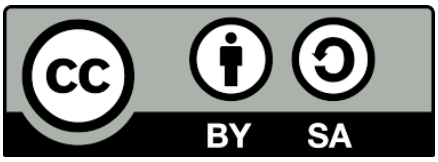
ΠΑΝΕΠΙΣΤΗΜΙΟ ΙΩΑΝΝΙΝΩΝ
ΑΝΟΙΚΤΑ ΑΚΑΔΗΜΑΪΚΑ ΜΑΘΗΜΑΤΑ

Τίτλος Μαθήματος: Αλγεβρικές Δομές Ι

Ενότητα: Υποομάδες και το Θεώρημα του Lagrange

Διδάσκων: Καθηγητής Νικόλαος Μαρμαρίδης, Καθηγητής Ιωάννης Μπεληγιάννης

Τμήμα: Μαθηματικών



Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

2. **Υποομάδες και το Θεώρημα του Lagrange**

Στο παρόν εδάφιο ενδιαφερόμαστε κυρίως για την έννοια της υποομάδας, δηλαδή ένα υποσύνολο $H \subseteq G$ μιας ομάδας $(G, \star)$ το οποίο αποτελεί ομάδα με πράξη τον περιορισμό της πράξης $\star$ στο υποσύνολο H. Στη συνέχεια θα δούμε ότι κάθε υποομάδα H ορίζει μια ενδιαφέρουσα σχέση ισοδυναμίας επί του συνόλου G, και επιπλέον, όταν το σύνολο G είναι πεπερασμένο, η επαγόμενη διαμέριση του G, δέιχνει ότι το πλήθος των στοιχείων της H διαιρεί το πλήθος των στοιχείων του G.

Υπενθυμίζουμε πρώτα την έννοια της ομάδας.

Ορισμός 2.1. *Μια* **ομάδα** *είναι ένα ζεύγος $(G, \star)$, όπου G είναι ένα σύνολο, και*

$$\star : G \times G \longrightarrow G, \quad \star(x, y) = x \star y$$

μια πράξη επί του G, για την οποία ικανοποιούνται τα ακόλουθα αξιώματα:

1. *Η πράξη $\star$ είναι* **προσεταιριστική**, *δηλαδή ισχύει:*

$$\forall x, y, z \in X : \qquad x \star (y \star z) = (x \star y) \star z$$

2. *Υπάρχει ένα στοιχείο $e \in G$, το οποίο καλείται* **ουδέτερο** *ή* **ταυτοτικό στοιχείο** *της G, έτσι ώστε να ισχύει:*

$$\forall x \in X : \qquad x \star e = x = e \star x$$

3. *Για κάθε $x \in G$, υπάρχει ένα στοιχείο $x' \in G$, το οποίο καλείται* **αντίστροφο** *ή* **αντίθετο στοιχείο** *του x, έτσι ώστε να ισχύει:*

$$\forall x \in G,\ \exists x' \in G : \qquad x \star x' = e = x' \star x$$

Μια ομάδα $(G, \star)$ καλείται **αβελιανή** *ή* **μεταθετική** *αν:*

4. *Η πράξη $\star$ είναι* **μεταθετική**, *δηλαδή ισχύει:*

$$\forall x, y \in X : \qquad x \star y = y \star x$$

Ορισμός 2.2. *Η* **τάξη** *μιας ομάδας $(G, \star)$ ορίζεται να είναι το πλήθος $|G|$ των στοιχείων του συνόλου G και από τώρα και στο εξής θα συμβολίζεται ως εξής:*

$$\mathsf{o}(G) := |G|$$

Η ομάδα $(G, \star)$ καλείται **πεπερασμένη**, *αν $\mathsf{o}(G) < \infty$. Διαφορετικά η $(G, \star)$ καλείται* **άπειρη** *ομάδα.*

Συμβολισμός: • Αν $(G, \star)$ είναι μια ομάδα, τότε συνήθως το αντίστροφο ή αντίθετο στοιχείο του $x \in G$ θα το συμβολίζουμε με x^{-1}, δηλαδή θα γράφουμε: $x' = x^{-1}$.

Επίσης για την πράξη $\star$ της ομάδας συνήθως θα γράφουμε $\cdot$ ή τίποτα. Για παράδειγμα θα γράφουμε:

$$x \star y' = x \cdot y^{-1} \ \text{ ή } \ xy^{-1}$$

Σε κάποιες περιπτώσεις το ουδέτερο στοιχείο e θα συμβολίζεται με 1 ή 1_G προς αποφυγή σύγχυσης.

• Αν η ομάδα $(G, \star)$ είναι αβελιανή, τότε για την πράξη «$\star$» θα χρησιμοποιούμε (συνήθως αλλά όχι πάντα) τον συμβολισμό «$+$». Επίσης το αντίστροφο ή αντίθετο στοιχείο του $x \in G$ θα το συμβολίζουμε με $-x$, δηλαδή θα γράφουμε: $x' = -x$. Για παράδειγμα θα γράφουμε:

$$x \star y' = x + (-y) := x - y$$

Τέλος το ουδέτερο στοιχείο e θα συμβολίζεται με 0 ή 0_G προς αποφυγή σύγχυσης.

2.1. **Βασικές ιδιότητες υποομάδων.** Από τώρα και στο εξής: $(G, \star)$ συμβολίζει μια ομάδα.

Υπενθυμίζουμε ότι ένα υποσύνολο H της ομάδας G είναι **κλειστό στην πράξη** $\star : G \times G \longrightarrow G$ αν:

$$\forall a, b \in H : \quad a \star b \in H$$

Αν το υποσύνολο H είναι κλειστό στην πράξη $\star$ της G, τότε η απεικόνιση $\star$ επάγει μια πράξη

$$\star : H \times H \longrightarrow H$$

στην H. Προφανώς η επαγόμενη πράξη $\star$ είναι προσεταιριστική.

Ορισμός 2.3. *Έστω $(G, \star)$ μια ομάδα και H ένα υποσύνολο τής G. Το H καλείται **υποομάδα** της G, αν:*

(1) *Το υποσύνολο $H \subseteq G$ είναι κλειστό στην πράξη της G.*
(2) *Το ζεύγος $(H, \star)$ αποτελεί ομάδα.*

Λήμμα 2.4. *Έστω ότι $(G, \star)$ είναι μια ομάδα και ότι H είναι μια υποομάδα της.*

(α') *Το ουδέτερο στοιχείο e_H τής H συμπίπτει με το ουδέτερο στοιχείο e_G τής G.*
(β') *Για κάθε $a \in H$, το αντίστροφό του a_H^{-1} στην H συμπίπτει με το αντίστροφό του a^{-1} στην G.*

Απόδειξη. (α') Παρατηρούμε ότι $e_H \star e_H = e_H$, επειδή το e_H είναι το ουδέτερο τής H και $e_H \star e_G = e_H$, επειδή το e_G είναι το ουδέτερο τής G. Επομένως, τα e_H και e_G είναι και τα δύο λύσεις τής εξίσωσης $e_H \star x = e_H$, ως προς x, στην ομάδα G. Αφού όμως η G είναι ομάδα, η προηγούμενη εξίσωση έχει ακριβώς μια λύση. Επομένως, $e_H = e_G$.

