ΠΑΝΕΠΙΣΤΗΜΙΟ ΙΩΑΝΝΙΝΩΝ
ΑΝΟΙΚΤΑ ΑΚΑΔΗΜΑΪΚΑ ΜΑΘΗΜΑΤΑ

Τίτλος Μαθήματος: Θεωρία Ομάδων

Ενότητα: Δράση Ομάδας επί ενός Συνόλου

Διδάσκων: Καθηγητής Νικόλαος Μαρμαρίδης

Τμήμα: Μαθηματικών

Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

Κεφάλαιο 1

Δράση Ομάδας επί ενός Συνόλου

1.1 Δράσεις και μετατακτικές Αναπαραστάσεις

Έστω $(G, \star)$ μια ομάδα και A ένα μη κενό σύνολο.

Ορισμός 1.1.1. Κάθε απεικόνιση $\phi : G \times A \to A$, $(g, a) \mapsto g\phi a$ που ικανοποιεί τα:

(α′) $\forall g_1, g_2 \in G, a \in A, (g_1 \star g_2)\phi a = g_1\phi(g_2\phi a)$, και

(β′) $\forall a \in A, e_G\phi a = a$ (όπου e_G το ουδέτερο στοιχείο τής G)

ονομάζεται μια *δράση τής ομάδας G επί τού συνόλου A*.

Παραδείγματα 1.1.1. Θεωρούμε τη διεδρική ομάδα $D_4 = \langle \rho, s : \rho^4 = \mathrm{Id}, s^2 = \mathrm{Id}, \rho s = s\rho^{-1} \rangle$, βλ. Παρατηρήσεις 0.0.1, (Φυλλάδιο Ασκήσεων 1, Θεωρία Ομάδων 14-02-2013), όπου $\rho = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$ η στροφή κατά γωνία $\pi/4$ γύρω από τον άξονα που είναι κάθετος στο επίπεδο τού τετραγώνου με φορά αυτήν που ακολουθούν κατά την κίνησή τους οι δείκτες τού ρολογιού και $s = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}$ η ανάκλαση ως προς τον άξονα συμμετρίας που διέρχεται από τις κορυφες 1 και 3.

Έστω $K = \{1, 2, 3, 4\}$ το σύνολο των κορυφών τού τετραγώνου τού Σχήματος 1.1.

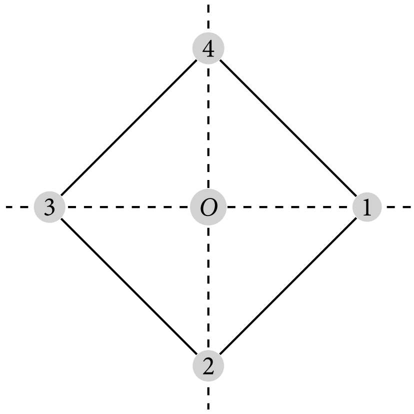
Ορίζουμε την απεικόνιση $\phi : D_4 \times K \to K$ ως ακολούθως

$$\forall \mu, \nu \in \mathbb{Z}, \forall \kappa \in K, (s^{\mu} \circ \rho^{\nu})\phi\kappa = s^{\mu}(\rho^{\nu}(\kappa)).$$

Αποδεικνύεται άμεσα ότι η D_4 δρα επί τού συνόλου $K = \{1, 2, 3, 4\}$ των κορυφών τού τετραγώνου (βλ. επόμενο Σχήμα 1.1).

Έστω $\Delta = \{\delta_1 = \{1, 3\}, \delta_2 = \{2, 4\}\}$ το σύνολο των διαγωνίων τού τετραγώνου και ψ η απεικόνιση

$$\psi : D_4 \times \Delta \to \Delta,$$



Σχήμα 1.1: Τετράγωνο

που ορίζεται ως

$$\forall \mu, \nu \in \mathbb{Z},\ \ \rho\psi\delta_1 = \delta_2, \rho\psi\delta_2 = \delta_1, s\psi\delta_1 = \delta_1, s\psi\delta_2 = \delta_2,$$

κατόπιν

$$\forall \mu \in \mathbb{Z}, \rho^{\mu}\psi\delta_1 = \rho^{\mu-1}(\delta_2), \rho^{\mu}\psi\delta_2 = \rho^{\mu-1}(\delta_1), s^{\mu}\psi\delta_1 = \delta_1, s^{\mu}\psi\delta_2 = \delta_2$$

και τέλος

$$\forall \mu, \nu \in \mathbb{Z}, \delta \in \Delta,\ \ (s^{\mu} \circ \rho^{\nu})\psi\delta = s^{\mu}(\rho^{\nu}(\delta)).$$

Αποδεικνύεται και πάλι ότι η D_4 δρα επί τού συνόλου Δ.
Αντίθετα, θεωρώντας το σύνολο $L = \{\ell_1 = \{1, 2\}, \ell_2 = \{3, 4\}\}$ παρατηρούμε ότι η απεικόνιση που επάγεται από τη δράση τής D_4 επί τού συνόλου των κορυφών K δεν ορίζει μια δράση επί τού L, αφού η πλευρά $\rho(\ell_1) = \{\rho(1), \rho(2)\} = \{4, 1\}$ δεν ανήκει στο σύνολο L.

Έστω A ένα μη κενό σύνολο και $(S_A, \circ)$ η συμμετρική ομάδα τού A, δηλαδή η ομάδα που απαρτίζεται από τις «$1 - 1$» και «επί» απεικονίσεις από το A στο A.

Πρόταση 1.1.1. *Αν $\phi : G \times A \longrightarrow G$ είναι μια δράση τής ομάδας G επί τού A, τότε η αντιστοιχία*

$$X(\phi) : G \longrightarrow S_A, g \mapsto X(\phi)(g) : A \longrightarrow A$$
$$a \mapsto [X(\phi)(g)](a) := g\phi a$$

είναι ένας ομομορφισμός ομάδων.
Αν $\chi : G \longrightarrow S_A$ είναι ένας ομομορφισμός ομάδων, τότε η απεικόνιση

$$\Phi(\chi) : G \times A \longrightarrow A, \quad (g, a) \mapsto g\Phi(\chi)a := \chi(g)(a)$$

είναι μια δράση τής G επί τού A.
Επιπλέον, $\Phi(X(\phi)) = \phi$, $X(\Phi(\chi)) = \chi$.

Γι' αυτό υπάρχει μια αμφιμονοσήμαντη αντιστοιχία μεταξύ τού συνόλου των δράσεων μιας ομάδας G επί ενός συνόλου A και τού συνόλου των ομομορφισμών $\mathrm{Hom}(G, S_A)$ από την ομάδα G στη συμμετρική ομάδα S_A.

Ορισμός 1.1.2. Κάθε ομομορφισμός από μια ομάδα G σε μια ομάδα συμμετρίας S_A ενός συνόλου A ονομάζεται μια *μετατακτική αναπαράσταση* τής G.

Παρατηρήσεις 1.1.1. Το γεγονός ότι μια δράση χορηγεί έναν ομομορφισμό και αντιστρόφως βοηθά πολύ στον προσδιορισμό *όλων των δράσεων* μιας ομάδας επί ενός συνόλου.
Για παράδειγμα, αν η ομάδα G είναι η $\mathbb{Z}_{13}$ και A είναι ένα σύνολο με οκτώ στοιχεία, τότε η μόνη δράση τής $\mathbb{Z}_{13}$ που ορίζεται επί τού A είναι η τετριμμένη, δηλαδή η

$$\phi : \mathbb{Z}_{13} \times A \longrightarrow A, [z]\phi a \mapsto a, \forall [z] \in \mathbb{Z}_{13}, a \in A,$$

αφού οποιαδήποτε δράση χορηγεί έναν ομομορφισμό $\mathbb{Z}_{13} \longrightarrow S_A$ και επειδή ο μόνος ομομορφισμός που υπάρχει από την $\mathbb{Z}_{13}$ στην S_A είναι ο τετριμμένος, αφού το $13 \nmid 8!$.

Ορισμός 1.1.3. *Πυρήνας μιας δράσης $\phi : G \times A \longrightarrow G$* είναι το υποσύνολο

$$K_\phi := \{g \in G \mid g\phi a = a, \forall a \in A\}.$$

Λήμμα 1.1.1. *Ο πυρήνας K_ϕ μιας δράσης $\phi : G \times A \longrightarrow G$ συμπίπτει με τον πυρήνα $\mathrm{Ker}X(\phi)$ τού επαγόμενου ομομορφισμού $X(\phi) : G \longrightarrow S_A$ και συνεπώς είναι μια ορθόθετη υποομάδα τής G.*

Ορισμός 1.1.4. Μια δράση $\phi : G \times A \longrightarrow G$ ονομάζεται *πιστή*, αν ο πυρήνας της είναι η τετριμμένη υποομάδα $K_\phi = \{e_G\}$.

Στην περίπτωση αυτή, η ομάδα G, που δρα επί του A, μπορεί να θεωρηθεί υποομάδα τής συμμετρικής ομάδας S_A, αφού $K_\phi = \mathrm{Ker} X(\phi)$.
Προσέξτε, ότι οποιαδήποτε δράση $\phi : G \times A \to G$ χορηγεί μια πιστή δράση τής πηλικοομάδας G/K_ϕ επί τού A, ως ακολούθως

$$\overline{\phi} : G/K_\phi \times A \to G, \quad (gK_\phi, a) \mapsto (gK_\phi)\overline{\phi}a := g\phi a$$

Προτείνουμε να ελέγξει μόνος του ο αναγνώστης, πρώτα ότι η $\overline{\phi}$ είναι μια καλά ορισμένη απεικόνιση και κατόπιν ότι ορίζει μια δράση τής G/K_ϕ επί τού A.

1.2 Τροχιές και Σταθερωτές

Έστω ότι $\phi : G \times A \to G$ μια δράση τής G επί τού A και η σχέση $\mathcal{R}_\phi \subseteq A \times A$ επί τού A, η οποία ορίζεται ως εξής:

$$\text{Αν } a, \in A, (a, b) \in \mathcal{R}_\phi \iff \exists g \in G : g\phi a = b.$$

Λήμμα 1.2.1. *Το $\mathcal{R}_\phi \subseteq A \times A$ είναι μια σχέση ισοδυναμίας επί τού A*

Απόδειξη. Πράγματι,

(α′) $\forall a \in A$, το $(a, a) \in \mathcal{R}_\phi$, αφού $e_G\phi a = a$.

