον πίνακα της S_3. Παρατηρούμε ότι $p_3^{-1} = p_3$ και, στην συνέχεια, υπολογίζουμε ότι, $p_3p_0p_3^{-1} = p_0$, $p_3p_1p_3^{-1} = p_5p_3^{-1} = p_2$, $p_3p_2p_3^{-1} = p_4p_3^{-1} = p_1$, $p_3p_3p_3^{-1} = p_0p_3^{-1} = p_3$, $p_3p_4p_3^{-1} = p_2p_3^{-1} = p_5$, $p_3p_5p_3^{-1} = p_1p_3^{-1} = p_4$. Η φ_g στην περίπτωση αυτή, συμπίπτει με την μετάθεση $\begin{pmatrix} p_0 & p_1 & p_2 & p_3 & p_4 & p_5 \\ p_0 & p_2 & p_1 & p_3 & p_5 & p_4 \end{pmatrix}$. Παρατηρούμε ότι η $p_3 \in \varphi_g(S_3)$ εξακολουθεί να διατειρεί την κορυφή 1, δεν συμβαίνει όμως το ίδιο και για τις άλλες συμμετρίες.
Υπάρχουν όμως και ομάδες, που παραμένουν αναλλοίωτες ως προς όλους τους εσωτερικούς αυτομορφισμούς των. Είναι δηλαδή, κατά κάποιο τρόπο "υπερσυμμετρικές"

Παρατήρηση. Τα στοιχεία $a, b \in G$ αντιμετατίθενται ανν $ab = ba$. Συνεπώς το μέτρο της μη αντιμεταθεσιμότητος των στοιχείων a και b της G, δίδεται από το γινόμενο $aba^{-1}b^{-1}$ το οποίο ισούται με e ανν $ab = ba$. Το στοιχείο $aba^{-1}b^{-1}$ καλείται και ***commutator*** των στοιχείων a και b.

Εισάγουμε την εξής σχέση R επί την G: $R = \{(a,b) \in G \times G \mid \exists x \in G \text{ με } b = x^{-1}ax\}$. Η R είναι μιά σχέση ισοδυναμίας. Πράγματι, α) $a = e^{-1}ae$. β) Αν $b = x^{-1}ax$, τότε και $a = xbx^{-1}$ οπότε αρκεί να λάβουμε $x = x^{-1}$. γ) Τέλος, αν έχουμε ότι $b = x^{-1}ax$ και $a = y^{-1}cy$, τότε, είναι και $b = x^{-1}y^{-1}cyx = (yx)^{-1}c(yx)$. Τα στοιχεία a και b της G, που είναι R ισοδύναμα, καλούνται ***συζυγή στοιχεία*** (conjugate elements) της G. Το σύνολο G/R περιέχει τις τάξεις $C_a = \{b \in G \mid \exists x \in G \text{ με } b = x^{-1}ax\}$. Τα στοιχεία $b \in C_a$ καλούνται ***συζυγή*** ως προς a στοιχεία. Οι τάξεις αυτές, αποτελούν έναν μερισμό της ομάδας G. Αν συνεπώς, η G έχει πεπερασμένο πλήθος στοιχείων και με $o(C_a)$ παραστήσουμε το πλήθος των στοιχείων της C_a, τότε, $o(G) = \sum_a o(C_a)$.

Ορισμός. Το σύνολο των στοιχείων x της G, που αντιμετατίθενται με το στοιχείο a, καλείται ***Normalizer*** N(a) του στοιχείου a. Είναι, λοιπόν, $N(a) = \{x \in G \mid xa = ax\}$.

Πρόταση. Η N(a) είναι υποομάδα της G. Πράγματι, με κάθε $n_1, n_2 \in N(a)$, $n_1n_2 \in N(a)$, μιά και $n_1n_2a = n_1an_2 = an_1n_2$. Εξ' άλλου, $\forall n \in N(a)$, είναι, και $n^{-1} \in N(a)$, μιά και, $n^{-1} \in G$, και $n \in N(a) \to n^{-1}a = n^{-1}ann^{-1} = n^{-1}nan^{-1}$. Άρα, $n^{-1}a = an^{-1}$, δηλαδή, $n^{-1} \in N(a)$.

Πρόταση. Για πεπερασμένη ομάδα G, ισχύει ότι, $o(C_a) = \frac{o(G)}{o(N(a))}$. Δηλαδή, το πλήθος των στοιχείων της C_a είναι ακριβώς τόσο, όσες είναι οι (δεξιά) τάξεις της N(a) εν G.

Απόδειξη. Θα δείξουμε ότι, α) δύο στοιχεία, που ανήκουν στην ίδια δεξιά τάξη ισοδυναμίας ως προς N(a) είναι συζυγή ως προς a στοιχεία, ενώ β) δύο στοιχεία της G, που ανήκουν σε διαφορετικές δεξιά τάξεις ως προς N(a), δεν είναι συζυγή ως προς a. Προς τούτο, αρκεί να δείξουμε ότι υπάρχει ένα-ένα απεικόνιση $\varphi : C_a \to G/N(a)$. Έστω, λοιπόν, ότι, $x, y \in N(a)z$.

