Χριστινα Τσατσου

Ταξινομηση Πεπρασμενων Ομαδων Ταξης μικροτερης η ισης του 16

Προπτυχιακη Εργασια

Πανεπιστήμιο Αιγαίου, Τμήμα Μαθηματικών
Σάμος 1 Μαρτίου 2013

Εισηγητης: Ευστράτιος Πρασίδης

Επιτροπη

Βασίλειος Μεταφτσής

Νικόλαος Παπαλεξίου

Στους γονείς μου!

Περιεχόμενα

Εισαγωγή

Κάθε περιοχή στα μαθηματικά έχει σαν σκοπό την ταξινόμηση των αντικειμένων που μελετά. Ένα από τα πιο βασικά προβλήματα στην Θεωρία Ομάδων είναι η ταξινόμηση των ομάδων, μετά από ισομορφισμούς. Αυτό είναι θεμελιώδες στην Θεωρία Ομάδων γιατί δείχνει ποιές είναι ακριβώς οι ομάδες που εμφανίζονται σε κάθε περίπτωση και τι ιδιότητες μπορεί να έχουν. Επίσης, περιορίζει την μελέτη των ιδιοτήτων των ομάδων στις συγκεκριμένες ομάδες που έχουμε ήδη χαρακτηρίσει. Είναι ευρέως γνωστό ότι η ταξινόμηση των πεπερασμένα παραγόμενων ομάδων δεν είναι εφικτή. Δηλαδή είναι ένα άλυτο πρόβλημα στα μαθηματικά. Αυτό προτείνει ότι ίσως μπορούμε να ταξινομήσουμε άλλες κατηγορίες ομάδων. Μ΄ αυτήν την λογική, πρώτα θεωρούμε τις πεπερασμένες ομάδες. Και φυσικά φαίνεται εφικτό να απαριθμήσουμε τις ομάδες συγκεκριμένης τάξης.

Παρατηρούμε ότι για ορισμένους αριθμούς (τους πρώτους) υπάρχει μόνο μια ομάδα αυτής της τάξης. Αυτό προτείνει και το αντίθετο. Δηλαδή, όσο πιο πολλούς πρώτους διαιρέτες έχει ο αριθμός τόσο πιο δύσκολο θα είναι να προσδιορίσουμε όλες τις ομάδες αυτής της τάξης. Το βασικό εργαλεία που χρησιμοποιούνται είναι η Ταξινόμηση των Πεπερασμένων Αβελιανών Ομάδων και, για τις μη-αβελιανές ομάδες, τα θεωρήματα του Sylow. Αυτά τα θεωρήματα μας επιτρέπουν να καθορίσουμε ότι οι ομάδες που μελετάμε έχουν υποοομάδες κάποιας συγκεκριμένης τάξης (δυνάμεις πρώτων αριθμών) και καθορίζουν τις ιδιότητες αυτών των ομάδων. Η ταξινόμηση γίνεται με το να θεωρήσουμε διάφορες περιπτώσεις που καθορίζουν πως οι διάφορες υποομάδες βρίσκονται μέσα στην κυρίως ομάδα.

Η εργασία αυτή περιορίζεται στην ταξινόμηση των ομάδων τάξης μικρότερης ή ίσης του 16. Ο λόγος είναι είναι ότι ο 16 είναι ο πρώτος αριθμός όπου εμφανίζονται πολλές ομάδες σε σύγκριση με τους προηγούμενους. Φυσικά αυτό οφείλεται στο ότι ο 16 είναι μια δύναμη του 2. Παρατηρούμε ότι παρόμοια πολυπλοκότητα εμφανίζεται και στις ομάδες τάξης 8. Η επόμενη τάξη που έχει μεγαλύτερη πολυπλοκότητα είναι το 24. Η πιο πολύπλοκη δομή, για αριθμούς μικρότερους του 100, είναι οι ομάδες τάξης 72. Υπάρχουν 50 ομάδες αυτής της τάξης.

Χρίστινα Τσάτσου, Σάμος 2013.

Κεφάλαιο 1

Θεωρήματα Sylow

Σ' αυτό το κεφάλαιο θα αποδείξουμε τα Θεωρήματα Sylow, που κατά κάποιον τρόπο, είναι αντίστροφα του Θεωρήματος Lagrange που αποδεικνύει ότι η τάξη H μιας υποομάδας μιας πεπερασμένης ομάδας G, διαιρεί την τάξη της ομάδας. Πιο συγκεκριμένα:

Θεώρημα 1.0.1 (Θεώρημα Lagrange)**.** *Έστω G μια πεπερασμένη ομάδα και H μια υποομάδα της. Τότε $|H|/|G|$. Πιο συγκεκριμένα*

$$[G:1] = [G:H][H:1],$$

όπου $[G:H]$ είναι ο αριθμός των H-συμπλόκων (αριστερών ή δεξιών).

Η ερώτηση που απαντάται μερικώς από την Θεωρία του Sylow είναι πότε, εάν $k/|G|$, υπάρχει υποομάδα της G τάξης k.

1.1 Δράσεις Ομάδων σε Σύνολα

Η βασική αναφορά είναι [2] και [3]. Έστω G μια ομάδα, πεπερασμένη ή άπειρη.

Ορισμός 1.1.1. *Μια δράση της G σε ένα σύνολο S είναι μια συνάρτηση:*

$$G \times S \to S, \quad (g, s) \mapsto gs$$

έτσι ώστε:

(i) $1s = s$, *για κάθε* $s \in S$.

(ii) $(g_1 g_2)s = g_1(g_2 s)$.

Τότε λέμε ότι η G δρα στο S.

Παρατήρηση 1.1.2. *Έστω, για ένα σύνολο S,*

$$A(S) = \{\phi : S \to S : \ \phi \text{ αμφιμονοσήμαντη αντιστοιχία}\}$$

Τότε $A(S)$ είναι ομάδα με πράξη την σύνθεση συναρτήσεων, δηλαδή η ομάδα μεταθέσεων του S. Για παράδειγμα, αν $|S| = n$, τότε $A(S) \cong S_n$. Είναι προφανές ότι τον ορισμό της δράσης μιας ομάδας G στο S είναι ένας ομομορφισμός ομάδων $\alpha : G \to A(S)$. Αντίστροφα, ένας ομομορφισμός α, όπως παραπάνω, ορίζει μια δράση της ομάδας G στο S.

- *Εάν η α δίνεται, τότε η δράση ορίζεται ως:* $gs = \alpha(g)(s)$.
- *Όταν η δράση δίνεται, τότε ο α ορίζεται ως:* $\alpha(g)(s) = gs$.

Παραδείγματα.

(i) Η δράση της συμμετρικής ομάδας S_n στο σύνολο $I_n = \{1, 2, \ldots n\}$ ως $\sigma i = \sigma(i)$.

(ii) Έστω G μια ομάδα και H μια υποομάδα της. Μια δράση της H στην G δίνεται:
$$H \times G \to G, \ \ (h, g) \mapsto hg.$$
Αυτή η δράση ονομάζεται (αριστερή) *μετάφραση*. Ειδικά, η G δρα στην G με αριστερές μεταφράσεις.

(iii) Εάν K είναι μια άλλη υποομάδα της G και S το σύνολο των αριστερών σύμπλοκων της K στην G, τότε H δρα στο S με μετάφραση:
$$H \times S \to S, \ \ (h, gK) \mapsto hgK.$$

(iv) Έστω G μια ομάδα και H μια υποομάδα της. Μια δράση της H στην G δίνεται:
$$H \times G \to G, \ \ (h, x) \mapsto hxh^{-1}$$
Αυτή η δράση του h καλείται δράση με συζυγίες και το στοιχείο hxh^{-1} καλείται ο συζυγής του x.

(v) Αν K είναι κάποια υποομάδα της G και $h \in H$, τότε hKh^{-1} είναι και αυτή υποομάδα της G ισόμορφη με την K. Έστω S το σύνολο όλων των υποομάδων της G. Τότε η H δρα στο S με συζυγίες:
$$H \times S \to S, \ \ (h, K) \mapsto hKh^{-1}.$$

(vi) Σε κάποιες περιπτώσεις, όταν το S έχει πιο πλούσια δομή (όπως όταν είναι ομάδα ή διανυσματικός χώρος) τότε μπορεί να απαιτήσουμε ότι η δράση της G διατηρεί αυτήν την δομή. Δηλαδή απαιτούμε ότι η δράση είναι μέσω ισομορφισμών ομάδων ή ισομορφισμούς διανυσματικών χώρων.

Το επόμενο αποτέλεσμα είναι βασικό για την ορολογία των δράσεων ομάδων. Η απόδειξή του είναι άμεση.

Θεώρημα 1.1.3. *Έστω G ομάδα που δρα σε ένα σύνολο X.*

(i) *η σχέση $x \sim x' \Leftrightarrow gx = x'$ για κάποιο στοιχείο $g \in G$, είναι μια σχέση ισοδυναμίας και*

(ii) *για κάθε $x \in X$, το σύνολο $G_x = \{g \in G : gx = x\}$ είναι υποομάδα της G.*

Παρατήρηση 1.1.4. *Οι κλάσεις ισοδυναμίας της σχέσης ισοδυναμίας του θεωρήματος λέγονται τροχιές του G στο S. Η τροχιά του $x \in S$ γράφεται ως $\bar{x}$. Γράφουμε $S/G = \{\bar{x} : \ x \in S\}$ για το σύνολο των τροχιών της S. Η υποομάδα G_x της ομάδας G λέγεται ομάδα ευστάθειας (stabilizer) του στοιχείου x.*

Παραδείγματα

(i) Αν μια ομάδα G δρα με συζυγίες στον εαυτό της, τότε η τροχιά του $x \in G$,

$$\bar{x} = \{gxg^{-1} | \ g \in G\}$$

και λέγεται *κλάση συζυγίας* του x.

(ii) Αν μια υποομάδα H δρα με συζυγίες στην G, η ομάδα ευστάθειας είναι

$$H_x = \{h \in H | hxh^{-1} = x\} = \{h \in H | hx = xh\}$$

ονομάζεται *κεντροποιητής* του x στην H και συμβολίζεται με $C_H(x)$. Άν $H = G$, $C_G(x)$ τότε τον λέμε απλά κεντροποιητής του x.

(iii) Αν η H δρα με συζυγίες στο σύνολο S όλων των υποομάδων της G, τότε η ομάδα ευστάθειας της H της $K \in S$ είναι $\{h \in H | \ hKh^{-1} = K\}$, λέγεται *κανονικοποιητής* του K στην H και γράφεται ως $N_H(K)$. Έχουμε ότι $K \lhd N_G(K)$ και K είναι κανονική υποομάδα της G αν και μόνο αν $N_G(K) = G$.

Θεώρημα 1.1.5. *Έστω G μια ομάδα που δρα σε ένα μη κενό σύνολο X. Το πλήθος των στοιχείων της τροχιάς $\bar{x}$ του στοιχείου $x \in X$ ισούται με το δείκτη $[G : G_x]$ της ομάδας ευστάθειας G_x του x στην ομάδα G.*

Απόδειξη. Έστω $\mathcal{L} = \{gG_x / g \in G\}$ το σύνολο όλων των συμπλόκων της G_x στην G. Ορίζουμε

$$\Phi : \mathcal{L} \to \bar{x}, \ \Phi(gG_x) = gx \ \text{ για κάθε } gG_x \in \mathcal{L}.$$

Πρώτα θα πρέπει να αποδείξουμε ότι η Φ είναι καλά ορισμένη: Πράγματι,

$$g_1 G_x = g_2 G_x \Rightarrow {g_1}^{-1} g_2 \in G_x \Rightarrow {g_1}^{-1} g_2 x = x \Rightarrow g_2 x = g_1 x.$$

Άρα αφού, $\Phi(g_1 G_x) = g_1 x$ και $\Phi(g_2 G_x) = g_2 x$ έχουμε ότι $\Phi(g_1 G_x) = \Phi(g_2 G_x)$. Επομένως η Φ είναι καλά ορισμένη. Απομένει να δείξουμε ότι είναι 1-1 και επί:

$$\Phi(g_1 G_x) = \Phi(g_2 G_x) \Rightarrow g_1 x = g_2 x \Rightarrow {g_2}^{-1} g_1 x = x \Rightarrow {g_2}^{-1} g_1 \in G_x \Rightarrow g_1 G_x = g_2 G_x.$$

Επομένως είναι 1-1. Έστω $x' \in \bar{x} \Rightarrow x' = gx$, τότε $\Phi(gG_x) = gx = x'$. Άρα είναι και επί. ☐

Παρατήρηση 1.1.6. *Έστω G ομάδα και K υποομάδα της.*

(i) *Έχουμε την δράση της G στον εαυτό της με συζυγίες και $x \in G$. Τότε $G_x = C_G(x)$. Οπότε ο αριθμός στοιχείων της τροχιάς του x, που είναι ο αριθμός των στοιχείων συζυγών με το x, είναι $[G : C_G(x)]$, το οποίο διαιρεί το $|G|$ από το Θεώρημα του Lagrange.*

(ii) *Αν $\bar{x}_1, \ldots, \bar{x}_n (x_i \in G)$ είναι οι κλάσεις συζυγίας της G, τότε*

$$|G| = \sum_{i=1}^{n} [G : C_G(x_i)].$$

(iii) *Με όμοιο τρόπο, μπορούμε να δείξουμε ότι το πλήθος των υποομάδων της G που είναι συζυγείς με το K είναι $[G : N_G(K)]$, και διαιρεί το $|G|$.*

Το επόμενο θεώρημα το έχουμε ήδη αναφέρει στην Παρατήρηση 1.1.2. Τώρα δίνουμε μια πιο αναλυτική απόδειξη της παρατήρησης.

Θεώρημα 1.1.7. *Έστω G ομάδα που δρα σε ένα σύνολο S, τότε αυτή η δράση επάγει έναν ομομορφισμό $G \to A(S)$ όπου $A(S)$ είναι η ομάδα όλων των μεταθέσεων του S.*

Απόδειξη. Έστω $g \in G$, ορίζουμε μια συνάρτηση

$$\tau_g : S \to S,\ x \mapsto gx.$$

Καθώς $x = g(g^{-1}x)$ για κάθε $x \in S$, τ_g είναι επί γιατί $\tau_g(g^{-1}x) = x$. Όμοια

$$gx = gy\ (x, y \in S) \Longrightarrow x = g^{-1}(gx) = g^{-1}(gy) = y,$$

άρα τ_g είναι $1-1$ και άρα αμφιμονοσήμαντη. Επομένως, εφόσον

$$\tau_{gg'} = \tau_g \tau_{g'} : S \to S, \text{ για όλα τα } g, g' \in G$$

η απεικόνιση $G \to A(S)$ με $g \mapsto \tau_g$ είναι ένας ομομορφισμός. □

Πόρισμα 1.1.8. *(Cayley) Αν G ομάδα, τότε υπάρχει μονομορφισμός $G \to A(G)$. Ως εκ τούτου κάθε ομάδα είναι ισόμορφη με μια υποομάδα μεταθέσεων. Στην ουσία κάθε πεπερασμένη ομάδα είναι ισόμορφη με μια υποομάδα της S_n, $n = |G|$.*

Απόδειξη. Έστω ότι η G δρα με αριστερή μετάφραση και σύμφωνα με το θεώρημα 1.1.7 υπάρχει ομοιομορφισμός $\tau : G \to A(G)$. Άν $\tau(g) = \tau_g = 1_G$, τότε $gx = \tau_g(x) = x$ για καθε $x \in G$. Δηλαδή, $ge = e$, που δίνει $g = e$ και άρα ο τ είναι μονομορφισμός γιατί έχει τετριμμένο πυρήνα. Για να αποδείξουμε την τελευταία πρόταση παρατηρούμε ότι αν $|G| = n$, τότε $A(G) \cong S_n$. □

Πόρισμα 1.1.9. *Έστω G ομάδα.*

(i) *Για κάθε $g \in G$, η συζυγία από το g επάγει αυτομορφισμό του G*

(ii) *υπάρχει ομοιομορφισμός $G \to AutG$ με πυρήνα το κέντρο της G.*

$$Z(G) = \{g \in G : gx = xg \text{ για όλα τα } x \in G\}$$

Απόδειξη. Είναι αποτέλεσμα της δράσης της G στον εαυτό της με συζυγίες. □

Παρατήρηση 1.1.10. (i) *Η συζυγία με g, γράφεται $\tau_g : G \to G$ και ονομάζεται εσωτερικός αυτομορφισμός της G.*

(ii) *Το κέντρο είναι κανονική υποομάδα της G, $Z(G) \lhd G$.*

(iii) *Η G είναι αβελιανή αν και μόνο αν $Z(G) = G$*

(iv) *Για το κέντρο και τους κεντροποιητές ισχύει:*

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

(v) *Ένα στοιχείο x είναι στο κέντρο αν και μόνο αν η κλάση συζυγίας του x είναι μόνο ένα στοιχείο, το ίδιο. Άρα:*

$$x \in Z(G) \Longleftrightarrow G = C_G(x) \Longleftrightarrow [G : C_G(x)] = 1.$$

(vi) *Η εξίσωση που προκύπτει από τις τροχιές της δράσης είναι:*

$$|G| = |Z(G)| + \sum_{i=1}^{m} [G : C_G(x_i)]$$

όπου $x_i \in G - Z(G)$ είναι αντιπρόσωποι των κλάσεων συζυγίας και $[G : C_G(x_i)] > 1$.