(β') Παρατηρούμε ότι $a \star a_H^{-1} = e_G$ και $a \star a^{-1} = e_G$. Συνεπώς, τα a_H^{-1} και a^{-1} είναι και τα δύο λύσεις τής εξίσωσης $a \star x = e_G$, ως προς x, στην ομάδα G. Αφού όμως η G είναι ομάδα, η προηγούμενη εξίσωση έχει ακριβώς μια λύση, επομένως, $a_H^{-1} = a^{-1}$. □

Λήμμα 2.5. *Έστω $(G, \star)$ μια ομάδα και H ένα υποσύνολό της. Τότε τα ακόλουθα είναι ισοδύναμα:*

(1) *Το H αποτελεί μια υποομάδα τής $(G, \star)$.*
(2) *$\emptyset \neq H$ και:*

$$\forall a, b \in H : \quad a \star b^{-1} \in H$$

Απόδειξη. $(1) \Longrightarrow (2)$ Έστω ότι το H είναι μια υποομάδα. Τότε, σύμφωνα με τον ορισμό τής υποομάδας, το H δεν είναι το κενό σύνολο. Επιπλέον, αν το (a, b) είναι στοιχείο τού $H \times H$, τότε το b ανήκει στην H και κατόπιν το b^{-1} ανήκει στην H, βλ. Λήμμα 2.4(β') και επειδή η H είναι υποομάδα, το $a \star b^{-1}$ είναι επίσης στοιχείο τής H.

$(2) \Longrightarrow (1)$ Υπάρχει κάποιο $a \in G$ με $a \in H$, αφού το $H \neq \emptyset$. Όμως τότε, το (a, a) είναι στοιχείο τού $H \times H$ και γι' αυτό, από την υπόθεση, το στοιχείο $a \star a^{-1} = e_G$ είναι στοιχείο τού H.

Για κάθε $a \in H$, το στοιχείο (e_G, a) είναι στοιχείο τού $H \times H$ και γι' αυτό, σύμφωνα με την υπόθεση, το στοιχείο $e_G \star a^{-1} = a^{-1}$ είναι στοιχείο τού H.

Θα δείξουμε τώρα ότι ο περιορισμός τής «$\star$» στο $H \times H$ ορίζει μια απεικόνιση από το $H \times H$ στο H, δηλαδή ότι αν $(a, b) \in H \times H$, τότε το $a \star b$ είναι στοιχείο τού H. Όταν όμως $(a, b) \in H \times H$, τότε $b \in H$ και όπως είδαμε παραπάνω το $b^{-1} \in H$. Συνεπώς, το ζεύγος (a, b^{-1}) ανήκει στο $H \times H$ και γι' αυτό εφαρμόζοντας και πάλι την υπόθεση, το στοιχείο $a \star (b^{-1})^{-1}$ ανήκει στο H. Αλλά $(b^{-1})^{-1} = b$, και επομένως το στοιχείο $a \star b$ είναι στοιχείο τού H.

Τέλος, επειδή η «$\star$» είναι μια προσεταιριστική πράξη επί των στοιχείων τής G, είναι φανερό ότι παραμένει προσεταιριστική και επί των στοιχείων τού υποσυνόλου H. Επομένως, η H είναι μια υποομάδα τής G. □

Παράδειγμα 2.6. *Είναι γνωστό ότι το σύνολο*

$$\mathsf{GL}_n(\mathbb{K}) = \left\{ A \in \mathsf{M}_n(\mathbb{K}) \mid \mathsf{det}(A) \neq 0 \right\}$$

των $n \times n$ αντιστρέψιμων πινάκων με συνιστώσες από ένα σώμα $\mathbb{K}$ εφοδιασμένο με την πράξη «$\cdot$» του πολλαπλασιασμού πινάκων αποτελεί μια ομάδα.

Θεωρούμε το υποσύνολο

$$\mathsf{SL}_n(\mathbb{K}) = \big\{A \in \mathrm{GL}_n(\mathbb{K}) \;\mid\; \mathsf{det}(A) = 1\big\}$$

Θα εφαρμόσουμε το Λήμμα 2.5 για να αποδείξουμε ότι το $\mathsf{SL}_n(\mathbb{K})$ *είναι υποομάδα της* $\mathsf{GL}_n(\mathbb{K})$. *Παρατηρούμε πρώτα ότι το* $\mathrm{SL}_n(\mathbb{K}) \neq \emptyset$, *αφού ο ταυτοτικός* $n \times n$ *πίνακας* I_n *είναι στοιχείο του συνόλου* $\mathsf{SL}_n(\mathbb{K})$. *Τώρα σύμφωνα με το Λήμμα 2.5, αρκεί να αποδείξουμε ότι αν* $A, B \in \mathsf{SL}_n(\mathbb{K})$, *τότε και ο πίνακας* $A \cdot B^{-1}$ *ανήκει επίσης στο* $\mathsf{SL}_n(\mathbb{K})$. *Πράγματικά έχουμε*

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

Σε μερικές περιπτώσεις ο έλεγχος αν ένα υποσύνολο μιας υποομάδας αποτελεί υποομάδα, είναι εξαιρετικά απλός, όπως δείχνει το επόμενο Λήμμα:

Λήμμα 2.7. *Έστω* $(G, \star)$ *μια ομάδα και* H *ένα μη κενό υποσύνολό της με πεπερασμένο το πλήθος στοιχεία. Αν το* H *είναι κλειστό ως προς την πράξη «*$\star$*» της* G, *τότε το* H *αποτελεί μια υποομάδα της* G.

Απόδειξη. Το ότι το σύνολο H είναι κλειστό ως προς την πράξη σημαίνει ότι $\forall a, b \in H$, το στοιχείο $a \star b$ ανήκει επίσης στην H και γι' αυτό ορίζεται η πράξη

$$\star : \; H \times H \;\longrightarrow\; H, \qquad (a, b) \;\longmapsto\; a \star b.$$

Σύμφωνα με τον Ορισμό 2.3 και το Λήμμα 2.4, για να είναι τώρα η H υποομάδα της G, πρέπει το ουδέτερο στοιχείο e_G να ανήκει στο H και για κάθε $a \in H$, το αντίστροφό του a^{-1} (το οποίο υπάρχει στην G) να ανήκει επίσης στο H.

Αφού το H είναι πεπερασμένο σύνολο, μπορούμε να υποθέσουμε ότι $H = \{a_1, a_2, \ldots, a_n\}$ με $n \in \mathbb{N}$. Ας είναι a ένα οποιοδήποτε αλλά συγκεκριμένο στοιχείο της H. Θεωρούμε την απεικόνιση

$$\ell_a : \; H \;\longrightarrow\; H, \;\; a_i \;\longmapsto\; \ell_a(a_i) := a \star a_i.$$

Η ℓ_a είναι μια «1-1» απεικόνιση, αφού αν a_i, a_j είναι στοιχεία της H με $\ell_a(a_i) = \ell_a(a_j)$, τότε $a \star a_i = a \star a_j$ και επομένως[21] $a^{-1} \star (a \star a_i) = a^{-1} * (a \star a_j)$, δηλαδή $a_i = a_j$. Αλλά μια «1-1» απεικόνιση από το πεπερασμένο σύνολο H στον εαυτό του είναι **και** «επί». Συνεπώς, υπάρχει κάποιο $a_j \in H$ με $a = \ell_a(a_j)$, δηλαδή $a = a \star a_j$. Άρα, $e_G = a_j \in H$. Ώστε το ουδέτερο στοιχείο της G ανήκει στην H.

Επιπλέον, αφού η ℓ_a είναι «επί» και αφού τώρα γνωρίζουμε ότι $e_G \in H$, συμπεραίνουμε ότι υπάρχει $a_j \in H$ με $\ell_a(a_j) = e_G$, δηλαδή $a \star a_j = e_G$. Συνεπώς, $a_j = a^{-1}$ και έτσι το $a_j \in H$ είναι το αντίστροφο τού στοιχείου a. □

2.2. **Ομάδες προερχόμενες από την ομάδα** $\mathbb{Z}$ **των ακεραίων.** Θεωρούμε την ομάδα $(\mathbb{Z}, +)$ των ακεραίων με πράξη την πρόσθεση. Η $(\mathbb{Z}, +)$ είναι μια άπειρη αβελιανή ομάδα. Στην παρούσα ενότητα θα δούμε κάποιες ομάδες οι οποίες προέρχονται από την ομάδα $\mathbb{Z}$.

