Ομάδες: Τρίτο μάθημα

Στο μάθημα αυτό αρχίζουμε σιγά-σιγά να εισερχόμεθα στην μελέτη νέων εννοιών στην Θεωρία Ομάδων. Στην αρχή θα παραθέσουμε τα τρία θεωρήματα των ισομορφισμών για υπενθύμιση και σχολιασμό.

Ας ξεκινήσουμε:

Τα Θεωρήματα ισομορφισμών

Πρώτο Θεώρημα ισομορφισμών.
Έστω $f : G \longrightarrow M$ ομομορφισμός ομάδων. Τότε υπάρχει ένας ισομορφισμός $\bar{f} = G/Kerf \longrightarrow Im f$.

Δεύτερο Θεώρημα ισομορφισμών.
Έστω G ομάδα και $A, B \leq G$. Υποθέτουμε ότι $B \lhd \langle A, B \rangle =$ AB. Τότε ισχύει $A \cap B \lhd A$ και $A/(A \cap B) \sim AB/B$.

Απόδειξη. Πρώτα απ' όλα $\langle A, B \rangle =$ AB (γιατί;)

Τί σημαίνει η υποομάδα η παραγομένη από τις A και B; Κάθε στοιχείο της $\langle A, B \rangle$ είναι της μορφής $h = a_1 b_1 a_2 b_2 \cdots a_n b_n$ με $a_i \in A$ και $b_i \in B$. Αλλά η B έχει υποτεθεί κανονική υποομάδα της $\langle A, B \rangle$ συνεπώς στην ανωτέρω γραφή του h "τμήματα" της μορφής $a_i bia_{i+1} = a_i a_{i+1} a_{i+1}^{-1} bia_{i+1}$ μπορούν να "αντικατασταθούν" από το $\bar{a_i}\bar{b_i}$, όπου $\bar{a_i} = a_i a_{i+1} \in A$ και $\bar{b_i} = a_{i+1}^{-1} bia_{i+1}$, οπότε τελικά $h = a \cdot b$ με $a \in A$, $b \in B$.

Τώρα ορίζουμε την εξής απεικόνιση $f : A \longrightarrow AB/B$ με $f(a) = aB$.

Δείξτε ότι η f είναι καλά ωρισμένη, ομομορφισμός ομάδων, επί και $Kerf = A \cap B$, οπότε από το πρώτο θεώρημα ισομορφισμών έπεται ότι $A/(A \cap B) \sim AB/B$.

□

Πριν προχωρήσουμε ας θυμηθούμε ορισμένα απλά αποτελέσματα.

Έστω $f : X \longrightarrow Y$ μια απεικόνιση συνόλων. Τότε για κάθε $A \subseteq X$ ορίζεται το σύνολο εικόνα $f(A) = \{ f(a) \mid a \in A \} \subseteq Y$.

Επίσης, για κάθε $B \subseteq Y$ ορίζεται η (πλήρης) αντίστροφη εικόνα $f^{-1}(B) = \{ a \in A \mid f(a) \in B \} \subseteq X$ (Προσοχή!! Εδώ το f^{-1} **δεν** συμβολίζει την αντίστροφη απεικόνιση της f, δεδομένου ότι η f ενδέχεται να μην αντιστρέφεται).

Προφανώς ισχύουν οι εξής σχέσεις: Για κάθε $B \subseteq Y$ ισχύει ότι $f(f^{-1}(B)) = B$ (γιατί;;)

Για κάθε $A \subseteq X$ ισχύει ότι $f^{-1}(f(A)) \supseteq A$ (γιατί;;)

Προσοχή!! Ενώ στην πρώτη περίπτωση έχουμε πάντα ισότητα, στην δεύτερη περίπτωση ενδέχεται να έχουμε γνήσιο εγκλεισμό. Μπορείτε να δώσετε ένα παράδειγμα όπου έχουμε γνήσιο εγκλεισμό;;

Ας δούμε τώρα τα προηγούμενα στην περίπτωση ομομορφισμών ομάδων.

Έστω $f : G \longrightarrow M$ ένας ομομορφισμός ομάδων. Τότε για κάθε $A \leq G$ ορίζεται ομάδα εικόνα $f(A) = \{ f(a) \mid a \in A \} \leq M$.

Επίσης, για κάθε $B \leq M$ ορίζεται η (πλήρης) αντίστροφη εικόνα $f^{-1}(B) = \{ a \in A \mid f(a) \in B \} \leq G$.

Εδώ, όπως προηγουμένως, έχουμε $f(f^{-1}(B)) = B$ και $f^{-1}(f(A)) \geq A$.

Στην δεύτερη σχέση μπορούμε να "μετρήσουμε την διαφορά" μεταξύ $f^{-1}(f(A))$ και A.

Συγκεκριμένα ισχύει:

$f^{-1}(f(A)) = Kerf \cdot A$. Να το αποδείξετε !!!!!

Πόρισμα. $(*)$ Αν η υποομάδα A περιέχει τον $Kerf$, τότε $f^{-1}(f(A)) = A$.

Αν ο ομομορφισμός f είναι μονομορφισμός, τότε $f^{-1}(f(A)) = A$ για κάθε υποομάδα A της G.

Θα δείξουμε ένα γενικό Θεώρημα: (*Θεώρημα της αντιστοιχίας*)

Θεώρημα 0.0.1. *Έστω $f : G \longrightarrow M$ ένας επιμορφισμός ομάδων. Έστω $\mathcal{T}$ το σύνολο όλων των υποομάδων της G, οι οποίες περιέχουν τον πυρήνα $Kerf$ και $\mathcal{S}$ το σύνολο των υποομάδων της M. Τότε υπάρχει μια απεικόνιση $\varrho : \mathcal{T} \longrightarrow \mathcal{S}$, η οποία είναι 1-1 και επί.*

Επιπλέον, για $H \in \mathcal{T}$, η H είναι κανονική στην G, αν και μόνο αν η $\varrho(H)$ είναι κανονική στην M. Στην περίπτωση αυτή ισχύει $G/H \sim M/\varrho(H)$.

Απόδειξη. Ορίζουμε την απεικόνιση $\varrho : \mathcal{T} \longrightarrow \mathcal{S}$ ως εξής:

$\varrho(A) = f(A)$, προφανώς η ϱ είναι καλά ορισμένη, 1-1 και επί (γιατί;;).

Όλα έχουν προηγηθεί. Να γράφετε κομψά την απόδειξη.

(Σημείωση: Μέχρι εδώ δεν χρησιμοποιήσαμε ότι η f είναι επί).

Έστω τώρα H μια κανονική υποομάδα της G. Θα δείξουμε ότι η $f(H)$ είναι κανονική υποομάδα της M.

Έστω $b \in f(H)$ και $r \in M$. Τότε υπάρχουν $a \in H$ και $g \in G$, ούτως ώστε $b = f(a)$ και $r = f(g)$ (εδώ χρησιμοποιούμε ότι η f είναι επί).

Οπότε, $rbr^{-1} = f(g)f(a)f(g^{-1}) = f(gag^{-1})$, αλλά η H έχει υποτεθεί κανονική υποομάδα της G, συνεπώς $rbr^{-1} \in f(H)$ και επομένως η $f(H)$ είναι κανονική υποομάδα της M.

