ΚΕΦΑΛΑΙΟ 3
Ημιομάδες και Ομάδες

Λίγα εισαγωγικά σχόλια: Λαβένταν δύο μη κενών συνόλων A και B, κάθε απεικόνιση $\theta: A \times B \to B$ ορίζει μια πράξη επί του B. Όταν $A = B$, οι πράξεις χαρακτηρίζονται ως εσωτερικές· διαφορετικά, ονομάζονται εξωτερικές. Οι αλγεβρικές δομές νοούνται σύνολα (διάφορα του κενού) τα οποία είναι εφοδιασμένα με μια τουλάχιστον (εσωτερική ή εξωτερική) πράξη. [Επί παραδείγματι, υπάρχει μέσω της Γ.Α εξοικείωση με την αλγεβρική δομή του διανυσματικού χώρου. Εκεί θεωρούμε μία εσωτερική ("Πρόσθεση") και μία – εν γένει – εξωτερική πράξη ("αριθμητικό ή βαθμωτό πολλαπλασιασμό").]

Η αλγεβρική δομή της "ομάδας" καθορίζεται μέσω του εφοδιασμού ενός μη κενού συνόλου με μία και μόνον εσωτερική πράξη, η οποία πληροί κάποιες "χαρακτηριστικές συνθήκες". Το ομαδοειδή, οι ημιομάδες και τα μονοειδή υπάγονται στους "προπομπούς" της.

Άλγεβρα – 16/3/06

§3.1 Ομαδοειδή και ημιομάδες

3.1.1 Ορισμός: Κάθε ζεύγος (A,Θ) αποτελούμενο από ένα (όχι κενό) σύνολο A και μια εσωτερική πράξη $\Theta: A\times A \to A$ καλείται **ομαδοειδές**

⚠ **3.1.2 Παρατήρηση:** Εξ' ορισμού η εικόνα ενός ζεύγους από το $A\times A$ **οφείλει** να ανήκει στο A^2. Επί παραδείγματος το $(\mathbb{Q},\Theta)$, όπου $\Theta(q,q') := q+q'+qq'$, $\forall (q,q')\in\mathbb{Q}\times\mathbb{Q}$ είναι ένα ομαδοειδές, ενώ το ζεύγος $(\mathbb{N},n)$ όπου $n(m,n)=m-n$, $\forall (m,n)\in\mathbb{N}\times\mathbb{N}$ **δεν** είναι.

3.1.3 Ορισμός: Έστω (A,Θ) ένα ομαδοειδές. Για απλούστερη έκφραση της εικόνας $\Theta(\alpha_1,\alpha_2)$ ενός ζεύγους $(\alpha_1,\alpha_2)\in A\times A$ χρησιμοποιούνται διάφοροι συμβολισμοί, όπως $\alpha_1\cdot\alpha_2$ (ή $\alpha_1\alpha_2$), $\alpha_1+\alpha_2$, $\alpha_1*\alpha_2$, $\alpha_1\odot\alpha_2$ κ.ά. Μια τέτοια πράξη, ας την πούμε $\odot$, καλείται

(i) **προσεταιριστική** (και το $(A,\odot)$ **προσεταιριστικό ομαδοειδές** ή **ημιομάδα**) όταν

$$\boxed{\alpha\odot(b\odot c)=(\alpha\odot b)\odot c \text{ για όλα τα } \alpha,b,c\in A.}$$

(ii) **μεταθετική** (και το $(A,\odot)$ **αβελιανό ομαδοειδές** ή **ομαδοειδές του Abel**) όταν:

$$\boxed{\alpha\odot b = b\odot\alpha \text{, για όλα τα } \alpha,b\in A}$$

3.1.4 Πρόταση: (Γενικευμένος προσεταιριστικός νόμος)
Έστω $(A,\odot)$ μια ημιομάδα και έστω $(\alpha_1,\dots,\alpha_n)\subset A^n$, $n\in\mathbb{N}$. Τότε, καθ' οιονδήποτε τρόπο και αν φτιάξουμε την πράξη "$\odot$" για καθένα των n όντων στοιχείων $\alpha_1,\dots,\alpha_n$ δηλαδή καθ' οιονδήποτε

τρόπο σχηματίσουμε $\alpha_1 \odot \alpha_2 \odot \dots \odot \alpha_n$, υπό τον όρο της τήρησεως της προειρημένης διατάξεως τους, λαμβάνουμε το ίδιο αποτέλεσμα (Απλούστερη διατύπωση: Για τον σχηματισμό του $\alpha_1 \odot \alpha_2 \odot \dots \odot \alpha_n$ δεν έχουμε χρεία παρεμβολής "παρενθέσεων").

Απόδειξη: Όταν $n \leq 3$, τότε αυτό είναι προφανές ($\alpha_1 = \alpha_2$: $\alpha_1 \odot \alpha_2 = \alpha_1 \odot \alpha_2$; $\alpha_1 \odot (\alpha_2 \odot \alpha_3) = (\alpha_1 \odot \alpha_2) \odot \alpha_3$).
Όταν $n \geq 4$, τότε εφαρμόζουμε μαθηματική επαγωγή επί του n.
Για κάθε $k \in \mathbb{N}$ ορίζουμε μια απεικόνιση

$$P_k : A^k \longrightarrow \Pi(A)$$
$$A^k = \underbrace{A \times A \times \dots \times A}_{k \text{ φορές}}$$

μέσω του αναδρομικού τύπου:
$P_1(\alpha) := \{\alpha\}$ και
$P_k(\alpha_1, \dots, \alpha_k) := \{ b \odot c \mid b \in P_j(\alpha_1, \dots, \alpha_j),\ c \in P_{k-j}(\alpha_{j+1}, \dots, \alpha_k)$ για κάποιο $j \in \{1, 2, \dots, k-1\} \}$

Τα στοιχεία του συνόλου $P_n(\alpha_1, \dots, \alpha_n)$ είναι ουσιαστικώς όλοι οι δυνατοί σχηματισμοί του $\alpha_1 \odot \alpha_2 \odot \dots \odot \alpha_n$ (με παχυμένη τη διάταξη των $\alpha_1, \alpha_2, \dots, \alpha_n$). Ας υποθέσουμε ότι ο ισχυρισμός είναι αληθής για κάθε j, όπου $1 \leq j < n$. Εξ' ορισμού, ένα τυχόν στοιχείο $d \in P_n(\alpha_1, \dots, \alpha_n)$ γράφεται υπό τη μορφή $b \odot c$, όπου $b \in P_j(\alpha_1, \dots, \alpha_j)$ και $c \in P_{k-j}(\alpha_{j+1}, \dots, \alpha_k)$ για κάποιο $j \in \{1, \dots, k-1\}$. Εάν έχουμε $j=1$, οπότε $b = \alpha_1$, τότε, κατά την επαγωγική μας υπόθεση, $d = \alpha_1 \odot (\alpha_2 \odot (\alpha_3 \odot (\dots \odot (\alpha_{n-1} \odot \alpha_n)) \dots))$.
Εάν, από την άλλη μεριά, έχουμε $j > 1$, τότε από τη (συνήθη) προσεταιριστικότητα και την επαγωγική μας υπόθεση, έπεται ότι
$d = [\alpha_1 \odot (\alpha_2 \odot (\alpha_3 \odot \dots (\alpha_{j-1} \odot \alpha_j) \dots))] \odot [\alpha_{j+1} \odot (\dots \odot (\alpha_{n-1} \odot \alpha_n)) \dots)] =$
$\alpha_1 \odot w$, για κάποιο $w \in P_{n+1}(\alpha_2, \dots, \alpha_n) =$
$= \alpha_1 \odot (\alpha_2 \odot (\alpha_3 \odot (\dots \odot (\alpha_{n-1} \odot \alpha_n)) \dots))$. Άρα το $P_n(\alpha_1, \dots, \alpha_n)$ είναι ένα μονοσύνολο, οπότε ο ισχυρισμός είναι αληθής και για n στοιχεία. □

διότι $A \times A \to A$ των

§3.2 Μονοειδή

3.2.1 Ορισμός: Έστω $(A, \odot)$ είναι ένα ομοδοειδές. Ένα στοιχείο e του A καλείται *εξ αριστερών* (και αντιστοίχως *εν δεξιών*) *ουδέτερο στοιχείο* ως προς την πράξη $\odot$ όταν ισχύει

$$\boxed{e \odot \alpha = \alpha \ , \forall \alpha \in A}$$ (και αντιστοίχως: $\boxed{\alpha \odot e = \alpha \ , \forall \alpha \in A}$)

3.2.2 Παράδειγμα: Έάν $A \neq 0$ $A \times A \to A$

$(\alpha, \alpha') \overset{\cup}{\longmapsto} \alpha \odot \alpha' := \alpha'$, τότε $\overset{\omega\omega}{\text{το}}$ ζεύγος $(A, \odot)$ είναι μια ημιομάδα, *μόνδε* στοιχείο της οποίας είναι εξ αριστερών ουδέτερο.

Αν $\text{Card} = 1 \Rightarrow \alpha \odot \alpha = \alpha$ και εν δεξιών και εξ αριστερών

Έαν, μάλιστα, $\text{Card}(A) \geq 2$, τότε η A *δεν* διαθέτει *μονάνα* εν δεξιών ουδέτερο στοιχείο.

3.2.3 Ορισμός: Έστω $(A, \odot)$ ένα ομοδοειδές. Ένα στοιχείο $\alpha \in A$ καλείται (*αμφιπλεύρως*) *ουδέτερο στοιχείο* όταν

$$\boxed{\alpha \odot e = e \odot \alpha = \alpha \ , \forall \alpha \in A}$$

3.2.4 Παραδείγματα: (i) Τα $(\mathbb{Z}, +)$ $(\mathbb{Z}, \cdot)$ αποτελούν ημιομάδες (η συνήθης πρόσθεση, ο συνήθης πολλαπλασιασμός) με ουδέτερα τους στοιχεία τα 0 και 1, αντιστοίχως.

(ii) Τα $(\mathbb{Z}_m, +), (\mathbb{Z}_m, \cdot)$ $m \in \mathbb{N}$, $m \geq 2$, ως προς τις πράξεις:

$$\left\{ \begin{array}{l} [n_1]_m + [n_2]_m := [n_1 + n_2]_m \\ [n_1]_m \cdot [n_2]_m := [n_1 n_2]_m \end{array} \right\}$$

είναι ημιομάδες με ουδέτερα στοιχεία της τα $[0]_m$ και $[1]_m$, αντίστοιχα.

(Άσκηση ν.δ.ο είναι αντεναλλάξιμοι δηλ. ότι $n +$ και $\cdot$ είναι καλώς ορισμένες

δύο διαφορετικοί $\Rightarrow$ δύο ίδιοι)

(iii) Έστω το A είναι ένα σύνολο, τότε τα ζεύγη $(\mathcal{P}(A), \cap)$, $(\mathcal{P}(A), \cup)$ είναι ημιομάδες με ουδέτερα τους στοιχεία τα A και $\emptyset$ αντιστοίχως.
(άσκηση)

3.2.5 Πρόταση: Έστω ότι το $\left\{\begin{array}{l} e \text{ είναι ένα εξ αριστερών ουδέτερο στοιχείο} \\ e' \text{ είναι ένα εκ δεξιών ουδέτερο στοιχείο} \end{array}\right\}$ ενός ομαδοειδούς $(A, \odot)$. Τότε $e = e'$ (και, ως εκ τούτου, το e δεν είναι "αμφιπλεύρως" ουδέτερο στοιχείο του A). Κατά συνέπειαν κάθε ομαδοειδές διαθέτει το πολύ ένα ουδέτερο στοιχείο.

Απόδειξη: Έχουμε $e \odot e' = e'$ (επειδή το e είναι εξ αριστερών ουδέτερο)
$e \odot e' = e$ (επειδή το e' είναι εκ δεξιών ουδέτερο)
$\Downarrow$
$e = e'$
□

3.2.6 Ορισμός: Κάθε ημιομάδα η οποία διαθέτει ουδέτερο στοιχείο, ονομάζεται μονοειδές.

3.2.7 Ορισμός: Έστω $(A, \odot)$ ένα ομαδοειδές που διαθέτει ουδέτερο στοιχείο (ας το ποιμε e). Έστω τώρα τυχόν στοιχείο $\alpha \in A$. Ένα στοιχείο $\alpha' \in A$ (και, αντιστοίχως, $\alpha'' \in A$) καλείται εξ αριστερών (και αντιστοίχως εκ δεξιών) συμμετρικό στοιχείο του α (ως προς την πράξη "$\odot$") όταν ισχύει: $\boxed{\alpha' \odot \alpha = e}$ (αντιστοίχως $\boxed{\alpha \odot \alpha'' = e}$). Ένα στοιχείο $\alpha' \in A$ καλείται συμμετρικό στοιχείο του α όταν είναι ταυτοχρόνως και εξ αριστερών και εκ δεξιών συμμετρικό στοιχείο του α, όταν δηλ. ισχύει $\boxed{\alpha \odot \alpha' = \alpha' \odot \alpha = e}$

3.2.8 Παράδειγμα: $A \neq \emptyset$,

$(A^A = A\Pi(A,A) =$

$= \{f : A \to A$, απεικονίσεις$\}, \bullet)$

μονοειδές με ουδέτερο του την Id_A

συμβ.	
"+" "αντίθετο"	$\alpha + x = 0$
"$\bullet$" "αντίστροφο"	$\alpha x = 1$

αντί για συμμετρικό $-\alpha$, α^{-1}

Κατά την πρόταση 1.2.17, οι μόνες $f \in A^A$ οι οποίες διαθέτουν ως δεξιόν συμμετρικό στοιχείο είναι οι επιρριπτικές, οι μόνες που διαθέτουν εξ αριστερών συμμετρικό στοιχείο είναι οι ενριπτικές και οι μόνες που διαθέτουν συμμετρικό στοιχείο είναι οι αμφιρριπτικές.

3.2.9 Πρόταση: Έστω το $(A, \circledcirc)$ είναι ένα μονοειδές με ουδέτερο στοιχείο του το e και το $\alpha \in A$ διαθέτει το α' ως εξ αριστερών συμμετρικό του και το α'' ως εν δεξιών συμμετρικό του, τότε $\boxed{\alpha' = \alpha''}$. Κατά συνέπειαν, κάθε $\alpha \in A$ διαθέτει το πολύ ένα συμμετρικό στοιχείο.

Απόδειξη: Προφανώς $\alpha'' = e \circledcirc \alpha''$ (e ουδέτερο στοιχείο)

$= (\alpha' \circledcirc \alpha) \circledcirc \alpha''$ (α' εξ αριστερών συμμετρικό του α)

$= \alpha' \circledcirc (\alpha \circledcirc \alpha'')$ (λόγω προσεταιριστικότητας της $\circledcirc$)

$= \alpha' \circledcirc e$ (α'' εν δεξιών συμμετρικό του α)

$= \alpha'$

□

§3.3 Ομάδες και υποομάδες

3.3.1 Ορισμός: Έστω G ένα μη κενό σύνολο. Ένα μονοειδές $(G, \circledcirc)$ [με το G ως υποκείμενο σύνολο του] καλείται ομάδα όταν για κάθε στοιχείο του G, υπάρχει το συμμετρικό του ως προς την "$\circledcirc$" (πρβλ.

πρόταση 3.2.9) Η τάξη $|G|$ είναι εξ' ορισμού ο πληθικός αριθμός $Card(G)$ του συνόλου G. Εάν η $|G|$ είναι πεπερασμένη, τότε η G λέμε πως έχει πεπερασμένη τάξη ή απλώς ότι η G είναι πεπερασμένη ομάδα και γράφουμε $|G|<\infty$ (Ειδάλλως, λέμε ότι η G είναι άπειρη ομάδα και γράφουμε $|G|=\infty$). Μια ομάδα λέγεται μεταθετική ή αβελιανή (ή ομάδα του Abel) όταν η πράξη, με την οποία είναι εφοδιασμένη, είναι μεταθετική.

3.3.2 Παραδείγματα: (i) Τα ζεύγη $(\mathbb{Z},+),(\mathbb{Q},+),(\mathbb{R},+)$ αποτελούν τα πιο "οικεία" παραδείγματα ομάδων του Abel. Το ζεύγος $(\mathbb{N}_0,+)$ είναι μόνον αβελιανό μονοειδές, διότι μονάχα $x\in\mathbb{N}$ δεν διαθέτει "αντίθετο" (=συμμετρικό) ΕΝΤΟΣ του $\mathbb{N}_0$

(iii) Το $(\mathbb{Z}_m,+)$ είναι αβελιανή ομάδα ($[0]_m$ ουδέτερο, $-[k]_m=[-k]_m$).

(iii) Τα $(\mathbb{Q}\setminus\{0\},\cdot),(\mathbb{R}\setminus\{0\},\cdot),(\mathbb{Q}_{>0},\cdot),(\mathbb{R}_{>0},\cdot)$ είναι αβελιανές ομάδες ενώ το $(\mathbb{Z}\setminus\{0\},\cdot)$ είναι μόνο αβελιανό μονοειδές (με το 1 ως ουδέτερο ή "μοναδιαίο" στοιχείο του) διότι μόνον τα ±1 διαθέτουν "αντίστροφο" (=συμμετρικό) στοιχείο ΕΝΤΟΣ ΤΟΥ $\mathbb{Z}\setminus\{0\}$ ∇_0^Δ

(iv) Το ζεύγος $(\mathbb{Q}_{>0},*)$, όπου $a*b:=\frac{ab}{2}$, $\forall(a,b)\in\mathbb{Q}_{>0}\times\mathbb{Q}_{>0}$, είναι αβελιανή ομάδα (άσκηση) η οποία έχει το 2 (∇_0^Δ) ως ουδέτερό της στοιχείο και το $\frac{4}{a}$ ως συμμετρικό στοιχείο οιουδήποτε $a\in\mathbb{Q}_{>0}$ (ως προς την πράξη "$*$").

Άλγεβρα – 21/3/06

(v) Το αβελιανό μονοειδές $(\mathbb{Z}_m, \cdot)$, $m \in \mathbb{N}$, $m \geq 2$ με ουδέτερο του στοιχείο το $[1]_m$, δεν είναι ομάδα, καθώς το $[0]_m$ δεν διαθέτει αντίστροφο στοιχείο.