Πρόταση 1.1.11. *Έστω H υποομάδα της ομάδας G και η G δρα στο σύνολο S όλων των αριστερών συμπλόκων της H στην G με αριστερή μετάφραση. Τότε ο πυρήνας του παραγόμενου ομοιομορφισμού $G \to A(S)$ περιέχεται στην H.*

Απόδειξη. Ο ομοιομορφισμός $G \to A(S)$ δίνεται απο το $g \mapsto \tau_g$, όπου $\tau_g : S \to S$ και $\tau_g(xH) = gxH$. Αν το g ανήκει στον πυρήνα, τότε $\tau_g = 1_s$ και $gxH = xH$ για κάθε $x \in G$, δηλαδή για $x = e$, $geH = eH = H$, από το οποίο έχουμε ότι $g \in H$. □

Πόρισμα 1.1.12. *Αν H μια υποομάδα δείκτη n στην G και η μόνη κανονική υποομάδα της G που περιέχεται στην H είναι η τετριμμένη, τότε η G είναι ισόμορφη με μια υποομάδα της S_n.*

Απόδειξη. Σύμφωνα με την Πρόταση 1.1.11 ο πυρήνας της $G \to A(S)$ είναι κανονική υποομάδα της G που περιέχεται στην H και θα είναι η τετριμμένη από την υπόθεση. Ως εκ τούτου, $G \to A(S)$ είναι ένας μονομορφισμός. Η G είναι ισόμορφη με μια υποομάδα ομάδας όλων των μεταθέσεων n αριστερών συμπλόκων της H και η τελευταία ομάδα είναι ισόμορφη με την S_n. □

Πόρισμα 1.1.13. *Αν η H είναι υποομάδα πεπερασμένης ομάδας G δείκτη p, όπου p ο μικρότερος πρώτος αριθμός που διαιρεί την τάξη της G, τότε η H είναι κανονική υποομάδα της G.*

Απόδειξη. Έστω το S να είναι το σύνολο όλων των αριστερών συμπλοκών της H στην G. Τότε $A(S) \cong S_p$ και $[G : H] = p$. Αν K είναι ο πυρήνας του ομοιομορφισμού $G \to A(S)$ της Πρότασης 1.1.11 τότε η K είναι κανονική υποομάδα της G και περιέχεται στην H. Επιπλέον G/K είναι ισόμορφη με υποομάδα της S_p, από το πρώτο Θεώρημα Ισομορφισμού. Έτσι η $|G/K|$ διαιρεί το $|S_p| = p!$. Αλλά κάθε διαιρέτης του $|G/K| = [G : K]$ πρέπει να διαιρεί το $|G| = |K|[G : K]$. Επειδή κανένας αριθμός μικρότερος του p (εκτός του 1) μπορεί να διαιρέσει την $|G|$, θα πρέπει να έχουμε $|G/K| = p$ ή 1. Επίσης $|G/K| = [G : K] = [G : H][H : K] = p[H : K] \geq p$. Έτσι $|G/K| = p$ και $[H : K] = 1,$ άρα $H = K$ και η H είναι κανονική υποομάδα στην G. □

Το επόμενο θεώρημα είναι ένα βασικό εργαλείο στους υπολογισμούς. Έστω $N \triangleleft G$. Ορίζουμε

$$S = \{H : N \leq H \leq G\}, \text{ και } T = \{K : K < G/N\}.$$

Θεώρημα 1.1.14 (Θεώρημα Αντιστοιχιών). *Με τον παραπάνω συμβολισμό, η αντιστοιχία:*

$$f : S \to T, \ H \mapsto H/N$$

είναι μια $1-1$ *και επί αντιστοιχία. Επιπλέον, οι κανονικές υποομάδες στο* S *αντιστοιχούν σε κανονικές υποομάδες στην* G/N*, και αν μια υποομάδα της* G/N *περιέχεται σε μια υποομάδα της* G/N*, τότε οι υποομάδες που αντιστοιχούν στο* S *έχουν την ίδια σχέση.*

Απόδειξη. Παρατηρούμε ότι η N είναι κανονική στη H γιατί είναι κανονική στην G.

f είναι 1-1. Έστω $f(H) = f(H')$. Τότε $H/N = H'/N$. Έστω $h \in H$. Τότε υπάρχει $h' \in H'$ έτσι ώστε $hN = h'N$. Άρα υπάρχει $x \in N$, $h = h'x$. Αλλά $N \leq H'$. Συνεπώς $x \in H'$ και συνεπώς $h \in H'$ που δίνει ότι $H < H'$. Όμοια μπορούμε να δείξουμε ότι $H' < H$ και έτσι $H = H'$.

f είναι επί. Έστω $K < G/N$. Έστω

$$H = \{x \in G : xN \in K\}.$$

Θα δείξουμε ότι $H \leq G$. Εάν $x, y \in H$, τότε $xN, yN \in K$ και $(xy^{-1})N \in K$. Συνεπώς $xy^{-1} \in H$, ολοκληρώνοντας την απόδειξη.

Τα άλλα αποτελέσματα είναι άμεσα από τον ορισμό της f. ☐

1.2 Θεωρήματα Sylow

Σ' αυτήν την ενότητα θα αποδείξουμε τα Θεωρήματα Sylow.

Λήμμα 1.2.1. *Αν μια ομάδα* H *τάξης* p^n *(*p *πρώτος) δρα σε πεπερασμένο σύνολο* S *και αν* $S_0 = \{x \in S |\ hx = x$ *για κάθε* $h \in H\}$ *τότε* $|S| \equiv |S_0| (mod p)$.

Απόδειξη. Μια τροχιά $\bar{x}$ περιέχει ακριβώς ένα στοιχείο εάν και μόνο εάν $x \in S_0$. Έτσι το S μπορεί να γραφεί σαν $S = S_0 \cup \bar{x}_1 \cup \bar{x}_2 \cup \cdots \cup \bar{x}_n$, με $|\bar{x}_i| > 1$ για κάθε i. Ως εκ τούτου $|S| = |S_0| + |\bar{x}_1| + |\bar{x}_2| + \cdots + |\bar{x}_n|$. Επίσης $p / |\bar{x}_i|$ για κάθε i αφού $|\bar{x}_i| > 1$ και $|\bar{x}_i| = [H : H_{x_i}]$ διαιρεί $|H| = p^n$. Έτσι $|S| = |S_0| (mod p)$. ☐

Θεώρημα 1.2.2. *(Cauchy) Έστω* G *πεπερασμένη ομάδα της οποίας η τάξη διαιρείται από έναν πρώτο αριθμό* p*, τότε η* G *περιέχει ένα στοιχείο τάξης* p.

Απόδειξη. Έστω S το σύνολο των p-άδων των στοιχείων της ομάδας που το γινόμενό τους είναι η ταυτότητα:

$$S = \{(a_1, a_2, \ldots, a_p),\ a_i \in G, a_1 a_2 \ldots a_p = e\}.$$

Καθώς το a_p προσδιορίζεται μοναδικά σαν $(a_1 a_2 \ldots a_{p-1})^{-1}$ έπεται ότι $|S| = n^{p-1}$ όπου $|G| = n$. Επίσης p/n και $|S| \equiv 0 (mod p)$. Έστω η ομάδα $\mathbb{Z}_p$ δρα στο S με κυκλική μετάθεση, δηλαδή

$$k(a_1, a_2, \ldots, a_p) = (a_{k+1}, a_{k+2}, \ldots, a_p, a_1, \ldots, a_k)$$

για κάθε $k \in \mathbb{Z}_p$. Αληθεύει ότι $(a_{k+1}, a_{k+2}, \ldots, a_k) \in S$ (χρησιμοποιώντας την ιδιότητα ότι σε μια ομάδα αν $ab = e$ έχουμε ότι $ba = (a^{-1}a)(ba) = a^{-1}(ab)a = e$). Ακόμη, για $0, k, k' \in Z_p$ και $x \in S$, $0x = x$ και $(k + k')x = k(k'x)$. Επομένως η δράση της ομάδας $\mathbb{Z}_p$ στο σύνολο S είναι καλά ορισμένη. Τώρα $(a_1, \ldots, a_p) \in S_0$ αν και μόνο αν $a_1 = a_2 = \cdots = a_p$. Είναι προφανές $(e, e, \ldots, e) \in S_0$ και ως εκ τούτου $|S_0| \neq 0$. Από το Λήμμα 1.2.1, $0 \equiv |S| \equiv |S_0| (modp)$. Αφού $|S_0| \neq 0$ θα πρέπει να υπάρχουν τουλάχιστον p στοιχεία στο S_0. Δηλαδή υπάρχει ένα $a \neq e$ τέτοιο ώστε $(a, a, \ldots, a) \in S_0$ και $a^p = e$. Αφού ο p είναι πρώτος, $|a| = p$. □

Μια ομάδα στην οποία κάθε στοιχείο έχει τάξη μια δύναμη σταθερού πρώτου αριθμού p, ονομάζεται p-ομάδα. Αν H είναι υποομάδα της ομάδας G και H είναι p-ομάδα, τότε η H ονομάζεται p-υποομάδα της G. Προφανώς $\langle e \rangle$ είναι μια p-υποομάδα της G, για κάθε πρώτο p καθώς $|\langle e \rangle| = 1 = p^0$.

Πόρισμα 1.2.3. *Μια πεπερασμένη ομάδα G είναι μια p-ομάδα αν και μόνο αν $|G|$ είναι μια δύναμη του p.*

Απόδειξη. Αν G είναι μια p-ομάδα και q πρώτος που διαιρεί την $|G|$, τότε η G περιέχει ένα στοιχείο τάξης q, από το Θεώρημα Cauchy. Αφού κάθε στοιχείο της G έχει τάξη μια δύναμη του p, $p = q$. Ως εκ τούτου $|G|$ είναι μια δύναμη του p. Το αντίστροφο είναι άμεση συνέπεια του Θεωρήματος Lagrange. □

Πόρισμα 1.2.4. *Έστω G είναι μια p-ομάδα. Τότε $Z(G) = 1$.*

Απόδειξη. Από την Παρατήρηση 1.1.10 έχουμε

$$|G| = |Z(G)| + \sum_{i=1}^{m} [G : C_G(x_i)]$$

και $[G : C_G(x_i)] > 1$. Επειδή $[G : C_G(x_i)]/|G|$, είναι θετική δύναμη του p. Άρα και το $|Z(G)|$ είναι μια θετική δύναμη του p και συνεπώς $|Z(G)| > 1$. □

Λήμμα 1.2.5. *Αν H είναι μια p-υποομάδα πεπερασμένης ομάδας G, τότε $[N_G(H) : H] \equiv [G : H] (modp)$.*

Απόδειξη. Έστω S το σύνολο των αριστερών συμπλόκων της H στην G και η H δρα στην S με αριστερή μετάφραση. Τότε $|S| = [G : H]$. Ακόμη,

$$\begin{aligned} xH \in S_0 &\Leftrightarrow hxH = xH \text{ για όλα τα } h \in H \\ &\Leftrightarrow x^{-1}hxH = H \text{ για όλα τα } h \in H \\ &\Leftrightarrow x^{-1}hx \in H \text{ για κάθε } h \in H \\ &\Leftrightarrow x^{-1}Hx = H \Leftrightarrow xHx^{-1} = H \Leftrightarrow x \in N_G(H). \end{aligned}$$

Επομένως, $|S_0|$ είναι ο αριθμός των συμπλόκων xH, με $x \in N_G(H)$, $|S_0| = [N_G(H) : H]$. Από το Λήμμα 1.2.1

$$[N_G(H) : H] = |S_0| \equiv |S| = [G : H] (modp).$$

□

Πόρισμα 1.2.6. *Αν H είναι p-υποομάδα πεπερασμένης ομάδας G και p διαιρεί την $[G : H]$, τότε $N_G(H) \neq H$.*

Απόδειξη. $0 \equiv [G : H] \equiv [N_G(H) : H](mod p)$. Αφού $[N_G(H) : H] \geq 1$ σε κάθε περίπτωση θα πρέπει να έχουμε $[N_G(H) : H] > 1$. Άρα, $N_G(H) \neq H$. □

Θεώρημα 1.2.7. *(Πρώτο Θεώρημα Sylow) Έστω G ομάδα. Αν p^a είναι μια δύναμη ενός πρώτου αριθμού που διαιρεί την τάξη της ομάδας G, τότε η G περιέχει μια υποομάδα τάξης p^a. Επίσης, κάθε υποομάδα τάξης p^a $(a < n)$ είναι κανονική σε μια υποομάδα τάξης p^{a+1}.*

Απόδειξη. Έστω X το σύνολο όλων των υποσυνόλων της G που έχουν τάξη p^a. Τότε η G δρα πάνω στο X με $gU = \{gu : u \in U\}$, για $U \in X$. Έστω $X_1, X_2, \ldots, X_s$ οι τροχιές αυτής της δράσης. Έχουμε

$$|X| = \sum_{i=1}^{s} |X_i|. \qquad (1)$$

Έστω ότι X_i είναι η τροχιά του υποσυνόλου U_i της G που έχει p^a στοιχεία. Αν H_i είναι η σταθεροποιούσα υποομάδα του U_i, τότε έχουμε ότι

$$|X_i| = \frac{|G|}{|H_i|}, i = 1, 2, \ldots, s. \qquad (2)$$

Αν $u \in U_i$ και $x \in H_i$, τότε $xu \in U_i$ αφού $xU_i = U_i$. Κρατώντας το u σταθερό και θεωρώντας το x να διατρέχει όλα τα στοιχεία της H_i, παίρνουμε $H_i u \subseteq U_i$. Άρα το U_i είναι η ένωση όλων των δεξιών κλάσεων $H_i u, u \in U_i$ (φυσικά όλες οι κλάσεις αυτές μπορεί να μην είναι διάφορες μεταξύ τους). Έστω r_i το πλήθος των διάφορων ανά δύο κλάσεων $H_i u, u \in U_i$. Τότε $|U_i| = r_i |H_i|$. Αυτό δείχνει ότι η τάξη $|H_i|$ της H_i διαιρεί την τάξη $|U_i| = p^a$. Συνεπώς έχουμε

$$|H_i| = p^{a_i}, a_i \leq a, i = 1, \ldots, s. \qquad (3)$$

Έστω $n = |G| = p^a m$. Από τις (2), και (3) έπεται ότι

$$|X_i| = p^{d_i} m, \text{όπου } d_i = a - a_i.$$

Επίσης έχουμε:

$$|X| = \binom{p^a m}{p^a} = \frac{(p^a m - p^a + 1) \ldots (p^a m)}{(p^a)!}.$$

Είναι φανερό ότι η μεγαλύτερη δύναμη του p που διαιρεί το X είναι η μεγαλύτερη δύναμη του p που διαιρεί το m. Αυτό συμβαίνει γιατί οι όροι στον αριθμητή που διαιρούνται από τις δυνάμεις του p είναι της μορφής $p^i k$, $1 \leq i \leq a$, και εμφανίζονται όλοι μόνο μία φορά. Αν p^t είναι η μεγαλύτερη δύναμη που διαιρεί τον m τότε, η δύναμη p^{t+1} δεν διαιρεί τον $|X|$. Επίσης $|X| = m(p^{d_1} + \cdots + p^{d_s})$. Αν ήταν $d_i > 0$, για όλα τα $i = 1, 2, \ldots, s$, τότε η δύναμη p^{t+1} θα διαιρούσε τον $|X|$ που είναι άτοπο. Άρα υπάρχει i, $d_i = 0$. Γι' αυτό το i θα έχουμε $a_i = a$, δηλαδή $|H_i| = p^a$ που αποδεικνύει το ζητούμενο.

