1. Βασικές έννοιες για τις ομάδες

Ορισμός. Ένα μη κενό υποσύνολο G εφοδιασμένο με μια (1.1)
εσωτερική πράξη $*$ λέγεται ομάδα αν ισχύουν τα εξής:
α) Για οποιαδήποτε $a, b, c \in G$ ισχύει $a*(b*c) = (a*b)*c$
δηλ. η πράξη $*$ είναι προσεταιριστική
β) Υπάρχει $e \in G$ τέτοιο ώστε $e*a = a \quad \forall a \in G$.
Το e χαρακτηρίζεται "ουδέτερο στοιχείο της πράξης $*$".
γ) Για κάθε $a \in G$ υπάρχει $a' \in G$ τέτοιο ώστε $a'*a = e$.
Το a' χαρακτηρίζεται "συμμετρικό του a".

Την παραπάνω ομάδα θα συμβολίζαμε με $(G, *)$. Όταν εννοείται (1.2)
και η πράξη, θα λέμε απλώς "η ομάδα G". Αν η πράξη
$*$ είναι αντιμεταθετική, δηλ. ισχύει $a*b = b*a$ για όλα τα
a και b του G, τότε η ομάδα θα λέγεται αντιμεταθετική
ή αβελιανή (προς τιμήν του Νορβηγού μαθηματικού N.H. Abel,
(1802-1829)).

Θεώρημα Αν $(G, *)$ είναι ομάδα και $a, b, c, \ldots$ είναι (1.3)
οποιαδήποτε στοιχεία της, τότε
α) $a*b = a*c \Rightarrow b = c$ (νόμος διαγραφής απ' τ' αριστερά).
β) Αν το e είναι ουδέτερο στοιχείο, τότε $a*e = a$
γ) Αν a' είναι συμμετρικό του a, που αντιστοιχεί στο ουδέτερο
στοιχείο e, τότε $a*a' = e$.
δ) Το ουδέτερο στοιχείο είναι μοναδικό.
ε) $b*a = c*a \Rightarrow b = c$ (νόμος διαγραφής απ' τα δεξιά).
στ) Κάθε μια απ' τις εξισώσεις $a*x = b$ και $y*a = b$, ως
προς αγνώστου το x και το y, αντιστοίχως, έχει αριβώς
μία λύση.
ζ) Το συμμετρικό κάθε στοιχείου a είναι μοναδικό.

Απόδειξη. Έστω e κάποιο ουδέτερο στοιχείο (δεν ξέρουμε ακό-
μη ότι αυτό είναι μοναδικό). Για κάθε $a \in G$ θα συμβολίζουμε
με a' το συμμετρικό του a (ως προς ουδέτερο στοιχείο το e).
Προχωράμε τώρα στην απόδειξη των (α) - (ζ) με τη βοήθεια

των (α)-(γ) του (1.1):

α) $a*b = a*c \Rightarrow a'*(a*b) = a'*(a*c) \Rightarrow$
$\Rightarrow (a'*a)*b = (a'*a)*c \Rightarrow e*b = e*c \Rightarrow b=c.$

β) Έστω ότι $a*e=b$. Θα δείξουμε ότι $b=a$: $a*e=b \Rightarrow$
$a'*(a*e) = a'*b \Rightarrow (a'*a)*e = a'*b \Rightarrow e*e = a'*b \Rightarrow$
$e = a'*b \Rightarrow a'*a = a'*b \Rightarrow$ (λόγω του α) $a=b$.

γ) Έστω $a*a'=b$. Θα δείξουμε ότι $b=e$.: $a*a'=b \Rightarrow$
$a'*(a*a') = a'*b \Rightarrow (a'*a)*a' = a'*b \Rightarrow e*a' = a'*b \Rightarrow$
$a' = a'*b \Rightarrow$ (λόγω του β) $a'*e = a'*b \Rightarrow$ (λόγω του α) $e=b$.

δ) Έστω $\tilde{e}$ ουδέτερο στοιχείο, δηλαδή $\tilde{e}*a = a \ \forall\, a \in G$.
Άρα $\tilde{e}*e = e$. Όμως λόγω του β θα πρέπει $\tilde{e}*e = \tilde{e}$,
δηλαδή $e = \tilde{e}$.

ε) $b*a = c*a \Rightarrow (b*a)*a' = (c*a)*a' \Rightarrow$
$b*(a*a') = c*(a*a') \Rightarrow b*e = c*e \Rightarrow$ (λόγω του β)
$b=c$.

στ) Το $x = a'*b$ επαληθεύει την $a*x=b$ (απλά). Επιπλέον
αποτελεί τη μοναδική λύση της εξίσωσης, διότι αν $a*x_1 = b$
και $a*x_2 = b$, τότε $a*x_1 = a*x_2$ άρα (λόγω του α) $x_1 = x_2$.
Όμοια διαπραγματευόμαστε και την εξίσωση $y*a=b$.

ζ) Κάθε συμμετρικό στοιχείο του a αποτελεί λύση της
εξίσωσης (ως προς y) $y*a = e$, άρα είναι μοναδικό, λόγω του ε.

□

Σημαντική παρατήρηση. Λόγω του (1.3) η συνθήκη β (1.4)
του (1.1) είναι ισοδύναμη με την (φαινομενικά) πολύ ισχυρότερή της:

β') Υπάρχει ένα μοναδικό $e \in G$, τέτοιο ώστε
$e*a = a = a*e \quad \forall\, a \in G$,

ενώ η συνθήκη γ του (1.1) είναι ισοδύναμη με την (φαινομενικά, επίσης) πολύ ισχυρότερή της

γ') Για κάθε $a \in G$ υπάρχει ένα μοναδικό $a' \in G$, τέτοιο
ώστε $a'*a = e = a*a'$.

Έτσι μπορούμε να λέμε "το ουδέτερο στοιχείο της G" καθώς
και "το συμμετρικό του $a \in G$".

Παρατήρηση επί του συμβολισμού. Συνήθως την πράξη της (1.5)
ομάδας συμβολίζομε, απλούστερα, με · και ; μάλιστα, αντί
$a \cdot b$ γράφομε ab (όπως και στην περίπτωση του πολλα-
σιασμού πραγματικών ή μιγαδικών αριθμών). Τότε χαρακτη-
ρίζομε την ομάδα πολλαπλασιαστική και το ουδέτερο στοι-
χείο της συμβολίζομε με 1, ενώ αντί του όρου "συμμετρι-
κό στοιχείο" χρησιμοποιούμε τον όρο "αντίστροφο στοιχείο"
το αντίστροφο του a συμβολίζομε με a^{-1}.
Ωρίσεται συχνά, επίσης, ειδικώς στην περίπτωση αβελιανών
ομάδων, η πράξη συμβολίζεται με + και τότε η ομάδα
χαρακτηρίζεται προσθετική. Το ουδέτερο στοιχείο της συμβο-
λίζεται με 0, αντί "συμμετρικό στοιχείο" λέμε "αντίθετο
στοιχείο" και το αντίθετο του a συμβολίζομε με $-a$.
Τονίζομε ότι ο χαρακτηρισμός μιας ομάδας ως πολλαπλα-
σιαστικής ή προσθετικής δεν αναφέρεται στην ουσία αλλ'
απλώς και μόνο στο συμβολισμό. Σε τούτες τις σημειώσεις
όλα τα γενικά θεωρήματα θα καθιστούν χρήση των συμβολι-
σμών των πολλαπλασιαστικών ομάδων.

Άσκηση. Δείξτε ότι αν a, b είναι δοσμένα στοιχεία (1.6)
μιας πολ/σιαστικής ομάδας G τότε
$$(ab)^{-1} = b^{-1}a^{-1} \quad \text{και} \quad (a^{-1})^{-1} = a$$
Διατυπώστε την αντίστοιχη πρόταση για προσθετικές ομά-
δες. Είναι άραγε να την αποδείξετε;

Πεπερασμένα γινόμενα – Δυνάμεις. Αν $a_1, \dots, a_\nu$ $(\nu \geq 2)$ (1.7)
είναι στοιχεία της $(G, \cdot)$, τότε ορίζομε το πεπερασμένο
γινόμενο $a_1 \cdots a_\nu$ επαγωγικά, ως εξής: Αν $\nu = 2$ τότε
αυτό ισούται με $a_1 a_2$, ενώ για $\nu > 2$
$$a_1 \cdots a_\nu = (a_1 \cdots a_{\nu-1}) \cdot a_\nu$$
Αν $a_1 = \dots = a_\nu = a$ τότε το πεπερασμένο γινόμενο συμβο-
λίζεται με a^ν. Ορίζομε $a^1 = a$ και $a^0 = 1$.
Ισχύουν οι εξής ειδικότητες (αποδείξτε τις ως άσκηση):

$a^{\mu} \cdot a^{\nu} = a^{\mu+\nu}$, $(a^{\mu})^{\nu} = a^{\mu\nu}$, $(ab)^{\nu} = b^{\nu} a^{\nu}$ (1.8)

Ορίζομε γιά θετικό ακέραιο ν, $a^{-\nu} = (a^{-1})^{\nu}$.

<u>Άσκηση.</u> Δείξτε ότι γιά κάθε θετικό ακέραιο ν ισχύει (1.9) $a^{-\nu} a^{\nu} = 1 = a^{\nu} a^{-\nu}$. Στή συνέχεια δείξτε ότι οί (1.8) αληθεύουν γιά οποιεσδήποτε τιμές τών ακεραίων μ, ν (καί όχι μόνο γιά θετικούς ακεραίους μ, ν).

<u>Σημείωση.</u> Στήν περίπτωση προσθετικής ομάδας αντί (1.10) τού πεπερασμένου γινομένου έχομε τό πεπερασμένο άθροισμα $a_1 + \dots + a_\nu$ καί αντί τής δύναμης a^{ν} έχομε τό πολλαπλάσιο νa. Άς σημειωθεί ότι αντί τού $a+(-b)$ γράφομε απλούστερα $a-b$.

<u>Άσκηση.</u> Διατυπώστε τά (1.7), (1.8) καί (1.9) στήν (1.11) περίπτωση προσθετικής ομάδας.

<u>Παραδείγματα ομάδων.</u> α) Οί μή μηδενικοί ρητοί αριθμοί (1.12) εφοδιασμένοι μέ τόν πολλαπλασιασμό (αβελιανή)

β) Οί ακέραιοι αριθμοί εφοδιασμένοι μέ τήν πρόσθεση (αβελιανή).

γ) Έστω K ένα σώμα καί άς θεωρήσομε όλους τούς n×n πίνακες μέ στοιχεία από τό K, οί οποίοι είναι αντιστρέψιμοι. Τό σύνολο αυτών τών πινάκων εφοδιασμένο μέ τόν πολλαπλασιασμό πινάκων αποτελεί ομάδα, ή οποία συμβολίζεται μέ GL(n,K) καί ονομάζεται <u>γενική γραμμική ομάδα τού K βαθμού n.</u>

δ) Τό σύνολο τών ορθογωνίων n×n πινάκων μέ στοιχεία από τό σώμα K (ορθογώνιος σημαίνει ότι ό ανάστροφος πίνακας είναι καί αντίστροφος), εφοδιασμένο μέ τόν πολλαπλασιασμό πινάκων.

ε) Τό σύνολο τών ακεραίων n×n πινάκων, τών οποίων ή ορίζουσα είναι ±1, εφοδιασμένο μέ τόν πολλαπλασιασμό πινάκων.

ς) Τό σύνολο τών μετασχηματισμών ενός συνόλου X≠∅ (αμφιμονοσήμαντες απεικονίσεις τού X επί τού X) μέ πράξη τή σύνθεση τών συναρτήσεων.

ζ) Οι συμμετρίες του ισοπλεύρου τριγώνου (ή του τετραγώνου) με πράξη τη σύνθεση των γεωμετρικών κινήσεων. (Για παράδειγμα αυτό θα αναπτυχθεί εκτενώς στο μάθημα).

η) Έστω m ακέραιος > 1. Στο $\mathbb{Z}$ ορίζουμε την εξής σχέση: $x \equiv y \pmod m$ όταν $m \mid x-y$.

Είναι πολύ εύκολο να δείξει κανείς ότι αυτή είναι μια σχέση ισοδυναμίας και ότι κάθε $x \in \mathbb{Z}$ είναι ισοδύναμος με έναν απ' τους αριθμούς $0, 1, \dots, (m-1)$. Συνεπώς, αν συμβολίσουμε με $\hat{x}$ την κλάση ισοδυναμίας του $x \in \mathbb{Z}$ τότε $\hat{x} = \hat{0}$ ή $\hat{1}$ ή ... ή $\widehat{(m-1)}$. Το σύνολο των κλάσεων ισοδυναμίας (δηλ. τα λεγόμενα σύνολα-πηλίκο) συμβολίζεται με $\mathbb{Z}_m$ και ισούται με $\{\hat{0}, \hat{1}, \dots, \widehat{(m-1)}\}$.

Στο $\mathbb{Z}_m$ ορίζουμε την εσωτερική πράξη + ως εξής:

$$\hat{a} + \hat{b} = \widehat{a+b}.$$

Αυτή είναι καλά ορισμένη (δηλ. αν $\hat{a}' = \hat{a}$ και $\hat{b}' = \hat{b}$, τότε $\hat{a}' + \hat{b}' = \hat{a} + \hat{b}$) και δίνει στο $\mathbb{Z}_m$ δομή αβελιανής ομάδας.

Στο $\mathbb{Z}_m$ μπορούμε να ορίσουμε και πολλαπλασιασμό ως εξής:

$$\hat{a} \cdot \hat{b} = \widehat{ab}$$

και να διαπιστώσουμε ότι η πράξη αυτή είναι, επίσης, καλά ορισμένη, αλλά το $(\mathbb{Z}_m, \cdot)$ δεν είναι ομάδα *.

θ) Έστω $\mathbb{Z}_m$ όπως στο παράδειγμα (η). Ορίζουμε $\mathbb{Z}_m^* = \{\hat{a} \in \mathbb{Z}_m : (a,m) = 1\}$. Το σύνολο αυτό είναι καλά ορισμένο, δηλ. αν $\hat{a} = \hat{b}$ και $(a,m) = 1$ τότε και $(b,m) = 1$ (ασκηση). Το $\mathbb{Z}_m^*$ εφοδιασμένο με τον πολ/σιασμό κλάσεων (βλ. τέλος του Παραδείγματος η) είναι ομάδα. (συνέχεια στη σελ. 5α)

Ασκήσεις α) Έστω $G \neq \emptyset$ ένα πεπερασμένο σύνολο εφοδιασμένο με μια εσωτερική πράξη $\cdot$ για την οποία ισχύουν τα α και β του (1.1) καθώς επίσης και ο νόμος της διαγραφής απ' τα δεξιά. Δείξτε τότε ότι το $(G, \cdot)$ είναι ομάδα. (1.13)

β) Με τη βοήθεια του α αποδείξτε τον τελευταίο ισχυρισμό του (1.12) η. Θυμηθείτε ότι ένας πρώτος διαιρεί

* Δες όμως το Παράδειγμα θ.

$(\mathbb{Z}_m^*, \cdot)$ είναι ομάδα

Το $\mathbb{Z}_m^*$ είναι κλειστό ως προς την $\cdot$, διότι, αν $\hat{a}, \hat{b} \in \mathbb{Z}_m^*$, τότε $(a,m)=1$, $(b,m)=1$ άρα και $(a\cdot b, m)=1$, που σημαίνει ότι $\hat{a}\cdot\hat{b} \in \mathbb{Z}_m^*$.

Η προσεταιριστικότητα της $\cdot$ στο $\mathbb{Z}_m^*$ είναι προφανής, ενώ το ουδέτερο στοιχείο είναι το $\hat{1}$.

Ο νόμος της διαγραφής από τα δεξιά ισχύει, επίσης. Πράγματι, αν $\hat{a}, \hat{b}, \hat{c} \in \mathbb{Z}_m^*$ και $\hat{a}\cdot\hat{c} = \hat{b}\cdot\hat{c}$ τότε $\hat{a\cdot c} = \hat{b\cdot c}$ άρα $m \mid ac - bc$, δηλ $m \mid (a-b)c$. Επειδή $(m,c)=1$, από γνωστή πρόταση της στοιχειώδους Θεωρίας Αριθμών συμπεραίνουμε ότι $m \mid a-b$, άρα $\hat{a} = \hat{b}$.

Συμφωνα με την άσκηση α, το $\mathbb{Z}_m^*$ με την πράξη $\cdot$ είναι ομάδα.

Είναι φανερό ότι το πλήθος των στοιχείων της ομάδας αυτής είναι όσοι και οι αριθμοί μεταξύ 0 και $m-1$, οι οποίοι είναι πρώτοι προς τον m. Αυτό το πλήθος δίνεται από τη λεγόμενη συνάρτηση φ του Euler. Ο τύπος της φ είναι ο εξής:

Αν $p_1, \dots, p_k$ είναι όλοι οι διαφορετικοί πρώτοι διαιρέτες του m, τότε

$$\varphi(m) = m\left(1-\frac{1}{p_1}\right)\cdots\left(1-\frac{1}{p_k}\right)$$

τό ζητούμενο δύο ακεραίων, όν και μόνο αν διαιρεί τον ένα, τουλάχιστον, από αυτούς.

γ.) Δείξτε ότι αν $(G,\cdot)$ είναι πεπερασμένη αβελιανή ομάδα με ν στοιχεία, τότε $a^{\nu}=1 \ \forall a\in G$.

δ.) Με τη βοήθεια των β και γ δείξτε ότι αν ο p είναι πρώτος αριθμός και a είναι ακέραιος μη διαιρετός από τον p, τότε $a^{p-1}\equiv 1 \pmod p$ (ή αλλιώς $p \mid a^{p-1}-1$. Αυτό είναι το λεγόμενο "μικρό θεώρημα του Fermat").

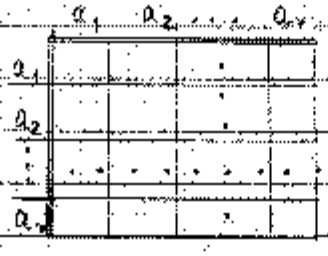
ε.) Έστω d θετικός ακέραιος, όχι τέλεια τετράγωνο. Αποδείξτε ότι το σύνολο $\mathbb{Z}[\sqrt{d}]=\{x+y\sqrt{d} \mid x,y\in\mathbb{Z} \text{ με } x^2-dy^2=1\}$ εφοδιασμένο με τον πολλαπλασιασμό του $\mathbb{R}$ είναι ομάδα.

ς.) Έστω $G\neq\emptyset$ ένα πεπερασμένο σύνολο εφοδιασμένο με μια εσωτερική πράξη $\cdot$ για την οποία ισχύουν τα α και β του (1.1). Δείξτε ότι το $(G,\cdot)$ είναι ομάδα αν και μόνο αν ικανοποιείται η συνθήκη: $\forall a\in G$ το σύνολο

$$Ga \overset{\text{ορ}}{=} \{xa \mid x\in G\}$$

ταυτίζεται με το G. Επίσης, αν το $(G,\cdot)$ είναι ομάδα, τότε $aG=G$.

Ο πίνακας της πράξης μιας πεπερασμένης ομάδας. Έστω ότι (1.14) τα στοιχεία της πεπερασμένης ομάδας είναι $a_1,\dots,a_\nu$. Τοποθετούμε σε ορίζοντια γραμμή τα $a_1,\dots,a_\nu$ και σε μια στήλη τα ίδια στοιχεία (με την ίδια διάταξη) ως εξής:



Έτσι σχηματίζεται ένας πίνακας με τετραγωνάκια: Στο τετραγωνάκι που αντιστοιχεί στη γραμμή του a_i και στη στήλη του a_j γράφουμε το αποτέλεσμα $a_i\cdot a_j$.

Λόγω της ύπαρξης (1.13) ε, κάθε γραμμή καθώς και κάθε στήλη του συμπληρωμένου κατ' αυτό τον τρόπο πίνακα αποτελείται από τα $a_1,\dots,a_\nu$ με κάποια διάταξη γραμμένα. (Δείχνω, επομένως, επαναληψη ενός στοιχείου στην ίδια

γραμμή ή στήλη). Π.χ. ο πίνακας της πρόσθεσης της ομάδας $(\mathbb{Z}_6, +)$ είναι

	$\hat{0}$	$\hat{1}$	$\hat{2}$	$\hat{3}$	$\hat{4}$	$\hat{5}$
$\hat{0}$	$\hat{0}$	$\hat{1}$	$\hat{2}$	$\hat{3}$	$\hat{4}$	$\hat{5}$
$\hat{1}$	$\hat{1}$	$\hat{2}$	$\hat{3}$	$\hat{4}$	$\hat{5}$	$\hat{0}$
$\hat{2}$	$\hat{2}$	$\hat{3}$	$\hat{4}$	$\hat{5}$	$\hat{0}$	$\hat{1}$
$\hat{3}$	$\hat{3}$	$\hat{4}$	$\hat{5}$	$\hat{0}$	$\hat{1}$	$\hat{2}$
$\hat{4}$	$\hat{4}$	$\hat{5}$	$\hat{0}$	$\hat{1}$	$\hat{2}$	$\hat{3}$
$\hat{5}$	$\hat{5}$	$\hat{0}$	$\hat{1}$	$\hat{2}$	$\hat{3}$	$\hat{4}$

Κατασκευάστε ως άσκηση τον πίνακα πολ/σιασμού της ομάδας $(\mathbb{Z}_7^*, \cdot)$.

Έστω ένα πεπερασμένο σύνολο $G\ (\neq \emptyset)$ εφοδιασμένο με μια εσωτερική πράξη $*$. Αν μας δοθεί ο πίνακας της πράξης αυτής μπορούμε να πάρουμε όλες τις απαραίτητες πληροφορίες προκειμένου να διαπιστώσουμε αν το $(G, *)$ είναι ή όχι ομάδα. Μια αναγκαία και ικανή συνθήκη για να ισχύουν τα β και γ του (1.1) είναι, ~~όπως εύκολα διαπιστώνουμε~~, κάθε γραμμή και κάθε στήλη του πίνακα να περιέχει τα στοιχεία του G χωρίς επαναλήψεις. (*) Αυτό που μένει να ελεγχθεί είναι η προσεταιριστικότητα της πράξης και αυτό είναι κάτι που απαιτεί πολλή (ούτε καν πολύ εύκολη) δουλειά, εκτός αν έχουμε κάποιες επιπλέον πληροφορίες για τη φύση της πράξης. Αν λ.χ. ξέρουμε ότι η πράξη είναι σύνθεση συναρτήσεων, ή πολ/σιασμός πινάκων, ή σύνθεση γεωμετρικών κινήσεων, τότε η προσεταιριστικότητα είναι εξασφαλισμένη.

Κάμια φορά, επίσης, καταφεύγουμε στην κατασκευή ενός μοντέλου - ομάδας, όπως στην περίπτωση του εξής παραδείγματος: Δίνεται το σύνολο $G = \{1, a, b, c, d, e\}$ με εσωτερική πράξη $\cdot$ και πίνακα

(*) Ένας, αν ο πίνακας είναι δίπλα σ' ένα πραγματικό φύλλο χαρτί, και υπάρχει στοιχείο a_i τ.ω. η γραμμή που αντιστοιχεί στο a_i να είναι $a_1, a_2, \ldots, a_i, \ldots, a_n$ και η στήλη του a_i η ίδια, γραμμένη κατακόρυφα. Αυτό ισοδυναμεί, προφανώς, με την ύπαρξη ουδετέρου στοιχείου.

	1	a	b	c	d	e
1	1	a	b	c	d	e
a	a	b	1	e	c	d
b	b	1	a	d	e	c
c	c	d	e	1	a	b
d	d	e	c	b	1	a
e	e	c	d	a	b	1

Το κριτήριο που υποδείξαμε πριν αλγοδείκνυε ότι οι συνθήκες β, γ του (1.1) ικανοποιούνται. Η προσεταιριστικότητα είναι πολύ κοπιαστικό και έλεγχθεί αφού απαιτεί την εξέταση $6^3 = 216$ περιπτώσεων (ευτυχώς ευκολες κι αν είναι αυτές). Κατασκευάζουμε ένα μοντέλο του αλγεβρικού συνόλου G ως εξής:

$$1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad a = \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix}, \quad b = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$$

$$c = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad d = \begin{pmatrix} 1 & 0 \\ -1 & -1 \end{pmatrix}, \quad e = \begin{pmatrix} -1 & -1 \\ 0 & 1 \end{pmatrix}$$

και ως προς θεωρούμε τον πολλαπλασιασμό πινάκων. Κάνοντας τον πίνακα πολλαπλασιασμού με αυτούς τους συγκεκριμένους 2×2 πίνακες βλέπουμε ότι είναι ο ίδιος με τον παραπάνω πίνακα της πράξης της G. Όμως η προσεταιριστικότητα στον πολλαπλασιασμό των πινάκων ισχύει, άρα και η προσεταιριστικότητα στον παραπάνω πίνακα είναι εξασφαλισμένη και, συνεπώς, το $(G, \cdot)$ είναι ομάδα.

Άσκηση Οι παραπάνω πίνακες περιγράφουν ομάδες; (1.15)

	a	b	c	d
a	b	d	a	c
b	d	c	b	a
c	a	b	c	d
d	c	a	d	b

	a	b	c	d
a	a	b	c	d
b	b	a	d	c
c	c	d	a	a
d	d	c	b	b

Υποομάδες. Έστω $(G,\cdot)$ μια ομάδα. Ένα μη κενό υποσύνο- (1.16)
λο H του G, εφοδιασμένο με την πράξη της G, θα λέγεται υποομάδα της G, αν το $(H,\cdot)$ είναι ομάδα.

Άσκηση. Αν η H είναι υποομάδα της G δείξτε ότι το ουδέτερο (1.17)
στοιχείο της H ταυτίζεται με το ουδέτερο στοιχείο της G. Επίσης, για κάθε $x\in H$ το συμμετρικό του x, είτε θεωρώντας την ομάδα H, είτε την ομάδα G, είναι το ίδιο.