2.2.1. *Η υποομάδα* $(n\mathbb{Z}, +)$. Για κάθε $n \geq 1$, το σύνολο

$$n\mathbb{Z} = \big\{nm \in \mathbb{Z} \mid m \in \mathbb{Z}\big\}$$

ακεραίων πολλαπλασίων του n είναι προφανώς μια (άπειρη) υποομάδα του $\mathbb{Z}$.

[21] Το αντίστροφο a^{-1} τού a υπάρχει στην G, αφού η G είναι ομάδα.

2.2.2. *Η προσθετική ομάδα* $(\mathbb{Z}_n, +)$. Έστω $n \geq 1$. Στο σύνολο $\mathbb{Z}$ θεωρούμε τη σχέση $\mathcal{R}_n$ η οποία ορίζεται ως εξής:

$$\forall a, b \in \mathbb{Z}: \quad a \sim_{\mathcal{R}_n} b \quad \Longleftrightarrow \quad n \,|\, a - b$$

Τότε η $\mathcal{R}_n$ είναι μια σχέση ισοδυναμίας επί του $\mathbb{Z}$, η οποία είναι συμβιβαστή με την πράξη της πρόσθεσης και επομένως από την Πρόταση 1.17 το σύνολο πηλίκο

$$\mathbb{Z}_n = \big\{[k] \subseteq \mathbb{Z} \mid 0 \leq k \leq n-1\big\}$$

αποτελεί ομάδα με πράξη την πρόσθεση η οποία επάγεται από την πρόσθεση ακεραίων. Η ομάδα $(\mathbb{Z}_n, +)$ είναι μια πεπερασμένη αβελιανή ομάδα με n το πλήθος στοιχεία.

2.2.3. *Η πολλαπλασιαστική ομάδα* $(\mathsf{U}(\mathbb{Z}_n), \cdot)$. Η παραπάνω σχέση ισοδυναμίας $\mathcal{R}_n$ είναι επίσης συμβατή με την πράξη του πολλαπλασιασμού στο σύνολο $\mathbb{Z}$ των ακεραίων. Έτσι αποκτούμε μιοα καλά ορισμένη πράξη πολλαπλασιασμού

$$\cdot : \ \mathbb{Z}_n \times \mathbb{Z}_n \ \longrightarrow \ \mathbb{Z}_n, \qquad [a]_n \cdot [b]_n = [ab]_n$$

Προφανώς αυτή η πράξη είναι προσεταιριστική και μεταθετική και έχει το στοιχείο $[1]_n$ ως ταυτοτικό στοιχείο.

Όμως το ζεύγος $(\mathbb{Z}_n, \cdot)$ δεν αποτελεί ομάδα διότι υπάρχουν στοιχεία του $\mathbb{Z}_n$ τα οποία δεν έχουν αντίστροφο ως προς την πράξη του πολλαπασιασμού, π.χ. το $[0]_n$. Αυτό που πρέπει λοιπόν να κάνουμε για να αποκτήσουμε δομή ομάδας είναι να περιορισθούμε στο σύνολο των στοιχείων του $\mathbb{Z}_n$ τα οποία έχουν αντίστροφο ως προς την πράξη του πολλαπλασιασμού.

Όμως:

$$\text{το στοιχείο} \quad [k]_n \quad \text{έχει πολλαπλασιαστικό αντίστροφο στο σύνολο} \ \ \mathbb{Z}_n \quad \Longleftrightarrow \quad (k, n) = 1$$

Πραγματικά: αν $(k, n) = 1$, τότε ως γνωστόν υπάρχουν ακέραιοι $u, v \in \mathbb{Z}$: $uk + vn = 1$. Τότε στο $\mathbb{Z}_n$ θα έχουμε:

$$[u]_n[k]_n + [v]_n[n]_n = [1]_n \quad \Longrightarrow \quad [u]_n[k]_n + [v]_n[0]_n = [1]_n \quad \Longrightarrow \quad [u]_n[k]_n + [0]_n = [1]_n$$
$$\Longrightarrow \quad [u]_n[k]_n = [1]_n = [k]_n[u]_n$$

Επομένως το στοιχείο $[k]_n$ είναι αντιστρέψιμο με αντίστροφο το στοιχείο $[u]_n$. Αντίστροφα αν αυτό ισχύει, τότε

$$[u]_n[k]_n = [uk]_n = [1]_n \quad \Longrightarrow \quad n/1-uk \quad \Longrightarrow \quad 1-uk = nv \quad \Longrightarrow \quad uk+nv = 1 \quad \Longrightarrow \quad (n, k) = 1$$

Επομένως το ζεύγος $(\mathsf{U}(\mathbb{Z}_n), \cdot)$, όπου:

$$\mathsf{U}(\mathbb{Z}_n) = \big\{[k]_n \in \mathbb{Z}_n \mid (k, n) = 1\big\}$$

αποτελεί μια, προφανώς πεπερασμένη αβελιανή, ομάδα.

Η ομάδα $\mathsf{U}(\mathbb{Z}_n)$ καλείται η **ομάδα των αντιστρεψίμων στοιχείων του** $\mathbb{Z}_n$ και η τάξη της είναι ίση με:

$$\varphi(n) = \big|\big\{k \in \mathbb{Z} \ \mid \ 1 \leq k \leq n \ \&\ (k, n) = 1\big\}\big|$$

την τιμή της **συνάρτησης** φ **του Euler στο** n.

2.3. **Υποομάδες και Σχέσεις Ισοδυναμίας.** Έστω $(G, \star)$ μια ομάδα. Ως συνήθως συμβολίζουμε με e το ουδέτερο στοιχείο της ομάδας G και με a^{-1} το αντίστροφο του στοιχείου $a \in G$.

Για κάθε υποσύνολο $H \subseteq G$ του συνόλου G, ορίζουμε τις ακόλουθες σχέσεις $\mathcal{R}_H$ και ${}_H\mathcal{R}$ επί του G:

$$\forall x, y \in G: \quad x \sim_{\mathcal{R}_H} y \quad \Longleftrightarrow \quad x^{-1} \star y \in H$$
$$\forall x, y \in G: \quad x \sim_{{}_H\mathcal{R}} y \quad \Longleftrightarrow \quad x \star y^{-1} \in H$$

Πρόταση 2.8. *Τα ακόλουθα είναι ισοδύναμα:*

(1) *Το υποσύνολο* H *είναι υποομάδα της* $(G, \star)$.

(2) *Η σχέση* $\mathcal{R}_H$ *είναι σχέση ισοδυναμίας επί του συνόλου* G.
(3) *Η σχέση* ${}_H\mathcal{R}$ *είναι σχέση ισοδυναμίας επί του συνόλου* G.

Απόδειξη. (1) $\Longrightarrow$ (2) Θα έχουμε:

- $\forall x \in G$: $x \sim_{\mathcal{R}_H} x$ διότι $x^{-1} \star x = e \in H$ επειδή η H είναι υποομάδα.
- $\forall x, y \in G$, έστω $x \sim_{\mathcal{R}_H} y$ και άρα $x^{-1} \star y \in H$. Επειδή η H είναι υποομάδα, έπεται ότι

$$(x^{-1} \star y)^{-1} \in H \implies y^{-1} \star (x^{-1})^{-1} = y^{-1} \star x \in H$$

και άρα $y \sim_{\mathcal{R}_H} x$.