Τότε, $x = n_1z$ και $y = n_2z$, άρα, $\exists n = n_1n_2^{-1} \in N(a)$, με $x = ny$, όπου $na = an$. Άρα και $x^{-1} = y^{-1}n^{-1}$. Ή $x^{-1}ax = y^{-1}n^{-1}ax$, οπότε και $x^{-1}ax = y^{-1}n^{-1}any = y^{-1}ay$. Συνεπώς, στα διαφορετικά στοιχεία x, y της ίδιας δεξιάς τάξεως N(a)z, αντιστοιχεί το αυτό στοιχείο $x^{-1}ax = y^{-1}ay \in C_a$. Για το β), έστω ότι τα x και y ανήκουν σε διαφορετικές δεξιές ως προς N(a) τάξεις. Θα δείξουμε ότι και τα συζυγή τους ως προς a στοιχεία είναι δυνατόν να ταυτίζονται. Πράγματι, αν $x^{-1}ax = y^{-1}ay$ θα είχαμε και $yx^{-1}a = ayx^{-1}$, δηλαδή, το στοιχείο $yx^{-1} \in N(a)$.

Πόρισμα. $o(G) = \sum_a \frac{o(G)}{o(N(a))}$. Η εξίσωση αυτή, ονομάζεται ***εξίσωση τάξεως*** (class equation) της ομάδας G.

Παρατήρηση. Στην περίπτωση, που η G είναι Αβελιανή, τότε, για κάθε $a \in G$, $C_a = \{a\}$, οπότε $o(C_a) = 1$, μιά και, $C_a = \{y \in G \mid \exists x \in G \text{ με } y = x^{-1}ax = a\}$.

Παράδειγμα. Θεωρούμε την συμμετρική ομάδα S_3 (βλέπε §32), και ζητάμε να βρούμε την εξίσωση τάξεως αυτής της ομάδας. Είναι, 1) $C_{p_0} = \{p_0\}$.

2) Για να βρούμε το $C_{p_1} = \{p \in S_3 \mid \exists x \in S_3 \text{ με } p = x^{-1}p_1x\}$, Σχηματίζουμε όλα τα γινόμενα της μορφής $x^{-1}p_1x$. Από τον πολλαπλασιαστικό πίνακα της S_3 έχουμε ότι,

$$p_1p_0 = p_1,\ p_1p_1 = p_2,\ p_1p_2 = p_0,\ p_1p_3 = p_4,\ p_1p_4 = p_5,\ p_1p_5 = p_3,$$

και στην συνέχεια, υπολογίζουμε ότι,

$p_0^{-1}p_1p_0 = p_1$, $p_1^{-1}p_1p_1 = p_1$, $p_2^{-1}p_1p_2 = p_1$, $p_3^{-1}p_1p_3 = p_2$, $p_4^{-1}p_1p_4 = p_2$, $p_5^{-1}p_1p_5 = p_2$. Άρα, $C_{p_1} = \{p_1, p_2\}$.

3) Λαβαίνουμε κάποιο στοιχείο p, το οποίο δεν ανήκει στην C_{p_0} ή την C_{p_1}. Έστω το p_3. Για να βρούμε το $C_{p_3} = \{p \in S_3 \mid \exists x \in S_3 \text{ με } p = x^{-1}p_3x\}$, σχηματίζουμε όλα τα γινόμενα $x^{-1}p_3x$. Από τον πολλαπλασιαστικό πίνακα της S_3 έχουμε ότι,

$$p_3p_0 = p_3,\ p_3p_1 = p_5,\ p_3p_2 = p_4,\ p_3p_3 = p_0,\ p_3p_4 = p_2,\ p_3p_5 = p_1,$$

και στην συνέχεια, υπολογίζουμε ότι, $p_0^{-1}p_3p_0 = p_3$, $p_1^{-1}p_3p_1 = p_4$, $p_2^{-1}p_3p_2 = p_5$, $p_3^{-1}p_3p_3 = p_3$, $p_4^{-1}p_3p_4 = p_5$, $p_5^{-1}p_3p_5 = p_4$. Άρα, $C_{p_3} = \{p_3, p_4, p_5\}$.

Δεν έχουμε πλέον, στοιχείο p, που να μη ανήκει σε κάποια τάξη.

Είναι, $o(G) = o(C_{p_0}) + o(C_{p_1}) + o(C_{p_3})$, ή $6 = 1 + 2 + 3$.

Ας υπολογίσουμε, τώρα, τις υποομάδες $N(p_0)$, $N(p_1)$, $N(p_3)$, οι οποίες πρέπει να έχουν 1, 2, 3 δεξιές τάξεις εν S_3 αντίστοιχα. 1) $N(p_0) = \{p \in S_3 \mid pp_0 = p_0p\}$. Όμως, το p_0 αντιμετατίθεται με όλα τα στοιχεία της ομάδας S_3.

Άρα $N(p_0) = S_3$, και $o(N(p_0)p_0) = o(S_3)/o(N(p_0)) = 1$

2) $N(p_1) = \{p \in S_3 \mid pp_1 = p_1p\}$. Από τον πολλαπλασιαστικό πίνακα της S_3 βρίσκουμε ότι, $N(p_1) = \{p_0, p_1, p_2\}$. Άρα και, $o(N(p_1)p_1) = o(S_3)/o(N(p_1)) = 2$.