3.3.3 Σημείωση: Από εδώ και στο εξής, όταν ασχοφερόμαστε σε ομάδες, θα υιοθετούμε ως επί το πλείστον τον πολλαπλασιαστικό συμβολισμό ή τον προσθετικό συμβολισμό για τις εκάστοτε θεωρούμενες πράξεις (χρόφοντας π.χ. $g_1 g_2$ ή, αντιστοίχως, $g_1 + g_2$ (αντί του $g_1 \odot g_2$ κ.λ.π.) για δύο στοιχεία g_1, g_2 μίας ομάδας G) ενώ θα εισαγάγουμε τη συντομογραφία:

$g^n = \underbrace{g \cdot \ldots \cdot g}_{n \text{ φορές}}$ (και, αντιστοίχως, $ng = \underbrace{g + \ldots + g}_{n \text{ φορές}}$

$[g^{-1}]$ $[-g]$

εν είδει "δυνάμεως" (αντ. εν είδει πολλαπλασίου) ενός $g \in G$ με κάθε $n \in \mathbb{N}$.

3.3.4 Πρόταση: Έστω $(G, \cdot)$ μια ομάδα με το e ως ουδέτερο της στοιχείο. Τότε ισχύουν τα ακόλουθα:

(i) Για κάθε $a, b, g \in G$

$ag = bg \Rightarrow a = b$ } (Νόμοι της διαγραφής)

$ga = gb \Rightarrow a = b$ }

(ii) $(g^{-1})^{-1} = g$, $\forall g \in G$

(iii) Έαν $k \in \mathbb{N}$ και $g_1, \ldots, g_k \in G$ τότε: $(g_1 \ldots g_k)^{-1} = g_k^{-1} g_{k-1}^{-1} \ldots g_2^{-1} g_1^{-1}$

(iv) Για οποιαδήποτε $a, b \in G$ οι εξισώσεις $ax = b$ και $ya = b$ επιδέχονται τα $x = a^{-1}b$ και $y = b \cdot a^{-1}$, αντιστοίχως, ως μοναδικές τους λύσεις.

Απόδειξη: (i) Πολλαπλασιάζοντας την πρώτη εξίσωση (εν δεξιών) με το g^{-1}, λαμβάνουμε $(ag)g^{-1} = (bg)g^{-1} \overset{\text{προσετ.}}{\Rightarrow} a(gg^{-1}) = b(gg^{-1}) \Rightarrow$

$\Rightarrow ae = be \Rightarrow a = b$. Κατ' αναλογίαν (ως τότε πολλαπλασιασμού με το g^{-1} εξ αριστερών) αποδεικνύεται και η δεύτερη συνεπαγωγή.

(iii) Επειδή $(g^{-1})^{-1} g^{-1} = e = g^{-1} \cdot ((g^{-1})^{-1})$ και $gg^{-1} = e = g^{-1}g$ έχουμε $(g^{-1})^{-1} = g$, $\forall g \in G$ λόγω της μοναδικότητας του αντιστρόφου (=συμμετρικού) στοιχείου (Βλ.3.2.9)

(iiii) Έστω $k=2$. Αρκεί (και πάλι λόγω της μοναδικότητας του αντιστρόφου) να δείξουμε ότι $(g_1 g_2)(g_2^{-1} g_1^{-1}) = e = (g_2^{-1} g_1^{-1})(g_1 g_2)$. Θέτοντας σε εφαρμογή τον γενικευμένο προσεταιριστικό νόμο (Βλ.3.1.4) λαμβάνουμε: $(g_1 g_2)(g_2^{-1} g_1^{-1}) = g_1 (\underbrace{g_2 g_2^{-1}}_{e}) g_1^{-1} = g_1 g_1^{-1} = e$.

Αναλόγως αποδεικνύεται ότι $e = (g_2^{-1} g_1^{-1})(g_1 g_2)$. Για $k \geq 3$ το ζητούμενο έπεται κάνοντας χρήση μαθηματικής επαγωγής (άσκηση

(iv) Κατ' αρχάς, $a(a^{-1}b) = (aa^{-1})b = eb = b$, οπότε το $a^{-1}b$ είναι όντως μια λύση της $ax = b$. Έστω $g \in G$ μια τυχούσα λύση της. Τότε: $(a^{-1})(ag) = a^{-1}b \Rightarrow (\underbrace{a^{-1}a}_{e})g = a^{-1}b \Rightarrow g = a^{-1}b$. Αναλόγως

αποδεικνύεται και το μοναδικόν της λύσεως της δεύτερης εξισώσεως. □

3.3.5 Πρόταση: Έστω $(G, \cdot)$ μια ομάδα με ουδέτερο στοιχείο της το e. Τότε $\forall g \in G$ και $\forall (m,n) \in \mathbb{Z}^2$ ισχύουν τα ακόλουθα

(i) $g^m g^n = g^{m+n} = g^n \cdot g^m$

(ii) $(g^m)^n = g^{mn} = (g^n)^m$

(iii) $g^{-m} = (g^{-1})^m = (g^m)^{-1}$

Απόδειξη: (i) Κατ' αρχάς υποθέτουμε ότι αμφότεροι οι m, n είναι θετικοί. Θα εφαρμόσουμε μαθηματική επαγωγή επί του m. (Αναλόγως επιχειρηματολογεί κανείς και για το n). Εάν $m=1$ τότε

- εξ' ορισμού - $gg^n = g^{1+n}$. Υποθέτοντας ότι $g^m g^n = g^{m+n}$, λαμβάνουμε $g^{m+1} g^n = (gg^m)g^n = g(g^m g^n) = g \cdot g^{m+n} = g^{m+n+1}$. Τώρα υποθέτουμε ότι ένας εκ των m, n είναι 0. Έστω $m=0$ τότε $g^0 g^n = eg^n = g^n = g^{0+n}$ (και αναλόγως, $g^m g^0 = g^m e = g^m = g^{m+0}$, όταν $n=0$). Εν συνεχεία, υποθέτουμε ότι αμφότεροι οι m, n είναι αρνητικοί. Τότε, $g^m g^n \underset{(iii)}{=} (g^{-m})^{-1}(g^{-n})^{-1} = (g^{-n}g^{-m})^{-1} = (g^{-n-m})^{-1} =$

$= (g^{-m-n})^{-1} = g^{m+n}$. Εξ' άλλου, επειδή $m+n = n+m$ έχουμε $g^m g^n = g^n g^m$. Ως εκ τούτου υπολείπεται η εξέταση της περίπτωσης κατά την οποία ο ένας εκ των m, n είναι αρνητικός και ο άλλος θετικός. Επειδή οι αποδείξεις είναι παρομοιότυπες, θα εξετάσουμε τι συμβαίνει μόνο όταν $m>0$ και $n<0$. Διακρίνουμε τρεις διαφορετικές περιπτώσεις:

(α) $\underline{m+n>0}$. Κάνοντας χρήση των όσων ισχύουν στην περίπτωση όπου αμφότεροι οι m, n είναι θετικοί, λαμβάνουμε $g^{m+n} g^{-n} = g^{(m+n)-n} = g^m$. Επειδή το g^{-n} είναι - εξ' ορισμού - το αντίστροφο του g^n, μπορούμε να "πολλαπλασιάσουμε" αμφότερες τις πλευρές (εκ δεξιών) με το g^n και να καταλήξουμε στο ζητούμενο: $g^{m+n} = g^m g^n$.

(β) $\underline{m+n=0}$. Τότε $n=-m$, οπότε το g^n είναι - εξ' ορισμού - το αντίστροφο του g^m και $g^m g^n = g^0 = e$.

(γ) $\underline{m+n<0}$. Κάνοντας χρήση των όσων ισχύουν στην περίπτωση όπου αμφότεροι οι m, n είναι θετικοί, λαμβάνουμε:

$g^{-(m+n)} g^m = g^{-m-n+m} = g^{-n} \underset{(iii)}{\Longrightarrow} g^{-(m+n)} = g^{-n} g^{-m} = g^{-m} g^{-n}$.

(iii) άσκηση

(iii)' Έπεται από το (iii).

□

3.3.6 Ορισμός: Ένα μη κενό υποσύνολο H του υποκείμενου συνόλου G μιας ομάδας $(G, \cdot)$ καλείται <u>υποομάδα της G</u> όταν το H καθίσταται αφεαυτού ομάδα (ως προς τον περιορισμό $\cdot|_H$ της πράξεως "$\cdot$" επί του H).

3.3.7 Παρατήρηση: Για τον έλεγχο του κατά πόσον είναι $H \subseteq G$, $H \neq \emptyset$ είναι ή δεν είναι υποομάδα δεν απαιτείται ο έλεγχος της ισχύος της προσεταιριστικής ιδιότητας διότι για κάθε $(x,y,z) \in H^3$, έχουμε αυτομάτως $(x,y,z) \in G^3$ όπου $x(yz) = (xy)z$. Η επόμενη πρόταση μας πληροφορεί για το ποιες (ικανές και αναγκαίες) συνθήκες οφείλουν να πληρούνται, ώστε ένα δεδομένο: $\emptyset \neq H \subseteq G$ να είναι υποομάδα της G.

3.3.8 Πρόταση: Έστω $(G,\cdot)$ μια ομάδα με ουδέτερο στοιχείο της το e_G και έστω $H \subseteq G$. Τότε τα (i), (ii) και (iii) είναι ισοδύναμα:

↝ (i) Το $(H, \cdot|_H)$ είναι μια υποομάδα της $(G,\cdot)$

↝ (ii) Το H πληροί τις εξής συνθήκες:

(a) $e_G \in H$

(b) $xy \in H$, $\forall (x,y) \in H \times H$

(c) $h^{-1} \in H$, $\forall h \in H$

↝ (iii) Το H πληροί τις εξής συνθήκες:

(a) $e_G \in H$

(b) $ab^{-1} \in H$, $\forall (a,b) \in H \times H$

Απόδειξη: (i) $\Rightarrow$ (iii) Η υποομάδα της $G \Rightarrow H \neq \emptyset$ και τα (b) και (c) ικανοποιούνται (εξ' ορισμού). Εξ' άλλου, η H διαθέτει ουδέτερο στοιχείο e_H για το οποίο ισχύει: $e_H h = h e_H = h$, $\forall h \in H$. Επειδή κάθε $h \in H$ ανήκει στο G θα έχουμε $h e_G = e_G h = h$ οπότε το μονοσήμαντο της επιλύσεως των προαναφερθέντων "εξισώσεων" (βλ. 3.3.4 (iv)) μας δηλοί ότι $e_H = e_G$.

(ii) $\Rightarrow$ (iii) Αρκεί να αποδειχθεί η ισχύς της (b) του (iii). Έστω $(a,b) \in H \times H$, τότε (κατά την (ii)(c)) $b^{-1} \in H$, οπότε $ab^{-1} \in H$ (δυνάμει της (ii)(b))

(iii) $\Rightarrow$ (ii) Όπως προείπαμε, ο έλεγχος της ισχύος της προσεταιριστικής ιδιότητας περιττεύει. Εξ' άλλου, $H \neq \emptyset$ λόγω

της (iii)(α). Υποθέτοντας λοιπόν ότι $ab^{-1}\in H$, $\forall (a,b)\in H\times H$ επιχειρηματολογούμε ως εξής: Εάν $a\in H$ τότε έχουμε $e_G = aa^{-1}\in H$ και $a^{-1} = e_G a^{-1}\in H$. Τούτο σημαίνει ότι η ύπαρξη αντιστρόφου οιουδήποτε στοιχείου του H εντός της H είναι διασφαλισμένη. Απομένει ο έλεγχος της "υλειότητας" της πράξεως "$\cdot|_H$" ήτοι $xy\in H$, $\forall (x,y)\in H\times H$.

Θέτοντας $\begin{matrix} a=x\in H \\ b=y^{-1}\in H \end{matrix}\}$ λαμβάνουμε μέσω εφαρμογής της (iii)(b):

$x(y^{-1})^{-1} = xy\in H$. Άρα η H είναι όντως υποομάδα της G.

□

3.3.9 Παρατήρηση: Οι συνθήκες (ii)(α) και (iii)(α) συμπεριελήφθησαν στην πρόταση 3.3.8 μόνο για να μας εξυπηρετούν ότι το θεωρούμενο σύνολο H είναι μη κενό. Επί παραδείγματι, εάν ένα δεδομένο H διαθέτει τουλάχιστον ένα στοιχείο, τότε εφαρμόζοντας την (iii)(b) με $a=b$, λαμβάνουμε αυτομάτως ότι $e_G\in H$.

3.3.10 Παραδείγματα: (i) Κάθε ομάδα περιέχει δύο τροφοδοτείς υποομάδες, ήτοι τον εαυτό της και την τετριμμένη υποομάδα (που αποτελείται μόνον από το ουδέτερο στοιχείο της).

(ii) Η ομάδα $(\{\pm 1\},\cdot)$ είναι υποομάδα της $(\mathbb{Q}\setminus\{0\},\cdot)$ (όπως έπεται άμεσα από την πρόταση 3.3.8).

(iii) Εάν $n\in\mathbb{Z}$ και $n\mathbb{Z} := \{nk \mid k\in\mathbb{Z}\}$, τότε η $(n\mathbb{Z},+)$ είναι υποομάδα της $(\mathbb{Z},+)$ (άσκηση).

(iv) Οι εγκλεισμοί $\mathbb{Z}\subsetneq\mathbb{Q}$, $\mathbb{Z}\subsetneq\mathbb{R}$, $\mathbb{Q}\subsetneq\mathbb{R}$ καθιστούν τα υποσύνολα αυτά υποομάδες (ως προς την πράξη της συνήθους προσθέσεως).

(v) $\mathbb{Q}\setminus\{0\}\subsetneq\mathbb{R}\setminus\{0\}$ (υποομάδα ως προς τον συνήθη πολλαπλασιασμό).

3.3.11 Πρόταση: Η τομή $\bigcap_{j\in J} H_j$ μιας οιουχένειας υποομάδων

$(H_j)_{j\in J}$ μιας ομάδας $(G,\cdot)$ αποτελεί μια υποομάδα της G.

Απόδειξη: Έστω e το ουδέτερο στοιχείο της G. Επειδή $e\in H_j$ $\forall j\in J$, έχουμε ότι $e\in \bigcap_{j\in J} H_j$ $(\neq\emptyset)$ $\overset{\text{άτομα } e\in \bigcap_{j\in J} H_j}{\longleftarrow}$

Εάν $h_1,h_2\in \bigcap_{j\in J} H_j$, είτε $[h_1,h_2\in H_j,\ \forall j\in J]$ $\xrightarrow[3.3.8(iii)]{}$

$\Rightarrow [h_1h_2^{-1}\in H_j,\ \forall j\in J] \rightarrow h_1h_2^{-1}\in \bigcap_{j\in J} H_j$.

Άρα το $\bigcap_{j\in J} H_j$ είναι όντως υποομάδα της G (μέσω του 3.3.8(iii)) □

3.3.12 Σημείωση: Η ένωση δύο υποομάδων μιας δεδομένης ομάδας G δεν είναι πάντοτε υποομάδα της G

3.3.13 Ορισμός: Για τυχόν υποσύνολο H μιας ομάδας $(G,\cdot)$ χαρακτηρίζουμε την τομή

$$\boxed{\langle H\rangle := \bigcap\{\text{υποομάδες } K \text{ της } G \mid H\subseteq K\}}$$

η οποία είναι η ελάχιστη υποομάδα της G που περιέχει το H ως την υποομάδα της G την παραγόμενη από το H. (Όταν $H=\emptyset$, τότε $\langle H\rangle :=$ τετριμμένη υποομάδα της G).

3.3.14 Πρόταση: Εάν $H\neq\emptyset$, είτε η $\langle H\rangle$, για την οποία λέμε πως έχει το H ως σύνολο ή σύστημα γεννητόρων της, ισούται με

$\langle H\rangle = \{g=h_1^{\varepsilon_1}h_2^{\varepsilon_2}\dots h_k^{\varepsilon_k} \mid (h_1,\dots,h_k)\in H^k$ και $\varepsilon_j\in\mathbb{Z}$, $\forall j$, $1\le j\le k$, $k\in\mathbb{N}\}$

Απόδειξη: Ορίζω $\Gamma=\{g=h_1^{\varepsilon_1}h_2^{\varepsilon_2}\dots h_k^{\varepsilon_k} \mid (h_1,\dots,h_k)\in H^k$ και $\varepsilon_j\in\mathbb{Z}$, $\forall j$, $1\le j\le k$, $k\in\mathbb{N}\}$.

Το σύνολο Γ είναι μια υποομάδα της G. Πράγματι για κάθε

ζεύγος $(h_1^{\varepsilon_1}h_2^{\varepsilon_2}\dots h_k^{\varepsilon_k}, s_1^{\rho_1}s_2^{\rho_2}\dots s_\nu^{\rho_\nu}) \in \Gamma\times\Gamma$ έχουμε

$(h_1^{\varepsilon_1}\dots h_k^{\varepsilon_k})(\xi_1^{\rho_1}\dots\xi_\nu^{\rho_\nu})^{-1} = h_1^{\varepsilon_1}\dots h_k^{\varepsilon_k}\xi_\nu^{-\rho_\nu}\dots\xi_1^{-\rho_1} \in \Gamma \xrightarrow[3.3.8(iii)]{} \Gamma$ υποομάδα της G.

Και επειδή $\forall x\in H,\ x=x'\in\Gamma$, λαμβάνουμε $H\subseteq\Gamma$. Αρκεί λοιπόν να αποδειχθεί ότι το Γ είναι η ελάχιστη υποομάδα της G που περιέχει το H. Προς τούτο υποθέτουμε ότι η B είναι τυχούσα υποομάδα της G, για την οποία ισχύει $H\subseteq B$. Τότε, για κάθε στοιχείο $h_1^{\varepsilon_1}\dots h_k^{\varepsilon_k}\in\Gamma$ έχουμε

$[h_j\in B$ και $\varepsilon_j\in\mathbb{Z}, \forall j\in\{1,\dots,k\}] \Rightarrow$

$\Rightarrow [h_j^{\varepsilon_j}\in B,\ \forall j\in\{1,\dots,k\}] \Rightarrow h_1^{\varepsilon_1}\dots h_k^{\varepsilon_k}\in B.$

Εξ' αυτών συνάγουμε ότι το Γ είναι υποομάδα της B, οπότε $\langle H\rangle=\Gamma$.