Αντίστροφα, έστω K κανονική υποομάδα της M, τότε η υποομάδα $H = f^{-1}(K)$ έχει την ιδιότητα $f(H) = K = \varrho(H)$ και είναι η μοναδική με αυτή την ιδιότητα (γιατί;)

Πράγματι, η $H = f^{-1}(K) \in \mathcal{T}$ και αν υπήρχε μια άλλη $L \in \mathcal{T}$ με $f(L) = K$, τότε αφ' ενός $f^{-1}(f(L)) = f^{-1}(K) = H$, αφ' ετέρου $f^{-1}(f(L)) = KerfL = L$ αφού $Kerf \leq L$ (διαφορετικά, δεν ξεχνάμε ότι η απεικόνιση ϱ είναι 1-1 και επί).

Επίσης, η $H = f^{-1}(K)$ είναι κανονική στην G (μπορούμε να κάνουμε τον έλεγχο κανονικότητας).

Αλλά μπορούμε να δούμε ότι αν πάρουμε την σύνθεση απεικονίσεων $f : G \longrightarrow M$ και $\varphi : M \longrightarrow M/K$, τότε $Ker(\varphi \circ f) = H$ καθ' ότι $(\varphi \circ f)(H) = \varphi(f(H)) = \varphi(K) = K$. Συνεπώς, από το πρώτο θεώρημα τψν ισομορφισμών έχουμε $G/H = G/Ker(\varphi \circ f) \sim M/K$ ...και τέλος.

□

Τρίτο Θεώρημα ισομορφισμών. Έστω G ομάδα και K κανονική υποομάδα της G. Για κάθε $M \leq G/K$ υπάρχει $H \leq G$ με $K \leq H \leq G$, ούτως ώστε $M = H/K$. Αν επιπλέον η M είναι κανονική στην G/K, τότε η H είναι κανονική στην G και ισχύει $G/H \sim (G/K)/(H/K)$.

Απόδειξη. Είναι απλή εφαρμογή των προηγουμένων.

Εδώ έχουμε για τον φυσικό επιμορφισμό $f : G \longrightarrow G/K$ να πληρούνται όλες οι υποθέσεις του προηγουμένου θεωρήματος. Επομένως $Kerf = K$ και για κάθε $H \leq G$ με $K \leq H$ έχουμε ότι η $H/K = f(H) \leq G/K$ και αν H κανονική στην G, τότε H/K είναι κανονική στην G/K και $G/H \sim (G/K)/(H/K)$.

□

Μια άσκηση.

Έστω A, B πεπερασμένες υποομάδες της G. Δείξτε ότι $\mid A \cdot B \mid = \frac{|A| \cdot |B|}{|A \cap B|}$.

Μερικά σχόλια. Το σύνολο **δεν** είναι κατ' ανάγκη υποομάδα.

Αν όμως μια από τις δύο υποομάδες είναι κανονική στην G τότε το σύνολο $A \cdot B$ είναι υποομάδα και τότε μπορούμε να εφαρμόσουμε το δεύτερο θεώρημα των ισομορφισμών και να απαντήσουμε (παν)εύκολα στο προηγούμενο πρόβλημα. Πράγματι, έχουμε

$A/(A \cap B) \sim AB/B$, οπότε το αποτέλεσμα είναι εμφανές.

Να δώσετε μια απάντηση στο ανωτέρω ερώτημα όταν καμία από τις υποομάδες δεν είναι κανονική υποομάδα.

0.0.1 Η παράγωγος υποομάδα

Έστω G μια ομάδα, η οποία δεν είναι αβελιανή. Γεννάται το ερώτημα: Πώς μπορούμε να να αποφανθούμε "πόσο απέχει" από του να είναι αβελιανή;

Η φράση "πόσο απέχει" δεν είναι μαθηματική και μόνο διαισθητικά μπορούμε να την δεχθούμε,

Θα προσπαθήσουμε να της προσδώσουμε περιεχόμενο.

Έστω G μια ομάδα και $g, r \in G$. Πέρνουμε τα γινόμενα gr και rg. Γενικά $gr \neq rg$.

Παρατηρούμε ότι $gr(rg)^{-1} = grg^{-1}r^{-1}$. Επομένως ισχύει ότι $gr \neq rg$, αν και μόνο αν $grg^{-1}r^{-1} \neq 1$. Συνεπώς το στοιχείο $[a, b] = grg^{-1}r^{-1}$ "μετρά" κατά πόσον τα στοιχεία a, b απέχουν από το να μετατίθενται. Μάλιστα δε θα ονομάζεται στο εξής ως ο **μεταθέτης** των a, b.

Προφανείς ιδιότητες ενός μεταθέτη είναι: $([a, b])^{-1} = [b, a]$ και για κάθε ενδομορφισμό $\vartheta : G \longrightarrow G$ ισχύει ότι $\vartheta([a, b]) = [\vartheta(a), \vartheta(b)]$.

Προσοχή! Το γινόμενο δύο μεταθετών δεν είναι, κατ' ανάγκη μεταθέτης. Μπορείτε να δώσετε ένα παράδειγμα; (τώρα ίσως είναι δύσκολο αργότερα θα δούμε τέτοια παραδείγματα).

Επειδή το γινόμενο όλων των μεταθετών μιας ομάδας G δεν αποτελεί (κατ' ανάγκη) υποομάδα, λαμβάνουμε την υποομάδα $G' = \langle [g, r] \mid g, r \in G \rangle$, την παραγωμένη από όλους τους μεταθέτες της G. Η G' θα ονομάζεται **παράγωγος** υποομάδα της G, ή ομάδα μεταθετών της G (συνήθως θα την συμβολίζουμε και με $[G, G]$, ή $\gamma_2(G)$).

Γενικά, αν A, B είναι δύο (μη κενά) υποσύνολα μιας ομάδας G, τότε ορίζεται η ομάδα $[A, B] = \langle [a, b] \mid a \in A, b \in B \rangle$.

Η παράγωγος υποομάδα μιας ομάδας είναι πολύ σημαντική στην μελέτη της ομάδας.

Θα αναφέρουμε μερικές ιδιότητες.

Πρόταση 0.0.2. *Έστω G μια ομάδα, για την παράγωγο υποομάδα της ισχύουν:*

i) Η G' είναι πλήρως αναλλοίωτη υποομάδα (συνεπώς και κανονική).

ii) Η ομάδα πηλίκων G/G' είναι αβελιανή.

iii) Αν $N \lhd G$ και G/N αβελιανή, τότε $G' \leq N$.

iv) Αν $G' \leq N$, τότε $N \lhd G$ και η G/N είναι αβελιανή.