Τώρα υποθέτουμε ότι $a < n$. Τότε, από το Λήμμα 1.2.5 και Πόρισμα 1.2.6,

$$1 < |N_G(H) : H| = [N_G(H) : H] \equiv [G : H] mod p \equiv 0 mod p.$$

Άρα $p / |N_G H/H|$ και η $N_G H/H$ περιέχει μια υποομάδα τάξης p. Αυτή η υποομάδα είναι της μορφής H_1/H, $H < H_1 < N_G(H)$ (Θεώρημα 1.1.14), και συνεπώς $H \triangleleft H_1$. Επίσης, τελικά,

$$|H_1| = |H||H_1/H| = p^a . p = p^{a+1}.$$

□

Ορισμός 1.2.8. *Έστω $|G| = p^a m$. Μια μέγιστη p-υποομάδα P ονομάζεται Sylow p-υποομάδα της G, δηλαδή αν H είναι μια p-υποομάδα της G και $P < H < G$ τότε $P = H$*

Πόρισμα 1.2.9. *Έστω G ομάδα τάξης $p^n m$, p πρώτος, $n \geq 1$ και $(m, p) = 1$. Έστω H μια p-υποομάδα της G.*

(i) *Η P είναι μια Sylow p-υποομάδα της G αν και μόνο αν $|P| = p^n$.*

(ii) *Κάθε συζυγής μιας Sylow p-υποομάδας είναι μια Sylow p-υποομάδα.*

(iii) *Αν υπάρχει μια μόνο Sylow p-υποομάδα P, τότε η P είναι κανονική υποομάδα της G.*

Απόδειξη. Για την (i), αν η P είναι Sylow p-υποομάδα, τότε $|P| = p^k$. Αν $k < n$, το Θεώρημα 1.2.7 δίνει μια υποομάδα τάξης $k+1$, που περιέχει την P, άτοπο γιατί η P είναι μέγιστη. Το (ii) είναι συνέπεια του (i) γιατί κάθε συζυγής της P είναι ισόμορφη με την P. Το (iii) είναι συνέπεια των δύο προηγούμενων. □

Θεώρημα 1.2.10. *(Δεύτερο Θεώρημα Sylow) Έστω H είναι μια p-υποομάδα της G και P μια Sylow p-υποομάδα. Τότε η H περιέχεται σε μια συζυγή της P. Ειδικότερα, κάθε δυο Sylow p-υποομάδες της G είναι συζυγείς.*

Απόδειξη. Έστω S το σύνολο των αριστερών συμπλόκων της P και η H δρα στο S με αριστερό πολλαπλασιασμό. Έχουμε (Λήμμα 1.2.1)

$$|S_0| \equiv |S| \equiv [G : P] mod p.$$

Αλλά $p \nmid [G : P]$ και επομένως $|S_0| \neq 0$. Αυτό σημαίνει ότι υπάρχει $xP \in S_0$. Επομένως, για κάθε $h \in H$

$$hxP = xP \Leftrightarrow x^{-1}hxP = P \Leftrightarrow x^{-1}Hx = P \Leftrightarrow H = xPx^{-1}.$$

Τώρα , αν η H είναι Sylow p-υποομάδα, τότε $|H| = |P| = |xPx^{-1}|$ και συνεπώς $H = xPx^{-1}$. □

Θεώρημα 1.2.11. *(Τρίτο Θεώρημα Sylow) Αν r είναι το πλήθος των Sylow p-υποομάδων μιας πεπερασμένης ομάδας G, τότε $r/|G|$ και $r \equiv 1 (mod p)$.*

Απόδειξη. Από το Δεύτερο Θεώρημα του Sylow ο αριθμός των Sylow p-υποομάδων είναι ο αριθμός των συζυγών οποιασδήποτε απ' αυτές, έστω P. Αυτός ο αριθμός είναι $[N_G(P) : P]$, που διαιρεί το $|G|$. Έστω $P_1, P_2, \ldots, P_r$ όλες οι Sylow p-υποομάδες της G. Η P_1 δρα πάνω στο σύνολο $\{P_1, P_2, \ldots, P_r\}$ με δράση $gP_i = gP_ig^{-1}, g \in P_1, i = 1, 2, \ldots, r$ (αφού η gP_ig^{-1} είναι μια Sylow p-υποομάδα). Κάτω από αυτή τη δράση η μόνη p-υποομάδα που μένει σταθερή είναι η P_1. Πράγματι, αν υπήρχε $i \in 2, 3, \ldots, r$ με $gP_ig^{-1} = P_i$, για κάθε $g \in P_1$, τότε η P_1 θα ήταν υποομάδα της κανονικοποιούσας υποομάδας $N_G(P_i)$ της P_i. Αλλά P_1 και P_i είναι δύο Sylow p-υποομάδες της G και άρα της $N_G(P_i)$. Άρα είναι συζυγείς στην $N_G(P_i)$. Αλλά η $N_G(P_i)$ κανονικοποιεί την P_i. Άρα $P_1 = P_i$ Συνεπώς, για αυτή τη δράση, μόνο μια τροχιά περιέχει μόνο ένα στοιχείο και αυτή είναι το μονοσύνολο $\{P_1\}$. Άρα το πλήθος των p-υποομάδων του Sylow που περιέχονται σε μια τροχιά διάφορη της P_1 πρέπει να διαιρεί την τάξη $|P_1|$, δηλαδή αυτό το πλήθος πρέπει να είναι μια δύναμη του p. Συνεπώς, $r = 1 +$ (άθροισμα δυνάμεων του p) και άρα $p | r - 1$. □

Κεφάλαιο 2

Ταξινόμηση Πεπερασμένων Ομάδων

Στο κεφάλαιο αυτό θα ταξινομήσουμε όλες τις ομάδες τάξης p, p^2, pq (pq πρώτοι) και όλες τις ομάδες μικρής τάξης ($n \leq 16$).

2.1 Ταξινόμηση ομάδων τάξης μέχρι 15

Πρώτα χαρακτηρίζουμε τις κυκλικές ομάδες.

Θεώρημα 2.1.1. *Κάθε άπειρη κυκλική ομάδα είναι ισόμορφη με την προσθετική ομάδα $\mathbb{Z}$ και κάθε πεπερασμένη κυκλική ομάδα τάξης m είναι ισόμορφη με την προσθετική ομάδα $\mathbb{Z}_m$.*

Απόδειξη. Άν $G = \langle a \rangle$ είναι μία κυκλική ομάδα τότε ορίζουμε την απεικόνιση

$$a : \mathbb{Z} \to G, \quad k \mapsto a^k.$$

Είναι προφανές ότι η συνάρτηση είναι ένας επιμορφισμός. Αν $Ker(a) = 0$, τότε ο a είναι και μονομορφισμός και $\mathbb{Z} \cong G$. Αν η $Ker(a) \neq 0$, τότε είναι μια μη τετριμένη υποομάδα της $\mathbb{Z}$ και ως εκ τούτου $Ker(a) = \langle m \rangle$, όπου m ο μικρότερος θετικός ακέραιος τέτοιος ώστε $a^m = e$. Για όλα τα $r, s \in \mathbb{Z}$,

$$a^r = a^s \Leftrightarrow a^{r-s} = e \Leftrightarrow r - s \in Ker(a) = \langle m \rangle \Leftrightarrow m|(r-s) \Leftrightarrow \bar{r} = \bar{s} \in \mathbb{Z}_m$$

Άρα η απεικόνιση $\beta : \mathbb{Z}_m \to G$ με $\bar{k} \mapsto a^k$ είναι ένας καλά ορισμένος επιμορφισμός. Έτσι

$$\beta(\bar{k}) = e \Leftrightarrow a^k = e = a^0 \Leftrightarrow \bar{k} = \bar{0} \in Z_m,$$

και β είναι μονομορφισμός και επομένως ισομορφισμός $Z_m \cong G$. □

Θεώρημα 2.1.2. *Έστω G μαι ομάδα με $|G| = p$, όπου p είναι πρώτος. Τότε η G είναι κυκλική.*

Απόδειξη. Έστω $x \in G - \{1\}$. Θα δείξουμε ότι $G = \langle x \rangle$. Έχουμε ότι $|\langle x \rangle| > 1$ και διαιρεί τον p. Άρα $|\langle x \rangle| = p$ και $\langle x \rangle = G$. □

Για τις πεπερασμένες αβελιανές ομάδες έχουμε το Θεώρημα Ταξινόμησης.

Θεώρημα 2.1.3. *Κάθε πεπερασμένη αβελιανή ομάδα τάξης n είναι ισόμορφη με το ευθύ γινόμενο των κυκλικών ομάδων τύπου $\mathbb{Z}_{p_1^{a_1}} \times \mathbb{Z}_{p_2^{a_2}} \times \ldots \mathbb{Z}_{p_r^{a_r}}$, όπου p_i πρώτοι (όχι υποχρεωτικά διαφορετικοί) και $p_1^{a_1} p_2^{a_2} \ldots p_r^{a_r} = n$.*

Πόρισμα 2.1.4. *Εάν $(n, m) = 1$, $\mathbb{Z}_n \times \mathbb{Z}_m = \mathbb{Z}_{nm}$.*

Επίσης χρειαζόμαστε και μια βασική ιδιότητα των αβελιανών ομάδων.

Πρόταση 2.1.5. *Έστω G μια ομάδα που κάθε στοιχείο της έχει τάξη 2. Τότε η G είναι αβελιανή.*

Απόδειξη. Έχουμε

$$(ab)^2 = a^2 b^2 = 1 \Longleftrightarrow abab = aabb \Longleftrightarrow ba = ab.$$

□

Το επόμενο βήμα είναι να ταξινομήσουμε τις πεπερασμένες ομάδες που η τάξη τους είναι το γινόμενο δυο διαφορετικών πρώτων. Χρειαζόμαστε τα ημιευθαία γινόμενα ομάδων. Έστω G και H δυο ομάδες και $\theta : H \to Aut(G)$ ένας ομομορφισμός ομάδων. Ορίζουμε την ομάδα $G \times_\theta H$ ως εξής. Σαν σύνολο η $G \times_\theta H$ είναι το καρτεσιανό γινόμενο $G \times H$. Ο πολλαπλασιασμός ορίζεται:

$$(g, h)(g', h') = (g[\theta(h)(g')], hh')$$

Το ταυτοτικό στοιχείο είναι $(1, 1)$. Για το αντίστροφο έχουμε:

$$(g, h)^{-1} = (\theta(h)(g^{-1}), h^{-1})$$

Παρατήρηση 2.1.6. (i) *Από τον ορισμό έχουμε ότι $G \lhd G \times_\theta H$.*

(ii) *Εάν θ είναι η τετριμμένη συνάρτηση τότε το ημιευθύ γινόμενο είναι απλά το ευθύ γινόμενο.*

Λήμμα 2.1.7. *Έστω $C_p = \langle p \rangle$ και $C_q = \langle q \rangle$ δύο κυκλικές ομάδες τάξης p και q αντίστοιχα. Υποθέτουμε ότι p και q είναι πρώτοι με $p > q$ και $q/p - 1$. Έστω s ένας ακέραιος έτσι ώστε*

$$s \not\equiv 1 mod p, \ s^q \equiv 1 mod p$$

Τότε

(i) *Η συνάρτηση*
$$\alpha : C_p \to C_p, \ \alpha(a^i) = a^{si}$$
είναι αυτομορφισμός.

(ii) *Η συνάρτηση*
$$\theta : C_q \to Aut(C_p), \ \theta(b^i) = \alpha^i$$
είναι ομομορφισμός.

(iii) *Εάν θέσουμε a για το $(a, 1)$ και b για το $(1, b)$ τότε η ομάδα $C_p \times_\theta C_q$ παράγεται από τα a και b σύμφωνα με τις σχέσεις:*
$$|a| = p, |b| = q, ba = a^s b.$$

Απόδειξη. Για το πρώτο αποτέλεσμα, παρατηρούμε ότι $s \not\equiv 0 mod p$. Άρα υπάρχει t έτσι ώστε $st \equiv 1 mod p$. Τότε η συνάρτηση

$$\alpha' : C_p \to C_p,\ \alpha'(a^i) = a^{ti},$$

είναι η αντίστροφη της α. Επομένως ο α είναι ισομορφισμός.

Για το δεύτερο, αρκεί να δείξουμε ότι ο θ είναι καλά ορισμένος. Έστω $i \equiv j mod q$, δηλαδή $i = mq + j$. Τότε $\theta(b^i) = \alpha^i$. Έχουμε:

$$\alpha^i(a^k) = a^{s^i k} = a^{ks^{mq}s^j} = a^{k(s^q)^m s^j} = a^{ks^j} = \alpha^j(a^k)$$

Άρα $\theta(b^i) - \theta(b^j)$ και η συνάρτηση είναι καλά ορισμένη.

Η ομάδα έχει τάξη pq γιατί, σαν σύνολο, είναι το καρτεσιανό γινόμενο. Θα δείξουμε ότι τα στοιχεία της $C_p \times_\theta C_q$ ικανοποιούν τις σχέσεις που δίνονται. Οι δύο πρώτες σχέσεις είναι προφανείς. Για την τρίτη σχέση υπολογίζουμε τις δύο πλευρές ανεξάρτητα:

$$ba = (1, b)(a, 1) = (\theta(b)(a), b) = (\alpha(a), b) = (a^s, b).$$

Παρατηρούμε $a^s = (a, 1)^s = (a^s, 1)$. Οπότε

$$a^s b = (a^s, 1)(1, b) = (a^s, b).$$

□

Πρόταση 2.1.8. *Έστω p, q πρώτοι, με $p > q$. Αν $q \nmid p - 1$, τότε κάθε ομάδα τάξης pq είναι ισόμορφη με την κυκλική ομάδα $\mathbb{Z}_{pq}$. Αν $q|p - 1$ τότε υπάρχουν ακριβώς δύο διακεκριμένες ομάδες τάξης pq. Η κυκλική ομάδα $\mathbb{Z}_{pq}$ και μια μη-αβελιανή ομάδα K που παράγεται από τα στοιχεία c και d τέτοια ώστε :*

$$|c| = p, |d| = q, dc = c^s d,\ \text{όπου}\ s \neq 1 (mod p), s^q \equiv 1 (mod p).$$

Απόδειξη. Έστω $|G| = pq$. Από το Τρίτο Θεώρημα του Sylow, ο αριθμός r_p των Sylow p-υποομάδων μπορεί να είναι 1, p, q ή pq. Επειδή $q < p$ και $r_p \equiv 1 mod p$, $r_p = 1$. Άρα υπάρχει μόνο μια Sylow p-υποομάδα P, που θα είναι υποχρεωτικά κανονική.