□

3.3.15 Ορισμός: Μια ομάδα καλείται πεπερασμένως παραγόμενη όταν διαθέτει ένα πεπερασμένο σύστημα γεννητόρων.

3.3.16 Παράδειγμα: Η $(\mathbb{Z},+)$ παράγεται τόσον από το (μονοσύνολο) $H_1=\{1\}$ όσον και από το σύνολο $H_2=\{-1\}$ η αυτόν και από το απειροσύνολο $H_3=\mathbb{N}$.

ΠΡΟΧΕΙΡΟ:

$\mathbb{Z}\ni n = n\cdot 1$

$(-n)(-1)$

$\mathbb{Z}\ni k$ < $1\cdot k+0\cdot\lambda,\ \lambda\in\mathbb{N}\setminus\{k\}$; $(-1)(-k)+0\cdot\lambda$

3.3.17 Ορισμός: Μια ομάδα καλείται μυωπική (ή μονογενής) όταν μπορεί να παραχθεί (υπό την έννοια του 3.3.13) από κάποιο μονοσύνολο.

Άλγεβρα – 28/3/06

3.3.17 Ορισμός: Μια ομάδα καλείται κυκλική (ή μονογενής) όταν μπορεί να παραχθεί από ένα μονοσύνολο.

3.3.18 Παραδείγματα: Η $(\mathbb{Z},+)$ (όπως προείπαμε στην 3.3.16) είναι κυκλική. Το ίδιο ισχύει και για την $(n\mathbb{Z},+)$. Επίσης, η $(\mathbb{Z}_m,+)$, $m\geq 2$ είναι κυκλική αφού παράγεται από την κλάση ισοτιμίας $[1]_m$. Αντιθέτως η $(\mathbb{Q},+)$ δεν είναι κυκλική, καθότι $\forall q\in\mathbb{Q}\setminus\{0\}$ η $\{nq \mid n\in\mathbb{Z}\}$ είναι μια γνήσια υποομάδα της $(\mathbb{Q},+)$.

3.3.19 Πρόταση: Κάθε κυκλική ομάδα είναι αβελιανή

Απόδειξη: Έστω $(G,\cdot)$ μια ομάδα με το e ως ουδέτερο της. Εάν $G=\langle g\rangle$ $(g\in G)$ και εάν $(x,y)\in G\times G$, τότε $x=g^m$, $y=g^n$, για κάποιους $m,n\in\mathbb{Z}$. Βάσει της προτάσεως 3.3.5(i) λαμβάνουμε $xy=g^m g^n=g^{m+n}=g^{n+m}=g^n g^m=yx$. Άρα η G είναι όντως αβελιανή

□

3.3.20 Πρόταση: Έστω $(G,\cdot)$ μια ομάδα με το e ως ουδέτερο της και έστω $g\in G$. Τότε για την κυκλική ομάδα $\langle g\rangle$ που παράγεται από το g υπάρχουν δύο ενδεχόμενα:
είτε όλες οι δυνάμεις g^n, $n=0,\pm1,\pm2,\dots$ είναι διαφορετικές, είτε $\exists n,m\in\mathbb{Z}$ με $n>m$ τέτοιοι ώστε να ισχύει $g^n=g^m \Leftrightarrow g^{n-m}=e$. Στην πρώτη περίπτωση η $\langle g\rangle$ έχει άπειρη τάξη και λέγεται άπειρη κυκλική ομάδα. Στην δεύτερη περίπτωση, $\langle g\rangle=\{e,g,g^2,\dots,g^{l-1}\}$, όπου $l:=\min\{k\in\mathbb{N} \mid g^k=e\}$

Απόδειξη: Αρκεί να δείξουμε ότι ο ισχυρισμός είναι αληθής

στη δεύτερη περίπτωση. Και' αρχάς, επειδή $\exists n,m \in \mathbb{Z}$ $n > m$, με $g^{n-m} = e$, το σύνολο $\{k \in \mathbb{N} \mid g^k = e\}$ είναι μη κενό. Έστω τώρα g^ν, $\nu \in \mathbb{N}$ τυχόν στοιχείο της $\langle g \rangle$. Δυνάμει της ταυτότητας της ευκλείδειας διαίρεσης (θλ. 2.1) $\exists (q,r) \in \mathbb{Z}^2$, $0 \le r < l$, τ.ω. $\nu = ql + r$. Κατά συνέπειαν, $g^\nu = g^{ql+r} = g^{ql} g^r = (g^l)^q g^r = e g^r = g^r$. Απομένει λοιπόν να αποδειχθεί ότι τα στοιχεία $e, g, \dots, g^{l-1}$ είναι ανά δύο διαφορετικά. Εάν υποτεθεί ότι $\exists \mu, \nu \in \{0,1,\dots,l-1\}$, για τους οποίους ισχύει $\mu > \nu$ και $g^\mu = g^\nu \Rightarrow g^{\mu-\nu} = e$, με $1 \le \mu - \nu \le l-1$, πράγμα που αντίκειται στην επιλογή του l (ως του ελάχιστου θετικού με αυτήν την ιδιότητα). □

3.3.21 Πρόταση: (i) Κάθε υποομάδα της $(\mathbb{Z}, +)$ είναι κυκλική.
(ii) Επιπροσθέτως, ισχύει κάτι ακόμη πιο ισχυρό, ήτοι κάθε υποομάδα μιας κυκλικής ομάδας είναι κυκλική.

Απόδειξη: (i) Έστω H μια υποομάδα της $(\mathbb{Z}, +)$. Εάν η H είναι τετριμμένη, τότε είναι προφανώς κυκλική. Εάν η H δεν είναι τετριμμένη, τότε περιέχει κάποιον $x \in \mathbb{Z} \setminus \{0\}$, οπότε και $-x \in$ (θετικό). Άρα η H περιέχει υποχρεωτικώς έναν θετικό. Έστω $d := \min\{k \in \mathbb{N} \mid k \in H\}$. Ισχυριζόμαστε ότι $H = \langle d \rangle$. Εάν $n \in H$, διαιρούμε τον n δια του d και λαμβάνουμε $n = qd + m$, $q, m \in \mathbb{Z}$, $0 \le m < d$.
Γνωρίζουμε ότι $d \in H$ και $m \in H \} \Rightarrow m = n - (-qd) \in H$. Αυτό H υποομάδα $\Rightarrow qd \in H$
όμως αντίκειται προς την επιλογή του d, εκτός και αν $m = 0$.
Κατά συνέπειαν, $n = qd$, οπότε $H = \langle d \rangle$.
(ii) Έστω $(G, \cdot)$ μια κυκλική ομάδα και έστω M μια μη τετριμμένη υποομάδα της $(G, \cdot)$. Εάν το $g \in G$ παράγει την G τότε κάθε στοιχείο της G, και κατ' επέκταση και της M είναι μια (ακέραια) δύναμη του g. Έστω
$H := \{n \in \mathbb{Z} \mid g^n \in M\}$. Είναι εύκολο να διαπιστώσουμε ότι το

Η είναι υποομάδα της $(\mathbb{Z},+)$ (έστω), οπότε λογικά το ii) θα είναι μυαλιιιή. Εάν $\langle d\rangle = H \Rightarrow \langle g^d\rangle = M$ □

3.3.22 Ορισμός: Έστω $(G,\cdot)$ μια ομάδα με ουδέτερο στοιχείο της το e. Τότε η τάξη $ord(g)$ ενός στοιχείου $g\in G$ ορίζεται ως εξής:

$$ord(g) := \begin{cases} \infty, & \text{όταν } g^k \neq e, \forall k\in\mathbb{N} \\ \min\{k\in\mathbb{N} \mid g^k = e\}, & \text{στην αντίθετη περίπτωση} \end{cases}$$

(Εάν G πεπερασμένη $\Rightarrow$ κάθε $g\in G$ έχει πεπερασμένη τάξη).

3.3.23 Παρατήρηση: Εάν $g\in G$, είτε, σύμφωνα με την πρόταση 3.3.20, έχουμε:

$$\boxed{ord(g) = |\langle g\rangle|}$$

3.3.24 Παράδειγμα: Στην $(\mathbb{Z}_4,+)$ τα στοιχεία $[0]_4, [1]_4, [2]_4, [3]_4$ έχουν τάξη 1, 4, 2 και 4 αντιστοίχως.

3.3.25 Πρόταση: Εάν $(G,\cdot)$ μια πεπερασμένη ομάδα. Τότε (η G είναι μυαλιιιή) $\leftrightarrow$ ($\exists g\in G : ord(g) = |G|$)

Απόδειξη: ($\rightarrow$) $\exists g\in G$ $G = \langle g\rangle$ και $ord(g) \overset{3.3.23}{=} |\langle g\rangle| = |G|$

($\leftarrow$) Εάν $\exists g\in G : ord(g) = |G|$ τότε

$$\left.\begin{array}{l} |\langle g\rangle| = |G| \\ \langle g\rangle = G \end{array}\right\} \rightarrow G = \langle g\rangle \left(\begin{array}{l}\text{Προβλ. λήμμα 1.5.5} \\ \text{και παρατήρηση 1.5.6}\end{array}\right)$$

□

3.3.26 Πρόταση: Έστω $(G,\cdot)$ μια ομάδα με το e ως ουδέτερο της στοιχείο. Έστω $g\in G$ με $ord(g) = n (\in\mathbb{N})$. Τότε

$(g^m = e$, για κάποιον $m\in\mathbb{Z}) \Leftrightarrow n \mid m$.

Απόδειξη: ($\Leftarrow$) Εάν $n\mid m \Rightarrow \exists q\in\mathbb{Z} : m = nq$. Επομένως,

$g^m = g^{nq} = (g^n)^q = e^q = e$.

($\Rightarrow$) Εάν $g^m = e$, για κάποιον $m \in \mathbb{Z}$, τότε $\exists (q,r) \in \mathbb{Z}^2$: $m = nq + r$, $0 \leq r < n$. Οπότε συνεπώς, $g^m = g^{nq+r} = (g^n)^q \cdot g^r = (e^n)^q g^r = e \cdot g^r = g^r$. Όμως ο n είναι ο ελάχιστος φυσικός αριθμός για τον οποίο ισχύει $g^m = e$. Άρα $\underline{r = 0} \Rightarrow n \mid m$ □

3.3.27 Πρόταση: Έστω $(G, \cdot)$ μια ομάδα (με το e ως ουδ. στ.) Τότε ισχύουν τα ακόλουθα:

(i) $\text{ord}(g) = \text{ord}(g^{-1})$, $\forall g \in G$.

(ii) $\text{ord}(h^{-1}gh) = \text{ord}(g)$, $\forall (g,h) \in G \times G$

(iii) $\text{ord}(gh) = \text{ord}(hg)$, $\forall (g,h) \in G \times G$.

(iv) Εάν κάθε στοιχείο της G έχει τάξη ≤ 2, τότε η G είναι αβελιανή

Απόδειξη: (i) Υποθέτουμε εν πρώτοις ότι $g \in G$ με $\text{ord}(g) = n \in \mathbb{N}$ Τότε $g^n = e \Rightarrow (g^n)^{-1} = e^{-1} = e \Rightarrow (g^{-1})^n = e$. Για να αποδείξουμε ότι $\text{ord}(g^{-1}) = n$ αρκεί να ισχύει $m \geq n$ για κάθε $m \in \mathbb{N}$ για τον οποίο $(g^{-1})^m = e$. Όμως $(g^{-1})^m = e \Rightarrow$
$\Rightarrow g^{-m} = e \Rightarrow (g^{-m})^{-1} = e^{-1} = e \Rightarrow g^m = e \xrightarrow[3.3.28]{} n \mid m \Rightarrow n \leq m$.

[Και αντιστρόφως εάν $\text{ord}(g^{-1}) = n \in \mathbb{N} \Rightarrow \text{ord}(g) = n$ (εναλλαγή ρόλων)]

Εν συνεχεία υποθέτουμε ότι $\text{ord}(g) = \infty$. Εάν $\text{ord}(g^{-1}) = n \in \mathbb{N}$ τότε θα καταλήγαμε σε άτοπο (διότι συμφώνως προς τα προηγούμενα θα έπρεπε να έχουμε $\text{ord}(g) = n$!). Άρα $\text{ord}(g^{-1}) = \infty$.
[Και αντιστρόφως (εναλλαγή ρόλων)].

(iii) Έστω $(g,h) \in G \times G$ με $\text{ord}(g) = n \in \mathbb{N}$ Καταλήξαμε στην άσκηση 12 του φυλ. 5 ισχύει η ισότητα $(h^{-1}gh)^n = h^{-1}g^n h = h^{-1}h = e$.

Και εάν $m \in \mathbb{N}$, με $(h^{-1}gh)^m = e$, τότε $(h^{-1}gh)^m = h^{-1}g^m h = e$
$\Rightarrow \underbrace{hh^{-1}}_{e} g^m \underbrace{hh^{-1}}_{e} = heh^{-1} = hh^{-1} = e \Rightarrow g^m = e \Rightarrow m \geq n.$

Άρα $ord(h^{-1}gh) = ord(g) = n$.
Εάν $ord(g) = \infty$. Και $ord(h^{-1}gh) = n \in \mathbb{N}$ ($\overset{\text{Πρόκ.}}{\Longrightarrow} n = ord(g)$) Άτοπο!
[Αντίστροφο: Άτοπον].

(iii) $hg = g^{-1}(gh)g \underset{(ii)}{\Rightarrow} ord(hg) = ord(gh)$.

(iv) Εάν $(a,b) \in G \times G$, τότε εξ υποθέσεως, έχουμε

$$\left.\begin{array}{l} a^2 = b^2 = (ab)^2 = e \Rightarrow \\ \end{array}\right\} \begin{array}{l} a = a^{-1} \\ b = b^{-1} \\ (ab)^{-1} = ab \end{array} \Rightarrow$$

$\Rightarrow ab = (ab)^{-1} = b^{-1}a^{-1} = ba$ □

3.3.28 Πρόταση: Έστω $(G, \cdot)$ μια ομάδα (πεπερασμένη) τάξεως $|G| = m \in \mathbb{N}$. Εάν η G είναι κυκλική, παραγόμενη από ένα στοιχείο $g \in G$, και $a := g^n$ (όπου $n \in \mathbb{N}$), τότε:
(i) Το a παράγει μια υποομάδα H της G τάξεως $\frac{m}{\mu\kappa\delta(m,n)}$.

(ii) $H = \langle g^{\mu\kappa\delta(m,n)} \rangle$.

Απόδειξη: (i) Κατά την πρόταση 3.3.21 η $H \overset{"}{\langle a \rangle}$ είναι κυκλική υποομάδα της G. Αρκεί λοιπόν να προσδιορίσουμε την τάξη της. Κατά την 3.3.26, εάν το e είναι το ουδ. στ. της G και $k \in \mathbb{N}$, $a^k = e \Leftrightarrow g^{nk} = e \Leftrightarrow m \mid nk$.
Άρα $|H| = \min\{k \in \mathbb{N} \mid m \mid nk\}$. Έστω $d := \mu\kappa\delta(m,n)$.
Τότε, επί τη βάσει του Θεωρήματος 2.2.5, υπάρχουν $\mu, \nu \in \mathbb{Z}$, τέτοιοι ώστε $d = \mu m + \nu n \overset{(*)}{\Leftrightarrow} 1 = \mu\left(\frac{m}{d}\right) + \nu\left(\frac{n}{d}\right)$. Άρα $\mu\kappa\delta\left(\frac{m}{d}, \frac{n}{d}\right) = 1$. Το ζητούμενο είναι ο προσδιορισμός του

ελαχίστου $k \in \mathbb{N}$: $\frac{nk}{m} = \frac{k(\frac{n}{d})}{(\frac{m}{d})} \in \mathbb{Z}$

: $\frac{m}{d} \mid k$ (βλ. 2.2.10). Κατά συνέπεια, $\min\{k \in \mathbb{N} \mid m \mid nk\} = \frac{m}{d} = |H|$.

(ii) Επειδή $a = g^n = g^{d(\frac{n}{d})} = (g^d)^{\frac{n}{d}} \Rightarrow a = g^n \in \langle g^d \rangle \rightarrow$ Η υποομάδα της $\langle g^d \rangle$. (1)

Από την άλλη μεριά, λόγω της (*), έχουμε

$g^d = g^{\mu m + \nu n} = (g^m)^\mu (g^n)^\nu = e^\mu (g^n)^\nu = e(g^n)^\nu =$

$= (g^n)^\nu \Rightarrow g^d \in \langle a \rangle = H. \Rightarrow \langle g^d \rangle$ υποομ. της H (2)

Από (1), (2) $\rightarrow H = \langle g^d \rangle = \langle g^{\mu\kappa\delta(m,n)} \rangle$

□

3.3.29 Πόρισμα: Έστω ότι n $(G, \cdot)$ είναι μια ομάδα και ότι $(m,n) \in \mathbb{N}^2$. Εάν $g \in G$, τότε ισχύει η ακόλουθη συνεπαγωγή.

$$|ord(g)| = m \Rightarrow ord(g^n) = \frac{m}{\mu\kappa\delta(m,n)}$$

Απόδειξη άμεση από 3.3.28 και ότι $|\langle g \rangle| = ord(g)$

3.3.30 Ειδική περίπτωση: Εάν $n \mid m \Rightarrow ord(g^n) = \frac{m}{n}$.

3.3.31. Παραδείγματα: (i) Εάν n $(G, \cdot)$ είναι μια ομάδα, $g \in G$ με $ord(g) = 12$, τότε π.χ. $ord(g^9) = \frac{12}{\mu\kappa\delta(12,9)} = \frac{12}{3} = 4$,

$ord(g^{10}) = \frac{12}{\mu\kappa\delta(12,10)} = \frac{12}{2} = 6$

(ii) Εντός της $(\mathbb{Z}_{48}, +)$ έχουμε $ord(\overline{47}_{48}) = 12$, όταν

$2\cdot[4]_{48}=[8]_{48}$ $\quad$ $9[4]_{48}=[36]_{48}$

$3\cdot[4]_{48}=[12]_{48}$ $\quad$ $10[4]_{48}=[40]_{48}$

$4[4]_{48}=[16]_{48}$ $\quad$ $11[4]_{48}=[44]_{48}$

$5[4]_{48}=[20]_{48}$ $\quad$ $12[4]_{48}=[48]_{48}=[0]_{48}$

$6[4]_{48}=[24]_{48}$

$7[4]_{48}=[28]_{48}$

$8[4]_{48}=[32]_{48}$

Επομένως τα $[12]_{48}$ και $[20]_{48}$ έχουν τάξη

$$ord(3[4]_{48})=\frac{12}{\mu\kappa\delta(12,3)}=\frac{12}{3}=4$$

$$ord(5[4]_{48})=\frac{12}{\mu\kappa\delta(12,5)}=\frac{12}{1}=12, \text{ αντιστοίχως.}$$

Γενικότερα ισχύει το ακόλουθο.