(β′) Αν $(a, b) \in \mathcal{R}_\phi$, τότε $\exists g \in G$ με $b = g\phi a$. Συνεπώς, $g^{-1}\phi b = a$ και $(b, a) \in \mathcal{R}_\phi$.

(γ′) Αν $(a, b) \in \mathcal{R}_\phi$ και $(b, c) \in \mathcal{R}_\phi$, τότε $\exists g_1, g_2 \in G$ με $b = g_1\phi a$ και $c = g_2\phi b$. Επομένως, $c = g_2\phi(g_1\phi a) = (g_2g_1)\phi a$ και γι' αυτό $(a, c) \in \mathcal{R}_\phi$.

□

Έστω ότι $\phi : G \times A \to G$ είναι μια δράση τής G επί τού A, ότι $\mathcal{R}_\phi$ είναι η αντίστοιχη σχέση ισοδυναμίας και ότι a είναι ένα στοιχείο τού A.

Ορισμός 1.2.1. Ονομάζουμε *τροχιά* τού στοιχείου $a \in A$ την κλάση ισοδυναμίας $[a]_{\mathcal{R}_\phi}$ τού a ως προς τη σχέση $\mathcal{R}_\phi$.

Προφανώς,

$$[a]_{\mathcal{R}_\phi} = \{g\phi a \mid g \in G\}.$$

Θα συμβολίζουμε την κλάση $[a]_{\mathcal{R}_\phi}$ ως $G\phi a$. Επιπλέον, αν $a \in A$

Ορισμός 1.2.2. Ονομάζουμε *σταθερωτή* τού στοιχείου $a \in A$ το υποσύνολο $G_a = \{g \in G \mid g\phi a = a\}$.

Προσέξτε ότι επειδή η $\mathcal{R}_\phi$ είναι σχέση ισοδυναμίας, το σύνολο A διαμερίζεται στις τροχιές του $G\phi a$, δηλαδή

$$A = \cup_{a \in A} G\phi a \text{ και αν, } a, b \in A \text{ με } G\phi a \cap G\phi b \neq \emptyset, \text{ τότε } G\phi a = G\phi b.$$

Ορισμός 1.2.3. Η G δρα *μεταβατικώς* επί τού συνόλου A αν, υπάρχει μόνο μια τροχιά.

Συνεπώς αν, η G δρα μεταβατικώς επί τού A και α, β είναι οποιαδήποτε στοιχεία τού A, τότε $\exists g \in G$ με $g\phi\alpha = \beta$.

Λήμμα 1.2.2. (α′) *Ο σταθερωτής G_a είναι μια υποομάδα τής G.*

(β′) *Αν a και b είναι δυο στοιχεία τού A, τα οποία ανήκουν στην ίδια τροχιά, τότε οι αντίστοιχοι σταθερωτές τους G_a και G_b είναι συζυγείς υποομάδες τής G.*

(Υπενθυμίζουμε ότι αν, K και L είναι δύο υποομάδες μιας ομάδας G, τότε η L ονομάζεται ***συζυγής*** *τής K, αν υπάρχει $h \in G$ με $L = hKh^{-1}$. Επειδή τότε και $K = h^{-1}Lh$, έπεται ότι η K είναι επίσης συζυγής τής L.*
Συζυγείς υποομάδες μιας ομάδας έχουν πάντοτε το ίδιο πλήθος στοιχείων, αφού για κάθε $h \in G$, η απεικόνιση $s_h : G \longrightarrow G, g \mapsto hgh^{-1}$ είναι ένας (εσωτερικός) αυτομορφισμός τής G. Γι αυτό, ο s_h χορηγεί μια αμφινομονοσήμαντη αντιστοιχία μεταξύ οποιουδήποτε υποσυνόλου T τής G και τής εικόνας του hTh^{-1}.)

Απόδειξη. (α′) Το σύνολο G_a δεν είναι κενό, αφού $e_G \in G_a$. Επιπλέον, αν $g_1, g_2 \in G_a$, τότε $g_1\phi a = a$, $g_2\phi a = a$ και συνεπώς $g_2^{-1}\phi a = a$.

$$(g_1 g_2^{-1})\phi a = g_1\phi(g_2^{-1}\phi a) = g_1\phi a = a$$

Ώστε, το G_a είναι μια υποομάδα τής G.
(β′) Αφού τα a, b ανήκουν στη ίδια τροχιά, υπάρχει κάποιο $h \in G$ με $h\phi a = b$. Αφήνουμε τον αναγνώστη να αποδείξει ως άσκηση ότι $G_b = hG_a h^{-1}$. □

Θεώρημα 1.2.1. *Έστω ότι $\phi : G \times A \longrightarrow G$ είναι μια δράση τής G επί τού A και ότι G_a είναι ο σταθερωτής ενός στοιχείου $a \in A$. Υπάρχει μια «$1-1$» και «επί» απεικόνιση μεταξύ τού συνόλου $G/G_a = \{gG_a \mid g \in G\}$ των αριστερών πλευρικών κλάσων τής G ως προς G_a και της τροχιάς $G\phi a$.*

Απόδειξη. Θεωρούμε την αντιστοιχία

$$G/G_a \longrightarrow G\phi a, \quad gG_a \quad \mapsto \quad g\phi a.$$

Η συγκεκριμένη αντιστοιχία είναι μια καλά ορισμένη απεικόνιση, δηλαδή ανεξάρτητη από την επιλογή τού αντιπροσώπου g τής πλευρικής κλάσης gG_a. Πράγματι αν, $g_1G_a = g_2G_a$, τότε $g_2^{-1}g_1 \in G_a$. Συνεπώς,

$$(g_2^{-1}g_1)\phi a = a \Rightarrow g_2\phi[(g_2^{-1}g_1)\phi a] = g_2\phi a \Rightarrow ((g_2g_2^{-1})g_1)\phi a = g_2\phi a \Rightarrow g_1\phi a = g_2\phi a.$$

Η απεικόνιση είναι «$1-1$» αφού από $g_1\phi a = g_2\phi a$, έπεται $(g_2^{-1}g_1)\phi a = a$. Επομένως, $g_2^{-1}g_1 \in G_a$ και γι' αυτό $g_1G_a = g_2G_a$. Τέλος, η απεικόνιση είναι «επί», αφού το στοιχείο $g\phi a$ τής τροχιάς $G\phi a$ είναι εικόνα τής αριστερής πλευρικής κλάσης gG_a. □

1.2.1 Το Θεώρημα Burnside

Αν $g \in G$, τότε συμβολίζουμε με A^g το υποσύνολο τού A που αποτελείται από τα στοιχεία τού $a \in A$ που παραμένουν σταθερά κάτω απο τη ϕ-δράση τού $g \in G$, δηλαδή

$$A^g = \{a \in A \mid g\phi a = a\}$$

Θεώρημα 1.2.2 (Burnside). *Έστω ότι $\phi : G \times A \longrightarrow G$ είναι δράση μιας **πεπερασμένης ομάδας** G επί ενός **πεπερασμένου** συνόλου A.*
Το πλήθος k των τροχιών στις οποίες διαμερίζεται το σύνολο A ισούται με

$$k := \frac{1}{[G:1]}\sum_{g\in G} \mid A^g \mid .$$

Απόδειξη. Θα υπολογίσουμε με δύο διαφορετικούς τρόπους το πλήθος των στοιχείων τού συνόλου

$$\mathcal{L} = \{(g,a) \in G \times A \mid g\phi a = a\}.$$

Για κάθε $g \in G$, θεωρούμε το σύνολο των στοιχείων $a \in A$ που παραμένουν αναλλοίωτα από τη ϕ-δράση τού g, δηλαδή θεωρούμε το σύνολο A^g. Συνεπώς,

$$\mid \mathcal{L} \mid = \sum_{g\in G} \mid A^g \mid . \tag{*}$$

Για κάθε $a \in A$, θεωρούμε τον σταθερωτή τού a, δηλαδή την υποομάδα $G_a = \{g \in G \mid g\phi a = a\}$. Επομένως,

$$\mid \mathcal{L} \mid = \sum_{a\in A} [G_a : 1].$$

Αν το πλήθος των τροχιών ισούται με k, τότε το A διαμερίζεται στις k διαφορετικές τροχιές $G\phi a_1, G\phi a_2, \ldots, G\phi a_k$ και γι' αυτό

$$\mid \mathcal{L} \mid = \sum_{a\in A} [G_a : 1] = \sum_{i=1}^{k} \sum_{a\in G\phi a_i} [G_a : 1]. \tag{**}$$

Από το Λήμμα 1.2.2 γνωρίζουμε ότι όλοι οι σταθερωτές που αντιστοιχούν στα στοιχεία a τής τροχιάς $G\phi a_i$ έχουν το ίδιο πλήθος στοιχείων, δηλαδή

$$\forall a \in G\phi a_i, [G_a : 1] = [G_{a_i} : 1].$$

Από το Θεώρημα 1.2.1 γνωρίζουμε ότι το πλήθος των στοιχείων τής τροχιάς $G\phi a_i$ ισούται με τον δείκτη $\frac{[G:1]}{[G_{a_i}:1]}$
Συνεπώς, η σχέση (**) γίνεται

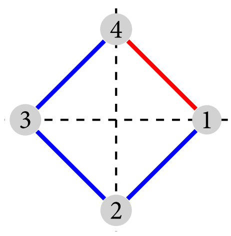
$$| \mathcal{L} |= \sum_{a \in A} [G_a : 1] = \sum_{i=1}^{k} \sum_{a \in G\phi a_i} [G_a : 1] = \sum_{i=1}^{k} \frac{[G : 1]}{[G_{a_i} : 1]} [G_{a_i} : 1] = k[G : 1]. \qquad (***)$$

Από τις σχέσεις (***) και (*) προκύπτει ότι

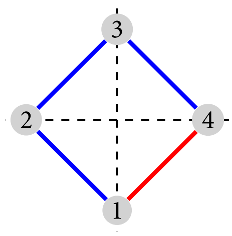
$$k[G : 1] = \sum_{g \in G} | A^g | \implies k = \frac{1}{[G : 1]} \sum_{g \in G} | A^g | .$$

□

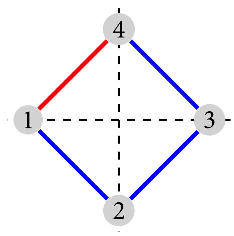
Εφαρμογη **1.2.1.** *Θεωρούμε ένα τετράγωνο τού οποίου κάθε πλευρά τη χρωματίζουμε κόκκινη ή μπλέ. Δύο τέτοια χρωματισμένα τετράγωνα λέμε ότι δεν διαφέρουν ουσιαστικώς, αν είτε περιστρέφοντας είτε αναποδογυρίζοντας το ένα από αυτά προκύπτει το άλλο χρωματισμένο τετράγωνο, βλ. Σχήμα 1.2.*



Αρχικό τετράγωνο.