Πρόταση. Έστω $(G,\cdot)$ ομάδα και $\emptyset\neq H\subseteq G$. Το H είναι υπο- (1.18)
ομάδα της G αν και μόνο αν (i) Το H είναι κλειστό ως προς την πράξη $\cdot$, και (ii) Για κάθε $x\in H$ είναι $x^{-1}\in H$.
Αν η G είναι πεπερασμένη ομάδα τότε για να είναι το H υποομάδα της αρκεί μονάχα η συνθήκη (i).
Απόδειξη. Ο πρώτος ισχυρισμός είναι μια πολύ απλή άσκηση. Για τον δεύτερο ισχυρισμό θα δείξουμε ότι η συνθήκη (i) συνεπάγεται την (ii). Πράγματι, αν η G είναι πεπερασμένη, τότε το $H\subseteq G$ είναι πεπερασμένο και κλειστό ως προς την $\cdot$. Άρα, αν $x\in H$ το σύνολο $xH=\{xa/a\in H\}\subseteq H$ ταυτίζεται με το H, αφού έχουν το ίδιο πλήθος στοιχείων. Άρα $\exists\, a\in H$ με $xa=x$, δηλ. $1\in H$. Τότε $\exists\, x'\in H$ με $x\cdot x'=1$, άρα $x'=x^{-1}$ και $x^{-1}\in H$. □

Τάξη ενός στοιχείου μιας ομάδας. Έστω $(G,\cdot)$ μια ομάδα (1.19)
και $x\in G$. Υπάρχουν δύο ενδεχόμενα: (i) ή υπάρχουν δύο διαφορετικοί ακέραιοι m,n τέτοιοι ώστε $x^m=x^n$, ή (ii) για κάθε ζεύγος διαφορετικών ακεραίων m,n είναι $x^m\neq x^n$.

Πρόταση. Στην περίπτωση (i) του (1.19) υπάρχει ένας (1.20)
θετικός ακέραιος g, τέτοιος ώστε $x^g=1$ και $x^n\neq 1$ για κάθε θετικό $n<g$. Ο g λέγεται τάξη του x και για κάθε $n\in\mathbb{Z}$ με $x^n=1$ ισχύει $g\mid n$.
Η περίπτωση (ii) του (1.19) ισχύει αν και μόνο αν $x^n\neq 1$ για κάθε μη μηδενικό ακέραιο n. Όταν ισχύει, τότε λέμε ότι το x είναι άπειρης τάξης.
Απόδειξη. Έστω ότι ισχύει η περίπτωση (i) του (1.19). Τότε, αν $m>n$, θα ισχύει $x^d=1$ όπου $d=m-n>0$

(απόδειξε το με καθε αντιστροφέτητα) Έστω λοιπόν g ο ελάχιστος απ' τους θετικούς ακεραίους d με $x^d = 1$. Μένει να δείξουμε ότι αν $x^n = 1$ για κάποιο $n \in \mathbb{Z}$, τότε $g \mid n$. Πράγματι, απ' την ταυτότητα της διαιρέσεως έχουμε $n = ag + v$, όπου $a \in \mathbb{Z}$ και $0 \le v < g$. Άρα $1 = x^n = (x^g)^a \cdot x^v = 1 \cdot x^v = x^v$. Αν ήταν $v > 0$, τότε θα έρχόμαστε σε αντίφαση με τον ορισμό του g. Άρα $v = 0$, δ.έ.δ.

Στη συνέχεια, έστω ότι ισχύει το (ii) του (1.19). Τότε, εξ υποθέσεως, $x^n \neq x^0 = 1$ για κάθε μη μηδενικό ακέραιο n. Αντίστροφα, αν ισχύει $x^n \neq 1$ για κάθε μη μηδενικό ακέραιο n τότε, βέβαια, δεν είναι δυνατόν να ισχύει $x^m = x^n$ με $m \neq n$, αλλιώς αυτή η σχέση θα συνεπαγόταν την $x^{m-n} = 1$ με $m - n \neq 0$. □

Άσκηση. Δείξτε ότι η τάξη ενός στοιχείου του και του αντιστρόφου του (πεπερασμένες είτε άπειρες τάξεις) συμπίπτουν. (1.21)

Άσκηση. Δείξτε ότι το σύνολο $\langle x \rangle \overset{\text{ορ}}{=} \{x^n \mid n \in \mathbb{Z}\}$ είναι υποομάδα της G και λέγεται (κυκλική) υποομάδα παραγόμενη απ' το x. (1.22)

Άσκηση. Έστω ο παρακάτω πίνακας πολλαπλασιασμού μιας ομάδας: (1.23)

	1	a	b	c	d	f	g	h	j	k	l	m
1	1	a	b	c	d	f	g	h	j	k	l	m
a	a	k	l	d	f	g	h	j	c	b	m	1
b	b	l	1	g	h	j	c	d	f	m	a	k
c	c	j	g	b	k	a	1	m	l	h	f	d
d	d	c	h	l	b	k	a	1	m	j	g	f
f	f	d	j	m	l	b	k	a	1	c	h	g
g	g	f	c	1	m	l	h	k	a	d	j	h
h	h	g	d	a	1	m	l	b	k	f	c	j
j	j	h	f	k	a	1	m	l	b	g	d	c
k	k	b	m	f	g	h	j	c	d	l	1	a
l	l	m	a	h	j	c	d	f	g	1	k	b
m	m	1	k	j	c	d	f	g	h	a	b	l

Υπολογίστε τις τάξεις των στοιχείων της και βρείτε τις υποομάδες που παράγονται από κάθε στοιχείο.

Κυκλικές ομάδες. Έστω $(G,\cdot)$ μια ομάδα. Αν υπάρχει $x\in G$ τέτοιο ώστε $G=\langle x\rangle$ (βλ. (1.22)), τότε η G χαρακτηρίζεται ως κυκλική ομάδα. Και αν μεν η τάξη του x είναι άπειρη, τότε η G χαρακτηρίζεται άπειρη κυκλική ομάδα· αν δε τάξη του x είναι g, τότε η G χαρακτηρίζεται κυκλική τάξης g. (1.24)

Εν γένει, τάξη μιας τυχούσας ομάδας G λέμε το πλήθος των στοιχείων της και τη συμβολίζουμε με $|G|$.

Πρόταση. Κάθε υποομάδα μιας κυκλικής ομάδας $(G,\cdot)$ (πεπερασμένης είτε άπειρης) είναι κυκλική. (1.25)

Απόδειξη. Έστω $G=\langle x\rangle$ για κάποιο $x\in G$ και H υποομάδα της G. Τα στοιχεία της H είναι της μορφής x^n με $n\in\mathbb{Z}$. Αν δεν υπάρχει $n\neq 0$ με $x^n\in H$, τότε $H=\langle 1\rangle$. Αν υπάρχει $n\neq 0$ με $x^n\in H$, τότε και $x^{-n}=(x^n)^{-1}\in H$, και ο ένας από τους αφαιρούμενους $n,-n$ είναι θετικός. Έστω λοιπόν σ' αυτήν την περίπτωση h ο ελάχιστος θετικός ακέραιος για τον οποίο $x^h\in H$. Τότε εύκολα μπορεί να δείξει κανείς (πρβλ. με την απόδειξη της πρότασης 1.20) ότι κάθε $m\in\mathbb{Z}$ για το οποίο $x^m\in H$, είναι πολλαπλάσιο του h. Συνεπώς $H\subseteq\langle x^h\rangle$. Προφανώς δε, $\langle x^h\rangle\subseteq H$, άρα $H=\langle x^h\rangle$. □

Για τις πεπερασμένες κυκλικές ομάδες μπορούμε να αποδείξουμε ένα πολύ πιο συγκεκριμένο αποτέλεσμα. Αυτό θα γίνει στο 3ο κεφάλαιο.

Ασκήσεις α) Δείξτε ότι για κάθε ακέραιο $n\geq 2$ το σύνολο των μιγαδικών n-οστών ριζών του 1, εφοδιασμένο με τον πολλαπλασιασμό του $\mathbb{C}$, αποτελεί κυκλική ομάδα τάξης n. (1.26)

β) Αν η G είναι κυκλική ομάδα τάξεως g και $G=\langle x\rangle$, τότε τα στοιχεία $1,x,\dots,x^{g-1}$ είναι διαφορετικά μεταξύ τους και $x^g=1$.

(1.27) Πρόταση. Έστω $\langle a \rangle$ κυκλική ομάδα τάξεως g. Αναγκαία και ικανή συνθήκη για να είναι το a^n γεννήτορας της $\langle a \rangle$ είναι $(n, g) = 1$.

Απόδειξη. Έστω a^n γεννήτορας της $\langle a \rangle$. Τότε, για κάποιο $k \in \mathbb{Z}$ έχουμε $a = (a^n)^k$, άρα $a^{nk-1} = 1$. Συνεπώς (Πρόταση 1.20), $g \mid nk-1$. Γράφοντας τώρα $nk - 1 = g \cdot l$, $l \in \mathbb{Z}$, βγαίνει φανερό ότι τα n, g δεν είναι δυνατόν να έχουν κοινό διαιρέτη > 1.

Αντιστρόφως, αν $(n, g) = 1$ τότε, λόγω γνωστής Πρότασης της Θεωρίας Αριθμών, υπάρχουν $k, l \in \mathbb{Z}$ τ.ώ. $kn + lg = 1$. Τότε $a = a^{kn} \cdot a^{lg} = a^{kn}$, διότι $a^g = 1$ (Άσκηση 1.26 (β)). Άρα $a \in \langle a^n \rangle$, απ' όπου βγαίνει φανερό $\langle a \rangle = \langle a^n \rangle$.

2. Μεταθέσεις

Ορισμός. Μετάθεση n αντικειμένων $a_1, \dots, a_n$ είναι μιά (2.1)
αμφιμονοσήμαντη απεικόνιση του συνόλου $\{a_1, \dots, a_n\}$ επί του εαυτού του. Έστω ότι σε μιά μετάθεση των $a_1, \dots, a_n$ έχουμε

$$a_1 \longrightarrow a_{i_1},\ a_2 \longrightarrow a_{i_2},\ \dots,\ a_n \longrightarrow a_{i_n}\ .$$

Τότε, είναι φανερό ότι όποια πληροφορία χρειαζόμαστε γι' αυτή τη μετάθεση την παίρνουμε άν ξέρουμε την αντίστοιχη μετάθεση του συνόλου δεικτών $\{1, \dots, n\}$, δηλ. τη μετάθεση: $1 \longrightarrow i_1,\ 2 \longrightarrow i_2,\ \dots,\ n \longrightarrow i_n$ (2.2)
Γι' αυτό, όταν μελετούμε τη γενική θεωρία των μεταθέσεων των n αντικειμένων, αρκεί να θεωρούμε ως αντικείμενα τους αριθμούς $1, \dots, n$. Η κανονική γραφή της μετάθεσης (2.2) είναι

$$\begin{pmatrix} 1 & 2 & \dots & n \\ i_1 & i_2 & \dots & i_n \end{pmatrix}, \qquad (2.3)$$

όπου, εννοείται ότι $\{i_1, i_2, \dots, i_n\} = \{1, 2, \dots, n\}$ (η διάταξη, εν γένει, δεν διατηρείται). Συνεπώς οι μεταθέσεις των n αντικειμένων είναι τόσες όσοι και οι τρόποι που μπορούμε να γράψουμε τους αριθμούς $1, 2, \dots, n$ στην κάτω γραμμή της (2.3), δηλ. $n!$ (βασική πρόταση της Συνδυαστικής). Επίσης, μπορούμε να θεωρήσουμε τη σύνθεση (ή πολλαπλασιασμό) δύο μεταθέσεων, ως ειδική περίπτωση της σύνθεσης απεικονίσεων. Επειδή η σύνθεση δύο αμφιμονοσήμαντων και "επί" απεικονίσεων είναι απεικόνιση του ίδιου τύπου, έπεται ότι η σύνθεση δύο μεταθέσεων των n αντικειμένων είναι, επίσης, μιά μετάθεση των n αντικειμένων. Επίσης, επειδή κάθε αμφιμονοσήμαντη αντιστοιχία ενός συνόλου επί του εαυτού του (μετασχηματισμός) έχει την αντίστροφή της αντιστοιχία, που είναι αμφιμονοσήμαντη και επί, έπεται ότι για κάθε μετάθεση των n πραγμάτων υπάρχει και η αντίστροφή της μετάθεση. Το ζητούμενο τους, δηλαδή, είναι η κανονική μετάθεση, δηλαδή, η μετάθεση

$$1=\begin{pmatrix}1 & 2 & \dots & n\\ 1 & 2 & \dots & n\end{pmatrix}$$

Τέλος, ή σύνθεση μεταθέσεων είναι πρόσεταιριστική πράξη, άφού ή σύνθεση των απεικονίσεων, έν γένει έχει αυτή την ιδιότητα.

Όλα τα προηγούμενα αποδεικνύουν λοιπόν το

<u>Θεώρημα</u>. Το σύνολο των μεταθέσεων των n αντικειμένων (2.4) εφοδιασμένο με τη σύνθεση των μεταθέσεων αποτελεί πεπερασμένη ομάδα τάξης $n!$ Η ομάδα αυτή ονομάζεται <u>συμμετρική ομάδα βαθμού n</u> και συμβολίζεται με S_n.

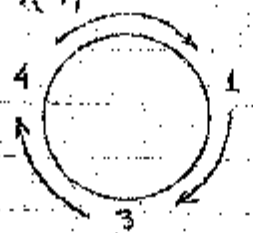
□

Ο ομάδα S_n δεν είναι αβελιανή. Πχ. για τις μεταθέσεις

$\sigma=\begin{pmatrix}1 & 2 & 3\\ 3 & 2 & 1\end{pmatrix}$ και $\tau=\begin{pmatrix}1 & 2 & 3\\ 2 & 1 & 3\end{pmatrix}$ έχομε $\sigma\tau=\begin{pmatrix}1 & 2 & 3\\ 2 & 3 & 1\end{pmatrix}$

ενώ $\tau\sigma=\begin{pmatrix}1 & 2 & 3\\ 3 & 1 & 2\end{pmatrix}$.

Πολλές φορές στα συμβολισμό μιας μετάθεσης παραλείπομε τα στοιχεία που μένουν αναλλοίωτα και γράφομε τα υπόλοιπα "κυκλικά". Για παράδειγμα, η μετάθεση $\sigma\in S_5$ με $\sigma=\begin{pmatrix}1 & 2 & 3 & 4 & 5\\ 3 & 2 & 4 & 1 & 5\end{pmatrix}$, θα μπορούσε να γραφτεί απλούστερα ως $\sigma=(1\,3\,4)$, που σημαίνει ότι το 2 και το 5 μένουν αναλλοίωτα, ενώ τα 1, 3, 4 μεταβάλλονται κατά το κυκλικό σχήμα



Γι' αυτό το συμβολισμό θα μπορούσε κανείς να προβάλει την αντίρρηση ότι γράφοντας π.χ. $(1\,3\,4)$ δεν είναι σαφές αν αναφερόμαστε σε μετάθεση των S_4, του S_5 ή του S_{18}! Πράγματι, έτσι είναι, αλλά στην πράξη αυτό γίνεται σαφές από τα συμφραζόμενα ή από ότι έχει προηγηθεί. Επίσης, μια άλλη παρατήρηση είναι ότι η $\sigma=(1\,3\,4)$

μπορεί να' γραφεί τοσοδύναμα καὶ ὡς (3 4 1) ἢ (4 1 3).
Ἂς θεωρήσωμε τώρα τὴ μετάθεση $\tau \in S_7$,
$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 2 & 5 & 7 & 3 & 6 & 1 \end{pmatrix}$. Αὐτὴ μπορεί να' γραφεί καὶ
ὡς (1 4 7)(3 5) ἢ (3 5)(1 4 7).
Ἡ μετάθεση (1 3 4) μπορεί να' ἰδωθεῖ ὡς μετάθεση τῶν
τριῶν "ἀντικειμένων" 1, 3, 4, τὰ ὁποῖα ἀναδιατάσσονται
(μετατίθενται) κυκλικά καὶ γι' αὐτὸ χαρακτηρίζεται
κυκλικὴ μετάθεση, ἢ ἁπλῶς κύκλος· καὶ τὸ πλῆθος τῶν
ἀντικειμένων τοῦ κύκλου λέγεται μῆκος τοῦ κύκλου.
(στὴν περίπτωση τῆς σ τὸ μῆκος εἶναι 3). Στὸ δεύτερο
παράδειγμα ἡ τ παριστάνεται ὡς γινόμενο δύο κύκλων
μὲ μῆκη 2 καὶ 3, οἱ ὁποῖοι ἀντιμετατίθενται. Στὴν
πραγματικότητα αὐτὸ εἶναι εἰδικὴ περίπτωση τοῦ παρακά-
τω ἀποτελέσματος.
Θεώρημα. Κάθε μετάθεση γράφεται ὡς γινόμενα κύκλων (2.5)
ξένων ἀνὰ δύο. Οἱ κύκλοι αὐτοὶ ἀντιμετατίθενται. Ἡ
διάσπαση τῆς μετάθεσης σὲ κύκλους ξένους ἀνὰ δύο εἶ-
ναι μοναδική, ἂν δὲν ληφθεῖ ὑπ' ὄψη ἡ σειρὰ μὲ τὴν ὁποί-
α γράφονται αὐτοὶ οἱ κύκλοι.
Ἀπόδειξη. Ἔστω $\sigma \in S_n$. Ἔστω $a \in \{1, \dots, n\}$ καὶ θεωροῦ-
με τὴ διαδοχὴ τῶν ἀριθμῶν $a, \sigma(a), \sigma^2(a), \dots$, οἱ ὁποῖοι,
φυσικά, ἀνήκουν στὸ $\{1, \dots, n\}$. Συνεπῶς γιά κάποιο k,
τὸ $\sigma^k(a)$ πρέπει να' συμπίπτει μὲ κάποιο ἀπὸ τὰ προηγού-
μενά του $a, \sigma(a), \dots, \sigma^{k-1}(a)$. Ἔστω λοιπὸν $\sigma^k(a) = \sigma^\ell(a)$
μὲ $0 \leq \ell < k-1$ (ἐννοεῖται ὅτι $\sigma^0 = 1 =$ ταυτοτικὴ μετάθεση).
Τότε $\sigma^{k-\ell}(a) = 1$, $k-\ell > 0$, ἄρα ὑπάρχει ἕνας ἐλάχιστος
θετικὸς ἀκέραιος r, τέτοιος ὥστε $\sigma^r(a) = a$. Ἐξ ὁρισμοῦ
τοῦ r, οἱ ἀριθμοὶ $a, \sigma(a), \dots, \sigma^{r-1}(a)$ εἶναι διαφορετικοί.
Εἶναι φανερὸ τώρα ὅτι ἡ σ μπορεῖ να' γραφεῖ ὡς γινόμενο
$$\sigma = \sigma' \circ (a\ \sigma(a) \dots \sigma^{r-1}(a))$$
ὅπου ἡ μετάθεση $\sigma' \in S_n$ ἀφήνει ἀναλλοίωτους ὅλους τοὺς
ἀριθμοὺς $a, \sigma(a), \dots, \sigma^{r-1}(a)$, ἐνῶ γιὰ $b \notin \{a, \sigma(a), \dots, \sigma^{r-1}(a)\}$
$(1 \leq b \leq n)$ $\sigma'(b) = \sigma(b)$. Ἂν $r = n$, τότε $\sigma' = 1$, ὁπότε ἡ

σ ταυτίζεται μὲ τὸν κύκλο $(a\ \sigma(a)\ \dots\ \sigma^{r-1}(a))$. Ἂν $r<n$, τότε ὑπάρχει $a' \in \{1,\dots,n\} - \{a, \sigma(a), \dots, \sigma^{r-1}(a)\}$. Ἐπαναλαμβάνω γιὰ τὸ a' καὶ τὴ σ' ὅ,τι ἔκανα γιὰ τὸ a καὶ τὴ σ προηγουμένως καὶ πετυχαίνω μιὰ ἀνάλυση

$$\sigma' = \sigma'' \circ (a'\ \sigma'(a') \dots, \sigma'^{r'-1}(a')) \quad (2.6)$$

Ἰσχυρίζομαι ὅτι οἱ κύκλοι τοῦ a καὶ τοῦ a' εἶναι ξένοι. Πράγματι, ἔστω ὅτι εἴχαμε $\sigma'^{\mu}(a') = \sigma^{\nu}(a)$ γιὰ κάποια μ καὶ ν $(0 \le \mu \le r'-1\ ,\ 0 \le \nu \le r-1)$. Ἐξ ὁρισμοῦ τῆς σ' εἶναι $\sigma'(\sigma^{\nu}(a)) = \sigma^{\nu}(a)$, συνεπῶς,

$$a' = \sigma'^{r'-\mu}(\sigma'^{\mu}(a')) = \sigma'^{r'-\mu}(\sigma^{\nu}(a)) = \sigma^{\nu}(a)$$

κι ἐρχόμαστε ἔτσι σὲ ἀντίφαση μὲ τὴν ἐκλογὴ τοῦ a'.
Ἔτσι, λόγῳ καὶ τῆς (2.6),

$$\sigma = \sigma'' \circ (a', \sigma'(a) \dots \sigma'^{r'-1}(a')) \circ (a\ \sigma(a) \dots \sigma^{r-1}(a))$$

ὅπου οἱ κύκλοι στὸ δεξιὸ μέλος εἶναι ξένοι. Ἐπίσης ἡ σ'' ἀφήνει ἀναλλοίωτους τοὺς ἀριθμοὺς τῶν δύο κύκλων καὶ συμπίπτει μὲ τὴ σ γιὰ τοὺς ἀριθμοὺς τοὺς ἐκτὸς τῶν δύο κύκλων (ἂν ὑπάρχουν). Ἔτσι, ἂν $r+r' = n$, τότε $\sigma'' = 1$ κι ἐχομε τελειώσει. Ἂν ὄχι ἐπαναλαμβάνομε τὴ διαδικασία ποὺ περιγράψαμε πρίν, κ.ὁ.κ. Κάποτε (ὅταν $r+r'+\dots = n$) θὰ σταματήσει ἡ διαδικασία καὶ τότε ἡ σ θὰ ἔχει βρεθεῖ ὡς γινόμενο ξένων κύκλων.
Τὸ γεγονὸς ὅτι οἱ κύκλοι εἶναι ξένοι ἀνὰ δύο μᾶς πείθει, μὲ μιὰ ματιά, ὅτι ἀντιμετατίθενται.
Ὅσον ἀφορᾶ στὴ μοναδικότητα τῆς ἀναλύσης, αὐτὴ προκύπτει ὡς συνέπεια τῶν ἑξῆς παρατηρήσεων, τῶν ὁποίων ἡ ἀπόδειξη δίνεται ὡς ἁπλὴ ἄσκηση. Ἔστω, περαιτέρω, καὶ ὅλα,

$$\sigma = (a_1\ a_2 \dots) \circ (b_1\ b_2 \dots) \circ (c_1\ c_2 \dots) \circ \dots \quad (2.7)$$

μιὰ ἀνάλυση τῆς σ σὲ γινόμενο ξένων κύκλων. Ἐννοεῖται ὅτι συμπεριλαμβάνονται καὶ κύκλοι μήκους 1. Λ.χ. ἕνας κύκλος τῆς μορφῆς (a), ἁπλῶς σημαίνει ὅτι $\sigma(a) = a$. Ἔτσι, ἡ ἀνάλυση τῆς τ τῆς προηγούμενης σελίδας εἶναι $\tau = (1\ 4\ 7) \circ (3\ 5) \circ (2) \circ (6)$. Τότε,
α) Ἡ σχέση ποὺ ὁρίζεται στὸ σύνολο $\{1,\dots,n\}$ ὡς ἑξῆς:

$$y \sim x \iff y = \sigma^{\nu}(x),\ \text{γιὰ κάποιο } \nu \in \mathbb{Z}$$

είναι σχέση ισοδυναμίας.

β) Η κλάση ισοδυναμίας του $x \in \{1, \dots, n\}$ είναι το σύνολο των αριθμών του μοναδικού κύκλου της ανάλυσης (2.7), στον οποίον ανήκει το x.

Συνεπώς το σύνολο των κλάσεων $\{a_1, a_2, \dots\}, \{b_1, b_2, \dots\}$ $\{c_1, c_2, \dots\}, \dots$ είναι το σύνολο-πηλίκο της ισοδυναμίας $\sim$ που ορίσαμε στο α). Όμως το σύνολο-πηλίκο εξαρτάται αποκλειστικά απ' τη σχέση ισοδυναμίας και είναι μοναδικό. Αυτό σημαίνει ότι οι παραπάνω κλάσεις είναι μοιρόφορα ορισμένες απ' τη σ και δεν εξαρτώνται απ' τον τρόπο που πετύχαμε την ανάλυση (2.7). Άρα το ίδιο ισχύει και για τους αντίστοιχους κύκλους. □

Ορισμός. Κάθε κύκλος μήκους 2 λέγεται αντιμετάθεση. (2.8)

Πόρισμα. Κάθε μη ταυτοτική μετάθεση γράφεται ως γινόμενο αντιμεταθέσεων. (2.9)

Απόδειξη. Παρατηρούμε ότι κάθε κύκλος $(a_1 a_2 \dots a_r)$ $(r \geq 2)$ γράφεται ως γινόμενο αντιμεταθέσεων, βάσει της ταυτότητας

$$(a_1 a_2 \dots a_r) = (a_1 a_r) \circ \dots \circ (a_1 a_3) \circ (a_1 a_2)$$

Στη συνέχεια εφαρμόζουμε το θεώρημα 2.5. □

Πρόταση. Κάθε κύκλος μήκους m έχει τάξη m. (2.10)

Απόδειξη. Έστω ο κύκλος $\kappa = (a_1 \dots a_m)$. Θέλουμε να βρούμε τον ελάχιστο θετικό ακέραιο d για τον οποίο $\kappa^d = 1$.