- $\forall x, y, z \in G$, έστω $x \sim_{\mathcal{R}_H} y$ και $y \sim_{\mathcal{R}_H} z$. Τότε $x^{-1} \star y \in H$ και $y^{-1} \star z \in H$. Επειδή η H είναι υποομάδα θα έχουμε:

$$(x^{-1} \star y) \star (y^{-1} \star z) = x^{-1} \star y \star y^{-1} \star z = x^{-1} \star e \star z = x^{-1} \star z \in H$$

και άρα $x \sim_{\mathcal{R}_H} z$.

Επομένως η σχέση $\mathcal{R}_H$ είναι σχέση ισοδυναμίας επί του συνόλου G.

(2) $\Longrightarrow$ (1) Θα έχουμε:

- Επειδή $\forall x \in G$: $x \sim_{\mathcal{R}_H} x$ και $e \in G$, θα έχουμε $e \sim_{\mathcal{R}_H} e$ δηλαδή $e^{-1} \star e = e \in H$. Έτσι $e \in H$ και ιδιαίτερα $H \neq \emptyset$.
- Έστω $x, y \in H$. Τότε:

$$H \ni x = e \star x = e^{-1} \star x \implies e \sim_{R_H} x \qquad \text{και} \qquad H \ni y = e \star y = e^{-1} \star y \implies e \sim_{R_H} y$$

Επειδή η σχέση $\mathcal{R}_H$ είναι σχέση ισοδυναμίας, θα έχουμε: $x \sim_{R_H} e$ και $e \sim_{R_H} y$, δηλαδή $x^{-1} \star e = x^{-1} \in H$ και $y^{-1} \star e = y^{-1} \in H$. Ιδιαίτερα: $x^{-1} \in H$, $\forall x \in H$.

Τέλος από τις παραπάνω σχέσεις θα έχουμε $x^{-1} \sim_{R_H} e$ και $e \sim_{\mathcal{R}_H} y^{-1}$. Λόγω της μεταβατικής ιδιότητας θα έχουμε: $x^{-1} \sim_{R_H} y^{-1}$ το οποίο σημαίνει ότι $(x^{-1})^{-1} \star y^{-1} = x \star y^{-1} \in H$. Απο το Λήμμα 2.5 τότε έπεται ότι το υποσύνολο H είναι υποομάδα της G.

Η απόδειξη (1) $\Longleftrightarrow$ (3) είναι παρόμοια και αφήνεται ως άσκηση. □

Από τωρα και στο εξής υποθέτουμε ότι: το υποσύνολο H είναι μια υποομάδα της ομάδας $(G, \star)$.

Τότε γνωρίζουμε ότι οι σχέσεις $\mathcal{R}_H$ και ${}_H\mathcal{R}$ είναι σχέσεις ισοδυναμίας επί του συνόλου G. Για κάθε $x \in G$, συμβολίζουμε με:

$$[x]_H = \{y \in G \mid y \sim_{R_H} x\} \qquad \text{και} \qquad {}_H[x] = \{y \in G \mid y \sim_{{}_H\mathcal{R}} x\}$$

την κλάση ισοδυναμίας του $x \in G$ ως προς τις σχέσεις ισοδυναμίας $\mathcal{R}_H$ και ${}_H\mathcal{R}$ αντίστοιχα.

Λήμμα 2.9. $\forall x \in G$*:*

$$[x]_H = x \star H := \{x \star h \in G \mid h \in H\}$$
$${}_H[x] = H \star x := \{h \star x \in G \mid h \in H\}$$

Απόδειξη. Για την πρώτη σχέση θα έχουμε (η δεύτερη αποδεικνύεται παρόμοια):

$$[x]_H = \{y \in G \mid y \sim_{R_H} x\} = \{y \in G \mid x \sim_{\mathcal{R}_H} y \in H\} = \{y \in G \mid x^{-1} \star y \in H\} =$$
$$= \{y \in G \mid x^{-1} \star y = h \in H\} = \{y \in G \mid y = x \star h, \ \ h \in H\} = \{x \star h \in G \mid h \in H\} = x \star H \quad \square$$

Ορισμός 2.10. *Η κλάση ισοδυναμίας* $[x]_H$ *του στοιχείου* $x \in G$ *ως προς την σχέση ισοδυναμίας* $\mathcal{R}_H$ *καλείται* **αριστερό σύμπλοκο** *του* x *ως προς την υποομάδα* H *και συμβολίζεται ως εξής:* $x \star H$.

Η κλάση ισοδυναμίας ${}_H[x]$ *του στοιχείου* $x \in G$ *ως προς την σχέση ισοδυναμίας* ${}_H\mathcal{R}$ *καλείται* **δεξιό σύμπλοκο** *του* x *ως προς την υποομάδα* H *και συμβολίζεται ως εξής:* $H \star x$.

Λήμμα 2.11. (1) $\forall x \in G$*: τα σύμπλοκα* $x \star H$ *και* $H \star x$ *έχουν το ίδιο πλήθος στοιχείων.*

(2) *Τα σύνολα-πηλίκα $G/\mathcal{R}_H$ και $G/_H\mathcal{R}$ έχουν το ίδιο πλήθος στοιχείων, δηλαδή: Το πλήθος των διακεκριμμένων αριστερών συμπλόκων της H στην G συμπίπτει με το πλήθος των διακεκριμμένων δεξιών συμπλόκων της H στην G.*

Απόδειξη. (1) Για κάθε $x \in G$, ορίζοντας

$$\phi:\ x\star H \ \longrightarrow\ H\star x, \quad \phi(x\star h) = h\star x$$

βλέπουμε εύκολα ότι αποκτούμε μια καλά ορισμένη απεικόνιση η οποία είναι 1-1 και επί.

(2) Ορίζοντας

$$\psi:\ G/\mathcal{R}_H \ \longrightarrow\ G/_H\mathcal{R}, \quad \psi(x\star H) = H\star x^{-1}$$

Θα δείξουμε ότι η ϕ είναι μια 1-1 και επί απεοκόνιση.

- Κατ' αρχήν η ψ είναι καλά ορισμένη: έστω $x\star H = y\star H$ και άρα $x\sim_{\mathcal{R}_H} y$. Τότε $x^{-1}\star y\in H$. Έστω $x^{-1}\star y = h\in H$. Τότε $x^{-1} = h\star y^{-1}\in H\star y^{-1} = {}_H[y^{-1}]$. Όπως γνωρίζουμε τότε τα στοιχεία x^{-1} και y^{-1} ορίζουν την ίδια κλάση ισοδυναμίας ως προς την σχέση ισοδυναμίας ${}_H\mathcal{R}$ και επομένως θα έχουμε ${}_H[x^{-1}] = {}_H[y^{-1}]$. Αυτό όμως σημαίνει ότι $H\star x^{-1} = H\star y^{-1}$ και άρα $\psi(x\star H) = \psi(y\star H)$, δηλαδή η ψ είναι καλά ορισμένη.
- Έστω $\psi(x\star H) = \psi(y\star H)$, δηλαδή $H\star x^{-1} = H\star y^{-1}$ ή ισοδύναμα ${}_H[x^{-1}] = {}_H[y^{-1}]$. Τότε όμως $x^{-1}\sim_{{}_H\mathcal{R}} y^{-1}$ και άρα $x^{-1}\star(y^{-1})^{-1}\in H$. Δηλαδή $x^{-1}\star y\in H$ και επομένως $x^{-1}\star y = h\in H$. Τότε $y = x\star h\in x\star H = [x]_H$ και άρα $[y]_H = [x]_H \implies y\star H = x\star H$. Επομένως η ψ είναι 1-1.
- Έστω ${}_H[z] = H\star z\in G/_H\mathcal{R}$. Τότε προφανώς $\psi([z^{-1}]_H) = \psi(z^{-1}\star H) = H\star(z^{-1})^{-1} = H\star z$ και άρα η ψ είναι επί. □

Από τώρα και στο εξής: εργαζόμαστε με την σχέση ισοδυναμίας $\mathcal{R}_H$:

$$\forall x,y\in G:\ \ x\sim_{\mathcal{R}_H} y \quad\Longleftrightarrow\quad x^{-1}\star y\ \in H$$

Ανάλογα συμπεράσματα ισχύουν για την σχέση ισοδυναμίας ${}_H\mathcal{R}$.

