Ομάδες: Πρώτο μάθημα

Στο μάθημα αυτό (όπως και στο επόμενο) θα προσπαθήσουμε να κάνουμε μια σύντομη εισαγωγή σε βασικές έννοιες της Θεωρίας Ομάδων, οι οποίες είναι απαραίτητες για να συνεχίσουμε. Η εισαγωγή αυτή θα γίνει ως εξής: Θα λαμβάνουμε μια άσκηση από το αρχείο των ασκήσεων *Μια πρώτη συλλογή ασκήσεων στην Θεωρία Ομάδων* και στην προσπάθεια να απαντήσουμε, θα αναφέρουμε και θα σχολιάζουμε όλες τις απαραίτητες έννοιες.

Ας ξεκινήσουμε:

i) **Έστω G ομάδα και $g \in G$ με τάξη του g ίση με n. Δείξτε ότι η τάξη του στοιχείου g^k είναι ίση με $\frac{n}{(n,k)}$.**

ii) **Δείξτε ότι για κάθε $a \in \mathbb{Z}$ ο μικρότερος θετικός ακέραιος k με την ιδιότητα $(k \cdot a) mod\, n \equiv o \, mod\, n$ είναι ο $\frac{n}{(n,a)}$.** (Είναι η άσκηση 17)

Πρώτα απ' όλα τι καλούμε τάξη στοιχείου μιας ομάδας;

.....

Εν προκειμένω έχουμε ένα στοιχείο $g \in G$ πεπερασμένης τάξης, έστω $o(g) = n$. Είναι προφανές ότι κάθε δύναμη g^k έχει πεπερασμένη τάξη; Επίσης, αν ισχύει ότι $g^m = 1$, $m \in \mathbb{Z}$, τί σχέση έχει η $o(g) = n$ με το m;

Προφανώς η τάξη $o(g) = n$ διαιρεί το m (γιατί;)

Θα εφαρμόσουμε την ταυτότητα της διαίρεσης...μπορούμε να επιχειρηματολογήσουμε μέχρι τέλους;

Ας έλθουμε τώρα στο ερώτημά μας; Έστω ότι $o(g^k) = x$ (δεν την γνωρίζουμε), Τότε, $(g^k)^x = g^{k \cdot x} = 1$, επομένως $n \mid k \cdot x$ (1).

Επίσης, έχουμε ότι $(g^k)^{\frac{n}{(n,k)}} = g^{k\frac{n}{(n,k)}} = g^{(\frac{k}{(n,k)})n} = 1$. Συνεπώς $x \mid \frac{n}{(n,k)}$.

Πώς συνεχίζουμε;

Από την σχέση (1) έχουμε ότι $\frac{n}{(n,k)} \mid \frac{k}{(n,k)} \cdot x$. Δηλαδή $\frac{n}{(n,k)} \mid x$ και τέλος (γιατί;)

Για το δεύτερο ερώτημα. Πώς μπορούμε να εφαρμόσουμε το πρώτο ερώτημα;

...Ποία είναι η ομάδα G, ποίο είναι το στοιχείο g, ποίος είναι ο "εκθέτης" k;

Προφανώς $G = (\mathbb{Z}_n, +)$, $g = 1$, $k = a$ και η ζητουμένη τάξη είναι ο εδώ ζητούμενος $k = \frac{n}{(n,a)}$.

(Δεν μπερδεύουμε τον ρόλο των δύο k στα δύο ερωτήματα).

Μπορείτε τώρα να απαντήσετε μόνοι σας στις ασκήσεις 18 και 19;

Ας δούμε τώρα μια άλλη άσκηση:

Δίνεται η ομάδα $G = \{ A \mid A \in \mathbb{R}^{\nu \times \nu}$, με $\mid A \mid \neq 0 \}$ και $S = \{ A \in G,$ με $\mid A \mid = 1 \}$. Δείξτε ότι:

i) **Η S είναι κανονική υποομάδα της G.**

ii) **Το πηλίκο G/S είναι αβελιανή ομάδα.**

iii) **Να βρεθούν τα στοιχεία πεπερασμένης τάξης της ομάδας G/S.** (Είναι η άσκηση 16)

Πρώτα απ' όλα όταν έχουμε μια ομάδα G και μια υποομάδα της H. Πότε η H ονομάζεται κανονική υποομάδα;

.....