3.3.32. Πόρισμα: Έστω n ένας φυσικός αριθμός ≥ 2. Τότε $\forall n\in\mathbb{Z}$ η τάξη του $[n]_m$ εντός της $(\mathbb{Z}_m,+)$ δίνεται από τον τύπο

$$\boxed{ord([n]_m)=\frac{m}{\mu\kappa\delta(m,n)}}$$

Απόδειξη: $|\mathbb{Z}_m|=m$

$$\mathbb{Z}_n=\langle[1]_m\rangle \Rightarrow |\langle[1]_m\rangle|=m$$

$$n\cdot[1]_m=[n]_m \underset{3.3.29}{\Longrightarrow} ord([n]_m)=ord(n[1]_m)=\frac{m}{\mu\kappa\delta(m,n)}$$

□

Αλγεβρα - 30/3/06

3.3.33 Πόρισμα: Έστω ότι η $G = \{e, g, g^2, \dots, g^{m-1}\} = \langle g \rangle$ είναι μια πεπ. κυκλική ομάδα τάξεως $m \geq 2$ και ότι $k, l \in \{1, \dots, m-1\}$, τότε:

$$\boxed{\langle g^k \rangle = \langle g^l \rangle \iff \mu\kappa\delta(k,m) = \mu\kappa\delta(l,m)}$$

Απόδειξη: ($\Rightarrow$) $|\langle g^k \rangle| = |\langle g^l \rangle| \Rightarrow$ $\mu\kappa\delta(k,m) = \mu\kappa\delta(l,m)$

$\|$ 3.3.28(i) $\|$

$\frac{m}{\mu\kappa\delta(m,l)}$ $\quad$ $\frac{m}{\mu\kappa\delta(m,l)}$

($\Leftarrow$) Εάν $\mu\kappa\delta(k,m) = \mu\kappa\delta(l,m) =: d \xrightarrow[3.3.28(i)]{} \langle g^{k\theta} \rangle = \langle g^d \rangle = \langle g^l \rangle$

$\square$

3.3.34 Πόρισμα: Έστω ότι η $G = \{e, g, g^2, \dots, g^{m-1}\} = \langle g \rangle$, και ότι $k \in \{1, \dots, m-1\}$. Τότε $\boxed{\langle g^k \rangle = G \iff \mu\kappa\delta(k,m) = 1}$

Ως εκ τούτου, $\boxed{\text{card}(\{\text{γεννήτορες της } G\}) = \varphi(m)}$

βλ. (2.4.18)

3.3.35 Παράδειγμα: $(\mathbb{Z}_8, +)$

$\{\underbrace{[0]_8}_{''}, [1]_8, [2]_8, [3]_8, [4]_8, [5]_8, [6]_8, [7]_8\}$

$\mathbb{Z}_8 = \langle [1]_8 \rangle = \langle [3]_8 \rangle = \langle [5]_8 \rangle = \langle [7]_8 \rangle$

3.3.36 Θεώρημα: Έστω ότι η $G = \{e, g, g^2, \dots, g^{m-1}\} = \langle g \rangle$ είναι μια κυκλική ομάδα τάξεως $m \geq 2$. Τότε ισχύουν τα εξής:

(i) Όταν $n \in \mathbb{N}$, η G διαθέτει μια υποομάδα τάξεως $n \iff n \mid m$.

(ii) Εάν $n \mid m$, τότε η G διαθέτει μια μονοσημάντως ορισμένη υποομάδα τάξεως n

Απόδειξη: (i) ($\Leftarrow$) Εάν $n \mid m \Rightarrow \frac{m}{n} \mid n \xrightarrow[3.3.30]{} \text{card}\left(g^{\frac{m}{n}}\right) =$

$= |\langle g^{\frac{m}{n}} \rangle| = \frac{m}{\frac{m}{n}} = n$, δηλαδή η $\langle g^{\frac{m}{n}} \rangle$ είναι υποομάδα της G τάξεως n. με $|H| = n$

($\Rightarrow$) Έστω H υποομάδα της G. Έστω η H είναι τετριμμένη, τότε δεν χρειάζεται περαιτέρω επιχειρηματολογία.
Εάν $\{e\} \subsetneq H$, τότε $H = \langle g^k \rangle$, για κάποιον $k \in \{1, \ldots, m-1\}$ (πρβλ. 3.3.21(ii)), οπότε (λόγω της 3.3.28 (ii)):
$|H| = \frac{m}{\mu\kappa\delta(k,m)} = n \Rightarrow n | m$.

(ii) Ας υποθέσουμε ότι οι H_1 και H_2 είναι δύο (μη τετριμμένες) υποομάδες της G τάξεως n και ότι $H_1 = \langle g^{k_1} \rangle$, $H_2 = \langle g^{k_2} \rangle$. Τότε $|H_1| = \frac{m}{\mu\kappa\delta(k_1,m)} = n = \frac{m}{\mu\kappa\delta(k_2,m)} = |H_2| \Rightarrow$

$\Rightarrow \mu\kappa\delta(k_1,m) = \mu\kappa\delta(k_2,m) \Rightarrow \underbrace{\langle g^{k_1} \rangle}_{H_1} = \underbrace{\langle g^{k_2} \rangle}_{H_2}$

□

<u>3.3.37 Πόρισμα:</u> Έστω ότι η $G = \{e, g, g^2, \ldots, g^{m-1}\} = \langle g \rangle$ είναι μια κυκλική ομάδα τάξεως $m \geq 2$ και ότι $d_1, d_2, \ldots, d_\nu$ είναι οι θετικοί διαιρέτες του m. Τότε οι $\langle g^{d_1} \rangle, \langle g^{d_2} \rangle, \ldots, \langle g^{d_\nu} \rangle$ είναι όλες οι σαφώς διακεκριμένες (ήτοι οι διαφορετικές μεταξύ τους ανά ζεύγη) υποομάδες της G.

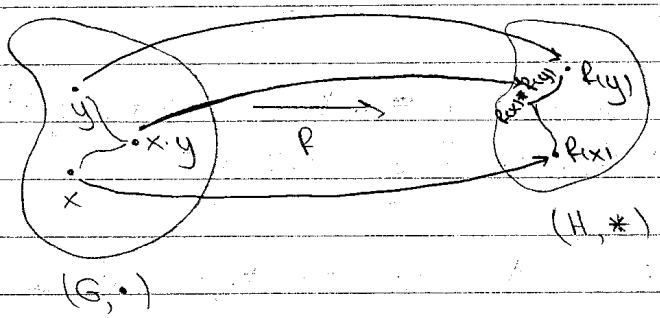
<u>Απόδειξη:</u> Επειδή $d_j | m$, $\forall j \in \{1, 2, \ldots, \nu\}$, έχουμε $\mu\kappa\delta(d_j, m) = d_j$. Εάν λοιπόν για κάποιους $j, j' \in \{1, \ldots, \nu\}$ ισχύει $\langle g^{d_j} \rangle = \langle g^{d_{j'}} \rangle$, τότε $|\langle g^{d_j} \rangle| = |\langle g^{d_{j'}} \rangle| \Rightarrow$
$\Rightarrow \underbrace{\mu\kappa\delta(d_j, m)}_{d_j} = \underbrace{\mu\kappa\delta(d_{j'}, m)}_{d_{j'}}$

□

3.3.38 Παράδειγμα: $(\mathbb{Z}_8, +)$. Υποομάδες της:
$\{[0]_8\}$
$\langle [2]_8 \rangle = \{[0]_8, [2]_8, [4]_8, [6]_8\}$
$\langle [4]_8 \rangle = \{[0]_8, [4]_8\}$

§3.4 ΟΜΟΜΟΡΦΙΣΜΟΙ ΟΜΑΔΩΝ

3.4.1 Ορισμός: Έστω ότι οι $(G, \cdot)$ και $(H, *)$ είναι δυο ομάδες. Μια απεικόνιση $f: G \to H$ καλείται ομομορφισμός (ομάδων) όταν



$$f(x \cdot y) = f(x) * f(y), \quad \forall (x, y) \in G \times G$$

3.4.2 Παραδείγματα: (i) Εάν η G είναι μια ομάδα και η U μια υποομάδα της, τότε η συνήθης ενδεική απεικόνιση $i: U \to G$ είναι ομομορφισμός.

(ii) Εάν $\alpha \in \mathbb{R}$ και ορίσουμε την $\mu_\alpha: (\mathbb{R}, +) \to (\mathbb{R}, +)$, τότε η μ_α είναι ομομορφισμός

$$x \longmapsto \mu_\alpha(x) := \alpha x$$ διότι
$$\mu_\alpha(x+y) = \alpha(x+y) = \alpha x + \alpha y = \mu_\alpha(x) + \mu_\alpha(y)$$
$$\forall (x, y) \in \mathbb{R} \times \mathbb{R}.$$

(iii) $(\mathbb{R}, +) \to (\mathbb{R} - \{0\}, \cdot)$
$$x \longmapsto e^x (= \exp(x))$$

3.4.3 Πρόταση: Εάν η $f: (G, \cdot) \to (H, *)$ είναι ομομορφισμός, τότε $f(e_G) = e_H$ (όπου e_G, e_H τα ουδ. στ. των G και H

αντιστοίχως) και η εικόνα του συμμετρικού στοιχείου $[g^{-1}]$

ενός $g \in G$ μέσω της f ταυτίζεται με το συμμετρικό στοιχείο του $f(g)$ εντός της H. $[f(g^{-1})]$

Απόδειξη: $f(e_G) * f(e_G) = f(e_G \cdot e_G) = f(e_G) \Rightarrow$

$\Rightarrow f(e_G) * \underbrace{f(e_G)}_{e_H} * f(e_G)^{-1} = \underbrace{f(e_G) * f(e_G)^{-1}}_{e_H} \Rightarrow f(e_G) = e_H.$

Επίσης, για κάθε $g \in G$, $f(g) * f(g^{-1}) = f(gg^{-1}) = f(e_G) =$
$= f(g^{-1}g) = f(g^{-1}) * f(g) \Rightarrow f(g^{-1}) = f(g)^{-1}$

3.4.4 Πρόταση: Εάν η $f:(G,\cdot) \to (H,*)$ είναι ομομορφισμός τότε

(i) Η εικόνα $f(M)$ οποιασδήποτε υποομάδας M της G μέσω της f είναι υποομάδα της H.

(ii) Η αντίστροφη εικόνα $f^{-1}(N)$ —″— N —″— H —″— —″— G.

Απόδειξη: (i) Εάν $u, v \in f(M) \Rightarrow \exists x, y \in M : f(x) = u, f(y) = v$.
Κατά συνέπειαν, $u * v^{-1} = f(x) * f(y)^{-1} = f(x) * f(y^{-1})$
$= f(x \cdot y^{-1}) \in f(M)$, οπότε η $f(M)$ αποτελεί υποομάδα της H βάσει της προτάσεως 3.3.8

(ii) άσκηση

□

3.4.5 Πόρισμα: Εάν η $f:(G,\cdot) \to (H,*)$ είναι ομομορφισμός, τότε

(i) η εικόνα $Im(f) := f(G)$ της G είναι υποομάδα της H.

(ii) Το σύνολο $\boxed{Ker(f) = f^{-1}(\{e_H\}) = \{g \in G \mid f(g) = e_H\}}$, το

οποίο καλείται ιδιαιτέρως πυρήνας της f είναι μια υποομάδα της G.

3.4.6 Ορισμός: Έστω $f:(G,\cdot)\to(H,*)$ ομομορφισμός ομάδων. Ο f καλείται

μονομορφισμός $\overset{\text{ορ.}}{\iff}$ η αντίστοιχη f είναι ένριψη

επιμορφισμός $\overset{\text{ορ.}}{\iff}$ —" — επίριψη

ισομορφισμός $\overset{\text{ορ.}}{\iff}$ —" — αμφίριψη

ενδομορφισμός $\overset{\text{ορ.}}{\iff}$ $(G,\cdot)=(H,*)$

αυτομορφισμός $\overset{\text{ορ.}}{\iff}$ η f είναι αμφιριπτικός ενδομορφισμός.

3.4.7 Παραδείγματα: (i) $(\mathbb{R},+)\to(\mathbb{R}_{>0},\cdot)$

$x\longmapsto \exp(x)$ ισομορφισμός με την $\log(x)$ ως αντίστροφό της.

(ii) Οι ομομορφισμοί μ_α (οι οριοθέτησες στο 3.4.2(ii)) είναι αυτομορφισμοί της $(\mathbb{R},+)$ $\forall \alpha\in\mathbb{R}\setminus\{0\}$ με τους $\mu_{\frac{1}{\alpha}}$ ως αντίστροφους τους. Ο μ_0 είναι προφανώς ο μηδενικός ενδομορφισμός.

3.4.8 Παρατήρηση: Σημειωτέον ότι η σύνθεση δύο ομοειδών «...μορφισμών» από τον αντίστοιχο κατάλογο μας δίνει έναν «...μορφισμό» του ίδιου είδους (βλ. Πρόταση 1.2.15 (i), (iii))

3.4.9 Πρόταση: Έστω ομομορφισμός ομάδων $f:(G,\cdot)\to(H,*)$ είναι μονομορφισμός $\iff \ker(f)=\{e_G\}$

Απόδειξη: ($\Rightarrow$) $\forall g\in\ker(f): f(g)=e_H=f(e_G)\xrightarrow[f\text{ ένριψη}]{} g=e_G$,

οπότε $\ker(f)=\{e_G\}$.

($\Leftarrow$) Εάν $\ker(f) = \{e_G\}$ και $f(g_1) = f(g_2)$, για κάποια $g_1, g_2 \in G$, τότε $f(g_2^{-1} g_1) = f(g_2)^{-1} * f(g_1) = f(g_2)^{-1} * f(g_2) = e_H$ οπότε $g_2^{-1} \cdot g_1 = e_G \Rightarrow g_1 = g_2$, δηλ. η f είναι όντως μια ένριψη.

□

3.4.10 Σημείωση: Λέμε πως δυο ομάδες $(G, \cdot)$ και $(H, *)$ είναι (μεταξύ τους) ισόμορφες (και σημειώνουμε $G \cong H$) όταν υπάρχει (τουλάχιστον) ένας ισομορφισμός ομάδων $f: (G, \cdot) \to (H, *)$. Είναι εύκολο να αποδειχθεί ότι η "$\cong$" είναι σχέση ισοδυναμίας επί της "πλάσεως" όλων των ομάδων. Ως εκ τούτου, δυο ομάδες λογίζονται ως (ομαδοθεωρητικώς) ταυτιζόμενες όταν είναι μεταξύ τους ισόμορφες. Το ακόλουθο ενδιαφέρον θεώρημα μας παρέχει τη δυνατότητα πλήρους ταξινομήσεως όλων των κυκλικών ομάδων "μέχρις ισομορφισμού"

3.4.11 Θεώρημα: Έστω $(G, \cdot)$ μια κυκλική ομάδα. Εάν η $(G, \cdot)$ είναι άπειρη κυκλική τότε είναι κατ' ανάγκην ισόμορφη με την $(\mathbb{Z}, +)$. Διαφορετικά, $(G, \cdot) \cong (\mathbb{Z}_m, +)$, όπου $m := |G|$.

Απόδειξη: Έστω ότι $G = \langle g \rangle$ $(g \in G)$. Εάν η $(G, \cdot)$ είναι άπειρη κυκλική, τότε η απεικόνιση $(\mathbb{Z}, +) \longrightarrow (G, \cdot)$ είναι ισομορφισμός ομάδων
$n \longmapsto g^n$ (άσκηση).

Εάν $(G, \cdot)$ πεπερασμένη τάξεως $m = |G|$, $G = \{e, g, g^2, \ldots, g^{m-1}\}$ ο ζητούμενος ισομορφισμός είναι ο $(\mathbb{Z}_m, +) \to (G, \cdot)$
$[n]_m \to g^n, \forall n \in \{0, \ldots, m\}$
(άσκηση)

□

Άλγεβρα - 4/4/06

3.4.12 Σημείωση: Έστω η G είναι τυχούσα ομάδα, τότε το ζεύγος $(Aut(G), \circ)$ όπου:
$Aut(G) := \{f: G \to G \mid f$ αυτομορφισμός ομάδων$\}$ αποτελεί μια ομάδα. Επί παραδείγματι, έστω $G = \mathbb{Z}$ η (προσθετική) ομάδα των ακεραίων, τότε κάθε $\theta \in Aut(\mathbb{Z})$ πρέπει να στέλνει το 1 να απεικονίζεται σε έναν ακέραιο αριθμό που παράγει τον $\mathbb{Z}$ καταρχήν συνέπειαν, $\theta(1) \in \{\pm 1\}$. Έστω $\theta(1) = 1 \Rightarrow \theta = Id_{\mathbb{Z}}$, ενώ έστω $\theta(1) = -1$ τότε $\theta(n) = -n \ \forall n \in \mathbb{Z}$. Ως εκ τούτου, $Aut(\mathbb{Z}) \cong \mathbb{Z}_2$.

