ΠΑΝΕΠΙΣΤΗΜΙΟ ΙΩΑΝΝΙΝΩΝ
ΑΝΟΙΚΤΑ ΑΚΑΔΗΜΑΪΚΑ ΜΑΘΗΜΑΤΑ

Τίτλος Μαθήματος: Θεωρία Ομάδων

Ενότητα: Θεωρία Sylow

Διδάσκων: Καθηγητής Νικόλαος Μαρμαρίδης

Τμήμα: Μαθηματικών

Ευρωπαϊκή Ένωση
Ευρωπαϊκό Κοινωνικό Ταμείο
ΕΠΙΧΕΙΡΗΣΙΑΚΟ ΠΡΟΓΡΑΜΜΑ
ΕΚΠΑΙΔΕΥΣΗ ΚΑΙ ΔΙΑ ΒΙΟΥ ΜΑΘΗΣΗ
επένδυση στην κοινωνία της γνώσης
ΥΠΟΥΡΓΕΙΟ ΠΑΙΔΕΙΑΣ & ΘΡΗΣΚΕΥΜΑΤΩΝ, ΠΟΛΙΤΙΣΜΟΥ & ΑΘΛΗΤΙΣΜΟΥ
ΕΙΔΙΚΗ ΥΠΗΡΕΣΙΑ ΔΙΑΧΕΙΡΙΣΗΣ
Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης
ΕΣΠΑ 2007-2013
πρόγραμμα για την ανάπτυξη
ΕΥΡΩΠΑΪΚΟ ΚΟΙΝΩΝΙΚΟ ΤΑΜΕΙΟ

Κεφάλαιο 2

Θεωρία Sylow

2.1 Τα Θεωρήματα Sylow

Ορισμός 2.1.1. Μια ομάδα $(G, \star)$ τάξης p^{α}, όπου p είναι ένας πρώτος αριθμός και $\alpha \in \mathbb{N} \cup \{0\}$ ονομάζεται μια *p–ομάδα.*

Παρατηρήσεις 2.1.1. (α′) Σύμφωνα με τον προηγούμενο ορισμό, η τετριμμένη ομάδα που αποτελείται από ένα και μόνο στοιχείο είναι p–ομάδα για κάθε πρώτο p.

(β′) Αν κάθε στοιχείο μιας πεπερασμένης ομάδας $G \neq \{e_G\}$ είναι δύναμη ενός πάγιου πρώτου αριθμού, τότε η G είναι μια p–ομάδα. Πράγματι, ο πρώτος αριθμός p διαιρεί την τάξη $[G : 1]$, αφού υπάρχουν στοιχεία με τάξη δύναμη τού συγκεκριμένου p. Αν q είναι ένας πρώτος διαιρέτης τής $[G : 1]$, τότε από το Θεώρημα Cauchy, βλ. Θ. 1.3.2, υπάρχει ένα στοιχείο τής G τάξης q. Συνεπώς, $q = p$ και η τάξη $[G : 1]$ είναι δύναμη τού p.

Για τις p–ομάδες ισχύουν τα ακόλουθα:

Πρόταση 2.1.1. *Έστω ότι $(G, \star)$ είναι μια p-ομάδα τάξης p^α, $\alpha \in \mathbb{N} \cup \{0\}$.*

(α′) Για κάθε $\beta \in \mathbb{N} \cup \{0\}$ με $\beta \leq \alpha$, υπάρχει μια υποομάδα $H \leq G$ με τάξη p^β.

(β′) Αν $\alpha \in \mathbb{N}$, τότε κάθε υποομάδα H τής G τάξης $p^{\alpha-1}$ είναι μια ορθόθετη υποομάδα τής G και επιπλέον, υπάρχει μια αλυσσίδα υποομάδων:

$$G_0 = \{e_G\} \trianglelefteq G_1 \trianglelefteq G_2 \trianglelefteq \cdots \trianglelefteq G_{\alpha-1} \trianglelefteq G_\alpha = G$$

με $[G_i : 1] = p^i, i = 0, \ldots, \alpha$ και όπου $\forall i, 0 \leq i \leq \alpha - 1$ η G_i είναι μια ορθόθετη υποομάδα τής G_{i+1}.

Απόδειξη. (α′) Θα εκτελέσουμε την απόδειξη με επαγωγή ως προς τη δύναμη $\alpha \in \mathbb{N} \cup \{0\}$ τού p. Για $\alpha = 0, 1$ ή 2, ο ισχυρισμός είναι προφανής. Έστω ότι η πρόταση είναι αληθής $\forall m, 2 \leq m < n$. Θα την αποδείξουμε για μια ομάδα G τάξης p^n.
Από το Θεώρημα 1.4.2 γνωρίζουμε ότι το κέντρο $Z(G)$ τής G είναι μη τετριμμένο. Ας είναι $x \in Z(G), x \neq e_G$ ένα στοιχείο τού κέντρου. Τότε η κυκλική υποομάδα $\langle x \rangle$ είναι μια ορθόθετη υποομάδα τής G.
Θεωρούμε τον φυσικό επιμορφισμό $\pi : G \to G/\langle x \rangle, g \mapsto g\langle x \rangle$. Η τάξη τής πηλικοομάδας $G/\langle x \rangle$ είναι p^{n-1} και λόγω τής επαγωγικής υπόθεσης διαθέτει $\forall \beta \in \mathbb{N} \cup \{0\}, 0 \leq \beta \leq n-1$, μια υποομάδα $\overline{H}$ τάξης p^β. Τότε η προεικόνα της $H = \pi^{-1}(\overline{H})$ είναι μια υποομάδα τής G τάξης $p^{\beta+1}$. Συνεπώς, η G διαθέτει $\forall \beta \in \mathbb{N} \cup \{0\}, 0 \leq \beta \leq n$, μια υποομάδα τάξης p^β.

(β′) Σύμφωνα με το (α′) υπάρχει μια αλυσσίδα υποομάδων

$$G_0 = \{e_G\} \leq G_1 \leq G_2 \leq \cdots \leq G_{\alpha-1} \leq G_\alpha = G,$$

όπου $\forall i, 0 \leq i \leq \alpha$, η τάξη τής G_i είναι p^i. Παρατηρούμε ότι $\forall i, 1 \leq i \leq \alpha$ ο δείκτης $[G_i : G_{i-1}]$ ισούται με τον πρώτο αριθμό p και επειδή πρόκειται για τον μικρότερο πρώτο που διαιρεί την τάξη τής ομάδας (αφού δεν υπάρχει άλλος), έπεται από το Πόρισμα 1.3.2 ότι η G_{i-1} είναι ορθόθετη υποομάδα τής G_i. □

Η προηγούμενη πρόταση γενικεύεται στη λεγόμενη Θεωρία Sylow που θα διαπραγματευθούμε τώρα αμέσως.

Ορισμός 2.1.2. Έστω ότι $(G, \star)$ είναι μια ομάδα τάξης $p^\alpha m$, όπου p είναι ένας πρώτος αριθμός, $\alpha \in \mathbb{N} \cup \{0\}$ και $p \nmid m$. Κάθε υποομάδα τής G τάξης p^α ονομάζεται μια *p–Sylow υποομάδα* τής G.

Συμβολίζουμε με $\mathrm{Syl}_p(G)$ το σύνολο των p–Sylow υποομάδων τής G και με $n_p(G)$, ή απλώς με n_p όταν είναι σαφές για ποια ομάδα πρόκειται, το πλήθος των στοιχείων τού συνόλου $\mathrm{Syl}_p(G)$.

Θα αποδείξουμε ένα από τα σημαντικότερα θεωρήματα τής κλασικής Θεωρίας Ομάδων

Θεώρημα 2.1.1 (Sylow). *Έστω ότι $(G, \star)$ είναι μια ομάδα τάξης $p^\alpha m$, όπου p είναι ένας πρώτος αριθμός, $\alpha \in \mathbb{N} \cup \{0\}$ και $p \nmid m$. Τότε ισχύουν τα επόμενα:*

(α′) *Το σύνολο $\mathrm{Syl}_p(G)$ δεν είναι κενό.*

(β′) *Αν P είναι οποιαδήποτε p–Sylow υποομάδα τής G και Q είναι οποιαδήποτε p–υποομάδα τής G, τότε υπάρχει $g \in G$ με $Q \leq gPg^{-1}$. Ιδιαιτέρως, όλες οι p–Sylow υποομάδες τής G είναι συζυγείς.*

(γ′) *Για το πλήθος $n_p(G)$ των p–Sylow υποομάδων τής G έχουμε:*

$$n_p(G) \equiv 1 \mathrm{mod} p \text{ και } n_p(G) = [G : N_G(P)],$$

όπου $P \in \mathrm{Syl}_p(G)$ και $N_G(P) = \{g \in G \mid gPg^{-1}\}$ είναι ο ορθοθέτης τής P. Ιδιαιτέρως, $n_G(P) \mid m$.