3) $N(p_3) = \{p \in S_3 \mid pp_3 = p_3p\}$. Από τον πολλαπλασιαστικό πίνακα της S_3 βρίσκουμε ότι, $N(p_3) = \{p_0, p_3\}$. Άρα και, $o(N(p_3)p_3) = o(S_3)/o(N(p_3)) = 3$.

Παρατήρηση. Η εξίσωση τάξεως, μπορεί να γραφεί, $o(G) = 1 + \sum_{a \neq e} \frac{o(G)}{o(N(a))}$, μιά και όταν $a = e$, $N(e) = \{x \in G \mid ex = xe\} = G$. Αν, τώρα, το πλήθος των στοιχείων $z \in G$, για τα οποία ισχύει η σχέση $\forall x \in G$, με $z = x^{-1}zx$, οπότε και γι' αυτά έχουμε $N(z) = G$, είναι ζ, τότε, η εξίσωση τάξεως γράφεται, $o(G) = \zeta + \sum_{a \neq z} \frac{o(G)}{o(N(a))}$. Το σύνολο όμως των στοιχείων $z \in G$ για τα οποία είναι $\forall x \in G,\ xz = zx$, το έχουμε καλέσει κέντον Z της ομάδας G. Η εξίσωση τάξεως γράφεται, λοιπόν, και $o(G) = o(Z) + \sum_{a \notin Z} \frac{o(G)}{o(N(a))}$.

Εφαρμογή. 1) Αν $o(G) = p^m$, p αριθμός πρώτος, τότε και $o(Z) = \mu p$, $\mu > 0$. Το συμπέρασμα αυτό, έπεται από μιά απλή εφαρμογή της εξίσωσης τάξεως, μιά και κάθε

όρος του αθροίσματος $\sum_{a\notin Z}\frac{o(G)}{o(N(a))}$ είναι θετικός ακέραιος (θεώρημα Lagrange) της μορφής $\lambda_a p$. Άρα ισχύει ότι $o(Z)=p^m-\sum_{a\notin Z}\lambda_a p=\mu p$.

2) Αν $o(G)=p^2$, τότε η G έχει υποομάδα τάξεως p. Η υποομάδα αυτή, δεν είναι άλλη από την Z. Πράγματι, είναι, $o(Z)=p^2-\sum_{a\notin Z}\lambda_a p=p\left\{p-\sum_{a\notin Z}\lambda_a\right\}$ και επειδή $o(Z)\,|\,o(G)$, αναγκαστικά είναι, $o(Z)=p$.

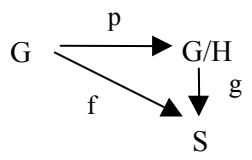
Η έννοια του Normalizer γενικεύεται: $N(a_i)=\{xa_ix^{-1}a_i^{-1},\ x\in G, a_i\in G,\ 1\le i\le n\}$ Το σύνολο $N(a_i),\ 1\le i\le n$ είναι και αυτό υποομάδα της G. Στην περίπτωση που η G είναι αβελιανή, $N(a_i)=\{e\}$.

10. Κανονικές (normal) υποομάδες. Στην §7 παρατηρήσαμε ότι, οι δεξιά τάξεις μιάς υποομάδας H εν G συμπίπτουν με τις αριστερές της τάξεις, αν και μόνον αν για κάθε $x\in G$ και $h\in H$, ισχύει ότι, $xh=hx$. Το γεγονός αυτό, μας οδηγεί στον Ορισμό:

Ορισμός. Μία υποομάδα H της ομάδας G λέγεται ***κανονική,*** (ή ***αναλλοίωτος,*** invarient), αν και μόνον αν, $\forall x\in G$ και κάθε $h\in H$, ισχύει ότι, $xhx^{-1}\in H$. Γράφουμε, τότε, και $H\lhd G$.

Παρατήρηση. Εφ' όσον η H υποομάδα και $xhx^{-1}\in H$, και το αντίστροφο στοιχείο του στοιχείου αυτού ανήκει στην H. Είναι, λοιπόν, και $xh^{-1}x^{-1}\in H$. Εξ' άλλου, αν αντί του $x\in G$ είχαμε λάβει το $x^{-1}\in G$, θα είχαμε και ότι $x^{-1}hx\in H$, ως επίσης και $x^{-1}h^{-1}x\in H$. Από τις σχέσεις αυτές έπεται ότι, η H είναι κανονική υποομάδα, αν και μόνον αν $\forall x\in G$, $xHx^{-1}=H$ Στην περίπτωση αυτή, πολύ εύκολα μπορούμε να δείξουμε ότι, οι δεξιά τάξεις της H εν G συμπίπτουν με τις αριστερά τάξεις της H εν G.

Αν H κανονική υποομάδα της G, τότε, το γινόμενο δύο δεξιά (αντ. αριστερά) τάξεων, είναι και πάλι μιά δεξιά (αντ. αριστερά) τάξις. Πράγματι είναι, $HaHb=HHab=Hab$. Το σύνολο συνεπώς G/H των δεξιά (ή αριστερά) τάξεων, αποτελεί ομάδα, αν και μόνον αν H κανονική υποομάς της G. Ουδέτερο στοιχείο της ομάδας αυτής, είναι το η τάξη $He=H$. Το πλήθος των στοιχείων της G/H είναι, βέβαια, ίσο προς $i_G(H)$. Έχουμε, λοιπόν, $o(G/H)=\frac{o(G)}{o(H)}$.