Έστω $q \nmid p - 1$. Τότε από το Τρίτο Θεώρημα του Sylow και πάλι, υπάρχει μόνο μια Sylow q-υποομάδα Q. Άρα η Q είναι κανονική κυκλική υποομάδα της G. Επίσης $P \cap Q = \{1\}$. Άρα (Πόρισμα 2.1.4).

$$G \cong P \times Q = \mathbb{Z}_p \times \mathbb{Z}_q \cong \mathbb{Z}_{pq}.$$

Έστω $q/p - 1$. Τότε ο αριθμός των Sylow q-υποομάδων $r_q = 1, p$. Εάν $r_q = 1$, τότε υπάρχει μόνο μια Sylow q-υποομάδα και αυτή θα είναι κανονική. Όπως και στην προηγούμενη περίπτωση $G \cong \mathbb{Z}_{pq}$. Έστω ότι $r_q = p$ και $Q = \langle b \rangle$ μια υποομάδα τάξης q. Επειδή $P = \langle a \rangle \lhd G$, $bab^{-1} = a^s$, για κάποιο s. Παρατηρούμε ότι $s \not\equiv 1 mod p$ γιατί σ' αυτήν την περίπτωση, θα είχαμε αβελιανή ομάδα όπως και πριν και η Q θα ήταν κανονική. Ισχύει ότι $b^j a b^{-j} = a^{s^j}$. Ειδικότερα, αν $j = q$, $s^q \equiv 1 mod p$. Τότε η G είναι η μη-αβελιανλή ομάδα που περιγράψαμε στο Λήμμα 2.1.7.

□

Η διεδρική ομάδα D_{2n} ορίζεται σαν την ομάδα συμμετριών του κανονικού n-γώνου. Μια παράστασή της είναι:

$$D_{2n} = \langle x, y : \ x^n = y^2 = 1, yx = x^{-1}y \rangle.$$

Πόρισμα 2.1.9. *Αν p είναι περιττός πρώτος, τότε κάθε ομάδα τάξης $2p$ είναι ισόμορφη είτε στην κυκλική ομάδα Z_{2p} είτε στην διεδρική ομάδα D_{2p}.*

Απόδειξη. Σύμφωνα με την Πρόταση 2.1.8, για $q = 2$, αν η G δεν είναι κυκλική, οι συνθήκες για το s δίνουν ότι $s \equiv -1 (mod p)$. Οπότε

$$G = \langle c, d; \ |d| = 2, |c| = p, dc = c^{-1}d \rangle.$$

Επομένως, $G \cong D_{2p}$ □

Τώρα μπορούμε να ταξινομήσουμε τις ομάδες με τάξη ≤ 7.

Θεώρημα 2.1.10.

- *$|G| = 1$, τότε $G = \{1\}$.*
- *$|G| = 2$, $G \cong \mathbb{Z}_2$ γιατί ο 2 είναι πρώτος.*
- *$|G| = 3$, $G \cong \mathbb{Z}_3$ γιατί ο 3 είναι πρώτος.*
- *$|G| = 4$. Τότε η G είναι αβελιανή, Αυτό είναι προφανές γιατί ή η G είναι κυκλική ή δεν είναι. Αν δεν είναι τότε κάθε στοιχείο έχει τάξη 2. Από την Πρόταση 2.1.5, η G είναι αβελιανή. Από την ταξινόμηση των πεπερασμένων αβελιανών ομάδων, $G \cong \mathbb{Z}_4$ ή $\mathbb{Z}_2 \times \mathbb{Z}_2$.*
- *$|G| = 5$, $G \cong \mathbb{Z}_5$ γιατί ο 5 είναι πρώτος.*
- *$|G| = 6$. Αν η G είναι αβελιανή τότε $G \cong \mathbb{Z}_6$. Αν η G δεν είναι αβελιανή, τότε είναι διεδρική από το Πόρισμα 2.1.9. Παρατηρούμε ότι σ' αυτήν την περίπτωση, $D_6 \cong S_3$.*
- *$|G| = 7$, $G \cong \mathbb{Z}_7$ γιατί ο 7 είναι πρώτος.*

Για τις ομάδες τάξης 8, θα αρχίσουμε από τις αβελιανές ομάδες. Από το Θεώρημα Ταξινόμησης έχουμε ότι οι αβελιανές ομάδες τάξης 8 είναι:

$$\mathbb{Z}_8, \mathbb{Z}_4 \times \mathbb{Z}_2, \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2.$$

Η ομάδα τετρακτονίων (group of quartenions) ορίζεται ως $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$ με πράξεις:

$$i^2 = j^2 = k^2 = 1, ij = -ji = k, jk = -kj = i, ki = -ik = j.$$

Μια παράσταση της Q_8 είναι:

$$Q_8 = \langle x, y; \ x^4 = 1, x^2 = y^2, yxy^{-1} = x^{-1} \rangle.$$

Απλά μπορούμε να διαλέξουμε $x = i$, $y = j$, με τον παραπάνω συμβολισμό.

Θεώρημα 2.1.11. *Οι Q_8 και D_8 είναι οι μόνες μη-αβελιανές ομάδες τάξης 8.*

Απόδειξη. Μια ομάδα τάξης 8 δεν έχει στοιχείο τάξης 8, εκτός αν η ομάδα είναι κυκλική. Επίσης, δεν είναι δυνατόν κάθε στοιχείο της να είναι τάξης 2 γιατί τότε θα ήταν αβελιανή (Πρόταση 2.1.5). Άρα έχει τουλάχιστον ένα στοιχείο a τάξης 4. Έστω $H = \langle a \rangle$ η ομάδα που παράγεται από το a. Τότε η H έχει δείκτη 2 στην G. Άρα είναι κανονική. Επίσης $G/H \cong \mathbb{Z}_2$. Έστω $b \in G - H$. Τότε $b \notin H$ αλλά $b^2 \in H$ (γιατί η G/H έχει δείκτη 2). Εάν $b^2 = a$, $b^2 = a^3$, τότε το b έχει τάξη 8, άτοπο. Άρα, έχουμε δύο περιπτώσεις: $b^2 = a^2$ και $b^2 = 1$. Επίσης, όμοια, $bab^{-1} = a$ ή $bab^{-1} = a^3$ (γιατί το bab^{-1} έχει την ίδια τάξη με τον a). Η πρώτη περίπτωση δεν μπορεί να συμβεί γιατί, εάν ίσχυε, η G θα ήταν αβελιανή. Άρα έχουμε:

(i) $a^4 = 1$, $a^2 = b^2$, $bab^{-1} = a^3 = a^{-1}$ και $G \cong Q_8$.

(ii) $a^4 = 1$, $b^2 = 1$, $bab^{-1} = a^3 = a^{-1}$ και $G \cong D_8$.

□

Για την περίπτωση $|G| = 12$, έχουμε τις εξής αβελιανές ομάδες: $\mathbb{Z}_{12}$, $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3$. Για τις μη-αβελιανές ομάδες, πρώτα θα δείξουμε κάποια αποτελέσματα για τις εναλλάσσουσες υποομάδες της S_n. Υπενθυμίζουμε ότι η εναλλάσουσα υποομάδα A_n της S_n είναι η υποομάδα των άρτιων μεταθέσεων δηλαδή των μεταθέσεων που μπορούν να γραφτούν σαν άρτιο γινόμενο 2-κύκλων. Τότε $[S_n : A_n] = 2$.

Λήμμα 2.1.12. *Έστω $r, s \in \{1, \dots n\}$ δύο διακεκριμένα στοιχεία. Τότε η A_n ($n \geq 3$) παράγεται από τους 3-κύκλους $\{(rsk) : \ 1 \leq k \leq n, k \neq r, s\}$*

Απόδειξη. Για $n = 3$, $A_3 = \{(1), (123), (132)\}$, το αποτέλεσμα είναι προφανές. Υποθέτουμε $n > 3$. Τότε, κάθε στοιχείο της A_n μπορεί να γραφτεί σαν γινόμενο στοιχείων της μορφής $(ab)(cd)$ ή $(ab)(ac)$, όπου a, b, c, d είναι διακεκριμένα στοιχεία του $\{1, \dots n\}$. Επειδή

$$(ab)(cd) = (acb)(acd), \ \ (ab)(ac) = (acb),$$

η A_n παράγεται από 3-κύκλους. Κάθε 3-κύκλος είναι της μορφής (rsa), (ras), (rab), (sab), ή (abc), όπου a b c είναι διακεκριμένα και $a, b, c \neq r, s$. Αλλά ισχύει

$$\begin{aligned} &(ras) = (rsa)^2, \ (rab) = (rsb)(rsa)^2, \\ &(sab) = (rsb)^2(rsa), \ (abc) = (rsa)^2(rsc)(rsb)^2(rsa). \end{aligned}$$

Αυτό αποδεικνύει και το αποτέλεσμα. □

Λήμμα 2.1.13. *Έστω $N \triangleleft A_n$ και περιέχει έναν 3-κύκλο. Τότε $N = A_n$*

Απόδειξη. Έστω $(rsc) \in N$, τότε για κάθε $k \neq r, s, c$,

$$(rsk) = (rs)(ck)(rsc)^2(ck)(rs) = [(rs)(ck)](rsc)^2[(rs)(ck)]^{-1} \in N$$

Άρα, από το προηγούμενο Λήμμα $N = A_n$. □

Πρόταση 2.1.14. *Έστω $H < S_n$, δείκτη 2. Τότε $H = A_n$.*

Απόδειξη. Για $n = 3$ το αποτέλεσμα είναι προφανές. Για $n > 3$, χρησιμοποιούμε ότι κάθε δύο 3-κύκλοι είναι συζυγείς. Αρκεί λοιπόν να δείξουμε ότι η H περιέχει έναν 3-κύκλο. Έχουμε περιπτώσεις:

(i) Εάν $\sigma = (1 \dots r)r \in H$, $r \geq 4$, τότε θέτουμε $\delta = (123)$ και

$$\sigma^{-1}\delta^{-1}\sigma\delta = (r \dots 1)(132)(1 \dots r)(123) = (23r) \in H$$

(ii) Έστω $\sigma = (123)(456)r \in H$, τότε θέτουμε $\delta = (124)$

$$\sigma^{-1}\delta^{-1}\sigma\delta = (132)(465)(142)(123)(456)(124) = (12436)$$

και τελειώσαμε όπως στην (i).

(iii) Εάν $\sigma = (123)r \in H$ και η r είναι γινόμενο 2-κύκλων, τότε $\sigma^2 = (132) \in H$.

(iv) $\sigma = (12)(34)\tau \in H$ και η τ είναι γινόμενο 2-κύκλων, τότε θέτουμε $\delta = (123)$ και

$$\sigma^{-1}\delta^{-1}\sigma\delta = (14)(23) = (124)(123)$$

και τελειώνουμε όπως στην (ii).

□

Φυσικά η A_4 είναι μια μη-αβελιανή ομάδα τάξης 12. Η επόμενη πρόταση χαρακτηρίζει τις ομάδες τάξης 12, που δεν είναι ισόμορφες της A_4.

Λήμμα 2.1.15. *Έστω $|G| = 12$, $G \ncong A_4$, τότε η G περιέχει ένα στοιχείο τάξης 6. Επιπλέον, η G περιέχει μια κανονική Sylow 3-υποομάδα, και συνεπώς περιέχει ακριβώς 2 στοιχεία τάξης 3.*

Απόδειξη. Έστω P μια Sylow 3-υποομάδα. Τότε $|P| = 3$ και P είναι κυκλική με γεννήτορα b. Επειδή $[G : P] = 4$, υπάρχει ομομορφισμός

$$\psi : G \to S_4, \quad K = \mathrm{Ker}(\psi) < P.$$

Άρα $K = 1$ ή $K = P$. Εάν $K = 1$, τότε η ψ είναι μονομορφισμός και η G είναι ισόμορφη με μια υποομάδα της S_4, δείκτη 2. Άρα, από την Πρόταση 2.1.14, $K \cong A_4$, άτοπο. Άρα, $K = P$ και $P \triangleleft G$, που σημαίνει ότι η P είναι η μόνη Sylow 3-υποομάδα της G και συνεπώς τα μόνο στοιχεία τάξης 3 της G είναι τα στοιχεία τάξης 3 της P, που είναι τα b και b^2. Αλλά, επιπλέον, $[G : C_G(b)]$ είναι μικρότερη ή ίση από τον αριθμό των συζυγών του b, που έχουν όλα τάξη 3. Άρα $[G : C_G(b)] \leq 2$ και συνεπώς $C_G(b) = 6$ ή 12. Σε κάθε περίπτωση το $C_G(b)$ περιέχει ένα στοιχείο a τάξης 2. Τότε το a μετατίθεται με το b και συνεπώς ab έχει τάξη 6. □

Ορίζουμε

$$T = \langle a, b : \ a^6 = 1, b^2 = a^3 = (ab)^2 \rangle$$

Παρατηρούμε ότι το b έχει τάξη 4. Έχουμε $ba = a^{-1}b$:

$$abab = a^3 \Rightarrow ba = a^2b^{-1} = a^2b^3 = a^2b^2b = a^5b = a^{-1}b.$$

Θα δείξουμε $T/\langle a \rangle = \{1, b\}$.

(i) Επειδή $b^2 \in \langle a \rangle$, $b^k \in \langle a \rangle$ (k άρτιος) και $b^k \in b\langle a \rangle$ (k περιττός).

(ii) Επειδή $aba = b$, $ab\langle a \rangle = b\langle a \rangle$ και $ab^k\langle a \rangle = b^k\langle a \rangle$ και ολοκληρώνουμε όπως στην (1). Όμοια και για τα σύμπλοκα της μορφής $b^kab\langle a \rangle$.

Άρα η T έχει τάξη 12.

Λήμμα 2.1.16. *Έχουμε* $D_{12} \cong S_3 \times \mathbb{Z}_2$.

Απόδειξη. Έστω $H = \{1, y, yx^2, x^2, yx^4, x^4\}$ και $K = \{1, x^3\}$, υποομάδες της D_{12}. Θα δείξουμε ότι $D_{12} \cong H \times K$. Είναι προφανές $H \cap K = \{1\}$. Αρκεί να δείξουμε ότι τα στοιχεία της H μετατίθενται με τα στοιχεία της K. Έχουμε $yx = x^{-1}y$. Άρα $yx^3 = x^{-3}y$ και φυσικά το x^3 μετατίθεται με τα άλλα στοιχεία της H. Επίσης, είναι προφανές ότι $H = \langle x^2, y\rangle \cong S_3$. □

Πρόταση 2.1.17. *Με τον παραπάνω συμβολισμό,* $T \ncong D_{12}$.

Απόδειξη. Έστω $H < T$, τάξης 6. Τότε $H \triangleleft T$ και $T/H \cong \mathbb{Z}_2$. Επειδή b έχει τάξη 4, τότε $b \notin H$, γιατί διαφορετικά, $\langle b\rangle < H$, άτοπο λόγω Θεωρήματος του Lagrange. Άρα το $T/H = \{H, bH\}$. Αλλά τότε, σύμφωνα με τους παραπάνω υπολογισμούς, $H = \langle a\rangle$. Αποδείξαμε ότι κάθε υποομάδα της T τάξης 6 είναι κυκλική. Αυτό δεν συμβαίνει με την D_{12} γιατί περιέχει την S_3 (Λήμμα 2.1.16). □

Θεώρημα 2.1.18. *Εάν η G είναι μη-αβελιανή ομάδα τάξης 12, τότε η G είναι ισόμορφη με D_{12}, T ή την A_4.*

Απόδειξη. Θα δείξουμε ότι αν η η G είναι μη-αβελιανή ομάδα τάξης 12 και $G \ncong A_4$, τότε είναι ισόμορφη με μια από τις άλλες δυο ομάδες. Έστω $K = \langle k\rangle$ η Sylow 3-υποομάδα, που είναι κανονική και P μια Sylow 2-υποομάδα της G και συνεπώς έχει τάξη 4. Επίσης, $G = KP$ γιατί η P είναι μέγιστη υποομάδα γιατί έχει δείκτη πρώτο αριθμό. Έχουμε $P = \mathbb{Z}_2 \times \mathbb{Z}_2$ ή $P = \mathbb{Z}_4$ (Θεώρημα 2.1.10).

Στην πρώτη περίπτωση, $P = \{1, x, y, z\}$, όλα τάξης 2. Δεν γίνεται όλα τα στοιχεία της P να μετατίθενται με το k γιατί τότε η G θα ήταν αβελιανή. Έστω λοιπόν ότι $xkx \neq k$. Αλλά το xkx είναι συζυγές του k, και άρα έχει τάξη 3. Επομένως $xkx = k^{-1}$ και $\langle x, k\rangle \cong D_6$, γιατί $D_6 = S_3$ είναι η μόνη μη-αβελιανή ομάδα τάξης 6. Εάν το y δεν μετατίθεται με το k, όπως και πριν, $yky = k^{-1}$. Οπότε $xkx = yky$ και το $z = xy$ μετατίθεται με το k. Θέτουμε $a = zk$ και έχουμε:

(i) $G = \langle a, x\rangle$. Κι αυτό γιατί η $\langle a, x\rangle$ περιέχει το zk άρα και το $(zk)^2 = k^2 = k^{-1}$. Άρα περιέχει και το k και συνεπώς και το z. Αφού περιέχει το z και το x, θα περιέχει και το $y = zx$. Επειδή περιέχει όλους τους γεννήτορες, θα είναι ολόκληρη η ομάδα G.