Απόδειξη. *i)* Ο ισχυρισμός είναι προφανής από την επισήμανση ότι, για κάθε ενδομορφισμό $\vartheta : G \longrightarrow G$ ισχύει ότι $\vartheta([a, b]) = [\vartheta(a), \vartheta(b)]$.

ii) Έστω $gG', rG' \in G/G'$, τότε $(gG') \cdot (rG') = (gr)G'$ και $(rG') \cdot (gG') = (rg)rG'$, αλλά $(gr) \cdot (rg)^{-1} = [g, r] \in G'$. Συνεπώς $(gG') \cdot (rG') = (rG') \cdot (gG')$ (γιατί;; Πότε δύο σύμπλοκα είναι ίσα;)

iii) Υποθέτουμε ότι η ομάδα G/N είναι αβελιανή. Για $gN, rN \in G/N$ έχουμε $(gN) \cdot (rN) = (gr)N$ και $(rN) \cdot (gN) = (rg)N$. Συνεπώς από την υπόθεση $(gN) \cdot (rN) = (rN) \cdot (gN)$ έπεται ότι $(gr)(rg)^{-1} = [g, r] \in N$ και αυτό για κάθε $g, r \in G$ συνεπώς $G' \leq N$.

iv) Έστω $g \in G$ και $r \in N$, τότε $grg^{-1} = grg^{-1}rr^{-1} = [g, r]r$, αλλά έχει υποτεθεί ότι $G' \leq N$, οπότε από την τελευταία ισότητα έπεται ότι $grg^{-1} \in N$. Άρα $N \lhd G$.

Προφανώς, όπως στο *ii)*, η ομάδα πηλίκων G/N είναι αβελιανή.

□

Ερώτημα: Θα μπορούσαμε στο *iv)* να δούμε με άλλο τρόπο ότι η G/N είναι αβελιανή;

Από την πρόταση αυτή έπεται ότι η παράγωγος υποομάδα G' είναι η "μικρότερη" κανονική υποομάδα της G, ούτως ώστε το πηλίκο να είναι αβελιανή ομάδα. (Εξ ου και το σχόλιο στην αρχή ότι η παράγωγος υποομάδα μας "δείχνει κατά πόσο απέχει η ομάδα από του να είναι αβελιανή").

Η υπολογισμός της παραγώγου υποομάδας μιας (τυχαίας) ομάδας τις περισσότερες φορές δεν είναι εφικτός. Ας δούμε όμως μερικά παραδείγματα.

i) Έστω $G = S_n,\ n \geq 3$ η συμμετρική ομάδα σε n σύμβολα. Θεωρούμε γνωστό το εξής:

$(*)$ Η εναλλάσουσα υποομάδα A_n, δηλαδή η ομάδα των αρτίων μεταθέσεων Παράγεται από τους κύκλους $(a,\, b,\, c)$ μήκους τρία.

Τώρα, είναι εύκολο να ελέγξουμε ότι $(a,\, b,\, c) = (b,\, c)(a,\, b)(b,\, c)(a,\, b) = [(b,\, c),\, (a,\, c)] \in S'_n$. Συνεπώς $A_n \leq S'_n$.

Προφανώς ισχύει και ο αντίστροφος εγκλισμός $A_n \geq S'_n$ (γιατί;). Άρα $A_n = S'_n$.

ii) Έστω $G = D_n$
$langle\, \varphi,\, \beta \mid \beta\varphi\beta = \varphi^{n-1} \rangle$, όπου ως γνωστόν κάθε στοιχείο της είναι της μορφής $\varphi^i\beta^j$ με $i = 1,\, 2,\, \dots,\, n$ και $j = 1,\, 2$.

Παρατηρούμε ότι $D'_n \leq \langle \varphi \rangle$ (γιατί;)

Επίσης, για τυχαία στοιχεία $a,\, b \in D_n$ ο μεταθέτης $[a,\, b] = \cdots = \varphi^{2k} \in\leq \langle \varphi^2 \rangle$ (γιατί;). Συνεπώς $D'_n \leq \langle \varphi^2 \rangle$.

Μπορούμε να συμπληρώσουμε τα $\cdots$ και να απαντήσουμε στα (γιατί;)

Θα μπορούσαμε να προσεγγίσουμε το πρόβλημα χωρίς να μπούμε στον κόπο να κάνουμε πράξεις.

Η υποομάδα $\langle \varphi^2 \rangle$ είναι κανονική στην D_n (γιατί;).

Το πηλίκο $D_n/\langle \varphi^2 \rangle$ είναι αβελιανή ομάδα (γιατί;)

Άρα $D'_n \leq \langle \varphi^2 \rangle$.

Τώρα, $[\varphi,\, \beta] = \varphi^2 \in D'_n$ (γιατί;).

Άρα τελικά $D'_n = \langle \varphi^2 \rangle$.

Ας απαντήσουμε στο

$(*)$ Η εναλλάσουσα υποομάδα A_n, δηλαδή η ομάδα των αρτίων μεταθέσεων Παράγεται από τους κύκλους $(a,\, b,\, c)$ μήκους τρία. $(*)$

Προφανώς κάθε άρτια μετάθεση (το λέει και το όνομά της) είναι γινόμενο από μεταθέσεις της μορφής

$(a,\, b)(c,\, d)$.Διακρίνουμε δύο περιπτώσεις:

1. Οι αντιμεταθέσεις έχουν κοινό στοιχείο. Στην περίπτωση αυτή έχουμε $(a,\, b)(b,\, d) = (b,\, d,\, a)$

2. Οι αντιμεταθέσεις είναι ξένες μεταξύ τους. Στην περίπτωση αυτή έχουμε

$(a,\, b)(c,\, d) = (a,\, b)(a,\, c)(c,\, a)(c,\, d) = (a,\, c,\, b)(c,\, d,\, a)$

και τέλος.

Στην έννοια της παραγώγου μιας ομάδας θα επανέλθουμε αργότερα.

Εδώ απλώς παραθέτουμε μια άσκηση.

Έστω G μια ομάδα και $K \lhd G$. Δείξτε ότι $\gamma_2(G/K) = (\gamma_2(G)K)/K$.

0.0.2 Δράσεις Ομάδων

Η έννοια της δράσης ομάδων επί συνόλων (είτε αυτά διαθέτουν δομή, είτε όχι) είναι πρωταρχική υπό την εξής έννοια: Πριν ακόμη διαμορφωθεί και "συνειδητοποιηθεί" η έννοια της ομάδος, όπως την γνωρίζουμε σήμερα, η έννοια της δράσης ομάδων είχε χρησιμοποιηθεί "ασυνειδήτως".

Ας ξεκινήσουμε με το "κλασσικό" παράδειγμα. Έστω ένα (μη κενό) σύνολο και έστω S_X η ομάδα μεταθέσεων (συμμετριών) του. Δεν ξεχνούμε ότι ένα στοιχείο του συνόλου S_X είναι μια απεικόνιση $\pi : X \longrightarrow X$, η οποία είναι 1-1 και επί.

Έστω $\pi \in S_n$ μια μετάθεση και $x \in X$. Τότε (προφανώς) έχουμε την (μοναδική) εικόνα $\pi(x) \in X$. Όπως βλέπουμε στο διατεταγμένο ζεύγος (π, x) αντιστοιχεί το στοιχείο $\pi(x)$ (η εικόνα του x μέσω της π).