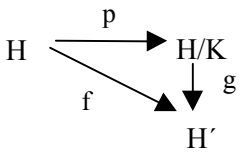


Ερχόμαστε, τώρα, να δούμε τις επιπτώσεις που έχει το Θεώρημα της §5 ενότητα "Σύνολα", για την περίπτωση που, η σχέση ισοδυναμίας R ορίζεται μέσω της κανονικής υποομάδος H. Έχουμε, τότε, το δίπλα αντιμεταθετικό διάγραμμα. Στο διάγραμμα αυτό, η προβολή p ορίζεται από την σχέση, $G\ni x\mapsto Hx\in G/H$. Η p είναι ένας ομομορφισμός της ομάδας G επί την ομάδα G/H.

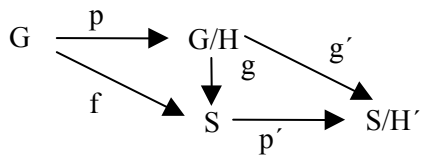
Πράγματι, $p(x_1x_2)=Hx_1x_2=H^2x_1x_2=Hx_1Hx_2=p(x_1)p(x_2)$. Αν f ομομορφισμός, που πληροί τις συνθήκες του θεωρήματος της §5, τότε, η $g:G/H\to S$ ισομορφισμός. Γράφουμε και $G/H\cong S$. Ακόμα, το διάγραμμα αυτό μας δείχνει ότι, $g(H)=f(e)$, και

το στοιχείο αυτό, είναι το ουδέτερο στοιχείο e΄ της ομάδας S. Εξ' άλλου, στο e΄ απεικονίζονται και όλα τα άλλα στοιχεία της υποομάδας H της G. Το H είναι, λοιπόν, υποσύνολο του πυρήνα K του ομομορφισμού f. Φανερά, ο f είναι ισομορφισμός, αν και μόνον αν $H = \{e\}$.

Ακόμα, μπορούμε να έχουμε το παραπάνω διάγραμμα και στην περίπτωση, που η f είναι ένας ομομορφισμός $f : G \to S$, με πυρήνα K, που συμπίπτει, όπως είδαμε, με το κέντρο Z της G, (βλέπε §34), και είναι φανερά, κανονική υποομάς της G.



Έστω H΄ μία υποομάς της S και $H = \{x \in G \mid f(x) \in H'\}$. Το H είναι, τότε, υποομάς της G, η οποία μάλιστα, περιέχει τον πυρήνα K του ομομορφισμού f. Πράγματι, αν $h_1, h_2 \in H$, τότε και $f(h_1h_2) = f(h_1)f(h_2) \in H'$, και συνεπώς, $h_1h_2 \in H$. Εξ' άλλου και $\forall h \in H$, και $h^{-1} \in H$ μιά και $f(h^{-1}) = f(h)^{-1} \in H'$. Αν επιπλέον $H' \lhd S$, τότε, και $H \lhd G$. Έχουμε, λοιπόν, και το δίπλα αντιμεταθετικό διάγραμμα όπου η g΄ ισομορφισμός. Αν λάβουμε ως S την G/K και ως H΄ την H/K, λόγω των g ισομορφισμών, έχουμε και τον



ισομορφισμό $i : G/H \to (G/K)/(H/K)$.

Εφαρμογή. Αν $i_G(H) = 2$, τότε $H \lhd G$, μιά και, η G μερίζεται ήτε ως {H, Hx}, $x \notin H$, ήτε {H, xH}. Άρα, $Hx = xH$. Εξ' άλλου, αν $x \in H$, τότε, $Hx = H = xH$.

Πρόταση. Αν $H \lhd G$ και A οιαδήποτε υποομάδα της G, τότε η $H \cap A \lhd G$, και έχουμε τον ισομορφισμό $A/(A \cap H) \cong HA/H$.

Απόδειξη. α) Το ότι η $H \cap A$ είναι ομάδα το γνωρίζουμε (βλέπε §31). Το ότι η $H \cap A$ είναι κανονική υποομάδα της A, έπεται από το γεγονός ότι $H \cap A \subseteq H \lhd G$. Η $A/(A \cap H)$ είναι λοιπόν ομάδα, και έχουμε τον ομομορφισμό $p : A \to A/(A \cap H)$.

β) Αρκεί να δείξουμε ότι, έχουμε και τον ομομορφισμό $f : A \to HA/H$. Παρατηρούμε ότι, τα στοιχεία της ομάδας πηλίκον HA/H έχουν την μορφή Hg όπου $g \in HA$. Ορίζουμε την f ως εξής: $A \ni a \mapsto Hha$, ή την $A \ni a \mapsto Ha$, που είναι ο γνωστός ομομορφισμός $p : A \to A/H$.

Παρατήρηση. Αν $H \lhd G$ και A οιαδήποτε υποομάδα της G, τέτοια ώστε, $H \lhd A \lhd G$, τότε είναι και $A/H \lhd G/H$.