Λήμμα 2.12. *Έστω $x,y\in G$. Τότε οι κλάσεις ισοδυναμίας $[x]_H$ και $[y]_H$ έχουν το ίδιο πλήθος στοιχείων. Ακριβέστερα η απεικόνιση*

$$\phi:\ [x]_H = x\star H \ \longrightarrow\ [y]_H = y\star H, \qquad \phi(x\star h) = y\star h$$

είναι 1-1 και επί.

Απόδειξη. Έστω $\phi(x\star h_1) = \phi(x\star h_2)$, δηλαδή $y\star h_1 = y\star h_2$. Τότε προφανώς, από τον Νόμο Διαγραφής, θα έχουμε $h_1 = h_2$ και άρα $x\star h_1) = x\star h_2$. Επομένως η ψ είναι 1-1.

Αν $y\star h\in y\star H$, τότε $\psi(x\star h) = y\star h$ και άρα η ψ είναι επί. □

Πόρισμα 2.13. *Έστω $(G,\star)$ μια ομάδα και $H\subseteq G$ μια υποομάδα της G. Τότε:*

$$\forall x\in G: \qquad \mathsf{o}(H) = |H| = |x\star H|$$

Απόδειξη. Θέτοντας $y = e$ στο παραπάνω Λήμμα, θα έχουμε ότι τα σύμπλοκα $e\star H$ και $x\star H$ έχουνε το ίδιο πλήθος στοιχείων. Όμως προφανώς

$$e\star H = \big\{e\star h\in G\mid h\in H\big\} = \big\{h\in G\mid h\in H\big\} = H$$

και επομένως, $\forall x\in G$:

$$\mathsf{o}(H) = |H| = |x\star H|$$ □

2.4. **Το Θεώρημα του Lagrange.** Έστω, όπως και πριν, $(G,\star)$ μια ομάδα και $H\subseteq G$ μια υποομάδα της G. Συμβολίζουμε με

$$G/H = G/\mathcal{R}_H = \big\{[x]_H \subseteq G \mid x\in G\big\} = \big\{x\star H\subseteq G \mid x\in G\big\}$$

το σύνολο-πηλίκο της G ως προς τη σχέση ισοδυναμίας $\mathcal{R}_H$. Το σύνολο G/H καλείται το **σύνολο των αριστερών συμπλόκων** της H στην G. Όπως γνωρίζουμε το σύνολο υποσυνόλων G/H αποτελεί μια διαμέριση του G και άρα θα έχουμε:

$$G=\bigcup_{x\in G}[x]_H=\bigcup_{x\in G}x\star H$$

Ορισμός 2.14. *Έστω $(G,\star)$ μια ομάδα και $H\subseteq G$ μια υποομάδα της G. Το πλήθος των στοιχείων του συνόλου G/H καλείται ο* **δείκτης** *της H στην G και συμβολίζεται με: $[G:H]$.*

Έτσι ο δείκτης $[G:H]$ της H στην G είναι το πλήθος των διακεκριμμένων αριστερών συμπλόκων της H στην G.

Σύμφωνα με το Λήμμα 2.11 ο δείκτης $[G:H]$ της H στην G είναι επίσης το πλήθος των διακεκριμμένων δεξιών συμπλόκων της H στην G.

Ιδιαίτερα αν η ομάδα G είναι πεπερασμένη, τότε και η υποομάδα H θα είναι πεπερασμένη και το σύνολο των διακεκριμμένων κλάσεων ισοδυναμίας των στοιχείων της ως προς τη σχέση ισοδυναμίας $\mathcal{R}_H$ θα είναι πεπερασμένο. Δηλαδή το σύνολο-πηλίκο G/H των αριστερών συμπλόκων της H στην G θα είναι πεπερασμένο.

Είδαμε ότι το πλήθος των αριστερών συμπλόκων μιας υποομάδας είναι ίσο με το πληθος των δεξιών συμπλόκων της υποομάδας. Αυτό δεν σημαίνει ότι ένα αριστερό σύμπλοκο είναι και δεξιό:

Παράδειγμα 2.15. *Θεωρούμε την συμμετρική ομάδα:*

$$S_3=\big\{(1),\ (12),\ (13),\ (23),\ (123),\ (132)\big\}$$

Τότε $H=\big\{(1),\ (12)\big\}$ είναι μια υποομάδα της S_3 και τα διεκεκριμμένα αριστερά σύμπλοκα της H στην S_3 είναι:

$$\big\{(1),(12)\big\},\quad \big\{(13),(123)\big\},\quad \big\{(23),(132)\big\}$$

Βλέπουμε ότι το δεξιό σύμπλοκο $H(13)=\big\{(13),(132)\big\}$ δεν συμπίπτει με κανένα αριστερό σύμπλοκο. Γενικότερα βλέπουμε ότι τα δεξιά σύμπλοκα της H της S_3 είναι

$$\big\{(1),(12)\big\},\quad \big\{(13),(132)\big\},\quad \big\{(23),(123)\big\}$$

άρα είναι όπως περιμένουμε τρία και κανένα δεξιό σύμλοκο (εκτός του H) δεν συμπίπτει με κανένα αριστερό σύμλοκο.

Έστω τώρα $(G,\star)$ μια πεπερασμένη ομάδα και H μια υποομάδα της G. Έστω:

(1) $\mathsf{o}(G)=n$
(2) $\mathsf{o}(H)=m$
(3) $[G:H]=k$ και έστω $G/H=\big\{[x_1]_H,[x_2]_H,\cdots,[x_k]_H\big\}=\big\{x_1\star H,x_2\star H,\cdots,x_k\star H\big\}$.

Επειδή τα υποσύνολα $[x_1]_H,[x_2]_H,\cdots,[x_k]_H$ αποτελούν μια διαμέριση του G, έπεται ότι θα έχουμε:

$$G=[x_1]_H\bigcup[x_2]_H\bigcup\cdots\bigcup[x_k]_H\qquad\text{και}\qquad [x_i]_H\bigcap[x_j]_H=\emptyset,\quad 1\le i\ne j\le k$$

Το ακόλουθο Θεώρημα, το οποίο οφείλεται στον Lagrange και είναι θεμελιώδες στην Θεωρία Ομάδων, δείχνει ότι με τους παραπάνω συμβολισμούς: $n=m\cdot k$, δηλαδή η τάξη της H διαιρεί την τάξη της G:

Θεώρημα 2.16. *(**Lagrange (1771)**) Έστω G μια πεπερασμένη ομάδα και H μια υποομάδα της G. Τότε:*

$$\mathsf{o}(G) = \mathsf{o}(H) \cdot [G : H]$$

Επομένως η τάξη μιας υποομάδας H μιας πεπερασμένης ομάδας G διαιρεί την τάξη της ομάδας:

$$\mathsf{o}(H) \,\big/\, \mathsf{o}(G)$$

Απόδειξη. Επειδή

$$G = [x_1]_H \bigcup [x_2]_H \bigcup \cdots \bigcup [x_k]_H$$

είναι μια διαμέριση του συνόλου G, σύμφωνα με την Παρατήρηση 1.6, θα έχουμε:

$$|G| = \sum_{i=1}^{k} |[x_i]_H| = \sum_{i=1}^{k} |x_i \star H|$$

Από το Πόρισμα 2.13, έχουμε: $|x_i \star H| = \mathsf{o}(H)$, $\forall i = 1, 2, \cdots, k$. Έτσι η παραπάνω σχέση δίνει:

$$\mathsf{o}(G) = |G| = \sum_{i=1}^{k} |x_i \star H| = k \cdot |H| = k \cdot \mathsf{o}(H) = [G : H] \cdot \mathsf{o}(H)$$ □