Ας δούμε ένα άλλο παράδειγμα. Έστω V ένας διανυσματκός χώρος επί ενός σώματος $\mathbb{F}$ και $\mathbb{F}^*$ η πολλαπλασιαστική του ομάδα. Έστω $\lambda \in \mathbb{F}^*$ και $v \in V$, τότε, ως γνωστόν, ορίζεται ένα (μοναδικό) $\lambda v \in V$ (ο αριθμητικός πολλαπλασιασμός στους διανυσματικούς χώρους). Όπως βλέπουμε στο διατεταγμένο ζεύγος (λ, v) αντιστοιχεί το στοιχείο λv.

Όπως βλέπουμε και στα δύο παραδείγματα έχουμε ακριβώς την "ίδια κατάσταση" . Δηλαδή έχουμε μια ομάδα και ένα σύνολο, στο πρώτο παράδειγμα την S_n και το σύνολο X, ενώ στο δεύτερο την $\mathbb{F}^*$, και το σύνολο V. Επομένως θα μπορούσαμε να γενικεύσουμε και να δώσουμε έναν (φαινομενικά) "αφηρημένο" ορισμό.

Ορισμός 0.0.3. *Έστω G μια ομάδα και X ένα (μη κενό) σύνολο. Μια απεικόνιση*
$f : (G \times X) \longrightarrow X$, η οποία πληροί τις ιδιότητες:
i) $f(1_G, x) = x$, για όλα τα $x \in X$.
ii) $f(g_2g_1, x) = f(g_2, f(g_1, x))$, για όλα τα $g_1, g_2 \in G$ και $x \in X$.
Θα ονομάζεται μια (αριστερή) δράση της ομάδας G επί του συνόλου X (συμβολικά $G \hookrightarrow X$).

Έχει επικρατήσει την εικόνα $f(g, x)$ να την συμβολίζουμε ως εξής:
$g \cdot x$ (ή και χωρίς $\cdot$). Οπότε, οι ανωτέρω ιδιότητες θα εκφράζονται:
$i)$ $1 \cdot x = x$ και $ii)$ $(g_2g_1) \cdot x = g_2 \cdot (g_1 \cdot x)$.

Σημείωση: Προφανώς(;;) στα δύο ανωτέρω παραδείγματα πληρούνται οι ιδιότητες της δράσης.

Στα επόμενα θα δούμε περισσότερα παραδείγματα δράσεων ομάδων επί συνόλων.

Πριν προχωρήσουμε, θα επισημάνουμε ότι ομοίως μπορούμε να ορίσουμε δράσεις από τα δεξιά ομάδων επί συνόλων. Συγκεκριμένα.

Ορισμός 0.0.4. *Έστω G μια ομάδα και X ένα (μη κενό) σύνολο. Μια απεικόνιση*
$\varphi : (X \times G) \longrightarrow X$, η οποία πληροί τις ιδιότητες:
i) $\varphi(x, 1_G) = x$, για όλα τα $x \in X$.
ii) $\varphi(x, g_1g_2) = \varphi(\varphi(x, g_1), g_2)$, για όλα τα $g_1, g_2 \in G$ και $x \in X$.
Θα ονομάζεται μια (δεξιά) δράση της ομάδας G επί του συνόλου X.

Προφανώς (;) όταν έχουμε μια αριστερή δράση της ομάδας G επί ενός συνόλου X, $f : G \times X \longrightarrow X$, τότε ορίζεται και μία δεξιά δράση της G επί του X ως εξής:
$\varphi : X \times G \longrightarrow X$ με $\varphi(x, g) = f(g^{-1}, x)$ (Να κάνετε τον έλεγχο ότι η φ είναι δράση, αν και μόνο αν η f είναι δράση). Επομένως δεν έχει (και πολλή) σημασία αν θεωρούμε δεξιές ή αριστερές δράσεις.

Εν προκειμένω θα ασχοληθούμε (μόνο) με αριστερές δράσεις χωρίς ιδιαίτερη μνεία.

Έστω $f : (G \times X) \longrightarrow X$ μια δράση της ομάδας G επί του συνόλου X, τότε για κάθε $H \leq G$ ορίζεται ο **περιορισμός** της δράσης $f : (H \times X) \longrightarrow X$.

Τροχιές δράσεων-σταθεροποιούσες στοιχείων.

Έστω $G \hookrightarrow X$ μια δράση της ομάδας G επί του συνόλου X.

Επιλέγουμε και σταθεροποιούμε ένα στοιχείο $x \in X$ και ορίζουμε το εξής σύνολο $Orb_G(x) = \{\, gx \mid g \in G \,\}$, το σύνολο $Orb_G(x)$ θα ονομάζεται **τροχιά** του στοιχείου x.

Ερώτημα. Πόσα στοιχεία έχει το σύνολο $Orb_G(x)$;;

Η τροχιά $Orb_G(x)$ (φαινομενικά) έχει τόσα στοιχεία όσα και η ομάδα G, είναι πράγματι έτσι;;

Ας το δούμε. Ενδέχεται να υπάρχουν δύο (διαφορετικά) $g_1, g_2 \in G$ με $g_1x = g_2x$. Τί σημαίνει αυτό; Σημαίνει ότι $(g_1^{-1}g_2)x = x$ δηλαδή υπάρχει (μη τετριμένο) στοιχείο της G, το οποίο *σταθεροποιεί* το στοιχείο x.

Έστω $Stab_G(x) = \{ g \in G \mid g \cdot x = x \}$.

Το σύνολο $Stab_G(x)$ προφανώς είναι υποομάδα της G (γιατί;) και ονομάζεται σταθεροποιούσα (ή ομάδα ισοτροπίας) του στοιχείου x.

Ας δούμε τώρα πόσα στοιχεία έχει η τροχιά $Orb_G(x)$ του στοιχείου x.

Ας κάνουμε"'ανάλυση" του προβλήματος.

Για κάθε $r \in Stab_G(x)$ έχουμε ότι $rx = x$, επομένως τα στοιχεία $rx = x \in Orb_G(x)$ θα "μετρήσουν" μόνο μια φορά στην καταμέτρηση των στοιχείων της τροχιάς $Orb_G(x)$. Από την άλλη πλευρά αν $r \in Stab_G(x)$, τότε $(gr)(x) = gx$, για κάθε $g \in G$, δηλαδή για όλα τα στοιχεία του συμπλόκου $g\,Srab_G(x)$ αντιστοιχεί ένα μόνο στοιχείο (το gx) από την τροχιά $Orb_G(x)$.

Αυτό μας οδηγεί στο να ορίσουμε μια απεικόνιση $f : T = \{ g\,Stab_G(x) \mid g \in G \} \longrightarrow Orb_G(c)$ ως εξής: $f(gH) = gx$. Η ανάλυση του προβλήματος, που προηγήθηκε, είναι ικανή για να αποδείξουμε ότι η απεικόνιση f είναι καλώς ορισμένη, 1-1 και επί.

Να γραφεί η απόδειξη με κάθε λεπτομέρια.

Πόσα στοιχεία έχει το σύνολο T των (διαφορετικών) αριστερών συμπλόκων; Φυσικά $[G : Stab_g(x)]$ (ο ορισμός του δείκτη υποομάδος σε ομάδα).

Επομένως αποδείξαμε το εξής βασικό θεώρημα.