(ii) Το a έχει τάξη 6 (προφανές).

(iii) Επίσης, $xax = xzkx = zxkx = zk^{-1} = a^{-1}$.

Επομένως $G \cong D_{12}$.

Στην δεύτερη περίπτωση, $P = \langle x\rangle \cong \mathbb{Z}_4$. Τώρα x και k δεν μετατίθενται γιατί η $G = \langle x, k\rangle$ δεν είναι αβελιανή. Άρα $xkx^{-1} = k^{-1}$. Αλλά το x^2 μετατίθεται με το k:

$$x^2kx^{-2} = x(xkx^{-1})x^{-1} = xk^{-1}x^{-1} = k.$$

Άρα το $a = x^2k$ έχει τάξη 6. Επειδή x^2 και k μετατίθενται, $a^3 = (x^2k)^3 = x^6k^3 = x^2$. Στο τέλος έχουμε:

$$(ax)^2 = axax = x^2kxx^2kx = xxkx^{-1}kx = x^2.$$

Άρα, δείξαμε $G \cong T$ σ' αυτήν την περίπτωση. □

2.2 Ταξινόμηση ομάδων τάξης 16

Χρησιμοποιούμε το υλικό από το [1]. Για να ταξινομήσουμε τις ομάδες τάξης 16, πρέπει να λάβουμε υπ' όψιν τις διαφορετικές περιπτώσεις για την τάξη του κέντρου. Καθώς $Z(G)$ είναι μια μη τετριμμένη υποομάδα (Πόρισμα 1.2.4), η $Z(G)$ θα πρέπει να διαιρεί την τάξη της ομάδας, οπότε τα ενδεχόμενα για την τάξη του $Z(G)$ είναι 16, 8, 4, 2. Έπειτα χρησιμοποιώντας το Θεώρημα Αντιστοιχιών εξάγουμε συμπεράσματα για τις ιδιότητες της ομάδας στις διάφορες περιπτώσεις.

Πρώτα έχουμε τις αβελιανές ομάδες τάξης 16:

$$\mathbb{Z}_{2^4} = \mathbb{Z}_{16}, \mathbb{Z}_{2^3} \times \mathbb{Z}_2 = \mathbb{Z}_8 \times \mathbb{Z}_2, \mathbb{Z}_{2^2} \times \mathbb{Z}_{2^2} = \mathbb{Z}_4 \times \mathbb{Z}_4,$$

$$\mathbb{Z}_{2^2} \times \mathbb{Z}_2 \times \mathbb{Z}_2 = \mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_2, \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$$

Επίσης έστω G_i οι υποομάδες τάξης 8 της G που περιέχουν το $Z(G)$, για κάποιους δείκτες i. Πρώτα εξετάζουμε κάποιες ιδιότητες των G_i.

Θεώρημα 2.2.1. *Το κέντρο της G_i περιέχει το κέντρο της $G, Z(G) \subset Z(G_i)$.*

Απόδειξη. Αν ένα στοιχείο είναι στο κέντρο αντιμετατίθεται με όλα τα στοιχεία, επομένως αντιμετατίθεται με όλα τα G_i. □

Λήμμα 2.2.2. *Έστω H και K δυο πεπερασμένες υποομάδες μιας ομάδας G. Τότε για το υποσύνολο HK της G,*

$$|HK| = \frac{|H|.|K|}{|H \cap K|}$$

Απόδειξη. Ορίζουμε

$$HK = \{hk : \ h \in H, k \in K\} \subset G.$$

Είναι προφανές ότι $|HK| \leq |H|.|K|$ γιατί κάποια στοιχεία του HK μπορούν να γραφτούν σαν γινόμενο στοιχείων του H και του K με πάνω από έναν τρόπο. Μπορεί να έχουμε $h_1k_1 = h_2k_2$ για $h_1, h_2 \in H$ και $k_1, k_2 \in K$. Τότε θέτουμε

$$a = h_1^{-1}h_2 = k_1k_2^{-1},$$

και $a \in H \cap K$ και $h_2 = h_1a$, $k_2 = ak_1$.

Επίσης έστω $h = h_1b^{-1}$ και $k = bk_1$ για $b \in H \cap K$. Τότε $hk = h_1k_1$, με $h \in H$, $k \in K$. Άρα, κάθε στοιχείο $hk \in HK$ μπορεί να γραφτεί στην μορφή h_ik_i, $h_i \in H$, $k_i \in K$, τόσες φορές όσες και τα στοιχεία της τομής $H \cap K$, δηλαδή $|H \cap K|$ φορές. Άρα $|HK| = |H|.|K|/|H \cap K|$. □

Θεώρημα 2.2.3. *Η τομή δυο G_i θα πρέπει να είναι ομάδα τάξης 4.*

Απόδειξη. Έστω G_i, G_j διακεκριμένες υποομάδες τάξης 8 που περιέχουν το κέντρο. Τότε (Λήμμα 2.2.2)

$$|G_iG_j| = \frac{|G_i||G_j|}{|G_i \cap G_j|} = \frac{8.8}{|G_i \cap G_j|} = \frac{64}{|G_i \cap G_j|}.$$

Καθώς η τομή μιας υποομάδας είναι υποομάδα, η τάξη της $G_i \cap G_j$ πρέπει να είναι $8, 4, 2$ ή 1. Αν $|G_i \cap G_j| = 8$, τότε οι ομάδες είναι ίδιες. Για τις τάξεις 1 ή 2, παίρνουμε ότι $|G_iG_j|$ είναι 64 και 32 αντίστοιχα. Αυτό μας οδηγεί σε αντίφαση, αφού έτσι η G_iG_j είναι μεγαλύτερη από την G. Έτσι η τάξη της τομής δύο διακεκριμένων G_i είναι μια ομάδα τάξης 4. □

Θεώρημα 2.2.4. *Έστω g_i, g_j στοιχεία των G_i, G_j που δεν περιέχονται στην $G_i \cap G_j$. Τότε $g_i g_j$ δεν είναι ούτε στην G_i, ούτε στην G_j.*

Απόδειξη. Χωρίς περιορισμό της γενικότητας, θα δείξουμε ότι $g_i g_j \notin G_i$. Υποθέτουμε το αντίθετο ότι υπάρχει $h_i \in G_i, h_i = g_i g_j$. Τότε $g_j = {g_i}^{-1} h_i$, το οποίο θα σημαίνει ότι το g_j είναι στην τομή των G_i και G_j, άτοπο γιατί το $g_j \notin G_i$. Οπότε το $g_i g_j$ δεν είναι ούτε στην G_i, ούτε στην G_j. □

Θεώρημα 2.2.5. *Έστω $G/Z(G)$ αβελιανή. Τότε ο αντιμεταθέτης μεταξύ των g_i, g_j, είναι ένα στοιχείο z' του κέντρου, $g_i g_j = z' g_j g_i$.*

Απόδειξη. Έστω $g_i Z(G), g_j Z(G) \in G/Z(G)$. Τότε αφού η ομάδα πηλίκο είναι αβελιανή, $(g_i Z(G))(g_j Z(G)) = (g_j Z(G))(g_i Z(G))$. Άν κάνουμε την πράξη στην ομάδα πηλίκο, παίρνουμε $g_i g_j Z(G) = g_j g_i Z(G)$, οπότε $g_i g_j = z' g_j g_i$ για $z \in Z(G)$ από τις ιδιότητες των συμπλόκων. □

2.2α′ $|Z(G)| = 16$

Τότε $|Z(G)| = 16 = |G|$. Καθώς ένα υποσύνολο πεπερασμένου συνόλου ισούται με το σύνολο αν έχουν τον ίδιο αριθμό στοιχείων, $Z(G) = G$ και επομένως η G είναι αβελιανή.

2.2β′ $|Z(G)| = 8$

Η ομάδα πηλίκο $G/Z(G)$ έχει τάξη $|G/Z(G)| = |G|/|Z(G)| = 16/8 = 2$. Άρα είναι κυκλική. Ακολουθεί ένα το θεώρημα:

Θεώρημα 2.2.6. *Αν $G/Z(G)$ είναι κυκλική, τότε η G είναι αβελιανή.*

Απόδειξη. Έστω ότι η $G/Z(G)$ παράγεται από το στοιχείο $gZ(G)$. Έστω $x, y \in G$, $x = g^i Z(G)$ και $y = g^j Z(G)$. Δηλαδή $x = g^i z$, $y = g^j z'$, $z, z' \in Z(G)$. Οπότε

$$xy = g^i z g^j z' = g^i g^j z z' = g^{i+j} z z' = g^j g^i z z' = g^j z' g^i z = yx$$

και η G είναι αβελιανή. □

Πόρισμα 2.2.7. *Μια ομάδα τάξης p^2, όπου p είναι πρώτος, είναι αβελιανή.*

Απόδειξη. Έστω $|G| = p^2$. Το κέντρο της G δεν είναι τετριμμένο. Αν $|Z(G)| = p^2$, τότε $G = Z(G)$ και η G είναι αβελιανή. Αν $|Z(G)| = p$, τότε $|G/Z(G)| = p$ και άρα είναι κυκλική. Από το προηγούμενο θεώρημα η G είναι αβελιανή και $|Z(G)| = p^2$, άτοπο. □

Μια αβελιανή ομάδα έχει ένα κέντρο ίσο με την ομάδα. Αν το κέντρο ισούται με την ομάδα, τότε η τάξη του κέντρου είναι 16 και όχι 8. Επομένως υπάρχει αντίφαση, οπότε δεν υπάρχει ομάδα τάξης 16 με κέντρο τάξης 8.

2.2γ′ $|Z(G)| = 4$

Τότε η τάξη του $G/Z(G)$ είναι $|G/Z(G)| = 4$. Τα ενδεχόμενα για την ομάδα πηλίκο είναι (Θεώρημα 2.1.10):

$$G/Z(G) \cong \mathbb{Z}_4 \text{ ή } G/Z(G) \cong \mathbb{Z}_2 \times \mathbb{Z}_2.$$

Άν $G/Z(G) \cong \mathbb{Z}_4$, τότε η ομάδα πηλίκο είναι κυκλική. Από το Θεώρημα 2.2.6 έχουμε ότι το κέντρο είναι τάξης 16 και όχι 4. Ως εκ τούτου η ομάδα πηλίκο πρέπει να είναι ισόμορφη με την $\mathbb{Z}_2 \times \mathbb{Z}_2$. Παρατηρούμε ότι σ' αυτήν την περίπτωση, υπάρχουν 3 υποομάδες της $G/Z(G)$ τάξης 2 και από το Θεώρημα Αντιστοιχιών, υπάρχουν 3 ομάδες G_i (η αντιστοιχία από το G στο $G/Z(G)$ είναι 4 προς 1, οπότε μια υποομάδα τάξης 2 στην ομάδα πηλίκο έχει τάξη 2.4 = 8 στην G). Επίσης η τομή δύο G_i έχει τάξη (Θεώρημα 2.2.3) και άρα είναι το κέντρο.

Ακόμη, με $|Z(G)| = 4$, όλες οι G_i είναι αβελιανές, αφού $|Z(G_i)| \geq |Z(G)| = 4$ και επομένως $G_i/Z(G_i)$ ή είναι τετριμμένη ή έχει τάξη 2. Σε κάθε περίπτωση είναι κυκλική και (Θεώρημα 2.2.6) η G_i είναι αβελιανή. Επομένως οι G_i είναι $\cong \mathbb{Z}_8, \mathbb{Z}_4 \times \mathbb{Z}_2$, ή $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.

Θεώρημα 2.2.8. *Αν $|Z(G)| = 4$, και $g_i \in G_i$, $g_j \in G_j$, με $i \neq j$ που δεν ανήκουν στο κέντρο, τότε δεν αντιμετατίθενται.*

Απόδειξη. Αν g_i, g_j αντιμετατίθενται όταν βρίσκονται σε διαφορετικό G_i, τότε το g_i αντιμετατίθεται με όλα τα στοιχεία στα $Z(G), g_iZ(G), g_jZ(G)$. Αυτό σημαίνει ότι υπάρχουν τουλάχιστον 12 στοιχεία στον κεντροποιητή του g_i (ο κεντροποιητής του g_i είναι όλα τα στοιχεία που αντιμετατίθενται με το g_i) και αφού ο κεντροποιητής είναι μια υποομάδα, η τάξη του κεντροποιητή πρέπει να διαιρεί την τάξη της ομάδας. Έτσι ο κεντροποιητής είναι τάξης 16 και άρα είναι όλη η ομάδα. Οπότε το g_i αντιμετατίθεται με όλα τα στοιχεία οπότε βρίσκεται στο κέντρο. Άρα τα g_i, g_j δεν αντιμετατίθενται, και ο αντιμεταθέτης είναι ένα μη τετριμμένο στοιχείο του κέντρου (Θεώρημα 2.2.5). □

Τώρα μπορούμε να ταξινομήσουμε τις ομάδες λαμβάνοντας υπόψιν ότι εφόσον το κέντρο είναι τάξης 4, θα είναι ισόμορφη με την $\mathbb{Z}_4$ ή την $\mathbb{Z}_2 \times \mathbb{Z}_2$, και θα διακρίνουμε αυτές τις δύο περιπτώσεις:

Πρώτη Περίπτωση: $Z(G) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$

Επειδή $Z(G) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$, γνωρίζουμε ότι κάθε G_i περιέχει μια υποομάδα ισόμορφη με την $\mathbb{Z}_2 \times \mathbb{Z}_2$. Αφού όλες οι G_i είναι αβελιανές και η $\mathbb{Z}_8$ δεν περιέχει υποομάδες ισόμορφες με την $\mathbb{Z}_2 \times \mathbb{Z}_2$, οι πιθανές κατηγορίες ισομορφισμού για τις τρείς G_i είναι $\mathbb{Z}_4 \times \mathbb{Z}_2$ ή $\mathbb{Z}_2 \times \mathbb{Z}_2$. Έχουμε τώρα τα εξής ενδεχόμενα : όλες οι $G_i \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$, δύο $G_i \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$, μια $G_i \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ και καμία $G_i \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ (άρα όλες ισόμορφες με την $\mathbb{Z}_4 \times \mathbb{Z}_2$)

(1) Έστω $G_1, G_2, G_3 \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$. Κάθε στοιχείο της G είναι σε μια G_i. Άρα κάθε στοιχείο της G έχει τάξη 2. Από την Πρόταση 2.1.5, η G είναι αβελιανή και $|Z(G)| = 16$, άτοπο.

(2) Έστω $G_1, G_2 \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$, $G_3 \cong \mathbb{Z}_4 \times \mathbb{Z}_2$.

Αναφέρουμε τώρα συνθήκες, που θα χρησιμοποιούμε συχνά στο εξής.