2.5. **Οι Υποομάδες της S_3.** Υπενθυμίζουμε ότι:

$$S_3 = \big\{(1),\ (12),\ (13),\ (23),\ (123),\ (132)\big\}$$

Πίνακας πολλαπλασιασμού της S_3

$\circ$	**(1)**	**(12)**	**(13)**	**(23)**	**(123)**	**(132)**
(1)	(1)	(12)	(13)	(23)	(123)	(132)
(12)	(12)	(1)	(132)	(123)	(23)	(13)
(13)	(13)	(123)	(1)	(132)	(12)	(23)
(23)	(23)	(132)	(123)	(1)	(13)	(12)
(123)	(123)	(13)	(23)	(12)	(132)	(1)
(132)	(132)	(23)	(12)	(13)	(1)	(123)

Τα ακόλουθα υποσύνολα είναι όλες οι υποομάδες της S_3:

(1) Υπομοάδες Τάξης 1: $H_0 = \{(1)\}$.
(2) Υπομοάδες Τάξης 2: $H_1 = \{(1), (12)\}$, $H_2 = \{(1), (13)\}$, $H_3 = \{(1), (23)\}$.
(3) Υπομοάδες Τάξης 3: $H_4 = \{(1), (123), (132)\}$.
(4) Υπομοάδες Τάξης 6: $H_5 = S_3$.

Επομένως βλέπουμε οτι για την S_3 ισχύει το αντίστροφο του Θεωρήματος του Lagrange, δηλαδή για κάθε διαιρέτη της $\mathsf{o}(S_3)$ υπάρχει (τουλάχιστον μια) υποομάδα της S_3 με τάξη τον διαιρέτη.

2.6. **Το αντίστροφο του Θεωρήματος του Lagrange και η Εναλλάσσουσα Ομάδα A_4.** Το αντίστροφο τοθ Θεωρήματος του Lagrange γενικά δεν ισχύει. Όπως θα δούμε αργότερα, υπάρχουν πεπερασμένες ομάδες G και διαιρέτες k της τάξης της ομάδας έτσι ώστε η G να μην έχει υποομάδες τάξης k.

Η μικρότερη ομάδα για την οποία το αντίστροφο τοθ Θεωρήματος του Lagrange δεν ισχύει, είναι η εναλλάσσουσα ομάδα A_4 με τάξη 12. Η A_4 έχει υποομάδες τάξης $1, 2, 3, 4, 12$ αλλά δεν έχει καμμία υποομάδα τάξης 6.

Υπενθυμίζουμε ότι η A_4 είναι η υποομάδα της συμμετρικής ομάδας S_4 η οποία αποτελείται από τις άρτιες μεταθέσεις:

$$A_4 = \big\{(1),\ (123),\ (124),\ (134),\ (234),\ (132),\ (142),\ (143),\ (243),\ (12)(34),\ (13)(24),\ (14)(23)\big\}$$

Ειδικότερα η A_4 αποτελείται, εκτός από την ταυτοτική μετάθεση (1), από τους οκτώ 3-κύκλους και τα τρία γινόμενα των ξένων 2-κύκλων. Παρακάτω, χάριν ευκολίας και για μεταγενέστερη χρήση, δίνουμε τον πίνακα πολλαλπασιασμού της ομάδας A_4:

Πίνακας πολλαπλασιασμού της A_4

$\circ$	**(1)**	**(123)**	**(124)**	**(134)**	**(234)**	**(132)**	**(142)**	**(143)**	**(243)**	**(12)(34)**	**(13)(24)**	**(14)(23)**
(1)	(1)	(123)	(124)	(134)	(234)	(132)	(142)	(143)	(243)	(12)(34)	(13)(24)	(14)(23)
(123)	(123)	(132)	(13)(24)	(234)	(12)(34)	(1)	(143)	(14)(23)	(124)	(134)	(243)	(142)
(124)	(124)	(14)(23)	(142)	(13)(24)	(123)	(134)	(1)	(243)	(12)(34)	(143)	(132)	(234)
(134)	(134)	(124)	(12)(34)	(143)	(13)(24)	(14)(23)	(234)	(1)	(132)	(123)	(142)	(243)
(234)	(234)	(13)(24)	(134)	(14)(23)	(243)	(142)	(12)(34)	(123)	(1)	(132)	(143)	(124)
(132)	(132)	(1)	(243)	(12)(34)	(134)	(123)	(14)(23)	(142)	(13)(24)	(234)	(124)	(143)
(142)	(142)	(234)	(1)	(132)	(14)(23)	(13)(24)	(124)	(12)(34)	(143)	(243)	(134)	(123)
(143)	(143)	(12)(34)	(123)	(1)	(142)	(243)	(13)(24)	(134)	(14)(23)	(124)	(234)	(132)
(243)	(243)	(143)	(14)(23)	(124)	(1)	(12)(34)	(132)	(13)(24)	(234)	(142)	(123)	(134)
(12)(34)	(12)(34)	(243)	(234)	(142)	(124)	(143)	(134)	(132)	(123)	(1)	(14)(23)	(13)(24)
(13)(24)	(13)(24)	(142)	(143)	(243)	(132)	(234)	(123)	(124)	(134)	(14)(23)	(1)	(12)(34)
(14)(23)	(14)(23)	(134)	(132)	(123)	(143)	(124)	(243)	(234)	(142)	(13)(24)	(12)(34)	(1)

Πρόταση 2.17. *Η εναλλάσσουσα ομάδα A_4 τάξης 12:*

(1) *έχει υποομάδες τάξης 1, 2, 3, 4, και 12.*

(2) *δεν έχει υποομάδα τάξης 6.*

Απόδειξη. (2) Υποθέτουμε ότι H είναι μια υποομάδα της A_4 με $\mathsf{o}(H) = 6$. Τότε προφανώς ο δείκτης

$$[A_4 : H] = 2$$

και επομένως η H έχει 2 διακεκριμμένα αριστερά σύμπλοκα στην A_4.

Θα δείξουμε ότι κάθε στοιχείο της A_4 το οποίο είναι της μορφής g^2, όπου $g \in A_4$, ανήκει στην H:

$$\mathcal{M} = \left\{g^2 \in A_4 \mid g \in A_4\right\} \subseteq H \qquad (*)$$

Πράγματι: έστω $g \in A_4$. Αν $g \in H$, τότε $g^2 \in H$ διότι η H είναι υποομάδα της A_4. Αν $g \notin H$, τότε τα σύμπλοκα $(1)H = H$ και gH, δεν συμπίπτουν, διότι διαφορετικά αν $H = gH$, τότε $g \in H$ που είναι άτοπο. Άρα επειδή τα σύμπλοκα $(1)H = H$ και gH είναι διαφορετικά και επειδή η H έχει 2 διακεκριμμένα αριστερά σύμπλοκα στην A_4, έπεται ότι τα σύμλοκα H και gH αποτελούν μια διαμέριση της A_4,και άρα:

$$A_4 = H \cup gH, \qquad H \cap gH = \emptyset$$

Το σύμπλοκο g^2H θα συμπίπτει με ένα εκ των H και gH. Αν $g^2H = gH$, τότε $(g^2)^{-1} \circ g = g^{-2} \circ g = g^{-1} \in H$. Επειδή η H είναι υποομάδα, θα έχουμε $g \in H$ το οποίο είναι άτοπο. Συμπεραίνουμε ότι: $g^2H = H$ κάτι το οποίο σημαίναι ότι $g^2 \in H$. Άρα η έγκλειση $(*)$ ισχύει.