Από το αρχικό κατόπιν στροφής κατά $\pi/4$ από αριστερά προς τα δεξιά.



Από το αρχικό κατόπιν κατοπτρισμού ως προς τον άξονα 4–2.

Σχήμα 1.2: Τα ανωτέρω τρία χρωματισμένα τετράγωνα δεν διαφέρουν ουσιαστικώς.

Θα υπολογίσουμε το πλήθος των ουσιαστικώς διαφορετικών τετραγώνων εφαρμόζοντας το Θεώρημα Burnside.

Έστω το σύνολο των χρωματισμένων τετραγώνων. Το A αποτελείται από 2^4 στοιχεία, αφού κάθε πλευρά τού τετραγώνου μπορεί να χρωματιστεί κόκκινη ή μπλέ.

Στο A δρα η διεδρική ομάδα D_4, αφού αυτή ακριβώς η ομάδα περιστρέφει η αναποδογυρίζει το τετράγωνο και το πλήθος των χρωματισμένων τετραγώνων που διαφέρουν ουσιαστικά συμπίπτει με το πλήθος k των τροχιών τού A κάτω από την δράση τής D_4.
Η D_4 αποτελείται από τα στοιχεία:

$$\mathrm{Id} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}, \rho = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} \textit{ στροφή κατά } \pi/4 \textit{ από αριστερά προς τα δεξιά},$$

$$\rho^2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} \textit{ στροφή κατά } \pi/2, \rho^3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix} \textit{ στροφή κατά } 3\pi/4,$$

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix} \textit{ ανάκλαση ως προς τον άξονα } 4-2,$$
$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix} \textit{ ανάκλαση ως προς τον άξονα } 3-1,$$

$$\begin{aligned} \mu = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} & \quad \textit{ανάκλαση ως προς τον άξονα διερχόμενο} \\ & \quad \textit{από τα μέσα των } \ 3-4 \textit{ και } 2-1, \\ \nu = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} & \quad \textit{ανάκλαση ως προς τον άξονα διερχόμενο} \\ & \quad \textit{από τα μέσα των } \ 1-4 \textit{ και } 2-3. \end{aligned}$$

Για κάθε $g \in D_4$, θα υπολογίσουμε το πληθος $\mid A^g \mid$ των στοιχείων τού A^g.

(α′) *Προφανώς, $\mid A^{\mathrm{Id}} \mid = 2^4$, αφού κάθε στοιχείο τού A παραμένει αναλλοίωτο από το ταυτοτικό στοιχείο τής D_4.*

(β′) *Το $\mid A^{\rho} \mid$ ισούται με 2, αφού για να ανήκει ένα στοιχείο τού A στο A^{ρ} θα πρέπει όλες οι πλευρές του να έχουν το ίδιο χρώμα, αφού διαφορετικά τουλάχιστον μια πλευρά θα απεικονιζόταν σε μια πλευρά διαφορετικού χρώματος. Επειδή διαθέτουμε δύο χρώματα, έχουμε $\mid A^{\rho} \mid = 2$.*

(γ′) *Το $\mid A^{\rho^2} \mid$ ισούται με 4. Εδώ ένα στοιχείο τού A ανήκει στο A^{ρ^2} ακριβώς τότε, όταν οι απέναντι πλευρές του τετραγώνου έχουν το ίδιο χρώμα, αφού κατά την περιστροφή κατά $\pi/2$ απεικονίζεται κάθε πλευρά στην απέναντί της. Συνεπώς υπάρχουν δύο επιλογές χρώματος για τη μία πλευρά (ας πούμε την $1-4$) και δύο για μια γειτονική της (ας πούμε την $1-2$).*

(δ′) *Το $\mid A^{\rho^3} \mid$ ισούται με 2. Η επιχειρηματολογία είναι αντίστοιχη τής περίπτωσης A^{ρ}.*

(ε′) *Το $\mid A^{\sigma} \mid$ ισούται με 2^2. Εδώ, για να ανήκει ένα χρωματισμένο τετράγωνο στο A^{σ}, οφείλουν οι πλευρές $1-4$ και $3-4$ να έχουν το ίδιο χρώμα καθώς επίσης και οι πλευρές $2-3$ και $1-2$.*

(στ′) Το $| A^{\tau} |$ *ισούται με* 2^2. *Η επιχειρηματολογία είναι αντίστοιχη τής περίπτωσης* A^{σ}.

(ζ′) Το $| A^{\mu} |$ *ισούται με* 2^3. *Εδώ παρατηρούμε ότι οι πλευρές* $3 - 4$ *και* $1 - 2$ *απεικονίζονται μέσω τού* μ *στον εαυτό τους, ενώ οι πλευρές* $1 - 4$ *και* $2 - 3$ *εναλλάσσονται. Συνεπώς, οι τελευταίες οφείλουν να έχουν το ίδιο χρώμα. Γι' αυτό έχουμε δύο επιλογές χρώματος για την πλευρά* $3 - 4$, *δύο επιλογές χρώματος για την πλευρά* $1 - 2$ *και δύο επιλογές χρώματος (ας πούμε) για την πλευρά* $1 - 4$. *Το χρώμα τής πλευράς* $2 - 3$ *οφείλει να είναι το ίδιο με το χρώμα τής πλευράς* $1 - 4$.

(η′) Το $| A^{\nu} |$ *ισούται με* 2^3. *Η επιχειρηματολογία είναι αντίστοιχη τής περίπτωσης* A^{μ}.

Τώρα εφαρμόζοντας το Θεώρημα Burnside παίρνουμε

$$k = \frac{1}{[D_4 : 1]} \left\{ | A^{\mathrm{Id}} | + | A^{\rho} | + | A^{\rho^2} | + | A^{\rho^3} | + | A^{\sigma} | + | A^{\tau} | + | A^{\mu} | + | A^{\nu} | \right\} =$$
$$\frac{1}{8} \left\{ 2^4 + 2 + 4 + 2 + 2^2 + 2^2 + 2^3 + 2^3 \right\} = 6.$$

Ώστε υπάρχουν έξι ουσιαστικώς διαφορετικά χρωματισμένα τετράγωνα.

1.3 Δράση Ομάδας επί Υποσυνόλων και Πλευρικών Κλάσεων

1.3.1 Αριστερή Δράση

Θεωρούμε μια ομάδα $(G, \star)$ και την απεικόνιση

$$\ell : G \times G \to G, (g, \alpha) \mapsto g\ell\alpha := g \star \alpha.$$

Μπορεί πολύ εύκολα να επαληθευθεί ότι η ℓ συνιστά μια δράση τής G επί τού εαυτού της, αφού κατ' ουσίαν η επαλήθευση βασίζεται στα αξιώματα που διέπουν την πράξη «$\star$» τής ομάδας.
Από εδώ και στο εξής θα σημειώνουμε με $g\alpha$ *το αποτέλεσμα* $g \star \alpha$ *τής πράξης «*$\star$*» στα* $g, \alpha \in G$.

1.3.2 Δράση στις αριστερές πλευρικές Κλάσεις

Έστω ότι $H \leq G$ είναι μια υποομάδα τής G και $G/H = \{\alpha H \mid \alpha \in G\}$ το σύνολο των αριστερών πλευρικών κλάσεων τής H στην G.
Παρατηρούμε ότι η αντιστοιχία

$$\pi_H : G \times G/H \to G/H, (g, \alpha H) \mapsto g\pi_H\alpha H := g\alpha H$$

είναι ανεξάρτητη από την επιλογή τού αντιπροσώπου α τής πλευρικής κλάσης αH και συνεπώς είναι μια καλά ορισμένη απεικόνιση.
Πράγματι,

$$\forall g, \alpha_1, \alpha_2 \in G, \alpha_1 H = \alpha_2 H \Leftrightarrow g\alpha_1 H = g\alpha_2 H \text{ (γιατί;)}.$$

Επιπλέον,

$$\forall g_1, g_2 \in G, \alpha H \in G/H, (g_1g_2)\pi_H\alpha H = (g_1g_2)\alpha H = g_1(g_2\alpha H) = g_1\pi_H(g_2\pi_H\alpha H),$$
$$\forall \alpha H \in G/H, e_G\pi_H\alpha H = (e_G\alpha)H = \alpha H, (e_G \text{ το ουδέτερο τής } G).$$

Παρατήρηση 1.3.1. Επιλέγοντας ως H την τετριμμένη υποομάδα $\{e_G\}$, διαπιστώνουμε ότι η δράση π_H συμπίπτει κατ' ουσίαν με τη δράση ℓ, αφού $\forall \alpha \in G$, οι πλευρικές κλάσεις αH συμπίπτουν με τα μονοσύνολα $\{\alpha\}$.