Θεώρημα 0.0.5. *Έστω ότι η ομάδα G δρα επί του συνόλου X. Το πλήθος των στοιχείων της τροχιάς $Orb_G(x)$ ενός $x \in X$ ισούται με τον δείκτη της σταθεροποιούσας του x στην G.*

($\mid Orb_G(x) \mid = [G : Stab_G(x)]$).

Υποθέτουμε ότι η ομάδα G επί του συνόλου X. Θα δούμε μια βασική ιδιότητα, που έχουν οι τροχιές των στοιχείων του συνόλου X.

Στο σύνολο X ορίζουμε μια σχέση ως εξής: $x \sim y$, αν υπάρχει $g \in G$, ούτως ώστε $gx = y$. Δείξτε ότι η σχέση $\sim$ είναι σχέση ισοδυναμίας.

Ας ανακαλύψουμε την κλάση ισοδυναμίας ενός στοιχείου $x \in X$. Έστω $C_x = \{ y \in X \mid y \sim x \}$. Προφανώς (γιατί; δείξτε το!) $C(x) = Orb_G(x)$.

Συνεπώς αποδείξα(με)τε ότι οι τροχιές των στοιχείων του συνόλου X αποτελούν μια διαμέριση του X. Αυτό μας δίνει ότι:

Δύο τροχιές στοιχείων του X είτε συμπίπτουν, είτε είναι ξένες μεταξύ τους.

Τώρα ένας απλός συνδυασμός των ανωτέρω μας οδηγεί στο εξής σημαντικό θεώρημα.

Θεώρημα 0.0.6. *Έστω ότι η ομάδα $G \hookrightarrow X$, με X πεπερασμένο, τότε ισχύει $\mid X \mid = \sum_{i=1}^{m}[G : Stab_G(x_i)]$, όπου κάθε x_i ανήκει σε διαφορετικές τροχιές.*

Απόδειξη. Γιατί πρόκειται για απλό συνδυασμό των ανωτέρω;;;

□

Αυτό το θεώρημα θα το συναντήσουμε σε πλείστες όσες εφαρμογές.

Ας δούμε ένα παράδειγμα: Όλοι(;) γνωρίζουμε(;) ότι μια μετάθεση αναλύεται σε γινόμενο κύκλων ξένων μεταξύ τους. Μάλιστα γνωρίζουμε(;) και μια "συνταγή" για το πώς αυτό επιτυγχάνεται.

Ας το δούμε υπό το πρίσμα των δράσεων.

Έστω το σύνολο $X = \{ 1, 2, \dots, n \}$ και έστω $\pi \in S_n$. Έστω $G = \langle \pi \rangle$ η κυκλική (υπο)ομάδα η παραγομένη από την π, η G δρα στο σύνολο X (γιατί;). Επομένως, σύμφωνα με τα προηγούμενα, το X διαμερίζεται σε τροχιές (κλάσεις ισοδυναμίας). Αν λάβουμε ένα στοιχείο $a \in X$, τότε η τροχιά του είναι $Orb_G(a) = \{ \pi(a), \pi^2(a), \dots, \pi^k(a) = a \}$, όπου k είναι ο μικρότερος θετικός ακέραιος με την ιδιότητα αυτή. Στην τροχιά αυτή αντιστοιχεί ο κύκλος $(\pi(a), \pi^2(a), \dots, \pi^k(a) = a)$.

Τώρα είναι (παν)εύκολο να δούμε ότι η μετάθεση π είναι το γινόμενο των ξένων κύκλων (ξένων τροχιών), οι οποίοι προκύπτουν από την δράση της G επί του X.

Ως παιχνίδι: Μπορείτε να δείτε ότι το μήκος κάθε κύκλου είναι διαιρέτης της τάξης της π;

Μπορείτε να βρήτε, αν έχουμε έναν κύκλο (a) μήκους 1, ποία είναι $Stab_G(a)$;

Ας δούμε τώρα το θεώρημα του Lagrage υπό το πρίσμα των δράσεων.

<u>Θεώρημα του Lagrage</u> Έστω G μια πεπερασμένη ομάδα και $H \leq G$. Τότε η τάξη της υποομάδας διαιρεί την τάξη της ομάδας.

Ορίζουμε την προφανή δράση της H επί της G (η ομάδα G εδώ θεωρείται το σύνολο X), δηλαδή $H \times G \longrightarrow G$ με $(h, g) \longrightarrow hg \in G$ (λόγω των ιδιοτήτων της πράξης στην G, έχουμε πράγματι μια δράση). Τότε η τροχιά ενός $g \in G$ είναι το σύνολο $Orb_H(g) = \{ hg \mid h \in H \} = Hg$, δηλαδή ένα δεξιό σύμπλοκο της H στην G και συνεπώς (γιατί;). $\mid G \mid = \mid Hg \mid \cdot [G : H]$.

Πριν προχωρήσουμε θα δώσουμε δύο ορισμούς για την απόκτηση ''λεξιλογίου''.

$i)$ Μια δράση μιας ομάδας G επί ενός συνόλου X θα ονομάζεται **μεταβατική** αν έχει μια μόνο τροχιά.

Στην περίπτωση αυτή, αν η G είναι πεπερασμένη, τότε το σύνολο X είναι αναγκαστικά πεπερασμένο και ο πληθικός του αριθμός είναι διαιρέτης της τάξης της ομάδας. (γιατί;;)

$ii)$ Μια δράση μιας ομάδας G επί ενός συνόλου X θα ονομάζεται **ελεύθερη**, αν δεν σταθεροποιεί στοιχεία, δηλαδή $Stab_G(x) = 1$ για όλα τα $x \in X$.

Στην περίπτωση αυτή, αν το X είναι πεπερασμένο, τότε η G είναι αναγκαστικά πεπερασμένη και η τάξη της είναι διαιρέτης του πληθικού αριθμού του συνόλου X.

Στο πρώτο παράδειγμα δράσης ομάδας επί ενός συνόλου X, είχαμε δεί ότι η συμμετρική ομάδα S_X δρά επί του συνόλου X.

Θα δούμε τώρα πώς αυτό μπορεί να ''γενικευθεί'', υπό την ευρεία έννοια του όρου.

Έστω $G \hookrightarrow X$ μια δράση της G επί του συνόλου X.

Ορίζουμε την απεικόνιση $\vartheta : G \longrightarrow S_X$ ως εξής:

$\vartheta(g) = \varrho_g \in S_X$, όπου η $\varrho_g : X \longrightarrow X$ είναι η μετάθεση στοιχείων του X, η οποία ορίζεται ως εξής: $\varrho_g(x) = gx$, δεν ξεχνάμε ότι με gx συμβολίζουμε το αποτέλεσμα της δράσης του στοιχείου $g \in G$ επί του στοιχείου $x \in X$.

Έχουμε πολλά να ελέγξουμε.

1. Η ϱ_g είναι μετάθεση (καλά ορισμένη, 1-1 και επί).
2. Η ϑ είναι ομομορφισμός ομάδων (καλά ορισμένη και διατηρεί τις πράξεις).

Αυτά θα τα ελέγξετε εσείς!!