Πριν από την απόδειξη τού θεωρήματος αποδεικνύουμε το

Λήμμα 2.1.1. *Αν P είναι μια p–Sylow υποομάδα τής G και Q είναι οποιαδήποτε p–υποομάδα τής G, τότε $N_G(P) \cap Q = P \cap Q$.*

Απόδειξη. Θέτουμε $H = N_G(P) \cap Q$. Από $P \leq N_G(P)$ έπεται ότι $P \cap Q \leq N_G(P) \cap Q = H$. Συνεπώς, για να δειχθεί η ισότητα τού λήμματος είναι αρκετό να δειχθεί ότι το $H = N_G(P) \cap Q$ περιέχεται στο $P \cap Q$. Αλλά $H \leq Q$ και γι' αυτό υπολείπεται η απόδειξη ότι $H \leq P$.

Θα αποδείξουμε ότι:

(Π) *Το σύνολο PH είναι μια υποομάδα τής G και μάλιστα μια p–υποομάδα.*

Κατόπιν, από $P \leq PH$ συμπεραίνουμε ότι $P = PH$, αφού η τάξη τής P είναι η μεγαλύτερη δύναμη τού p που διαιρεί την τάξη $[G : 1] = p^\alpha m$. Τέλος, από $P = PH$, συμπεραίνουμε ότι $H \leq P$ που ολοκληρώνει την απόδειξη.

Η απόδειξη τής (Π) Επειδή $H \leq N_G(P)$, έχουμε $\forall h \in H, hP = Ph$ και γι' αυτό η PH είναι μια υποομάδα τής G.

Για το πλήθος των στοιχείων τής PH γνωρίζουμε, βλ. Πρόταση 1.3.1, ότι

$$\mid PH \mid = \frac{\mid P \mid\mid H \mid}{\mid P \cap H \mid}. \tag{*}$$

Ο αριθμητής τής σχέσης (*) είναι δύναμη τού p, επειδή και η $\mid P \mid$ είναι δύναμη τού p, αφού η P είναι p–Sylow υποομάδα τής G, και η $\mid H \mid$ είναι δύναμη τού p, αφού η H είναι μια p–υποομάδα, ως υποομάδα τής p–υποομάδας Q. Για τους ίδιους λόγους και ο παρονομαστής τής σχέσης (*) είναι μια δύναμη τού p.

Συνεπώς, η PH είναι μια p–υποομάδα. □

Είμαστε τώρα σε θέση να αποδείξουμε τον πρώτο ισχυρισμό τού Θεωρήματος Sylow, βλ. Θ. 2.1.1:

(α′) *Το σύνολο* $\mathrm{Syl}_p(G)$ *δεν είναι κενό.*

Απόδειξη. Η απόδειξη θα εκτελεστεί με επαγωγή ως προς $[G:1]$. Αν $[G:1]=1$ δεν χρειάζεται να αποδειχθεί κάτι. Ας δούμε τι συμβαίνει στην περίπτωση $[G:1]=2$. Η G είναι μια 2–ομάδα και $Syl_2(G)=\{G\}$.

Έστω ότι ο ισχυρισμός είναι αληθής για κάθε ομάδα G' με τάξη $[G':1]<[G:1]$, δηλαδή ότι $\mathrm{Syl}_p(G')\neq\emptyset$, όταν $p\mid[G':1]$.

Για την ομάδα G, θεωρούμε την Εξίσωση των Κλάσεων, βλ. Θεώρημα 1.4.2:

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

όπου τα στοιχεία g_j διατρέχουν τους αντιπροσώπους από τις κλάσεις συζυγίας με περισσότερα τού ενός στοιχεία. Συνεπώς, $\forall j, 1\leq j\leq \ell$, $[G:C_G(g_j)]\geq 2$

Αν ο πρώτος p διαιρεί την τάξη τού κέντρου $Z(G)$, τότε υπάρχει $g\in Z(G), g\neq e_G$. Η κυκλική υποομάδα $\langle g\rangle$ περιέχεται στο $Z(G)$ και συνεπώς είναι ορθόθετη. Θεωρούμε τον κανονικό επιμορφισμό $\pi: G\to G/\langle x\rangle$. Η τάξη τής $G/\langle x\rangle$ ισούται με $[G:1]/p=p^{\alpha-1}m$. Λόγω της επαγωγικής υπόθεσης η $G/\langle x\rangle$ διαθέτει μια υποομάδα P' τάξης $p^{\alpha-1}$. Τώρα η υποομάδα $P=\pi^{-1}(P')$ τής G έχει τάξη p^{α} και $P\in\mathrm{Syl}_p(G)$.

Αν ο πρώτος p δεν διαιρεί την τάξη τού κέντρου $Z(G)$, τότε δεν διαιρεί τουλάχιστον για ένα $k, 1\leq k\leq\ell$ κάποιον προσθετέο $[G:C_G(g_k)]\geq 2$. Επειδή

$$p^{\alpha}m=[G:1]=[G:C_G(g_k)][C_G(g_k):1],$$

έπεται ότι ο p^{α} διαιρεί την τάξη $[C_G(g_k):1]$, η οποία είναι γνησίως μικρότερη από την τάξη $[G:1]$ τής G. Λόγω τής επαγωγικής υπόθεσης, η υποομάδα $C_G(g_k)$ διαθέτει μια p–Sylow υποομάδα P τάξης p^{α}. Η P ως έχουσα τάξη p^{α} είναι μια p–Sylow υποομάδα τής G. □

Πριν προχωρήσουμε στην απόδειξη των (β′) και (γ′) τού Θεωρήματος 2.1.1 θα κάνουμε ορισμένες παρατηρήσεις.

Ήδη έχουμε αποδείξει ότι $\mathrm{Syl}_p(G)\neq\emptyset$. Έστω ότι P είναι μια υποομάδα με $P\in\mathrm{Syl}_p(G)$ και ότι

$$\mathcal{S}=\{gPg^{-1}\mid g\in G\}=\{P_1,P_2,\ldots,P_r\}$$

είναι το σύνολο των υποομάδων τής G που είναι συζυγείς τής P. Οποιαδήποτε υποομάδα H τής G δρά μέσω συζυγίας επί τού $\mathcal{S}$, δηλαδή

$$H\times\mathcal{S}\to\mathcal{S}, (h,P_i)\mapsto hP_ih^{-1}$$

και διαμερίζει το $\mathcal{S}$ σε s το πλήθος τροχιές $\mathcal{O}_i, 1\leq i\leq s$ και συνεπώς $r=\sum_{i=1}^{s}|\mathcal{O}_i|$. Προσέξτε, ότι ενώ το πλήθος r των στοιχείων τού $\mathcal{S}$ είναι σταθερό, το πλήθος s των τροχιών μπορεί να μεταβάλλεται, ανάλογα με την υποομάδα H. Για παράδειγμα, αν $H=G$, τότε $s=1$, ενώ αν $H=\{e_G\}$, τότε $s=r$. Σε κάθε περίπτωση βέβαια, $s\leq r$.

Επιλέγουμε ως H μια p–υποομάδα Q τής G και αριθμούμε εκ νέου, αν είναι απαραίτητο, τα στοιχεία τού $\mathcal{S}$ έτσι, ώστε τα πρώτα s να είναι οι αντιπρόσωποι των διαφορετικών τροχιών $\mathcal{O}_i, 1 \leq i \leq s$ τής δράσης συζυγίας $Q \times \mathcal{S} \longrightarrow \mathcal{S}$. Από το Θεώρημα 1.2.1 γνωρίζουμε ότι το πλήθος των στοιχείων τής τροχιάς $\mathcal{O}_i$ ισούται με τον δείκτη $[Q : N_Q(P_i)]$, αφού ο σταθερωτής τού P_i ως προς τη δράση τής συζυγίας είναι ο ορθοθέτης $N_Q(P_i) = \{q \in Q \mid qP_iq^{-1} = P_i\}$. Παρατηρούμε ότι $N_Q(P_i) = N_G(P_i) \cap Q$ και επειδή από το Λήμμα 2.1.1 γνωρίζουμε ότι $N_G(P_i) \cap Q = P_i \cap Q$, συμπεραίνουμε ότι $N_Q(P_i) = P_i \cap Q$. Συνεπώς,

$$\mid \mathcal{O}_i \mid = [Q : P_i \cap Q], \forall i, 1 \leq i \leq s.$$

Θα δείξουμε ότι για το πλήθος $\mid \mathcal{S} \mid$ *των στοιχείων τού συνόλου* $\mathcal{S}$ *ισχύει*

$$\mid \mathcal{S} \mid \equiv 1 \bmod p.$$

Απόδειξη. Επιλέγουμε να δράσει μέσω συζυγίας επί τού $\mathcal{S}$ η p–Sylow υποομάδα P_1, η οποία είναι βεβαίως και στοιχείο τού $\mathcal{S}$.