Θεώρημα 1.3.1. (α′) *Η δράση $\pi_H : G \times G/H \longrightarrow G/H$ είναι μεταβατική.*

(β′) *Ο σταθερωτής G_{eH} τής αριστερής πλευρικής κλάσης eH ισούται με H.*

(γ′) *Ο πυρήνας τής δράσης π_H ισούται με την υποομάδα $\bigcap_{\alpha\in G} \alpha H\alpha^{-1}$, η οποία είναι η μεγαλύτερη (ως προς τη σχέση υποσυνόλου «$\subseteq$») ορθόθετη (κανονική) υποομάδα τής G που περιέχεται στην H.*

Απόδειξη. (α′) Αν $\alpha H, \beta H \in G/H$, τότε επιλέγοντας $g = \beta\alpha^{-1} \in G$ έχουμε $g\alpha H = \beta H$, δηλαδή $g\pi_H\alpha H = \beta H$ και συνεπώς η π_H είναι μια μεταβατική δράση.
(β′)

$$g \in G_{eH} \Leftrightarrow g\pi_H eH = eH \Leftrightarrow geH = eH \Leftrightarrow g \in eH = H.$$

(γ′) Υπενθυμίζουμε ότι ο πυρήνας τής δράσης π_H ισούται με τον πυρήνα τού επαγόμενου ομομορφισμού $\chi(\pi_H) : G \longrightarrow S_{G/H}$.
Έχουμε:

$$\mathrm{Ker}\chi(\pi_H) = \{g \in G \mid g\alpha H = \alpha H, \forall \alpha H \in G/H\} = \{g \in G \mid \alpha^{-1}g\alpha H = H, \forall \alpha \in G\} = \{g \in G \mid \alpha^{-1}g\alpha \in H, \forall \alpha \in G\}.$$

Επειδή $\alpha^{-1}g\alpha \in H \Leftrightarrow g \in \alpha H\alpha^{-1}$, έπεται ότι

$$\mathrm{Ker}\chi(\pi_H) = \{g \in G \mid \alpha^{-1}g\alpha \in H, \forall \alpha \in G\} = \bigcap_{\alpha\in G} \alpha H\alpha^{-1}.$$

Προφανώς, η τομή $\cap_{\alpha\in G}\alpha H\alpha^{-1} \leq H$ και αφού ισούται με τον $\mathrm{Ker}\chi(\pi_H)$ είναι μια ορθόθετη υποομάδα τής G.
Αν $N \leq H$ είναι μια ορθόθετη υποομάδα τής G που περιέχεται στην H, τότε $\forall \alpha \in G$, $\alpha^{-1}N\alpha = N \leq H$. Συνεπώς, $\forall \alpha \in G, N \leq \alpha H\alpha^{-1}$ και επομένως $N \leq \cap_{\alpha\in G}\alpha H\alpha^{-1}$. □

Πόρισμα 1.3.1 (Cayley). *Κάθε ομάδα $(G, \star)$ είναι ισόμορφη με μια υποομάδα τής συμμετρικής ομάδας $(S_G, \circ)$.*

Απόδειξη. Θεωρούμε την τετριμμένη υποομάδα $H = \{e_G\}$ τής G και τον επαγόμενο ομομορφισμό ομάδων

$$\chi(\pi_{\{e_G\}}) : G \longrightarrow S_{G/\{e_G\}}.$$

Σύμφωνα με το προηγούμενο θεώρημα, ο πυρήνας $\mathrm{Ker}\chi(\pi_{\{e_G\}})$ ισούται με

$$\bigcap_{\alpha\in G}\alpha H\alpha^{-1}=\bigcap_{\alpha\in G}\alpha\{e_G\}\alpha^{-1}=\{e_G\}.$$

Επομένως, ο $\chi(\pi_{\{e_G\}})$ είναι ένας μονομορφισμός ομάδων και γι' αυτό η G είναι ισόμορφη με μια υποομάδα τής $S_{G/\{e_G\}}$. Αλλά η $S_{G/\{e_G\}}$ μπορεί να ταυτιστεί με την S_G, αφού όπως έχουμε ήδη πει, το σύνολο των αριστερών πλευρικών κλάσεων τής $\{e_G\}$ στην G, δηλαδή το $G/\{e_G\}=\{\alpha\{e_G\}\mid \alpha\in G\}$ μπορεί να ταυτιστεί με το σύνολο $G=\{\alpha\in G\}$ των στοιχείων τής G. □

Πόρισμα 1.3.2. *Αν $(G,\star)$ είναι μια ομάδα με πεπερασμένη τάξη και αν υπάρχει μια υποομάδα της $H\leq G$ με δείκτη $[G:H]=p$ τον μικρότερο πρώτο αριθμό που διαιρεί την τάξη τής G, τότε η H είναι μια ορθόθετη υποομάδα τής G.*

Απόδειξη. Θεωρούμε τη δράση $\pi_H: G\times G/H\to G/H$ και τον επαγόμενο ομορφισμό ομάδων $\chi(\pi_H): G\to S_{G/H}$. Επειδή $\mathrm{Ker}\chi(\pi_H)\leq H\leq G$ έχουμε

$$[G:\mathrm{Ker}\chi(\pi_H)]=[G:H][H:\mathrm{Ker}\chi(\pi_H)]=p[H:\mathrm{Ker}\chi(\pi_H)]. \qquad (*)$$

Η πηλικοομάδα $G/\mathrm{Ker}\chi(\pi_H)$ είναι ισόμορφη με μια υποομάδα τής $S_{G/H}$ και αφού το πλήθος των στοιχείων τού συνόλου G/H ισούται με $[G:H]=p$, η τάξη τής $S_{G/H}$ ισούται με $p!$. Σύμφωνα με το Θεώρημα Lagrange, η τάξη τής $G/\mathrm{Ker}\chi(\pi_H)$, που ισούται με $[G:\mathrm{Ker}\chi(\pi_H)]$ είναι ένας διαιρέτης τής τάξης $p!$ τής $S_{G/H}$. Λαμβάνοντας υπ' όψιν την $(*)$ συμπεραίνουμε ότι ο αριθμός $[H:\mathrm{Ker}\chi(\pi_H)]$ διαιρεί το $(p-1)!$.

Αν όμως ο αριθμός $[H:\mathrm{Ker}\chi(\pi_H)]$ είναι $\neq 1$, τότε οποιοσδήποτε πρώτος διαιρέτης q τού συγκεκριμένου αριθμού είναι και διαιρέτης τού $(p-1)!$ και γι' αυτό κάθε τέτοιος πρώτος διαιρέτης q είναι μικρότερος από τον πρώτο αριθμό p. Αλλά κάθε τέτοιος πρώτος q είναι και διαιρέτης τής τάξης $[G:1]$ τής G, αφού

$$[G:1]=[G:H][H:\mathrm{Ker}\chi(\pi_H)][\mathrm{Ker}\chi(\pi_H):1].$$

Αυτό όμως είναι άτοπο, αφού από την υπόθεση γνωρίζουμε ότι ο μικρότερος πρώτος διαιρέτης τής $[G:1]$ είναι ο p. Επομένως, $[H:\mathrm{Ker}\chi(\pi_H)]=1$ και συνεπώς η $H=\mathrm{Ker}\chi(\pi_H)$ είναι μια ορθόθετη υποομάδα τής G. □

Ως τελευταία εφαρμογή τής θεωρίας που αναπτύξαμε μέχρι τώρα παρουσιάζουμε την ακόλουθη πολύ γνωστή πρόταση:

Πρόταση 1.3.1. *Έστω ότι $(G,\star)$ είναι μια πεπερασμένη ομάδα και $H,K\leq G$ δύο υποομάδες τής G.*
Το πλήθος $\mid HK\mid$ των στοιχείων τού συνόλου $HK=\{hk\mid h\in H, k\in K\}$ ισούται με

$$\mid HK\mid=\frac{[H:1][K:1]}{[H\cap K:1]}.$$

Απόδειξη. Θεωρούμε το σύνολο $G/K = \{gK \mid g \in G\}$ των αριστερών πλευρικών κλάσεων τής K στην G. Η απεικόνιση

$$\phi : H \times G/K \to G/K, (h, gK) \quad \mapsto \quad h\phi gK := hgK$$

είναι μια δράση τής H επί τού συνόλου G/K.

Το σύνολο HK ισούται με την ένωση $\cup_{h \in H} hK$. Παρατηρούμε ότι τα σύνολα $hK, h \in H$ είναι ακριβώς τα στοιχεία τής τροχιάς $\mathcal{O}_H(K)$ τού στοιχείου $eK = K \in G/K$ κάτω από τη ϕ–δράση τής H.

Επειδή η τροχιά $\mathcal{O}_H(K)$ περιέχεται στο σύνολο G/K το οποίο είναι πεπερασμένο, έπεται ότι και η τροχιά $\mathcal{O}_H(K)$ αποτελείται από πεπερασμένο το πλήθος στοιχεία, ας πούμε ότι $\mathcal{O}_H(K) = \{h_1K, h_2K, \ldots, h_\ell K\}$.

Συνεπώς,

$$HK = \bigcup_{h \in H} hK = \bigcup_{i=1}^{\ell} h_iK, \quad \text{όπου } \ell \text{ το πλήθος των στοιχείων τής τροχιάς } \mathcal{O}_H(K).$$

Παρατηρούμε ότι αν, $i \neq j$, τότε $h_iK \cap h_jK = \emptyset$, αφού πρόκειται για αριστερές πλευρικές κλάσεις τής K στην G. Επιπλέον, επειδή το πλήθος των στοιχείων οποιασδήποτε αριστερής πλευρικής κλάσης hK ισούται με $[K : 1]$, έπεται ότι

$$\mid HK \mid = \left| \bigcup_{i=1}^{\ell} h_iK \right| = \sum_{i=1}^{\ell} \mid h_iK \mid = \ell[K : 1]. \qquad (*)$$

Αλλά το πλήθος ℓ των στοιχείων τής τροχιάς $\mathcal{O}_H(K)$ ισούται με τον δείκτη $[H : H_{eK}]$, όπου $H_{eK} = \{h \in H \mid heK = eK\}$ είναι ο σταθερωτής τής κλάσης eK κάτω από τη ϕ–δράση τής H.

Τώρα, $H_{eK} = \{h \in H \mid heK = eK\} = \{h \in H \mid h \in K\} = H \cap K$ και έτσι από τη σχέση (*) έπεται

$$\mid HK \mid = [H : H_{eK}][K : 1] = [H : H \cap K][K : 1] = \frac{[H : 1][K : 1]}{[H \cap K : 1]}.$$

□

1.3.3 Το Θεώρημα Cauchy

Έστω ότι $\phi : G \times A \to A$ είναι δράση μιας ομάδας G επί ενός συνόλου A.