Παρατηρούμε ότι $\kappa(a_1) = a_2$, $\kappa(a_2) = a_3$, $\dots$, $\kappa(a_{m-1}) = a_m$ και $\kappa(a_m) = a_1$, οπότε $\kappa^m(a_1) = a_1$. Λόγω του ότι $\kappa = (a_2 \dots a_m a_1)$, έπεται όμοιως ότι $\kappa^m(a_2) = a_2$ κ.ο.κ. Άρα $\kappa^m(a_i) = a_i$ $\forall\, i = 1, 2, \dots, m$. Επιπλέον, για κάθε d $(d \geq 1)$ είναι $\kappa^d(a_1) = a_{d+1} \neq a_1$, που αποκλείει να είναι $\kappa^d = 1$. Συνεπώς $\kappa^m = 1$ και m είναι ο ελάχιστος με αυτή την ιδιότητα. □

Πρόταση. Έστω $\sigma \in S_n$ και $\sigma = x_1 x_2 \dots x_\nu$ η ανάλυση της (2.11) σε ξένους κύκλους (πρβλ. Θεώρημα 2.6), των οποίων τα μήκη είναι $m_1, \dots, m_\nu$. Τότε η τάξη της σ είναι ίση με το ελάχιστο κοινό πολλαπλάσιο των $m_1, \dots, m_\nu$.

Απόδειξη. Επειδή, συμφωνα με το θεώρημα 2.8, οι κύκλοι $x_1, \dots, x_\nu$ αντιμετατίθενται, είναι εύκολο να δούμε ότι για κάθε θετικό ακέραιο n είναι $\sigma^n = (x_1 x_2 \dots x_\nu)^n = x_1^n x_2^n \dots x_\nu^n$. Ειδικώτερα, αν n είναι η τάξη της σ, τότε $\sigma^n = x_1^n \dots x_\nu^n$. Επειδή οι κύκλοι $x_1, \dots, x_\nu$ είναι ξένοι είναι φανερό ότι $x_1^n \dots x_\nu^n = 1$ αν και μόνο αν $x_i^n = 1$ $\forall i = 1, \dots, \nu$. Απ' τις προτάσεις 1.20 και 2.10 είναι $x_i^n = 1$ αν και μόνο αν m_i / n. Κατ' συνέπεια, $\sigma^n = 1$ αν και μόνο αν το n είναι πολλαπλάσιο όλων των $m_1, \dots, m_\nu$. Επειδή το n είχαμε το ελάχιστο με την παραπάνω ιδιότητα, θα πρέπει να ταυτίζεται με το ελάχιστο κοινό πολλαπλάσιο των $m_1, \dots, m_\nu$. □

Ασκήσεις. α) Αναλύστε τις παρακάτω μεταθέσεις σε γινόμενο ξένων κύκλων και βρείτε τις τάξεις τους: (2.12)

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 6 & 5 & 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 3 & 2 & 6 & 4 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 5 & 6 & 4 & 1 & 3 \end{pmatrix},$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 6 & 9 & 7 & 2 & 5 & 8 & 1 & 3 \end{pmatrix}, \begin{pmatrix} a & b & c & d & e & f \\ c & e & d & f & b & a \end{pmatrix},$$

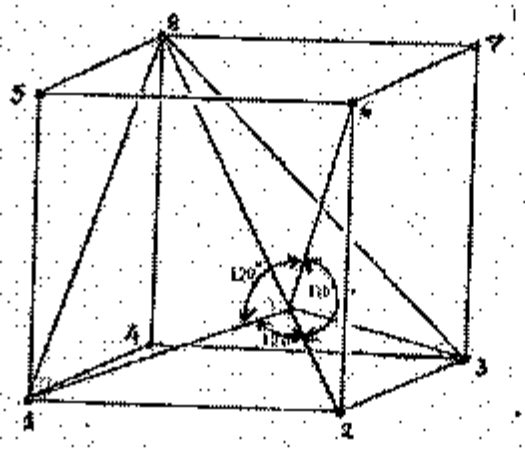
$(1\,2\,3\,4)(5\,6\,7)(2\,6\,1)(4\,7)$, $(1\,2\,3\,4\,5)(6\,7)(1\,2\,3\,7)(1\,6\,3)$, $(1\,4)(1\,2\,3)(4\,5)(1\,4)$.

β) Παρασκήψατε την ομάδα συμμετριών του ρόμβου σαν ομάδα μεταθέσεων των κορυφών του. Κατασκευάστε τον πίνακα πολλαπλασιασμού.

γ) Όμοιο ζήτημα με το β για τις συμμετρίες του κύβου, οι οποίες αφήνουν σταθερή μια δεδομένη κορυφή του.

(βλ. σελ. 17α)

Έστω Σ ένα πεπερασμένο είτε άπειρο σύνολο σημείων στον τριδιάστατο ευκλείδιο χώρο. Με τον όρο συμμετρία του Σ εννοούμε μια στροφή περί ένα άξονα, που περνά απ' την αρχή Ο, η οποία απεικονίζει το Σ επί τον εαυτό του.



Συμμετρία του κύβου που αφήνουν σταθερή την κορυφή 2 (άρα είναι στροφή με άξονα τη διαγώνιο 2-6)

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

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

Άρτιες και περιττές μεταθέσεις. Θεωρούμε το πολυώνυμο (2.13)
των n μεταβλητών $x_1, \dots, x_n$

$$P = P(x_1, \dots, x_n) = \prod_{1 \le i < j \le n} (x_i - x_j)$$

Έστω μιά αντιμετάθεση $\alpha = (r\ s)$ $(r<s)$ των $x_1, \dots, x_n$ και
ας θεωρήσουμε το πολυώνυμο

$$P_\alpha = P_\alpha(x_1, \dots, x_n) \overset{\text{ορισμός}}{=} P(\alpha(x_1), \dots, \alpha(x_n)) = \prod_{1 \le i < j \le n} (\alpha(x_i) - \alpha(x_j))$$

Θα δείξουμε ότι $P_\alpha = \pm P$.
Σε κάθε παράγοντα $x_i - x_j$, $i<j$ αντιστοιχούμε $i-1$ το ζεύγος (x_i, x_j). Η μετάθεση α στέλνει αυτό το ζεύγος στο $(\alpha(x_i), \alpha(x_j))$, δηλ. στον παράγοντα $\alpha(x_i) - \alpha(x_j)$ της P_α.
Προφανώς, $\alpha(x_i) - \alpha(x_j) = x_I - x_J$ για κάποιους δείκτες I, J. Αν $I<J$, τότε ο παράγων αυτός εμφανίζεται και στο P, άν όχι, ο αντίθετός του εμφανίζεται στο P. Μένει τώρα να δειχθεί ότι, άν $i_1 < j_1$ και $i_2 < j_2$ και $(i_1, j_1) \neq (i_2, j_2)$ τότε $\alpha(x_{i_2}) - \alpha(x_{j_2}) \neq \pm (\alpha(x_{i_1}) - \alpha(x_{j_1}))$, αλλά αυτό ελέγχεται εύκολα.
Η άσκηση 2.17(α) μάς λέει, πιό συγκεκριμένα, ότι $P_\alpha = -P$.

Τώρα, ξέρουμε από το (2.9) ότι κάθε μετάθεση $\sigma \in S_n$ είναι γινόμενο αντιμεταθέσεων. Συνεπώς, άν ορίσουμε $P_\sigma = P(\sigma(x_1), \dots, \sigma(x_n))$, τότε και πάλι $P_\sigma = \pm P$

Ορισμός. Έστω $P_\sigma = \varepsilon(\sigma) P$ όπου $\varepsilon(\sigma) \in \{1, -1\}$. (2.14)
Άν $\varepsilon(\sigma) = +1$ η μετάθεση σ λέγεται άρτια· διαφορετικά λέγεται περιττή.

Πρόταση. Άν $\sigma_1, \sigma_2 \in S_n$ τότε $\varepsilon(\sigma_1 \sigma_2) = \varepsilon(\sigma_1)\varepsilon(\sigma_2)$ (2.15)
Απόδειξη. $\varepsilon(\sigma_1\sigma_2)P = P_{\sigma_1\sigma_2} = P(\sigma_1\sigma_2(x_1), \dots, \sigma_1\sigma_2(x_n)) =$
$= P_{\sigma_1}(\sigma_2(x_1), \dots, \sigma_2(x_n)) = \varepsilon(\sigma_1) \cdot P(\sigma_2(x_1), \dots, \sigma_2(x_n)) =$
$= \varepsilon(\sigma_1) P_{\sigma_2} = \varepsilon(\sigma_1)\varepsilon(\sigma_2) P$, από όπου το αποδεικτέο. □

Θεώρημα. Οἱ ἄρτιες μεταθέσεις τῆς ὁμάδας S_n εἶναι ὑποομάδα τῆς S_n τάξεως $\frac{1}{2}n!$, ἡ ὁποία συμβολίζεται A_n καὶ λέγεται **ἐναλλασσουσα ὁμάδα βαθμοῦ n.** (2.16)

Ἀπόδειξη. Ἂν $\sigma_1, \sigma_2 \in S_n$ εἶναι ἄρτιες μεταθέσεις, τότε ἀπὸ τὰ (2.14) καὶ (2.15) ἕπεται ὅτι καὶ ἡ $\sigma_1\sigma_2$ εἶναι ἄρτια μετάθεση, δηλ. τὸ σύνολο A_n εἶναι κλειστὸ ὡς πρὸς τὴ σύνθεση τῶν μεταθέσεων. Ἄρα, ἀπὸ τὴν πρόταση 1.18, εἶναι ὑποομάδα τῆς S_n. Θὰ δείξουμε τώρα ὅτι ἡ τάξη τῆς A_n εἶναι $\frac{1}{2}n!$
Ἔστω σ_0 μιὰ αὐθαίρετα ἐπιλεγμένη, ἀλλὰ σταθερὴ μέχρι τὸ τέλος τῆς ἀπόδειξης, περιττὴ μετάθεση. Ἔστω B_n τὸ σύνολο τῶν περιττῶν μεταθέσεων τῆς S_n. Ὁρίζουμε τὴν ἀπεικόνιση $\phi : A_n \longrightarrow B_n$ ὡς ἑξῆς : $\phi(\sigma) = \sigma\sigma_0$, ἡ ὁποία εἶναι καλὰ ὁρισμένη λόγῳ τοῦ (2.15). Ἐπειδὴ ἡ S_n εἶναι ὁμάδα, εἶναι εὔκολο νὰ ἀποδείξουμε ὅτι ἡ ϕ εἶναι ἀμφιμονοσήμαντη καὶ "ἐπί" (ἀσκηση). Ἄρα τὰ σύνολα A_n καὶ B_n εἶναι ἰσοπληθῆ. Ἐπιπλέον εἶναι ξένα καὶ ἡ ἕνωσή τους δίνει τὸ S_n μὲ $n!$ στοιχεῖα (βλ. θεώρημα 2.4). Ἄρα, καθένα ἀπὸ τὰ σύνολα A_n, B_n ἔχει $\frac{1}{2}n!$ στοιχεῖα. □

Ἀσκήσεις. α) Ἔστω ἡ μετάθεση $\sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ a_1 & a_2 & \dots & a_n \end{pmatrix}$. (2.17)

Γιὰ κάθε $i = 1, 2, \dots, n$ συμβολίζουμε μὲ ν_i τὸ πλῆθος τῶν a_j γιὰ τὰ ὁποῖα εἶναι γραμμένα δεξιώτερα τοῦ a_i καὶ εἶναι μικρότερά του a_i. Π.χ. γιὰ τὴ μετάθεση $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 6 & 2 & 5 & 1 \end{pmatrix}$

εἶναι $\nu_1 = 2$, $\nu_2 = 2$, $\nu_3 = 3$, $\nu_4 = 1$, $\nu_5 = 1$. Ἀποδεῖξτε ὅτι $\varepsilon(\sigma) = (-1)^{\nu_1 + \dots + \nu_{n-1}}$. Π.χ. στὸ συγκεκριμένο παράδειγμα πιὸ πάνω εἶναι $\varepsilon(\sigma) = (-1)^9 = -1$, ἄρα ἡ σ εἶναι περιττὴ μετάθεση.
β) Κάνετε τὸν πίνακα πολλαπλασιασμοῦ τῆς S_3. Γράψετε τὰ στοιχεῖα τῆς A_3 καὶ κάνετε τὸν πίνακα πολλαπλασιασμοῦ της.
γ) Δείξτε ὅτι κάθε ἀντιμετάθεση εἶναι περιττὴ μετάθεση, ἐνῶ κάθε κύκλος μήκους 3 εἶναι ἄρτια μετάθεση.

Ορισμός. Έστω $(G,\cdot)$ ομάδα και A ένα μη κενό υποσύνολο του G. Λέμε ότι η G παράγεται από το A (συμβολικά, $G=\langle A\rangle$) αν για κάθε $x\in G$ υπάρχουν $a_1,\dots,a_k\in A$ και $\nu_1,\dots,\nu_k\in\mathbb{Z}$, είς τρόπον ώστε $x=a_1^{\nu_1}\cdots a_k^{\nu_k}$. (2.18)

Πρόταση. Αν $n\geq 3$ τότε η εναλλάσσουσα ομάδα A_n παράγεται από τους $n-2$ κύκλους $(1\,2\,3),(1\,2\,4),\dots,(1\,2\,n)$. (2.19)

Απόδειξη. Από το (2.8) και την ταυτότητα $(a\,b)=(1\,a)(1\,b)(1\,a)$, έπεται ότι η S_n παράγεται από όλους τους κύκλους $(1\,i),1<i$. Αναφερόμενοι τώρα στην άσκηση 2.17 (α) έχομε για τη μετάθεση $(1\,i)$: $\nu_1=i-1$, $\nu_2=1,\dots,\nu_{i-1}=1$, $\nu_i=0$, $\nu_{i+1}=0,\dots,\nu_n=0$. Συνεπώς $\nu_1+\nu_2+\cdots+\nu_n=(i-1)+(i-2)=2i-3$, περιττός αριθμός, που σημαίνει ότι η μετάθεση $(1\,i)$ είναι περιττή. Όμως κάθε $\sigma\in A_n$ είναι γινόμενο αντιμεταθέσεων της μορφής $(1\,i)$ όπότε, αναγκαστικά, το πλήθος τους πρέπει να είναι άρτιο (γινόμενο δύο περιττών μεταθέσεων είναι άρτια μετάθεση). Άρα η A_n παράγεται από το σύνολο των μεταθέσεων της μορφής $(1\,i)(1\,j)$, $(i,j>1)$. Επειδή $(1\,i)(1\,i)=$ ταυτοτική μετάθεση, μπορούμε να υποθέσομε $i\neq j$, όπότε $(1\,i)(1\,j)=(1\,j\,i)$. Μένει να δείξομε ότι κάθε τέτοιος κύκλος παράγεται από τους κύκλους που αναφέρονται στην εκφώνηση. Πράγματι: αν $j=2$ τότε $(1\,j\,i)=(1\,2\,i)$ με $i>2$ άρα η $(1\,j\,i)$ ανήκει στους κύκλους της εκφώνησης. Αν $i=2$ τότε $(1\,j\,i)=(1\,j\,2)=(1\,2\,j)^2$ με $j>2$ πάλι άρα η $(1\,j\,i)$ είναι το τετράγωνο κάποιου κύκλου της εκφώνησης. Τέλος, αν $i>2$ και $j>2$, τότε ισχύει η σχέση $(1\,j\,i)=(1\,2\,i)^{-1}\cdot(1\,2\,j)\cdot(1\,2\,i)$, άρα η $(1\,j\,i)$ παράγεται και πάλι από τους κύκλους της εκφώνησης.

□

3. Πλευρικές κλάσεις και κανονικές υποομάδες.

Ορισμός. Έστω $(G,\cdot)$ ομάδα και H υποομάδα της G. Για (3.1)
κάθε $a\in G$ ορίζουμε τα σύνολα:
$aH=\{ax \mid x\in H\}$ και $Ha=\{xa \mid x\in H\}$,
τα οποία λέγονται, αντιστοίχως, αριστερή πλευρική κλάση
του a και δεξιά πλευρική κλάση του a (ως προς H, ή
modulo H).
Εν γένει είναι $aH\neq Ha$. Αν η G είναι αβελιανή, τότε
$aH=Ha$ $\forall\, a\in G$.

Πρόταση. Έστω H υποομάδα της G. (α) Τα εξής είναι (3.2)
ισοδύναμα:
(i) $a^{-1}b\in H$, (ii) $aH=bH$, (iii) $b\in aH$.
Επίσης, τα εξής είναι ισοδύναμα:
(i) $ab^{-1}\in H$, (ii) $Ha=Hb$, (iii) $b\in Ha$.
(β) Δύο διαφορετικές αριστερές πλευρικές κλάσεις είναι
ξένες. Η ένωση όλων των αριστερών κλάσεων ισούται με G.
Ανάλογα ισχύουν και για τις δεξιές πλευρικές κλάσεις.
Απόδειξη. (α) (i) $\Rightarrow$ (ii). Έστω $a^{-1}b\in H$, δηλαδή $a^{-1}b=x\in H$.
Τότε $b=ax$, άρα $bH=aH$. Πράγματι, έστω $y\in bH$. Τότε
$y=bh$ με $h\in H$, άρα $y=(ax)h=a(xh)\in aH$, μια και
$xh\in H$. Αντίστροφα, έστω $y'\in aH$, δηλαδή $y'=ah'$ με $h'\in H$.
Άρα $y'=(bx^{-1})h'=b(x^{-1}h')\in bH$, αφού $x^{-1}h'\in H$.
(ii) $\Rightarrow$ (iii). Έστω $aH=bH$. Επειδή $1\in H$, θα είναι
$b=b\cdot 1\in bH=aH$.
(iii) $\Rightarrow$ (i). Έστω $b\in aH$, δηλαδή $b=ah$ με $h\in H$. Τότε
$a^{-1}b=h\in H$.
Εντελώς ανάλογα αποδεικνύεται η ισοδυναμία των (i),
(ii) και (iii) στην περίπτωση των δεξιών πλευρικών κλάσεων.
(β). Θα δείξουμε ότι, αν $aH\cap bH\neq\emptyset$, τότε $aH=bH$.
Πράγματι, αν $x\in aH\cap bH$, τότε $x=ah_1$ και $x=bh_2$ για
κάποια $h_1,h_2\in H$. Άρα $a^{-1}b=(h_1x^{-1})b=h_1(x^{-1}b)=h_1h_2^{-1}$
και $h_1h_2^{-1}\in H$. Άρα $a^{-1}b\in H$, δηλαδή από το (α) έπεται ότι
$aH=bH$ κι έρχεται έτσι σε αντίφαση με την υπόθεσή μας.

Το ότι η ένωση όλων των αριστερών πλευρικών κλάσεων ίσουται με G είναι προφανές, αφού για κάθε $a \in G$ έχομε $a \in aH$. Η απόδειξη για τους αναλόγους ισχυρισμούς περί των δεξιών κλάσεων είναι εντελώς όμοια. □

Θεώρημα (Lagrange). Σε κάθε πεπερασμένη ομάδα, η τάξη (3.3) οποιασδήποτε υποομάδας διαιρεί την τάξη της ομάδας.

Απόδειξη. Έστω η $(G, \cdot)$ πεπερασμένη ομάδα και H υποομάδα της G. Έστω n η τάξη της G και m η τάξη της H. Ας θεωρήσομε τώρα μια οποιαδήποτε αριστερή πλευρική κλάση aH. Τότε η απεικόνιση $\phi : H \longrightarrow aH$, που ορίζεται $\phi(x) = ax \ \forall x \in H$ είναι αμφιμονοσήμαντη και "επί". Συνεπώς, το πλήθος των στοιχείων της aH ίσουται με το πλήθος των στοιχείων της H, δηλαδή με m. Επειδή η G είναι πεπερασμένη, το πλήθος των αριστερών πλευρικών κλάσεων ως προς H είναι πεπερασμένο, έστω k και κάθε τέτοια κλάση έχει m στοιχεία. Επιπλέον αυτές οι k κλάσεις είναι ξένες ανά δύο και η ένωσή τους κάνει τη G (βλ. (3.2)β). Άρα $km = n$, που είναι το αποδεικτέο.

□

Το θεώρημα του Lagrange έχει πολλές ενδιαφέρουσες συνέπειες. Μια απ' αυτές δίνεται ως άσκηση.

Άσκηση. Έστω G ομάδα τάξεως p, όπου ο p είναι πρώτος αριθμός. Δείξτε πρώτα ότι η G δεν έχει άλλες υποομάδες πλην των τετριμμένων (δηλ. των $\langle 1 \rangle$ και G) και, στη συνέχεια, ότι η G είναι κυκλική. (3.4)

Πρόταση. Αν η G είναι πεπερασμένη ομάδα τάξεως n, τότε (3.5)
$a^n = 1 \quad \forall a \in G$

Απόδειξη. Έστω $a \in G$ και ν η τάξη της υποομάδας $\langle a \rangle$. Η $\langle a \rangle$, ως κυκλική ομάδα, είναι αβελιανή, άρα απ' το (1.13)γ, $a^\nu = 1$. Αφ' ετέρου, λόγω του θεωρήματος του Lagrange, θα' είναι $n = \nu k$ για κάποιον ακέραιο k. Άρα
$a^n = (a^\nu)^k = 1^k = 1$.

□

Το παρακάτω θεώρημα αποτελεί συμπλήρωση της πρότασης 1.25

Θεώρημα. Έστω $(G,\cdot)$ κυκλική ομάδα τάξεως g $(<+\infty)$. (3.6)
Έστω $G=\langle a\rangle$. Τότε, για κάθε διαιρέτη d του g υπάρχει ακριβώς μία υποομάδα της G τάξεως d. Όλοι γεννήτορες αυτής της υποομάδας είναι οι $a^{g/d}$

Απόδειξη. Αν $d|g$, έστω θέτουμε $g=d\cdot n$, οπότε $a^{g/d}=a^n$. Τα στοιχεία $1, a^n, a^{2n}, \dots, a^{(d-1)n}$ είναι διαφορετικά μεταξύ τους αφού, εξ υποθέσεως, τα $1, a, a^2, \dots, a^{g-1}$ είναι όλα τα διαφορετικά στοιχεία της G. Επειδή $a^g=1$, είναι $a^{dn}=1$.
Άρα $\langle a^n\rangle$ είναι μια υποομάδα της G τάξεως d. Έστω τώρα H μια οποιαδήποτε υποομάδα της G τάξεως d. Θα δείξουμε ότι $H=\langle a^n\rangle$. Επί την πρόταση 1.25 είναι $H=\langle x\rangle$ για κάποιο $x\in G$, ενώ από την άσκηση 1.26 (β) $x^d=1$. Όμως $x\in\langle a\rangle$, άρα $x=a^m$ για κάποιο $m\in\mathbb{Z}$, οπότε $a^{md}=1$. Συνεπώς, από την πρόταση 1.20, $md=kg$ με $k\in\mathbb{Z}$, άρα $md=kdn$, απ' όπου $m=kn$ και $x=(a^n)^k$. Η τελευταία σχέση δείχνει ότι η $H=\langle x\rangle$ είναι υποομάδα της $\langle a^n\rangle$. Επειδή όμως η τάξη της συμπίπτει με την τάξη της $\langle a^n\rangle$, πρέπει $H=\langle a^n\rangle$.

□

Πρόταση. Έστω $(G,\cdot)$ κυκλική ομάδα τάξεως g $(<+\infty)$ και $G=\langle a\rangle$. Αναγκαία και ικανή συνθήκη για να είναι το στοιχείο a^n γεννήτορας της G είναι ο $\text{ΜΚΔ}(n,g)=1$. (3.7) (*)

Απόδειξη. Έστω $G=\langle b\rangle$, όπου $b=a^n$. Θα δείξουμε ότι $\text{ΜΚΔ}(n,g)=1$. Αν αυτό δεν άληθευε, τότε $\text{ΜΚΔ}(n,g)=d>1$ και θέτουμε $n=dx$, $g=dy$. Από την άσκηση 1.26 (β) τα στοιχεία $1, b, \dots, b^{g-1}$ είναι διαφορετικά, δηλ. τα στοιχεία $1, a^n, a^{2n}, \dots, a^{(g-1)n}$ είναι διαφορετικά. Όμως $1<y<g$, άρα ανάμεσα στα $a^n, \dots, a^{(g-1)n}$ περιλαμβάνεται και το a^{yn}, που θα 'πρεπε, σύμφωνα με την προηγούμενη παρατήρηση, να είναι $\neq 1$. Όμως $a^{yn}=a^{ydx}=a^{gx}=(a^g)^x=1^x=1$, άτοπο. Συνεπώς $\text{ΜΚΔ}(n,g)=1$.
Αντίστροφα, έστω $\text{ΜΚΔ}(n,g)=1$. Θα δείξουμε ότι $G=\langle a^n\rangle$. Αρκεί να δείξουμε ότι τα $1, a^n, \dots, a^{(g-1)n}$ είναι διαφορετικά.

(*) Η πρόταση αυτή έχει ήδη αποδειχθεί (πρόταση 1.27) πολύ απλούστερα, αλλά χρησιμοποιώντας μία πρόταση της Θεωρίας Αριθμών.

Πράγματι, έστω $a^{kn} = a^{\lambda n}$ με $0 \le k < \lambda < g$. Τότε $a^{dn} = 1$, όπου $d = \lambda - k$, $d \in \{1, 2, \dots, g-1\}$. Απ' την πρόταση 1.20 $g \mid dn$. Όμως λόγω του ότι ΜΚΔ$(g,n) = 1$, θα' πρέπει $g \mid d$, άτοπο, πράγμα που ολοκληρώνει την απόδειξη. □

Σημείωση. Έστω η G όπως στην προηγούμενη πρόταση. Τα στοιχεία της είναι τα $1, a, a^2, \dots, a^{g-1}$. Συμφωνα με ό,τι αποδείχθηκε, το a^n είναι γεννήτορας της G αν και μόνο αν ο n είναι πρώτος προς τον g. Άρα η G έχει τόσους γεννήτορες όσοι και οι ακέραιοι αριθμοί $n \in \{1, 2, \dots, g-1\}$, οι οποίοι είναι πρώτοι προς τον g. Το πλήθος αυτών των ακεραίων n, που φυσικά εξαρτάται απ' το g, συμβολίζεται με $\varphi(g)$, όπου φ είναι η λεγόμενη συνάρτηση του Euler. Αν $g = p_1^{\nu_1} \cdots p_k^{\nu_k}$ είναι η κανονική ανάλυση του g σε πρώτους παράγοντες, τότε αποδεικνύεται στη στοιχειώδη Θεωρία Αριθμών ότι

$$\varphi(g) = g\left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_k}\right) =$$

$$= p_1^{\nu_1 - 1} \cdots p_k^{\nu_k - 1} (p_1 - 1) \cdots (p_k - 1).$$

(3.8)

Πρόταση Έστω $(G, \cdot)$ ομάδα και H υποομάδα της G. Τότε, ως προς την H, το σύνολο των δεξιών πλευρικών κλάσεων βρίσκεται σε αμφιμονοσήμαντη και "επί" αντιστοιχία με το σύνολο των αριστερών πλευρικών κλάσεων. Ο κοινός πληθάριθμος του συνόλου των δεξιών είτε αριστερών πλευρικών κλάσεων ονομάζεται δείκτης της H στην G και συμβολίζεται $[G : H]$. Αν ο δείκτης αυτός δεν είναι πεπερασμένος, τότε γράφουμε $[G : H] = \infty$. Αν η G είναι πεπερασμένη, τότε $[G : H] = |G|/|H|$.