§3.5 ΟΜΑΔΕΣ ΜΕΤΑΤΑΞΕΩΝ

3.5.1 Ορισμός: Έστω A ένα μη κενό σύνολο και $S_A := \{\sigma: A \to A \mid \sigma$ αμφίρριψη$\} \subseteq \Pi(A, A)$. Το ζεύγος $(S_A, \circ)$ αποτελεί μια ομάδα, την λεγόμενη συμμετρική ομάδα επί του A. Από "ομαδοθεωρητική" άποψη, η ομάδα S_A δεν εξαρτάται από το ίδιο το σύνολο A, αλλά μόνο από τον πληθικό του αριθμό $card(A)$. (Πράγματι, έστω το B είναι ένα άλλο μη κενό σύνολο με $card(A) = card(B)$, τότε $\exists f: A \to B$ αμφίρριψη οπότε η απεικόνιση: $S_A \to S_B$, $\sigma \mapsto f^{\vee} \circ \sigma \circ f$ είναι ένας ισομορφισμός ομάδων (άσκηση). Έστω το θεωρούμενο σύνολο A είναι πεπερασμένο με $card(A) = n$, μπορούμε δίχως βλάβη της γενικότητας να υποθέσουμε ότι $A = \{1, 2, \dots, n\}$. Σε αυτή την περίπτωση, συμβολίζουμε την S_A ως S_n (συμμετρική ομάδα σε n σύμβολα).

3.5.2 Ορισμός: Κάθε στοιχείο της S_n ονομάζεται μετάταξη. Συνήθως γράφουμε τις μεταταξεις $\sigma \in S_n$ υπό την μορφή

$$\begin{bmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{bmatrix}, \quad n \begin{bmatrix} x_1 & x_2 & \dots & x_n \\ \sigma(x_1) & \sigma(x_2) & \dots & \sigma(x_n) \end{bmatrix}$$

στην περίπτωση που τα $x_1, x_2, \dots, x_n$ αποτελούν κάποια αναδιάταξη των $1, 2, \dots, n$. Αυτός ο τρόπος γραφής μας διευκολύνει κατά τον υπολογισμό της συνθέσεως δύο μεταθέσεων:

$\tau, \sigma \in S_n$

$$\begin{bmatrix} 1 & \dots & n \\ \tau(\sigma(1)) & \dots & \tau(\sigma(n)) \end{bmatrix} = \begin{bmatrix} 1 & \dots & n \\ \tau(1) & \cdots & \tau(n) \end{bmatrix} \circ \begin{bmatrix} 1 & \dots & n \\ \sigma(1) & \cdots & \sigma(n) \end{bmatrix}$$

π.χ.

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

3.5.3 Παρατήρηση: (i) Έαν $\sigma \in S_n$, τότε σ^{-1} γράφεται

$$\begin{bmatrix} 1 & \dots & n \\ \sigma(1) & \cdots & \sigma(n) \end{bmatrix} \quad \begin{bmatrix} \sigma(1) & \cdots & \sigma(n) \\ 1 & \dots & n \end{bmatrix}$$

(iii) Για λόγους συντομίας θα συμβολίζουμε το ουδέτερο στοιχείο του S_n απλώς ως Id (αντί του Id_{S_n})

(iii) Όταν $n \geq 3$ η S_n δεν είναι αβελιανή. Πράγματι ορίζοντας τις $\sigma, \tau \in S_n$ ως ακολούθως:

$$\begin{cases} \sigma(1)=1, \sigma(2)=3, \sigma(3)=2, \sigma(i)=i \ \forall i \in \{4, \dots, n\} \\ \tau(1)=2, \tau(2)=1, \tau(3)=3, \tau(i)=i \ \forall i \in \{4, \dots, n\} \end{cases}$$

λαμβάνουμε

$(\tau\circ\sigma)(1) = 2 \neq 3 = (\sigma\circ\tau)(1) \Rightarrow \tau\circ\sigma \neq \sigma\circ\tau$

3.5.4 Πρόταση: $|S_n| = n!$

Απόδειξη: Με τη βοήθεια της μαθηματικής επαγωγής θα αποδείξουμε χαλαρότερα του ακόλουθο ισχυρισμό:

Ισχυρισμός: Έαν τα $A = \{x_1, \dots, x_n\}$ και $B = \{y_1, \dots, y_n\}$ είναι δύο σύνολα που περιέχουν (ακριβώς) n στοιχεία, τότε το σύνολο $B_{ij}(A,B) = \{f : A \to B \mid f \text{ αμφίρριψη}\}$ έχει ακριβώς $n!$

στοιχεία.

Απόδειξη Ισχυρισμού: Για $n=1$, προφανώς. Ας υποθέσουμε ότι για κάποιο $n>1$ ισχύει η $\mathrm{card}(B_{i;j}(A',B'))=(n-1)!$ για κάποια A',B' που περιέχουν ακριβώς $n-1$ στοιχεία. Για κάθε $i\in\{1,\dots,n\}$ ορίζουμε το: $B_{i;j}=\{R\in B_{i;j}(A,B)\mid R(x_i)=y_i\}$.
Προφανώς η απεικόνιση

$$\begin{array}{ccc} B_{i;j}(A,B)_i & \longrightarrow & B_{i;j}(A\setminus\{x_i\},B\setminus\{y_i\}) \\ \cup & & \cup \\ R & \longmapsto & R|_{A\setminus\{x_i\}} \end{array}$$

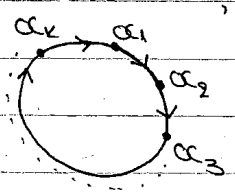
είναι αμφιμονοσήμαντη. Κατά την επαγωγική υπόθεση:
$\mathrm{card}(B_{i;j}(A,B)_i)=(n-1)!\ ,\forall i\in\{1,\dots,n\}$.
Επιπροσθέτως, $B_{i;j}(A,B)=\coprod_{i=1}^{n} B_{i;j}(A,B)_i$ $\xrightarrow[1.3.5]{1.3.4(iii)}$

$$\mathrm{card}(B_{i;j}(A,B))=\sum_{j=1}^{n}\mathrm{card}(B_{i;j}(A,B)_i)=n(n-1)!=n!$$

□

3.5.5 Ορισμός: (i) Μια μετάταξη $\sigma\in S_n$ λέγεται κύκλος μήκους k (ή k-κύκλος) όταν υπάρχουν k διαφορετικοί αριθμοί $\alpha_1,\dots,\alpha_k$ από το $\{1,\dots,n\}$ $(1\le k\le n)$ έτσι ώστε να ισχύει

$$\begin{cases}\sigma(\alpha_1)=\alpha_2,\ \sigma(\alpha_2)=\alpha_3,\dots\sigma(\alpha_{k-1})=\alpha_k,\ \sigma(\alpha_k)=\alpha_1\\ \sigma(\beta)=\beta,\ \forall\beta\in\{1,\dots,n\}\setminus\{\alpha_1,\dots,\alpha_k\}.\end{cases}$$



συμβολισμός: $[\alpha_1\ \alpha_2\dots\alpha_k]$
(ii) Δύο κύκλοι $[\alpha_1\ \alpha_2\dots\alpha_k]$ και $[\beta_1\ \beta_2\dots\beta_l]$ λέμε ότι είναι ξένοι μεταξύ τους όταν $\{\alpha_1,\dots,\alpha_k\}\cap\{\beta_1,\dots,\beta_l\}=\emptyset$
(iii) Οι 2-κύκλοι ονομάζονται επίσης και αντιμεταθέσεις.

3.5.6 Πρόταση: Οι k-κύκλοι έχουν τις ακόλουθες ιδιότητες:
(i) $[\alpha_1\alpha_2\dots\alpha_k]=[\alpha_2\alpha_3\dots\alpha_k\alpha_1]=[\alpha_k\alpha_1\dots\alpha_{k-1}]$ είναι κυκλικές εναλλαγές των k στοιχείων ενός k-κύκλου αμφι-

νουν τον κύκλο αναλλοίωτο.

(ii) $[\alpha_1\alpha_2\dots\alpha_k]=[\alpha_1\dots\alpha_j]\circ[\alpha_j\alpha_{j+1}\dots\alpha_k]$ $\forall j\in\{2,3,\dots,k-1\}$

(iii) $[\alpha_1\alpha_2\dots\alpha_k]=[\alpha_1\alpha_2]\circ[\alpha_2\alpha_3]\circ\dots\circ[\alpha_{k-1}\alpha_k]$

(iv) $[\alpha_1\alpha_2\dots\alpha_k]^m=\begin{bmatrix}\alpha_1 & \dots & \alpha_k\\ \alpha_{m+1} & & \alpha_{m+k}\end{bmatrix}$, όπου οι δείκτες της

κάτω γραμμής οφείλουν να "διαβάζονται" κατά μόδιο k, ήτοι $\alpha_{k+1}=\alpha_1,\alpha_{k+2}=\alpha_2,\dots,\alpha_{k+t}=\alpha_t$ όπου $t=l(\mathrm{mod}\,k)$

(v) $\mathrm{ord}([\alpha_1\dots\alpha_k])=k$

(vi) $[\alpha_1\dots\alpha_k]^{-1}=[\alpha_k\alpha_{k-1}\dots\alpha_2\alpha_1]$.

Απόδειξη: Το (i) είναι εξ' ορισμού προφανές.

Το (ii) είναι άμεση συνέπεια του υπολογισμού του "γινομένου" (=συνθέσεως). (Ο στόχος, θα πρέπει να σημειωθεί ότι σε αυτή σύνθεση προηγείται η εφαρμογή της δεξιάς αντιμετάθεσης και έπεται η εφαρμογή της αριστερής).

Το (iii) έπεται από το (ii) (όταν $j=2$) κατόπιν χρήσεως μαθηματικής επαγωγής (άσκηση).

Το (iv) έπεται κατ' αρχάς μέσω μαθηματικής επαγωγής

$$[\alpha_1\dots\alpha_k]^{m+1}=\begin{bmatrix}\alpha_1 & \alpha_k\\ \alpha_{m+1} & \alpha_{m+k}\end{bmatrix}\circ\begin{bmatrix}\alpha_1 & \alpha_k\\ \alpha_2 & \alpha_{k+1}\end{bmatrix}=\begin{bmatrix}\alpha_1 & \dots & \alpha_k\\ \alpha_{m+1} & & \alpha_{m+1+k}\end{bmatrix}$$

(v) Έστω $\sigma:=[\alpha_1\dots\alpha_k]$. Από την (iv) λαμβάνουμε:

$$\sigma^k=[\alpha_1\dots\alpha_k]^k=\begin{bmatrix}\alpha_1 & \dots & \alpha_k\\ \alpha_{k+1} & & \alpha_{k+k}\end{bmatrix}=\begin{bmatrix}\alpha_1 & \dots & \alpha_k\\ \alpha_1 & \dots & \alpha_k\end{bmatrix}=Id$$

Εάν $\rho\in\mathbb{N}$, $\rho\in\{1,2,\dots,k-1\}$, τότε $\sigma^\rho(\alpha_i)=\alpha_{i+\rho}$, $\forall i\in\{1,\dots,k\}$ $\Rightarrow i+\rho\not\equiv i(\mathrm{mod}\,k)\Rightarrow\sigma^l\neq Id$. Άρα $\mathrm{ord}([\alpha_1\dots\alpha_k])=k$.

(vi) $[\alpha_1\dots\alpha_k]^{-1}\underset{(v)}{=}[\alpha_1\dots\alpha_k]^{k-1}\underset{(iv)}{=}\begin{bmatrix}\alpha_1 & \dots & \alpha_k\\ \alpha_k & & \alpha_{2k-1}\end{bmatrix}=$

$=\begin{bmatrix}\alpha_1 & \dots & \alpha_k\\ \alpha_k & \dots & \alpha_{k-1}\end{bmatrix}=[\alpha_k\alpha_{k-1}\dots\alpha_1]$ □

α_{2k-1}: $(k-1)+k\equiv(k-1)\ \mathrm{mod}\,k$

3.5.7 Λήμμα: Δύο τυχόντες κύκλοι (ανήκουν στον S_n), οι οποίοι είναι ξένοι μεταξύ τους, μετατίθενται αμοιβαίως.

Απόδειξη: Θεωρούμε δύο τέτοιους κύκλους $\sigma=[\alpha_1\alpha_2\dots\alpha_k]$
$\tau=[\beta_1\beta_2\dots\beta_l]$
(με $\{\alpha_1,\dots\alpha_k\}\cap\{\beta_1,\dots\beta_l\}=\emptyset$).
Θα δείξουμε ότι $\sigma\circ\tau(j)=\tau\circ\sigma(j)$, $\forall j\in\{\alpha_1,\dots\alpha_k\}\cup\{\beta_1,\dots,\beta_l\}$.
Παρατηρούμε ότι $\sigma\circ\tau(\alpha_\rho)=\sigma(\alpha_\rho)=\tau\circ\sigma(\alpha_\rho)$, $\forall\rho\in\{1,\dots,k\}$, διότι η τ δεν "κινεί" ούτε το α_ρ ούτε το $\sigma(\alpha_\rho)=\alpha_{\rho+1}$ (και το $\sigma(\alpha_k)=\alpha_1$)
Ανακλόγως, $\sigma\circ\tau(\beta_\nu)=\tau\circ\sigma(\beta_\nu)$, $\forall\nu\in\{1,\dots,l\}$ □

3.5.8 Θεώρημα: Κάθε (μη ταυτοτική) μετάταξη από την S_n, $n\geq 2$ μπορεί να γραφεί είτε ως ένας κύκλος είτε ως μια πεπερασμένη ακολουθία συντιθέμενων, ανά δύο ξένων μεταξύ τους κύκλων μήκους ≥ 2. Και μάλιστα, μια τέτοια έκφραση είναι μονοσημάντως ορισμένη (ενδεχομένως ίσως από κάποιους αναδιάταξη των μετεχόντων κύκλων).

Απόδειξη: Όταν $n=2$, έχουμε $S_2=\{Id,[1\,2]\}$, οπότε ο ισχυρισμός είναι αληθής αφού $Id=[1\,2]\circ[1\,2]$. Υποθέτουμε ότι είναι αληθής για δοθέν $n\geq 2$ θα αποδείξουμε επαγωγικώς την ορθότητα του και για το $n+1$. Έστω λοιπόν $\sigma\in S_{n+1}\setminus\{Id\}$
1η περίπτωση: $\boxed{\sigma(n+1)=n+1}$. Τότε το $\sigma':\sigma|_{\{1,\dots,n\}}:\{1,\dots,n\}\to\{1,\dots,n\}$
είναι ένα στοιχείο της S_n. Από την επαγωγική υπόθεση:
$\sigma'=\underbrace{c'_1\circ\dots\circ c'_\nu}_{\substack{\text{σύνθεση ανά}\\ \text{2 ξένων κύκλων}\\ \geq 2\\ (\nu\in\mathbb{N})}}$. Έστω c_j η επέκταση του κύκλου
c_j που ορίζεται από τον τύπο: $c_j:\{1,\dots,n+1\}\to\{1,\dots,n+1\}$.

$$\boxed{c_j(l)=\begin{cases}c'_j(l), & 1\leq l\leq n\\ n+1, & l=n+1\end{cases}\quad\forall j\in\{1,\dots,\nu\}}$$ Αλλιώς τότε

$\boxed{\sigma = C_1 \circ \dots \circ C_\nu}$

2η περίπτωση: $\boxed{\sigma(n+1) \neq n+1}$ Επειδή το σύνολο των $n+2$ αμερσίων: $n+1, \sigma(n+1), \sigma^2(n+1), \dots, \sigma^{n+1}(n+1)$ περιέχεται στο $\{1,2,\dots,n+1\}$ θα υπάρχουν $(k,l) \in \{0,\dots,n+1\}^2$, $k<l$, με $\sigma^k(n+1) = \sigma^l(n+1)$. Θέτοντας $m := l-k$, έχουμε $\sigma^m(n+1) = n+1$. Επειδή το $\{q \in \{1,\dots,n+1\} \mid \sigma^q(n+1) = n+1\}$ είναι μη κενό υποσύνολο του $\mathbb{N}$, από την αρχή του καλού διατάξεως θα περιέχει ελάχιστο στοιχείο, ας το πούμε ρ.

Ισχυρισμός: $\operatorname{card}(\{n+1, \sigma(n+1), \sigma^2(n+1), \dots, \sigma^{\rho-1}(n+1)\}) = \rho$.

Πράγματι: εάν οι ρ αμέρσιοι $n+1, \sigma(n+1), \dots, \sigma^{\rho-1}(n+1)$ δεν ήταν ασφαλώς διαφορετικοί, τότε θα υπήρχαν $(k,l) \in \{0,1,\dots,\rho-1\}^2$, $k<l$, με $\sigma^k(n+1) = \sigma^l(n+1)$. Θέτοντας ως $q := l-k$, θα έχουμε $\sigma^q(n+1) = n+1$ με $q \leq \rho-1$, πράγμα άτοπο λόγω της επιλογής του ρ.

Έστω $C := [n+1 \ \sigma(n+1) \dots \sigma^{\rho-1}(n+1)]$ και έστω $\boxed{\rho := C^{-1} \circ \sigma}$. Τότε $\rho(n+1) = C^{-1}(\sigma(n+1)) = n+1$. Τώρα εμπίπτουμε με στην 1η περίπτωση για το εν λόγω ρ $\Rightarrow$

$\Rightarrow \exists \underbrace{C_1, \dots, C_\nu}_{\text{κύκλοι ξένοι με μήκους} \geq 2} \in S_{n+1} : \rho = C_1 \circ \dots \circ C_\nu$

Επειδή τα $\rho(n+1) = n+1, \rho(\sigma(n+1)) = \sigma(n+1), \dots, \rho(\sigma^{\rho-1}(n+1)) = \sigma^{\rho-1}(n+1)$ μένουν "αμετάβλητα" οι κύκλοι $C_1, C_2, \dots, C_\nu$ δεν περιέχουν κανένα στοιχείο από τα $n+1, \sigma(n+1), \dots, \sigma^{\rho-1}(n+1)$, δίοτι είναι μήκους ≥ 2

$\Rightarrow \boxed{\sigma = C \circ C_1 \circ C_2 \circ \dots \circ C_\nu}$

Το "μοναδικό" αυτής της χωρίσης

Έστω $\sigma = \underbrace{C_1 \circ \dots \circ C_\nu}_{\text{κύκλοι ξένοι μεταξύ τους μήκους} \geq 2} = \underbrace{d_1 \circ \dots \circ d_{\nu'}}_{\text{κύκλοι ξένοι μεταξύ τους μήκους} \geq 2}$, $\nu, \nu' \in \mathbb{N}$.