Το σύνολο των στοιχείων τού A που παραμένουν σταθερά από τη δράση ϕ τής G, δηλαδή το $\{\alpha \in A \mid g\phi a = a, \forall g \in G\}$, το ονομάζουμε *σύνολο των ϕ-σταθερών στοιχείων* τού A και το συμβολίζουμε με $\mathrm{Fix}_\phi(A)$.

Έστω $\mid A \mid$ (αντιστοίχως $\mid \mathrm{Fix}_\phi(A) \mid$) το πλήθος των στοιχείων τού A (αντιστοίχως τού $\mathrm{Fix}_\phi(A)$).

Λήμμα 1.3.1. *Έστω ότι $\phi : G \times A \to A$ είναι δράση μιας ομάδας $(G, \star)$ επί ενός πεπερασμένου συνόλου A.*
Αν η τάξη τής G είναι p^n, όπου ο p είναι ένας πρώτος αριθμός και ο n είναι ένας φυσικός, τότε ο p διαιρεί τη διαφορά $\mid A \mid - \mid \mathrm{Fix}_\phi(A) \mid$.

Απόδειξη. Το A διαμερίζεται μέσω τής δράσης ϕ σε ένα πεπερασμένο πλήθος r τροχιών $\mathcal{O}_i, 1 \leq i \leq r$, αφού $| A | < \infty$. Έτσι έχουμε:

$$A = \mathcal{O}_1 \cup \mathcal{O}_2 \cup \cdots \cup \mathcal{O}_\ell \cup \mathcal{O}_{\ell+1} \cup \cdots \cup \mathcal{O}_r,$$

όπου το πλήθος $| \mathcal{O}_i |$ των στοιχείων τής $\mathcal{O}_i, 1 \leq i \leq \ell$ ισούται με 1 και το πλήθος $| \mathcal{O}_i |$ των στοιχείων τής $\mathcal{O}_i, \ell+1 \leq i \leq r$ είναι ίσο ή μεγαλύτερο τού 2.

Το σύνολο $\mathrm{Fix}_\phi(A)$ των ϕ-σταθερών στοιχείων τού A ισούται με $\mathcal{O}_1 \cup \mathcal{O}_2 \cup \cdots \cup \mathcal{O}_\ell$ και γι' αυτό $| \mathrm{Fix}_\phi(A) | = \ell$. Διαπιστώνουμε ότι ο πρώτος p διαιρεί τον αριθμό $| \mathcal{O}_i |$, όταν αυτός είναι ≥ 2, αφού $| \mathcal{O}_i | = [G : G_{a_i}]$, όπου a_i είναι οποιοδήποτε στοιχείο τής τροχιάς $\mathcal{O}_i$. Ώστε ο p διαιρεί τον $| \mathcal{O}_i |, \forall i, \ell+1 \leq i \leq r$.
Συνεπώς,

$$| A | = \sum_{i=1}^{r} | \mathcal{O}_i | = \sum_{i=1}^{\ell} | \mathcal{O}_i | + \sum_{i=\ell+1}^{r} | \mathcal{O}_i | = | \mathrm{Fix}_\phi(A) | + \kappa p.$$

Επομένως, ο p διαιρεί την διαφορά $| A | - | \mathrm{Fix}_\phi(A) |$. □

Θεώρημα 1.3.2 (Cauchy). *Έστω $(G, \star)$ μια ομάδα τάξης $[G : 1] = n \in \mathbb{N}$ και p ένας πρώτος διαιρέτης τού n. Τότε υπάρχει ένα στοιχείο $g \in G$ με τάξη p.*

Απόδειξη. Είναι αρκετό να αποδείξουμε ότι υπάρχει κάποιο $g \neq e_G$ με $g^p = e_G$, αφού τότε η τάξη τού g είναι ένας διαιρέτης τού p και επειδή ο p είναι πρώτος και $g \neq e_G$ έχουμε ότι η τάξη τού g είναι p.
Σχηματίζουμε το σύνολο

$$A = \{(g_1, g_2, \ldots, g_p) \mid g_i \in G, \forall i, 1 \leq i \leq p \text{ με } g_1 g_2 \ldots g_p = e_G\}.$$

Το πλήθος $| A |$ των στοιχείων τού A ισούται με $[G : 1]^{(p-1)}$, αφού τα $g_1, g_2, \ldots, g_{p-1}$ μπορεί να είναι οποιαδήποτε στοιχεία τής G, ενώ το g_p είναι μοναδικώς καθορισμένο από τα $g_1, g_2, \ldots, g_{p-1}$, αφού $g_p = (g_1 g_2 \ldots g_{p-1})^{-1}$.
Επειδή ο p διαιρεί τον n έχουμε $n = \kappa p$ και συνεπώς

$$| A | = [G : 1]^{(p-1)} = \kappa^{(p-1)} p^{(p-1)}. \qquad (*)$$

Παρατηρούμε ότι αν,

$$g_1 g_2 \ldots g_i g_{i+1} \ldots g_p = e_G, \text{ τότε } g_{i+1} g_{i+2} \ldots g_p = (g_1, g_2 \ldots g_i)^{-1},$$

και γι' αυτό $(g_{i+1} g_{i+2} \ldots g_p)(g_1 g_2 \ldots g_i) = e_G$.

Συνεπώς αν, η p–άδα $(g_1, g_2, \ldots, g_p)$ ανήκει στο A, τότε και οποιαδήποτε άλλη p–άδα $(g_{i+1}, g_{i+2}, \ldots, g_p, g_1, g_2, \ldots, g_i)$, η οποία προκύπτει από την πρώτη κατόπιν κυκλικής εναλλαγής των συνιστωσών της, ανήκει επίσης στο A.

Θεωρούμε την αβελιανή ομάδα $(\mathbb{Z}_p, +)$ και ορίζουμε την απεικόνιση

$$\phi : \mathbb{Z}_p \times A \longrightarrow A, ([i], (g_1, g_2, \ldots, g_p)) \mapsto (g_{(i+1)\bmod p}, g_{(i+2)\bmod p}, \ldots, g_{(i+p)\bmod p}),$$

όπου οι δείκτες $(i{+}1)\bmod p$, $(i{+}2)\bmod p, \ldots, (i{+}p)\bmod p$ διατρέχουν τους αντιπροσώπους j των κλάσεων $\bmod p$ με j μεταξύ των αριθμών 1 και p.

Η απεικόνιση ϕ είναι μια δράση τής ομάδας $\mathbb{Z}_p$ επί τού συνόλου A. Παρατηρούμε ότι ένα στοιχείο $(g_1, g_2, \ldots, g_p) \in A$ ανήκει στο σύνολο $\mathrm{Fix}_\phi(A)$ των ϕ–σταθερών στοιχείων τού A, αν και μόνο αν,

$$\begin{aligned}
&[1]\phi(g_1, g_2, \ldots, g_{p-1}, g_p) = (g_1, g_2, \ldots, g_{p-1}, g_p) \Leftrightarrow \\
&(g_{(1+1)\bmod p}, g_{(1+2)\bmod p}, \ldots, g_{(1+(p-1))\bmod p}, g_{(1+p)\bmod p}) = (g_1, g_2, \ldots, g_p) \Leftrightarrow \\
&(g_2, g_3, \ldots, g_p, g_1) = (g_1, g_2, \ldots, g_p) \Leftrightarrow g_1 = g_2 = g_3 = \cdots = g_p.
\end{aligned}$$

Συνεπώς, τα στοιχεία τού συνόλου $\mathrm{Fix}_\phi(A)$ συμπίπτουν με τις p–άδες $(g, g, \ldots, g)$, όπου $g \in G$ με $g^p = e_G$. Το πλήθος $|\ \mathrm{Fix}_\phi(A)\ |$ τού $\mathrm{Fix}_\phi(A)$ είναι ≥ 1, αφού η p–άδα $(e_G, e_G, \ldots, e_G)$ ανήκει στο $\mathrm{Fix}_\phi(A)$.
Σύμφωνα με το προηγούμενο λήμμα, η τάξη p τής $\mathbb{Z}_p$ διαιρεί τη διαφορά $|\ A\ | - |\ \mathrm{Fix}_\phi(A)\ |$ και επειδή, λόγω τής $(*)$, η τάξη τού A είναι πολλαπλάσιο τού p, έπεται ότι ο p διαιρεί τον αριθμό $|\ \mathrm{Fix}_\phi(A)\ | \geq 1$. Επομένως, $|\ \mathrm{Fix}_\phi(A)\ | \geq p \geq 2$ και γι' αυτό υπάρχει ένα στοιχείο $(g, g, \ldots, g) \in \mathrm{Fix}_\phi(A) \subseteq A$ με $g \neq e_G$. Ώστε, $g^p = e_G$ με $g \neq e_G$. Προφανώς, το g έχει τάξη p. □

1.4 Συζυγία

Θεωρούμε τώρα μία ακόμα δράση μιας ομάδας επί τού εαυτού της, η οποία όπως θα δούμε σύντομα θα χορηγήσει πολλά και ουσιαστικά αποτελέσματα στη Θεωρία Ομάδων.

Η απεικόνιση

$$\sigma : G \times G \longrightarrow G, (g, \alpha) \ \mapsto \ g\sigma\alpha := g\alpha g^{-1}$$

ορίζει μια δράση τής G επί του εαυτού της, αφού

$$\begin{aligned}
&\forall g_1, g_2, \alpha \in G : (g_1 g_2)\sigma\alpha = (g_1 g_2)\alpha(g_1 g_2)^{-1} = g_1(g_2 \alpha g_2^{-1})g_1^{-1} = g_1\sigma(g_2\sigma\alpha) \text{ και} \\
&\forall \alpha \in G : e_G\sigma\alpha = e_G\alpha(e_G)^{-1} = \alpha.
\end{aligned}$$

Ορισμός 1.4.1. Η δράση $\sigma : G \times G \longrightarrow G, (g, \alpha) \mapsto g\sigma\alpha := g\alpha g^{-1}$ ονομάζεται *δράση συζυγίας* επί των στοιχείων τής G.