Συνθήκη (*): Έστω $g_i \in G_i, G_j \in G_j$ στοιχεία τέτοια ώστε $g_i, g_j \notin G_i \cap G_j$. Έστω g' ο αντιμεταθέτης των g_i, g_j (δηλαδή $g_ig_j = g'g_ig_j$). Υποθέτουμε ότι $g' \in Z(G)$,

$$(g_ig_j)^2 = g_i(g_jg_i)g_j = g_ig'g_ig_j{}^2 = g'g_i{}^2g_j{}^2.$$

Επιλέγουμε στοιχεία $r \in G_3, s \in G_1$ με την Συνθήκη (*) τέτοιο ώστε $|r| = 4$ και $|s| = 2$. Επιλέγουμε αυτά τα στοιχεία γιατί υπάρχει κυκλική υποομάδα τάξης 4 στην G_3 και μια υποομάδα της G_1 ισόμορφη με την $\mathbb{Z}_2 \times \mathbb{Z}_2$ που δεν είναι το κέντρο. Έστω τώρα z' ο αντιμεταθέτης των s και r. Έχουμε $r^2 \in Z(G)$, αφού $|r|^2 = 2$ και όλα τα στοιχεία τάξης 2 στην G_3 είναι στο κέντρο (από τις ιδιότητες της $\mathbb{Z}_4 \times \mathbb{Z}_2$). Ακόμη $rs \in G_2$ (Θεώρημα 2.2.4), οπότε η τάξη της είναι 2 και επομένως

$$e = (rs)^2 = zr^2s^2 = zr^2.$$

Άρα $z = (r^2)^{-1} = r^2$, οπότε $sr = r^2rs = r^3s = r^{-1}s$. Ως εκ τούτου παίρνουμε την υποομάδα $H = \{e, r, r^2, r^3, s, rs, r^2s, r^3s\} < G$. Βλέπουμε ότι η H είναι κλειστή υποομάδα (χρησιμοποιώντας τον κανόνα της αντιμετάθεσης) και έχει αντίστροφα στοιχεία (τα στοιχεία στο $\langle r \rangle$ έχουν αντίστροφους στο $< r >$ και τα στοιχεία που δεν ανήκουν στο $\langle r \rangle$ έχουν τάξη 2). Επιλέγουμε ένα $z \in Z(G)$, τέτοιο ώστε $z \neq e, r^2$, και έχουμε ότι $\{z, e\} = \langle r \rangle = K$ είναι υποομάδα. Ακόμη, $H \cap K = \{e\}$, και (Λήμμα 2.2.2) $|HK| = |H||K|/|H \cap K| = 8 * 2/1 = 16$, άρα $HK = G$, και εφόσον η K είναι υποομάδα του κέντρου, έχουμε $hk = kh$ για κάθε $k \in K, h \in H$. Άρα η G είναι ευθύ εσωτερικό γινόμενο της $H \cong D_4$ και $K \cong \mathbb{Z}_2$, άρα $G \cong H \times K \cong D_4 \times \mathbb{Z}_2$. Αυτή η ομάδα αναπαρίσταται ως

$$G = \langle r^\alpha s^\beta z^\gamma : r^4 = s^2 = z^2 = e, sr = r^{-1}s, zr = rz, zs = sz \rangle.$$

(3) Έστω $G_1 \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2, G_2, G_3 \cong \mathbb{Z}_4 \times \mathbb{Z}_2$.

Σ' αυτήν την περίπτωση επιλέγουμε στοιχεία g_2, g_3, με τη Συνθήκη (*), τα οποία αφού δεν είναι στο κέντρο θα έχουν τάξη 4. Έστω z' ο αντιμεταθέτης των g_3, g_2 και έστω $g_2^2 = z_2, g_3^2 = z_3$ αφού τα τετράγωνα των στοιχείων είναι στο κέντρο. Ακόμη, $g_2g_3 \in G_1$, και $|g_2g_3| = 2$. Αυτό σημαίνει ότι $e = (g_2g_3)^2 = z'{g_2}^2{g_3}^2 = z'z_2z_3$. Στη συνέχεια ακολουθεί το επόμενο θεώρημα για την $\mathbb{Z}_2 \times \mathbb{Z}_2$:

Θεώρημα 2.2.9. *Έστω a, b, c μη ταυτοτικά στοιχεία στην $\mathbb{Z}_2 \times \mathbb{Z}_2$. Τότε $abc = e$ αν και μόνο αν κανένα ζεύγος στοιχείων από τα στοιχεία είναι ίσα.*

Απόδειξη. ($\Leftarrow$) Άν $c \neq a, c \neq b$ και $c \neq e$, τότε έχουμε ότι $c = ab$, γιατί είναι το μόνο στοιχείο που έμεινε. Συνεπώς $abc = cc = c^2 = e$.

($\Rightarrow$) Θα αποδείξουμε τώρα το αντίθετο-αντίστροφο. Άρα έστω δύο από στοιχεία να είναι ίσα και θέλουμε να δείξουμε ότι $abc \neq e$. Χωρίς περιορισμό της γενικότητας υποθέτουμε $a = b$. Τότε $abc = a^2c = c \neq e$ και αφού το αντιθετο-αντίστροφο ισχύει, ισχύει και η πρόταση, άρα $abc = e$ αν και μόνο αν $a \neq b \neq c \neq a$. ☐

Από το παραπάνω θεώρημα, βλέπουμε ότι $z' \neq z_2 \neq z_3$, άρα $z' = z_2z_3$ από τις ιδιότητες $\mathbb{Z}_2 \times \mathbb{Z}_2$. Έτσι έχουμε

$$g_3g_2 = (z_2z_3)g_2g_3 = z_2g_2z_3g_3 = g_2^3g_3^3 = g_2^{-1}g_3^{-1}.$$

Έπειτα έχουμε ότι

$$\langle g_2 \rangle = \{e, g_2, z_2, z_2g_2\},\ \langle g_3 \rangle = \{e, g_3, z_3, z_3g_3\}.$$

Άρα $\langle g_2 \rangle \cap \langle g_3 \rangle = \{e\}$. Άρα έχουμε 16 άμεσα αποτελέσματα τύπου $g_2^\alpha g_3^\beta$, και η ομάδα είναι η

$$G = \{g_2^\alpha g_3^\beta : g_2^4 = g_3^4 = e, g_3g_2 = g_2^{-1}g_3^{-1}\}.$$

Έχουμε ότι $G \cong (\mathbb{Z}_2 \times \mathbb{Z}_2) \times_\alpha \mathbb{Z}_4$ όπου το $\mathbb{Z}_4$ δρα στο $\mathbb{Z}_2 \times \mathbb{Z}_2$ με έναν αυτομορφισμό τάξης 2 (οποιονδήποτε). Ουσιαστικά $Aut(\mathbb{Z}_2 \times \mathbb{Z}_2) \cong S_3$, δηλαδή όλες οι μεταθέσεις των τριών στοιχείων τάξης 2.

(4) $G_1, G_2, G_3 \cong \mathbb{Z}_4 \times \mathbb{Z}_2$.

Έστω $i \in G_1, j \in G_2$ με την Συνθήκη (*), οπότε εφόσον δεν είναι στο κέντρο, έχουμε $|i| = |j| = 4$. Τα τετράγωνα τους είναι στο κέντρο από τις ιδιότητες της $\mathbb{Z}_4 \times \mathbb{Z}_2$, επομένως έστω $i^2 = z_1, j^2 = z_2$. Ακόμη $ij \in G_3$, άρα $|ij| = 4$ και άρα $z_3 = (ij)^2$. Αυτό σημαίνει ότι $z_3 = (ij)^2 = ijij = iz'ij^2 = z'i^2z_2 = z'z_1z_2$. Λύνοντας ως προς z' παίρνουμε ότι $z' = z_1z_2z_3$. Αφού $z' \neq e$ (αν $abc \neq e$, τότε τουλάχιστον 2 στοιχεία είναι ίσα), και έχουμε τα εξής ενδεχόμενα:
(α) όλα από τα z_1, z_2, z_3 είναι ίσα, ή (β) δύο είναι ίσα.

(α) Σ' αυτήν την περίπτωση έχουμε $z' = z_1z_2z_3 = z_1^3 = z_1$, και φτιάχνουμε το σύνολο

$$H = \{e, i, z_1, z_1i = i^{-1}, j, z_1j = j^{-1}, ij, z_1ij = ji = (ij)^{-1}\}.$$

Το H είναι υποομάδα με αντίστροφο όπως φαίνεται (για παράδειγμα $ij(ji) = ij^2i = iz_1i = ii^2i = i^4 = e$) και είναι κλειστή. Έπειτα παίρνουμε ένα $z \neq z_1$, και την ομάδα $\{e, z\} = \langle z \rangle = K$. Ακόμη έχουμε ότι $H \cap K = \{e\}$, και $|HK| = |H||K|/|H \cap K| = 8 * 2/1 = 16$ οπότε $HK = G$. Επίσης αφού η K είναι υποομάδα του κέντρου, $hk = kh$ για κάθε $h \in H, k \in K$. Άρα η G είναι ευθύ εσωτερικό γινόμενο της $H \cong Q_8$ και $K \cong \mathbb{Z}_2$, άρα $G \cong H \times K \cong Q_8 \times \mathbb{Z}_2$. Η G γράφεται ως

$$G = \{i^\alpha j^\beta z^\gamma : i^2 = j^2, i^4 = j^4 = z^2 = e, ji = i^{-1}j, zi = iz, jz = zj\}.$$

(β) Χωρίς περιορισμό της γενικότητας υποθέτουμε ότι $z_2 = z_3$ (μπορούμε να το κάνουμε γιατί σ' αυτήν την περίπτωση $z' = z_1z_2z_3 = z_1$ και όταν $z_1 = z_2$, τότε $z' = z_1z_2z_3 = z_3$ ή $z_1 = z_3$ που σ' αυτήν την περίπτωση $z' = z_1z_2z_3 = z_1z_3z_2 = z_2$, άρα οποιαδήποτε δύο από τα i, j ή ij έχουν τα τετράγωνά τους ίσα, πάντα παίρνουμε το τρίτο ως αντιμεταθέτη). Επομένως $\langle i \rangle = \{e, i, z_1, z_1i\}$ και $\langle j \rangle = \{e, j, z_2, z_2j\}$. Για αυτές τις 2 υποομάδες $\langle i \rangle \cap \langle j \rangle = \{e\}$, και $|\langle i \rangle||\langle j \rangle| = |\langle i \rangle||\langle j \rangle|/|\langle i \rangle \cap \langle j \rangle| = 4 * 4/1 = 16$, άρα έχουμε 16 αποτελέσματα της μορφής $i^\alpha j^\beta$ και κανόνα αντιμετάθεσης $ji = z'ij = i^2ij = i^{-1}j$. Η ομάδα γράφεται ως

$$G = \{i^\alpha j^\beta : i^4 = j^4 = e, ji = i^{-1}j\}$$

και αυτό είναι ημιευθύ γινόμενο των $\mathbb{Z}_4$ και $\mathbb{Z}_4$, $G \cong \mathbb{Z}_4 \times_\alpha \mathbb{Z}_4$, όπου το $\mathbb{Z}_4$ δρα με έναν αυτομορφισμό τάξης 2 ου απεικονίζει τον γεννήτορα στον αντίστροφό του.

Δεύτερη Περίπτωση: $Z(G) \cong \mathbb{Z}_4$

Αφού $Z(G) \cong \mathbb{Z}_4$, ξέρουμε ότι κάθε G_i περιέχει μια υποομάδα ισόμορφη με την $\mathbb{Z}_4$. Εφόσον όλες οι G_i είναι αβελιανές και ξέρουμε ότι η $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ δεν έχει υποομάδα ισόμορφη με την $\mathbb{Z}_4$, άρα οι μόνες πιθανές κατηγορίες ισομορφισμού είναι οι $\mathbb{Z}_8$ και $\mathbb{Z}_4 \times \mathbb{Z}_2$. Επομένως έχουμε 4 ενδεχόμενα :(α) και οι 3 $G_i \cong \mathbb{Z}_4 \times \mathbb{Z}_2$, (β) 2 $G_i \cong \mathbb{Z}_4 \times \mathbb{Z}_2$, (γ) μια $G_i \cong \mathbb{Z}_4 \times \mathbb{Z}_2$, και (δ) καμία $G_i \cong \mathbb{Z}_4 \times \mathbb{Z}_2$.

(α) $G_1, G_2, G_3 \cong \mathbb{Z}_4 \times \mathbb{Z}_2$.
Έστω g_1, g_2 με την Συνθήκη (*) και έστω $|g_1| = |g_2| = 2$. Επίσης $g_1 g_2 \in G_3$ δεν είναι στο κέντρο, οπότε η τάξη του είναι 4 ή 2. Παίρνουμε $(g_1 g_2)^2 = z' {g_1}^2 {g_2}^2 = z'$. Αν $z' \in Z(G) \cong \mathbb{Z}_4$, έχει τάξη 4, τότε $|g_i g_j| = 8$ το οποίο συνεπάγεται $G_3 \cong \mathbb{Z}_8$ οπότε $|g_i g_j| = 4$ και $|z'| = 2$. Αν επιλέξουμε έναν γεννήτορα $z \in Z(G)$, (ώστε $z^2 = z'$ και $\langle z \rangle = Z(G)$) τότε $G_1 = Z(G) \cup g_1 Z(G)$, άρα κάθε στοιχείο στην G_1 γράφεται σαν $z^\alpha g_1^\beta$ (αλλά αφού $|g_1| = 2$, τότε $\beta = 0$ (αν είναι στο $Z(G)$) ή $\beta = 1$ (αν είναι στι $g_1 Z(G)$)). Έπειτα έχουμε $\langle g_2 \rangle = \{e, g_2\}$ και $G_1 \cap \langle g_2 \rangle = e$. Άρα η ομάδα $G_1 \langle g_2 \rangle$ έχει τάξη $|G_1 \langle g_2 \rangle| = |G_1||\langle g_2 \rangle|/|G_1 \cap \langle g_2 \rangle| = 2 * 8/1 = 16$. Άρα έχουμε 16 γινόμενα της μορφής $z^\alpha g_1^\beta g_2^\gamma$, με κανόνα αντιμετάθεσης $g_2 g_1 = z' g_1 g_2 = z^2 g_1 g_2$ και χρησιμοποιώντας το έχουμε την αναπαράσταση της

$$G = \{z^\alpha g_1^\beta g_2^\gamma : z^4 = g_1^2 = g_2^2 = e, g_1 z = z g_1, g_2 z = z g_2 g_2 g_1 = z^2 g_1 g_2\}.$$

Αυτή είναι η ομάδα των πινάκων Pauli, $\mathcal{S}U(2)$.

(β) $G_1 \cong \mathbb{Z}_8, G_2, G_3 \cong \mathbb{Z}_4 \times \mathbb{Z}_2$
Όπως και πριν, επιλέγουμε g_2, g_3 με την Συνθήκη (*), να έχουν και τα δύο τάξη 2. Ακόμη, $g_2 g_3 \in G_1$ δεν είναι στο κέντρο αλλά έστω τώρα $g_2 g_3$ να είναι τάξης 8. Άρα $(g_1 g_2)^2 = z'$ έχει τάξη 4. Διατυπώνουμε το ακόλουθο θεώρημα το οποίο δείχνει ότι αυτό είναι αδύνατο.