(3.9)

Απόδειξη. Έστω $\mathcal{A}$ και $\mathcal{D}$ το σύνολο των αριστερών και δεξιών κλάσεων ως προς H, αντιστοίχως. Θεωρούμε την απεικόνιση $f : \mathcal{A} \longrightarrow \mathcal{D}$, που ορίζεται ως εξής:

$$f(xH) = Hx^{-1}.$$

Η f είναι καλά ορισμένη. Πρέπει δηλαδή να δείξουμε ότι αν $x_1 H = x_2 H$, τότε $f(x_1 H) = f(x_2 H)$. Θα' κάνουμε χρήση της πρότασης 3.2 μερικές φορές. Η σχέση $x_1 H = x_2 H$ συνεπά-

γεται ότι $x_2 = x_1 h$ με $h \in H$. Άρα $Hx_2^{-1} = Hh^{-1}x_1^{-1} = Hx_1^{-1}$, δηλ. $f(x_2 H) = f(x_1 H)$.
Η f είναι αμφιμονοσήμαντη. Πράγματι, αν $f(x_1 H) = f(x_2 H)$ τότε $Hx_1^{-1} = Hx_2^{-1}$, άρα $x_1^{-1}x_2 \in H$ δηλαδή και $x_2^{-1}x_1 = (x_1^{-1}x_2)^{-1} \in H$. Συνεπώς $x_2 H = x_1 H$.
Τέλος, η f είναι "επί". Γιατί αν $Hy \in \mathcal{D}$, τότε $y^{-1}H \subset A$ και $f(y^{-1}H) = H(y^{-1})^{-1} = Hy$.
Έστω τώρα ότι η G είναι πεπερασμένη, δηλαδή ο δείκτης της H στην G είναι πεπερασμένος. Το πλήθος των αριστερών πλευρικών κλάσεων ισούται με $[G:H]$ και, όπως είδαμε στην απόδειξη του Θεωρήματος του Lagrange, κάθε τέτοια κλάση έχει $|H|$ το πλήθος στοιχεία. Επειδή οι κλάσεις είναι ανά δύο ξένες, πρέπει τότε $[G:H] \times |H| = |G|$, που είναι το ζητούμενο.

□

(3.10) Κλάσεις συζυγίας. Έστω $(G, \cdot)$ ομάδα. Ορίζουμε στην G τη σχέση $\sim$ ως εξής:

$$a \sim b \iff \text{υπάρχει } x \in G \text{ τέτοιο ώστε } b = xax^{-1}$$

Αποδεικνύεται εύκολα ότι η $\sim$ είναι σχέση ισοδυναμίας στο G και συνεπώς διαμερίζει το σύνολο G σε κλάσεις ισοδυναμίας, οι οποίες λέγονται κλάσεις συζυγίας. Η κλάση συζυγίας του $a \in G$ συμβολίζεται με (a). Είναι προφανές ότι $(1) = \{1\}$.
Ορίζουμε επίσης το κέντρο του $a \in G$ ως εξής:

$$C(a) = \{x \in G : ax = xa\}.$$

Είναι προφανές ότι το $C(a)$ είναι υποομάδα της G

(3.11) Πρόταση. Τα στοιχεία της (a) βρίσκονται σε αμφιμονοσήμαντη και "επί" αντιστοιχία με τις αριστερές (καθώς και με τις δεξιές) πλευρικές κλάσεις ως προς $C(a)$. Επιπλέον, αν ο δείκτης της $C(a)$ στην G είναι πεπερασμένος, τότε

$$|(a)| = [G : C(a)]$$

(όπου για τυχόν πεπερασμένο σύνολο A, $|A|$ σημαίνει το πλήθος των στοιχείων του).

Απόδειξη. Αν με $\mathcal{A}$ συμβολίσουμε το σύνολο των αριστερών κλάσεων modulo $C(a)$ τότε ορίζουμε την εξής απεικόνιση:

$$\theta: \mathcal{A} \longrightarrow (a) \text{ τέτοια ώστε } \theta(x\cdot C(a)) = xax^{-1}.$$

Η θ είναι καλά ορισμένη: Έστω $x\cdot C(a) = y\cdot C(a)$. Τότε $x^{-1}y \in C(a)$, που σημαίνει ότι $x^{-1}y\,a = a\,x^{-1}y$, άρα και $xax^{-1} = yay^{-1}$, δηλ. $\theta(x\cdot C(a)) = \theta(y\cdot C(a))$.

Η θ είναι αμφιμονοσήμαντη: Έστω $\theta(x\cdot C(a)) = \theta(y\cdot C(a))$. Τότε $xax^{-1} = yay^{-1}$, άρα και $ax^{-1}y = x^{-1}y\,a$, που σημαίνει ότι $x^{-1}y \in C(a)$. Αυτό συνεπάγεται όμως ότι $x\cdot C(a) = y\cdot C(a)$.

Τέλος, η θ είναι "επί": Έστω $b \in (a)$. Αυτό εξ ορισμού σημαίνει ότι $b = xax^{-1}$ για κάποιο $x \in G$, οπότε $\theta(x\cdot C(a)) = xax^{-1} = b$. □

Πόρισμα. Έστω $(G,\cdot)$ πεπερασμένη ομάδα τάξεως g. Για κάθε $a \in G$ θέτουμε $\nu_a = |(a)|$. Τότε ο ν_a είναι διαιρέτης του g. (3.12)

Απόδειξη. Από την πρόταση 3.11 είναι $\nu_a = [G : C(a)] = |G|/|C(a)|$ (λόγω της πρότασης 3.9). Άρα $g = \nu_a \cdot |C(a)|$. □

Έστω τώρα ότι η G είναι πεπερασμένη και $(a_1), \dots, (a_k)$ είναι όλες οι κλάσεις συζυγίας της. Μια απ' αυτές είναι και η $(1) = \{1\}$, οπότε χωρίς βλάβη της γενικότητας υποθέτουμε ότι $a_1 = 1$. Προφανώς $G = (a_1) \cup (a_2) \cup \dots \cup (a_k)$ και τα σύνολα $(a_1), \dots, (a_k)$ είναι ξένα ανά δύο. Αν θέσουμε $|(a_i)| = \nu_i$ $(\nu_1 = 1)$ τότε θα έχουμε τη σχέση

$$g = 1 + \nu_2 + \dots + \nu_k,$$

που λέγεται εξίσωση κλάσεων της G.

Ορισμός. Έστω $(G,\cdot)$ ομάδα. Ορίζουμε το κέντρο της G ως (3.13)

$$Z = \{z \in G : zx = xz \ \ \forall x \in G\}.$$

Δηλαδή το κέντρο της G αποτελείται από εκείνα τα στοιχεία της G, που αντιμετατίθενται με όλα τα στοιχεία της G. Είναι άμεση άσκηση ν' αποδείξει κανείς ότι το Z είναι υποομάδα της G και, μάλιστα, το Z είναι αβελιανή ομάδα.

Πρόταση. Έστω $(G,\cdot)$ ομάδα και Z το κέντρο της. Το $a\in G$ (3.14)
ανήκει στο Z άν και μόνο άν $(a)=\{a\}$.
Απόδειξη. Έστω $a\in Z$. Θα δείξουμε ότι το μοναδικό στοιχείο στην (a) είναι το a. Πράγματι, έστω $b\in(a)$. Τότε υπάρχει $x\in G$ τέτοιο ώστε $b=xax^{-1}$. Όμως από την σχέση $a\in Z$ έπεται ότι $xa=ax$, δηλαδή $b=(ax)x^{-1}=a$.
Αντίστροφα, έστω ότι $(a)=\{a\}$. Άν $x\in G$, τότε $x^{-1}ax\in(a)$, εξ ορισμού της (a). Λόγω της υπόθεσής μας τότε, $x^{-1}ax=a$, δηλαδή $ax=xa$. Η τελευταία σχέση ισχύει για κάθε $x\in G$, άρα $a\in Z$.

□

Πρόταση. Έστω $(G,\cdot)$ ομάδα τάξεως p^m, όπου ο p είναι (3.15)
πρώτος (και $m>0$). Άν Z είναι το κέντρο της G, τότε

$$|Z|=p^\mu \quad , \quad 0<\mu\leq m.$$

Απόδειξη. Επειδή το Z είναι υποομάδα της G, η τάξη της θα είναι διαιρέτης του p^m (θεώρημα του Lagrange), άρα $|Z|=p^\mu$ με $0\leq\mu\leq m$. Μένει ν' αποκλείσουμε την περίπτωση $\mu=0$, δηλαδή την περίπτωση που $Z=\{1\}$.
Πράγματι, έστω $(a_1)=\{1\}$, $(a_2),\dots,(a_k)$ όλες οι κλάσεις συζυγίας της G και $\nu_2,\dots,\nu_k$ οι αντίστοιχοι πληθάριθμοί τους. Η εξίσωση των κλάσεων της G γίνεται στην περίπτωσή μας $p^m=1+\nu_2+\dots+\nu_k$ και λόγω του (3.12) τα ν_i είναι διαιρέτες του p^m. Ειδικώτερα αυτό συνεπάγεται ότι τα ν_i είναι ίσα με 1 ή είναι πολλαπλάσια του p. Αποκλείεται όμως όλα τα $\nu_2,\dots,\nu_k$ να είναι πολλαπλάσια του p, γιατί τότε η εξίσωση των κλάσεων θα συνεπαγόταν μια σχέση της μορφής $p^m=1+\text{πολ}\cdot p$, που είναι αδύνατη. Άρα υπάρχει κάποιο $i\in\{2,\dots,k\}$ με $\nu_i=1$. Αυτό σημαίνει ότι $(a_i)=\{a_i\}$, άρα, από την πρόταση 3.14, $a_i\in Z$. Όμως $a_i\neq 1$, άρα $Z\neq\{1\}$.

□

Κανονικές υποομάδες. Έστω $(G,\cdot)$ ομάδα. Η υποομάδα H (3.16)
της G λέγεται κανονική υποομάδα της G άν για κάθε $x\in G$ ισχύει $xH=Hx$, δηλ άν η αριστερή και η δεξιά πλευ-

ρική κλάση του x, ως προς την H, συμβολίζεται. Συμβολικά γράφομε $H \lhd G$. Άντι του όρου κανονική υποομάδα χρησιμοποιείται, επίσης, και ο όρος αναλλοίωτη υποομάδα.

Άσκηση Έστω $(G,\cdot)$ όμαδα. Αποδείξτε τα εξής: (3.17)

α) Άν $H \lhd G$ τότε $x^{-1}Hx = H \ \forall x \in G$. ($x^{-1}Hx \overset{\text{συμ}}{=} \{x^{-1}hx / h \in H\}$).
Άν H υποομάδα της G και $x^{-1}hx \in H \ \forall x \in G, \forall h \in H$, τότε $H \lhd G$.

β) Το κέντρο Z της G είναι κανονική υποομάδα.

γ) Η τομή μιας δποιασδήποτε οικογένειας κανονικών υποομάδων της G είναι κανονική υποομάδα της G. (Υπόδειξη: Αποδείξτε πρώτα ότι για μια οικογένεια $(H_i)_{i\in I}$ υποομάδων της G (όχι, αναγκαστικά, κανονικών) ισχύει $x^{-1}(\bigcap_{i\in I} H_i)x = \bigcap_{i\in I}(x^{-1}H_i x)$.

δ) Άν η υποομάδα H της G έχει δείκτη 2 στην G, τότε η H είναι κανονική υποομάδα της G.

Απλές ομάδες. Είναι προφανές ότι σε μια αβελιανή ομάδα (3.18) όλες οι υποομάδες είναι κανονικές. Στα άλλα άκρα βρίσκονται εκείνες οι ομάδες, που δεν έχουν κανονικές υποομάδες εκτός, φυσικά, των τετριμμένων, δηλ της υποομάδας $\{1\}$ και ολόκληρης της ομάδας. Τέτοιες ομάδες ($με τάξη > 1$) λέγονται απλές. Φυσικά, μια πεπερασμένη ομάδα, της οποίας η τάξη είναι πρώτος αριθμός, είναι απλή ομάδα. Στη συνέχεια αυτού του κεφαλαίου θα δούμε ένα μη τετριμμένο παράδειγμα απλής ομάδας χρησιμοποιώντας τις γνώσεις του κεφαλαίου των μεταθέσεων.

Πρόταση Η εναλλάσσουσα ομάδα A_n είναι κανονική υποομάδα της συμμετρικής ομάδας S_n. (3.19)

Απόδειξη Από τα θεωρήματα (2.4) και (2.16) έχομε, αντιστοίχως, $|S_n| = n!$ και $|A_n| = \frac{1}{2}n!$. Από την πρόταση 3.3 τότε $[S_n : A_n] = 2$, άρα από την άσκηση 3.17 (δ) έπεται ότι $A_n \lhd S_n$. □

Σημείωση Η Πρόταση 3.19 είναι ειδική περίπτωση της Πρότασης 3.23, και θ' αποδείξαμε παρακάτω.

Άσκηση Θεωρήστε τις μεταθέσεις $\sigma=(12)(34)$ και $\tau=(13)(24)$ (3.20)
της S_4. Αποδείξτε ότι $\sigma\tau=\tau\sigma$ και $\sigma^2=\tau^2=1$ και ότι η ύπο-
ομάδα V που παράγουν είναι κανονική υποομάδα και της S_4 και
της A_4. (Γενικά, κάθε ομάδα που παράγεται από στοιχεία
a, b για τα οποία $a^2=b^2=1$ και $ab=ba$ (άρα έχει 4 στοιχεία),
χαρακτηρίζεται ως "ομάδα των τεσσάρων του Klein").

Θεώρημα Αν $n\neq 4$ τότε η όμαδα A_n είναι απλή. (3.21)
Απόδειξη. Επειδή $|A_3|=3$, η A_3 είναι απλή. Επίσης, αρκεί-
να με την άσκηση 3.20, η όμαδα V είναι γνήσια κανονική υπο-
ομάδα της A_4, οπότε η A_4 δεν είναι απλή. Συνεπώς, από
παρακάτω μπορούμε να υποθέτουμε ότι $n\geq 4$. Θα έχουμε απο-
δείξει το θεώρημα αν, υποθέτοντας $H\trianglelefteq A_n$ και $|H|>1$, κατα-
φέρουμε να δείξουμε ότι, αναγκαστικά, $H=A_n$.
Θα κάνουμε χρήση και της επόμενης παρατήρησης: Αν
$\sigma\in H$ και $\tau\in A_n$ τότε, λόγω της $H\trianglelefteq A_n$, $\tau\sigma\tau^{-1}\in H$ και,
συνεπώς, $\sigma^{-1}\tau\sigma\tau^{-1}\in H$.
Η απόδειξη χωρίζεται σε μερικά βήματα.
α) Αρκεί ν' αποδείξουμε ότι η H περιέχει ένα τουλάχιστον
κύκλο μήκους 3. Διότι τότε, όπως θα δούμε αμέσως μετά,
περιέχει όλους τους κύκλους μήκους 3, δηλαδή, από την πρό-
ταση 2.19 ταυτίζεται με την A_n. Πράγματι, έστω ότι
$\sigma=(a\,b\,c)\in H$ και $\tau=(x\,y\,z)$ είναι δοσμένοι κύ-
κλοι μήκους 3. Θεωρώ μια οποιαδήποτε μετάθεση $\phi\in S_n$
τέτοια ώστε $\phi(a)=x$, $\phi(b)=y$, $\phi(c)=z$. Τότε διαπιστώ-
νεται εύκολα (άσκηση) ότι $\phi\sigma\phi^{-1}=\tau$.* Αφ' ετέρου, επειδή
$n\geq 5$, υπάρχουν στοιχεία d, e διαφορετικά από τα a, b, c
καθώς και διαφορετικά μεταξύ τους, οπότε θεωρούμε την
αντιμετάθεση $\psi=(de)$. Προφανώς, επειδή οι κύκλοι σ και
ψ είναι ξένοι, ισχύει $\sigma\psi=\psi\sigma$, άρα $(\phi\psi)\sigma(\phi\psi)^{-1}=$
$=\phi(\psi\sigma\psi^{-1})\phi^{-1}=\phi\sigma\phi^{-1}=\tau$. Δηλαδή μέχρι στιγμής από-
δείξαμε ότι

$$\phi\sigma\phi^{-1}=\tau \quad \text{και} \quad (\phi\psi)\sigma(\phi\psi)^{-1}=\tau, \tag{3.22}$$

Όμως η ψ είναι περιττή μετάθεση (άσκηση 2.17(γ)), άρα

* Αρκεί ν' αποδειχθεί ότι οι $\phi\sigma\phi^{-1}$ και τ παίρνουν τις ίδιες τιμές στα x, y, z
και οι $\phi\sigma$ και $\tau\phi$ παίρνουν τις ίδιες τιμές στα a, b, c.

ή $\phi \in A_n$ ή $\phi\psi \in A_n$ καί λόγω της $H \trianglelefteq A_n$ τότε,
ή $\phi\sigma\phi^{-1} \in A_n$ ή $(\phi\psi)\sigma(\phi\psi)^{-1} \in A_n$. Καί στίς δύο περιπτώσεις δέμιος, ή (3.22) λέει ότι $\tau \in H$ καί διολληρώνει την απόδειξη τού ισχυρισμού μας.

Στό παρακάτω, λοιπόν, η προσπάθεια μας θά είναι στό να δείξουμε ότι η H περιέχει ένα τουλάχιστον κύκλο μήκους 3. Σύμφωνα με το θεώρημα 2.3 το κυκλικό στοιχείο ϕ της H γράφεται ως γινόμενο (πεπερασμένου πλήθους) κύκλων ξένων ανά δύο: $\sigma = \kappa_1 \dots \kappa_m$.

β) Αν για κάποιο $\sigma \in H$ ένας απ' τούς κύκλους $\kappa_1, \dots, \kappa_m$ έχει μήκος ≥ 3, τότε η H περιέχει ένα κύκλο μήκους 3. Πράγματι, έστω π.χ. $\kappa_1 = (a_1 a_2 \dots a_\nu)$, $\nu \geq 3$. Θεωρούμε τόν κύκλο $\tau = (a_1 a_2 a_3)$, ό δποίος αντιμετατίθεται με τούς $\kappa_2, \dots, \kappa_m$, ως ξένος προς αυτούς. Συνεπώς $\alpha_1 = \tau\sigma\tau^{-1} = \tau(\kappa_1 \kappa_2 \dots \kappa_m)\tau^{-1} = (\tau\kappa_1\tau^{-1})\kappa_2 \dots \kappa_m$. Όμως η τ είναι άρτια μετάθεση (Άσκηση 2.17 (γ)) άρα, λόγω της $H \trianglelefteq A_n$, $\tau\sigma\tau^{-1} \in H$. Συνεπώς $\sigma^{-1}\alpha_1 \in H$. Επειδή οί κύκλοι $\kappa_2, \dots, \kappa_m$ αντιμετατίθενται με όλους τούς κύκλους τούς ξένους προς αυτούς, έπεται ότι

$$\sigma^{-1}\alpha_1 = \sigma^{-1}(\tau\sigma\tau^{-1}) = \kappa_1^{-1}(a_1 a_2 a_3)\kappa_1(a_1 a_3 a_2)$$

Εύκολα διαπιστώνεται ότι

$(a_1 a_2 a_3)\kappa_1(a_1 a_3 a_2) = (a_2 a_3 a_4 a_4 \dots a_\nu)$ καί ότι $\kappa_1^{-1} = (a_\nu a_{\nu-1} \dots a_3 a_2 a_1)$. Συνεπώς,

$\sigma^{-1}\alpha_1 = (a_1 a_3 a_\nu)$, που είναι το αποδεικτέο.

Λόγω καί (β) αρκεί να εξετάσουμε στά παρακάτω τί γίνεται όταν για κάθε $\sigma \in H$ οί κύκλοι $\kappa_1, \dots, \kappa_m$ στούς δποίους αναλύεται είναι όλοι μήκους ≤ 3.

γ) Έστω ότι υπάρχει $\sigma \in H$, καί δποιοι δύο, τουλάχιστον, κύκλοι έχουν μήκος 3. Τότε $\sigma = (a_1 a_2 a_3)(b_1 b_2 b_3)\sigma'$, όπου οί κύκλοι $(a_1 a_2 a_3), (b_1 b_2 b_3)$ καί οί κύκλοι της σ' είναι ξένοι ανά δύο. Τότε θεωρούμε τον κύκλο $\tau = (a_2 a_3 b_1)$, ό δποίος αντιμετατίθεται με την σ'. Άρα η H περιέχει τό στοιχείο $\sigma^{-1}\tau\sigma\tau^{-1}$, τό δποίο ίσούται με

$$(a_1 a_2 a_3)^{-1}(b_1 b_2 b_3)^{-1}(a_2 a_3 b_1)(a_1 a_2 a_3)(b_1 b_2 b_3)(a_2 a_3 b_1)^{-1} =$$

$= (a_1 a_3 a_2)(b_1 b_3 b_2)(a_2 a_3 b_1)(a_1 a_2 a_3)(b_1 b_2 b_3)(a_2 b_1 a_3) =$
$= (a_1 a_2 b_1 a_3 b_3)$.

Συνεπῶς, ἡ H περιέχει ἕνα κύκλο μήκους 5, γεγονός πού ἀντίκειται στήν ὑπόθεση πού κάναμε μόλις πρίν ἀπ' τό (γ).

δ) Ἔστω ὅτι ὑπάρχει $\sigma \in H$ τέτοιο ὥστε μεταξύ τῶν κύκλων $\kappa_1, \ldots, \kappa_m$ στούς ὁποίους ἀναλύεται νά ὑπάρχει ἕνας, τοὐλάχιστον, μήκους 3. Τότε $\sigma = (a_1 a_2 a_3)\sigma'$, ὅπου ἡ σ' εἶναι γινόμενο ἀντιμεταθέσεων καί, συνεπῶς, $\sigma'^2 = 1$. Ἄρα, $\sigma^2 = (a_1 a_2 a_3)^2 = (a_1 a_3 a_2)$ καί $\sigma^2 \in H$ ὁπότε, καί πάλι, ἐρχόμαστε στήν περίπτωση (α).

ε) Μένει ἡ περίπτωση κατά τήν ὁποία ὅλες οἱ μεταθέσεις $\sigma \in H$, πλήν τῆς ταυτοτικῆς, εἶναι γινόμενα ἀντιμεταθέσεων. Ἐπειδή, ὅπως ἤδη ξέρομε, κάθε ἀντιμετάθεση εἶναι περιττή μετάθεση, θά πρέπει τό πλῆθος τῶν ἀντιμεταθέσεων στίς ὁποῖες ἀναλύεται κάθε $\sigma \in H$ νά εἶναι ἄρτιο. Ἔτσι κάθε $\sigma \in H$ εἶναι τῆς μορφῆς $\sigma = (a_1 a_2)(b_1 b_2)\sigma'$, ὅπου οἱ ἀντιμεταθέσεις $(a_1 a_2), (b_1 b_2)$ καί ἐκεῖνες στίς ὁποῖες ἀναλύεται ἡ σ' εἶναι ξένες ἀνά δύο. Θεωροῦμε τώρα ἕνα στοιχεῖο c διαφορετικό ἀπ' τά a_1, a_2, b_1, b_2 (αὐτό εἶναι δυνατόν ἐπειδή $n \geq 5$) καί τίς μεταθέσεις $\tau = (a_2 b_1 b_2)$ καί $\phi = (a_1 b_2 c)$. Κατασκευάζομε νέες μεταθέσεις τῆς H ὡς ἑξῆς:

$$\sigma_1 = \tau\sigma\tau^{-1} = (a_2 b_1 b_2)(a_1 a_2)(b_1 b_2)(a_2 b_2 b_1)\sigma' = (a_1 b_1)(a_2 b_2)\sigma'$$

$$\sigma_2 = \sigma\sigma_1 = (a_1 a_2)(b_1 b_2)(a_1 b_1)(a_2 b_2) = (a_1 b_2)(a_2 b_1)$$

$$\sigma_3 = \phi\sigma_2\phi^{-1} = (a_1 b_2 c)(a_1 b_2)(a_2 b_1)(a_1 b_2 c)^{-1} = (a_1 b_2 c)(a_1 b_2)(a_2 b_1)(a_1 c\, b_2) = (a_2 b_1)(b_2 c)$$

$$\sigma_2\sigma_3 = (a_1 b_2)(a_2 b_1)(a_2 b_1)(b_2 c) = (a_1 b_2 c)$$

Ἔτσι $(a_1 b_2 c) \in H$ καί αὐτό ἀντιφάσκει πρός τήν ὑπόθεση πού κάναμε στήν ἀρχή τοῦ (ε).

□

Τό θεώρημα πού ἀποδείξαμε λέει ὅτι ἡ ὁμάδα A_n, γιά

$n \neq 4$ δεν έχει μη τετριμμένες κανονικές υποομάδες. Το παρακάτω θεώρημα περιγράφει ακριβέστερα την κατάσταση για την ομάδα S_n. Θα χρειαστούμε πιό πρώτα μια ορισμή προτάση.

Πρόταση: Αν G είναι ομάδα μεταθέσεων ($|G| \geq 1$) τότε (3.23) το σύνολο των άρτιων μεταθέσεων της G αποτελεί κανονική υποομάδα της G, η οποία είτε ταυτίζεται με την G, είτε ο δείκτης της στην G ισούται με 2.