Στη συγκεκριμένη περίπτωση οι τροχιές στις οποίες διαμερίζεται η G μέσω τής δράσης συζυγίας σ ονομάζονται *κλάσεις συζυγίας*.

Δύο στοιχεία $\alpha, \beta \in G$ ανήκουν στην ίδια κλάση, αν και μόνο αν, $\exists g \in G$ με $g\alpha g^{-1} = \beta$.

Στοιχεία που ανήκουν στην ίδια κλάση συζυγίας ονομάζονται *συζυγή στοιχεία*.

Η κλάση συζυγίας τού στοιχείου $\alpha \in G$ είναι το σύνολο $\mathcal{K}_\alpha = \{g\alpha g^{-1} \mid g \in G\}$.

Αν η G είναι μια πεπερασμένη ομάδα, τότε το πλήθος των κλάσεων συζυγίας είναι επίσης πεπερασμένο, αφού η κλάσεις συζυγίας αποτελούν μια διαμέριση τής G.

Παρατηρήσεις 1.4.1. (α′) Αν η G είναι μια αβελιανή ομάδα, τότε η δράση τής συζυγίας είναι τετριμμένη, αφού $\forall g, \alpha \in G$ είναι $g\sigma\alpha = g\alpha g^{-1} = gg^{-1}\alpha = e_G\alpha = \alpha$.

(β′) Αν $[G : 1] > 1$, τότε η δράση τής συζυγίας δεν είναι μεταβατική, αφού η κλάση συζυγίας $\mathcal{K}_{e_G}$ τού ουδέτερου στοιχείου e_G τής G είναι το μονοσύνολο $\mathcal{K}_{e_G} = \{e_G\}$.

(γ′) Γενικώς, η κλάση συζυγίας $\mathcal{K}_\alpha$ ενός στοιχείου $\alpha \in G$ είναι μονοσύνολο (και τότε βέβαια αποτελείται μόνο από το στοιχείο α) αν, και μόνο αν, το α ανήκει στο *κέντρο* τής ομάδας

$$Z(G) = \{\alpha \in G \mid \alpha g = g\alpha, \forall g \in G\}.$$

(δ′) Κάθε στοιχείο $\beta \in G$ που ανήκει στην κλάση συζυγίας $\mathcal{K}_\alpha$ τού $\alpha \in G$ έχει την ίδια τάξη με το α, αφού $\forall g \in G$, η απεικόνιση $\phi_g : G \to G, \alpha \mapsto g\alpha g^{-1}$ είναι ένας αυτομορφισμός τής G.

Παραδείγματα 1.4.1. Οι κλάσεις συζυγίας τής συμμετρικής ομάδας $(S_3, \circ)$ είναι οι:

$$\mathcal{K}_{\mathrm{Id}_3} = \{\mathrm{Id}_3\}, \ \mathcal{K}_{(12)} = \{(12), (13), (23)\} \ \text{ και } \ \mathcal{K}_{(123)} = \{(123), (132)\}.$$

Υπενθυμίζουμε ότι δύο κύκλοι τής $(S_n, \circ)$ με το ίδιο μήκος είναι πάντοτε συζυγείς. Πράγματι, αν $c_1 = (i_1 i_2 \dots i_\ell)$ και $c_2 = (j_1 j_2 \dots j_\ell)$, τότε για κάθε $\tau \in S_n$ με $\tau(i_r) = j_r, \forall r, 1 \leq r \leq \ell$ είναι

$$\tau c_1 \tau^{-1} = \tau(i_1 i_2 \dots i_\ell)\tau^{-1} = (\tau(i_1)\tau(i_2)\dots\tau(i_\ell)) = (j_1 j_2 \dots j_\ell) = c_2.$$

1.4.1 Επεκτείνοντας τη Δράση Συζυγίας

Η δράση τής συζυγίας πάνω στο σύνολο των στοιχείων τής ομάδας G επεκτείνεται σε μια δράση $\tilde{\sigma}$ επί τού συνόλου $\mathcal{P}^\star(G)$ όλων των μη κενών υποσυνόλων τής G:

$$\tilde{\sigma} : G \times \mathcal{P}^\star(G) \to \mathcal{P}^\star(G), (g, A) \mapsto g\tilde{\sigma}A := gAg^{-1}.$$

Αν η G είναι μια πεπερασμένη ομάδα, τότε το πλήθος των στοιχείων τής τροχιάς $\mathcal{O}_A$ τού $A \subseteq G$ ισούται με τον δείκτη $[G : G_A]$, όπου $G_A = \{g \in G \mid gAg^{-1}\}$ είναι ο σταθερωτής τού συνόλου A.

Όταν το A είναι ένα μονοσύνολο, ας πούμε $A = \{\alpha\}$, τότε ο σταθερωτής $G_{\{\alpha\}}$ ονομάζεται ο *κεντρωτής* τού στοιχείου α και συμβολίζεται με $C_G(\alpha)$. Ώστε,

$$C_G(\alpha) = \{g \in G \mid g\alpha g^{-1} = \alpha\} = \{g \in G \mid g\alpha = \alpha g\}.$$

Όταν η G είναι μια πεπερασμένη ομάδα, τότε το πλήθος των συζυγών στοιχείων τού α, δηλαδή το πλήθος των στοιχείων τής κλάσης συζυγίας $\mathcal{K}_\alpha$ ισούται με $[G : C_G(\alpha)]$. Προφανώς, για το κέντρο $Z(G)$ μιας ομάδας G έχουμε:

$$Z(G) = \bigcap_{\alpha \in G} C_G(\alpha).$$

Όταν το $H \leq G$ είναι μια υποομάδα τής G, τότε ο σταθερωτής G_H τού H ονομάζεται ο *ορθοθέτης* ή *κανονικοποιητής* ή *ορθοθέτρια υποομάδα* τής H και συμβολίζεται με $N_G(H)$. Συνεπώς,

$$N_G(H) = \{g \in G \mid gHg^{-1} = H\}.$$

Παρατήρηση 1.4.1. Αν $H \leq G$ είναι μια υποομάδα τής G, τότε ο σταθερωτής $N_G(H)$ τής G είναι η μεγαλύτερη (ως προς τη σχέση υποσυνόλου «$\subseteq$») υποομάδα τής G εντός τής οποίας η H είναι ορθόθετη, δηλαδή $H \trianglelefteq N_G(H)$.

Μια υποομάδα $H \leq$ τής G είναι ορθόθετη αν, και μόνο αν, $N_G(H) = G$.

1.4.2 Η Εξίσωση των Κλάσεων

Θεώρημα 1.4.1. *Αν, G είναι μια ομάδα με πεπερασμένη τάξη $[G : 1] < \infty$ και αν, $\alpha_1, \alpha_2, \ldots, \alpha_\ell$ είναι οι αντιπρόσωποι από τις διαφορετικές κλάσεις συζυγίας που έχουν περισσότερα τού ενός στοιχεία, τότε*

$$[G : 1] = [Z(G) : 1] + \sum_{j=1}^{\ell} [G : C_G(\alpha_j)].$$

Απόδειξη. Θεωρούμε τη διαμέριση τής G στις κλάσεις συζυγίας:

$$G = \mathcal{Z}_1 \cup \mathcal{Z}_2 \cup \cdots \cup \mathcal{Z}_t \cup \mathcal{K}_1 \cup \mathcal{K}_2 \cup \cdots \cup \mathcal{K}_\ell, \tag{*}$$

όπου $\mathcal{Z}_i, 1 \leq i \leq t$ είναι οι κλάσεις συζυγίας που καθεμιά τους αποτελείται από ακριβώς ένα στοιχείο και $\mathcal{K}_j, 1 \leq j \leq \ell$ είναι οι κλάσεις που καθεμιά τους αποτελείται από περισσότερα τού ενός στοιχεία. Όπως ήδη έχουμε πει, η κλάση συζυγίας ενός στοιχείου $\alpha \in G$ αποτελείται μόνο από το α αν, και μόνο αν, το α ανήκει στο κέντρο $Z(G)$ τής G. Γι' αυτό το πλήθος t των κλάσεων συζυγίας με ένα στοιχείο ισούται με την τάξη $[Z(G) : 1]$ τού κέντρου. Επιπλέον, το πλήθος των στοιχείων τής $\mathcal{K}_j, 1 \leq j \leq \ell$ ισούται με τον δείκτη $[G : C_G(\alpha_j)]$, όπου α_j είναι οποιοδήποτε στοιχείο τής κλάσης $\mathcal{K}_j$.

Γι΄αυτό από την (*) προκύπτει η

$$[G : 1] = [Z(G) : 1] + \sum_{j=1}^{\ell} [G : C_G(\alpha_j)].$$

□

Η ανωτέρω ισότητα αυτή ονομάζεται η *Εξίσωση των Κλάσεων*.

Παραδείγματα 1.4.2. (α′) Αν η G είναι μια πεπερασμένη αβελιανή ομάδα, τότε η ισότητα των κλάσεων χορηγεί την ισότητα $[G : 1] = [Z(G) : 1]$, που προφανώς είναι αλήθές, αφού $G = Z(G)$.

(β′) Θα αποδείξουμε κάθε ομάδα με 15 στοιχεία είναι αβελιανή.

Ας υποθέσουμε ότι υπάρχει μια ομάδα G με 15 στοιχεία που δεν είναι αβελιανή. Χρησιμοποιώντας την Εξίσωση των Κλάσεών της που θα την προσδιορίσουμε θα καταλήξουμε σε άτοπο.

Πρώτα παρατηρούμε ότι η τάξη $[Z(G) : 1]$ τού κέντρου της οφείλει να είναι ή 1 ή 3 ή 5 ή 15 ως διαιρέτης τού 15. Αφού η G δεν είναι αβελιανή, το $[Z(G) : 1] \neq 15$. Επίσης, $[Z(G) : 1] \neq 5$ (αντιστοίχως $\neq 3$), αφού τότε η πηλικοομάδα $G/Z(G)$ είναι κυκλική, ως έχουσα τάξη 3 (αντιστοίχως 5) και τότε η G θα ήταν μια αβελιανή ομάδα. Επομένως, $[Z(G) : 1] = 1$.