Όμως το πλήθος των στοιχείων του συνόλου $\mathcal{M}$ των τετραγώνων στοιχείων της A_4 είναι, όπως βλέπουμε από τον πίνακα πολλαπλασιασμού της A_4:

$$\mathcal{M} = \left\{(1),\ (123),\ (124),\ (134),\ (234),\ (132),\ (142),\ (143),\ (243)\right\}$$

δηλαδή όλοι οι 3-κύκλοι και η ταυτοτική μετάθεση. Άρα $|\mathcal{M}| = 9$ και επομένως δεν μπορεί να ισχύει η σχέση $(*)$, διότι $|H| = 6$. Στο άτοπο καταλήξαμε υποθέτοντας ότι η A_4 έχει μια υποομάδα τάξης 6. Άρα η εναλλάσσουσα ομάδα A_4 δεν έχει υποομάδα τάξης 6.

(1) Προφανώς η A_4 έχει υποομάδες τάξης 1, και 12. Το στοιχείο $(12)(34)$ παράγει μια κυκλική ομάδα τάξης 2, το στοιχείο (123) παράγει μια υποομάδα τάξης 3, και το σύνολο

$$\{(1), (12)(34), (13)(24), (14)(23)\}$$

είναι μια υποομάδα τάξης 4. □

Παρατήρηση 2.18. *Το αμέσως επόμενο, ως προς το μέγεθος, παράδειγμα ομάδας στην οποία δεν ισχύει το αντίστροφο του Θεωρήματος Lagrange αποτελεί η ομάδα* $\mathsf{SL}_2(\mathbb{Z}_3)$ *των* 2×2 *πινάκων με ορίζουσα* 1 *υπεράνω του σώματος* $\mathbb{Z}_3$ *των ακεραίων modulo 3. Η* $\mathsf{SL}_2(\mathbb{Z}_3)$ *είναι μια μη-αβελιανή ομάδα τάξης 24 και άρα οι διαιρέτες της τάξης της είναι:* $1, 2, 3, 4, 6, 8, 12, 24$. *Μπορεί κανείς να δεί ότι η* $\mathsf{SL}_2(\mathbb{Z}_3)$ *υποομάδες τάξης* $1, 2, 3, 4, 6, 8, 24$ *αλλά δεν έχει υποομάδες τάξης* 12.

Παρατήρηση 2.19. *Όπως θα δούμε κάθε κυκλική ομάδα (πεπερασμένης τάξης) ικανοποιεί το αντίστροφο του Θεωρήματος Lagrange. Γενικότερα μπορεί να δειχθεί ότι κάθε:*

- (α) *πεπερασμένη αβελιανή ομάδα,*
- (β) *ομάδα με τάξη δύναμη ενός πρώτου αριθμού, και*
- (γ) *«διεδρική» ομάδα,*

ικανοποιεί το αντίστροφο του Θεωρήματος του Lagrange.

2.7. **Εφαρμογές του Θεωρήματος Lagrange (I).** Στην παρούσα ενότητα θα δούμε κάποιες άμεσες εφαρμογές του Θεωρήματος Lagrange.

Πρόταση 2.20. *Έστω* H *και* K *δύο υποομάδες μιας πεπερασμένης ομάδας* $(G, \star)$*, και υποθέτουμε ότι:*

$$K \subseteq H \subseteq G$$

Τότε:

$$[G : K] = [G : H] \cdot [H : K]$$

Απόδειξη. Προφανώς η K είναι υποομάδα της H και άρα από το Θεώρημα του Lagrange για τις υποομάδες H και K, θα έχουμε:

$$\mathsf{o}(G) = \mathsf{o}(H) \cdot [G : H] \qquad \mathsf{o}(G) = \mathsf{o}(K) \cdot [G : K] \qquad \mathsf{o}(H) = \mathsf{o}(K) \cdot [H : K]$$

Επομένως

$$\mathsf{o}(G) = \mathsf{o}(K) \cdot [H : K] \cdot [G : H] \quad \text{και} \quad \mathsf{o}(G) = \mathsf{o}(K) \cdot [G : K] \qquad \Longrightarrow \qquad [G : K] = [G : H] \cdot [H : K]$$

□

Πρόταση 2.21. *Έστω* H *και* K *δύο υποομάδες μιας πεπερασμένης ομάδας* $(G, \star)$*, και έστω* $\mathsf{o}(H) = m$ *και* $\mathsf{o}(K) = n$*. Αν* $(m, n) = 1$*, τότε:*

$$H \bigcap K = \{e\}$$

Απόδειξη. Όπως γνωρίζουμε η τομή υποομάδων μιας ομάδας είναι υποομάδα και έτσι έχουμε ότι η τομή $H \cap K$ είναι υποομάδα των πεπεπερασμένων ομάδων H και K. Απο το Θεώρημα του Lagrange θα έχουμε:

$$\mathsf{o}(H \cap K)/\mathsf{o}(H) = m \qquad \text{και} \qquad \mathsf{o}(H \cap K)/\mathsf{o}(K) = n$$

Τότε όμως $\mathsf{o}(H \cap K)/(m, n)$, και επειδή $(m, n) = 1$, θα έχουμε $\mathsf{o}(H \cap K) = 1$ ή ισοδύναμα: $H \cap K = \{e\}$. □

Θα ολοκληρώσουμε την παρούσα ενότητα με την παρακάτω ενδιαφέρουσα πρόταση η απόδειξη της οποίας αποτελεί εφαρμογή της Πρότασης 1.9.

Κατ' αρχήν υπενθυμίζουμε ότι αν $H, K \subseteq G$ είναι υποσύνολα μιας ομάδας G, τότε:

$$HK = \big\{hk \in G \mid h \in H,\ k \in K\big\}$$

Σημειώνουμε ότι αν τα υποσύνολα $H, K \subseteq G$ είναι υποομάδες της G, τότε γενικά το υποσύνολο HK δεν είναι υποομάδα της G.

Πρόταση 2.22. *Έστω H, K δύο πεπερασμένες υποομάδες της ομάδας G. Τότε το πλήθος $\big|HK\big|$ των στοιχείων του συνόλου HK είναι:*

$$|HK| = \frac{\mathsf{o}(H)\,\mathsf{o}(K)}{\mathsf{o}(H \cap K)}$$

Απόδειξη. Θεωρούμε την απεικόνιση

$$f:\ H \times K\ \longrightarrow HK, \quad f(h,k) = hk$$

η οποία προφανώς είναι επί. Από την υπο-ενότητα 1.4, θα έχουμε ότι η f ορίζει μια σχέση ισοδυναμίας $\mathcal{R}_f$ επί του συνόλου $H \times K$ και υπάρχει μια 1-1 και επί απεικόνιση μεταξύ του συνόλου πηλίκο $(H \times K)/\mathcal{R}_f$ και της εικόνας $\mathsf{Im}(f) = HK$. Επομένως:

$$\big|(H \times K)/\mathcal{R}_f\big| \ = \ \big|HK\big|$$

Όπως γνωρίζουμε, τα στοιχεία του συνόλου πηλίκο $(H \times K)/\mathcal{R}_f$ είναι οι διακεκριμμένες κλάσεις ισοδυναμίας $[(h,k)]_{\mathcal{R}_f}$ και από την Πρόταση 1.9,

$$[(h,k)]_{\mathcal{R}_f} = f^{-1}\{f(h,k)\} = f^{-1}\{hk\}$$

Θα δείξουμε ότι:

$$f^{-1}\{hk\} = \big\{(hr, r^{-1}k) \in G \times G \mid r \in H \cap K\big\} \qquad (\dagger)$$