11. Το θεώρημα του Sylow. Το θεώρημα του Lagrange βεβαιώνει ότι, αν η ομάδα G έχει υποομάδα H, τότε είναι $o(H) \mid o(G)$. Ισχύει άραγε το αντίστροφο; Αν δηλαδή $k \mid o(G)$, υπάρχει υποομάδα H της G, με $o(H) = k$; Η απάντηση είναι όχι. Για παράδειγμα η εξ' εναλλαγής ομάδα A_4 με $o(A_4) = 12$, ουδεμία υποομάδα έχει τάξεως $k = 6$ (βλέπε §31). Έχουμε, όμως, το (πρώτο) θεώρημα του Sylow: Έστω ομάς G, p πρώτος, και p^m η μεγαλύτερη δύναμη του p που διαιρεί την τάξη της G. Η G περιέχει, τότε, μία υποομάδα H με $o(H) = p^m$. Η ομάς αυτή H, καλείται και ***Sylow p-υποομάς*** της ομάδας G.

Για παράδειγμα, Η S_4 έχει $o(S_4)=24=2^3\times 3$, και περιέχει την υποομάδα των συμμετριών του τετραγώνου, που έχει $2^3=8$ στοιχεία, ως επίσης την ομάδα $\{p_0,\tau_1,\tau_2\}$, υποομάδα της A_4, για την οποία έχουμε ότι, $\tau_1\tau_2=p_0=\tau_2\tau_1$ και $\tau_1^2=\tau_2$, $\tau_2^2=\tau_1$ (βλέπε §32).

Θα αποδείξουμε, πρώτα, το θεώρημα του Sylow, για την περίπτωση, που η G είναι Αβελιανή ομάδα.Αρχίζουμε με το

Θεώρημα του Cauchy (για Αβελιανές ομάδες 1854). Έστω G πεπερασμένη Αβελιανή ομάς και $p\,|\,o(G)$, p πρώτος. $\exists$ τότε $a\in G$, με $a^p=e$.
Απόδειξη, με επαγωγή πάνω στην $o(G)$. Για $o(G)=1$ το θεώρημα ισχύει τετριμμένα. Επίσης αν $o(G)=p$, τότε, όπως είδαμε στη §33, η G είναι κυκλική ομάς, και άρα, $\forall a\in G,\ a\neq e$, είναι $a^p=e$. Έστω, λοιπόν, ότι $o(G)=n$, και ότι το θεώρημα ισχύει $\forall k<n$. Θα δείξουμε ότι ισχύει και για την τιμή $k=n$. Ας υποθέσουμε, λοιπόν, ότι η G έχει την υποομάδα $N\neq\{e\}$ για την οποία ισχύει η επαγωγική μας υπόθεση, ότι δηλαδή, $\exists\ b\in N$, με $b^p=e$ και $p\,|\,o(N)$. Θα πρέπει να δείξουμε ότι και $p\,|\,o(G)$. Έστω, λοιπόν, ότι ο p δεν διαιρεί την τάξη της ομάδας G. Θεωρούμε την ομάδα G/N για την οποία έχουμε ότι, $o(G/N)=\dfrac{o(G)}{o(N)}$ και επειδή $p\,|\,o(N)$, $p\,|\,\dfrac{o(G)}{o(N)}<o(G)$. Εξ' άλλου, η G/N είναι Αβελιανή, μιά και η G είναι και αυτή Αβελιανή. Πληροί, λοιπόν, την επαγωγική μας υπόθεση και έστω X μία τάξη της G/N, $X\neq N$, (που είναι το ουδέτερο στοιχείο της G/N), για την οποία $X^p=N$. Είναι, $X=Nc$, $c\notin N$, οπότε και $c\neq b$, και συνεπώς, $N=X^p=(Nc)^p=Nc^p$. Άρα $c^p\in N$, οπότε και $e=(c^p)^{o(N)}=(c^{o(N)})^p$. Όμως, και $b^p=(b^{o(N)})^p=e$. Άρα, $c^{o(N)p}=b^{o(N)p}$, απ' όπου $c=b$, άτοπον.

Θεώρημα του Cauchy. Αν p αριθμός πρώτος και $p\,|\,o(G)$, τότε η G έχει κυκλική υποομάδα τάξεως p.

Θεώρημα. Αν $p^m\,|\,o(G)$ αλλά $p^{m+1}\nmid o(G)$, p πρώτος, τότε υπάρχει υποομάδα της G τάξεως p^m.

Απόδειξη. Θα βρούμε ένα στοιχείο $a\in G$, τέτοιο ώστε, $a^p=e$. Υποθέτουμε ότι, το θεώρημα ισχύει για κάθε υποομάδα G΄ της G, τάξεως $o(G')<o(G)$. (Επαγωγική μας υπόθεση). Έστω ότι, ο p δεν διαιρεί την τάξη καμιάς υποομάδας της G. Ιδιαίτερα, έστω το $a\notin Z$, και θεωρούμε την $N(a)\neq G$. Έχουμε ότι, (βλέπε §35), $o(G)=o(Z)+\sum_{a\notin Z}\dfrac{o(G)}{o(N(a))}$, απ' όπου, όπως είδαμε, προκύπτει ότι, $p\,|\,o(Z)$, αντίθετα με την υπόθεσή μας. Άρα, $Z=G$, οπότε η G είναι Αβελιανή, και ερχόμαστε στην προηγούμενη περίπτωση.
Απόδειξη. Με επαγωγή. Το θεώρημα αληθεύει, όπως είδαμε, για $o(G)=p^2$. Υποθέτουμε ότι το θεώρημα αληθεύει για κάθε υποομάδα της G (επαγωγική υπόθεση). Έστω ότι $o(G)=p^mq$. Θεωρούμε την ομάδα G/Z. Αυτή, λόγω της υποθέσεως της επαγωγής μας, περιέχει μιά Sylow υποομάδα τάξεως p^{m-1}, την H/Z. Έχουμε, όμως, ότι $i:G/H\to(G/Z)/(H/Z)$ (βλέπε §36). Άρα, και,

$o(G/H) = o(G/Z)/o(H/Z)$, ή $\frac{p^m q}{h} = \frac{p^{m-1} q}{p^{m-1}}$, ή $h = p^m$, όπου h η τάξη της ομάδας H.