Επομένως, τι έχουμε επιτύχει;;

Για κάθε δράση μιας ομάδας G επί ενός συνόλου X ορίζεται/ επάγεται ένας ομομορφισμός ομάδων με πεδίο ορισμού την ομάδα G και πεδίο τιμών την συμμετρική ομάδα S_n.

Ο ανωτέρω επαγόμενος ομομορφισμός ονομάζεται **αναπαράσταση** της G, ως προς την δοθείσα δράση.

Τώρα στο πρώτο παράδειγμα δράσης, που είχαμε δεί, όπου η συμμετρική ομάδα ενός συνόλου X δρά επί του X, τι είχαμε; Η μετάθεση π δρά επί του στοιχείου $x \in X$ με αποτέλεσμα δράσης $\pi(x)$ (την εικόνα του x μέσω της π).

Τώρα, αν εφαρμόσουμε τα προηγούμενα, θα έχουμε τον επάγομενο ομομορφισμό $\vartheta : S_X \longrightarrow S_X$ με $\vartheta(\pi) = \varrho_\pi = \pi$, για κάθε $\pi \in S_X$, δηλαδή ο επαγόμενος ομομορφισμός ϑ είναι ο ταυτοτικός ομομορφισμός $\iota : S_X \longrightarrow S_X$.

Το ωραίο είναι ότι ισχύει και το αντίστροφο:

Πώς φανταζόμαστε το αντίστροφο;;

Έστω G μια ομάδα και X ένα σύνολο. Υποθέτουμε ότι έχουμε έναν ομομορφισμό ομάδων $\vartheta : G \longrightarrow S_X$.

Ορίζουμε μια δράση της ομάδας G επί του συνόλου X ως εξής:

$f : G \times X \longrightarrow X$ με $f(g, x) = \vartheta(g)(x)$, δεν ξεχνάμε ότι το $\vartheta(g)$ είναι μετάθεση!

Τώρα είναι εύκολο να δούμε ότι πράγματι η f είνα μια δράση της ομάδας G επί του συνόλου X.

Να το κάνετε!!

Ανακεφαλαιώνοντας έχουμε ότι: "Δράση ομάδας επί ενός συνόλου" και "Ομομορφισμός ομάδων από μια ομάδα σε μια ομάδα μεταθέσεων" είναι ισοδύναμες έννοιες.

Τώρα, αφού έχουμε έναν ομομορφισμό $\vartheta : G \longrightarrow S_X$ ομάδων, ενδιαφερόμαστε για τις ιδιότητές του.

Ας προσπαθήσουμε να υπολογίσουμε τον πυρήνα $Ker\,\vartheta$.

Έστω $g \in Ker\,\vartheta$, τι σημαίνει αυτό;

$\vartheta(g) = 1 \in S_X$ (η ταυτοτική μετάθεση). Αλλά πώς ορίζεται ο ϑ; Έχουμε $\vartheta(g) = \varrho_g$ με $\varrho_g(x) = g\,x$, για όλα τα $x \in X$. Συνεπώς πρέπει να έχουμε $g\,x = x$ για όλα τα $x \in X$. Πού καταλήξαμε; Στο ότι $g \in Stab_G(x)$, για όλα τα $x \in X$. Δηλαδή τελικά καταλήξαμε ότι $Ker\,\vartheta \subset \bigcap_{x\in X} Stab_G(x)$. Προφανώς ισχύει και το αντίστροφο (γιατί;).

Πρόταση 0.0.7. *Έστω ότι η ομάδα G δρα επί του συνόλου X με αντίστοιχη αναπαράταση $\vartheta : G \longrightarrow S_X$, τότε $Ker\,\vartheta = \bigcap_{x\in X} Stab_G(x)$.*

Απόδειξη. Η απόδειξη έχει προηγηθεί.

□

Στην περίπτωση, όπου $Ker\,\vartheta = 1$, τότε η ομάδα G εμφυτεύται στην ομάδα S_X και η αναπαράσταση θα ονομάζεται **πιστή**.

Στον αντίποδα, όταν έχουμε $Ker\,\vartheta = G$, τότε έχουμε την **τετριμμένη** δράση.

Ας δούμε ένα (πολύ σημαντικό) παράδειγμα πιστής αναπαράστασης.

Το Θεώρημα Cayley Κάθε ομάδα G μπορεί να εμφυτευθεί σε μια ομάδα μεταθέσεων.

Προφανώς (το έχουμε ήδη αναφέρει) η G δρά επί του εαυτού της μέσω της πράξης της $(g, x) \longrightarrow gx$, προσοχή στον διττό ρόλο της G, μια φορά ως ομάδα και μια φορά ως σύνολο $(X = G)$ επί του οποίου δρα η G.

Προφανώς (γιατί;) η δράση είναι πιστή (δεν ξεχνάμε ότι $gx = x$, αν και μόνο αν $g = 1$). Συνεπώς, η G εμφυτεύεται στην S_G!

Η σπουδαιότητα του αποτελέσματος αυτού έγκειται ότι η μελέτη, οποιασδήποτε ομάδας, ανάγεται στην μελέτη των ομάδων (και των υποομάδων τους) των ομάδων μεταθέσεων. Αλλά αυτό δεν έχει αντιμετωπισθεί (και ούτε θα αντιμετωπισθεί), οπότε η "αξία" του ανωτέρου θεωρήματος, μάλλον έχει φιλοσοφική διάσταση.

Αρκεί να αναλογισθούμε ότι μια ομάδα με n το πλήθος στοιχεία "χάνεται" όταν εμφυτευθεί σε μια ομάδα με $n!$ το πλήθος στοιχεία.

Άσχετο με την αξία (ή μη) του ανωτέρω θεωρήματος. Ας αναλογισθούμε ότι προχωρώντας μεθοδικά και νηφάλια φθάνουμε στο σημείο σημαντικά αποτελέσματα να απορρέουν ως παραδείγματα... Αυτή είναι η (ανεκτίμητη) αξία της μελέτης των Μαθηματικών.

Ας δούμε τώρα μια άσκηση.

Άσκηση. Έστω ότι η ομάδα $G \hookrightarrow, X$ και $g \in G$, $x \in X$. Να βρεθεί η σχέση μεταξύ $Stab_G(x)$ και $Stab_G(gx)$.

Έστω $r \in Stab_G(gx)$, τότε $r(gx) = (rg)x = gx$. Από την τελευταία ισότητα έχουμε ότι $g^{-1}(rg)x = x$, αυτό σημαίνει ότι $g^{-1}rg \in Stab_G(x)$, Από την τελευταία σχέση έπεται ότι (γιατί;) $r \in gStab_G(x)g^{-1}$. Άρα αποδείξαμε ότι $Stab_G(gx) \subseteq gStab_G(x)g^{-1}$.

Παρομοίως αποδεικνύεται (κάντε το!) ότι $Stab_G(gx) \supseteq gStab_G(x)g^{-1}$.

Τελικά, $Stab_G(gx) = gStab_G(x)g^{-1}$.

Αυτό είναι σημαντικό αποτέλεσμα και θα το συναντήσουμε κατωτέρω.