$\sigma \in S_n$ [ξένοι]

Επειδή $\sigma \neq Id \Rightarrow \exists i \in \{1,\dots,n\} : \sigma(i) \neq i$ καθώς και
$r \in \{1,\dots,v\}$
$r' \in \{1,\dots,v'\}$: $i \in \underbrace{C_r \cap d_{r'}}_{\text{συνολοθεωρητικά}}$

Όπως και προηγουμένως, $\exists \rho \in \mathbb{N}$: $\begin{cases} i, \sigma(i), \dots, \sigma^{\rho-1}(i) \text{ να είναι} \\ \text{σαφώς διαμεριμένοι} \\ \text{και } \sigma(i) = i \end{cases}$

οπότε $C_r = d_{r'} = [i, \sigma(i) \dots \sigma^{\rho-1}(i)] \Rightarrow v = v'$ και
$\{C_1, \dots, C_v\} = \{d_1, \dots, d_{v'}\}$

□

Άλγεβρα – 6/4/06

3.5.9 Πόρισμα: Κάθε μετάταξη εκτός της S_n, $n \geq 2$, μπορεί να γραφεί υπό τη μορφή επάλληλων αντιμεταθέσεων (=2 κύκλων)

Απόδειξη
Άμεση από το Θεώρημα 3.5.8 και την Πρ. 3.5.6 (iii) □

3.5.10 Παρατήρηση: Ο αντίστροφος τρόπος γραφής (σε αντίθεση με ό,τι ισχύει για τους κύκλους στο Θ.3.5.8) δεν είναι μονοσημάντως ορισμένος. Π.χ.

$$\begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 4 & 3 & 6 & 1 & 2 & \end{bmatrix} = [15]\circ[246] = [15]\circ[26]\circ[24]$$

Επειδή $[246] = [624]$, μπορούμε να γράψουμε αυτό το στοιχείο της S_6 και ως

$$\begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 4 & 3 & 6 & 1 & 2 \end{bmatrix} = [15]\circ[624] = [15]\circ[64]\circ[62] =$$

$$= [15]\circ[46]\circ[26]$$

3.5.11 Ορισμός: (i) Έστω $\sigma \in S_n$ μια μετάταξη. Ορίζουμε ως παραβατικό ζεύγος (για την σ) κάθε διατεταγμένο ζεύγος $(i,j) \in \{1,2,\ldots,n\} \times \{1,2,\ldots,n\}$ για το οποίο ισχύει η συνεπαγωγή
$i < j \Rightarrow \sigma(i) > \sigma(j)$
(ii) Ως αρτιόνιση προσημάνσεως (των στοιχείων της S_n) ορίζουμε την απεικόνιση

$$sgn : (S_n, \circ) \to (\{\pm 1\}, \cdot)$$

μέσω του τύπου:

$$sgn(\sigma) = \begin{cases} +1, & \text{όταν η } \sigma \text{ διαθέτει άρτιο αριθμό παραβατικών ζευγών} \\ -1, & \text{---''---} \quad \underline{\text{περιττό}} \text{---} \\ & \text{---''---} \quad \text{---} \end{cases}$$

(iii) Μια μετάθεση σε S_n ονομάζεται *άρτια* (αντ. *περιττή*) όταν $\mathrm{sgn}(\sigma) = +1$ (αντ. $= -1$)

3.5.12 Παράδειγμα: Τα παραβατικά ζεύγη της

$\sigma := \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{bmatrix}$ είναι τα $(1,2)$ και $(3,4)$ (οπότε $\mathrm{sgn}(\sigma) =$

3.5.13 Λήμμα: Για κάθε αντιμετάθεση ($=$ 2-κύκλο) της S_n $\overset{n \geq 2}{\forall}$ έχουμε $\mathrm{sgn}(\sigma) = -1$.

Απόδειξη

Έστω $\tau = [i\ j]$. Αρκεί να υπολογίσουμε το πλήθος των παραβατικών ζευγών της. Γράφοντας την σε πλήρη έκταση, λαμβάνουμε $\tau = \begin{bmatrix} 1 & \dots & i-1 & \boxed{i} & i+1 \dots & \boxed{j} & j+1 \dots n \\ 1 & & i-1 & \boxed{j} & i+1 \dots & \boxed{i} & j+1 \dots n \end{bmatrix}$

Προφανώς, τα παραβατικά ζεύγη – πέραν του ίδιου του (i,j) – ανήκουν στην ένωση δύο συνόλων
$\{(i,k) \mid i+1 \leq k \leq j-1\} \cup \{(l,j) \mid i+1 \leq l \leq j-1\}$.
Επειδή καθένα εξ αυτών έχει πληθικό αριθμό ίσον με $j-i-1$, η τ διαθέτει εν συνόλω $2(j-i-1)+1$ παραβατικά ζεύγη (ήτοι έναν *περιττό* αριθμό παραβατικών ζευγών). □

3.5.14 Λήμμα: Η αμφί που λαμβάνει οιαδήποτε μετάταξη σε S_n μέσω της απεικονίσεως sgn μπορεί να εκφρασθεί με τη βοήθεια του ακολούθου «ιδιότυπου τύπου»:

$$\mathrm{sgn}(\sigma) = \prod_{1 \leq i < j \leq n} \frac{\sigma(j) - \sigma(i)}{j - i}$$

Απόδειξη

Έστω s ο αριθμός των παραβατικών ζευγών (για την σ).

Τότε $\prod_{1\le i<j\le n}(\sigma(j)-\sigma(i)) = \left(\prod_{\substack{1\le i<j\le n\\ \sigma(i)<\sigma(j)}}(\sigma(j)-\sigma(i))\right)(-1)^s\left(\prod_{\substack{1\le i<j\le n\\ \sigma(i)>\sigma(j)}}|\sigma(j)-\sigma(i)|\right)$

$= (-1)^s \prod_{1\le i<j\le n}|\sigma(j)-\sigma(i)| = (-1)^s \prod_{1\le i<j\le n}(j-i)$. □

3.5.15 Θεώρημα: (i) Για τυχούσες $\sigma,\tau\in S_n$ έχουμε

$$\boxed{Sgn(\tau\circ\sigma) = Sgn(\tau)\cdot Sgn(\sigma)}$$

(ήτοι η Sgn είναι ομομορφισμός ομάδων).

(ii) Για κάθε $\sigma\in S_n$ έχουμε $\boxed{Sgn(\sigma) = Sgn(\sigma^{-1})}$

(iii) Εάν η $\sigma=\tau_1\circ\dots\circ\tau_k\in S_n$ συνίσταται από k αντιμεταθέσεις (=2-κύκλους) $\tau_1,\dots,\tau_k$ (Πρβλ. 3.5.9), τότε

$$\boxed{Sgn(\sigma) = (-1)^k}$$

(iv) Εάν μια μετάταξη $\sigma\in S_n$ γράφεται υπό τη μορφή επαλλήλων συνθέσεων $\sigma=\tau_1\circ\tau_2\circ\dots\circ\tau_k=\tau'_1\circ\tau'_2\circ\dots\circ\tau'_l$ k αντιμεταθέσεων $\tau_1,\tau_2,\dots,\tau_k$ και αντιστοίχως l αντιμεταθέσεων $\tau'_1,\dots,\tau'_l$, τότε είτε το k είτε και το l είναι η πάντοτε άρτιος η πάντοτε περιττός αριθμός

Απόδειξη

(i) Σύμφωνα με το λήμμα 3.5.14 έχουμε:

$$Sgn(\tau\circ\sigma) = \prod_{1\le i<j\le n}\frac{\tau(\sigma(j))-\tau(\sigma(i))}{j-i} = \underbrace{\prod_{1\le i<j\le n}\frac{\tau(\sigma(j))-\tau(\sigma(i))}{\sigma(j)-\sigma(i)}}_{Sgn(\tau)\ [?]}\cdot\underbrace{\prod_{1\le i<j\le n}\frac{\sigma(j)-\sigma(i)}{j-i}}_{Sgn(\sigma)}.$$

Το πρώτο γινόμενο γράφεται ως εξής:

$$\prod_{\substack{1\le i<j\le n\\ \sigma(i)<\sigma(j)}} \frac{\tau(\sigma(j))-\tau(\sigma(i))}{\sigma(j)-\sigma(i)} \prod_{\substack{1\le i<j\le n\\ \sigma(i)>\sigma(j)}} \frac{\tau(\sigma(j))-\tau(\sigma(i))}{\sigma(j)-\sigma(i)} =$$

$$= \prod_{\substack{1\le i<j\le n\\ \sigma(i)<\sigma(j)}} \frac{\tau(\sigma(j))-\tau(\sigma(i))}{\sigma(j)-\sigma(i)} \prod_{\substack{1\le j<i\le n\\ \sigma(i)<\sigma(j)}} \frac{\tau(\sigma(j))-\tau(\sigma(i))}{\sigma(j)-\sigma(i)} =$$

$$= \prod_{\sigma(i)<\sigma(j)} \frac{\tau(\sigma(j))-\tau(\sigma(i))}{\sigma(j)-\sigma(i)}$$

Επειδή η σ είναι αμφιμονοσήμαντη θα $\exists\, l,m\in\{1,\dots,n\}$ για κάθε i,j τέτοια ώστε $\sigma(j)=l$, $\sigma(i)=m$. Επομένως, το τελευταίο αυτό γινόμενο περιέχει (ενδεχομένως παραγοντοποιημένους κατά έναν διαφορετικό τρόπο, πράγμα αυτοματωμένως αδιάφορο) τους ίδιους παράγοντες με το γινόμενο $\prod_{\lambda<\mu} \frac{\tau(\lambda)-\tau(\mu)}{\lambda-\mu}$ (που ισούται με το $\mathrm{Sgn}(\tau)$).

(ii) Άμεσο επακόλουθο του (i) (αφού $\sigma\circ\sigma^{-1}=Id$ και $\mathrm{Sgn}(Id)=1$).

(iii) Τούτο έπεται μέσω του λήμματος 3.5.13 και του (i).

(iv) Προφανώς, $\tau_1\circ\dots\circ\tau_k=\tau'_1\circ\dots\circ\tau'_l \Rightarrow$

$\Rightarrow (\tau_1\circ\dots\circ\tau_k)(\tau'_1\circ\dots\circ\tau'_l)^{-1}=Id \overset{(ii),(iii)}{\Rightarrow}$

$\mathrm{Sgn}(\tau_1\circ\dots\circ\tau_k)\,\mathrm{Sgn}(\tau'_1\circ\dots\circ\tau'_l)=1 \overset{(iii)}{\Rightarrow}$

$(-1)^k(-1)^l=1 \Rightarrow (-1)^{k+l}=1 \Rightarrow k+l\equiv 0 \pmod 2 \Rightarrow$

$\Rightarrow$ { είτε αμφότεροι οι k και l άρτιοι
— " — περιττοί } □

3.5.16 Ορισμός: Ο πυρήνας $A_n := \mathrm{Ker}(\mathrm{Sgn}) = \{\sigma\in S_n \mid \mathrm{Sgn}(\sigma)=1\}$ του ομομορφισμού Sgn είναι μια υποομάδα της συμμετρικής ομάδας S_n (βλ. 3.4.5 (ii)), απαρτίζεται από όλες τις άρτιες μεταθέσεις της S_n και καλείται εναλλάσσουσα ομάδα (σε n σύμβολα).

(σημειωτέον ότι το σύνολο $\{\sigma \in S_n \mid sgn(\sigma) = -1\}$ δεν είναι υποομάδα της S_n, καθότι δεν περιέχει το ταυτοτικό (ουδέτερο) στοιχείο της S_n ∇_o).

3.5.17 Πρόταση: Η τάξη της A_n ισούται με $|A_n| = \frac{n!}{2}$ $(n \geq 2)$

Απόδειξη

Έστω $\tau \in S_n$ μια μετάθεση και έστω: $A_n\tau := \{\sigma\circ\tau \mid \sigma \in A_n\}$. Παρατηρούμε ότι, εάν $sgn(\tau) = 1$, τότε $A_n\tau = A_n$. Εάν $sgn(\tau) = -1$, τότε για κάθε $\sigma \in S_n$ με $sgn(\sigma) = -1$ έχουμε $sgn(\sigma\circ\tau^{-1}) = 1$, οπότε $\sigma \in A_n\tau$ (διότι $\sigma = (\sigma\circ\tau^{-1})\circ\tau$). Άρα $\{\sigma \in S_n \mid sgn(\sigma) = -1\} \subseteq A_n\tau$, οπότε τελικώς $\{\sigma \in S_n \mid sgn(\sigma) = -1\} = A_n\tau$ (διότι ο αντίστροφος εγγυήσεως είναι προφανώς) και $A_n\tau \cap A_n = \emptyset$. Επειδή η απεικόνιση $A_n \longrightarrow A_n\tau$ είναι αμφιμονοσήμαντη λαμβάνουμε (μέσω του $\sigma \overset{\psi}{\longmapsto} \sigma\circ\tau$) και $S_n = A_n \amalg A_n\tau$

1.5.3): $n! = |S_n| = |A_n| + card(A_n\tau) = 2|A_n| \Rightarrow |A_n| = \frac{n!}{2}$. □

Η σημασία των ομάδων μεταθέσεων στη Θεωρία Ομάδων παρεμφαίνεται από το ακόλουθο Θεώρημα του Cayley:

3.5.18 Θεώρημα του Cayley: Κάθε ομάδα G είναι ισόμορφη με μια υποομάδα της S_G.

Απόδειξη

Κάθε στοιχείο $g \in G$ μας δίνει μια μετάθεση L_g οριζόμενη ως εξής:

$$L_g : G \to G, \quad L_g(x) := gx, \quad \forall x \in G$$

Η απεικόνιση L_g είναι ενριπτική, διότι εάν $L_g(x) = L_g(y)$, για κάποια $x, y \in G$, τότε $gx = gy \Rightarrow g^{-1}gx = g^{-1}gy \Rightarrow e_G x = e_G y \Rightarrow x = y$. Η L_g είναι, επιπροσθέτως, και επιριπτική διότι εάν $z \in G$, τότε $L_g(g^{-1}z) = gg^{-1}z = e_G z = z$.

(Η L_g ονομάζεται η αριστερή μετατόπιση μέσω του g).

Έστω $G' := \{L_g \mid g \in G\} \subseteq S_G$.

Η πράξη με την οποία είναι εφοδιασμένη η S_G είναι η σύνθεση απεικονίσεων. Ως εκ τούτου,

$L_g(L_h(x)) = L_g(hx) = g(hx) = (gh)x = L_{gh}(x)$, $\forall (g,h) \in G \times G$ και $\forall x \in G$.

Επίσης, $e_{S_G} = Id_G \in G'$ (διότι $Id_G = L_{e_G}$), και το συμμετρικό οποιασδήποτε L_g εντός της S_G ισούται με την $L_{g^{-1}}$ (η οποία ανήκει στην G'). Άρα το $(G', \circ)$ αποτελεί υποομάδα της $(S_G, \circ)$.

Η απεικόνιση $G \to G'$ είναι προφανώς επιριπτική και

$$g \overset{\psi}{\longmapsto} L_g$$

μετατρέπει τον "πολλαπλασιασμό" (= πράξη) της G στη σύνθεση απεικονίσεων της G' (δηλ. $gh \xrightarrow{\psi} L_{gh} = L_g L_h$)

Εξάλλου, η εν λόγω απεικόνιση είναι και ενριπτική, διότι, δεδομένης μιας ισότητας της μορφής $L_g = L_h$, έχουμε $g = L_g(e_G) = L_h(e_G) = h$

Κατ' αυτόν τον τρόπο καταδείξαμε έναν ισομορφισμό μεταξύ της G και της υποομάδας G' της S_G. □

35.19 Πόρισμα: Εάν η G είναι πεπερασμένης τάξεως n, τότε η G είναι ισόμορφη με μια υποομάδα της S_n. ($S_G \cong S_n$). □

Άλγεβρα – 11/4/06

§3.6 Πλευρικές κλάσεις και δείκτες υποομάδων

3.6.1 Ορισμός: Εάν η H είναι μια υποομάδα μιας ομάδας $(G,\cdot)$ και $g\in G$, τότε το σύνολο $Hg := H\{g\} = \{hg \mid h\in H\}$ [ασυ. στα φυλλ. 5]

(αντ., $gH = \{gh \mid h\in H\}$.)
Καλείται δεξιά (αντ., αριστερή) πλευρική κλάση της H εντός της G.

3.6.2 Ορισμός: Έστω $(G,\cdot)$ μια ομάδα και έστω H μια υποομάδα της. Επί του συνόλου G ορίζουμε μια δυαδική σχέση ως ακολούθως $x\sim_\delta y \underset{\text{ορ.}}{\iff} xy^{-1}\in H$.

3.6.3 Πρόταση: Η "$\sim_\delta$" είναι μια σχέση ισοδυναμίας επί του G.

Απόδειξη: (α) "ανακλαστική": $e_G = xx^{-1}\in H \iff x\sim_\delta x$, $\forall x\in G$.
(β) συμμετρική: $x\sim_\delta y \underset{\text{ορ.}}{\iff} xy^{-1}\in H \Rightarrow \underbrace{(xy^{-1})^{-1}}_{yx^{-1}}\in H \underset{\text{ορ.}}{\iff} y\sim_\delta x$.

(γ) μεταβατική: $\left.\begin{matrix} x\sim_\delta y \\ y\sim_\delta z\end{matrix}\right\} \iff \left\{\begin{matrix} xy^{-1}\in H \\ yz^{-1}\in H\end{matrix}\right\} \Rightarrow (xy^{-1})(yz^{-1}) =$

$= x\underbrace{(y^{-1}y)}_{e_H} z^{-1} = xz^{-1}\in H \underset{\text{ορ.}}{\iff} x\sim_\delta z$ $\square$

3.6.4 Πρόταση: Η κλάση ισοδυναμίας $[g]_{\sim_\delta} := \{y\in G \mid y\sim_\delta g\}$ οιουδήποτε $g\in G$ με την δεξιά πλευρική κλάση Hg.

Απόδειξη: $[g]_{N_\delta} = \{y \in G \mid yg^{-1} \in H\} = \{y \in G \mid yg^{-1} = h \in H\} =$
$= \{y \in G \mid y = hg, h \in H\} = \{hg \mid h \in H\} = H_g$ □

3.6.5 Πόρισμα: Έστω η H είναι υποομάδα μιας ομάδας $(G, \cdot)$ τότε:

$$G = \coprod_{H_g \in (G/N_\delta)} H_g \quad (*)$$

(με $H_{g_1} \cap H_{g_2} \neq \emptyset \Leftrightarrow g_1 g_2^{-1} \in H \Leftrightarrow H_{g_1} = H_{g_2}$, $\forall (g_1, g_2) \in G_1 \times G_2$)
Ιδιαιτέρως δε, για τυχόν $g \in G$ ισχύει η αμφίπλευρη συνεπαγωγή:
$g \in H \Leftrightarrow H_g = H$.