Θεώρημα 2.2.10. *Αν ο αντιμεταθέτης μεταξύ δυο στοιχείων είναι στο κέντρο, τότε θα πρέπει να είναι στοιχείο τάξης 2(ή το e).*

Απόδειξη. Ανεξάρτητα από το ποιες G_i είναι ισόμορφες με την $\mathbb{Z}_4 \times \mathbb{Z}_2$ ή την $\mathbb{Z}_8$, όταν υψώσουμε ένα στοιχείο στο τετράγωνο, παίρνουμε ένα στοιχείο της $Z(G)$ (αφού υψώνοντας ένα στοιχείο στο τετράγωνο στην $\mathbb{Z}_8$ μας πηγαίνει στην μόνη ομάδα τάξης 4, που σ' αυτή την περίπτωση είναι το κέντρο, και τετραγωνίζοντας ένα στοιχείο στην $\mathbb{Z}_4 \times \mathbb{Z}_2$ παίρνουμε είτε $(0,0)$ είτε $(2,0)$ τα οποία στις 3 υποομάδες τάξης 4). Σύμφωνα με την Συνθήκη (*) για τα g_i, g_j παίρνουμε $g_j g_i^2 = g_i^2 g_j$. Παρόλα αυτά χρησιμοποιώντας τον κανόνα αντιμετάθεσης έχουμε

$$g_j g_i^2 = z' g_i g_j g_i = (z')^2 g_i^2 g_j$$

και άρα $g_i^2 g_j = {z'}^2 {g_i}^2 g_j$ από το οποίο έχουμε $e = (z')^2$ άρα $|z'| = 2$ ή $z' = e$. □

(γ) $G_1, G_2 \cong \mathbb{Z}_8, G_3 \cong \mathbb{Z}_4 \times \mathbb{Z}_2$
Παίρνουμε πάλι στοιχεία g_1, g_2 με την Συνθήκη (*). Αφού δεν ανήκουν στην υποομάδα της $G_2 \cong \mathbb{Z}_8$ τάξης 4 (το οποίο είναι το κέντρο), έχουν τάξη 8. Έστω $g_1^2 = z$, άρα $z \in Z(G)$ και $|z| = 4$. Επιπλέον μπορούμε να επιλέξουμε ένα $g_2 \in G_2$ τέτοιο ώστε $|g_2| = 8$ και $g_2^2 = z$. Αν πάρουμε τώρα ένα $g_3 = g_1 g_2$ και z' να είναι ο αντιμεταθέτης των g_2, g_1, τότε $g_3 \in G_3$ και άρα το $|g_3| = 4$ ή 2. Ακόμη,

$$g_3^2 = (g_1 g_2)^2 = z' g_1^2 g_2^2 = z' z^2.$$

Τώρα αν ο αντιμεταθέτης z' είναι τάξης 4, τότε $g_3^2 = z$ ή $g_3^2 = z^3$ (εξαρτάται αν $z' = z$ ή $z' = z^{-1}$). Σε κάθε περίπτωση αυτό θα σήμαινε ότι $|g_3^2| = 4$ (z και z^3 έχουν τάξη 4) και άρα $|g_3| = 8$. Άρα $G_3 \cong \mathbb{Z}_8$, που είναι άτοπο. Άρα z' πρέπει να είναι τάξης 2 και αφού $Z(G) \cong \mathbb{Z}_4, z' = z^2$. Επομένως $g_3^2 = z' z^2 = z^4 = e$ και

$|g_3| = 2$. Άρα $\langle g_3\rangle = \{e, g_3\}$ είναι υποομάδα τάξης 2 και παρατηρούμε ότι αφού $\langle g_1\rangle = G_1, |G_1\langle g_3\rangle| = |G_1||\langle g_3\rangle|/|G_1 \cap \langle g_3\rangle| = 8 * 2/1 = 16$. Άρα έχουμε 16 γινόμενα της μορφής $g_1^\alpha g_2^\beta$ και αφού

$$g_3g_1 = (g_1g_2)g_1 = g_1(g_2g_1) = g_1(z'g_1g_2) = z'g_1(g_1g_2) = z'g_1g_3,$$

έχουμε τον κανόνα αντιμετάθεσης: $g_3g_1 = z'g_1g_3 = z^2g_1g_3 = g_1^4g_1g_3 = g_1^5g_3$. Μια παράσταση της G είναι:

$$G = \{g_1^\alpha g_2^\beta : g_1^8 = g_3^2 = e, g_3g_1 = g_1^5g_3\}.$$

Αυτή είναι η ομάδα του Isanowa ή Modular Group οφ τάξης 16, M_{16}.

(δ) $G_1, G_2, G_3 \cong \mathbb{Z}_8$
Με τη γνωστή διαδικασία, επιλέγουμε πάλι g_2, g_3 με τη Συνθήκη (*) με $|g_2| = 8 = |g_3|$ και $g_2^2 = z = g_3^2$. Έχουμε $g_1 = g_2g_3$ με $g_1 \in G_1, |g_1| = 8$ και $g_1^2 = (g_2g_3)^2 = z'z^2$. Αν η τάξη του z' είναι 2 τότε $|g_1| = 2$ το οποίο έρχεται σε αντίφαση για την τάξη του g_1, άρα $|z'| = 4$. Τότε $z' = z^{\pm 1}$. Θα δείξουμε ότι αυτό είναι άτοπο.

(i) Έστω $z' = z$. Τότε $g_2g_3 = zg_3g_2$. Πολλαπλασιάζουμε και τις δυο μεριές επί g_2 από τα αριστερά:

$$g_2^2g_3 = zg_2g_3g_2 \Rightarrow zg_3 = z^2g_3g_2^2 = z^3g_3 \Rightarrow z^2 = e \text{ (Άτοπο)}.$$

(ii) Έστω $z' = z^{-1}$. Τότε $g_2g_3 = z^{-1}g_3g_2$. Πολλαπλασιάζουμε και τις δυο μεριές επί g_3 από τα δεξιά:

$$g_2g_3^2 = z^{-1}g_3g_2g_3 \Rightarrow zg_2 = z^{-2}g_2g_3^2 = z^{-1}g_2 \Rightarrow z^2 = e \text{ (Άτοπο)}.$$

Άτοπο άρα δεν υπάρχουν ομάδες με αυτήν την ιδιότητα.

2.2δ′ $|Z(G)| = 2$

Σ′ αυτήν την περίπτωση $Z(G) \cong \mathbb{Z}_2$. Τότε η κεντρική ομάδα πηλίκο έχει τάξη $|G/Z(G)| = |G|/|Z(G)| = 16/2 = 8$, οπότε η $G/Z(G)$ είναι ισόμορφη με μια από τις ομάδες τάξης 8, άρα έχουμε 5 περιπτώσεις: (α) $\mathbb{Z}_8$, (β) $\mathbb{Z}_4 \times \mathbb{Z}_2$, (γ) $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$, (δ) D_8 ή (ε) Q_8.

(α) $\underline{G/Z(G) \cong \mathbb{Z}_8}$
Σ άυτή την περίπτωση η κεντρική ομάδα πηλίκο είναι κυκλική, άρα η ομάδα είναι αβελιανή (Θεώρημα 2.2.6) και $Z(G) = G$ άρα $|Z(G)| = 16$ το οποίο αποκλείει το $|Z(G)| = 2$. Επομένως $G/Z(G) \ncong \mathbb{Z}_8$

(β) $\underline{G/Z(G) \cong \mathbb{Z}_4 \times \mathbb{Z}_2}$
Η $\mathbb{Z}_4 \times \mathbb{Z}_2$ έχει τρεις υποομάδες, δύο ισόμορφες με την $\mathbb{Z}_4$(η οποία έχει μια υποομάδα ισόμορφη με την $\mathbb{Z}_2$) και μια υποομάδα $\cong \mathbb{Z}_2 \times \mathbb{Z}_2$ (η οποία έχει 3 υποομάδες $\cong \mathbb{Z}_2$). Από το θεώρημα αντιστοιχιών αυτό σημαίνει ότι υπάρχουν 3 υποομάδες τάξης 8 που περιέχουν το κέντρο, δύο από τις οποίες έχουν μια υποομάδα τάξης 4 που περιέχει το κέντρο (έστω G_1, G_2) και μια υποομάδα τάξης 8 η οποία περιέχει 3 υποομάδες τάξης 4 μαζί και το κέντρο (έστω G_3). Ακολουθεί το θεώρημα:

Θεώρημα 2.2.11. *Αν $|Z(G)| = 2$ και η G_i περιέχει μια υποομάδα τάξης 4, και το κέντρο, τότε η G_i είναι είτε ισόμορφη με την $\mathbb{Z}_8$ ή με την $\mathbb{Z}_4 \times \mathbb{Z}_2$*

Απόδειξη. Γνωρίζουμε ότι το κέντρο του G_i περιέχει το $Z(G)$ (Θεώρημα 2.2.1). Όμως, από τις ιδιότητες των ομάδων τάξης 8, βλέπουμε ότι οι μη-αβελιανές ομάδες (D_8 και Q_8) έχουν 3 υποομάδες που περιέχουν το κέντρο, άρα ομάδες μ' αυτήν την ιδιότητα δεν είναι αβελιανές. Επίσης δεν μπορεί να είναι ισόμορφες με την $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$, διότι κάθε υποομάδα τάξης 2 περιέχεται σε 3 υποομάδες τάξης 4 και όχι 1. Ακόμη, αν $G_i \cong \mathbb{Z}_4 \times \mathbb{Z}_2$ τότε θα πρέπει να περιέχεται στην υποομάδα ισόμορφη με την $\mathbb{Z}_2 \times \mathbb{Z}_2$, αφού οι δύο υποομάδες ισόμορφες με την $\mathbb{Z}_4$ μοιράζονται την ίδια υποομάδα τάξης 2. Οι μόνες επιλογές είναι λοιπόν, $G_i \cong \mathbb{Z}_8, \mathbb{Z}_4 \times \mathbb{Z}_2$. □

Έτσι, αφού οι G_1, G_2 έχουν 1 υποομάδα τάξης 4 και περιέχουν το κέντρο, είναι αβελιανές (από την ταξινόμηση των ομάδων τάξης 8). Αποδεικνύουμε τώρα ότι αυτό μας οδηγεί σε αντίφαση.

Θεώρημα 2.2.12. *Αν η G έχει δύο G_i αβελιανές (θα μπορούσε ακόμα να είναι ισόμορφες με την $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$), τότε το κέντρο έχει τάξη τουλάχιστον 4.*

Απόδειξη. Έστω G_i, G_j διακεκριμένες και αβελιανές. Τότε $G_iG_j = G$, επειδή $|G_iG_j| = |G_i||G_j|/|G_i \cap G_j| = 8 * 8/4 = 16$ και, αφού είναι αβελιανές, κάθε στοιχείο στην $G_i \cap G_j$ αντιμετατίθεται με κάθε στοιχείο στην G_i και G_j. Ακόμη, αν $g \in G_i \cap G_j$, τότε το g αντιμετατίθεται με κάθε στοιχείο στην G_iG_j (το g αντιμετατίθεται με όλα τα $g_i \in G_i$, $g_j \in G_j$, και ένα αυθαίρετο στοιχείο στην G_iG_j το g_ig_j, και $g(g_ig_j) = (gg_i)g_j = (g_ig_j)g$). Αφού αντιμετατίθεται με κάθε στοιχείο στην ομάδα, είναι και στο κέντρο. Αυτό σημαίνει ότι κάθε στοιχείο στην $G_i \cap G_j$ είναι στο κέντρο, και καθώς υπάρχουν 4 στοιχεία στην $G_i \cap G_j$, θα πρέπει να υπάρχουν 4 στοιχεία στο κέντρο. □

Αφού έχουμε δυο αβελιανές ομάδες G_1, G_2) το κέντρο θα πρέπει να είναι τουλάχιστον τάξης 4, αλλά αυτό σημαίνει ότι το κέντρο δεν είναι τάξης 2. Ως εκ τούτου $G/Z(G) \ncong \mathbb{Z}_4 \times \mathbb{Z}_2$

(γ) $\underline{G/Z(G) \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2}$
Αφού κάθε στοιχείο στην ομάδα πηλίκο έχει τάξη 2, $Z(G) = (gZ(G))^2 = g^2Z(G)$ άρα κάθε στοιχείο υψωμένο στο τετράγωνο είναι στο κέντρο. Ακόμη εφόσον η ομάδα δεν είναι αβελιανή, υπάρχει ένα στοιχείο g για το οποίο δεν ισχύει $g^2 = e$. Αλλά, $g^2 \in Z(G)$ και παίρνουμε $g^2 = z$. Έχουμε ότι

$$\langle g \rangle = \{e, g, g^2 = z, g^3 = zg\}$$

είναι μια υποομάδα που περιέχει το κέντρο. Άρα από το Θεώρημα Αντιστοιχιών υπάρχει μια ομάδα πηλίκο τάξης 2 στην $G/Z(G)$ (σ' αυτή την περίπτωση, $\langle gZ(G) \rangle = \{Z(G), gZ(G)\}$). Αυτή η ομάδα περιέχεται στις τρεις υποομάδες τάξης 4 (καθεμιά υποομάδα τάξης 2 περιέχεται σε τρεις υποομάδες στην $G/Z(G) \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$). Ονομάζουμε τις υποομάδες αυτές G_1, G_2, G_3 και έστω τουλάχιστον 2 από αυτές να είναι μη αβελιανές (αν δύο από αυτές είναι αβελιανές δίνει ότι το κέντρο έχει τάξη 4). Χωρίς περιορισμό της γενικότητας, υποθέτουμε ότι G_2, G_3 είναι μη αβελιανές. Τότε αν $g_2 \in G_2$, $g_3 \in G_3$ δεν ανήκουν στην τομή (που σ' αυτή την περίπτωση είναι το $\langle g \rangle$) τότε $g_2g_3 \in G_1$ και δεν ανήκει στο $\langle g \rangle$. Έτσι αφού $g \notin Z(G_3), Z(G_3)$, παίρνουμε ένα $z, g_2g = zgg_2$(ομοίως και για το g_3). Έχουμε

$$(g_2g_3)g = g_2(g_3g) = g_2(zgg_3) = z(g_2g)g_3 = z(zgg_2)g_3 = z^2g(g_2g_3) = g(g_2g_3).$$

Άρα το g αντιμετατίθεται με το $g_2g_3 \in G_1$, και το g αντιμετατίθεται με $\langle g\rangle \cup (g_2g_3)\langle g\rangle$, που είναι 8 στοιχεία στην G_1, άρα ισούται με G_1, άρα $g_1 \in Z(G_1)$ και το κέντρο της G_1 έχει τουλάχιστον 3 στοιχεία (g, e, z) οπότε θα πρέπει να είναι αβελιανή. Το κέντρο δεν έχει στοιχεία τάξης 8, γιατί δεν ισχύει $g^2 = z$ και η $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ δεν έχει στοιχεία τάξης 4, άρα $G_1 \cong \mathbb{Z}_4 \times \mathbb{Z}_2$.

Έστω τώρα $g_1 \in Z(G), g_1 \notin \langle g\rangle$. Αν το $h_2 \in G_2$ αντιμετατίθεται με το g_1 τότε ${g_1}^{\alpha}{h_2}^{\beta}g^{\gamma}$ είναι αβελιανή ομάδα με 8 στοιχεία, αφού όλα αντιμετατίθενται με όλα, και περιέχει 8 στοιχεία για κάθε ελληνικό γράμμα τότε $G_i = \{{g_i}^{\alpha}{h_2}^{\beta}z^{\gamma}\}$ είναι αβελιανή. Έχουμε 2 αβελιανές ομάδες τάξης 8 στην περίπτωσή μας. Αυτόο δίνει ότι $|Z(G)| \geq 4$ το οποίο είναι άτοπο γιατί $|Z(G)| = 2$. Άρα h_2 δεν αντιμετατίθεται με το g_1. Παρατηρούμε όμως ότι g_1g δεν είναι στην $\langle g\rangle$ (αφού τότε $g_1 = g^{-1}g^n = g^{n-1}$ θα είναι στην $\langle g\rangle$). Αλλά $gg_1g_2 = g(zg_2g_1) = z(gg_2)g_1 = z^2g_2gg_1 = g_2(gg_1)$ και το g_2 αντιμετατίθεται με το gg_1 το οποίο είναι άτοπο.

(δ) $\underline{G/Z(G) \cong Q_8}$
Από τις ιδιότητες της Q_8, η ομάδα πηλίκο έχει τρεις υποομάδες τάξης 4, και η καθεμία έχει 1 υποομάδα τάξης 2. Από το Θεώρημα Αντιστοιχιών, αυτό συνεπάγεται ότι υπάρχουν 3 υποομάδες τάξης 8 στην G, και η καθεμιά με μία υποομάδα τάξης 4 (τις ονομάζουμε G_i). Από το Θεώρημα 2.2.11 και οι 3 υποομάδες είναι αβελιανές, και αφού υπάρχουν 2 αβελιανές G_i, το κέντρο θα είναι τάξης 4 και όχι τάξης 2, το οποίο είναι άτοπο. Άρα καμιά ομάδα τάξης 16 δεν έχει αυτή την ιδιότητα.