Ορισμός: Η Η ονομάζεται **κανονική** (συμβολισμός $H \lhd G$), αν για κάθε $g \in G$ ισχύει ότι $gHg^{-1} := \{ ghg^{-1} \mid h \in H \} = H$.

Ισοδύναμοι ορισμοί:

$i)$ Για κάθε $g \in G$, ισχύει ότι: $gH = Hg$.

$ii)$ Για κάθε $g \in G$ και κάθε $h \in H$ ισχύει ότι $ghg^{-1} \in H$.

$iii)$ Για κάθε $r \in G$ υπάρχει $g \in G$, ούτως ώστε $rH = Hg$.

$iv)$ Η υποομάδα H είναι κανονική στην G.

Οι Προτάσεις $i)$ έως $vi)$ είναι ισοδύναμες.

Προφανώς (;) σε μια αβελιανή ομάδα κάθε υποομάδα της είναι κανονική.

Το αντίστροφο ισχύει;

.....

Τώρα, αν έχουμε μια H κανονική υποομάδα μιας ομάδας G, το σύνολο $G/H = \{ gH \mid g \in G \}$ όλων των αριστερών συμπλόκων της H στην G με πράξη $(aH) \cdot (bH) := (ab)H$ αποτελεί ομάδα, η οποία ονομάζεται **ομάδα πηλίκων**. Ποίο είναι το ουδέτερο στοιχείο της ομάδας αυτής, ποίο είναι το αντίστροφο στοιχείο $(aH)^{-1}$ του aH;;

Ισχύει και το αντίστροφο: Έστω $H \leq G$. Υποθέτουμε ότι το σύνολο $G/H = \{ gH \mid g \in G \}$ όλων των αριστερών συμπλόκων της H στην G με πράξη $(aH) \cdot (bH) := \{ (ah_1)(bh_2) \mid h_1, h_2 \in H \}$ αποτελεί ομάδα, τότε η H είναι κανονική υποομάδα της G. Μπορείτε να το αποδείξετε;

.....

Τώρα ερχόμεθα στην άσκησή μας.

Το πρώτο ερώτημα είναι προφανές. Υπάρχει κάποιος που δεν μπορεί να το δει;

Για το δεύτερο ερώτημα. Θέλουμε να αποδείξουμε ότι η ομάδα πηλίκων G/S είναι αβελιανή. Έστω $aS, bS \in G/S$ (Προσοχή! Για να μην μπερδευόμαστε, εδώ τα πεζά γράμματα a, b παριστάνουν πίνακες). Τί θέλουμε να αποδείξουμε; $(aS)(bS) = (bS)(aS)$. Δηλαδή θέλουμε να αποδείξουμε ότι $(ab)S = (ba)S$. Δηλαδή θέλουμε να αποδείξουμε ότι .... $(ab)^{-1}(ba) \in S$, το οποίο προφανώς (;) ισχύει.

Για το τρίτο ερώτημα. Έστω $aS \in G/S$ ένα στοιχείο πεπερασμένης τάξης. Άρα υπάρχει $n \in \mathbb{N}$, ώστε $(aS)^n = a^n S = S$. Άρα τι ιδιότητες έχει ο πίνακας a ;;;;

Η επομένη άσκηση

Έστω $A, B \leq G$ **και** $x, y \in G$. **Δείξτε ότι το σύνολο** $xA \cap yB$ **είναι είτε το κενό σύνολο, είτε ένα αριστερό σύμπλοκο της** $A \cap B$ **στη** G. (Είναι η άσκηση 25)

Προηγουμένως ασχοληθήκαμε με σύμπλοκα. Μπορούμε να τα χειριστούμε με ευχέρεια;

Πριν προχωρήσουμε στην "τυπική" απόδειξη. Ας δούμε το πρόβλημα γεωμετρικά. Είμαστε στον τρισδιάστατο χώρο $V = \mathbb{R}^3$. Δεν έχουμε την δυνατότητα για παρουσίαση με σχήματα, αλλά μπορούμε να τα φανταστούμε. Ποίοι είναι οι υπόχωροί του (εκτός τον τετριμμένο και ολόκληρο τον χώρο); Προφανώς (;) οι ευθείες, οι οποίες διέρχονται από την αρχή των αξόνων και τα επίπεδα, τα οποία διέρχονται από την αρχή των αξόνων. Έστω τώρα ένας υπόχωρος A (μια ευθεία, ή ένα επίπεδο) και v ένα στοιχείο του χώρου V. Ποίο είναι το σύμπλοκο $v + A$;;