Απόδειξη: Οι δύο πρώτες αμφίπλευρες συνεπαγωγές, καθώς και το ότι το υπουλείμενο σύνολο G της θεωρούμενης ομάδας ισούται με την αποσυνδετική ένωση $(*)$ των μελών της οικογένειας $\{H_g \mid H_g \in (G/N_\delta)\}$ (της αποτελούμενης από όλες τις σαφώς διαφορετικές δεξιές πλευρικές κλάσεις της H εντός της G).
Προκύπτουν άμεσα από τις προτάσεις 1.3.5, 3.6.3 και 3.6.4. Εξάλλου, θέτοντας $g_1 = g$ και $g_2 = e_G$, λαμβάνουμε (διαιτέρως) την αμφίπλευρη συνεπαγωγή
$g \in H \Leftrightarrow H_g = H$ □

3.6.6 Πρόταση: Για κάθε ζεύγος $(g_1, g_2) \in G \times G$, η απεικόνιση $f_{(g_1,g_2)} : H_{g_1} \to H_{g_2}$
$hg_1 \longmapsto hg_2 \ (\forall h \in H)$
είναι αμφιρριπτική και $|H| = \mathrm{card}(H_g)$, $\forall g \in G$.

Απόδειξη: Η $f_{(g_1,g_2)}$ είναι προφανώς επιρριπτική.
Εξάλλου, για οιαδήποτε ζεύγος $(h_1, h_2) \in H \times H$, για το

οποίο ισχύει $f_{(g_1,g_2)}(h_1,g_1)=f_{(g_1,g_2)}(h_2,g_1)$, λαμβάνουμε $h_1g_2=h_2g_2 \xrightarrow[\text{νόμος διαγραφής}]{} h_1=h_2$. Άρα η $f_{(g_1,g_2)}$ είναι και ενριπτική $\forall_o$

Ιδιαιτέρως, η $f_{(g_1,g_2)}$ είναι αμφιρριπτική, οπότε $|H|=\text{card}(H)=\text{card}(H_g)$, $\forall g\in G$.

□

3.6.7 Ορισμός: Εάν η H είναι μια υποομάδα μιας ομάδας $(G,\cdot)$, τότε **δείκτης της H εντός της G** $:=|G:H|=\text{card}(G/_{\sim_\delta})$

3.6.8 Παραδείγματα: (i) Προφανώς, $|G:\{e_G\}|=|G|$, $|G:G|=1$

(ii) $G=$ προσθ. ομάδα $\mathbb{Z}$ των ακεραίων, $H=n\mathbb{Z}$, για κάποια $n\in\mathbb{N}$, τότε $|\mathbb{Z}:n\mathbb{Z}|=n$.

$[k\sim_\delta l \Leftrightarrow k-l\in\mathbb{Z}]$

3.6.9 Παρατήρηση: Όταν επιθυμούμε την ευτέλεση συχνά μεριμνών υπολογισμών με τον δείκτη $|G:H|$, χρησιμοποιούμε συνήθως (για πρακτικούς λόγους) κάποιο πλήρες σύστημα εκπροσώπων από το $G/_{\sim_\delta}$, δηλαδή κάποια αμοιχένια $(g_i)_{i\in I}$ στοιχείων της G, τέτοια ώστε $(\forall (i_1,i_2)\in I\times I : i_1\neq i_2) \Rightarrow Hg_{i_1}\cap Hg_{i_2}=\emptyset$

Δοθέντος ενός πλήρους συστήματος εκπροσώπων $(g_i)_{i\in I}$, έχουμε $\text{card}(G/_{\sim_\delta})=|G:H|=\text{card}(I)\Rightarrow$

$$\Rightarrow \boxed{G=\coprod_{i\in I}[g_i]_\delta=\coprod_{i\in I}Hg_i} \quad (**)$$

3.6.10 Θεώρημα: Εάν η H είναι μια υποομάδα μιας ομάδας $(G,\cdot)$, τότε ισχύει η ισότητα:

$$\boxed{|G|=|G:H||H|}$$

Απόδειξη: Έστω $(g_i)_{i\in I}$ ένα πλήρες σύστημα εκπροσώπων των αριστερών συμπλοκών ως προς την "$\sim_\delta$".

Η απεικόνιση: $f: \coprod_{i\in I} Hg_i \longrightarrow I \times H$ είναι μια αμφίρριψη

$$Hg_i \ni hg_i \longmapsto f(hg_i) = (i,h),\ \forall h\in H$$

Όπως είπαμε, λαμβάνοντας υπ' όψιν την (**) συμπεραίνουμε ότι $|G| = \mathrm{card}(\coprod_{i\in I} Hg_i) = \mathrm{card}(I\times H) = \mathrm{card}(I)\mathrm{card}(H) = |G:H|\,|H|$.
(συνολοθεωρία)

□

3.6.11 Σημείωση: Εάν συλλάχιστον δυο εκ των ως άνω πληθικών αριθμών $|G|, |G:H|, |H|$ είναι πεπερασμένοι τότε και ο τρίτος θα είναι και αυτ' αυτόματα πεπερασμένος.

3.6.12 Πόρισμα (Θεώρημα του Lagrange): Εάν η G είναι μια πεπερασμένη ομάδα, τότε η τάξη της $|G|$ διαιρείται δια της τάξεως οιασδήποτε υποομάδος της.

Απόδειξη: Εάν $|G| = n \in \mathbb{N}$ και η H τυχούσα υποομάδα της G, τότε $|H| = m \leq n \Rightarrow |G:H| < \infty \Rightarrow$
($m \in \mathbb{N}$; 3.6.11)

$\overset{3.6.10}{\Rightarrow} m \mid n$

□

3.6.13 Πόρισμα: $|G| < \infty \Rightarrow \mathrm{ord}(g) \mid |G|$.

Απόδειξη: $\forall g\in G: \mathrm{ord}(g) = |\langle g\rangle| \overset{3.6.12}{\Longrightarrow} \mathrm{ord}(g) \mid |G|$ □

3.6.14 Πόρισμα: Εάν μια ομάδα G έχει ως τάξη της

ένων πρώτο αριθμό $p \geq 2$, τότε η G είναι κυκλική.

Απόδειξη: Επειδή $|G| = p \geq 2 \Rightarrow \exists g \in G \setminus \{e_G\}$ με $|\langle g \rangle| > 1$

$\text{ord}(g) \geq 2 \xrightarrow[3.6.13]{} \text{ord}(g) \mid p$, p πρώτος $\Rightarrow \text{ord}(g) = p = |G| \Rightarrow |G| = \langle g \rangle \Rightarrow$

G κυκλική. □

3.6.15 Πόρισμα: Εάν η $(G, \cdot)$ είναι μια πεπερασμένη ομάδα (με το e_G ως ουδέτερο της), τότε

$$\boxed{g^{|G|} = e_G, \forall g \in G}$$

Απόδειξη: Έστω τυχόν $g \in G$. Εάν $m := \text{ord}(g)$, τότε $g^m = e_G$ και, σύμφωνα με το πόρισμα 3.6.13 η τάξη $\text{ord}(g)$ του g είναι διαιρέτης της $|G|$, οπότε

$$g^{|G|} = g^{m\left(\frac{|G|}{m}\right)} = \left(g^m\right)^{\frac{|G|}{m}} = e_G^{\frac{|G|}{m}} = e_G$$

□

3.6.16 Πόρισμα (Ομαδοθεωρητική απόδειξη του Θεωρήματος 2.4.23 του Euler περί ισοτιμιών)
Εάν $a \in \mathbb{Z} \setminus \{0\}$, $m \in \mathbb{N}$ με $\text{μκδ}(a, m) = 1$, τότε

$$\boxed{a^{\varphi(m)} \equiv 1 \pmod m}$$

Απόδειξη: Έστω $G = \mathbb{Z}_m^\times = \{[k]_m \in \mathbb{Z}_m \mid 1 \leq k \leq m-1, \text{μκδ}(k, m) = 1\}$ η πολλαπλασιαστική ομάδα των αντιστρέψιμων στοιχείων του $(\mathbb{Z}_m, \cdot)$ (βλ. ασκ. 1, φυλ. 6). Τότε $|\mathbb{Z}_m| = \varphi(m)$. Διαιρώντας τον a δια του m λαμβάνουμε υπόλοιπο k, όπου $[k]_m \in \mathbb{Z}_m^\times$. Από το

πόρισμα 3.6.15 γνωρίζουμε ότι $([k]_m)^{\varphi(m)} = [1]_m \Rightarrow$

$\Rightarrow [k^{\varphi(m)}]_m = [1]_m$ οπότε $[\alpha]_m = [k]_m \rightarrow$
$\Rightarrow [\alpha^{\varphi(m)}]_m = [k^{\varphi(m)}]_m = [1]_m \Rightarrow \alpha^{\varphi(m)} \equiv 1 \pmod m$

□

3.6.17 Πόρισμα: Εάν ο p είναι ένας πρώτος αριθμός και $\alpha \in \mathbb{Z}$, τότε $\boxed{\alpha^p \equiv \alpha \pmod p}$

Απόδειξη: Εάν $\mu\kappa\delta(\alpha, p) = 1$, τότε, λαμβάνοντας υπ' όψιν ότι $\varphi(p) = p-1$ (κατά το λήμμα 2.4.20) έχουμε
$\alpha^{p-1} \equiv 1 \pmod p \Rightarrow \alpha^p \equiv \alpha \pmod p$. (από το 3.6.16)
Ο αντίστροφος είναι αληθής επίσης και όταν $\mu\kappa\delta(\alpha, p) > 1$ (δηλ. εάν $\alpha = \lambda p$, $\lambda \in \mathbb{Z}$, τότε
$\alpha^p - \alpha = (\lambda p)^p - \lambda p = p(\lambda^p p^{p-1} - \lambda) \equiv 0 \pmod p$

□

3.6.18 Παρατήρηση: Έστω $(G, \cdot)$ μια ομάδα και έστω H μια υποομάδα της. Επί του G μπορούμε να ορίσουμε μια δυαδική σχέση ως ακολούθως: $x \sim_\alpha y \overset{\text{ορ.}}{\Leftrightarrow} x^{-1}y \in H$
Οι κύριες ιδιότητες των δεξιών πλευρικών κλάσεων της H εντός της G, οι οποίες οφείλονται στη σχέση ισοδυναμίας "$\sim_\delta$" μεταφέρονται (ουσιαστικώς κατά γράμμα) και στις αριστερές πλευρικές κλάσεις όταν χρησιμοποιείται η "$\sim_\alpha$" αντί της "$\sim_\delta$" (βλ. πρ. 3.6.3, 3.6.4, 3.6.5, 3.6.6)

3.6.19 Πρόταση: Εάν η H είναι υποομάδα ομάδας $(G, \cdot)$ τότε η απεικόνιση $\beta : (G/\sim_\delta) \rightarrow (G/\sim_\alpha)$
$\beta(Hg) := g^{-1}H$, $\forall g \in G$.
είναι αμφιρριπτική.

Απόδειξη: Επειδή για κάθε ζεύγος $(g_1, g_2) \in G \times G$

ισχύουν οι αμφίπλευρες συνεπαγωγές: $Hg_1 = Hg_2 \Leftrightarrow$
$\Leftrightarrow g_1 g_2^{-1} \in H \Leftrightarrow (g_1 g_2^{-1})^{-1} = g_2 g_1^{-1} \in H \Leftrightarrow g_1^{-1} H = g_2^{-1} H$

η β είναι μια (καλώς ορισμένη) ενριπτική απεικόνιση. Επιπλέον, για οιαδήποτε αριστερή πλευρική κλάση $[g^{-1}]_\delta = gH$ της H εντός της G ορίζεται η δεξιά πλευρική κλάση $[g^{-1}]_\delta = Hg^{-1}$ για την οποία ισχύει: $\beta([g^{-1}]_\delta) = (g^{-1})^{-1} H = gH = [g]_\alpha$, οπότε η β είναι και επί. ▽ ∎

3.6.20 Σημείωση: Λόγω της πρότασεως 3.6.19 θα μπορούσε κανείς να ορίσει τον δείκτη $|G:H|$ και ως τον πληθικό αριθμό των συνόλων διαμερισμένων αριστερών πλευρικών κλάσεων της H εντός της G. Το ότι ο πληθικός αριθμός των συνόλων δια. δεξιών πλ. κλάσεων ισούται με τον πληθικό αρ. των συνόλων δια. αριστερών πλ. κλ. δεν σημαίνει ότι ο διαμερισμός της G σε σύνολα δια. δεξιές πλ. κλάσεις ταυτίζεται (από συνολοθεωρητική σκοπιά, στοιχείο προς στοιχείο) με το διαμερισμό της G σε αριστερές πλευρικές κλάσεις ▽ (βλ. Παρ. 3.6.21) Ωστόσο, υπάρχουν υποομάδες (οι λεγόμενες ορθόδεξες υποομάδες, μεταξύ των οποίων συγκαταλέγονται και οι αβελιανές, στις οποίες κάθε δ. πλ. κλ. είναι και αρ. πλ. κλ. (και αντιστρόφως)

3.6.21 Παράδειγμα: $S_3 = \{Id, [1\,2], [1\,3], [2\,3], [1\,2\,3], [1\,3\,2]\}$.
U|
$H = \{Id, [1\,2]\}$

Αριστερές πλευρικές κλάσεις της H εντός της S_3:

$Id\ H = H$

$[1\,2]H = \{[1\,2], Id\} = H$

$[1\,3]H = \{[1\,3], [1\,2\,3]\}$

$[2\,3]H = \{[2\,3], [1\,3\,2]\}$

$[1\,2\,3]H = \{[1\,2\,3], [1\,3]\}$

$[1\,3\,2]H = \{[1\,3\,2], [2\,3]\}$

Δεξιές πλ. κλάσεις της H ανεξ της S_3

$H\,Id = H$

$H\,[1\,2] = H$

$H\,[1\,3] = \{[1\,3], [1\,3\,2]\}$

$\neq$ $H\,[2\,3] = \{[2\,3], [1\,2\,3]\}$

$\neq$ $H\,[1\,2\,3] = \{[1\,2\,3], [2\,3]\}$

$\neq$ $H\,[1\,3\,2] = \{[1\,3\,2], [1\,3]\}$

δείχνω $\boxed{|S_3 : H| = 3}$

Άλγεβρα - 13/4/06

3.6.22 Θεώρημα: Εάν η $(G,\cdot)$ είναι μια ομάδα και οι $K \subseteq H \subseteq G$ υποομάδες της, τότε $\boxed{|G:K| = |G:H||H:K|}$.

Απόδειξη: Έστω $(g_i)_{i\in I}$ ένα πλήρες σύστημα εκπροσώπων των αριστερών διακεκριμένων αριστερών πλευρικών κλάσεων της H εντός της G και $(\gamma_j)_{j\in J}$ ένα τέτοιον είδους σύστημα για την K εντός της H. Τότε
$G = \coprod_{i\in I} [g_i]_n = \coprod_{i\in I} g_i H = \coprod_{i\in I} g_i\left(\coprod_{j\in J}\gamma_j K\right)$. Πράς σαχμή,

ας σημειώσουμε ότι οι ενώσεις είναι ασυνδέτες, χρησιμοποιώντας την ασυ. 20 του φυλ. 5 το δεξιό μέλος της ισότητας μας μπορεί να γραφεί ως εξής:
$G = \bigcup_{(i,j)\in I\times J} g_i\gamma_j K$.

Τώρα θα αποδείξουμε ότι και αυτή η ένωση είναι ασυνδέτη; Ας υποθέσουμε ότι ισχύει η ισότητα $g_{i_1}\gamma_{j_1}K = g_{i_2}\gamma_{j_2}K$ για κάποιους δείκτες $(i_1,i_2)\in I\times I$ και $(j_1,j_2)\in J\times J$. Τότε

$g_{i_1}\gamma_{j_1}KH = g_{i_2}\gamma_{j_2}KH$ } $\Rightarrow g_{i_1}\gamma_{j_1}H = g_{i_2}\gamma_{j_2}H$ } $\Rightarrow$
K υποομ. της $H \Rightarrow KH = H$ } $\gamma_{j_1},\gamma_{j_2}\in H$

$\Rightarrow g_{i_1}H = g_{i_2}H \Rightarrow i_1 = i_2$. Όμως είχαμε $g_{i_1} = g_{i_2} \Rightarrow$

$\Rightarrow \gamma_{j_1}K = \gamma_{j_2}K \Rightarrow j_1 = j_2$

Άρα τελικώς, $G = \coprod_{(i,j)\in I\times J} g_i\gamma_j K \Rightarrow |G:K| = \mathrm{coard}(I\times J) =$

$\mathrm{coard}(I)\,\mathrm{coard}(J) = |G:H||H:K|$

□

3.6.23 Λήμμα: Έαν οι H, K είναι υποομάδες μιας ομάδας G και $g \in G$, τότε:
$Hg \cap Kg = (H \cap K)g$.

Απόδειξη: Προφανώς $(H \cap K)g \subseteq Hg \cap Kg$. Έστω $z \in Hg \cap Kg$. Τότε $z = hg = kg$, για κάποια $h \in H$, $k \in K$. Από τον νόμο της διαγραφής, $h = k \in H \cap K \Rightarrow z \in (H \cap K)g$. □

3.6.24 Ορισμός: Κάθε υποομάδα H μιας ομάδας G, για την οποία $|G:H| \in \mathbb{N}$, ονομάζεται υποομάδα πεπερασμένου δείκτη (εντός της G).