Για το πλήθος των στοιχείων τής τροχιάς $\mathcal{O}_1$, έχουμε $|\mathcal{O}_1| = [P_1 : P_1 \cap P_1] = 1$. (Θυμηθείτε με ποιον τρόπο αριθμούμε κάθε φορά τα στοιχεία τού $\mathcal{S}$).
Ενώ για το πλήθος των στοιχείων οποιασδήποτε άλλης τροχιάς $\mathcal{O}_i, i \geq 2$, έχουμε $|\mathcal{O}_i| = [P_1 : P_i \cap P_1] \geq 2$. Αυτό είναι αληθές, επειδή η τομή $P_i \cap P_1$ περιέχεται γνήσια εντός τής P_i, αφού αν, $P_i \cap P_1 = P_i$, τότε θα ήταν $P_i = P_1$, διότι τα P_i και P_1 έχουν το ίδιο πλήθος στοιχείων. Συνεπώς για κάθε $i, 2 \leq i \leq s$, το πλήθος $|\mathcal{O}_i| = [P_1 : P_i \cap P_1]$ είναι μια θετική δύναμη n_i τού πρώτου αριθμού p, αφού είναι ένας διαιρέτης ≥ 2 τής τάξης $[P_1 : 1] = p^{\alpha}$.

Τώρα είναι

$$\mid \mathcal{S} \mid = \sum_{i=1}^{s} \mid \mathcal{O}_i \mid = 1 + p^{n_2} + \cdots + p^{n_s}, \text{ όπου } n_i \in \mathbb{N}, \forall i = 2, \ldots, s.$$

Ώστε,

$$\mid \mathcal{S} \mid \equiv 1 \bmod p.$$

□

Θα αποδείξουμε τώρα τα (β′) και (γ′) τού Θεωρήματος 2.1.1.

> (β′) *Αν P είναι οποιαδήποτε p–Sylow υποομάδα τής G και Q είναι οποιαδήποτε p–υποομάδα τής G, τότε υπάρχει $g \in G$ με $Q \leq gPg^{-1}$. Ιδιαιτέρως, όλες οι p–Sylow υποομάδες τής G είναι συζυγείς.*

Απόδειξη. Έστω μια p–υποομάδα Q και P μια σταθερώς επιλεγμένη p–Sylow υποομάδα τής G. Αν δεν υπάρχει $g \in G$ με $Q \leq gPg^{-1}$, τότε η Q δεν περιέχεται σε κανένα από τα στοιχεία τού $\mathcal{S} = \{gPg^{-1} \mid g \in G\} = \{P_1, P_2, \ldots, P_r\}$. Επομένως, $\forall i, 1 \leq i \leq r, Q \cap P_i \lneqq Q$ και γι' αυτό $\forall i, 1 \leq i \leq r, [Q : Q \cap P_i] \gneqq 1$. Επομένως, $\forall i, 1 \leq i \leq r$, ο δείκτης $[Q : Q \cap P_i]$ είναι μια θετική δύναμη τού πρώτου p, επειδή η Q είναι μια p–υποομάδα τής G. Τότε όμως επιτρέποντας να δράσει η Q μέσω συζυγίας επί τού $\mathcal{S}$ διαπιστώνουμε ότι ο p διαιρεί το πλήθος των στοιχείων οποιασδήποτε τροχιάς $\mathcal{O}$, αφού το πλήθος $|\ \mathcal{O}\ |$ ισούται με τον δείκτη $[Q : Q \cap P_i]$, όπου P_i είναι οποιοδήποτε στοιχείο τής τροχιάς $\mathcal{O}$. Τότε όμως ο p διαιρεί και το πλήθος $|\ \mathcal{S}\ |$, το οποίο μόλις προηγουμένως είδαμε ότι ικανοποιεί την $|\ \mathcal{S}\ | \equiv 1 \mathrm{mod} p$. Αυτό είναι άτοπο. Επομένως, υπάρχει $g \in G$ με $Q \leq gPg^{-1}$.

Επιλέγοντας ως Q οποιαδήποτε p–Sylow υποομάδα P', διαπιστώνουμε ότι $\exists g \in G$ με $P' \leq gPg^{-1}$ και αφού πρόκειται για πεπερασμένα σύνολα με το ίδιο πλήθος στοιχείων , έπεται $P' = gPg^{-1}$. Συνεπώς, οποιαδήποτε p–Sylow υποομάδα είναι συζυγής με την P και $\mathrm{Syl}_p(G) = \mathcal{S} = \{gPg^{-1} \mid g \in G\}$. □

(γ′) *Για το πλήθος $n_p(G)$ των p–Sylow υποομάδων τής G έχουμε:*

$$n_p(G) \equiv 1 \mathrm{mod} p \text{ και } n_p(G) = [G : N_G(P)],$$

όπου $P \in \mathrm{Syl}_p(G)$ και $N_G(P) = \{g \in G \mid gPg^{-1}\}$ είναι ο ορθοθέτης τής P.
Ιδιαιτέρως, $n_p(G) \mid m$.

Απόδειξη. Προηγουμένως διαπιστώσαμε ότι $\mathrm{Syl}_p(G) = \mathcal{S} = \{gPg^{-1} \mid g \in G\}$. Αφού $|\ \mathcal{S}\ | \equiv 1 \mathrm{mod} p$ και $n_p(G)$ είναι το πλήθος των στοιχείων τού $\mathrm{Syl}_p(G)$, συμπεραίνουμε ότι $n_p(G) \equiv 1 \mathrm{mod} p$.

Στο σύνολο $\mathrm{Syl}_p(G)$ δρα μέσω συζυγίας και η ίδια η ομάδα G και μάλιστα μεταβατικώς. Το πλήθος $n_p(G)$ των στοιχείων τής μοναδικής τροχιάς ως προς αυτή τη δράση ισούται με τον δείκτη $[G : N_G(P)]$ τού σταθερωτή $N_G(P)$ οποιουδήποτε στοιχείου $P \in \mathrm{Syl}_p(G)$. Επομένως, $n_p(G) \mid p^{\alpha} m$ και αφού $n_p(G) \equiv 1 \mathrm{mod} p$, συμπεραίνουμε ότι $n_p(G) \mid m$. □

Παραδείγματα 2.1.1. Έστω ότι $(G, \star)$ είναι μια πεπερασμένη ομάδα και ότι p είναι ένας πρώτος αριθμός.

(α′) Αν $p \nmid [G : 1]$, τότε $\mathrm{Syl}_p(G) = \{e_G\}$.

(β′) Αν $[G : 1] = p^n$, τότε $\mathrm{Syl}_p(G) = \{G\}$.

(γ′) Αν A είναι μια αβελιανή ομάδα, τότε για κάθε πρώτο διαιρέτη p τής τάξης τής A, υπάρχει ακριβώς μία p–Sylow υποομάδα. Πράγματι, το σύνολο των p–Sylow υποομάδων $\mathrm{Syl}_p(G)$ δεν είναι κενό και δύο οποιεσδήποτε p–Sylow υποομάδες P, P' που ανήκουν σε αυτό είναι συζυγείς. Δηλαδή, υπάρχει $a \in A$ με $aP'a^{-1} = P$. Επειδή η A είναι μια αβελιανή ομάδα, έχουμε $aP'a^{-1} = P'aa^{-1} = P'$. Επομένως, $P' = P$.

2.2 Εφαρμογές τής Θεωρίας Sylow

Εφαρμογη **2.2.1.** *Οι Sylow υποομάδες τής συμμετρικής ομάδας* $(S_3, \circ)$.

Η τάξη τής S_3 είναι $[S_3 : 1] = 3! = 2 \cdot 3$.