Απόδειξη: Έστω A το σύνολο των άρτιων μεταθέσεων της G. Επειδή το γινόμενο δύο άρτιων μεταθέσεων είναι άρτια μετάθεση, καθώς και η αντίστροφη μετάθεση μιάς άρτιας μετάθεσης είναι άρτια, έπεται ότι η A είναι υποομάδα της G. Αν $A \neq G$, τότε υπάρχει περιττή μετάθεση $\sigma \in G$. Προφανώς η κλάση σA είναι διαμερετική από την A, ως αποτελούμενη από περιττές μεταθέσεις. Θα δείξουμε ότι κάθε περιττή μετάθεση της G ανήκει στη σA. Πράγματι, αν $\tau \in G$ είναι περιττή, τότε η σ^{-1} είναι περιττή, άρα $\sigma^{-1}\tau \in A$, δηλαδή (πρόταση 3.2) $\tau \in \sigma A$. Έτσι, οι άρτιες πλευρικές κλάσεις ως προς A είναι δύο: η A, που αποτελείται από τις άρτιες μεταθέσεις της G και η σA, που αποτελείται από τις περιττές μεταθέσεις της G. Συνεπώς $[G:A] = 2$ και από την άσκηση 3.17(δ) έπεται ότι $A \trianglelefteq G$.

□

Θεώρημα: Αν $n > 4$, η μόνη μη τετριμμένη κανονική υποομάδα της S_n είναι η A_n. (3.24)

Απόδειξη: Κατ' αρχάς $A_n \trianglelefteq S_n$ λόγω της πρότασης 3.19. Έστω τώρα $H \trianglelefteq S_n$, $|H| > 1$. Θα δείξουμε ότι αν $H \neq S_n$, τότε $H = A_n$.

α) Πρώτα θα δείξουμε ότι $|H| \geq 2$. Πράγματι, αν ήταν $|H| = 2$, τότε $H = \{\iota, \sigma\}$ με $\sigma^2 = 1$. Από το (2.9) συμπεραίνουμε ότι η σ είναι αντιμετάθεση ή είναι γινόμενο δύο, τουλάχιστον, αντιμεταθέσεων. Στην πρώτη περίπτωση θέτουμε $\sigma = (a\,b)$ και θεωρούμε και τη μετάθεση $(a\,c) \in S_n$ όπου $c \neq a, b$. Θα πρέπει $H \ni (a\,c)(a\,b)(a\,c)^{-1} = (a\,c)(a\,b)(a\,c) = (b\,c) \neq 1, \sigma$,

δπότε ἀδηγούμαστε σε ἀντίφαση. Στη δεύτερη περίπτωση θέτουμε $\sigma = (a_1 a_2)(b_1 b_2)\sigma'$, ὅπου $a_2 \neq b_1, b_2$ καὶ ἡ μετάθεση σ' εἶναι γινόμενο κύκλων, κανεὶς ἀπ' τοὺς ὁποίους δὲν περιέχει τὸ ἀριθμὸ τὸ b_2 ⊛. Θέτουμε τώρα $\tau = (a_2 b_1 b_2)$, ὁπότε $\tau\sigma\tau^{-1} \in H$. Ὅμως εὔκολα διαπιστώνεται ὅτι $\tau\sigma\tau^{-1} \neq 1, \sigma$, ἄρα ἐρχόμαστε σε ἀντίφαση.

β) Ἔστω A τὸ σύνολο τῶν ἀρτίων μεταθέσεων τῆς H. Ἀπὸ τὴν πρόταση 3.23, $[H:A] \leq 2$ ἄρα $|A| = \frac{|H|}{[H:A]} \geq \frac{1}{2}|H|$.

Ὅμως $|H| \geq 2$ λόγω τοῦ (α), δηλαδὴ $|A| \geq 1$. Τώρα παρατηροῦμε ὅτι $A \neq A_n$. Πράγματι, ἔστω $\alpha \in A_n$. Τότε (βλ. ὑπόδειξη τοῦ (3.17)γ), $\alpha^{-1}A\alpha = \alpha^{-1}(H \cap A_n)\alpha = (\alpha^{-1}H\alpha) \cap (\alpha^{-1}A_n\alpha) = H \cap A_n = A$, ἄρα $A \trianglelefteq A_n$. Λόγω τώρα τῆς $|A| > 1$ καὶ τοῦ θεωρήματος 3.21 συμπεραίνουμε ὅτι $A = A_n$. Ὅμως $A = H \cap A_n$, δηλαδὴ $H \supseteq A_n$ καὶ, συνεπῶς, $|H| \geq |A_n| = \frac{1}{2}n!$ Ἀφ' ἑτέρου ἡ τάξη $|H|$ εἶναι διαιρέτης τοῦ $n!$ μικρότερος τοῦ $n!$ Τέτοιος διαιρέτης, ὁ ὁποῖος καὶ εἴπαμε, συγχρόνως, καὶ $\geq \frac{1}{2}n!$, δὲν ὑπάρχει ἄλλος πλὴν τοῦ $\frac{1}{2}n!$. Ἄρα $|H| = \frac{1}{2}n! = |A_n|$.

□

⊛ Ἀπόδειξη τοῦ ἰσχυρισμοῦ: Ἂν ἡ ἀνάλυση τῆς σ σὲ κύκλους ξένους ἀνὰ δύο (θεώρημα 2.5) μᾶς δώσει τοὐλάχιστον δύο κύκλους $(a_1 a_2 \cdots), (b_1 b_2 \cdots)$, τότε ὁ ἰσχυρισμὸς εἶναι φανερός. Ἂν ὄχι, τότε $\sigma = (a_1 a_2 \cdots a_r)$ μὲ $r \geq 3$, ἄρα $\sigma = (a_1 a_2)(a_1 a_3)\cdots(a_1 a_r)$. Τότε θέτουμε $b_1 = a_1$, $b_2 = a_2$ καὶ $\sigma' =$ γινόμενο τῶν ὑπολοίπων ἀντιμεταθέσεων.

4. Ὁμάδες-πηλίκα καὶ ὁμομορφισμοὶ ὁμάδων

Ἔστω $(G,\cdot)$ ὁμάδα καὶ $H \leq G$. Τότε οἱ δεξιὲς καὶ οἱ ἀριστερὲς πλευρικὲς κλάσεις ὡς πρὸς H συμπίπτουν. Συνήθως σ' αὐτὲς τὶς περιπτώσεις θὰ χρησιμοποιοῦμε τὸ συμβολισμὸ τῶν ἀριστερῶν πλευρικῶν κλάσεων. Τὸ σύνολο τῶν κλάσεων αὐτῶν συμβολίζομε μὲ G/H. Στὸ G/H ὁρίζομε μιὰ ἐσωτερικὴ πρᾶξη ὡς ἑξῆς:

$$(x_1H)\cdot(x_2H) \stackrel{\text{ορ}}{=} (x_1x_2)H \qquad (4.1)$$

Πρόταση. Ἡ πρᾶξη ποὺ ὁρίζεται στὴν (4.1) εἶναι καλὰ ὁρισμένη καὶ καθιστᾶ τὸ G/H ὁμάδα (ὁμάδα-πηλίκο τῆς G ὡς πρὸς H).

Ἀπόδειξη. Ἔστω $x_1H = y_1H$ καὶ $x_2H = y_2H$. Θὰ ἀποδείξομε ὅτι $(x_1x_2)H = (y_1y_2)H$. Πράγματι, ἀπ' τὴν ὑπόθεση συμπεραίνομε ὅτι $y_1 \in x_1H$ καὶ $y_2 \in x_2H = Hx_2$. Θέτομε $y_1 = x_1h_1$ καὶ $y_2 = h_2x_2$, ὅπου $h_1, h_2 \in H$. Τότε $y_1y_2 = x_1hx_2$, ὅπου $h = h_1h_2 \in H$. Ὅμως $Hx_2 = x_2H$, ὁπότε $hx_2 = x_2h'$ γιὰ κάποιο $h' \in H$. Συνεπῶς $y_1y_2 = x_1hx_2 = x_1x_2h' \in (x_1x_2)H$. Ἄρα $(y_1y_2)H = (x_1x_2)H$.

Ἡ πρᾶξη (4.1) εἶναι προφανῶς προσεταιριστική. Τὸ οὐδέτερο στοιχεῖο της εἶναι τὸ $H = 1\cdot H$, ἐνῶ τὸ ἀντίστροφο τοῦ xH εἶναι τὸ $x^{-1}H$. □

Παραδείγματα (4.2)

α) Ἔστω ἡ ὁμάδα $(\mathbb{Z},+)$ καὶ ἡ ὑποομάδα $m\mathbb{Z} = \{mx \mid x \in \mathbb{Z}\}$, ὅπου m ἀκέραιος ≥ 1. Ἐπειδὴ ἡ $\mathbb{Z}$ εἶναι ἀβελιανὴ ὁμάδα, εἶναι $m\mathbb{Z} \trianglelefteq \mathbb{Z}$. Εὔκολα διαπιστώνεται ὅτι $\mathbb{Z}/m\mathbb{Z} = \{m\mathbb{Z}, 1+m\mathbb{Z}, 2+m\mathbb{Z}, \ldots, (m-1)+m\mathbb{Z}\}$, καθὼς καὶ ὅτι $x+m\mathbb{Z} = y+m\mathbb{Z}$ ἂν καὶ μόνο ἂν $x \equiv y \pmod m$ (βλ. (1.12)η). Σὰν ἄσκηση κατασκευάστε τὸν πίνακα πράξεως τῆς ὁμάδας $\mathbb{Z}/6\mathbb{Z}$.

β) Ἂς θεωρήσομε τὴν ὁμάδα τῶν τεσσαρικῶν (quaternion) $(G,\cdot)$, ἡ ὁποία παράγεται ἀπὸ δύο στοιχεῖα a, b, ποὺ ὑπακούουν στὶς σχέσεις

$$a^4 = 1,\ a^2 = b^2 \neq 1;\ ba = a^3b$$

Διαπιστώνεται τότε (ἄσκηση) ὅτι ἡ G ἔχει τὰ ἑξῆς 8

Διαφορετικά στοιχεία:

$$G = \{1, a, a^2, a^3, b, ab, a^2b, a^3b\}.$$

Η G δεν είναι αβελιανή διότι π.χ. $ab \neq ba$. Η ομάδα $\langle a^2\rangle = \{1, a^2\}$ είναι κανονική υποομάδα της G (άσκηση) και

$$|G/\langle a^2\rangle| = [G : \langle a^2\rangle] = |G|/|\langle a^2\rangle| = 8:2 = 4.$$

Οι κλάσεις $\langle a^2\rangle$, $a\langle a^2\rangle$, $b\langle a^2\rangle$, $ab\langle a^2\rangle$ είναι διαφορετικές, άρα αποτελούν ακριβώς τα στοιχεία της $G/\langle a^2\rangle$.

Ο πίνακας πολ/σιασμού της $G/\langle a^2\rangle$ είναι ο εξής:

	$\langle a^2\rangle$	$a\langle a^2\rangle$	$b\langle a^2\rangle$	$ab\langle a^2\rangle$
$\langle a^2\rangle$	$\langle a^2\rangle$	$a\langle a^2\rangle$	$b\langle a^2\rangle$	$ab\langle a^2\rangle$
$a\langle a^2\rangle$	$a\langle a^2\rangle$	$\langle a^2\rangle$	$ab\langle a^2\rangle$	$b\langle a^2\rangle$
$b\langle a^2\rangle$	$b\langle a^2\rangle$	$ab\langle a^2\rangle$	$\langle a^2\rangle$	$a\langle a^2\rangle$
$ab\langle a^2\rangle$	$ab\langle a^2\rangle$	$b\langle a^2\rangle$	$a\langle a^2\rangle$	$\langle a^2\rangle$

Από τον πίνακα φαίνεται ότι η ομάδα-πηλίκο είναι αβελιανή.

γ) Έστω K ένα σώμα και $GL(n,K)$ η γενική γραμμική ομάδα του K βαθμού n (βλ. (1.12) γ). Έστω E το σύνολο των $n\times n$ πινάκων με στοιχεία από το K, των οποίων η ορίζουσα είναι 1. Είναι πολύ εύκολο να αποδείξει κανείς ότι το E είναι υποομάδα της $GL(n,K)$. Ακόμη περισσότερο, $E \trianglelefteq GL(n,K)$. Πράγματι αν $x \in GL(n,K)$, τότε $\det(x) \neq 0$ άρα για $u \in E$ έχομε $\det(x^{-1}ux) = \det(x)^{-1}\cdot 1\cdot \det(x) = 1$, δηλ. $x^{-1}ux \in E$. Από το (3.17)α έπεται τότε ότι $E \trianglelefteq GL(n,K)$. Εύκολα διαπιστώνεται επίσης ότι $x_1E = x_2E$ αν και μόνο αν $\det(x_1) = \det(x_2)$, οπότε τα στοιχεία της ομάδας-πηλίκο $GL(n,K)/E$ είναι της μορφής dE, όπου d είναι διαγώνιος $n\times n$ πίνακας της μορφής $\begin{pmatrix} d & & \\ & 1 & \\ & & \ddots \end{pmatrix}$, $d \in K$, $d \neq 0$.

Πρόταση (4.3) Αν η ομάδα $(G,\cdot)$ δεν είναι αβελιανή και Z είναι το κέντρο της G, τότε η ομάδα G/Z δεν είναι κυκλική.

Απόδειξη. Αν η G/Z ήταν κυκλική, τότε όλα τα στοιχεία της θα ήταν της μορφής a^vZ όπου $v \in \mathbb{Z}$. Τότε $a \notin Z$ γιατί σε αντίθετη περίπτωση $G/Z = \{Z\}$, που σημαίνει ότι $G = Z$ άτοπο γιατί η Z είναι αβελιανή ομάδα ενώ η G, εξ υποθέσεως, δεν είναι.

Ἂς θεωρήσουμε τώρα δυό ὁποιαδήποτε στοιχεῖα $x, y \in G$. Τότε $xZ = a^\mu Z$ καί $yZ = a^\nu Z$ γιά κατάλληλους ἀκεραίους μ καί ν. Ἄρα $x = a^\mu z_1$ καί $y = a^\nu z_2$, ὅπου $z_1, z_2 \in Z$ καί, συνεπῶς ἀντιμετατίθενται μέ ὅλα τά στοιχεῖα τῆς G. Τότε $xy = a^\mu z_1 a^\nu z_2 = a^\mu a^\nu z_1 z_2 = a^{\mu+\nu} z_1 z_2$ καί, ἀνάλογα, $yx = a^{\mu+\nu} z_1 z_2$. Ἔτσι $xy = yx$ γιά ὁποιαδήποτε $x, y \in G$, γεγονός πού ἀντιμαρτύρεται μέ τήν ὑπόθεσή μας. □

Πόρισμα (4.4) Κάθε ὁμάδα τάξεως p^2, ὅπου p εἶναι πρῶτος ἀριθμός, εἶναι πάντ' ἀπλῶς ἀβελιανή.

Ἀπόδειξη. Ἔστω ἡ ὁμάδα $(G, \cdot)$ μέ $|G| = p^2$ καί Z τό κέντρο της. Ἀπ' τήν πρόταση 3.15 εἶναι $|Z| = p$ ἢ p^2. Στήν δεύτερη περίπτωση εἶναι $Z = G$, ἄρα ἡ G εἶναι ἀβελιανή. Στήν πρώτη περίπτωση $|G/Z| = |G|/|Z| = p^2 : p = p$, ἄρα (βλ. ἄσκηση 3.4) ἡ G/Z εἶναι κυκλική, κάτι πού ἀντιφάσκει πρός τήν πρόταση 4.3. Ἔτσι, αὐτή ἡ περίπτωση ἀποκλείεται καί, συνεπῶς, ἡ G εἶναι ἀβελιανή. □

Ὁμομορφισμοί ὁμάδων (4.5) Ἔστω $(G, \cdot)$, $(G', \cdot)$ δυό ὁμάδες. Μιά ἀπεικόνιση $\phi : G \longrightarrow G'$ λέγεται ὁμομορφισμός μεταξύ τῶν ὁμάδων G καί G' ἄν γιά κάθε ζεύγος $x, y \in G$ ἰσχύει $\phi(x \cdot y) = \phi(x) \cdot \phi(y)$. Ἄν ὁ ὁμομορφισμός ϕ εἶναι, ἐπιπλέον, ἀμφιμονοσήμαντη ἀπεικόνιση τότε ὁ ϕ λέγεται μονομορφισμός, ἄν εἶναι ἀπεικόνιση "ἐπί", τότε λέγεται ἐπιμορφισμός καί, τέλος, ἄν εἶναι ἀμφιμονοσήμαντη καί "ἐπί" ἀπεικόνιση, τότε ὁ ϕ λέγεται ἰσομορφισμός. Σ' αὐτή τήν περίπτωση οἱ ὁμάδες G καί G' λέγονται ἰσόμορφες· συμβολικά $G' \cong G$.

Ἰσόμορφες ὁμάδες ἔχουν ἀκριβῶς τίς ἴδιες ἰδιότητες. Π.χ. ἄν καί οἱ δυό εἶναι πεπερασμένες, τότε ἔχουν τήν ἴδια τάξη, οἱ δέ πίνακες τῶν πράξεών τους εἶναι οἱ ἴδιοι, ἄν γράψουμε μέ κατάλληλη σειρά τά στοιχεῖα τῶν ὁμάδων κι ἄν ἀγνοήσουμε τά διαφορετικά σύμβολα μέ τά ὁποῖα παριστάνονται τά στοιχεῖα τῶν δυό ὁμάδων. Γιά παράδειγμα, ἄς θεωρή-

πάρε την δυναμοδα της $(\mathbb{R}^*, \cdot)$ $(\mathbb{Q}^* = \mathbb{Q} - \{0\})$, η δποία παράγεται απ' το -1 κι ό,τι συμβολίσαμε με H. Τότε $H = \{1, -1\}$. Θεωρούμε και την ομάδα $\mathbb{Z}_2$ (βλ. (1.12) η). Είναι $\mathbb{Z}_2 = \{\hat{0}, \hat{1}\}$. Η απεικόνιση $\phi: H \longrightarrow \mathbb{Z}_2$ για την δποία $\phi(1) = \hat{0}$ και $\phi(-1) = \hat{1}$ είναι, όπως εύκολα διαπιστώνεται, ισομορφισμός. Άρα $H \cong \mathbb{Z}_2$. Συγκρίνετε τους πίνακες των δυο πράξεων.

(H)	1	-1
1	1	-1
-1	-1	1

$(\mathbb{Z}_2)$	$\hat{0}$	$\hat{1}$
$\hat{0}$	$\hat{0}$	$\hat{1}$
$\hat{1}$	$\hat{1}$	$\hat{0}$

Παρατηρήσατε ότι αν στον πρώτο πίνακα συμβολίζαμε το στοιχείο 1 με το σύμβολο $\hat{0}$ και το -1 με το σύμβολο $\hat{1}$, τότε ο πίνακας θα ήταν ο ίδιος με τον δεύτερο πίνακα.

Περισσότερα παραδείγματα. Ασχοληθήκατε στα παραδείγματα του (4.2):

(4.6)

α) Ας θεωρήσουμε την ομάδα $\mathbb{Z}_m$ (βλ. (1.12) η). Η απεικόνιση $\phi: \mathbb{Z}_m \longrightarrow \mathbb{Z}/m\mathbb{Z}$ η δποία ορίζεται απ' την σχέση $\phi(\hat{a}) = a + m\mathbb{Z}$ είναι ισομορφισμός. Έτσι $\mathbb{Z}_m \cong \mathbb{Z}/m\mathbb{Z}$.

β) Θεωρήστε την ομάδα των τετραδών του Κλάιν, που παράγεται απ' τις μεταθέσεις σ και τ της άσκησης 3.2α, έστω V. Τότε η απεικόνιση $\phi: V \longrightarrow G/\langle a^2 \rangle$ για την δποία $\phi(1) = \langle a^2 \rangle$, $\phi(\sigma) = a\langle a^2 \rangle$, $\phi(\tau) = b\langle a^2 \rangle$, $\phi(\sigma\tau) = ab\langle a^2 \rangle$, είναι ισομορφισμός. Αν συμβολίζαμε τα στοιχεία $\langle a^2 \rangle$, $a\langle a^2 \rangle$, $b\langle a^2 \rangle$ με τα $1, \sigma, \tau$, αντιστοίχως, τότε οι πίνακες πράξεων των δυο ομάδων θα ήταν οι ίδιοι.

γ) Είδαμε ότι η ομάδα $GL(n, K)/E$ αποτελείται από τα στοιχεία (κλάσεις) της μορφής dE όπου d είναι ο διαγώνιος πίνακας $\begin{pmatrix} d & & \\ & 1 & \\ & & \ddots \end{pmatrix}$ για κάποιο $d \in K^*$. Εύκολα βλέπει κανείς ότι η απεικόνιση $\phi: K^* \longrightarrow GL(n, K)$ για την δποία $\phi(d) = dE$, όπου d ο παραπάνω διαγώνιος πίνακας, είναι ισομορφισμός. Συνεπώς $GL(n, K)/E \cong K^*$.

Πυρήνας ενός ομομορφισμού. (4.7)
Έστω ότι $(G,\cdot)$ και $(G',\cdot)$ είναι ομάδες. Συμβολίζουμε τα μοναδιαία στοιχεία τους με 1 και $1'$, αντιστοίχως. Έστω ότι $\phi: G \longrightarrow G'$ είναι ομομορφισμός.
Το σύνολο $\{x \in G : \phi(x) = 1'\}$ λέγεται πυρήνας του ϕ και συμβολίζεται με $\ker\phi$. Ο πυρήνας του ϕ είναι υποομάδα της G, δηλαδή είναι κλειστός ως προς την πράξη της G ⊛
(απόδειξη: $x,y \in \ker\phi \Rightarrow \phi(x)=\phi(y)=1' \Rightarrow \phi(xy) = \phi(x)\phi(y) = 1'\cdot 1' = 1' \Rightarrow xy \in \ker\phi$) και διότι $x \in \ker\phi \Rightarrow x^{-1} \in \ker\phi$. Για την απόδειξη της τελευταίας συνεπαγωγής χρειαζόμαστε τις έξης δύο γενικές και πολύ χρήσιμες σχέσεις:

$$1 \in \ker\phi \quad \& \quad \phi(x^{-1}) = \phi(x)^{-1} \quad \forall\, x \in G \qquad (4.8)$$

Η πρώτη απ' τις (4.8) αποδεικνύεται ως εξής: Έστω $x \in G$. Τότε $\phi(x) = \phi(x\cdot 1) = \phi(x)\cdot\phi(1)$, δηλ. $\phi(x)\cdot\phi(1) = \phi(x)\cdot 1'$, απ' όπου $\phi(1) = 1'$.
Απόδειξη της δεύτερης στην (4.8): Έστω $x \in G$. Τότε $1' = \phi(1) = \phi(x\cdot x^{-1}) = \phi(x)\cdot\phi(x^{-1})$, δηλ. το αντίστροφο του $\phi(x)$ είναι το $\phi(x^{-1})$, δ.έ.δ.
Τώρα, αν $x \in \ker\phi$, δε' ίσχυει $1' = \phi(x)$ άρα και $1' = \phi(x)^{-1} = \phi(x^{-1})$, που σημαίνει ότι $x^{-1} \in \ker\phi$.
Την εικόνα του ομομορφισμού ϕ συμβολίζουμε με $\mathrm{Im}\phi$ ή με $\phi(G)$ και είναι υποομάδα της G' (άσκηση).

Θεμελιώδες θεώρημα του ισομορφισμού ομάδων. (4.9)
Αν $\phi: G \longrightarrow G'$ είναι ομομορφισμός ομάδων τότε $\ker\phi \trianglelefteq G$ και $\phi(G) \cong G/\ker\phi$.
Απόδειξη. Έστω $x \in G$ και $u \in \ker\phi$. Τότε $\phi(x^{-1}ux) = \phi(x^{-1})\phi(u)\phi(x) = \phi(x)^{-1}\cdot 1'\cdot\phi(x) = 1'$, που σημαίνει ότι $x^{-1}ux \in \ker\phi$. Άρα (βλ. (3.17)α) $\ker\phi \trianglelefteq G$.
Ορίζουμε τώρα την εξής απεικόνιση

$$\tilde{\phi}: G/\ker\phi \longrightarrow \phi(G)$$
$$\tilde{\phi}(x\cdot\ker\phi) = \phi(x).$$

α) Η $\tilde{\phi}$ είναι καλά ορισμένη: Έστω $x\cdot\ker\phi = y\cdot\ker\phi$. Τότε $y^{-1}x \in \ker\phi$ άρα $\phi(y^{-1}x) = 1'$. Συνεπώς $\phi(y)^{-1}\phi(x) = 1'$, που σημαίνει ότι $\phi(x) = \phi(y)$. Άρα

⊛ Μία πολύ χρήσιμη παρατήρηση (άλλη άσκηση) είναι η εξής: Το ϕ είναι ενφιπονομήματος (μονομορφισμός) $\Longleftrightarrow \ker\phi = \langle 1\rangle$.

$\tilde{\phi}(x\cdot\ker\phi) = \tilde{\phi}(y\cdot\ker\phi)$ κτλ.

β) Η $\tilde{\phi}$ είναι αμφιμονοσήμαντη: Έστω $\tilde{\phi}(x\cdot\ker\phi)=\tilde{\phi}(y\cdot\ker\phi)$. Τότε $\phi(x)=\phi(y)$. Άρα $\phi(y^{-1}x)=\phi(y)^{-1}\phi(x)=1'$, δηλ. $y^{-1}x\in\ker\phi$, οπότε και $x\cdot\ker\phi = y\cdot\ker\phi$.

γ) Η $\tilde{\phi}$ είναι προφανώς επί, αφού αν $x'\in\phi(G)$, τότε $x'=\phi(x)$ για κάποιο $x\in G$, άρα $\tilde{\phi}(x\cdot\ker\phi)=\phi(x)=x'$.

δ) Η $\tilde{\phi}$ είναι ομομορφισμός: $\tilde{\phi}[(x\cdot\ker\phi)(y\cdot\ker\phi)] =$
$= \tilde{\phi}(xy\cdot\ker\phi) = \phi(xy) = \phi(x)\phi(y) = \tilde{\phi}(x\ker\phi)\cdot\tilde{\phi}(y\ker\phi)$.