Επομένως αν έχουμε δύο υποχώρους A, B και δύο διανύσματα $v, w \in V$ ποία είναι η τομή $(v + A) \cap (w + B)$ τους;

Τί μας έλεγε ο "δάσκαλος": *"Αν έχουμε δύο επίπεδα στον χώρο, έστω* E_1, E_2, *τα οποία τέμνονται κατά μια ευθεία, έστω* ϵ *και πάρουμε ένα έπίπεδο* Π_1 *παράλληλο προς το επίπεδο* E_1 *και ένα επίπεδο* Π_2 *παράλληλο προς το επίπεδο* E_2, **τότε** *τα επίπεδα* Π_1 Π_2 *τέμνονται κατά μία ευθεία, έστω* e, *ή οποία είναι παράλληλη προ την ευθεία* ϵ.

Αυτό το **τότε** μπορούσε να το αποδείξει;

Επομένως, αν τα επίπεδα E_1, E_2 διέρχονται από την αρχή των αξόνων, δηλαδή είναι υπόχωροι, τότε η τομή τους ϵ είναι μια ευθεία που διέρχεται από την αρχή των αξόνων, δηλαδή ένας υπόχωρος. Τί είναι τα επίπεδα $\Pi_1,\ \Pi_2$; Σύμπλοκα ως προς τα επίπεδα E_1, E_2

αντίστοιχα. Τί είναι η τομή τους, δηλαδή η ευθεία e; Είναι σύμπλοκο ως προς την ευθεία (υπόχωρο) ϵ, δηλαδή παράλληλη προς αυτήν.

Τώρα θα προσπαθήσουμε να απαντήσουμε στην άσκησή μας.

Έχουμε τις υποομάδες A, B (όπου προηγουμένως είχαμε υποχώρους, ευθείες, επίπεδα, εδώ έχουμε υποομάδες), Έστω τα σύμπλοκα xA και yB. Άν η τομή $xA \cap yB$ είναι το κενό σύνολο έχει καλώς. Υποθέτουμε ότι η τομή $xA \cap yB$ δεν είναι το κενό σύνολο. Έστω $g \in xA \cap yB$, τότε υπάρχουν $a \in A$ και $b \in B$, ώστε $g = xa = yb$. Ας δούμε τι απορρέει από τις τελευταίες ισότητες. Έχουμε ότι $x = ga^{-1}$ και $y = gb^{-1}$, οπότε $xA = (ga^{-1})A = gA$ (γιατί;). Όμοια $yB = (gb^{-1})B = gB$. Επομένως $xA \cap yB = gA \cap gB = \cdots = g(A \cap B)$ και τέλος (;). Όχι, να συμπληρώσετε τις $\cdots$.

Η επομένη άσκηση

Έστω $\varphi : G_1 \longrightarrow G_2$ ένας ομομορφισμός ομάδων και $a \in G_1$ πεπερασμένης τάξης. Δείξτε ότι η τάξη της εικόνας $\varphi(a)$ διαιρεί την τάξη του στοιχείου a.

Έστω A μια πεπερασμένη υποομάδα της G_1, δείξτε ότι η τάξη της εικόνας $\varphi(A)$ διαιρεί την τάξη της A. (Είναι η άσκηση 9)

Πριν ξεκινήσουμε την λύση, ας δούμε ορισμένα θέματα με ομομορφισμούς ομάδων.

Έστω $f : G \longrightarrow M$ ένας ομορφισμός ομάδων (όλοι γνωρίζουμε; τον ορισμό του ομομορφισμού). Δύο υποομάδες είναι σημαντικές και "συνδέονται" με τον ομομορφισμό f.

1) Ο πυρήνας της f. $Kerf = \{ r \in G, \text{με } f(r) = 1_M \}$.

Δείξτε ότι ο πυρήνας $Kerf$ είναι κανονική υποομάδα του πεδίου ορισμού G.

2) Η εικόνα της f. $Imf = \{ f(g) \mid g \in G \} = f(G)$.

Δείξτε ότι Imf είναι υποομάδα του πεδίου τιμών M.