Για το πλήθος n_3 των 3–Sylow υποομάδων γνωρίζουμε ότι

$$n_3 \equiv 1 \bmod 3 \;\text{ και } n_3 \mid 2 \Rightarrow n_3 = 1.$$

Συνεπώς, η S_3 έχει μια ορθόθετη υποομάδα τάξης 3. Πρόκειται για την εναλλάσσουσα υποομάδα $\mathbb{A}_3$. Για το πλήθος n_2 των 2–Sylow υποομάδων γνωρίζουμε ότι

$$n_2 \equiv 1 \bmod 2 \;\text{ και } n_2 \mid 3 \Rightarrow n_2 = 1 \text{ ή } 3.$$

Συνεπώς, η S_3 έχει ή μία ορθόθετη υποομάδα τάξης 2 ή τρεις υποομάδες τάξης 2. Αλλά αφού έχει τουλάχιστον δύο διαφορετικά στοιχεία τάξης 2, που προφανώς δεν μπορεί να ανήκουν στην ίδια υποομάδα τάξης 2, έπεται ότι έχει τρεις υποομάδες τάξης 2. Πρόκειται για τις υποομάδες $\langle\begin{pmatrix}1 & 2\end{pmatrix}\rangle$, $\langle\begin{pmatrix}1 & 3\end{pmatrix}\rangle$ και $\langle\begin{pmatrix}2 & 3\end{pmatrix}\rangle$.

Εφαρμογη **2.2.2.** *Οι Sylow υποομάδες τής εναλλάσσουσας υποομάδας $\mathbb{A}_4$ τής συμμετρικής ομάδας $(S_4, \circ)$.*

Η τάξη τής $\mathbb{A}_4$ είναι $[S_4 : 1]/2 = 4!/2 = 12 = 2^2 \cdot 3$.

Για το πλήθος n_2 των 2–Sylow υποομάδων γνωρίζουμε ότι

$$n_2 \equiv 1 \bmod 2 \;\text{ και } n_2 \mid 3 \Rightarrow n_2 = 1 \text{ ή } 3.$$

Αλλά μεταξύ των υποομάδων τής $\mathbb{A}_4$, οι οποίες εχουν τάξη 4 είναι και η

$$V = \{\mathrm{Id}_{S_4}, \begin{pmatrix}1 & 2\end{pmatrix}\circ\begin{pmatrix}3 & 4\end{pmatrix}, \begin{pmatrix}1 & 3\end{pmatrix}\circ\begin{pmatrix}2 & 4\end{pmatrix}, \begin{pmatrix}1 & 4\end{pmatrix}\circ\begin{pmatrix}2 & 3\end{pmatrix},\}$$

Η συγκεκριμένη υποομάδα V είναι μια 2–Sylow υποομάδα τής $\mathbb{A}_4$ και επιπλέον είναι ορθόθετη υποομάδα τής $\mathbb{A}_4$. Επειδή κάθε 2–Sylow υποομάδα H τής $\mathbb{A}_4$ είναι συζυγής με την ορθόθετη V, έπεται ότι $H = V$ και γι' αυτό $n_2 = 1$

Για το πλήθος n_3 των 3–Sylow υποομάδων γνωρίζουμε ότι

$$n_3 \equiv 1 \bmod 3 \;\text{ και } n_3 \mid 4 \Rightarrow n_3 = 1 \text{ ή } 4.$$

Επειδή η $\mathbb{A}_4$ διαθέτει τουλάχιστον δύο υποομάδες τάξης 3, τις $\langle\begin{pmatrix}1 & 2 & 3\end{pmatrix}\rangle$ και $\langle\begin{pmatrix}1 & 2 & 4\end{pmatrix}\rangle$, έπεται ότι $n_3 \geq 2$ και επομένως $n_3 = 4$. Οι υπόλοιπες 3–Sylow υποομάδες είναι οι $\langle\begin{pmatrix}2 & 3 & 4\end{pmatrix}\rangle$ και $\langle\begin{pmatrix}1 & 3 & 4\end{pmatrix}\rangle$.

Εφαρμογη **2.2.3.** *Οι Sylow υποομάδες τής συμμετρικής ομάδας $(S_4, \circ)$.*

Η τάξη τής S_4 είναι $[S_4 : 1] = 4! = 2^3 \cdot 3$.

Για το πλήθος n_3 των 3–Sylow υποομάδων γνωρίζουμε ότι

$$n_3 \equiv 1 \bmod 3 \;\text{ και } n_3 \mid 8 \Rightarrow n_3 = 1 \text{ ή } 4, \text{ ή } 8.$$

Όμως κάθε 3–Sylow υποομάδα τής S_4 είναι τάξης 3 και παράγεται από έναν κύκλο μήκους 3. Γι' αυτό κάθε υποομάδα τάξης 3 είναι και υποομάδα τής $\mathbb{A}_4$. Όπως είδαμε στην αμέσως προηγούμενη εφαρμογή, η $\mathbb{A}_4$ έχει τέσσερεις 3–Sylow υποομάδες. Επομένως, $n_3 = 4$.

Για το πλήθος n_2 των 2–Sylow υποομάδων γνωρίζουμε ότι

$$n_2 \equiv 1 \bmod 2 \;\text{ και } n_2 \mid 3 \Rightarrow n_2 = 1 \text{ ή } 3.$$

Κάθε 2–Sylow υποομάδα τής S_4 έχει 8 οκτώ στοιχεία. Μεταξύ των υποομάδων τάξης 8 είναι και η διεδρική υποομάδα $D_4 = \langle \begin{pmatrix}1 & 2 & 3 & 4\end{pmatrix}, \begin{pmatrix}2 & 4\end{pmatrix} \rangle$, βλ. Παραδείγματα 1.1.1. Κάθε άλλη 2–Sylow υποομάδα είναι συζυγής τής D_4. Παρατηρούμε ότι η η υποομάδα $\langle \begin{pmatrix}1 & 2 & 4 & 3\end{pmatrix}, \begin{pmatrix}2 & 3\end{pmatrix} \rangle$ είναι συζυγής τής D_4 και δεν ταυτίζεται με αυτήν. Αφού λοιπόν έχουμε τουλάχιστον δύο διαφορετικές 2–Sylow υποομάδες τάξης, το πλήθος τους n_2 δεν ισούται με 1 και έτσι $n_2 = 3$. Η τρίτη 2–Sylow υποομάδα είναι η $\langle \begin{pmatrix}1 & 3 & 2 & 4\end{pmatrix}, \begin{pmatrix}3 & 4\end{pmatrix} \rangle$.

Εφαρμογη **2.2.4.** *Οι Sylow υποομάδες τής συμμετρικής ομάδας* $(S_5, \circ)$.

Η τάξη τής S_5 είναι $[S_5 : 1] = 4! = 2^3 \cdot 3 \cdot 5$.

Για το πλήθος n_5 των 5–Sylow υποομάδων γνωρίζουμε ότι

$$n_5 \equiv 1 \bmod 5 \;\text{ και } n_5 \mid 2^3 \cdot 3 = 24 \Rightarrow n_5 = 1 \text{ ή } 6.$$

Όμως κάθε 5–Sylow υποομάδα τής S_5 είναι τάξης 5 και παράγεται από έναν κύκλο μήκους 5. Αλλά υπάρχουν τουλάχιστον δύο διαφορετικές υποομάδες τής S_5 τάξης 5. Επί παραδείγματι, οι $\langle \begin{pmatrix}1 & 2 & 3 & 4 & 5\end{pmatrix} \rangle$ και $\langle \begin{pmatrix}1 & 2 & 4 & 3 & 5\end{pmatrix} \rangle$ είναι δύο διαφορετικές υποομάδες τάξης 5. Γι' αυτό $n_5 = 6$.

Για το πλήθος n_3 των 3–Sylow υποομάδων γνωρίζουμε ότι

$$n_3 \equiv 1 \bmod 3 \;\text{ και } n_3 \mid 2^3 \cdot 5 = 40 \Rightarrow n_3 = 1 \text{ ή } 4 \text{ ή } 10 \text{ ή } 40.$$

Το πλήθος των στοιχείων τάξης 3 τής S_5, δηλαδή των κύκλων μήκους 3 ισούται με $(5 \cdot 4 \cdot 3)/3 = 20$. Επομένως, $n_3 > 1$. Αν $n_3 = 4$, τότε το πλήθος των στοιχείων τάξης 3 ισούται με $4 \cdot 2 = 8$, επειδή η τομή δύο διαφορετικών κυκλικών ομάδων με τάξη πρώτο αριθμό ισούται πάντοτε με την τετριμμένη υποομάδα που αποτελείται από το ουδέτερο στοιχείο. Ώστε, $n_3 \neq 4$. Χρησιμοποιώντας το ίδιο επιχείρημα διαπιστώνουμε ότι είναι αδύνατο να έχουμε $n_3 = 40$, αφού τότε προκύπτουν $40 \cdot 2 = 80$ στοιχεία τάξης 3. Επομένως, $n_3 = 10$.