Για άλλη μια φορά βλέπουμε ότι σημαντικά αποτελέσμτα απορρέουν ως ασκήσεις.

Μια άλλη άσκηση.

Έστω V ένας διανυσματικός χώρος διάστασης n επί ενός σώματος $\mathbb{F}$. Έχουμε δει στην αρχή ότι η πολλαπλασιαστική ομάδα $G = \mathbb{F}^*$ του σώματος δρα επί του συνόλου $X = V$

(ο αριθμητικός πολλαπλασιασμός). Έστω $v \in V$, μπορούμε να πριγράψουμε την τροχιά του $Orb_G(v)$; Μπορούμε να περιγράψουμε την σταθεροποιούσα $Stab_G(v)$;

Απάντηση: Η τροχιά του v είναι μια ευθεία (ο φορέας του v) (γιατί;) (προσοχή! στην απάντηση!)

Η σταθεροποιούσα του v είναι ....

Μπορείτε να λεπτολογήσετε περισσότερο,όταν το σώμα $\mathbb{F}$ είναι πεπερασμένο;

Ας δούμε τώρα μερικά ακόμα σημαντικά παραδείγματα δράσεων.

1^0 Παράδειγμα: Έστω G ομάδα και $H \leq G$. Έστω $X = \{\, rH \mid r \in G \,\}$ το σύνολο των αριστερών συμπλόκων της H στην G.

Η G δρα φυσιολογικά επί του X ως εξής: $(g, rH) \longrightarrow (gr)H$. Ποία είναι η τροχιά ενός $rH \in X$;; Έχουμε ότι $Orb_G(rH) = \{\, (gr)H \mid g \in G \,\} = X$, δηλαδή η δράση είναι μεταβατική (γιατί;;). Ποία είναι η σταθεροποιούσα του στοιχείου $H \in X$;; Προφανώς $Stab_G(H) = H$ (γιατί;;). Συνεπώς, από το γενικό αποτέλεσμα, που έχουμε αποδείξει έχουμε ότι $\mid Orb_G(H) \mid = \mid X \mid = [G : Stab_G(H)]$.

Τι παριστούν οι δύο τελευταίες ισότητες;; Μα φυσικά το Θεώρημα του Lagrage.

Άρα έχουμε μια άλλη απόδειξη του Θεωρήματος Lagrage (παράβαλε με το θεώρημα Lagrage στην σελίδα 7).

Ποία είναι η σταθεροποιούσα ενός τυχαίου συμπλόκου rH;; Προφανώς $Stab_G(rH) = rHr^{-1}$ (γιατί;;) (ιδέ σελ. 8).

Τώρα, η δράση αυτή επάγει έναν ομομορφισμό $\vartheta : G \longrightarrow S_{[G:H]}$. Ποίος είναι ο $Ker\,\vartheta$;;; Προφανώς $Ker\,\vartheta = \bigcap_{x\in X} Stab_G(x) = \bigcap_{rH\in X} Stab_G(rH) = \bigcap_{rH\in X} rHr^{-1}$. Τι απορρέει από την τελευταία ισότητα;;

Μα, προφανώς $Ker\,\vartheta = H_G$. Όπου H_G είναι η core της υποομάδας H. (βλέπε "Δεύτερο μάθημα" σελ. 6).

Τώρα μια ...σειρά ασκήσεων.

i) Έστω G άπειρη ομάδα. Δείξτε ότι δεν περιέχει απλή υποομάδα πεπερασμένου δείκτη.

ii) Έστω G άπειρη ομάδα και H υποομάδα της πεπρασμένου δείκτη. Δείξτε ότι υπάρχει K κανονική υποομάδα της G, η οποία είναι πεπερασμένου δείκτη, μάλιστα δε $K \leq H$.

iii) Έστω G μια άπειρη ομάδα πεπερασμένα γεννώμενη. Δείξτε ότι, για κάθε θετικό ακέραιο n, υπάρχουν πεπερασμένο το πλήθος υποομάδες της G με δείκτη n.

iv) Έστω G άπειρη ομάδα πεπερασμένα γεννώμενη και H υποομάδα της πεπρασμένου δείκτη. Δείξτε ότι υπάρχει K χαρακτηριστική υποομάδα της G, η οποία είναι πεπερασμένου δείκτη, μάλιστα δε $K \leq H$.

v) Έστω G άπειρη ομάδα πεπερασμένα γεννώμενη και H υποομάδα της πεπερασμένου δείκτη.

Αν $Aut(G)$, η ομάδα αυτομορφισμών της G, δείξτε ότι υπάρχει R κανονική υποομάδα της $Aut(G)$ πεπερασμένου δείκτη.

vi) Έστω G πεπερασμένη ομάδα και p ο μικρότερος πρώτος διαιρέτης της τάξης της ομάδας $\mid G \mid$. Αν $H \leq G$ με δείκτη $[G, : H] = p$, δείξτε ότι η H είναι κανονική υπομάδα.

Θα ασχοληθούμε με την άσκηση *iii*).

Αν η ομάδα μας δεν έχει υποομάδες δείκτου n, έχει καλώς (έχει μηδέν το πλήθος υποομάδες δείκτου n). Υποθέτουμε ότι έχουμε μια H υποομάδα δείκτου n. Από τα προηγούμενα έπεται ότι έχουμε έναν ομομορφισμό $\vartheta : G \longrightarrow S_n$.

Η ομάδα μας όμως είναι πεπερασμένα γεννώμενη ($G = \langle\, a_1, a_2, \ldots, a_k \,\rangle$), επομένως κάθε ϑ ομομορφισμός ομάδων με πεδίο ορισμού την G είναι πλήρως καθορισμένος από τις εικόνες των γεννητόρων $\vartheta(a_i)$ (γιατί;). Στην συγκεκριμένη περίπτωση το πεδίο τιμών είναι πεπερασμένη (είναι η S_n). Συνεπώς έχουμε πεπερασμένες το πλήθος επιλογές για τις τιμές των $\vartheta(a_i)$, δηλαδή πεπερασμένο το πλήθος ομομορφισμοί μπορούν να ορισθούν από την

G στην S_n. Επομένως υπάρχουν πεπερασμένο το πλήθος κανονικές υποομάδες της G, οι οποίες θα μπορούσαν να είναι πυρήνες ομομορφισμών. Έστω K μια τέτοια υποομάδα, τότε, επειδή το πηλίκο G/K είναι πεπερασμένο, υπάρχουν πεπερασμένο το πλήθος υποομάδες Η με $K \leq H \leq G$. Σε αυτές τις υποομάδες συγκαταλέγονται και οι υποομάδες δείκτου n. Άρα έχουμε πεπερασμένο το πλήθος υποομάδων δείκτου n.

Επικαλούμενοι τώρα την άσκηση αυτή, μπορείτε να αποδείξετε την $iv)$;;;

Παρατηρήσεις.

Η άσκηση αυτή είναι "υπαρξιακή", δηλαδή αποδεικνύει ότι υπάρχουν πεπερασμένο το πλήθος υποομάδες συγκεκριμένου δείκτη, αλλά δεν μας πληροφορεί για το πόσες είναι. Παρ' όλα ταύτα είναι ένα σημαντικό θεώρημα και στην πορεία θα δούμε πλήστες όσες εφαρμογές.