Πραγματικά: αν $(hr, r^{-1}k) \in G \times G$, όπου $h \in H$, $k \in K$, και $r \in H \cap K$, τότε προφανώς $(hr, r^{-1}k) \in H \times K$, και $f(hr, r^{-1}k) = hrr^{-1}k = hek = hk$ και επομένως $(hr, r^{-1}k) \in f^{-1}\{hk\} = [(h,k)]_{\mathcal{R}_f}$. Αντίστροφα αν $(x,y) \in f^{-1}\{hk\} = [(h,k)]_{\mathcal{R}_f}$, τότε $x \in H$, $y \in K$, και $f(x,y) = hk$. Επομένως $hk = xy$ και τότε $x^{-1}hk = y$ και άρα:

$$x^{-1}h = yk^{-1} \ \in \ H \cap K$$

διότι το $x^{-1}h \in H$ επειδή $x, h \in H$ και H είναι υπομάδα, και $yk^{-1} \in K$ επειδή $y, k \in K$ και K είναι υποομάδα. Ισοδύναμα επειδή το υποσύνολο $H \cap K$ είναι υποομάδα, θα έχουμε:

$$(x^{-1}h)^{-1} = (yk^{-1})^{-1} \ \in \ H \cap K \quad \Longrightarrow \quad h^{-1}x = ky^{-1} := r \ \in \ H \cap K$$

Τότε θα έχουμε:

$$(x,y) = (ex, ye) = \big((hh^{-1})x, y(k^{-1}k)\big) = \big(h(h^{-1}x), (yk^{-1})k\big) = (hr, r^{-1}k)$$

Άρα αποδείξαμε την σχέση (†) με βάση την οποία ορίζουμε μια απεικόνιση, $\forall h \in H, \forall k \in K$:

$$\phi:\ H \cap K\ \longrightarrow\ f^{-1}\{hk\}, \quad \phi(r) = (hr, r^{-1}k)$$

Η παραπάνω ανάλυση δείχνει ότι η απεικόνιση ϕ είναι καλά ορισμένη και είναι απεικόνιση επί. Επιπλέον η ϕ είναι 1-1 διότι αν $\phi(r) = \phi(s)$ τότε $(hr, r^{-1}k) = (hs, s^{-1}k)$ και άρα: $hr = hs$ και $r^{-1}k = s^{-1}k$. Τότε προφανώς θα έχουμε $r = s$ και έτσι η ϕ είναι 1-1 και επί.

Αυτό σημαίνει ότι για κάθε κλάση ισοδυναμίας $[(h,k)]_{\mathcal{R}_f}$ θα έχουμε:

$$\mathsf{o}(H \cap K) = \big|H \cap K\big| = \big|[(h,k)]_{\mathcal{R}_f}\big|$$

Επειδή το σύνολο όλων των κλάσεων ισοδυναμίας αποτελεί μια διαμέριση του $H \times K$, επειδή κάθε κλάση ισοδυναμίας έχει τόσα στοιχεία όσα και η υποομάδα $H \cap K$, και επειδή το πλήθος των διακεκριμμένων κλάσεων ισοδυναμίας είναι ίσο με το πλήθος $\big|HK\big|$, θα έχουμε:

$$\big|H \times K\big| = \big|H \cap K\big| \cdot \big|HK\big|$$

και επομένως:

$$|HK| = \frac{\big|H \times K\big|}{\big|H \cap K\big|} = \frac{\big|H\big|\,\big|K\big|}{\mathsf{o}(H \cap K)} = \frac{\mathsf{o}(H)\,\mathsf{o}(K)}{\mathsf{o}(H \cap K)}$$

□

Θα δούμε τώρα κάποιες εφαρμογές της παραπάνω Πρότασης.

Πόρισμα 2.23. *Έστω H και K δύο υποομάδες μιας πεπερασμένης ομάδας G. Τότε:*

$$\mathsf{o}(H) > \sqrt{\mathsf{o}(G)} \quad \textit{και} \quad \mathsf{o}(K) > \sqrt{\mathsf{o}(G)} \implies H \cap K \neq \{e\}$$

Απόδειξη. Από την παραπάνω πρόταση θα έχουμε:

$$\mathsf{o}(G) \geq |HK| = \frac{\mathsf{o}(H)\,\mathsf{o}(K)}{\mathsf{o}(H \cap K)} > \frac{\sqrt{\mathsf{o}(G)}\,\sqrt{\mathsf{o}(G)}}{\mathsf{o}(H \cap K)} = \frac{\mathsf{o}(G)}{\mathsf{o}(H \cap K)} \implies \mathsf{o}(H \cap K) > 1 \qquad \square$$

Πόρισμα 2.24. *Έστω G μια ομάδα τάξης $\mathsf{o}(G) = pq$, όπου p, q είναι πρώτοι αριθμοί με $p > q$. Τότε η G έχει το πολύ μια υποομάδα τάξης p.*

Απόδειξη. Έστω H και K δύο υποομάδες της G τάξης p. Τότε ικανοποιούνται τετριμμένα οι υποθέσεις του παραπάνω πορίσματος και άρα $H \cap K \neq \{e\}$, δηλαδή $\mathsf{o}(H \cap K) > 1$. Όμως επειδή η $H \cap K$ είναι υποομάδα της H και της K, και επειδή η τάξη της H και η τάξη της K είναι ο πρώτος αριθμός p, από το Θεώρημα του Lagrange έπεται ότι $\mathsf{o}(H \cap K) \,\big|\, p$ και άρα $\mathsf{o}(H \cap K) = p$ διότι όπως είδαμε $\mathsf{o}(H \cap K) > 1$. Τότε όμως $H \cap K = H$ και $H \cap K = K$, δηλαδή $H \subseteq K$ και $K \subseteq H$. Επομένως $H = K$. $\square$

Παρατήρηση 2.25. *Ως ειδική περίπτωση (Θεώρημα Cauchy) ενός σημαντικού Θεωρηματος το οποίο οφείλεται στον Sylow, έπεται ότι κάθε ομάδα G τάξης $\mathsf{o}(G) = pq$, όπου p, q είναι πρώτοι αριθμοί με $p > q$, έχει τουλάχιστον μια υποομάδα τάξης p. Έτσι σύμφωνα με το παραπάνω πόρισμα, έπεται ότι η G έχει ακριβώς μια υποομάδα τάξης p.*

Ανοικτά Ακαδημαϊκά Μαθήματα

Πανεπιστήμιο Ιωαννίνων

Τέλος Ενότητας

Χρηματοδότηση

- Το παρόν εκπαιδευτικό υλικό έχει αναπτυχθεί στα πλαίσια του εκπαιδευτικού έργου του διδάσκοντα.
- Το έργο «**Ανοικτά Ακαδημαϊκά Μαθήματα στο Πανεπιστήμιο Ιωαννίνων**» έχει χρηματοδοτήσει μόνο τη αναδιαμόρφωση του εκπαιδευτικού υλικού.
- Το έργο υλοποιείται στο πλαίσιο του Επιχειρησιακού Προγράμματος «Εκπαίδευση και Δια Βίου Μάθηση» και συγχρηματοδοτείται από την Ευρωπαϊκή Ένωση (Ευρωπαϊκό Κοινωνικό Ταμείο) και από εθνικούς πόρους.

Σημειώματα

Σημείωμα Αναφοράς

Σημείωμα Αδειοδότησης