Για το πλήθος n_2 των 2–Sylow υποομάδων γνωρίζουμε ότι

$$n_2 \equiv 1 \bmod 2 \;\text{ και } n_2 \mid 3 \cdot 5 = 15 \Rightarrow n_2 = 1 \text{ ή } 3 \text{ ή } 5 \text{ ή } 15.$$

Κάθε 2–Sylow υποομάδα τής S_5 έχει $2^3 = 8$ στοιχεία. Επειδή κάθε υποομάδα τής S_4 είναι και υποομάδα τής S_5, οι 2–Sylow υποομάδες τής S_4, που έχουν 8 στοιχεία, είναι και 2–Sylow υποομάδες τής S_5. Γι' αυτό η S_5 έχει τουλάχιστον τις 2–Sylow υποομάδες τις

$$\langle \begin{pmatrix}1 & 2 & 3 & 4\end{pmatrix}, \begin{pmatrix}2 & 4\end{pmatrix} \rangle, \langle \begin{pmatrix}1 & 2 & 4 & 3\end{pmatrix}, \begin{pmatrix}2 & 3\end{pmatrix} \rangle \text{ και } \langle \begin{pmatrix}1 & 3 & 2 & 4\end{pmatrix}, \begin{pmatrix}3 & 4\end{pmatrix} \rangle.$$

Επιπλέον τρεις διαφορετικές από τις προηγούμενες 2–Sylow υποομάδες τής S_5 προκύπτουν αντικαθιστώντας, ας πούμε το 2 από το 5. Έτσι προκύπτουν οι

$$\langle \begin{pmatrix}1 & 5 & 3 & 4\end{pmatrix}, \begin{pmatrix}5 & 4\end{pmatrix} \rangle, \langle \begin{pmatrix}1 & 5 & 4 & 3\end{pmatrix}, \begin{pmatrix}5 & 3\end{pmatrix} \rangle \text{ και } \langle \begin{pmatrix}1 & 3 & 5 & 4\end{pmatrix}, \begin{pmatrix}3 & 4\end{pmatrix} \rangle.$$

Γι' αυτό $n_2 > 6$ και επομένως $n_2 = 15$.

Πρόταση 2.2.1. *Κάθε ομάδα $(G,\star)$ τάξης $2p$, όπου ο p είναι ένας περιττός πρώτος, είναι ισόμορφη ή με την κυκλική ομάδα $\mathbb{Z}_{2p}$ ή με τη διεδρική ομάδα D_p.*

Απόδειξη. Για το πλήθος n_p των p–Sylow υποομάδων τής G γνωρίζουμε ότι

$$n_p \equiv 1 \mathrm{mod} p \ \text{ και } n_p \mid 2 \Rightarrow n_p = 1.$$

Ώστε, υπάρχει μια ορθόθετη υποομάδα R τής G με τάξη τον πρώτο αριθμό p. Γι' αυτό $R = \langle \rho \rangle$, όπου η τάξη τού ρ ισούται με p.

Για το πλήθος n_2 των 2–Sylow υποομάδων τής G γνωρίζουμε ότι

$$n_2 \equiv 1 \mathrm{mod} 2 \ \text{ και } n_2 \mid p \Rightarrow n_2 = 1 \text{ ή } p.$$

Έστω S μια 2–Sylow υποομάδα τής G. Η S είναι κυκλική, δηλαδή $S = \langle s \rangle$ και η τάξη τού s ισούται με 2. Επειδή $R \cap S = \{e_G\}$, τα στοιχεία τής G

$$e_G, \rho, \rho^2, \ldots, \rho^{p-1}, s, s\rho, s\rho^2, \ldots, s\rho^{p-1}$$

είναι ανά δύο διαφορετικά και αφού το πλήθος τους ισούται με $2p$, έπεται ότι

$$G = \{e_G, \rho, \rho^2, \ldots, \rho^{p-1}, s, s\rho, s\rho^2, \ldots, s\rho^{p-1}\}.$$

Παρατηρούμε ότι το στοιχείο $s\rho s^{-1}$ οφείλει να ανήκει στην ορθόθετη υποομάδα R. Ας πούμε ότι $s\rho s^{-1} = \rho^i, 1 \leq i \leq p-1$. Τότε $s\rho^\ell s^{-1} = \rho^{i\ell}$. Λαμβάνοντας υπ' όψιν ότι $s^{-1} = s$ έχουμε $\rho = s(s\rho s)s = s\rho^i s^{-1} = (s\rho s^{-1})^i = \rho^{i^2}$ (*) και γι' αυτό $p \mid (i^2 - 1)$. Επομένως, $i = 1$ ή $i = p-1$.

Στην περίπτωση $i = 1$, η σχέση (*) δίνει $s\rho s^{-1} = \rho \Leftrightarrow s\rho = \rho s$ και η G είναι μια αβελιανή ομάδα. Επιπλέον, η απεικόνιση

$$\phi : R \times S \to G, (\alpha, \beta) \mapsto \alpha\beta$$

είναι ένας ομομορφισμός ομάδων με $\mathrm{Ker}\phi = \{e_G\}$, αφού $R \cap S = \{e_G\}$. Επειδή $[R \times S : 1] = 2p = [G : 1]$, ο ϕ είναι ισομορφισμός. Το ευθύ γινόμενο $R \times S$ είναι ισόμορφο με $\mathbb{Z}_p \times \mathbb{Z}_2$ που με τη σειρά του είναι ισόμορφο με την κυκλική ομάδα $\mathbb{Z}_{2p}$.

Στην περίπτωση $i = p-1$, η σχέση (*) δίνει $s\rho s^{-1} = \rho^{p-1} \Leftrightarrow \rho s = s\rho^{p-1}$. Έτσι η G ορίζεται μέσω γεννητόρων και σχέσεων ως

$$G = \langle \rho, s \mid \rho^p = e_G, s^2 = e_G, \rho s = s\rho^{p-1} \rangle$$

Συνεπώς, η G είναι ισόμορφη με τη διεδρική ομάδα D_p, που ορίζεται από δύο γεννήτορες, οι οποίοι ικανοποιούν ακριβώς τις σχέσεις που ικανοποιούν και οι γεννήτορες τής G. □

Πρόταση 2.2.2. *Κάθε ομάδα $(G,\star)$ τάξης pq, όπου οι p,q είναι πρώτοι αριθμοί με $p < q$ και $p \nmid q-1$, είναι ισόμορφη με την κυκλική ομάδα $\mathbb{Z}_{pq}$.*

Απόδειξη. Για το πλήθος n_p των p–Sylow υποομάδων τής G γνωρίζουμε ότι

$$n_p \equiv 1 \bmod p \ \text{ και } n_p \mid q \Rightarrow n_p = 1 \text{ ή } q.$$

Αλλά αν, $n_p = q$, τότε $q \equiv 1 \bmod p$. Πράγμα άτοπο, αφού $p \nmid q - 1$. Επομένως, $n_p = 1$ και έτσι υπάρχει μία ορθόθετη p–Sylow υποομάδα $P = \langle \alpha \rangle$ τής G, η οποία είναι κυκλική, αφού η τάξη της είναι ο πρώτος αριθμός p.

Για το πλήθος n_q των q–Sylow υποομάδων τής G γνωρίζουμε ότι

$$n_q \equiv 1 \bmod q \ \text{ και } n_q \mid p \Rightarrow n_q = 1 \text{ ή } p.$$

Όμως $p < q$ και έτσι $n_q = 1$. Συνεπώς, υπάρχει μία ορθόθετη q–Sylow υποομάδα $Q = \langle \beta \rangle$ τής G, η οποία είναι κυκλική, αφού η τάξη της είναι ο πρώτος αριθμός q.

Παρατηρούμε ότι $\alpha\beta = \beta\alpha$, επειδή το στοιχείο $\alpha\beta\alpha^{-1}\beta^{-1} = e_G$, αφού ανήκει στην τομή $P \cap Q = \{e_G\}$. Γι' αυτό ορίζεται η απεικόνιση $P \times Q \longrightarrow G$, $(\alpha^i, \beta^j) \mapsto \alpha^i\beta^j$, η οποία είναι μονομορφισμός και συνεπώς ισομορφισμός, διότι $[P \times Q : 1] = pq = [G : 1]$.

Επομένως η G είναι ισόμορφη με την ομάδα $\mathbb{Z}_p \times \mathbb{Z}_q \cong \mathbb{Z}_{pq}$. □

Αν $p \mid q - 1$, τότε αποδεικνύεται ότι υπάρχει μια μοναδική (με ακρίβεια ισομορφισμού) μη αβελιανή ομάδα τάξης pq.