Εφαρμογή. Αν $(m,n) = 1$, τότε η $\mathbb{Z}_m \times \mathbb{Z}_n$ είναι κυκλική και ισόμορφος της $\mathbb{Z}_{mn}$. Το συμπέρασμα αυτό εύκολα επεκτείνεται και στην περίπτωση, που έχουμε r παράγοντες ανά δύο πρώτους μεταξύ τους. Μετά από όσα είδαμε μέχρις εδώ, ο αναγνώστης αντιλαμβάνεται, ότι η πρόταση αυτή, δεν είναι τίποτα άλλο, από μία μεταφορά του θεμελειώδους θεωρήματος της αριθμητικής (βλέπε §15) στις ομάδες. Έτσι, αν $o(G) = n$, και $n = \prod_{i=1}^{k} p_i^{m_i}$ μία ανάλυση του n σε γινόμενο πρώτων παραγόντων, υπάρχουν, τότε, k υποομάδες τάξεως $o(H_i) = p_i^{m_i}$, το γινόμενο των οποίων είναι ισόμορφο της G. Προσοχή όμως. Ενώ η παράστασις $\prod_{i=1}^{k} p_i^{m_i}$ είναι μοναδική, η $G = \times_{i=1}^{k} H_i$ δεν είναι.

12. Υποκανονικές και Κανονικές σειρές. Επιλύσιμες ομάδες. ***Υποκανονική σειρά*** της ομάδας G, ονομάζουμε μιά πεπερασμένη ακολουθία $H_0 \subseteq H_1 \subseteq \ \ldots \ \subseteq H_n$, όπου $H_i \lhd H_{i+1}$, $H_0 = \{e\}$ και $H_n = G$. ***Κανονική*** καλείται η προηγούμενη ακολουθία, αν και μόνον αν, $H_i \lhd G$. Παρατηρούμε ότι, μία κανονική σειρά είναι πάντα και υποκανονική, όχι όμως και το αντίθετο, εκτός και αν η G είναι Αβελιανή ομάδα. Για παράδειγμα, εν S_4, έχουμε την υποκανονική σειρά $\{p_0\}$, $\{p_0, p_h\}$, K, G (βλέπε §32). Μία υποκανονική (αντ. κανονική) σειρά $\{K_j\}$ είναι ***λεπτοτέρα*** της $\{H_i\}$, αν και μόνον αν, η $\{K_j\}$ έχει τους ίδιους άκρους όρους με την $\{H_i\}$, και κάθε όρος της σειράς $\{H_i\}$ είναι και όρος της σειράς $\{K_j\}$. Μία λεπτοτέρα σειρά K, έχει συνεπώς πλήθος όρων $\geq$ του πλήθους των όρων της σειράς H.

Ορισμός. Μία ομάδα G, η οποία δεν περιέχει υποομάδα $H \subset G$ τέτοια ώστε $H \lhd G$, καλείται ***απλή*** (simple). Η υποομάδα H καλείται ***μεγίστη*** εν G, αν και μόνον αν δεν υπάρχει άλλη υποομάδα H′ εν G, τέτοια ώστε, $H \subset H' \subset G$.

Παρατήρηση. Μία ομάδα G είναι δυνατόν να έχει περισσότερες από μία υποομάδες, που να είναι μέγιστες μέσα σ' αυτήν. Για να τις προσδιορίσουμε, ανατρέχουμε στο διάγραμμα του Hasse των υποομάδων της ομάδας G. Έτσι, αν $G = S_3$, οι υποομάδες $\{p_0, p_i\}$, i = 3, 4, 5 και A_3 είναι μέγιστες υποομάδες.

Κριτήριο. Η υποομάδα H είναι ***μεγίστη κανονική*** υποομάδα της G, αν και μόνον αν, η G/H είναι απλή ομάδα. Στην περίπτωση αυτή ο δείκτης $i(H)_G$ είναι αριθμός πρώτος.

Ορισμός. Δύο υποκανονικές (κανονικές) σειρές $\{H_i\}$ και $\{K_j\}$ της ιδίας ομάδος G είναι ισόμορφες, αν υπάρχει αντιστοιχία ένα προς ένα ανάμεσα στις ομάδες πηλίκα $\{H_{i+1}/H_i\}$ και $\{K_{j+1}/K_j\}$ έτσι ώστε, οι αντίστοιχες ομάδες πηλίκα, να είναι ισόμορφες.