□

Παραδείγματα εφαρμογής του θεωρήματος 4.9. (4.10)

α) Έστω η απεικόνιση $\phi: \mathbb{Z} \longrightarrow \mathbb{Z}_m$ (m ακέραιος ≥ 1), η οποία ορίζεται: $\phi(x) = \hat{x}$ $\forall x\in\mathbb{Z}$. Από τον τρόπο που έχει οριστεί το $\mathbb{Z}_m$ και η πράξη + σ' αυτό προκύπτει ότι η ϕ είναι ένας επιμορφισμός. Άρα, σύμφωνα με το θεώρημα 4.9, $\mathbb{Z}_m \cong \mathbb{Z}/\ker\phi$. Όπως είναι εύκολο να δει κανείς ότι $x\in\ker\phi$ αν και μόνο αν ο x είναι πολλαπλάσιο του m, άρα $\ker\phi = m\mathbb{Z}$. Συμπεραίνομε λοιπόν ότι $\mathbb{Z}_m \cong \mathbb{Z}/m\mathbb{Z}$, και το οποίο ήδη διαπιστώσαμε στο (4.6)α.

β) Θεωρούμε τις ομάδες $\mathbb{Z}_{12}$ και $\mathbb{Z}_4$. Τα στοιχεία τους (κλάσεις) συμβολίζομε, προς αποφυγή συγχύσεως, με $\hat{a}$ και $\bar{a}$, αντιστοίχως. Θεωρούμε την απεικόνιση $\phi: \mathbb{Z}_{12} \longrightarrow \mathbb{Z}_4$, που ορίζεται ως εξής:

$\phi(\hat{a}) = \overline{v(a)}$, όπου $v(a)$ είναι το υπόλοιπο της διαίρεσης του a με το 4 ($v(a)\in\{0,1,2,3\}$). Η ϕ είναι επιμορφισμός και $\ker\phi = \{\hat{a},\hat{4},\hat{8}\} = \langle\hat{4}\rangle$. Άρα $\mathbb{Z}_{12}/\langle\hat{4}\rangle \cong \mathbb{Z}_4$.

Ως μία ακόμη εφαρμογή δίνεται η παρακάτω άσκηση.

Άσκηση. Έστω $\phi: G \longrightarrow G'$ ομομορφισμός ομάδων. Αν (4.11) η G είναι πεπερασμένη τότε η τάξη της ομάδας $\mathrm{Im}\phi$ είναι διαιρέτης του $|G|$. Επιπλέον για κάθε $x'\in G'$ ή δεν υπάρχει κανένα x τέτοιο ώστε $\phi(x)=x'$ ή υπάρχουν ακριβώς τόσα όση η τάξη του $\ker\phi$.

Εσωτερικό άθροισμα δομάδων: Έστω ότι $(H,\cdot)$ και $(K,\cdot)$ είναι δύο οποιεσδήποτε ομάδες (οι ομάδες μπορεί να είναι εντελώς άσχετες μεταξύ τους, όπως οι πράξεις τους, αν και συμβολίζονται με το ίδιο σύμβολο $\cdot$, εν γένει, δεν έχουν καμμία σχέση). Το σύνολο (καρτεσιανό γινόμενο) $H\times K$ εφοδιασμένο με την πράξη

$$(h_1,u_1)\cdot(h_2,u_2)=(h_1\cdot h_2,\ u_1\cdot u_2)$$

(νέα πράξη; πράξη της H; πράξη της K)

είναι ομάδα (πολύ εύκολη η απόδειξη).
Κάθε ομάδα G ισόμορφη προς την νέα αυτή ομάδα που βρίσκαμε, χαρακτηρίζεται ως εσωτερικό άθροισμα των ομάδων H και K. Συμβολικά: $G=H\oplus K$.

Σημαντικά παραδείγματα: Αν $m,n>1$ ακέραιοι και $(m,n)=1$, τότε $\mathbb{Z}_m\oplus\mathbb{Z}_n\cong\mathbb{Z}_{mn}$.
Απόδειξη. Γενικά συμβολίζουμε: Αν $a\in\mathbb{Z}$ και ν θετικός ακέραιος, συμβολίζω με $[a]_\nu$ την κλάση του a mod ν. Τα στοιχεία της $\mathbb{Z}_m\oplus\mathbb{Z}_n$ έχουν τη μορφή $([a]_m,[b]_n)$. Λόγω του "κινέζικου θεωρήματος" της Θεωρίας Αριθμών, επειδή $(m,n)=1$, υπάρχει ακέραιος x τ.ώ. $x\equiv a\ (\mathrm{mod}\ m)$ & $x\equiv b\ (\mathrm{mod}\ n)$, δηλ. $([a]_m,[b]_n)=([x]_m,[x]_n)$. Ορίζουμε τώρα

$$f:\mathbb{Z}_m\oplus\mathbb{Z}_n\longrightarrow\mathbb{Z}_{mn},\quad f([a]_m,[b]_n)=([x]_m,[x]_n)$$

και εύκολα αποδεικνύεται ότι η f είναι ομομορφισμός. Επειδή όμως οι τάξεις και των δύο ομάδων, δηλ. της $\mathbb{Z}_m\oplus\mathbb{Z}_n$ και της $\mathbb{Z}_{mn}$ είναι ίσες (και ίσες με mn), η f είναι και "επί", άρα ισομορφισμός.
Άσκηση. Αποδείξτε ότι οι ομάδες $\mathbb{Z}_2\oplus\mathbb{Z}_4$, $\mathbb{Z}_2\oplus\mathbb{Z}_2\oplus\mathbb{Z}_2$ είναι αβελιανές αλλά όχι κυκλικές. Επίσης, δεν είναι ισομορφες μεταξύ τους.

Ταξινόμηση ομάδων. Αν μάς δοθεί μια ομάδα G θέλουμε να ξέρουμε αν αυτή είναι ισόμορφη με κάποια ομάδα - "μοντέλο", δηλ. με κάποια ομάδα την οποία έχουμε ξεχωρίσει π.χ. λόγω της σημασίας της. Π.χ. όλες οι άπειρες κυκλικές ομάδες είναι ισόμορφες με την ομάδα $(\mathbb{Z}, +)$. Η προσθετική ομάδα των ακεραίων, λοιπόν, αποτελεί το πρότυπο για όλες τις άπειρες κυκλικές ομάδες. Συνεπώς, αν η G είναι μια τέτοια ομάδα, οποιαδήποτε πληροφορία χρειαζόμαστε για αυτήν (στον αφορά, αποκλειστικά, τη δομή της ως ομάδος) την παίρνουμε απ' τη μελέτη της ομάδας $(\mathbb{Z}, +)$. (4.12)

Επίσης, αν δούμε ένας θετικός ακέραιος n θέλουμε να ξέρουμε όλες τις ομάδες - πρότυπα, εών οποίων η τάξη είναι n. Το πρόβλημα θα έχει λυθεί όταν καταφέρουμε να βρούμε πεπερασμένα πλήθος ομάδων $G_1, \ldots, G_k$, οι οποίες είναι ανά δύο μη ισόμορφες και τέτοιες ώστε: για κάθε ομάδα τάξεως n υπάρχει (ακριβώς) μία ομάδα G_i απ' τις παραπάνω, τέτοια ώστε $G \cong G_i$. Αν πετύχουμε κάτι τέτοιο, τότε λέμε ότι έχουμε ταξινομήσει τις πεπερασμένες ομάδες τάξεως n. Μερικές φορές αυτό επιτυγχάνεται εύκολα. Για παράδειγμα, η καθε ομάδα τάξεως p, όπου p πρώτος, είναι ισόμορφη με την ομάδα $(\mathbb{Z}_p, +)$. Πράγματι, αν για την ομάδα $(G, \cdot)$ είναι $|G| = p$ τότε η G είναι κυκλική (άσκηση 3.4), οπότε $G = \{1, a, \ldots, a^{p-1}\}$ για κάποιο κατάλληλο $a \in G$, για το οποίο $a^p = 1$. Τότε η απεικόνιση $\phi: G \longrightarrow \mathbb{Z}_p$ με $\phi(a^\nu) = \hat{\nu}$, όπου $\nu \in \{0, 1, \ldots, p-1\}$, είναι ισομορφισμός, άρα $G \cong \mathbb{Z}_p$. Εν γένει, το πρόβλημα της ταξινόμησης των πεπερασμένων ομάδων είναι εξαιρετικά δύσκολο.

Παρακάτω θα επιχειρήσουμε την ταξινόμηση των ομάδων με τάξη ≤ 8.

Επειδή, σύμφωνα με όσα είπαμε λίγο παραπάνω, η ταξινόμηση των ομάδων τάξεως $2, 3, 5, 7$ είναι άμεση, αρκεί να ταξινομήσουμε τις ομάδες τάξεως $4, 6$ και 8. (4.13)

Υπάρχουν ακριβώς δύο πρότυπα ομάδων τάξεως 4. Και οι δύο (4.14)

είναι αβελιανές.

Πράγματι, έστω $|G|=4$. Αν $a\in G$ και η τάξη του a είναι 4, τότε $G=\langle a\rangle$ και η G είναι η κυκλική ομάδα τάξεως 4. Έστω τώρα ότι κανένα στοιχείο της G δεν έχει τάξη 4. Τότε, από το θεώρημα του Lagrange, όλα τα στοιχεία της G που είναι διαφορετικά του 1, θα έχουν τάξη 2. Αν λοιπόν $G=\{1,a,b,c\}$, τότε $a^2=b^2=c^2=1$. Προφανώς $ab\neq 1, a, b$, άρα $c=ab$. Τότε, από την $(ab)^2=1$ έχουμε $abab=a^2b^2$, από όπου $ba=ab$. Συνεπώς η G σ'αυτήν την περίπτωση παράγεται από τα a, b, για τα οποία ισχύουν οι σχέσεις $a^2=b^2=1$ και $ab=ba$. Είναι δηλαδή η G η "ομάδα των τεσσάρων του Klein" (σρβλ. 3.20).

(4.15) Υπάρχουν ακριβώς δύο προτυπα ομάδων τάξεως 6. Η μία είναι κυκλική και η άλλη μη αντιμεταθετική.

Απόδειξη. Έστω $|G|=6$. Αν η G περιέχει ένα στοιχείο τάξεως 6, τότε είναι κυκλική με την ίδια τάξη.

Ας θεωρήσουμε τώρα ότι αυτό δεν ισχύει. Τότε κάθε στοιχείο της G, πλην του 1, έχει τάξη 2 ή 3. Θα δείξουμε πρώτα ότι δεν είναι δυνατόν όλα τα στοιχεία, πλην του 1, να έχουν τάξη 2. Γιατί έστω ότι αυτό συνέβαινε και $a, b\in G-\{1\}$. Από τις σχέσεις $a^2=b^2=1$, έπεται ότι $ab\neq 1, a, b$. Στη συνέχεια, $(ab)^2=1$ άρα (όπως στο 4.14) $ab=ba$. Δηλαδή τότε η G θα είχε την υποομάδα $\langle a,b\rangle$, η οποία είναι η ομάδα των 4 του Klein. Αυτό, όμως, αντιφάσκει στο θεώρημα του Lagrange. Συνεπώς υπάρχει κάποιο $a\in G$ με τάξη 3. Ας θεωρήσουμε τώρα ένα $b\in G-\{1,a,a^2\}$. Τότε είναι εύκολη άσκηση να δει κανείς ότι τα έξη στοιχεία

$$1,\ a,\ a^2,\ b,\ ba,\ ba^2 \qquad (4.16)$$

είναι διαφορετικά ανά δύο, άρα συνιστούν την G.

Τώρα το b^2 πρέπει να είναι ένα από τα στοιχεία (4.16). Αν $b^2\neq 1$, τότε η τάξη του b είναι 3 και $b^2\in\{a, a^2, b, ba, ba^2\}$. Από την $b^2=a$ έπεται ότι $1=b^3=ba$, άτοπο. Όμοια αποδεικνύεται ότι $b^2\neq a^2$. Τέλος, το ότι $b^2\neq b, ba, ba^2$, αυτό είναι φανερό. Αναγκαστικά λοιπόν, είναι $b^2=1$.

Στη συνέχεια, επειδή $ab \in G$, θα πρέπει τό ab να είναι κάποιο από τα στοιχεία 4.16. Αλλά τα $1, a, a^2, b$ προφανώς αποκλείονται. Άρα $ab = ba$ ή $ab = ba^2$. Αν ίσχυε τό πρώτο, τότε $(ab)^2 = abab = abba = ab^2a = a \cdot 1 \cdot a = a^2 \neq 1$ και $(ab)^3 = (ab)^2 ab = a^2 ab = a^3 b = 1 \cdot b = b \neq 1$. Άφού δέον $(ab)^2 \neq 1$ και $(ab)^3 \neq 1$, θα έπρεπε τό ab να είναι τάξεως 6, κάτι που έχει αποκλεισθεί εξ υποθέσεως. Άρα, μένει η περίπτωση της $ab = ba^2$, που συνδυαζεται, λόγω και των $a^3 = b^2 = 1$, με την $(ab)^2 = 1$. Μέχρι στιγμής, λοιπόν, καταλήξαμε στις σχέσεις

$$a^3 = b^2 = (ab)^2 = 1. \tag{4.17}$$

Με τη βοήθεια αυτών των σχέσεων βλέπαμε ότι, αν επιχειρήσουμε την κατασκευή του πίνακα πολλαπλασιασμού της G, υπάρχει ένα και μόνο ένας πίνακας, δηλ. η σχέση $G = \langle a, b \rangle$ μαζί με τις (4.17) καθορίζει μοναδικά την δομάδα G. (4.18)

Άσκηση. Κατασκευάστε τον πίνακα της $(G, \cdot)$ για την ομάδα $G = \langle a, b \rangle$ και ισχύουν οι (4.17).

Υπάρχουν πέντε πρότυπα μη-ισόμορφα είδη ομάδων τάξεως 8: Η κυκλική ομάδα τάξεως 8, δύο αβελιανές ομάδες, εκτός της κυκλικής*, και δύο μη αντιμεταθετικές (η διεδρική ομάδα D_4 και η ομάδα των τεταρτονίων (βλ. (4.2)β.)). (4.19)

Απόδειξη. Έστω ότι $|G| = 8$. Αν η G έχει κάποιο στοιχείο τάξεως 8, τότε είναι κυκλική με αυτήν την τάξη. Αν όχι, τότε κάθε στοιχείο της G, πλην του 1, θα έχει τάξη 2 ή 4.

Υποθέτουμε πρώτα ότι η G έχει κάποιο στοιχείο a τάξεως 4. Τότε θεωρούμε $b \in G - \{1, a, a^2, a^3\}$, οπότε (άσκηση) τα στοιχεία

$$1, a, a^2, a^3, b, ab, a^2b, a^3b \tag{4.20}$$

είναι διαφορετικά ανά δύο και, συνεπώς, απαριθμούν την G. Κάνοντας χρήση του γεγονότος ότι κάθε στοιχείο της G, πλην του 1, έχει τάξη 2 ή 4, συμπεραίνουμε ότι $b^2 = 1$ ή $b^2 = a^2$. Έτσι, διακρίνουμε δύο περιπτώσεις:

* Από την άσκηση της σελ. 39α συμπεραίνουμε όμως, αναγκαστικά, αλλιώς οι δύο αβελιανές ομάδες είναι οι $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$ και $\mathbb{Z}_2 \oplus \mathbb{Z}_4$.

i) Ισχύει $b^2=1$. Τότε (άσκηση) είναι αναγκαστικά $ba=ab$ ή a^3b. Στην πρώτη περίπτωση είναι πολύ εύκολο να δεί κανείς ότι η ομάδα είναι αβελιανή και να κατασκευάσει τον πίνακα πολλαπλασιασμού της. Η G σ' αυτήν την περίπτωση χαρακτηρίζεται από τις σχέσεις

$$G=\langle a,b\rangle,\ a^4=b^2=1,\ ab=ba,$$

μοναδήμαντα. Στη δεύτερη περίπτωση η G χαρακτηρίζεται μοναδήμαντα από τις σχέσεις

$$G=\langle a,b\rangle,\ a^4=b^2=1,\ ba=a^3b.$$

Όμως αυτές ακριβώς οι σχέσεις χαρακτηρίζουν τη διεδρική ομάδα D_4, η οποία δεν είναι αβελιανή.

ii) Ισχύει $b^2=a^2\neq 1$. Τότε είναι φανερό ότι $ba\neq 1,a,a^2,a^3,b$. Αν $ba=ab$, τότε θεωρούμε τα στοιχεία $c=ab^{-1}$ για τα οποία ισχύει $c^2=1$, $ca=ac$, $c\neq 1,a,a^2,a^3$. Λόγω της $b=c^{-1}a$ το b στην (4.20) μπορεί ν' αντικατασταθεί από το c, οπότε $G=\langle a,c\rangle$, $a^4=c^2=1$, $ac=ca$, άρα η G είναι εκείνη που βρήκαμε στο (i). Αν $ba\neq ab$, τότε λόγω και της $ba\neq ba^2$, θα είναι $ba=a^3b$ και η G χαρακτηρίζεται μοναδήμαντα (όπως φαίνεται αν επιχειρήσουμε την κατασκευή του πίνακα πολλαπλασιασμού) από τις σχέσεις

$$G=\langle a,b\rangle,\ a^4=1,\ a^2=b^2\neq 1,\ ba=a^3b.$$

Είναι δηλ. η G η ομάδα των τεσσάρων (πρβλ. (4.22)β). Η ομάδα αυτή δεν είναι αβελιανή.

Στη συνέχεια, ας υποθέσουμε ότι όλα τα στοιχεία της G, πλην του 1, έχουν τάξη 2. Τότε (βλ. άσκηση 4.21) η G είναι αβελιανή. Ας πάρουμε τα $a,b\in G-\{1\}$ με $a\neq b$. Τότε η ομάδα $\langle a,b\rangle$ είναι η ομάδα των 4 του Klein, άρα $\langle a,b\rangle\neq G$. Συνεπώς μπορώ να θεωρήσω ένα στοιχείο $c\in G-\langle a,b\rangle$. Τότε φαίνεται εύκολα ότι τα στοιχεία

$$1,a,b,c,ab,ac,bc,abc$$

είναι ανά δύο διαφορετικά, άρα αυτά απαριθμούν την G. Τώρα είναι εύκολη η κατασκευή του πίνακα πολλαπλασιασμού της G, η οποία μένεται μοναδήμαντα. Σ' αυτήν την περίπτωση

λοιπόν, η ομάδα G χαρακτηρίζεται μοναδικά από τις σχέσεις

$$G = \langle a, b, c \rangle \;;\; a^2 = b^2 = c^2 = 1.$$

Έτσι ολοκληρώθηκε η απόδειξη του ισχυρισμού (4.19).

Άσκηση. Αποδείξτε ότι αν σε μια ομάδα κάθε στοιχείο (4.21)
έχει τάξη 2, τότε η ομάδα είναι αβελιανή.

Άσκηση. Κατασκευάστε τους πίνακες πολ/σμού για (4.22)
όλες τις ομάδες τάξης 8.

Άσκηση. Βρείτε όλα τα στοιχεία τάξεως 2 της D_4. Δείξτε ότι κάθε (4.23)
υποομάδα τάξεως 2 της D_4 περιέχεται σε μία υποομάδα τάξεως 4.

5. Τα θεωρήματα του L. Sylow

Αρχικά δίνουμε μερικές έννοιες και αποτελέσματα γενικού χαρακτήρα.

Έστω $(G, \cdot)$ ομάδα και A, B υποομάδες της. Ορίζουμε (5.1)

$$A \cdot B = \{ x \in G : x = a \cdot b \text{ για κάποια } a \in A \text{ και } b \in B \}.$$

Θεώρημα α) Το σύνολο AB είναι ομάδα (υποομάδα της G) (5.2)
αν και μόνο αν

$$A \cdot B = B \cdot A \tag{5.3}$$

β) Έστω ότι οι υποομάδες A, B είναι πεπερασμένες.
Τότε

$$|A \cdot B| = \frac{|A| \cdot |B|}{|A \cap B|}$$

γ) Βλ. σελ 44α

Απόδειξη α) Έστω ότι ισχύει η (5.3). Ας θέσουμε $H = AB$.
Θα δείξουμε την κλειστότητα της H ως προς την πράξη. Πράγματι,
έστω $a_1 b_1$ και $a_2 b_2$ δύο στοιχεία της H. Λόγω της (5.3), υπάρχουν
$a' \in A$ και $b' \in B$ τέτοια ώστε $b_1 a_2 = a' b'$. Άρα $(a_1 b_1)(a_2 b_2) =$
$= a_1 (b_1 a_2) b_2 = a_1 a' b' b_2 \in A \cdot B = H$. Έστω τώρα $a b \in H$. Τότε
$(ab)^{-1} = b^{-1} a^{-1} \in BA = AB = H$. Συμφωνα με την πρόταση 1.18
συμπεραίνουμε λοιπόν ότι η H είναι υποομάδα της G.
Αντίστροφα, έστω ότι η H είναι υποομάδα της G. Έστω ότι
τα $a \in A$ και $b \in A$ είναι τυχόντα. Τότε $a^{-1} b^{-1} \in H$, άρα $(a^{-1} b^{-1})^{-1} \in H$,
δηλαδή και $b a \in H$. Δηλαδή $B \cdot A \subseteq H = AB$. Τότε, για οποια-
δήποτε $a \in A$, $b \in B$ θα είναι $b^{-1} a^{-1} \in AB$, δηλ $b^{-1} a^{-1} = a' b'$ με
$a' \in A$ και $b' \in B$. Συνεπώς, $ab = (b^{-1} a^{-1})^{-1} = (a' b')^{-1} = b'^{-1} a'^{-1} \in BA$,

Συμπλήρωση στο Θεώρημα 5.2:

(γ) Έστω η σχέση $\sim$, η οποία ορίζεται στα στοιχεία του G ως εξής: $x \sim y \Leftrightarrow \exists\, a \in A, \exists\, b \in B : y = axb$

Δείξτε (i) Η σχέση $\sim$ είναι ισοδυναμία

(ii) Αν τα A, B είναι πεπερασμένα, τότε ο πληθάριθμος της πλάσεως ισοδυναμίας $[x]$ του $x \in G$, δίνεται από την σχέση

$$|[x]| = \frac{|A||B|}{|A \cap xBx^{-1}|}$$

Απόδειξη των (γ): Το (i) είναι γεγραμμένο

(ii) Προφανώς $[x] = AxB = \{axb \mid a \in A, b \in B\}$

Επίσης, για τυχόν υποσύνολο S του G και τυχόντα $g_1, g_2 \in G$ ισχύει $|S| = |g_1 S g_2|$. Άρα,

$$|[x]| = |AxB| = |(AxB)x^{-1}| = |A \cdot (xBx^{-1})|$$

Εφαρμόζοντας το (β) για τις υποομάδες A και xBx^{-1}, έχουμε

$$|[x]| = |A \cdot (xBx^{-1})| = \frac{|A||xBx^{-1}|}{|A \cap xBx^{-1}|} = \frac{|A||B|}{|A \cap xBx^{-1}|},$$

που σημαίνει ότι, επίσης, $AB \subseteq BA$, δ' ε' δ.

β) Προφανώς το σύνολο $D = A \cap B$ είναι υποομάδα της A, καθώς και της B. Έστω ότι $Db_1, \ldots, Db_n$ είναι όλες οι διαφορετικές δεξιές κλάσεις της B ως προς την υποομάδα της D. Τότε, εξ ορισμού, $n = [B:D]$ άρα $n = |B|/|D|$ (βλ. (3.3)). Λόγω της σχέσης $B = Db_1 \cup \ldots \cup Db_n$, όπότε είναι πολύ εύκολο να δει κανείς ότι $AB = (AD)b_1 \cup \ldots \cup (AD)b_n$. Αλλά η D είναι υποομάδα της A, άρα $AD = A$ (γιατί;). Συνεπώς

$$AB = Ab_1 \cup \ldots \cup Ab_n \qquad (5.4)$$

Αν είχαμε $Ab_i = Ab_j$ με $i \neq j$, τότε $b_i b_j^{-1} \in A$ και, λόγω της $b_i b_j^{-1} \in B$, θα προέκυπτε $b_i b_j^{-1} \in D$, δηλαδή $Db_i = Db_j$, γεγονός που αντιφάσκει με την υπόθεσή μας. Άρα οι κλάσεις στο δεξιό μέλος της (5.4) είναι διαφορετικές και, συνεπώς, ξένες. Επιπλέον, όλες έχουν τον ίδιο πληθάριθμο, δηλαδή ίσούται με $|A|$. Άρα η (5.4) συνεπάγεται ότι $|AB| = n|A| = \frac{|B|}{|D|}\cdot|A|$, δ' ε' δ.

□

Δράση ομάδας επί συνόλου. Μια ομάδα $(G, \cdot)$ λέμε ότι (5.5) δρα επί του (μη κενού) συνόλου $\mathcal{P}$ αν υπάρχει μια απεικόνιση $\phi : \mathcal{P} \times G \longrightarrow \mathcal{P}$ με τις εξής ιδιότητες:

i) $\phi(A, \varepsilon) = A \quad \forall A \in \mathcal{P}$

ii) $\phi(A, x_1 x_2) = \phi(\phi(A, x_1), x_2) \quad \forall x_1, x_2 \in G$ & $\forall A \in \mathcal{P}$

Δεν έχει απαραίτητα

Συχνά αντί του $\phi(A, x)$ γράφαμε A^x, όπότε οι (i) και (ii) ισοδυναμούν, αντιστοίχως, με τις

(i)' $A^\varepsilon = A \quad \forall A \in \mathcal{P}$, (ii)' $A^{x_1 x_2} = (A^{x_2})^{x_1} \quad \forall x_1, x_2 \in G$ & $\forall A \in \mathcal{P}$

Το σύνολο που ορίζεται για κάθε $A \in \mathcal{P}$ ως εξής,

$$A^G = \{ A^x \in \mathcal{P} \mid x \in G \}$$

λέγεται τροχιά του x (υπό τη δράση της G).