Προφανώς η f είναι 1-1 (μονομορφισμός) αν και μόνο αν ο πύρήνας $Kerf$ είναι η τετριμμένη υποομάδα της f (γιατί είναι προφανές;)

Προφανώς η f είναι επί (επιμορφισμός) αν και μόνο αν $Imf = M$

Πώς "συνδέονται" ο πυρήνας και η εικόνα ;;

Το 1^o Θεώρημα των ισομορφισμών.

Έστω $f : G \longrightarrow M$ ένας ομορφισμός ομάδων. Τότε υπάρχει ένας (άλλος) ομομορφισμός ομάδων $\bar{f} : G/Kerf \longrightarrow Imf$, οποίος είναι ισομορφισμός. Δηλαδή οι ομάδες $G/Kerf$ και Imf είναι ισόμορφες ($G/Kerf \approx Imf$).

Απόδειξη: Θέλουμε, με την βοήθεια της f, να ορίσουμε μια άλλη απεικόνιση $\bar{f}$.

Θα κάνουμε την εξής παρατήρηση. Έστω $r \in Kerf$, τότε για κάθε $g \in G$ ισχύει ότι: $f(gr) = f(g)$ (γιατί;). Επίσης, $(gr)Kerf = gKerf$ (γιατί;).

Αυτό μας οδηγεί να ορίσουμε την $\bar{f} : G/Kerf \longrightarrow Imf$. Ορίζουμε $\bar{f}(gKerf) = f(g)$.

Πρέπει να αποδείξουμε τα εξής:

- Η $\bar{f}$ είναι πράγματι απεικόνιση (καλώς ορισμένη).
- Η $\bar{f}$ είναι ομομορφισμός.
- Η $\bar{f}$ είναι 1-1 (μονομορφισμός).
- Η $\bar{f}$ είναι επί (επιμορφισμός).

Θα αποδείξουμε μόνο το καλώς ορισμένη. Τα υπόλοιπα είστε θέση να τα αποδείξετε μόνοι σας, (αρκεί να θέλετε να προσπαθήσετε).

Προφανώς για κάθε $gKerf \in G/Kerf$ υπάρχει το $f(g) \in Imf$, ώστε $\bar{f}(gKerf) = f(g)$ (κάθε πρότυπο έχει εικόνα).

Το ερώτημα είναι, αν είναι μοναδική. Έστω $g_1Kerf = g_2Kerf$ (δύο ίσα πρότυπα). Τί σημαίνει αυτό; $g_1^{-1}g_2 \in Kerf$. Συνεπώς $f(g_1^{-1}g_2) = 1$, δηλαδή $f(g_1^{-1}) \cdot f(g_2) = 1$ εξ ου $f(g_1) = f(g_2)$, αλλά $f(g_1) = \bar{f}(g_1Kerf)$ και $f(g_2) = \bar{f}(g_2Kerf)$.

Άρα αποδείξαμε την ζητουμένη συνεπαγωγή $g_1Kerf = g_2Kerf \implies \bar{f}(g_1Kerf) = \bar{f}(g_2Kerf)$.

Συνεχίστε μόνοι σας για να ολοκληρώσετε την απόδειξη του θεωρήματος.

Ας επανέλθουμε στην άσκησή μας.

Το πρώτο ερώτημα είναι προφανές και στηρίζεται στον ορισμό της τάξης στοιχείου. Απαντήστε....

Το δεύτερο ερώτημα "φαντάζει" πιο δύσκολο, αλλά είναι και αυτό πανεύκολο.

Έχουμε την απεικόνιση $\varphi : G_1 \longrightarrow G_2$. Λαμβάνουμε τον περιορισμό της στην υποομάδα A $\varphi_{|A} : A \longrightarrow G_2$. Τί έχουμε από το 1^o Θεώρημα των ισομορφισμών; $A/Ker\varphi_{|A} \approx \varphi_{|A}(A) = \varphi(A)$. Τέλος, γιατί; Μα αφού $| A/Ker\varphi_{|A} | = | A | / | Ker\varphi_{|A} |$ (γιατί;).

Με αφορμή το τελευταίο (γιατί;) ας θυμίσουμε το Θεώρημα του Lagrage.

Έστω G μια ομάδα και $H \leq G$. Τότε το πλήθος των (διαφορετικών) αριστερών συμπλόκων της H στην G ισούται με το πλήθος των (διαφορετικών) δεξιών συμπλόκων της H στην G. (γιατί;) αυτό το γιατί; θα το πάρετε ως άσκηση. Το πλήθος αυτών συμπλόκων (αριστερών, ή δεξιών δεν έχει πλέον σημασία) το ονομάζουμε **δείκτη** της υποομάδας H στην ομάδα G και τον συμβολίζουμε $[G : H]$.