Παρατηρήσεις. Κάθε κυκλική ομάδα της οποίας η τάξις είναι αριθμός πρώτος, είναι απλή. Μία ***συνθετική σειρά*** (composition series) της ομάδας G, είναι μία υποκανονική σειρά της G, της οποίας κάθε όρος είναι απλή ομάς, και $\neq$ της {e}. Συνεπώς μία συνθετική σειρά δεν έχει άλλες εκλεπτύνσεις πλην του εαυτού της. Κάθε πεπερασμένη ομάδα G, έχει μία τουλάχιστον συνθετική σειρά. Η σειρά αυτή κατασκευάζεται αν λάβουμε την μεγίστη κανονική υποομάδα N_1 της G, στην συνέχεια την μεγίστη κανονική υποομάδα N_2 της N_1, κ.ο.κ. μέχρις όου φθάσουμε στην {e}.

Θεώρημα των Jordan - Hölder. Δύο συνθετικές σειρές μιάς πεπερασμένης ομάδας G, είναι ισόμορφες.

Απόδειξη. Έστω οι συνθετικές σειρές

$$G \rhd N_1 \lhd \ \dots \ \lhd N_\kappa = \{e\} \quad (1) \quad \text{και} \quad G \rhd M_1 \lhd \ \dots \ \lhd M_\lambda = \{e\} \quad (2).$$

Θα πρέπει να δείξουμε ότι, $\kappa = \lambda$ και ότι, $N_i / N_{i+1} \cong M_i / M_{i+1}$. Αν $\kappa = 1$, έχουμε την συνθετική σειρά $G \lhd \{e\}$, η οποία είναι και η μοναδική, μιά και η ομάδα G είναι απλή. Κάνουμε επαγωγή στο κ. Υποθέτουμε ότι το θεώρημα ισχύει για όλες τις $<$ του κ τιμές. **Παρατήρηση.** Αν είναι $N_1 = M_1$, τότε δεν έχουμε τίποτα να αποδείξουμε, μιά και καλυπτώμεθα από την επαγωγική υπόθεση.

Ας είναι, λοιπόν, $N_1 \neq M_1$, σχηματίζουμε την τομή $N_1 \cap M_1 \lhd G$, και την συνθετική σειρά που αυτή παράγει. Παρατηρούμε ότι, $N_1 M_1 = G$, μιά και αν $N_1 M_1 \neq G$, επειδή $N_1 M_1 \rhd N_1$ η N_1 (όμοια και για την M_1), δεν θα ήταν μεγίστη.

Ισχύει ότι, (βλέπε §36), $G / N_1 \cong M_1 / N_1 \cap M_1$ και $G / M_1 \cong N_1 / N_1 \cap M_1$. Θεωρούμε, τώρα, και τις συνθετικές σειρές:

$$G \rhd N_1 \lhd N_1 \cap M_1 \lhd K_3 \lhd \ \dots \ \lhd K_\mu = \{e\} \quad (3)$$

$$\text{και} \quad G \rhd M_1 \lhd N_1 \cap M_1 \lhd K_3 \lhd \ \dots \ \lhd K_\mu = \{e\} \quad (4).$$

Οι συνθετικές σειρές (1) και (3) ως επίσης και οι (2) και (4), καλύπτονται από την προηγούμενη παρατήρηση. Απομένουν, συνεπώς δύο "διαφορετικές" συνθετικές σειρές: Οι (3) και (4). Το θεώρημα θα έχει αποδειχθεί, αν και μόνον αν $G / N_1 \cong G / M_1$, ή ισοδύναμα, ότι $M_1 / N_1 \cap M_1 \cong N_1 / N_1 \cap M_1$, ισομορφισμός, που καλύπτεται από την επαγωγική υπόθεση.

Πόρισμα (Schreier). Δύο υποκανονικές (κανονικές) σειρές μιάς ομάδας G, έχουν ισόμορφες εκλεπτύνσεις.

Ορισμός. Μία ομάδα G είναι ***επιλύσιμος,*** αν και μόνον αν έχουμε υποκανονική (κανονική) σειρά, τέτοια ώστε, $i(H_{i+1})_{H_i}$ = αριθμός πρώτος.

Παρατήρηση. Μία ομάδα G που έχει συνθετική σειρά, για την οποία $i(H_{i+1})_{H_i}$ = αριθμός πρώτος, είναι και επιλύσιμος, σύμφωνα με το παραπάνω κριτήριο.

Παραδείγματα 1. Η ***εξ' εναλλαγής ομάδα*** (= η υποομάδα των αρτίων μεταθέσεων) A_n είναι μεγίστη κανονική υποομάδα της S_n. Πράγματι, είναι $i(A_n)_{S_n} = 2$. Άρα, (βλέπε §36), η $A_n \lhd S_n$, και, για τον ίδιο λόγο, η A_n / S_n απλή. Σύμφωνα, λοιπόν, με το παραπάνω κριτήριο η A_n είναι μεγίστη.

2. Ας βρούμε τις συνθετικές σειρές της S_n, για n = 1, 2, 3, 4, ...