3.6.25 Θεώρημα Poincaré: Έστω ότι οι H, K είναι υποομάδες μιας ομάδας G. Τότε
(i) ισχύει η ανισότητα: $|G:H \cap K| \leq |G:H||G:K|$, και, ως εκ τούτου, εάν αμφότερες οι H, K είναι πεπερασμένου δείκτη, τότε και η $H \cap K$ θα είναι πεπερασμένου δείκτη
(ii) Εάν αμφότερες οι H, K είναι υποομάδες πεπερασμένου δείκτη, τότε ισχύει η συνεπαγωγή:
$\text{μκδ}(|G:H|, |G:K|) = 1 \rightarrow |G:H \cap K| = |G:H||G:K|$

Απόδειξη: (i) Από το Λήμμα 3.6.23 κάθε δεξιά πλευρική κλάση της $H \cap K$ εντός της G είναι της μορφής $Hg \cap Kg$, όπου $g \in G$. Όμως δεξιές πλευρικές κλάσεις αυτής της μορφής, οι οποίες είναι ασφαλώς διακεκριμένες, υπάρχουν το πολύ $|G:H||G:K|$ τ.
(ii) $H \cap K$ είναι υποομάδα εξ ορισμού της H όσον και της K. Εφαρμόζοντας, λοιπόν δύο φορές το Θεώρημα 3.6.22 συνάγουμε ότι
$|G:H \cap K| = |G:H||H:H \cap K| = |G:K||K:H \cap K|$. Επειδή αμφότεροι οι δείκτες $|G:H|$ και $|G:K|$ διαιρούν τον $|G:H \cap K|$ και είναι εξ υποθέσεως πρώτοι μεταξύ τους,

και το γινόμενο τους θα διαιρεί τον $|G:H\cap K|$. Τούτο σημαίνει ότι $|G:H||G:K|\leq|G:H\cap K|$. Από (i) έπεται η ζητούμενη ισότητα. □

§3.7 Πηλικοομάδες και Θεωρήματα ισομορφισμών

3.7.1 Ορισμός: Έστω $(G,\cdot)$ μια ομάδα. Μια υποομάδα H της G καλείται ορθόδεση (συμβολίζεται ως $H\trianglelefteq G$) όταν $gH=Hg$, $\forall g\in G$.

3.7.2 Πρόταση: Έστω $(G,\cdot)$ μια ομάδα και έστω $H\trianglelefteq G$. Τότε το σύνολο των πλευρικών υλάσεων της H εντός της G εφοδιάζεται ομάδα μέσω της (πολλαπλασιαστικά συμβολιζόμενης) πράξεως: $(gH)(g'H):=(gg')H$, $\forall(g,g')\in G\times G$.

Απόδειξη: Εάν $g,g',g''\in G$, τότε
$((gH)(g'H))(g''H)=(gg')H(g''H)=((gg')g'')H=$
$=(g(g'g''))H=(gH)((g'H)(g''H))$.
(β) $\forall g\in G$: $gH=(gH)H=(Hg)H=H(gH)\Rightarrow$ η ίδια η $H=e_GH$ είναι το ουδέτερο στοιχείο της εν λόγω πράξεως.
(γ) $\forall g\in G$: $(gH)^{-1}=Hg^{-1}=g^{-1}H$
$(gH^{-1})(gH)=(g^{-1}H)(gH)=H$

3.7.3 Ορισμός: Η ομάδα που δημιουργήθηκε μέσω της Προτάσεως 3.7.2 καλείται πηλικοομάδα (ή ομάδα πηλίκων) της G ως προς την H και συμβολίζεται ως G/H.
(iii) Σημειωτέον ότι οι αριστερές (ή δεξιές) πλευρικές υλάσεις της H εντός της G συχνοτούν ένα διαμέλισμό της G. Ως εκ τούτου, κάθε μία εξ αυτών αναπαριστά ένα και μόνον στοιχείο της G/H.
[$G/H=G/\mathcal{R}_H$, $\mathcal{R}_H\subseteq G\times G$, $(x,y)\in\mathcal{R}_H\overset{\text{ορ.}}{\Longleftrightarrow}x^{-1}y\in H$. Προφανώς $[x]_{\mathcal{R}_H}=xH$] Γι' αυτό είναι εύλογο, υπό αυτήν την έννοια,

να ομαδοποιήσουμε [- συνειδοχικώς - για πλήθος στοιχείων της G ουσιαστικά στην H ή - εμφραγμένοι αφαιρετικώς -] για διαίρεση «της G διά της H»

(iii) $\boxed{|G/H| = |G:H|}$ (εξ ορισμού)

(iv) $\rho: G \to G/H$, $\rho(g) = gH$ (φυσικός επιμορφισμός)

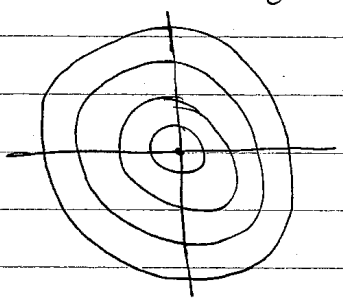
3.7. 4 Παραδείγματα: (i) G ομάδα $\Rightarrow \{e_G\} \trianglelefteq G \Rightarrow$
$[x \sim y \Leftrightarrow x^{-1}y = e \Leftrightarrow x = y]$ $\Rightarrow G/\{e_G\} = \{x \mid x \in G\} = G$

(ii) G ομάδα $\Rightarrow G \trianglelefteq G \Rightarrow G/G = \{e_G\}$
$[x \sim_\alpha y \Leftrightarrow x^{-1}y \in G]$

(iii) Κάθε μη τετριμμένη υποομάδα της $(\mathbb{Z}, +)$ είναι της μορφής $(m\mathbb{Z}, +)$, για κάποιον $m \in \mathbb{N}$
$[x \sim_\alpha y \Leftrightarrow y - x \in m\mathbb{Z} \Leftrightarrow m \mid y - x]$ Και συνεπώς, $\mathbb{Z}/m\mathbb{Z} = \mathbb{Z}_m$
"$\sim_\alpha$" = "$\sim_m$"

(iv) $\mathbb{S}^1 = \{z \in \mathbb{C}\setminus\{0\} \mid |z| = 1\} \trianglelefteq (\mathbb{C}\setminus\{0\}, \cdot)$. Έστω $z_0 \in \mathbb{C}\setminus\{0\}$,
$[z_1 \sim_{\mathbb{S}^1} z_2 \underset{\text{ορ.}}{\Leftrightarrow} z_1 z_2^{-1} \in \mathbb{S}^1]$.
τότε η πλευρική κλάση $\mathbb{S}^1_{z_0}$ γράφεται ως εξής:
$[\mathbb{S}^1]_{z_0} = \{z \in \mathbb{C}\setminus\{0\} \mid z z_0^{-1} \in \mathbb{S}^1\} = \{z \in \mathbb{C}\setminus\{0\} \mid |z z_0^{-1}| = 1\} =$
$= \{z \in \mathbb{C}\setminus\{0\} \mid |z| = |z_0|\}$ = περιφέρειες με κέντρο το $0 \in \mathbb{C}$ και ακτίνα ίση με $|z_0|$

$\mathbb{C}\setminus\{0\}/\mathbb{S}^1 = \{$ομόκεντρες περιφέρειες με κέντρο το $0 \in \mathbb{C}$ [και θετική ακτίνα]$\}$



(v) $(\mathbb{Z},+) \trianglelefteq (\mathbb{Q},+)$

$\mathbb{Q}/\mathbb{Z} = \{x+\mathbb{Z} \mid x \in \mathbb{Q} \cap [0,1)\}$

(άσκηση)

(vi) $A_n \trianglelefteq S_n$ $\Longleftrightarrow$

($\forall \tau \in A_n, \sigma \in S_n : \sigma\circ\tau\circ\sigma^{-1} \in A_n$, διότι

$\operatorname{sgn}(\sigma\circ\tau\circ\sigma^{-1}) = \operatorname{sgn}(\sigma)\operatorname{sgn}(\tau)\operatorname{sgn}(\sigma^{-1}) = \operatorname{sgn}(\underbrace{\sigma\circ\sigma^{-1}}_{Id}) = 1$)

(vii) $SL_n(F) \trianglelefteq GL_n(F)$ (όπου F σώμα)

($\forall B \in SL_n(F)$ και $A \in GL_n(F) : ABA^{-1} \in SL_n(F)$, διότι

$\det(ABA^{-1}) = \det(A)\det(B)\det(A^{-1})$

3.7.5 Πρόταση: $\left.\begin{matrix} H \trianglelefteq G \\ K \trianglelefteq G \end{matrix}\right\} \rightarrow H \cap K \trianglelefteq G$

Απόδειξη: Εάν $g \in G$ και $y \in H \cap K \Rightarrow gyg^{-1} \in H$ και $gyg^{-1} \in K \Rightarrow gyg^{-1} \in H \cap K \Rightarrow g(H\cap K) = (H\cap K)g$. □

3.7.6 Πρόταση: $\left.\begin{matrix} H \text{ υποομάδα της } G \\ |G:H| = 2 \end{matrix}\right\} \Rightarrow H \trianglelefteq G$

Απόδειξη: $|G:H| = 2 \Rightarrow G = H \amalg (G\setminus H) \rightarrow H, G\setminus H$ οι μόνες αΗ όπου $a \notin H$

δεξιές (αντ. αρ) πλ. κλάσεις θα ταυτίζονται. □

3.7.7 Παράδειγμα

π.χ. $\left.\begin{matrix} |S_n| = n! \\ |A_n| = \frac{n!}{2} \\ |S_n : A_n| = |S_n| / |A_n| = 2 \end{matrix}\right\} \rightarrow A_n \trianglelefteq S_n$

3.7.8 Πρόταση: $f : G \rightarrow H$ $\rightarrow \operatorname{Ker}(f) \trianglelefteq G$.

ομομορφ. ομάδων

Απόδειξη: Ο s χωστόν, ο πυρήνας της f είναι υποομάδα της G. Επιπροσθέτως, $\forall y \in \ker(f)$ και $\forall g \in G$.
$f(gyg^{-1}) \underset{f\text{ομομ.}}{=} f(g)f(y)f(g^{-1}) = f(g)e_H f(g)^{-1} = e_H \Rightarrow$
$\Rightarrow gyg^{-1} \in \ker(f)$. Άρα $\ker(f) \trianglelefteq G$.

3.7.9 Εφαρμογές: (i) $sgn : (S_n, \cdot) \to (\{\pm 1\}, \cdot)$ ομομ. $\Rightarrow$ $\ker(sgn) = A_n \trianglelefteq S_n$
(ii) $\det : (GL_n(F), \cdot) \to (F \setminus \{0_F\}, \cdot)$ ομομ. $\to$ $\ker(f) = SL_n(F) \trianglelefteq GL_n(F)$.

3.7.10 Πρόταση: Εάν η $f : G \to H$ είναι ομομορφισμός ομάδων τότε:
(i) $K \trianglelefteq H \to f^{-1}(K) \trianglelefteq G$
(ii) f επιμορφισμός $\}$ $P \trianglelefteq G \to f(P) \trianglelefteq H$

Απόδειξη: Άσκηση. □

Εν συνεχεία, παρατίθενται τα λεγόμενα "Θεωρήματα ισομορφισμών ομάδων" που αφορούν σε πηλικοομάδες (και είναι πολύ χρήσιμα ως θεωρητικά τεχνικά μέσα).

3.7.11 1ο Θεώρημα Ισομορφισμού Ομάδων: Εάν η $f : G \to H$ είναι ομομορφισμός ομάδων, τότε

$$\boxed{G/\ker(f) \cong \mathrm{Im}(f)}$$

Απόδειξη: Έχουμε ήδη αποδείξει στην πρόταση 3.7.8 ότι $K := \ker(f) \trianglelefteq G$. Ορίζουμε την $\phi : G/K \to \mathrm{Im}(f)$
$gK \mapsto \phi(gK) := f(g)$

• Παρατηρούμε ότι $\forall (g_1, g_2) \in G \times G$ ισχύουν οι αμφίπλευρες συνεπαγωγές:

$g_1 K = g_2 K \Rightarrow g_1 g_2^{-1} \in K \Leftrightarrow f(g_1 g_2^{-1}) = e_H \Leftrightarrow$

$\Leftrightarrow f(g_1) = f(g_2) \Leftrightarrow \phi(g_1 K) = \phi(g_2 K)$

"$\Rightarrow$" καλώς ορ. της ϕ

"$\Leftarrow$" ενριπτικότητα της ϕ

• Η ϕ είναι προφανώς επιριπτική

• ϕ ομομορφισμός $\phi((aK)(bK)) = \phi(abK) = f(ab) \overset{f \text{ ομομ.}}{=} f(a) f(b) = \phi(aK)\phi(bK)$

$\forall a, b \in G.$ □

3.7.12 Εφαρμογές: (i) $\mathbb{Z} \to \mathbb{Z}_m$, $n \mapsto [n]_m$, πυρήνας $= m\mathbb{Z} \overset{3.7.11}{\Rightarrow}$

$\mathbb{Z}/m\mathbb{Z} \cong \mathbb{Z}_m$.

(ii) $(\mathbb{R}, +) \to (\mathbb{S}^1, \cdot)$, $x \mapsto e^{2\pi i x}$, πυρήνας $= \mathbb{Z} \overset{3.7.11}{\Rightarrow} \mathbb{R}/\mathbb{Z} \cong \mathbb{S}^1$.

(iii) $(\mathbb{C}\setminus\{0\}, \cdot) \xrightarrow{f} (\mathbb{S}^1, \cdot)$, $\ker(f) = \{z \in \mathbb{C}\setminus\{0\} \mid z = |z|\} =$

$= \mathbb{R}_{>0}$, $z \mapsto \frac{z}{|z|}$

$$\boxed{\mathbb{C}\setminus\{0\}/\mathbb{R}_{>0} \cong \mathbb{S}^1}$$

(iv) $\det: (GL_n(F), \cdot) \xrightarrow[\text{επιμ.}]{} (F\setminus\{0_F\}, \cdot) \overset{3.7.11}{\Rightarrow}$

$$\boxed{GL_n(F)/SL_n(F) \cong F\setminus\{0_F\}}$$

(v) $\mathrm{Sgn}: (S_n, \circ) \to (\{\pm 1\}, \cdot) \xrightarrow[3.7.11]{} \boxed{S_n/A_n \cong \{\pm 1\}}$

(vi) $(\mathbb{S}^1, \cdot) \xrightarrow{P} (\mathbb{S}^1, \cdot)$, $\mathrm{Ker}(P) = \{z \in \mathbb{S}^1 \mid z^2 = 1\} = \{\pm 1\}$

$z \mapsto z^2$

$\xrightarrow[3.7.11]{} \boxed{\mathbb{S}^1/\{\pm 1\} \cong \mathbb{S}^1}$

3.7.13 2ο Θεώρημα Ισομορφισμών Ομάδων:

Εάν $K \trianglelefteq G$, H υποομάδα $\Big\} \to HK$ υποομάδα της G, $H \cap K \trianglelefteq H$ και

$$\boxed{HK/K \cong H/H \cap K}$$

Απόδειξη: $K \trianglelefteq G \Rightarrow gK = Kg, \forall g \in G \Rightarrow HK = KH \xrightarrow[\text{φυλ. 5}]{\text{ασκ. 20(ii)}}$

HK υποομάδα της G.

Θεωρούμε τον φυσικό επιμορφισμό

$P: G \to G/K$, $\mathrm{Ker}(P) = K$

$g \mapsto gK$

Εν συνεχεία, θεωρούμε τον περιορισμό $\rho|_H : H \to G/K$.

Προφανώς, $\mathrm{Ker}(\rho|_H) = H \cap K$, διότι $\mathrm{Ker}(\rho|_H) = \{h \in H \mid hK = K\}$

$= \{h \in H \mid h \in K\} = H \cap K$.

Άρα $H \cap K \trianglelefteq H$ και από το 1ο Θ.Ι.Ο 3.7.11:

$H/H \cap K \cong \mathrm{Im}(P|_H)$

$\{hK \mid h \in H\} = \{hK \mid hk \in HK\} = HK/K$ □

3.7.14 Παράδειγμα $V \overset{4}{:=} \{Id, [12][34], [13][24], [14][23]\}$ ομάδα του Klein

$V \trianglelefteq S_4$, $S_3 V = S_4$ (άσκηση) $\Big\} \xrightarrow{3.7.13} S_4/V \cong S_3 V/V \cong$

$\cong S_3/\underbrace{S_3 \cap V}_{\text{τετρ.}} \cong S_3$

3.7.15 3ο Θεώρημα Ισομορφισμών Ομάδων:

$K \trianglelefteq G$, $K \subseteq H \subseteq G$ → (i) $H \trianglelefteq G \Leftrightarrow H/K \trianglelefteq G/K$

K υποομάδα H υποομάδα G → (iii) Εάν $H \trianglelefteq G$, τότε

$$\boxed{G/H \cong (G/K)/(H/K)}$$

Απόδειξη: Έστω $p: G \to G/K$ ο φυσ. επιμορφισμός

(i) "$\Rightarrow$" $H \trianglelefteq G \Rightarrow p(H) = H/K \trianglelefteq G/H$

"$\Leftarrow$" Έστω ότι $H/K \trianglelefteq G/H$ θεωρούμε τον φυσικό επιμορφισμό:

$\psi: G/K \xrightarrow{\text{επί}} (G/K)/(H/K)$

$p \uparrow$, $\psi \circ p$ επιμορφισμός

G

$\operatorname{Ker}(\psi \circ p) = \{gK \in G/K \mid (gK)(H/K) = H/K\} =$

$= \{gK \in G/K \mid gK \in H/K\} = H \trianglelefteq G$

(iii) Το 1ο ΘΙΟ 3.7.11, εφαρμοζόμενο για τον επιμορφισμό $\psi \circ p$, μας δίνει $G/\operatorname{Ker}(\psi \circ p) = G/H \cong \operatorname{Im}(\psi \circ p) =$

$= (G/K)/(H/K)$ □

3.7.16 Παράδειγμα: $m, n \in \mathbb{Z}$, $m\mathbb{Z} \trianglelefteq \mathbb{Z}$ και $n\mathbb{Z} \trianglelefteq \mathbb{Z}$

$m\mathbb{Z} \trianglelefteq n\mathbb{Z} \Leftrightarrow n \mid m$

Από το 3ο ΘΙΟ 3.7.15: $(\mathbb{Z}/m\mathbb{Z})/(n\mathbb{Z}/m\mathbb{Z}) \cong$

$\cong \mathbb{Z}/n\mathbb{Z} \underset{\text{1ο ΘΙΟ 3.7.11}}{\cong} \mathbb{Z}_n$.