Πρόταση 2.2.3. *Κάθε ομάδα $(G, \star)$ τάξης 12 διαθέτει μια μη τετριμμένη ορθόθετη υποομάδα τάξης 3 ή 4.*

Απόδειξη. Για το πλήθος n_3 των 3–Sylow υποομάδων τής G γνωρίζουμε ότι

$$n_3 \equiv 1 \bmod 3 \ \text{ και } n_3 \mid 4 \Rightarrow n_3 = 1 \text{ ή } 4.$$

Αν $n_3 = 1$, τότε βέβαια υπάρχει μία ορθόθετη υποομάδα τής G τάξης 3 που ικανοποιεί τον ισχυρισμό τής πρότασής μας.

Αν $n_3 \neq 1$, θα αποδείξουμε ότι το πλήθος n_2 των 2–Sylow υποομάδων τής G ισούται με 1 και γι' αυτό θα υπάρχει μία ορθόθετη υποομάδα τής G τάξης 4, η οποία θα ικανοποιεί τον ισχυρισμό τής πρότασής μας. Ας δούμε πως θα το πετύχουμε αυτό.

Αν $n_3 \neq 1 \Rightarrow n_3 = 4$ και ως εκ τούτου η G διαθέτει $4 \cdot 2 = 8$ στοιχεία τάξης 3. Αν P είναι οποιαδήποτε 3–Sylow υποομάδα, τότε γνωρίζουμε ότι κάθε άλλη 3–Sylow υποομάδα είναι συζυγής τής P και ότι το πλήθος τους n_3 ισούται με τον δείκτη $[G : N_G(P)]$. Επομένως, $4 = n_3 = [G : N_G(P)]$. Προσέξτε ότι επειδή $[G : P] = 4 = [G : N_G(P)]$ και αφού $P \leqq N_G(P)$, έχουμε $N_G(P) = P$.

Η G δρα μέσω συζυγίας πάνω στο σύνολο $\mathrm{Syl}_3(G)$ που έχει τέσσερα στοιχεία και η συγκεκριμένη δράση χορηγεί έναν ομομορφισμό

$$\chi : G \longrightarrow S_{\mathrm{Syl}_3(G)}, \text{ όπου } S_{\mathrm{Syl}_3(G)} \text{ η συμμετρική ομάδα τού συνόλου } \mathrm{Syl}_3(G).$$

Ένα στοιχείο $g \in G$ ανήκει στον $\mathrm{Ker}\chi$ αν, και μόνο αν, $\forall \overline{P} \in \mathrm{Syl}_3(G), g\overline{P}g^{-1} = \overline{P}$. Ιδιαιτέρως, $gPg^{-1} = P$ και γι' αυτό $g \in \mathrm{Ker}\chi \Rightarrow g \in N_G(P) = P$. Ώστε, $\mathrm{Ker}\chi \leq P$. Συνεπώς,

$\mathrm{Ker}\chi = \{e_G\}$ ή $\mathrm{Ker}\chi = P$, αφού $[P:1] = 3$. Αλλά $\mathrm{Ker}\chi \neq P$, διότι η P δεν είναι ορθόθετη υποομάδα[1] τής G. Επομένως, $\mathrm{Ker}\chi = \{e_G\}$ και η G είναι ισόμορφη με την εικόνα της $\chi(G)$. Συνεπώς, η εικόνα τής G περιέχει ακριβώς 8 στοιχεία τάξης 3. Ταυτίζοντας την $S_{\mathrm{Syl}_3(G)}$ με την S_4 παρατηρούμε ότι όλα τα στοιχεία τάξης 3 είναι άρτιες μετατάξεις και γι' αυτό περιέχονται στην εναλλάσσουσα υποομάδα $\mathbb{A}_4$. Γι' αυτό η τομή $\chi(G) \cap \mathbb{A}_4$, που είναι μια υποομάδα τής $\mathbb{A}_4$, έχει τουλάχιστον οκτώ στοιχεία. Αφού όμως $[\mathbb{A}_4 : 1] = 12$ συμπεραίνουμε, χρησιμοποιώντας το Θεώρημα Lagrange, ότι $\chi(G) \cap \mathbb{A}_4 = \mathbb{A}_4$ και αφού και η $\chi(G)$ έχει 12 στοιχεία, καταλήγουμε στο ότι $\chi(G) = \mathbb{A}_4$. Επομένως, $G \cong \mathbb{A}_4$. Αφού όμως η $\mathbb{A}_4$ διαθέτει μια ορθόθετη υποομάδα τάξης 4, βλ. Εφαρμογή 2.2.2, το ίδιο συμβαίνει και με την ισόμορφή της G. Ώστε $n_2(G) = 1$ και η G διαθέτει μια ορθόθετη 2–Sylow υποομάδα τάξης 4. □

Οι ομάδες τάξης $12 = 2^2 \cdot 3$ εμπεριέχονται στην επόμενη γενική περίπτωση:

Πρόταση 2.2.4. *Κάθε ομάδα $(G, \star)$ τάξης p^2q, όπου οι p, q είναι πρώτοι αριθμοί με $p \neq q$, διαθέτει μια μη τετριμμένη ορθόθετη υποομάδα.*

Απόδειξη. Αν $p > q$, τότε από $n_p \equiv 1 \mathrm{mod} p$ και $n_p \mid q \Rightarrow n_p = 1$ και γι' αυτό η G διαθέτει μια ορθόθετη p–Sylow υποομάδα.

Αν $p < q$, τότε από $n_q \equiv 1 \mathrm{mod} q$ και $n_q \mid p^2 \Rightarrow n_p = 1$ ή $n_p = p$ ή $n_p = p^2$.

(α′) Η περίπτωση $n_q = 1$, οδηγεί αμέσως στο συμπέρασμα ότι η G διαθέτει μια ορθόθετη q–Sylow υποομάδα.

(β′) Η περίπτωση $n_q = p$ είναι αδύνατη, αφού από $p = n_q \equiv 1 \mathrm{mod} q$, έπεται $q \mid p - 1$. Πράγμα άτοπο, επειδή $p < q$.

(γ′) Η περίπτωση $n_q = p^2$ και αφού $n_q \equiv 1 \mathrm{mod} q$, δίνει είτε $q \mid p-1$ είτε $q \mid p+1$ και αφού η περίπτωση $q \mid p-1$ οδηγεί σε άτοπο, βλ. την αμέσως προηγούμενη περίπτωση (β′), έπεται $q \mid p+1$. Αφού όμως, $p < q$, έπεται $q = p+1$ και επειδή οι p, q είναι πρώτοι αριθμοί, συμπεραίνουμε ότι $p = 2, q = 3$. Ώστε η G είναι μια ομάδα τάξης 12, που μόλις προηγουμένως αποδείξαμε ότι διαθέτει μια μη τετριμμένη ορθόθετη υποομάδα.

□

Πρόταση 2.2.5. *Κάθε ομάδα $(G, \star)$ τάξης 99 είναι ισόμορφη ή με την κυκλική ομάδα $\mathbb{Z}_{99}$ ή με την αβελιανή ομάδα $\mathbb{Z}_{11} \times \mathbb{Z}_3 \times \mathbb{Z}_3$.*

Απόδειξη. Για το πλήθος n_{11} των 11–Sylow υποομάδων τής G γνωρίζουμε ότι

$$n_{11} \equiv 1 \mathrm{mod} 11 \text{ και } n_{11} \mid 9 \Rightarrow n_{11} = 1.$$

[1] Αν ήταν θα είχαμε $n_3 = 1$.

Συνεπώς, η G διαθέτει μια ορθόθετη υποομάδα P τάξης 11 και γι' αυτό $P \cong \mathbb{Z}_{11}$. Για το πλήθος n_3 των 3–Sylow υποομάδων τής G γνωρίζουμε ότι

$$n_3 \equiv 1 \bmod 3 \;\text{ και }\; n_3 \mid 9 \Rightarrow n_3 = 1.$$

Συνεπώς, η G διαθέτει μια ορθόθετη υποομάδα Q τάξης 9. Οι ομάδες τάξης p^2 είναι κυκλικές και επομένως ή $Q \cong \mathbb{Z}_9$ ή $Q \cong \mathbb{Z}_3 \times \mathbb{Z}_3$.

Αν $a \in P$ και $b \in Q$, τότε το $aba^{-1}b^{-1} \in P \cap Q$, διότι $aba^{-1} \in Q$, αφού η Q είναι ορθόθετη και $ba^{-1}b^{-1} \in P$ αφού η P είναι ορθόθετη. Αλλά $P \cap Q = \{e_G\}$, επειδή η τάξη της είναι διαιρέτης των $[P : 1] = 11$ και $[Q : 1] = 9$. Γι' αυτό $aba^{-1}b^{-1} = e_G$ και $\forall a \in P, b \in Q, ab = ba$.