Από το Θεώρημα Cauchy γνωρίζουμε ότι η G διαθέτει τουλάχιστον ένα στοιχείο α με τάξη $\circ(\alpha) = 3$ και ένα $\beta \in G$ με τάξη $\circ(\beta) = 3$.

Η κυκλική υποομάδα $\langle\alpha\rangle$ περιέχεται στον κεντρωτή $C_G(\alpha)$. Συνεπώς, ο αριθμός $3 \mid [C_G(\alpha) : 1]$ και επειδή $C_G(\alpha) < G$, αφού αν ίσχυε η ισότητα, τότε το α θα ανήκε στο $Z(G)$, συμπεραίνουμε ότι $[C_G(\alpha) : 1] = 3$ και η κλάση συζυγίας $\mathcal{K}_\alpha$ τού α αποτελείται από $[G : C_G(\alpha)] = 5$ στοιχεία.

Αποδεικνύεται με ανάλογο τρόπο ότι $\langle\beta\rangle = C_G(\beta)$ και η κλάση συζυγίας $\mathcal{K}_\alpha$ τού β αποτελείται από $[G : C_G(\beta)] = 3$ στοιχεία.

Αφού η G δεν είναι αβελιανή, κάθε στοιχείο $\neq e_G$ τής G έχει τάξη 3 ή 5 και έτσι

$$\begin{aligned} 15 = {} & [Z(G) : 1] + \mid \mathcal{K}_\alpha \mid + \mid \mathcal{K}_\beta \mid + \text{ το πλήθος} \\ & \text{των στοιχείων κάποιων επιπλέον κλάσεων συζυγίας } \mathcal{K}' = \\ & 1 + 5 + 3 + \text{ το πλήθος των στοιχείων κάποιων επιπλέον κλάσεων συζυγίας } \mathcal{K}'. \end{aligned}$$

Προφανώς, το πλήθος των στοιχείων οποιασδήποτε επιπλέον κλάσης συζυγίας $\mathcal{K}'$ πρέπει να ισούται με 3, αφού αν κάποια $\mathcal{K}'$ διέθετε 5 στοιχεία, τότε η ισότητα

$$15 = 1 + 5 + 3 + 5 + \sum_{i=1}^{\ell} x_i$$

δεν μπορεί να συμπληρωθεί με κατάλληλα $x_i = 3$ ή 5 ώστε να δώσει το 15. Γι΄αυτό η μοναδική περίπτωση είναι

$$15 = 1 + 5 + 3 + 3 + 3.$$

Επομένως, η G έχει διαμεριστεί στην

(α′) κλάση συζυγίας με ένα στοιχείο, την $Z(G)$,

(β′) στην κλάση $\mathcal{K}_\alpha$ η οποία αποτελείται από 5 στοιχεία τάξης ίσης με την τάξη τού α, δηλαδή τάξης 3,

(γ′) στην κλάση $\mathcal{K}_\beta$ η οποία αποτελείται από 3 στοιχεία τάξης ίσης με την τάξη τού β, δηλαδή τάξης 5 (δ′) και σε άλλες δύο κλάσεις $\mathcal{K}_\gamma, \mathcal{K}_\delta$ που καθεμιά τους αποτελείται από 3 στοιχεία τάξης 5, επειδή ο κεντρωτής $C_G(\gamma)$ (αντιστοίχως $C_G(\delta)$) έχει τάξη 5 και $\{e_G\} < \langle\gamma\rangle \leq C_G(\gamma)$ (αντιστοίχως $\{e_G\} < \langle\delta\rangle \leq C_G(\delta)$).

Συνεπώς, η G διαθέτει 5 στοιχεία τάξης 3 και 9 στοιχεία τάξης 5. Τα στοιχεία τάξης 5 είναι διαμοιρασμένα σε υποομάδες τής G τάξης 5, που ανά δύο έχουν ως τομή μόνο το ουδέτερο στοιχείο, αφού πρόκειται για κυκλικές υποομάδες με τάξη πρώτο αριθμό. Αλλά, αν H_1, H_2 είναι δύο από αυτές, τότε οι H_1 και H_2 περιέχουν ακριβώς 8 διαφορετικά στοιχεία τάξης 5. Έτσι όμως μένει ένα επιπλέον στοιχείο τ τάξης 5 το οποίο δεν ανήκει ούτε στην H_1 ούτε στην H_2 με $\langle\tau\rangle \cap H_1 = e_G$ και $\langle\tau\rangle \cap H_2 = e_G$. Αλλά τώρα η $\langle\tau\rangle$ δίνει ακόμα τέσσερα στοιχεία (μαζί με το τ) τάξης 5. Έτσι συνολικά έχουμε τουλάχιστον 12 στοιχεία τάξης 5, πράγμα άτοπο.

Επομένως, η G είναι αβελιανή ομάδα.

(γ′) Θα υπολογίσουμε τις κλάσεις συζυγίας τής ομάδας τετρανίων

$$Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}, \text{ με } (-1)^2 = 1, i^2 = j^2 = k^2 = ijk = -1$$

και όπου το 1 είναι το ταυτοτικό στοιχείο τής Q_8 και το -1 μετατίθεται με οποιοδήποτε άλλο στοιχείο.

Το κέντρο $Z(Q_8)$ τής Q_8 ισούται με $\{1, -1\}$. Συνεπώς έχουμε ακριβώς δύο κλάσεις συζυγίας τις $\mathcal{K}_1, \mathcal{K}_{-1}$ που καθεμιά τους έχει μόνο ένα στοιχείο. Παρατηρούμε ότι $[D_4 : H_i] = 2, i = 1, 2, 3$ και $\forall g \in H_1 \cup H_2 \cup H_3 \setminus Z()$επειδή η $\langle i\rangle$ περιέχεται στον κεντρωτή $C_{Q_8}(i)$ τού i και $C_{Q_8}(i) \lneqq Q_8$, αφού $i \notin Z(Q_8)$, η σχέση

$$2 = [Q_8 : \langle i\rangle] = [Q_8 : C_{Q_8}(i)][C_{Q_8}(i) : \langle i\rangle]$$

δίνει $C_{Q_8}(i) = \langle i\rangle$. Επομένως, το πλήθος των στοιχείων τής $\mathcal{K}_i$ ισούται με τον δείκτη $[Q_8 : \langle i\rangle] = 2$ και $\mathcal{K}_i = \{i, -i\}$, αφού

$$jij^{-1} = ji(-j) = (-1)jij = (-1)jk = -i.$$

Παρομοίως προκύπτει $\mathcal{K}_j = \{j, -j\}$ και $\mathcal{K}_k = \{k, -k\}$.

(δ′) Τέλος, θα υπολογίσουμε τις κλάσεις συζυγίας τής διεδρικής ομάδας

$$D_4 = \{\sigma, \alpha \mid \sigma^2 = \mathrm{Id}, \alpha^4 = \mathrm{Id}, \alpha\sigma = \sigma\alpha^3\}.$$

Το κέντρο $Z(D_4)$ τής D_4 ισούται με $\{\mathrm{Id}, \alpha^2\}$. Συνεπώς έχουμε ακριβώς δύο κλάσεις συζυγίας τις $\mathcal{K}_{\mathrm{Id}}, \mathcal{K}_{\alpha^2}$ που καθεμιά τους έχει μόνο ένα στοιχείο.

Θεωρούμε τις υποομάδες $H_1 = \{\mathrm{Id}, \alpha, \alpha^2, \alpha^3\}$, $H_2 = \{\mathrm{Id}, \sigma, \alpha^2, \sigma\alpha\}$ και $H_3 = \{\mathrm{Id}, \sigma, \alpha^3, \sigma\alpha^3\}$.

Παρατηρούμε ότι $\forall g \in H_i \setminus Z(D_4), i = 1, 2, 3$ η υποομάδα H_i περιέχεται στον κεντρωτή $C_{D_4}(g)$, ο οποίος είναι γνήσια υποομάδα τής D_4, αφού $g \notin Z(D_4)$. Επειδή ο δείκτης $[D_4 : H_i] = 2, i = 1, 2, 3$, έχουμε $H_i = C_{D_4}(g), \forall g \in H_i \setminus Z(G), i = 1, 2, 3$ και γι' αυτό η κλάση συζυγίας κάθε $g \in H_1 \cup H_2 \cup H_3 \setminus Z(G)$ αποτελείται από ακριβώς δύο στοιχεία. Έχουμε $\mathcal{K}_\alpha = \{\alpha, \alpha^3\}, \mathcal{K}_\sigma = \{\sigma, \sigma\alpha^2\}, \mathcal{K}_{\sigma\alpha} = \{\sigma\alpha, \sigma\alpha^3\}$.

Θεώρημα 1.4.2. *Κάθε ομάδα $(G, \star)$ τάξης p^α, $\alpha \geq 1$, όπου p είναι ένας πρώτος αριθμός, έχει μη τετριμμένο κέντρο.*

Απόδειξη. Από την εξίσωση κλάσεων γνωρίζουμε ότι

$$[G:1] = [Z(G):1] + \sum_{j=1}^{\ell} [G : C_G(\alpha_j)],$$

όπου τα $\alpha_j, j = 1, \ldots, \ell$ είναι οι αντιπρόσωποι των κλάσεων με περισσότερα τού ενός στοιχεία. Ο πρώτος αριθμός p διαιρεί την τάξη $[G:1]$ τής G καθώς και κάθε δείκτη $[G : C_G(\alpha_j)]$, αφού $[G : C_G(\alpha_j)] \geq 2$. Επομένως, ο p διαιρεί την τάξη $[Z(G):1]$ τού κέντρου τής G και γι' αυτό $[Z(G):1] \geq p \geq 2$. □

Θεώρημα 1.4.3. *Κάθε ομάδα $(G, \star)$ τάξης p^2, όπου ο p είναι πρώτος αριθμός, είναι αβελιανή και μάλιστα ισόμορφη ή με την $\mathbb{Z}_{p^2}$ ή με την $\mathbb{Z}_p \times \mathbb{Z}_p$.*

Απόδειξη. Το κέντρο $Z(G)$ τής G είναι μη τετριμμένο και γι' αυτό $[Z(G) : 1] = p^2$ ή $[Z(G) : 1] = p$. Στην πρώτη περίπτωση η G είναι αβελιανή, αφού $G = Z(G)$ και στη δεύτερη περίπτωση η G είναι και πάλι αβελιανή, αφού η πηλικοομάδα $G/Z(G)$ είναι κυκλική ως έχουσα τάξη τον πρώτο αριθμό p.
Ώστε η G είναι σε κάθε περίπτωση αβελιανή.