α) Για $n=1$, $S_1=\{p_0\}$, και, συνεπώς, πρόκειται για τετριμμένη περίπτωση επιλυσίμου ομάδος.
β) Για $n=2$, $S_2=\{p_0,\ (1\ \ 2)\}$. Η υποκανονική σειρά S_2, $\{p_0\}$ δείχνει ότι, η S_2 είναι επιλύσιμος.
γ) Για $n=3$, $o(S_3)=6$ και ανατρέχουμε στο διάγραμμα των υποομάδων της S_3 στην §36.
Έχουμε τις σειρές S_3, A_3, $\{p_0\}$ και S_3, $\{p_0,p_i\}$, $\{e\}$, με i = 3, 4, 5. Οι τάξεις των ομάδων αυτών, είναι αντίστοιχα, 6, 3, 1 και 6, 2, 1. Σε κάθε σειρά με κ στοιχεία, αντιστοιχούμε την με $\kappa-1$ στοιχεία σειρά των δεικτών $i(H_{i+1})_{H_i}=o(H_{i+1})/o(H_i)$. Για να είναι η σειρά των υποομάδων συνθετική, θα πρέπει κάθε όρος της, να είναι απλή ομάδα. Για τις παραπάνω συνθετικές σειρές, έχουμε σειρά δεικτών {2, 3} και {3, 2}. Κάθε μία σειρά, λοιπόν, απ' αυτές, είναι και συνθετική. Άρα η S_3 είναι επιλύσιμος ομάς.
δ) Για $n=4$, $o(S_4)=24$, $A_4=12$, $i(A_4)_{S_4}=2$. Μπορούμε, συνεπώς, να αρχίσουμε την κατασκευή τις συνθετικής μας σειράς με δύο πρώτους όρους τις ομάδες S_4 και A_4. Το A_4, όπως είδαμε, δεν έχει υποομάδες με τάξη 6 και δείκτη 2. Έχει όμως, δύο (Sylow) υποομάδες με τάξη 4 και δείκτη 3. Κάθε μία απ' αυτές, έχει τρείς υποομάδες με τάξη 2 και δείκτη 2. Τέλος, κλείνουμε τις συνθετικές σειρές μας, με την $\{p_0\}$. Η S_4 είναι, λοιπόν, επιλύσιμος.
ε) Για $n\geq 5$ θα δείξουμε ότι, η A_n δεν περιέχει καμία κανονική υποομάδα $\neq\{p_0\}$, δηλαδή, ότι η A_n είναι απλή. Για τον σκοπό αυτό, αποδεικνύουμε πρώτα το

Λήμμα. Αν η $H\lhd A_n$, $n>3$, περιέχει μία κυκλική υποομάδα τάξεως 3, τότε, $H=A_n$.

Απόδειξη. Υποθέτουμε ότι η κυκλική μας υποομάδα Η, παράγεται από την κυκλική μετάθεση $(1\ \ 2\ \ 3)$. Για $n=3$, $H=A_3$, και δεν έχουμε να αποδείξουμε τίποτα. Για $n>3$, επειδή η Η είναι κανονική υποομάδα της A_n, περιέχει κάθε μετάθεση της μορφής $p^{-1}(1\ \ 2\ \ 3)p$, όπου p αρτία μετάθεση της S_n. Ιδιαίτερα αν $p=(3\ \ 2\ \ k),\ k>3$, $p^{-1}(1\ \ 2\ \ 3)p=(1\ \ k\ \ 2)\in H$ και συνεπώς, $(1\ \ k\ \ 2)^2=(1\ \ 2\ \ k)\in H$, για $k=3,\ 4,\ \ldots$. Όμως, ακριβώς αυτές είναι όλες οι άρτιες μεταθέσεις της S_n. Άρα $H=A_n$.
Είμαστε, τώρα, έτοιμοι να δείξουμε ότι, η Η είναι απλή υποομάδα της A_n, για $n\geq 5$.
Απόδειξη. Έστω $H\lhd A_n$. Κάθε στοιχείο της Η είναι μία μετάθεση, την οποία μπορούμε να την γράψουμε ως γινόμενο κυκλικών μεταθέσεων (βλέπε §30) Το τυχόν $h\in H$ γράφεται, λοιπόν, $h=h_1\ \ldots\ h_k$, όπου h_i ανεξάρτητοι κύκλοι της μορφής $h_i=(1\ \ldots\ i)$. Η μετάθεση $p=(1\ \ 2\ \ 3)\in H$ και αντιμετατίθεται με κάθε στοιχείο της Η. Αν $h\in H$ τότε και $p^{-1}(h_1\ \ldots\ h_k)p=h_1\ \ldots\ p^{-1}h_kp\in H$. Θεωρούμε, τώρα, και το $(p^{-1}h_kp)h_k^{-1}\in H$. Είναι,
$(1\ \ 2\ \ 3)(1\ \ldots\ k)(3\ \ 2\ \ 1)(k\ \ldots\ 1)=(2\ \ 3\ \ 1\ \ 4\ \ldots\ k)(k\ \ldots\ 1)=(1\ \ 3\ \ k)\in H$
.
Η Η περιέχει, λοιπόν, κυκλική υποομάδα, αυτήν που παράγεται από την $(1\ \ 3\ \ k)$, τάξεως 3. Σύμφωνα με το λήμμα είναι, $H=A_n$.

Για $n \geq 5$ έχουμε την συνθετική σειρά $S_n \triangleright A_n \triangleright \{p_0\}$ με αντίστοιχο σειρά δεικτών 2, $\frac{n!}{2}$. Ο $\frac{n!}{2}$ όμως δεν είναι πρώτος. Άρα η S_n δεν είναι επιλύσιμος.