Η μετάθεση των στοιχείων τής P με τα στοιχεία τής Q επιτρέπει να συμπεράνουμε ότι η απεικόνιση

$$\phi : P \times Q \to G, (a, b) \;\; \to \phi((a, b)) := ab$$

είναι ένας ομομορφισμός ομάδων με τετριμμένο πυρήνα, αφού, αν $a \in P, b \in Q$ με $ab = e_G$, δίνει ότι το στοιχείο $a = b^{-1}$ ανήκει στην τομή $P \cap G = \{e_G\}$. Τώρα, επειδή $[P \times Q : 1] = 99 = [G : 1]$, ο ϕ είναι και επιμορφισμός και γι' αυτό $P \times Q \cong G$. Ώστε, ή $G \cong \mathbb{Z}_{99}$ ή $G \cong \mathbb{Z}_{11} \times \mathbb{Z}_3 \times \mathbb{Z}_3$. □

Πρόταση 2.2.6. *Κάθε ομάδα $(G, \star)$ τάξης 66 είναι ισόμορφη ή με την κυκλική ομάδα $\mathbb{Z}_{66}$ ή με την διεδρική ομάδα D_{33} ή με το ευθύ γινόμενο $D_{11} \times \mathbb{Z}_3$ ή με το ευθύ γινόμενο $D_3 \times \mathbb{Z}_{11}$, όπου D_3 και D_{11} είναι οι διεδρικές ομάδες.*

Απόδειξη. Για το πλήθος n_{11} των 11–Sylow υποομάδων τής G γνωρίζουμε ότι

$$n_{11} \equiv 1 \bmod 11 \;\text{ και }\; n_{11} \mid 6 \Rightarrow n_{11} = 1.$$

Επομένως, η G διαθέτει μια ορθόθετη 11–Sylow υποομάδα K.

Έστω H οποιαδήποτε 3–Sylow υποομάδα τής G. Το σύνολο HK είναι μια υποομάδα τής G, αφού $HK = KH$. Επιπλέον,

$$[HK : 1] = \frac{[H : 1][K : 1]}{[H \cap K : 1]} = \frac{11 \cdot 3}{1} = 33.$$

Η HK είναι τάξης $33 = 3 \cdot 11$ και αφού $3 \nmid (11 - 1)$ έπεται, βλ. Πρόταση 2.2.2, ότι είναι κυκλική, ας πούμε $HK = \langle a \rangle$ και ισόμορφη με την $\mathbb{Z}_{33}$. Ο δείκτης $[G : HK] = 2$ και γι' αυτό η HK είναι μια ορθόθετη υποομάδα τής G. Έστω $\langle b \rangle$ μια οποιαδήποτε 2–Sylow υποομάδα τής G. Παρατηρούμε ότι $HK \cap \langle b \rangle = \{e_G\}$.

Τα στοιχεία

$$e_G, a, a^2, \ldots, a^{31}, a^{32}, b, ab, a^2b, \ldots, a^{31}b, a^{32}b$$

είναι ανά δύο διαφορετικά και το πλήθος τους ισούται με 66. Συνεπώς το σύνολο αυτών των στοιχείων είναι ακριβώς το σύνολο των στοιχείων τής G.

Με ποιό από προηγούμενα στοιχεία είναι ίσο το γινόμενο ba;

Επειδή η $HK = \langle a \rangle$ είναι ορθόθετη υποομάδα τής G, έχουμε ότι $bab^{-1} = a^i \in HK$ και αφού $b = b^{-1}$, έχουμε $ba = a^i b$ (*).
Ποιές είναι οι δυνατές τιμές που μπορεί να λάβει το $i, 1 \leq i \leq 32$;
Έχουμε $a = b(bab^{-1})b^{-1} = ba^i b^{-1} = a^{i^2}$. Συνεπώς, $a^{i^2-1} = e_G$ και γι' αυτό $33 \mid i^2 - 1$. Άρα, $i = 1, 10, 23, 32$.

Έτσι με τη βοήθεια τής (*) συμπεραίνουμε ότι οι γεννήτορες a, b ικανοποιούν ακριβώς μία από τις επόμενες σχέσεις:

$$ba = ab, \quad ba = a^{10}b, \quad ba = a^{23}b, \quad ba = a^{32}b$$

και γι' αυτό μια ομάδα τάξης 66 διαθέτει ακριβώς μία από τις επόμενες πιθανές παραστάσεις:

$$\langle a, b \mid a^{33} = e_G, b^2 = e_G, ba = ab \rangle, \qquad \langle a, b \mid a^{33} = e_G, b^2 = e_G, ba = a^{32}b \rangle,$$
$$\langle a, b \mid a^{33} = e_G, b^2 = e_G, ba = a^{23}b \rangle, \qquad \langle a, b \mid a^{33} = e_G, b^2 = e_G, ba = a^{10}b \rangle.$$

Όπως θα δούμε αμέσως, υπάρχουν τέσσερεις μη ισόμορφες ομάδες τάξης 66. Συνεπώς και οι τέσσερεις προηγούμενες πιθανές παραστάσεις, που οφείλουν να προέρχονται από μη ισόμορφες ομάδες, αντιστοιχούν σε παραστάσεις αυτών των τεσσάρων μη ισόμορφων ομάδων τάξης 66. Οι τέσσερεις μη ισόμορφες ομάδες τάξης 66 είναι οι $\mathbb{Z}_{66}, D_{33}, D_{11} \times \mathbb{Z}_3, D_3 \times \mathbb{Z}_{11}$. □

Πρόταση 2.2.7. *Κάθε ομάδα $(G, \star)$ τάξης 30 διαθέτει μια μη τετριμμένη ορθόθετη υποομάδα.*

Απόδειξη. Για το πλήθος n_3 των 3–Sylow υποομάδων τής G γνωρίζουμε ότι

$$n_3 \equiv 1 \bmod 3 \;\; \text{και} \;\; n_3 \mid 10 \Rightarrow n_3 = 1 \text{ ή } 10.$$

Για το πλήθος n_5 των 5–Sylow υποομάδων τής G γνωρίζουμε ότι

$$n_5 \equiv 1 \bmod 5 \;\; \text{και} \;\; n_5 \mid 6 \Rightarrow n_3 = 1 \text{ ή } 6.$$

Αν $n_3 = 1$ (αντιστοίχως $n_5 = 1$), τότε υπάρχει μια ορθόθετη 3–Sylow υποομάδα P (αντιστοίχως 5–Sylow υποομάδα Q), η οποία μαζί με μια οποιαδήποτε 5–Sylow υποομάδα Q (αντιστοίχως 3–Sylow υποομάδα P), δίνει την υποομάδα PQ, η οποία έχει τάξη 15 και δείκτη $[G : PQ] = 2$ και γι' αυτό είναι μια μη τετριμμένη ορθόθετη υποομάδα τής G. (Η απόδειξη αυτών των παρατηρήσεων εκτελείται όπως και στην αρχή τής απόδειξης τής Πρότασης 2.2.6.)

Υπολείπεται να αποδείξουμε ότι είτε $n_3 = 1$ είτε $n_5 = 1$. Πράγματι, αν ήταν $n_3 \neq 1$ και $n_5 \neq 1$, τότε θα ήταν $n_3 = 10$ και $n_5 = 6$ και γι' αυτό θα είχαμε μια συλλογή Λ αποτελούμενη από 10 υποομάδες τής G που η καθεμιά τους θα είχε τρία στοιχεία και από 6 υποομάδες τής G που η καθεμιά τους θα είχε πέντε στοιχεία. Επειδή η τομή δύο διαφορετικών υποομάδων τής Λ ισούται πάντοτε με το ουδέτερο στοιχείο, συμπεραίνουμε ότι η G θα διέθετε $10 \times 2 = 20$ στοιχεία τάξης 3 και $6 \times 4 = 24$ στοιχεία τάξης 5. Αλλά 44 στοιχεία είναι πάρα πολλά για μια ομάδα που έχει μόνο 30 στοιχεία. Επομένως, είτε $n_3 = 1$ είτε $n_5 = 1$. □

Σύντομα θα αποδείξουμε ότι στην περίπτωση μιας ομάδας με 30 στοιχεία υπάρχει και μια ορθόθετη 3–Sylow υποομάδα και μια ορθόθετη 5–Sylow υποομάδα. Για την συγκεκριμένη απόδειξη θα χρειαστούμε ορισμένες απλές παρατηρήσεις που αναπτύσσουμε στις επόμενες γραμμές.