Τα κατά σύνολον δύο στοιχεία του $\mathcal{P}$ στην ίδια τροχιά, είναι σχέση ισοδυναμίας με αντίστοιχο σύνολο-πηλίκο το σύνολο όλων των τροχιών. Ειδικώτερα, αν το $\mathcal{P}$ είναι πεπε-

Στοιχεία τροχιών

ραμένα σύνολα, τότε υπάρχουν $A_1, \dots, A_n \in \mathcal{P}$, τέτοια ώστε οι τροχιές $A_1^G, \dots, A_n^G$ να είναι όλες οι δυνατές διαφορετικές τροχιές ως προς τη G, τότε

$$|\mathcal{P}| = |A_1^G| + \dots + |A_n^G|.$$

(Λόγου, γενικά, για ένα πεπερασμένο σύνολο A, $|A|$ είναι ο πληθάριθμος του A). Επίσης ορίζουμε για κάθε $A \in \mathcal{P}$

$$N_G(A) = \{x \in G : A^x = A\}$$

και είναι απλή άσκηση να δείξει κανείς ότι το σύνολο $N_G(A)$ είναι υποομάδα της G. Ας εξετάσουμε τώρα και διαφορετικά στοιχεία της τροχιάς του A: Είναι $A^x = A^y \Leftrightarrow A^{yx^{-1}} = A \Leftrightarrow yx^{-1} \in N_G(A) \Leftrightarrow xN_G(A) = yN_G(A)$. Άρα τα στοιχεία της τροχιάς του A έρχονται σε 1-1 και επί αντιστοιχία με τις αριστερές πλευρές της G ως προς $N_G(A)$. Αυτό σημαίνει, ειδικώτερα, ότι αν $[G : N_G(A)] < \infty$, τότε

$$|A^G| = [G : N_G(A)] \tag{5.6}$$

και, ειδικώτερα:

Αν η G είναι πεπερασμένη, η $|A^G|$ είναι διαιρέτης του $|G|$.

Δεν είναι

Λήμμα (5.7) Αν $(A, \cdot)$ είναι πεπερασμένη αβελιανή ομάδα, της οποίας η τάξη διαιρείται από τον πρώτο p, τότε η A περιέχει ένα στοιχείο τάξης p.

Απόδειξη. Θέτουμε $|A| = n \cdot p$, όπου $n \geq 1$. Θ' αποδείξουμε το λήμμα με επαγωγή επί του n. Αν $n = 1$, τότε ο ισχυρισμός είναι φανερός (άσκηση 3.4). Έστω τώρα ότι $n > 1$ και το λήμμα ισχύει για όλες τις αβελιανές ομάδες τάξης kp με $1 \leq k < n$. Θεωρούμε μια maximal γνήσια υποομάδα της A. Δηλαδή μια υποομάδα M της A, τέτοια ώστε $M \neq G$ και δεν υπάρχει καμία υποομάδα H της A με την ιδιότητα $M \subsetneq H \subsetneq A$. Είναι $|M| < |A| = np$. Συνεπώς, αν $p \mid |M|$, τότε $|M| = kp$ με $k < n$, οπότε από την επαγωγική υπόθεση η M (άρα και η A) έχει ένα στοιχείο τάξης p. Αν $p \nmid |M|$, τότε θεωρούμε ένα $a \in A - M$. Επειδή η A είναι αβελιανή, το θεώρημα 5.2(α) λέει ότι το σύνολο $M \cdot \langle a \rangle$ είναι υποομάδα της A. Αυτή η υποομάδα περιέχει γνησίως

τη M (αφού περιέχει τό a, πού δέν ανήκει στη M), άρα, λόγω του ότι η M είναι maximal, θα ταυτίζεται με την A. Λόγω και του (5.2)β τότε, $|A| = |M \cdot \langle a \rangle| = |M| \cdot |\langle a \rangle| / |M \cap \langle a \rangle|$. Επειδή $p \mid |A|$ θα πρέπει τότε $p \mid |M| \cdot |\langle a \rangle|$. Όμως $p \nmid |M|$, άρα $p \mid |\langle a \rangle|$. Δηλαδή ο p διαιρεί την τάξη, έστω r, του a. Τότε, από τό θεώρημα 3.6 τό στοιχείο $a^{r/p}$ έχει τάξη p, ό.έ.δ.

□

(5.8) <u>1ο Θεώρημα του Sylow</u>: Έστω G μιά πεπερασμένη ομάδα τάξεως $p^m r$, όπου ο p είναι πρώτος, ο m είναι μή αρνητικός ακέραιος και $p \nmid r$. Τότε η G έχει τουλάχιστον μία υποομάδα τάξεως p^m.

Απόδειξη: Αν $p^m r = 1$, τό θεώρημα είναι τετριμμένο. Έστω $p^m r > 1$ και υποθέτουμε ότι τό θεώρημα ισχύει για όλες τις ομάδες των οποίων η τάξη είναι $< p^m r$ (επαγωγική υπόθεση). Αν $m = 0$, τό θεώρημα είναι τετριμμένο. Έστω τώρα ότι $m \geq 1$. Θα χρησιμοποιήσουμε συμβολισμούς και αποτελέσματα των (3.10)-(3.14):

Έστω $\{1\} = (a_1), (a_2), \ldots, (a_k)$ όλες οι κλάσεις συζυγίας της G και $|(a_i)| = \nu_i$ $(\nu_i > 1)$. Έστω $C(a_i)$ τό κέντρο του a_i και ας θέσουμε $|C(a_i)| = n_i$. Από τό (3.11) ξέρουμε ότι $\nu_i = |G|/n_i = p^m r / n_i$. Αφ' ετέρου, η εξίσωση κλάσεων της G είναι

$$p^m r = 1 + \nu_2 + \ldots + \nu_k$$

Ας υποθέσουμε πρώτα ότι κάποιο ν_i είναι > 1 και όχι διαιρετό από τό p. Τότε, λόγω της $\nu_i n_i = p^m r$, θα πρέπει $p^m \| n_i$,* ενώ $n_i < p^m r$. Άρα η επαγωγική υπόθεση ισχύει για την ομάδα $C(a_i)$, όπότε υπάρχει υποομάδα της $C(a_i)$ (άρα και της G) τάξεως p^m.

Στην συνέχεια, λοιπόν, υποθέτουμε ότι κάθε ν_i ή ίσούται με 1 ή διαιρείται διά p. Αν z είναι τό πλήθος εκείνων των ν_i για τα οποία $\nu_i = 1$, τότε η εξίσωση κλάσεων της G γίνεται

$$p^m r = z + q \cdot p \,, \quad q, z \text{ θετικοί ακέραιοι.}$$

Όμως $\nu_i = 1 \iff (a_i) = \{a_i\} \iff a_i \in Z$ (= κέντρο της G), λόγω του 3.14. Έχουμε $|Z| = z$ = πολλαπλάσιο του p και έπειτα

* $p^m \| n$ σημαίνει, γενικά, $p^m \mid n$ και $p^{m+1} \nmid n$.

δή ή Z είναι αβελιανή ὁμάδα, τό λῆμμα 5.7 λέει ὅτι περιέχει ἕνα στοιχεῖο τάξης p. Ἔστω P ἡ ὁμάδα πού παράγει αὐτό τό στοιχεῖο. Τότε $|P|=p$ καί $P \lhd G$, ἀφοῦ $P \subseteq Z$. Τότε ἡ ὁμάδα G/P ἔχει τάξη $p^m r/p = p^{m-1} r$ ἄρα, ἀπ' τήν ἐπαγωγική ὑπόθεση, θά περιέχει μιά ὑποομάδα S/P τάξης p^{m-1}. Ἡ S τότε εἶναι ὑποομάδα τῆς G καί ἡ τάξη της εἶναι $|S| = |S/P| \cdot |P| = p^{m-1} \cdot p = p^m$, ὅ.ἔ.δ.

□

Ὁρισμός Ἔστω G μιά ὁμάδα ἴσως ἀπό (5.8). Κάθε ὑποομάδα (5.9) τῆς τάξεως p^m (τουλάχιστον μία τέτοια ὑπάρχει, λόγω τοῦ 5.8) λέγεται p-ὁμάδα Sylow τῆς G.

Πρίν προχωρήσουμε στό δεύτερο θεώρημα τοῦ Sylow κάνουμε ὁρισμένες προκαταρκτικές παρατηρήσεις: Ἄν ἡ $(G, \cdot)$ εἶναι ὁμάδα καί $H \leq G$, τότε γιά τυχόν $x \in G$, τό xHx^{-1} εἶναι ὑποομάδα τῆς G. Οἱ ὑποομάδες H καί xHx^{-1} χαρακτηρίζονται συζυγεῖς. Δηλαδή, οἱ ὑποομάδες H καί K τῆς G λέγονται συζυγεῖς, ἄν ὑπάρχει $x \in G$ τ.ὥ. $K = xHx^{-1}$. Ἡ σχέση συζυγίας μεταξύ τῶν ὑποομάδων τῆς G εἶναι ἰσοδυναμία (εὔκολο). (5.10)

2ο Θεώρημα τοῦ Sylow Ὅλες οἱ p-ὁμάδες Sylow τῆς G εἶναι συζυγεῖς. (5.11)

Ἀπόδειξη Ἔστω $|G| = p^m r$, $m \geq 0$, $p \nmid r$. Γιά $m=0$ τό θεώρημα εἶναι τετριμμένο. Ἔστω, λοιπόν, $m \geq 1$ καί A, B δύο p-ὁμάδες Sylow τῆς G. Θεωροῦμε τήν ἰσοδυναμία $\sim$ καί Θεωρήματος 5.2 (γ) καί ἔστω ὅτι $[x_1], \ldots, [x_\nu]$ εἶναι ὅλες οἱ διαφορετικές κλάσεις ἰσοδυναμίας, ὁπότε

$$p^m r = |G| = |[x_1]| + \cdots + |[x_\nu]|. \quad (*)$$

Γιά κάθε $i = 1, \ldots, \nu$ εἶναι, βάσει τοῦ 5.2 (γ)(ii), $|[x_i]| = p^{2m - \alpha_i}$, ὅπου $p^{\alpha_i} = |A \cap (x_i B x_i^{-1})|$ καί, συνεπῶς $\alpha_i \leq m$. Γιά $\alpha_i < m$ εἶναι $|[x_i]| = p^{2m-\alpha_i} \equiv 0 \pmod{p^{m+1}}$. Ὅμως, λόγω τῆς $(*)$, εἶναι ἀδύνατον ὅλοι οἱ ἀριθμοί $|[x_i]|$ νά εἶναι διαιρετοί διά p^{m+1},

ἄρα ὑπάρχει i τ.ώ. $\alpha_i = m$. Αὐτό σημαίνει ὅτι $|A \cap (x_i B x_i^{-1})| = p^m = |A|$, ἄρα $A \cap (x_i B x_i^{-1}) = A$, δηλαδή $A \subseteq x_i B x_i^{-1}$. Τά δύο σύνολα δεξιά καί ἀριστερά τοῦ $\subseteq$ ἔχουν τόν ἴδιο πληθάριθμο, συνεπῶς, $A = x_i B x_i^{-1}$, δηλ. οἱ ὑποομάδες A καί B εἶναι συζυγεῖς. □

3ο Θεώρημα τοῦ Sylow. Τό πλῆθος τῶν p-ὁμάδων Sylow μιᾶς ὁμάδας εἶναι $\equiv 1 \pmod p$ καί διαιρεῖ τήν τάξη τῆς ὁμάδας. (5.12)

Ἀπόδειξη. Ἔστω $(G, \cdot)$ μ' ὁμάδα, $|G| = p^m \cdot r$, $m \geq 0$, $p \nmid r$. Ἄν $m = 0$, τό θεώρημα εἶναι τετριμμένο, ὁπότε ἄς ὑποθέσωμε $m \geq 1$. Ἔστω P μία p-ὁμάδα Sylow τῆς G (ὑπάρχει λόγῳ τοῦ (5.2)). Ὅλες οἱ p-ὁμάδες Sylow τῆς G εἶναι συζυγεῖς τῆς P (λόγῳ τοῦ (5.11)) καί ἔστω k τό πλῆθος τους. Ὁρίζομε τόν κανονικοποιητή $N(P)$ τῆς P: $N(P) = \{x \in G \mid xP = Px\}$· εἶναι ὑποομάδα τῆς G κι ἄς θεωρήσωμε τίς ἀριστερές πλευρικές κλάσεις τῆς G ὡς πρός τόν $N(P)$. Εἶναι $xN(P) = yN(P) \Leftrightarrow y^{-1}x \in N(P) \Leftrightarrow y^{-1}xN(P) = N(P)y^{-1}x \Leftrightarrow xPx^{-1} = yPy^{-1}$. Συνεπῶς, οἱ διαφορετικές ἀριστερές κλάσεις εἶναι τόσες ὅσες καί οἱ ὑποομάδες αἱ συζυγεῖς πρός τόν P. Ἄρα $|G|/|N(P)| = |G/N(P)| = k$ (*), ἄρα $k \mid |G|$ καί ἀποδείξαμε τό δεύτερο ἰσχυρισμό τοῦ θεωρήματος. Τώρα θεωροῦμε τόν ἰσοδυναμία $\sim$ τοῦ θεωρήματος 5.2(γ') μ' $A = B = P$ καί ἔστω ὅτι $[x_1], \ldots, [x_\nu]$ εἶναι ὅλες οἱ κλάσεις ἰσοδυναμίας. Τότε $G = [x_1] \cup \ldots \cup [x_\nu]$ (**). Ἰσχυρισμός: Ὑπάρχουν $i_1, \ldots, i_\mu \in \{1, \ldots, \nu\}$ ἔτσι ὥστε $N(P) = [x_{i_1}] \cup \ldots \cup [x_{i_\mu}]$ (#). Αὐτό εἶναι ἄμεση συνέπεια τοῦ ὅτι, ἄν $[x] \cap N(P) \neq \emptyset$, τότε $[x] \subseteq N(P)$ (δηλαδή ἀτακτο). Λόγῳ τῶν (**) & (#) ἔχομε $|G| = |N(P)| + \sum_{i \notin \{i_1, \ldots, i_\mu\}} |[x_i]|$ ($). Ἄν $i \notin \{i_1, \ldots, i_\mu\}$, τό $[x_i]$ εἶναι ξένη πρός τήν ὑποομάδα $N(P)$, ἄρα $x_i \notin N(P)$, δηλ. $x_i P x_i^{-1} \nsubseteq P$. Ἔπεται ὅτι $|P \cap (x_i P x_i^{-1})| = p^{\alpha_i}$, $\alpha_i < m$, ἄρα (βλ. (5.2)(γ)(ii)) $|[x_i]| = p^{2m - \alpha_i} \equiv 0 \pmod{p^{m+1}}$. Ἔτσι, ἀπό τήν ($), $|G| = |N(P)| + a \cdot p^{m+1}$, $a \in \mathbb{Z}$, $a \geq 0$. Ἀλλά $p^m \| |G|$, ἄρα, τέλος

τελευταία ἰσότητα συνεπάγεται $p^{m+1} \| |N(P)|$. Ἡ ἴδια ἰσότητα καὶ ἡ (*) δίνουν $k = 1 + a \cdot p^{m+1} / |N(P)|$, ἀρά τὸ τελευταῖο πλάϊσμα εἶναι ἀκέραιος καὶ, μάλιστα, διαιρετὸς διὰ p. □

Θεώρημα. Ἂν ἡ ὁμάδα G ἔχει τάξη pq, ὅπου p, q εἶναι πρῶτοι, $p < q$ καὶ $q \not\equiv 1 (\mathrm{mod}\, p)$, τότε ἡ G εἶναι ἀβελιανή. (5.13)

Ἀπόδειξη. Ἔστω r τὸ πλῆθος τῶν p-ὁμάδων Sylow τῆς G. Τότε, ἀπὸ τὸ (5.12), $r = 1 + kp$ καὶ $r \mid pq$. Οἱ δύο σχέσεις μαζὶ συνεπάγονται τὴν $r \mid q$, ὁπότε $r = 1$ ἢ q. Τὸ δεύτερο ἐνδεχόμενο δὲν συμβαίνει, ἀφοῦ θὰ εἴχαμε $q \equiv 1 (\mathrm{mod}\, p)$, πού ἀποκλείεται ἀπὸ τὴν ὑπόθεση. Ἄρα $r = 1$, πού σημαίνει (ἄσκηση 1) ὅτι ἡ G ἔχει μία ἀκριβῶς ὑποομάδα P τάξεως p, ἡ ὁποία εἶναι κανονική. Προφανῶς ἡ P εἶναι κυκλική καὶ ἔστω $P = \langle a \rangle$. Ἔτσι λοιπὸν δείξαμε ὅτι

$$P = \langle a \rangle, \ |P| = p \ \text{καὶ} \ P \lhd G. \tag{5.14}$$

Ἔστω τώρα s τὸ πλῆθος τῶν q-ὁμάδων Sylow τῆς G. Τότε, πάλι, $s = 1 + lq$ καὶ $s \mid pq$, οἱ ὁποῖες συνεπάγονται ὅτι $s \mid p$. Ἂν ἦταν $l \geq 1$, τότε $s \geq 1 + q > p$, πού ἀντιβαίνει στὴν $s \mid p$. Συνεπῶς $l = 0$ καὶ $s = 1$. Ὅπως καὶ πρίν αὐτὸ σημαίνει ὅτι ὑπάρχει μιὰ κυκλικὴ ὑποομάδα Q τῆς G, τέτοια ὥστε

$$Q = \langle b \rangle, \ |Q| = q \ \text{καὶ} \ Q \lhd G. \tag{5.15}$$

Ἔστω $d = |P \cap Q|$. Τότε, ἐπειδὴ ἡ $P \cap Q$ εἶναι ὑποομάδα καὶ τῆς P καὶ τῆς Q, θὰ πρέπει $d \mid p$ καὶ $d \mid q$, ἄρα $d = 1$. Δηλαδὴ $P \cap Q = \{1\}$, πού σὲ συνδυασμὸ μὲ τὶς (5.14), (5.15) καὶ τὴν ἄσκηση 4, δίνει

$$ab = ba. \tag{5.16}$$

Ἂς θεωρήσουμε τὰ στοιχεῖα

$$a^i b^j \qquad 0 \leq i \leq p-1, \quad 0 \leq j \leq q-1 \tag{5.17}$$

Αὐτὰ εἶναι ἀκριβῶς διαφορετικά, λόγῳ τῶν (5.14), (5.15) καὶ τῆς $P \cap Q = \{1\}$ καὶ τὸ πλῆθος τους εἶναι $p \cdot q$. Ἄρα αὐτὰ εἶναι, ἀκριβῶς, ὅλα τὰ στοιχεῖα τῆς G. Τώρα, λόγῳ τῆς (5.16), δύο ὁποιαδήποτε στοιχεῖα τῆς μορφῆς (5.17) ἀνταλλάσσονται, ἄρα ἡ G εἶναι ἀβελιανή.

□

Ασκήσεις του Κεφαλαίου 5.

1) Έστω P μία p-ύμάδα Sylow της πεπερασμένης ύμάδας G. Δείξτε ότι η P είναι μοναδική p-ύμάδα Sylow αν και μόνο αν $P \trianglelefteq G$.

2) Δείξτε ότι δεν υπάρχει απλή ύμάδα τάξεως 200.

3) Δείξτε ότι δεν υπάρχει απλή ύμάδα τάξεως 30, ή τάξεως 56.

4) Αν $A \trianglelefteq G$ και $B \trianglelefteq G$ και $A \cap B = \{1\}$, τότε για οποιαδήποτε $a \in A$ και $b \in B$ ισχύει $ab = ba$.
(Υπόδειξη: Θεωρήστε το στοιχείο $c = a^{-1}b^{-1}ab$ και αποδείξτε ότι $c \in A \cap B$.).

5) Αποδείξτε ότι κάθε ύμάδα τάξεως 45 έχει κανονική υποομάδα τάξεως 9.

6) Πόσα στοιχεία τάξεως 7 βρίσκονται σε μία ύμάδα τάξεως 168;

7) Κάθε ύμάδα τάξεως 35^3 έχει κανονική υποομάδα τάξεως 125.

8) Δείξτε ότι δεν υπάρχουν απλές ύμάδες τάξεως 148.

9) Δείξτε ότι δεν υπάρχει απλή ύμάδα τάξεως $8p^k$ (p περιττός πρώτος, $k \neq 1$). (Υπόδειξη: Δείξτε πρώτα ότι αν υπάρχει απλή ύμάδα τάξεως $8p^k$ τότε $p = 3$ ή 7. Χρησιμοποιείστε το γεγονός ότι οι ύμάδες τάξεως 8, 24 και 56 δεν είναι απλές).

Το τέχνασμα του Poincaré

Αν η $(G,\cdot)$ είναι ομάδα και $H \leq G$ με $[G:H] = p$, τότε υπάρχει ομομορφισμός $\phi: G \longrightarrow S_p$ τ.ώ. $\ker\phi \leq H$

Πραγματι ο ϕ ορίζεται ως εξης: Εστω $H, a_2H, \dots, a_pH$ όλες οι διαφορετικές αριστερές πλευρικές κλάσεις modulo H. Τότε

$$G \ni x \longmapsto \phi(x) = \sigma_x := \begin{pmatrix} H & a_2H & \cdots & a_pH \\ xH & xa_2H & \cdots & xa_pH \end{pmatrix} \in S_p$$

(προφανώς, ομομορφισμός).

Αν $x \in \ker\phi$, τότε $\sigma_x = id$ άρα, ειδικώτερα $xH = H$ άρα $x \in H$, δηλαδή $\ker\phi \leq H$.

Ασκήσεις που λύνονται με το τέχνασμα του Poincaré

1) Αν μια απλή ομάδα A περιέχει υποομάδα με δείκτη $p > 1$, τότε η A έχει ένα ισόμορφο αντίγραφο της μέσα στην S_p.

2) Αποδείξτε ότι η A_6 δεν έχει υποομάδα με 72 στοιχεία.

3) Αν η G είναι ομάδα περιττής τάξεως και η υποομάδα της H έχει δείκτη 3, τότε $H \trianglelefteq G$.

4) Αν η τάξη της ομάδας G είναι $p \cdot m$, όπου p πρώτος και $m < p$, τότε η G έχει κανονική υποομάδα τάξεως p.

5) Αν η τάξη της ομάδας G είναι p^ν, όπου p πρώτος $> \nu \geq 1$, τότε κάθε υποομάδα της G τάξεως $p^{\nu-1}$ είναι κανονική.

6) Δείξτε ότι δεν υπάρχει απλή ομάδα με 24 στοιχεία.

1) $\phi : A \longrightarrow S_\phi \quad \phi(x) = \sigma_x = \begin{pmatrix} H & a_2H & \cdots & a_\nu H \\ xH & xa_2H & \cdots & xa_\nu H \end{pmatrix}$

$H \leq A$

$x \in \ker\phi \Rightarrow \sigma_x = id \Rightarrow xH = H \Rightarrow x \in H$ άρα $\ker\phi \leq H$

Αφ' ετέρου, $\ker\phi \trianglelefteq A$ κι A απλή άρα $\ker\phi = \{1\}$ ή $\ker\phi = A$

(Η 2η περίπτωση δεν συνεπάγεται $A \leq H$ άρα $H = A$, άρα $p = 1$, άτοπο

(Η 1η περίπτωση συνεπάγεται ότι η ϕ είναι μονομορφισμός, άρα

$\phi(A)$ είναι ισόμορφο αντίγραφο της A μέσα στην S_ν

2) Έστω $H \leq A_6$, $|H| = 72$. Τότε $[A_6 : H] = 360 : 72 = 5$, άρα,

σύμφωνα με την (1) η A_6 έχει ισόμορφο αντίγραφο μέσα στην

S_5, άτοπο διότι $|A_6| = 360$, ενώ $|S_5| = 120$

3) $H \leq G$, $[G : H] = 3$, $|G| \equiv 1 \pmod 2$

$\phi : G \longrightarrow S_3$, $\phi(g) = \sigma_g = \begin{pmatrix} H & a_2H & a_3H \\ gH & ga_2H & ga_3H \end{pmatrix}$

Όπως στην (1), $\ker\phi \leq H$. Επίσης $\mathrm{Im}\phi \cong G/\ker\phi$

Επομ. $|\mathrm{Im}\phi| = \frac{|G|}{|\ker\phi|} = \frac{|G|}{|H|} \cdot \left|\frac{H}{\ker\phi}\right| =$ περιττ. 3. Όμως $\mathrm{Im}\phi \leq S_3$ και

$|S_3| = 6$, δηλ. $\mathrm{Im}\phi = 3$ ή 6. Το 2ο ενδεχόμενο δεν συνεπάγεται

$|G| = |\ker\phi| \cdot 6$, άτοπο διότι $|G|$ περιττός. Άρα $|\mathrm{Im}\phi| = 3$,

που σημαίνει $\left|\frac{H}{\ker\phi}\right| = 1$ δηλ. $H = \ker\phi \trianglelefteq G$

4) Απόδειξη δίχως χρήση του 3ου Θ. Sylow:

Έστω H η p-Sylow δομάδα της G, $[G : H] = \nu$

$\phi : G \longrightarrow S_\nu$, $\phi(g) = \sigma_g = \begin{pmatrix} H & a_2H & \cdots & a_\nu H \\ gH & ga_2H & \cdots & ga_\nu H \end{pmatrix}$, $\ker\phi \leq H$

$\mathrm{Im}\phi \cong G/\ker\phi$, άρα $|\mathrm{Im}\phi| = \frac{p^\nu}{|\ker\phi|}$, $p^\nu = |\mathrm{Im}\phi| \cdot |\ker\phi|$.

Όμως $|\mathrm{Im}\phi| \mid |S_\nu| = \nu!$ άρα $(|\mathrm{Im}\phi|, p) = 1$, δηλ. $p \nmid |\ker\phi|$

Αφ' ετέρου $|\ker\phi| \leq |H| = p$, άρα $|\ker\phi| = p$, άρα $H = \ker\phi \trianglelefteq G$.

Απόδειξη με χρήση του 3ου Θ. Sylow Έστω H η p-Sylow δομάδα της G. Αρκεί

να δείξω ότι είναι η μοναδική. Το πλήθος των p-Sylow της G, έστω r.