Η υπόθεση η ομάδα μας να είναι πεπερασμένα γεννώμενη είναι απαραίτητη. Μπορείτε να δώσετε ένα παράδειγμα απείρως γεννώμενης ομάδας με άπειρο το πλήθος υποομάδες συγκεκριμένου δείκτου n;;

Θα ασχοληθούμε με την άσκηση $vi)$.

Τί έχουμε αποδείξει προηγουμένως; Η ομάδα G δρα επί του συνόλου των αριστερών συμπλόκων της H στην G και η δράση αυτή επάγει έναν ομομορφισμό $\vartheta : G \longrightarrow S_{[G:H]}$ με $Ker\,\vartheta = \bigcap_{x\in X} Stab_G(x) = \bigcap_{rH\in X} Stab_G(rH) = \bigcap_{rH\in X} rHr^{-1} = H_G$. Όπου H_G είναι η core της υποομάδας H.

Τώρα, από την υπόθεση έχουμε ότι $[G : H] = p$, συνεπώς $\mid S_{[G:H]} \mid = p!$ με την ομάδα πηλίκων G/H_G να εμφυτεύται στην $S_{[G:H]}$ (γιατί;). Από εδώ και πέρα έχουμε απλή αριθμητική. $\mid G/H_G \mid = [G : H_G] = [G : H]\cdot[H : H_G] = p\cdot[H : H_G]$ (γιατί;). Από την τελευταία ισότητα έχουμε ότι ο δείκτης $[H : H_G]$ διαιρεί το $(p-1)!$, συνεπώς έχουμε την "κατάσταση" ο δείκτης $[H : H_G]$ να διαιρεί την τάξη της ομάδας G και ταυτόχρονα να διαιρεί το $(p-1)!$, εξ' ου το συμπέρασμα ότι $[H : H_G] = 1$ (γιατί;). Άρα $H = H_G$, το οποίο αποδεικνύει τον ισχυρισμό μας.

2^0 Παράδειγμα: Έστω μια ομάδα G. Ορίζουμε μια δράση της G στον εαυτό της μέσω της συζυγίας. Δηλαδή $(g, x) \longrightarrow gxg^{-1}$.

Προφανώς;; πράγματι πρόκειται για δράση της G στον εαυτό της.

Έστω $x \in G$. Ποία είναι η τροχιά του; $Orb_G(x) = \{\, gxg^{-1} \mid g \in G \,\}$, η **κλάση συζυγίας** του x. Ποία είναι η σταθεροποιούσα του x; $Stab_g(x) = \{\, g \in G : gxg^{-1}x \,\} = \{\, g \in G : gx = xg \,\} = C_G(x)$, κεντροποιούσα του στοιχείου x.

Ποίος είναι πυρήνας της αντίστοιχης αναπαράστασης $\tau : G \longrightarrow S_G$; $Ker\,\tau = \bigcap_{x\in G} C_G(x) = \zeta(G)$, το κέντρο της G.

Εδώ θα κάνουμε μια παρατήρηση. το πηλίκο $G/\zeta G$ είναι ισόμορφο με μια υποομάδα της S_G, δηλαδή είναι μια υποομάδα μεταθέσεων των στοιχείων της G. Εδώ όμως ισχύει κάτι πολύ πιο ισχυρό δεν είναι απλώς μια ομάδα μεταθέσεων, τα στοιχεία της είναι οι εσωτερικοί αυτομορφισμοί, το έχουμε ήδη δει.

Με αφορμή αυτή την παρατήρηση, βλέπουμε ότι έχουμε δράσεις ομάδων επί συνόλων, οι οποίες "διατηρούν" την δομή (αν υπάρχει) του συνόλου επί του οποίου δρουν.

Επ' αυτού θα επανέλθουμε αργότερα.

Ας επανέλθουμε στο παράδειγμά μας.

Τι είχαμε δει γενικά. Κάθε κλάση συζυγίας έχει $\mid Orb_G(x) \mid = [G : C_G(x)]$ το πλήθος στοιχεία. Συνεπώς έχουμε την σχέση $G = \bigcup_{x\in G} Orb_G(x)$ και στην περίπτωση των πεπερασμένων ομάδων έχουμε ότι $\mid G \mid = \sum_{i=1}^{k}[G : C_G(x_i)]$, όπου $k = k(G)$ είναι το πλήθος των (διαφορετικών) κλάσεων συζυγίας της G.

Ο αριθμός $k = k(G)$ (class number ή class equation) είναι κάτι που χαρακτηρίζει την ομάδα. Για παράδειγμα. Σε μια πεπερασμένη ομάδα $k(G) = \mid G \mid$, αν και μόνο αν η G είναι αβελιανή.

Ας δούμε μερικές εφαρμογές υπό μορφήν ασκήσεων.

$i)$ Δείξτε ότι κάθε ομάδα G με τάξη δύναμη ένος πρώτου αριθμού ($|G| = p^n$) έχει μη τεριμμένο κέντρο.

Έχουμε δεί ότι για την ομάδα G ισχύει ότι: $|G| = \sum_{i=1}^{k}[G : C_G(x_i)]$. Δηλαδή ο πληθικός αριθμός κάθε κλάσης συζυγίας διαιρεί την τάξη της ομάδας, εν προκειμένω μια δύναμη του p. Επίσης τα στοιχεία (και μόνο αυτά) του κέντρου της ομάδας είναι κλάσεις συζυγίας, οι οποίες είναι μονοσύνολα (γιατί;). Συνεπώς, αν υποθέσουμε ότι το κέντρο της ομάδος είναι τετριμένο, θα έχουμε $p^n = 1 + p^{m_1} + p^{m_2} + \cdots + p^{m_k}$ με κάθε $m_i \neq 0$, άτοπο.

$ii)$ Δείξτε ότι κάθε ομάδα τάξης p^2, p-πρώτος, είναι αβελιανή.

$iii)$ Δείξτε ότι η τάξη κάθε πεπερασμένης απλής μη αβελιανής ομάδας διαιρείται από τουλάχιστον δύο διαφορετικούς πρώτους αριθμούς.

$iv)$ Έστω G μη αβελιανή ομάδα με τάξη $|G| = p^3$, p-πρώτος. Δείξτε ότι $|\zeta(G)| = p$ και $k(G) = p^2 + p - 1$.

$v)$ Δείξτε με την χρήση της class equation το θεώρημα του Cauchy. Δηλαδή, σε μια πεπερασμένη ομάδα για κάθε πρώτο διαιρέτη της τάξης της, υπάρχει στοιχείο με αυτή την τάξη.

Είναι;; γνωστό ότι το θεώρημα ισχύει για πεπερασμένες αβελιανές ομάδες;

$vi)$ Έστω G πεπερασμένη ομάδα. Δείξτε ότι για κάθε $x \in G$ ισχύει ότι $|C_G(x)| \geq |G/G'|$, όπου G' είναι παράγωγος υποομάδα της G.

$vii)$ Έστω G πεπερασμένη μη αβελιανή ομάδα. Δείξτε ότι $k(G) > |\zeta(G)| + 1$.