Τα αριστερά σύμπλοκα αποτελούν μια διαμέριση της ομάδας G, συνεπώς

$G = \bigcup gH$

(διακεκριμένη ένωση), αυτό είναι το Θεώρημα του Lagrage και δεν πρέπει να μας εντυπωσιάζει ούτε να μας ...τρομάζει. Απλώς να το έχουμε καταλάβει, διότι διέπει όλα τα Μαθηματικά και όχι μόνο την Θεωρία Ομάδων.

Τώρα στην περίπτωση των πεπερασμένων ομάδων έχουμε, από την προηγουμένη σχέση, ότι $| G | = | g_1H | + | g_2H | + \cdots + | g_kH |$ (η ανωτέρω ένωση είναι διακεκριμένη), όπου $k = [G : K]$. Αλλά $| g_iH | = | H |$, για κάθε i (γιατί;). Επομένως έχουμε

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

Αυτή είναι η εκδοχή του Θεωρήματος του Lagrage στην περίπτωση των πεπερασμένων ομάδων.

Η επομένη άσκηση

α) Δείξτε ότι η $f : \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z}$, $f(x, y) = x - 2y$ είναι ομομορφισμός προσθετικών ομάδων και να βρεθεί ο πυρήνας $Kerf$ και η εικόνα $f(\mathbb{Z} \times \mathbb{Z}) = Imf$.

β) Έστω G μια ομάδα και $g \in G$. Δείξτε ότι η $f : \mathbb{Z} \longrightarrow G$ με $f(k) = g^{2k}$ είναι ομομορφισμός. Ποιά είναι η Imf αν η τάξη του g είναι 6 ή 7; (Είναι η άσκηση 21).

Πρώτα απ' όλα συνειδητοποιούμε ότι η πράξη στο καρτεσιανό γινόμενο $\mathbb{Z} \times \mathbb{Z}$ είναι η πρόσθεση κατά συντεταγμένες $(a_1, b_1) + (a_2, b_2) = (a_1 + a_2, b_1 + b_2)$. Τώρα είναι εύκολο να δούμε ότι πράγματι η f είναι ομομορφισμός ομάδων (κάντε το!).

Ως προς τον πυρήνα: Έστω $(x, y) \in Kerf$, τότε $f(x, y) = x - 2y = 0$. Τί σημαίνει αυτό; ότι $x = 2y$. Συνεπώς $Kerf \subseteq \{ (2y, y) \mid y \in \mathbb{Z} \}$, αντίστροφος εγκλεισμός $\supseteq$ είναι προφανής.

Για την εικόνα $f(\mathbb{Z} \times \mathbb{Z}) = Imf$, έχουμε ότι $Imf = \{ f(x, y) = x - 2y \mid x, y \in \mathbb{Z} \}$. Αναρωτιέμαστε αν η f είναι επί. Τί σημαίνει αυτό; ο τυχαίος ακέραιος αριθμός z μπορεί να γραφεί στην μορφή $z = x - 2y$ με $x, y \in \mathbb{Z}$; Διακρίνουμε περιπτώσεις.

Αν ο z είναι άρτιος $z = 2k$, τότε εύκολα βλέπουμε ότι $z = 4k - 2k$. Συνεπώς υπάρχει το ζεύγος $(4k, k)$ με $f(4k, k) = 4k - 2k = z$. Δηλαδή ο άρτιος αριθμός z έχει πρότυπο. Τώρα αν ο z είναι περιττός $\zeta = 2\kappa + 1$, εσείς να ελέγξετε αν (πράγματι) υπάρχει ζεύγος $9x, y)$, ώστε $f(x, y) = x - 2y = z$.... Άρα η f είναι επί.

Για το δεύτερο ερώτημα: Προφανώς η f είναι ομομορφισμός (ελέγξετέ το!).

Για την τάξη της Imf. Έχουμε $Imf = \{ g^{2k} \mid k \in \mathbb{Z} \}$ (περίπτωση, όπου $o(g) = 6$). Έχουμε $Imf = \{ g^2, g^{2\cdot 2}, g^{2\cdot 3} = 1, ... \}$, άρα $| Imf | = 3$ (γιατί;)

Προσπαθήστε για $o(g) = 7$.