Αν η G διαθέτει ένα στοιχείο τάξης p^2, τότε $G \cong \mathbb{Z}_{p^2}$.
Διαφορετικά κάθε στοιχείο τής G, που δεν είναι το ουδέτερο, έχει τάξη p. Θεωρούμε ένα τέτοιο στοιχείο $x \in G, x \neq e_G$ και ένα ακόμα στοιχείο $y \in G \setminus \langle x \rangle$. Αμφότερα τα x, y έχουν τάξη p και $\langle x \rangle \cap \langle y \rangle = \{e_G\}$, αφού η τάξη $[\langle x \rangle \cap \langle y \rangle : 1]$ είναι, ως διαιρέτης τής τάξης $[\langle x \rangle : 1]$, ή 1 ή p. Αλλά αν, $[\langle x \rangle \cap \langle y \rangle : 1] = p$, τότε $y \in \langle x \rangle$, πράγμα άτοπο.

Θεωρούμε την απεικόνιση

$$\psi : \langle x \rangle \times \langle y \rangle \to G, (x^i, y^j) \mapsto \psi((x^i, y^j)) := x^i y^j.$$

Η ψ είναι ένας ομομορφισμός ομάδων, αφού

$$\begin{aligned} &\psi((x^{i_1}, y^{j_1})(x^{i_2}, y^{j_2})) = \psi((x^{i_1}x^{i_2}, y^{j_1}y^{j_2})) = \\ &x^{i_1}x^{i_2}y^{j_1}y^{j_2} = x^{i_1}y^{j_1}x^{i_2}y^{j_2} = \psi((x^{i_1}, y^{j_1}))\psi((x^{i_2}, y^{j_2})) \end{aligned}$$

Επιπλέον, $\mathrm{Ker}\psi = \{(e_G, e_G)\}$, αφού

$$\begin{aligned} &\psi((x^i, y^j)) = e_G \Leftrightarrow x^i y^j = e_G \Leftrightarrow x^i = y^{-j} \Rightarrow \\ &x^i = y^{-j} \in \langle x \rangle \cap \langle y \rangle = \{e_G\} \Rightarrow x^i = y^j = e_G \Rightarrow (x^i, y^j) = (e_G, e_G). \end{aligned}$$

Συνεπώς, ο ψ είναι μονομορφισμός και επομένως ισομορφισμός, αφού
$[\langle x \rangle \times \langle y \rangle : 1] = p^2 = [G : 1]$. Αλλά $\langle x \rangle \cong \mathbb{Z}_p$ και $\langle y \rangle \cong \mathbb{Z}_p$.
Επομένως, $G \cong \mathbb{Z}_p \times \mathbb{Z}_p$. □

Ποια είναι η Πιθανότητα δύο Στοιχεία μιας Ομάδας να μετατίθενται;

Έστω ότι $(G, \star)$ είναι μια ομάδα τάξης $[G:1] < \infty$ και g, α δύο οποιαδήποτε στοιχεία της, όχι απαραιτήτως διαφορετικά. Θα εξετάσουμε ποιες τιμές μπορεί να λάβει η πιθανότητα $\Pr(G)$ ώστε $g\alpha = \alpha g$.

Αν η G είναι μια αβελιανή ομάδα, τότε $\Pr(G) = 1$, αφού $\forall (g, \alpha) \in G \times G$ είναι $g\alpha = \alpha g$.

Θεωρούμε το σύνολο

$$L = \{(g, \alpha) \in G \times G \mid g\alpha = \alpha g\},$$

τότε,

$$\Pr(G) = \frac{\mid L \mid}{\mid G \times G \mid} = \frac{\mid L \mid}{[G:1]^2},$$

όπου με $\mid S \mid$ συμβολίζουμε, ως συνήθως, το πλήθος των στοιχείων ενός συνόλου S.

Θεώρημα 1.4.4. *Αν $(G, \star)$ είναι μια ομάδα τάξης $[G:1] < \infty$, τότε*

$$\Pr(G) = \frac{r}{[G:1]}, \text{ όπου } r \text{ είναι το πλήθος των κλάσεων συζυγίας τής } G.$$

Επιπλέον, αν η G δεν είναι αβελιανή, τότε $\Pr(G) \leq \frac{5}{8}$.

Απόδειξη. Παρατηρούμε ότι

$$L = \bigcup_{g \in G} L_g, \text{ όπου } L_g = \{(g, \alpha) \mid \alpha \in G, g\alpha = \alpha g\}.$$

Τα σύνολα $L_g, g \in G$ χορηγούν μια διαμέριση τού L, αφού αν $L_g \cap L_h \neq \emptyset$, τότε $\exists (x, y) \in L_g \cap L_h$ και τότε $g = x = h$. Επομένως, $L_g = L_h$.

Έτσι έχουμε

$$\mid L \mid = \sum_{g \in G} \mid L_g \mid .$$

Αλλά, $\forall g \in G$ το πλήθος $\mid L_g \mid$ ισούται με το πλήθος των στοιχείων τού συνόλου $G^g = \{\alpha \in G \mid g\alpha g^{-1} = \alpha\}$, αφού η απεικόνιση

$$L_g \to G^g, (g, \alpha) \mapsto \alpha$$

είναι «1–1» και «επί», επειδή

$$(g, \alpha) \in L_g \Leftrightarrow g\alpha = \alpha g \Leftrightarrow g\alpha g^{-1} = \alpha \Leftrightarrow \alpha \in G^g.$$

Επομένως,

$$\mid L \mid = \sum_{g \in G} \mid L_g \mid = \sum_{g \in G} \mid G^g \mid \qquad (*)$$

Όμως για κάθε $g \in G$, το $G^g = \{\alpha \in G \mid g\alpha g^{-1} = \alpha\}$ είναι το σύνολο των στοιχείων τής G που μένουν σταθερά από το g ως προς τη δράση τής συζυγίας $G \times G \to G$, $(g, \alpha) \mapsto g\alpha g^{-1}$ και από τον τύπο τού Burnside, βλ. Θεώρημα 1.2.2, έχουμε ότι το πλήθος r των κλάσεων συζυγίας ισούται με

$$r = \frac{1}{[G:1]} \sum_{g \in G} \mid G^g \mid . \tag{**}$$

Από τις (*) και (**) έπεται $[G:1]r = \mid L \mid$ και συνεπώς

$$\Pr(G) = \frac{\mid L \mid}{[G:1]^2} = \frac{[G:1]r}{[G:1]^2} = \frac{r}{[G:1]}.$$

Θα αποδείξουμε τώρα ότι αν, η G δεν είναι αβελιανή, τότε το $5/8$ είναι το ελάχιστο άνω φράγμα για την πιθανότητα $\Pr(G)$.

Θεωρούμε τη διαμέριση τής G στις κλάσεις συζυγίας της:

$$G = \mathcal{Z}_1 \cup \mathcal{Z}_2 \cup \cdots \cup \mathcal{Z}_t \cup \mathcal{K}_1 \cup \mathcal{K}_2 \cup \cdots \cup \mathcal{K}_\ell,$$

όπου οι $\mathcal{Z}_i, 1 \leq i \leq t$ είναι οι κλάσεις συζυγίας με ένα στοιχείο και $\mathcal{K}_j, 1 \leq j \leq \ell$ οι κλάσεις συζυγίας με τουλάχιστον δύο στοιχεία. Η ένωση $\mathcal{Z}_1 \cup \mathcal{Z}_2 \cup \cdots \cup \mathcal{Z}_t$ ισούται με το κέντρο $Z(G)$ τής G και γι' αυτό $[Z(G):1] = t$.

Από την Εξίσωση των Κλάσεων παίρνουμε

$$[G:1] = [Z(G):1)] + \sum_{j=1}^{\ell} \mid \mathcal{K}_j \mid \geq [Z(G):1)] + 2\ell,$$

επειδή $\mid \mathcal{K}_j \mid \geq 2$.

Συνεπώς,

$$\frac{[G:1] - [Z(G):1]}{2} \geq \ell.$$

Επομένως, για το πλήθος r των κλάσεων συζυγίας έχουμε ότι

$$r = [Z(G):1] + \ell \leq [Z(G):1] + \frac{[G:1] - [Z(G):1]}{2} = \frac{[G:1] + [Z(G):1]}{2}$$

Όμως, αφού η G δεν είναι αβελιανή, πρέπει να ισχύει $[Z(G):1] \leq [G:1]/4$. Αφού διαφορετικά, δηλαδή αν, $[Z(G):1] > [G:1]/4$, τότε $4 > ([G:1]/[Z(G):1]) = [G/Z(G):1]$ και τότε η $G/Z(G)$ είναι κυκλική, που συνεπάγει ότι η G είναι αβελιανή.

Έτσι διαπιστώνουμε ότι για το πλήθος r των κλάσεων συζυγίας έχουμε

$$r = [Z(G):1] + \ell \leq \frac{[G:1] + [Z(G):1]}{2} \leq \frac{[G:1]}{2} + \frac{[G:1]/4}{2} = \frac{5}{8}[G:1].$$

Επομένως,

$$\Pr(G) = \frac{r}{[G:1]} \leq \frac{\frac{5}{8}[G:1]}{[G:1]} = \frac{5}{8}.$$

□

Παρατηρήσεις 1.4.2. Ο αριθμός $5/8$ είναι όντως το ελάχιστο άνω φράγμα στην περίπτωση των μη αβελιανών ομάδων. Για παράδειγμα, αν η ομάδα G είναι η διεδρική ομάδα D_4 ή η ομάδα των τετρανίων Q_8, τότε $\mathrm{Pr}(G) = 5/8$, αφού και στις δύο συγκεκριμένες περιπτώσεις, το πλήθος των κλάσεων συζυγίας ισούται με 5 και το πλήθος των στοιχείων των ομάδων ισούται με 8.

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