(ε) $\underline{G/Z(G) \cong D_8}$
Στην περίπτωση αυτή η ομάδα πηλίκο έχει μια υποομάδα τάξης 4 με 1 υποομάδα τάξης 2 και 2 υποομάδες τάξης 4 με 3 υποομάδες τάξης 2. Από το θεώρημα αντιστοιχιών, έχουμε 1 υποομάδα τάξης 8 με μια υποομάδα τάξης 4 που περιέχει το κέντρο (θα την ονομάσουμε G_1 και $G_1 \cong \mathbb{Z}_8$ ή $G_1 \cong \mathbb{Z}_4 \times \mathbb{Z}_2$ από το Θεώρημα 2.2.11) και 2 υποομάδες τάξης 8 με τρεις υποομάδες που περιέχουν το κέντρο (έστω G_2, G_3). Οι G_2, G_3 είναι μη-αβελιανές, αφού αν ήταν αβελιανές το κέντρο θα είχε τάξη 4. Πριν καθορίσουμε αυτές τις υποομάδες θα πρέπει να δούμε πώς αυτά τα στοιχεία αντιμετατίθεται. Ορίζουμε την υποομάδα αντιμεταθέσεων:

Ορισμός 2.2.13. *Η υποομάδα αντιμεταθέσεων G', ορίζεται ως*

$$G' = \langle ghg^{-1}h^{-1} : g, h \in G\rangle,$$

δηλαδή είναι η υποομάδα της G που παράγεται από τους μεταθέτες.

Παρατήρηση 2.2.14. (i) *Έχουμε ότι $G' \triangleleft G$ και G/G'' είναι αβελιανή.*

(ii) *Η G'' έχει την εξής καθολική ιδιότητα: Έστω $f : G \to A$ ένας ομομορφισμός και A είναι αβελιανή ομάδα. Τότε υπάρχει ομομορφισμός $\phi : G/G' \to A$ έτσι ώστε $f = \phi \circ p$, όπου $p : G \to G/G'$ είναι η κανονική προβολή.*

Παρατηρούμε ότι $Z(G) \subset Z(G_2)$ (Θεώρημα 2.2.1) και σ' αυτές τις μη αβελιανές ομάδες τάξης 8, το κέντρο έχει τάξη 2, άρα $Z(G) = Z(G_2)$. Ακόμη, το κέντρο περιέχεται στον αντιμεταθέτη, σύμφωνα με τις ιδιότητες των ομάδων αυτών. Αν $G_2 \cong D_8$ τότε $z = r^2$ είναι ένα μη-τετριμμένο στοιχείο του κέντρου, και $z = r^2 = srs^{-1}r^{-1}$. Άρα $z \in G'$. Αν $G_2 \cong Q_8$ τότε $z = -1 = i^2$ είναι μη-τετριμμένο στοιχείο του κέντρου και $z = -1 = i^2 = iji^{-1}j^{-1} \in G'$. Έστω $Z(G/Z(G)) = \{Z(G), g'Z(G)\}$. Αυτό σημαίνει ότι το $g'Z(G)$ παριστά το r^2 στην D_8. Αν επιλέξουμε $g_1Z(G)$, $g_2Z(G)$ στην $G/Z(G)$ έτσι ώστε να μην αντιμετατίθενται, τότε από τις ιδιότητες της D_8, ο μεταθέτης τους είναι ένα στοιχείο του κέντρου. Δηλαδή

$$g_1g_2Z(G) = (g_1Z(G))(g_2Z(G)) = (g'Z(G))(g_2Z(G))(g_1Z(G)) = g'g_2g_1Z(G).$$

Άρα $g_1g_2 = g'z_0g_2g_1$, με $z_0 \in Z(G)$. Άρα $g' = z_0g_1^{-1}g_2^{-1} \in G'$, γατί $z_0 \in Z(G) < G'$. Όμοια $zg' \in G'$. Παρατηρούμε ότι αυτά το σύνολο $\{1, z, g', zg'\}$ αποτελεί ομάδα και ότι δεν υπάρχουν άλλοι γεννήτορες της G'. Κι αυτό γιατί αν c ήταν ένας μεταθέτης, $gh = chg$. Αν $c \in Z(G) = \{e, z\}$, τελειώσαμε. Αν $c \notin Z(G)$, τότε $gZ(G)$, $hZ(G)$ δεν αντιμετατίθενται στην $G/Z(G)$. Από τους παραπάνω υπολογισμούς, $c = g'z_0$, με $z_0 \in Z(G)$. Αυτό σημαίνει ότι $c \in \{g', zg'\}$, ολοκληρώνοντας τον ισχυρισμό. Έτσι δεν έχουμε άλλους γεννήτορες και $G' = \{e, z, g', zg'\}$. Παρατηρούμε ακόμη ότι G' αντιστοιχεί στο κέντρο της $G/Z(G)$ και το κέντρο περιέχεται στις 4 υποομάδες τάξης 4 και άρα από το Θεώρημα Αντιστοιχιών αυτή η υποομάδα είναι και στις 3 υποομάδες τάξης 8 και περιέχει το κέντρο ($G' \subset G_1, G_2, G_3$) και επειδή $|G_i \cap G_j| = 4$, η τομή δύο G_i είναι η G'.

Θεώρημα 2.2.15. *Αν $G/Z(G) \cong D_8$ τότε μια από τις G_i είναι κυκλική.*

Απόδειξη. Ήδη γνωρίζουμε ότι $G_1 \cong \mathbb{Z}_8$ ή $\mathbb{Z}_4 \times \mathbb{Z}_2$, οπότε θα το αποδείξουμε με επαγωγή σε άτοπο. Υποθέτουμε ότι $G_1 \cong \mathbb{Z}_4 \times \mathbb{Z}_2$. Αυτό σημαίνει ότι η υποομάδα τάξης 4 που περιέχει το κέντρο, είναι ισόμορφη με την $\mathbb{Z}_2 \times \mathbb{Z}_2$. Γνωρίζουμε ότι G_2, G_3 είναι μη-αβελιανές, οπότε είναι ισόμορφες με τις Q_8, D_4. Όμως καμιά από τις ομάδες δεν είναι ισόμορφη με την Q_8. Κι αυτό γιατί οι υποομάδες τάξης 4 στην Q_8 είναι κυκλικές, και αυτό σημαίνει ότι $G' = G_1 \cap G_i \cong \mathbb{Z}_4$ είναι κυκλική το οποίο έρχεται σε αντίφαση με το ότι είναι η $\mathbb{Z}_2 \times \mathbb{Z}_2$. Αυτό αποκλείει λοιπόν ότι $G_2, G_3 \cong D_8$. Επειδή υπάρχουν 5 στοιχεία τάξης 2 στην D_8, επιλέγουμε ένα g_2 τέτοιο ώστε $|g_2| = 2$. Για $g_1 \in G_1$ (και g' ο αντιμεταθέτης g' των g_2, g_1), τότε

$$g_1 = {g_2}^2g_1 = g_2g'g_1g_2 = zg'g_2g_1g_2 = zg'g'g_1{g_2}^2 = z{g'}^2g_1$$

(σημειώνουμε ότι $g', g_2 \in G_2$ αντιμετατίθεται με στοιχείο του κέντρου από τις ιδιότητες των ομάδων τάξης 8). Αποκλείουμε το g_1 και $e = {g'}^2z$ άρα ${g'}^2 = z^{-1} = z$ (ως αντίστροφος στοιχείο τάξης 2 είναι το ίδιο το στοιχείο), επομένως $|g'| = 4$. Αλλά αυτό έρχεται σε αντίφαση με το ότι ομάδα τάξης 4 που περιέχει το κέντρο είναι ισόμορφη με την $\mathbb{Z}_4 \times \mathbb{Z}_2$, οπότε δεν υπάρχει τρόπος για την $G_1 \cong \mathbb{Z}_4 \times \mathbb{Z}_2$. ☐

Τώρα που γνωρίζουμε ότι $G_1 \cong \mathbb{Z}_8$, έχουμε τα εξής 3 περιπτώσεις: (α) $G_2, G_3 \cong Q_8$, (β) $G_2 \cong Q_8, G_3 \cong D_8$ ή (γ) $G_2, G_3 \cong D_8$

(α) $G_2, G_3 \cong Q_8$
Έστω g_1, g_2 με την Συνθήκη (*). Αφού $G_1 \cong \mathbb{Z}_8$ έχει την ίδια υποομάδα τάξης 4 με την $G_2 \cong Q_8$. Τότε έχουμε $g_1^4 = (g')^2 = g_2^2 = z$. Επίσης, $g_1g_2 \in G_3$. Άρα

$$\begin{aligned} z &= (g_1g_2)^2 = g_1g_2g_1g_2 = g_1g'g_1g_2g_2 = g'g_1^2z \Rightarrow e = g'{g_1}^2 \Rightarrow \\ g' &= (g_1^2)^{-1} = {g_1}^{-2} = g_1^6. \end{aligned}$$

Αν πάρουμε $\langle g_1 \rangle = G_1$ και $\langle g_2 \rangle = \{e, g_2, z, zg_2\}$ (άρα $G_1 \cap \langle g_2 \rangle = \{e, z\}$) και παίρνουμε το $G_1\langle g_2 \rangle$, τότε η τάξη του είναι $|G_1\langle g_2 \rangle| = ||G_2||\langle g_2 \rangle|/|G_1 \cap \langle g_2 \rangle| = 8 * 4/2 = 16$. Επομένως υπάρχουν 16 στοιχεία της μορφής $g_1^\alpha g_2^\beta$ και κανόνας αντιμετάθεσης $g_2g_1 = g'g_1g_2 = g_1^6g_1g_2 = {g_1}^7g_2 = g_1^{-1}g_2$. Άρα η ομάδα αναπαρίσταται ως

$$G = \{g_1^\alpha g_2^\beta : g_1^4 = g_2^2, g_1^8 = g_2^4 = e, g_2g_1 = g_1^{-1}g_2\}.$$

Αυτή είναι η δικυκλική ομάδα βαθμού 4, Dic_4.

(β) $G_2 \cong D_8, G_3 \cong Q_8$
Έστω g_1, g_3 με την Συνθήκη (*), και $g_1 g_3 \in G_2 \cong D_8$ δεν είναι στην κυκλική ομάδα τάξης 4, άρα έχει τάξη 2, $(g_1 g_3)^2 = e$. Αυτό σημαίνει ότι

$$e = (g_1 g_3)^2 = g_1 g_3 g_1 g_3 = g_1 g' g_1 g_3^2 = g_1^2 g' (g_1^4) = g' g_1^6 \Rightarrow g' = (g_1^6)^{-1} = g_1^{-6} = g_1^2.$$

Αν τώρα $g_2 = g_1 g_3$, τότε για να ορίσουμε τον αντιμεταθέτη μεταξύ των g_2 και g_1 παίρνουμε $g_2 g_1 = g_1 g_3 g_1 = g_1 g' g_1 g_3 = g_1^2 g_1 (g_1 g_3) = g_1^3 g_2$, και έχουμε ότι αφού $|g_2| = 2, \langle g_2 \rangle = \{e, g_2\}$, και $\langle g_1 \rangle = G_1$ και $|G_1 \langle g_2 \rangle| = |G_1| \langle g_2 \rangle|/|G_1 \cap < g_2 > | = 8 * 2/1 = 16$ άρα έχουμε 16 στοιχεία της μορφής ${g_1}^\alpha {g_2}^\beta$, και χρησιμοποιώντας τις τάξεις και τον κανόνα αντιμετάθεσης έχουμε την ομάδα

$$G = \{g_1^\alpha g_2^\beta : g_1^8 = g_2^2 = e, g_2 g_1 = g_1^3 g_2\}.$$

Αυτή είναιη ημιδιεδρική ομάδα βαθμού 2, SD_2.

(γ) $G_2, G_3 \cong D_8$
Έστω τώρα $g_1 \in G_1, g_2 \in G_2$ με την Συνθήκη (*). Ο g' είναι ο αντιμεταθέτης τους και $g_2 g_1 = g' g_1 g_2$ και $|g_2| = 2$. Αφού $g_1 g_2 \in G_3 \cong D_8$ και δεν ανήκει σε κυκλική ομάδα τάξης 4, $|g_1 g_2| = 2$. Ακόμη

$$e = (g_1 g_2)^2 = g_1 g_2 g_1 g_2 = g_1 g' g_1 {g_2}^2 = g' g_1^2 \Rightarrow g' = (g_1^2)^{-1} = g_1^6.$$

Έπειτα έχουμε $\langle g_1 \rangle = G_1$ και $\langle g_2 \rangle = \{e, g_2\}$ άρα $|G_1 \langle g_2 \rangle| = |G_1||\langle g_2 \rangle|/|G_1 \cap \langle g_2 \rangle| = 8 * 2/1 = 16$. Επομένως υπάρχουν 16 στοιχεία της μορφής ${g_1}^\alpha {g_2}^\beta$ με κανόνα αντιμετάθεσης $g_2 g_1 = g' g_1 g_2 = g_1^6 g_1 g_2 = g_1^7 g_2 = g_1^{-1} g_2$ και η ομάδα είναι

$$G = \{g_1^\alpha g_2^\beta : g_1^8 = g_2^2 = e, g_2 g_1 = g_1^{-1} g_2\}.$$

Αυτή είναι η διεδρική ομάδα τάξης 16, D_8.

ΠΙΝΑΚΑΣ

Τάξη	Ομάδες
1	$\{1\}$
2	$\mathbb{Z}_2$
3	$\mathbb{Z}_3$
4	$\mathbb{Z}_2,\ \mathbb{Z}_2\times\mathbb{Z}_2$
5	$\mathbb{Z}_5$
6	$\mathbb{Z}_6,\ S_3 \cong D_3$
7	$\mathbb{Z}_7$
8	$\mathbb{Z}_8,\ \mathbb{Z}_4\times\mathbb{Z}_2,\ \mathbb{Z}_2\times\mathbb{Z}_2\times\mathbb{Z}_2,$ $D_8,\ Q_8 = \{\pm 1, \pm i, \pm j, \pm k\} = \langle x, y :\ x^4 = e, x^2 = y^2, y^{-1}xy = x^{-1}\rangle$
9	$\mathbb{Z}_9,\ \mathbb{Z}_3\times\mathbb{Z}_3$
10	$\mathbb{Z}_{10},\ D_5$
11	$\mathbb{Z}_{11}$
12	$\mathbb{Z}_{12},\ \mathbb{Z}_2\times\mathbb{Z}_2\times\mathbb{Z}_3,\ D_{12},\ A_4,$ $T = \langle a, b :\ a^6 = e, b^2 = a^3 = (ab)^2\rangle$
13	$\mathbb{Z}_{13}$
14	$\mathbb{Z}_{14},\ D_7$
15	$\mathbb{Z}_{15}$
16	$\mathbb{Z}_{16},\ \mathbb{Z}_8\times\mathbb{Z}_2,\ \mathbb{Z}_4\times\mathbb{Z}_4,\ \mathbb{Z}_4\times\mathbb{Z}_2\times\mathbb{Z}_2,\ \mathbb{Z}_2\times\mathbb{Z}_2\times\mathbb{Z}_2\times\mathbb{Z}_2,\ D_8,\ D_8\times\mathbb{Z}_2,\ Q_8\times\mathbb{Z}_2,$ $M_{16} = \langle a, x :\ a^8 = x^2 = e, xax^{-1} = a^5\rangle,\ SD_2 = \langle a, x :\ a^8 = x^2 = e, xax^{-1} = a^3\rangle$ $\mathbb{Z}_4 \rtimes \mathbb{Z}_4 = \langle a, b :\ a^4 = b^4 = e, bab^{-1} = a^3\rangle,$ $(\mathbb{Z}_2\times\mathbb{Z}_2)\rtimes\mathbb{Z}_4 = \langle a, b, c :\ a^4 = b^2 = c^2 = e, ab = ba, bc = cb, cac^{-1} = ab\rangle,$ $\mathcal{S}U(2) = \langle a, x, y :\ a^4 = x^2 = e, a^2 = y^2, xax = a^{-1}, ay = ya, xy = yx\rangle,$ $Dic_4 = \langle a, b :\ a^8 = e, b^2 = a^4, b^{-1}ab = a^{-1}\rangle$

Βιβλιογραφία

[1] Clausen, D. *Classifying All Groups of Order 16*,

`http://buzzard.ups.edu/courses/2012spring/projects/clausen-groups-16-ups-434-2012.pdf.`

[2] Hungerford, Thomas W. *Algebra*. Reprint of the 1974 original. Graduate Texts in Mathematics, 73. Springer-Verlag, New York-Berlin, 1980.

[3] Judson, Thomas W. *Abstract Algebra: Theory and Applications*, LaVergne, TN: PWS Publishing Company, 2010 Edition.