Τότε $r \equiv 1 \pmod p$ κι $r \mid |G| = \nu p$. Αλλά η 1η σχέση $\Rightarrow (r, p) = 1$, άρα

$r \mid \nu$. Αν ήταν $r > 1$, τότε θα ήταν $r \geq 1 + p$ δηλ. θα έπρεπε $1 + p \mid \nu$,

άτοπο

5) $|G|=p^\nu$, $|H|=p^{\nu-1}$, $[G:H]=p$

$\phi: G \longrightarrow S_p$; $\phi(g)=\sigma_j=\begin{pmatrix} H & a_2H & \cdots & a_pH \\ gH & ga_2H & \cdots & ga_pH \end{pmatrix}$

$\ker\phi \leq H$, $\mathrm{Im}\phi \cong G/\ker\phi$

$|\mathrm{Im}\phi| = \frac{|G|}{|\ker\phi|} = \frac{|G|}{|H|}\cdot\frac{|H|}{|\ker\phi|}$ ... Λόγω των $\ker\phi \leq H$ $|H|=p^{\nu-1}$, έπεται ότι $|\ker\phi|=p^\alpha$, $0\leq\alpha\leq\nu-1$

Άν $\alpha<\nu-1$, τότε $\frac{|H|}{|\ker\phi|} \equiv 0 \pmod p$, δηλαδή $|\mathrm{Im}\phi|=p^2$, άτοπο

διότι $\mathrm{Im}\phi \leq S_p$ & $p^2 \nmid |S_p|$ Άρα $|\ker\phi|=p^{\nu-1}=|H|$, δηλαδή

$H=\ker\phi \trianglelefteq G$

6) Έστω $|A|=24$ και H η 2-δράση Sylow της A, δηλαδή $|H|=8$ και $[A:H]=3$. Λόγω της (1) η A έχει πολύφορφο αντίγραφο της φτιάσα στην S_3, άτοπο αφού $|A|=24$ και $|S_3|=6$.

§4. Αβελιανές ομάδες (Συμπληρώσεις Σ.Κ. Πηχωρίδη)

(4.1) Στην παράγραφο αυτή θα χρησιμοποιήσουμε ένα πολύ σημαντικό θεώρημα, το οποίο θα περιγράψουμε με τον εξής ισοδύναμο τρόπο τις Αβελιανές ομάδες G με τάξη ένα φυσικό αριθμό n. Το θεώρημα χαρακτηρίζει διάφορες χαρακτηριστικές (θα αναφέρουμε δύο από αυτές) και είναι πολύ χρήσιμο και πέρασε της θεωρίας των ομάδων (π.χ. στην Αλγεβρική Τοπολογία). Για την καταανόηση αυτών που θα ακολουθούν συνιστάται στον αναγνώστη να επαναλάβει τα δύο §§ μας μέχρι τώρα για κυκλικές ομάδες και αβελιανές.

Το κεντρικό θεώρημα είναι το επόμενο "Θεώρημα δομής για Αβελιανές ομάδες":

Θεώρημα Α. *Κάθε πεπερασμένη Αβελιανή ομάδα ισούται με το ευθύ άθροισμα κυκλικών υποομάδων της.*

Πριν προχωρήσουμε στην απόδειξη θα κάνουμε μερικές παρατηρήσεις και σχόλια.

i) Στην περίπτωση που η τάξη της ομάδας G είναι ένας πρώτος αριθμός, τότε η κατάσταση είναι πολύ απλή. Η ομάδα G είναι κυκλική και ισόμορφη με την $\mathbb{Z}_n$, $n = |G|$.

ii) Κάθε κάθε κυκλική ομάδα είναι ισόμορφη με μία ομάδα της μορφής $\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_k}$, με $n_1, n_2, \ldots, n_k \in \mathbb{N}$, (η $\mathbb{Z}$, αν η ομάδα είναι άπειρη) το θεώρημα Α συνεπάγεται ότι οι ομάδες της μορφής $\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_k}$, $n_1, n_2, \ldots, n_k \in \mathbb{N}$, εξαντλούν τις πεπερασμένες Αβελιανές ομάδες (δηλ. κάθε πεπερασμένη Αβελιανή ομάδα είναι ισόμορφη με μία ομάδα της παραπάνω μορφής).

iii) Είναι δυνατόν η "αριθμητική" απόδειξη ότι η παραπάνω μία Αβελιανή πεπερασμένη ομάδες είναι

αυτό άθροισμα κυκλικών είναι μοναδικό". Σαν αντιπαράδειγμα πάρτε την $\mathbb{Z}_{30}$ η οποία "ισούται" με $\mathbb{Z}_{15}+\mathbb{Z}_2$ και με $\mathbb{Z}_5+\mathbb{Z}_6$ ("ισούται" εδώ σημαίνει "είναι ισόμορφη με"). Αυτό είναι εύκολο να το ελέγξουμε, αλλά είναι ακόμη καλλίτερα να δείξουμε ένα γενικότερο και απλό αποτέλεσμα.

<u>Πρόταση Β</u>. "$\mathbb{Z}_m+\mathbb{Z}_n \cong \mathbb{Z}_{mn}$ αν και μόνο αν $(m,n)=1$"

(Η απόδειξη είναι εύκολη. Αν $(m,n)=1$ τότε το στοιχείο $(1,1)$ της $\mathbb{Z}_m+\mathbb{Z}_n$ έχει τάξη mn, διότι $\lambda(1,1)=(\lambda,\lambda)=(0,0)$ συνεπάγεται $m|\lambda$ και $n|\lambda$. Αν τώρα $(m,n)=d>1$, τότε $[m,n]=\frac{mn}{(m,n)}<mn$ και κάθε στοιχείο της $\mathbb{Z}_m+\mathbb{Z}_n$ έχει τάξη $\leq [m,n]$ άρα δεν υπάρχει στοιχείο με τάξη mn.

Εδώ χρησιμοποιούμε το συμβολισμό <u>λa αντί a^λ, $\lambda\in\mathbb{Z}$, $a\in G$</u>, το οποίο και θα κάνουμε συστηματικά για Αβελιανές ομάδες G.

<u>iv)</u> Ένα πρώτο βήμα για την απόδειξη του θεωρήματος Α είναι η εξής ενδιαφέρουσα πρόταση.

<u>Πρόταση Γ</u>. <u>Κάθε πεπερασμένη Αβελιανή ομάδα ισούται με το ευθύ άθροισμα των Sylow υποομάδων της.</u>

<u>Απόδειξη</u>. Ας είναι $|G|=p_1^{m_1}p_2^{m_2}\cdots p_k^{m_k}$ η ανάλυση του $|G|$ σε πρώτους παράγοντες. Επειδή η G είναι Αβελιανή οι Sylow υποομάδες της θα είναι κανονικές. Και επομένως θα υπάρχουν ακριβώς k Sylow υποομάδες, τάξεων $p_1^{m_1}, p_2^{m_2},\dots,p_k^{m_k}$ αντίστοιχα. Ας ονομάσουμε $P_1,P_2,\dots,P_k$ αυτές τις υποομάδες. Πρέπει να δείξουμε ότι $G=P_1\oplus P_2\oplus\cdots\oplus P_k$, δηλ. (α) $G=P_1P_2\cdots P_k$ και (β) για κάθε $g\in G$ η παράσταση $g=g_1g_2\cdots g_k$ με $g_1\in P_1,\dots,g_k\in P_k$ είναι μοναδική.
Το θεώρημα της σελίδας 44 των σημειώσεων δείχνει εύκολα ότι αν ισχύει το (β) τότε η υποομάδα $P_1P_2\cdots P_k$ της G έχει $|P_1\cdots P_k|=|P_1|\cdots|P_k|=|G|$ στοι-

γεία καὶ ἐπομένως ἰσχύει τὸ (i). Ἀρκεῖ λοιπὸν νὰ δείξουμε τὸ (ii). Ἂς ὑποθέσουμε ὅτι ἔχουμε $g = g_1 g_2 \cdots g_k = g_1' g_2' \cdots g_k'$ μὲ $g_1, g_1' \in P_1, \ldots, g_k, g_k' \in P_k$. Τότε θὰ ἰσχύει: $g_1(g_1')^{-1} = (g_2 g_2'^{-1})\cdots(g_k' g_k^{-1})$ καὶ ἐπομένως, ἂν $a = g_1(g_1')^{-1}$ θὰ ἔχουμε $a^{p_1^{m_1}} = a^{p_2^{m_2}\cdots p_k^{m_k}}$. Συμπεραίνουμε ὅτι ἡ τάξη τοῦ a διαιρεῖ τὸν $p_1^{m_1}$ καὶ τὸν $p_2^{m_2}\cdots p_k^{m_k}$, ποὺ εἶναι πρῶτοι μεταξύ τους, καὶ ἐπομένως $o(a)=1$, δηλ. $a = g_1(g_1')^{-1} = e$ ἢ $g_1 = g_1'$. Ὅμοια δείχνουμε ὅτι $g_2 = g_2', \ldots, g_k = g_k'$. ∎

Ἡ πρόταση Γ καὶ μόλις δείξαμε ἀνάγει τὴν μελέτη τῶν Θεωρημάτων Α στὴν περίπτωση τῶν p-Ἀβελιανῶν ὁμάδων, δηλ. Ἀβελιανῶν ὁμάδων τῶν ὁποίων ἡ τάξη εἶναι δύναμη ἑνὸς πρώτου p. Γιὰ τὶς ὁμάδες αὐτὲς ἰσχύει καὶ παραπάνω ἡ ἀνάλυση σὲ εὐθὺ ἄθροισμα κυκλικῶν εἶναι μοναδικὴ μὲ τὴν ἔννοια ποὺ περιγράφει ἡ παρακάτω διατύπωση:

<u>Θεώρημα Δ: Ἂν p πρῶτος καὶ m φυσικός, τότε γιὰ κάθε Ἀβελιανὴ ὁμάδα G μὲ $|G| = p^m$, ὑπάρχουν μονοσήμαντα καθορισμένοι φυσικοὶ (ἀριθμοὶ) $n_1, n_2, \ldots, n_k$ μὲ $n_1 \geq n_2 \geq \cdots \geq n_k$ καὶ ὑπάρχουν $g_1, g_2, \ldots, g_k \in G$ τ.ω. $G = (g_1)\oplus(g_2)\oplus\cdots\oplus(g_k)$</u> (ὅπου φυσικὰ (g) σημαίνει τὴν κυκλικὴ ὁμάδα μὲ γεννήτορα g).

<u>γ</u>) Σχετικὰ μὲ τὸ Θεώρημα Δ τονίζουμε ὅτι δὲν εἶναι οἱ κυκλικὲς ὁμάδες $(g_1), \ldots, (g_k)$ ποὺ καθορίζονται μονοσήμαντα ἀλλὰ οἱ τάξεις τους $p^{n_1}, \ldots, p^{n_k}$. Π.χ. γιὰ τὴν 4-ὁμάδα τοῦ Klein $V = \{e, a, b, ab\}$, $a^2 = b^2 = (ab)^2$ ἔχουμε $n_1 = n_2 = 1$, ἀλλὰ $V = \{e,a\}\oplus\{e,b\} = \{e,a\}\oplus\{e,ab\}$.

Η γραφική $\Pi(n)$ για τη πλήθος των διαφορετικών τρόπων με τους οποίους ο φυσικός η γράφεται σαν άθροισμα $n = n_1 + n_2 + \dots + n_k$ με $n_1 \geq n_2 \geq \dots \geq n_k \geq 1$, τότε οι αντίστοιχες ομάδες $Z_{p^{n_1}} + Z_{p^{n_2}} + \dots + Z_{p^{n_k}}$ θα είναι όλες οι Αβελιανές ομάδες G με $|G| = p^n$, δηλ. κάθε τάξεως ομάδα θα είναι ισόμορφη με μία από τις παραπάνω ομάδες των μορφής $Z_{p^{n_1}} + \dots + Z_{p^{n_k}}$. Από την άλλη οι ομάδες είναι ανά δύο διαφορετικές (δηλ. μη ισόμορφες). Οι παρατηρήσεις αυτές είναι άμεση συνέπεια του Θεωρήματος Δ (σύνθεση αναλλοίωτων για πεπερασμένες παραγωγές ομάδες μέσω των ιδιών των θεωρημάτων Δ).

Μία ενδιαφέρουσα ερώτηση των παραπάνω είναι πόσες οι πλήθος των διαφορετικών Αβελιανών ομάδων τάξεως p^n, p πρώτος, είναι $\Pi(n)$, δηλ. είναι μόνιμο ανεξάρτητο του p (!). Έτσι οι υπάρχουν τρεις ομάδες τάξεως 8 και κάθε 3 τάξεως είναι Z_8, $Z_4 + Z_2$, $Z_2 + Z_2 + Z_2$ και Z_{21}, $Z_7 + Z_3$, $Z_3 + Z_3 + Z_3$.

ψ) Με λίγη δουλειά παραπάνω μπορούμε να απαντήσουμε και στο γενικότερο ερώτημα: Πόσες Αβελιανές ομάδες τάξης n υπάρχουν; Απάντηση: Αν $n = p_1^{n_1} \dots p_k^{n_k}$ η πολλαπλότητα των n σε πρώτους παράγοντες, τότε υπάρχουν $\Pi(n_1)\Pi(n_2)\dots\Pi(n_k)$ μη ισόμορφες ανά δύο Αβελιανές ομάδες τάξης n. Το αποτέλεσμα αυτό είναι άμεση συνέπεια των θεωρημάτων Α και Δ και της παρατήρησης: i) Δύο ομάδες είναι ισόμορφες αν και μόνο αν οι Sylow υποομάδες είναι ισόμορφες.

ii) Αν $(A \oplus B \oplus \dots \oplus M) \oplus (A_1 \oplus B_1 \oplus \dots \oplus N_1) = G$, $A, B, \dots, M, A_1, B_1, \dots, N_1$ κυκλικές, $|A|, |B|, \dots, |M|$ δυνάμεις ενός πρώτου p και $|A_1|, |B_1|, \dots, |N_1|$ πρώτοι προς τον p, τότε η $A \oplus B \oplus \dots \oplus M$ είναι η p-Sylow υποομάδα της G.

Άσκηση: Συμπλήρωση της αποδείξεως.

viii) Το θεώρημα A ισχύει και για πεπερασμένα παραγόμενες ομάδες (Αβελιανές), δηλ. ομάδες G για τις οποίες υπάρχει ένα πεπερασμένο υποσύνολό τους $\{g_1, g_2, \dots, g_k\}$ τέτοιο ώστε $G = \langle g_1, g_2, \dots, g_k \rangle$. Αν και η απόδειξη δεν είναι δυσκολότερη από την απόδειξη του θεωρήματος A και όπως θα γίνεται αυτή είναι πολύ χρήσιμη δεν θα ασχοληθούμε με αυτήν. Θα αναφέρουμε μια σημαντική εικασία του Burnside που απαντήθηκε πρόσφατα. Η εικασία του Burnside είναι η εξής: Κάθε πεπερασμένα παραγόμενη ομάδα (όχι αναγκαστικά Αβελιανή) της οποίας όλα τα στοιχεία έχουν τάξη μικρότερη ενός δοσμένου αριθμού n είναι πεπερασμένη. Η απάντηση είναι αρνητική και αποδείχτηκε πρόσφατα (1968) από τους Novikov και Adjan. Πιο συγκεκριμένα έδειξαν ότι για κάθε περιττό αριθμό $n \geq 665$ ~~[illegible]~~ και κάθε $m > 2$ υπάρχει ομάδα G με m γεννήτορες τ.ω. $g \in G \Rightarrow g^n = e$ και η οποία είναι άπειρη.

Ας σημειώσουμε τέλος ότι στην περίπτωση των πεπερασμένα παραγόμενων (Αβελιανών) ομάδων G θεωρούμε κατ' αρχήν την υποομάδα H στρέψεως της (δηλ. τα $g \in G$ με $o(g) < \infty$). Τα υπόλοιπα στοιχεία της G συνεισφέρουν στην ανάλυση σε ~~[illegible]~~ ευθύ άθροισμα κυκλικών ένα αριθμό άπειρων κυκλικών υποομάδων ενώ τα ~~[illegible]~~ στοιχεία της H ένα αριθμό πεπερασμένων κυκλικών υποομάδων. Για την υποομάδα στρέψεως το θεώρημα συνήθως δίνεται με τη μορφή: "Υπάρχουν κυκλικές υποομάδες της H, $H_1, H_2, \dots, H_k$ τ.ω. $H = H_1 \oplus H_2 \oplus \dots \oplus H_k$ και όπου η τάξη της H_i διαιρεί την τάξη της H_{i+1}, $i = 1, 2, \dots, k-1$."

Άσκηση α) Δείξτε ότι πράγματι η H είναι υποομάδα της G. β) Δείξτε την παραπάνω υπογραμμισμένη πρόταση στην περίπτωση πεπερασμένης Αβελιανής ομάδας H.

γ) Δείξτε ότι η εικασία του Burnside αληθεύει για Αβελιανές ομάδες.

viii) Το Θεώρημα Α μπορεί να αναδιατυπωθεί και ως εξής:
Αν G είναι μια πεπερασμένη (δηλαδή και μια πεπερασμένα παραγόμενη) Αβελιανή ομάδα, τότε υπάρχουν στοιχεία στην G με τάξεις $m_1, m_2, \ldots, m_k$ με την ιδιότητα: για κάθε $g \in G$ υπάρχει μοναδική παράσταση του g με τη μορφή $g = x_1 g_1 + \cdots + x_k g_k$, όπου τα $x_1, x_2, \ldots, x_k$ ανήκουν στα $Z_{m_1}, \ldots, Z_{m_k}$ αντίστοιχα (αν $m_i = \infty$ για κάποιο i, τότε το αντίστοιχο x_i θα ανήκει στο Z). Αν αφήναμε όλα τα x_i να ανήκουν στο Z, τότε φυσικά θα είχαμε πάλι το παραπάνω αποτέλεσμα αλλά η παράσταση δεν θα ήταν μοναδική.

Με τη μορφή αυτή το θεώρημα θυμίζει το θεώρημα ύπαρξης βάσεως πεπερασμένης διάστασης γραμμικών χώρων. Στην Άλγεβρα ορίζεται μια δομή ανάλογη με τη δομή των γραμμικών χώρων πάνω σε ένα σώμα F και ονομάζεται R-module. Η διαφορά είναι ότι τα βαθμωτά μεγέθη αντί να προέρχονται από ένα σώμα F προέρχονται από ένα δακτύλιο R (προτείνουμε να διαβάσει ο αναγνώστης τους ορισμούς και μετά ελέγξτε τους ψάχνοντας κάποιο βιβλίο Άλγεβρας). Οι Αβελιανές ομάδες συμπεριφέρονται σαν Z-modules. Με κατάλληλες προϋποθέσεις για τον δακτύλιο R το θεώρημα Α ισχύει και για πεπερασμένα παραγόμενα R-modules (η συνήθης προϋπόθεση είναι ότι ο R είναι δακτύλιος κυρίων ιδεωδών).

(4.2) Απόδειξη Θεωρήματος Δ

Αν πιστέψουμε προς στιγμή το θεώρημα, τότε βλέπουμε εύκολα ότι ο αριθμός m_1 είναι η μέγιστη τάξη που έχουν τα στοιχεία της G. Με οδηγό αυτή την παρατήρηση παίρνουμε για g_1 ένα στοιχείο μέγιστης τάξης της G.

Ἄν $o(g_1)=p^{n_1}$ καί $p^{n_1}=|G|$, τότε τελειώσαμε. Ἄν $n_1<n$, τότε θεωροῦμε τήν ὁμάδα $H_1=(g_1)$ καί ἔστω $\bar{g}_2 H_1$ ἕνα στοιχεῖο μέγιστης τάξης τῆς G/H. Ἐπειδή προφανῶς $\bar{g}_2^{\,p^{n_1}} \in eH_1$, ἡ τάξη τοῦ $\bar{g}_2 H_1$, ἔστω p^{n_2}, θα εἶναι μικρότερη ἤ ἴση ἀπό τήν p^{n_1}, δηλ. $n_2 \le n_1$. Ἀρκεῖ για ἀποδείξουμε ἀκέραιο j τό στοιχεῖο $(\bar{g}_2 g_1^{-j})H_1$ ἔχει ἴδια τάξη p^{n_2} (ἀφοῦ $\bar{g}_2 H_1 = \bar{g}_2 g_1^{-j} H_1$). Θα διαλέξουμε τό j ἔτσι ὥστε ἡ τάξη τοῦ στοιχείου $\bar{g}_2 g_1^{-j}$ νά εἶναι ἀκριβῶς p^{n_2}. Γράφουμε $g_2=\bar{g}_2 g_1^{-j}$ καί παρατηροῦμε ὅτι ἡ τάξη τοῦ g_2 εἶναι προφανῶς $\ge p^{n_2}$. Ἀρκεῖ ἐπομένως νά βροῦμε j τ.ώ. $g_2^{\,p^{n_2}}=(\bar{g}_2 g_1^{-j})^{p^{n_2}}=e$. Ἄς παρατηρήσουμε πρῶτα ὅτι ὑπάρχει $\lambda\in\mathbb{Z}$ μέ $\bar{g}_2^{\,p^{n_2}}=g_1^{\lambda}$ καί ἐπομένως $e=\bar{g}_2^{\,p^{n_1}}=g_1^{\lambda p^{n_1-n_2}}$. Συνάγουμε ὅτι $p^{n_1}/\lambda p^{n_1-n_2}$, δηλ. p^{n_2}/λ. Ὑπάρχει λοιπόν ἀκέραιος ϑ τ.ώ. $\bar{g}_2^{\,p^{n_2}}=g_1^{\vartheta p^{n_2}}$ δηλ. $(\bar{g}_2 g_1^{-\vartheta})^{p^{n_2}}=e$ καί ἀρκεῖ νά πάρουμε $j=\vartheta$.

Ἰσχυρίζομαι ἀκόμη ὅτι $(g_1)\cap(g_2)=\{e\}$. Πραγματικά ἄν για κάποιο ἀκέραιο ν $g_2^{\nu}\in(g_1)$, τότε $(g_2 H_1)^{\nu}=(g_1)$ καί ἐπομένως p^{n_2}/ν, ὁπότε $g_2^{\nu}=e$.

Ἄς ἀνακεφαλαιώσουμε. Εἴδαμε ὅτι ἄν $n_1<n$, τότε ὑπάρχει $n_2\le n_1$ καί $g_1,g_2\in G$ μέ $o(g_1)=p^{n_1}$, $o(g_2)=p^{n_2}$ καί $(g_1)\cap(g_2)=\{e\}$. Ἄν ἐπομένως $n_1+n_2=n$ τελειώσαμε. Ἄν $n_1+n_2<n$ καί p^{n_3} ἡ μέγιστη τάξη τῶν στοιχείων τῆς $G/(g_1)(g_2)$, τότε μέ τόν ἴδιο ἀκριβῶς τρόπο δείχνουμε τήν ὕπαρξη $n_3\le n_2$ καί g_3 μέ $o(g_3)=p^{n_3}$ τ.ώ. $(g_3)\cap(g_1)(g_2)=e$. Ἄν $n_1+n_2+n_3=n$ τελειώσαμε, ἀλλιῶς συνεχίζουμε μέ τόν ἴδιο τρόπο. Ἐπειδή ἡ G εἶναι πεπερασμένη ἡ διαδικασία αὐτή θα τελειώσει σέ πεπερασμένο πλῆθος βημάτων καί μαζί μέ αὐτήν καί ἡ ἀπόδειξη τῆς ὕπαρξης τῶν $g_1, g_2, \dots, g_k$.

<u>Άσκηση</u>. Δείξτε τους παραπάνω ισχυρισμούς για τα g_3, g_2. (Υπόδειξη: Βρείτε $\bar{g}_3$ με $\{\bar{g}_3 (g_1)(g_2)\}^{p^{n_3}} = (g_1)(g_2)$ όπου p^{n_3} η μεγίστη τάξη στην $G/(g_1)(g_2)$ και γράψτε $\bar{g}^{p^{n_3}} = g_1^{\lambda} g_2^{\mu}$. Δείξτε τώρα ότι $p^{n_3}|\lambda$ και $p^{n_3}|\mu$, παρατηρώντας πρώτα ότι $g_2^{\mu(p^{n_2}-p^{n_3})} \in (g_1)$ ....).

Μένει να δείξουμε ότι οι αριθμοί $n_1, n_2, \dots, n_k$ είναι μονοσήμαντα καθορισμένοι. Υποθέτουμε λοιπόν ότι έχουμε δύο αναλύσεις $(g_1)\oplus\cdots\oplus(g_k) = G = (h_1)\oplus\cdots\oplus h_\nu$ που αντιστοιχούν στους αριθμούς $n_1 \geq n_2 \geq \dots \geq n_k$ και $m_1 \geq m_2 \geq \dots \geq m_\nu$.

Είναι πολύ εύκολο να δούμε ότι το σύνολο $H = \{g \in G : g^p = e\}$ είναι υποομάδα της G και μάλιστα

$$H = (g_1^{p^{n_1-1}})\oplus\cdots\oplus(g_k^{p^{n_k-1}}) = (h_1^{p^{m_1-1}})\oplus\cdots\oplus(h_\nu^{p^{m_\nu-1}})$$

Άμεση συνέπεια είναι ότι $|H| = p^k = p^\nu$, δηλ. $k = \nu$. Είναι επίσης εύκολο να δούμε ότι

$$G/H \cong (g_1^p)\oplus\cdots\oplus(g_k)^p \quad \text{και} \quad G/H = (h_1^p)\oplus\cdots\oplus(h_k^p)$$

Τα $g_1^p, \dots, g_k^p$ και $h_1^p, \dots, h_k^p$ έχουν τάξεις $p^{n_1-1}, \dots, p^{n_k-1}$ και $p^{m_1-1}, \dots, p^{m_k-1}$ αντίστοιχα και η απόδειξη συμπληρώνεται εύκολα με επαγωγή ως προς n.

Οι αριθμοί $n_1, n_2, \dots, n_k$ λέγονται <u>αναλλοίωτες</u> της p-ομάδας G.

<u>Πόρισμα Ε</u>. <u>Δύο Αβελιανές πεπερασμένες ομάδες είναι ισόμορφες αν έχουν την ίδια τάξη και για κάθε πρώτο διαιρέτη p της τάξης τους, οι αντίστοιχες p-Sylow υποομάδες τους έχουν τις ίδιες αναλλοίωτες.</u>

<u>Απόδειξη</u>. Άμεση συνέπεια του Θεωρήματος Δ και της παρατήρησης (VI).