2.2.1 Αυτομορφισμοί Ομάδας και χαρακτηριστικές Υποομάδες

Υπενθυμίζουμε ότι αν, $(G, \star)$ είναι μια ομάδα, τότε με $\mathrm{Aut}(G)$ συμβολίζουμε το σύνολο

$$\{\phi : G \to G \mid \phi \text{ ισομορφισμός ομάδων }\}.$$

Αποδεικνύεται πολύ εύκολα ότι

Πρόταση 2.2.8. *Το ζεύγος* $(\mathrm{Aut}(G), \circ)$, *όπου «*$\circ$*» είναι η σύνθεση των απεικονίσεων, αποτελεί μια ομάδα.*

Ορισμός 2.2.1. Η ομάδα $(\mathrm{Aut}(G), \circ)$ ονομάζεται η *ομάδα αυτομορφισμών* τής $(G, \star)$ και τα στοιχεία της ονομάζονται *αυτομορφισμοί*.

Η μελέτη μιας ομάδας $(G, \star)$ είναι στενά συνδεδεμένη με την ομάδα των αυτομορφισμών της $(\mathrm{Aut}(G), \circ)$.

Ορισμός 2.2.2. Μια υποομάδα $H \leq G$ μιας ομάδας $(G, \star)$ ονομάζεται *χαρακτηριστική* αν, για κάθε αυτομορφισμό $\phi \in \mathrm{Aut}(G)$ είναι $\phi(H) = H$.

Παραδείγματα 2.2.1. Κάθε υποομάδα μιας κυκλικής ομάδας είναι χαρακτηριστική.

Πράγματι, αν η $(G, \star)$ είναι μια κυκλική ομάδα με άπειρο το πλήθος στοιχείων, τότε η $\mathrm{Aut}(G)$ αποτελείται μόνο από δύο αυτομορφισμούς:

$$\mathrm{Id} : G \to G, g \mapsto g \text{ και } \ \phi : G \to G, g \mapsto g^{-1}.$$

Προφανώς, κάθε υποομάδα τής G είναι χαρακτηριστική.

Αν η $(G, \star)$ είναι μια κυκλική ομάδα με πεπερασμένο το πλήθος στοιχείων, τότε σε κάθε διαιρέτη d τής τάξης της υπάρχει ακριβώς μία υποομάδα τάξης d. Γι' αυτό, αν $\phi \in \mathrm{Aut}(G)$ είναι οποιοσδήποτε αυτομορφισμός της και $H \leq G$ είναι οποιαδήποτε υποομάδα της, τότε η τάξη τής εικόνας $\phi(H)$ ισούται με την τάξη τής H και έτσι $\phi(H) = H$. Επομένως, κάθε υποομάδα τής G είναι χαρακτηριστική.

Παρατηρήσεις 2.2.1. Για να είναι μια υποομάδα H μιας ομάδας G χαρακτηριστική, αρκεί $\forall \phi \in \mathrm{Aut}(G)$, να είναι $\phi(H) \leq H$. Πράγματι, αν $\phi \in \mathrm{Aut}(G)$, τότε επίσης $\phi^{-1} \in \mathrm{Aut}(G)$. Τώρα από $\phi^{-1}(H) \leq H$, έπεται $H = \phi(\phi^{-1}(H)) \leq \phi(H) \leq H$. Συνεπώς, $\phi(H) = H$.

Πρόταση 2.2.9. *Έστω ότι $(G, \star)$ είναι μια πεπερασμένη ομάδα, ότι p είναι ένας πρώτος με $p \mid [G : 1]$ και ότι P είναι μια p–Sylow υποομάδα της. Τα επόμενα είναι ισοδύναμα:*

(α$'$) *Η υποομάδα P είναι η μοναδική p–Sylow υποομάδα τής G.*

(β$'$) *Η υποομάδα P είναι μια ορθόθετη υποομάδα τής G.*

(γ$'$) *Η υποομάδα P είναι μια χαρακτηριστική υποομάδα τής G.*

(δ$'$) *Κάθε υποομάδα τής G, η οποία παράγεται από ένα σύνολο στοιχείων X, όπου κάθε $x \in X$ έχει τάξη μια δύναμη τού p, είναι μια p–υποομάδα τής G.*

Απόδειξη. (α$'$) $\Leftrightarrow$ (β$'$) Όλες οι p–Sylow υποομάδες είναι συζυγείς. Επομένως, υπάρχει μία μοναδική p–Sylow υποομάδα P αν, και μόνο αν, η P είναι μια αρθόθετη υποομάδα.
(γ$'$) $\Rightarrow$ (β$'$) Κάθε στοιχείο $g \in G$ χορηγεί τον εσωτερικό αυτομορφισμό
$\sigma_g : G \to G$, $\alpha \to g\alpha g^{-1}$. Αφού η P είναι μια χαρακτηριστική υποομάδα τής G, αυτή παραμένει αναλλοίωτη κάτω από οποιονδήποτε εσωτερικό αυτομορφισμό $\sigma_g, g \in G$. Γι' αυτό $\forall g \in G, \sigma_g(P) = P$, δηλαδή $\forall g \in G, gPg^{-1} = P$.
(α$'$) $\Rightarrow$ (γ$'$) Αν ϕ είναι οποιοδήποτε στοιχείο τής $\mathrm{Aut}(G)$, τότε η $\phi(P)$ είναι επίσης μια p–Sylow υποομάδα τής G, αφού $[\phi(P) : 1] = [P : 1]$. Αλλά η P είναι η μοναδική p–Sylow υποομάδα, επομένως $P = \phi(P)$.
(α$'$) $\Rightarrow$ (δ$'$) Κάθε $x \in X$ παράγει μια κυκλική υποομάδα $\langle x \rangle$ τάξης p. Αυτή περιέχεται σε κάποια p–Sylow υποομάδα P τής G. Λόγω τής υπόθεσης, η $\langle x \rangle$ περιέχεται στη μοναδική p–Sylow υποομάδα P. Επομένως, $\forall x \in X$ έχουμε $x \in P$. Ώστε, $X \subseteq P$ και συνεπώς $\langle X \rangle \subseteq P$. Αλλά κάθε υποομάδα τής P έχει τάξη μια δύναμη τού πρώτου p. Επομένως, η $\langle X \rangle$ είναι μια p–υποομάδα τής G.
(δ$'$) $\Rightarrow$ (α$'$) Θεωρούμε όλες τις p–Sylow υποομάδες τής G και ας είναι X η ένωσή τους, δηλαδή $X = \cup_{P \in \mathrm{Syl}_p(G)} P$. Επειδή κάθε στοιχείο $x \in X$ περιέχεται σε τουλάχιστον μία p–Sylow υποομάδα, διαπιστώνουμε ότι η τάξη τού x είναι μια δύναμη τού p και έτσι, σύμφωνα με την υπόθεση, έχουμε ότι η $\langle X \rangle$ είναι μια p–υποομάδα. Συνεπώς, η $\langle X \rangle$ οφείλει, ως p–υποομάδα, να περιέχεται σε κάποια συγκεκριμένη p–Sylow υποομάδα $\overline{P}$. Επομένως έχουμε:

$$X = \cup_{P \in \mathrm{Syl}_p(G)} P \subseteq \langle X \rangle \subseteq \overline{P}.$$

Γι' αυτό $\forall P \in \mathrm{Syl}_p(G)$, $P \subseteq \overline{P}$. Αλλά οι P και $\overline{P}$ έχουν το ίδιο πλήθος στοιχείων, εφόσον πρόκειται για p–Sylow υποομάδες. Επομένως $\forall P \in \mathrm{Syl}_p(G), P = \overline{P}$. □

Παρατηρήσεις 2.2.2. Αν H, K είναι δυο υποομάδες μιας ομάδας $(G, \star)$ με την H χαρακτηριστική υποομάδα τής K και την K ορθόθετη υποομάδα τής G, τότε και H είναι ορθόθετη υποομάδα τής G.

Πράγματι, για κάθε $g \in G$, ο εσωτερικός αυτομορφισμός $\sigma_g : G \to G, \alpha \to g\alpha g^{-1}$ περιορισμένος στην υποομάδα K αποτελεί έναν αυτομορφισμό τής K, αφού πρόκειται για μια ορθόθετη υποομάδα τής G. Η υποομάδα H είναι χαρακτηριστική υποομάδα τής K, επομένως $\forall g \in G, \sigma_g(H) = H$, δηλαδή $\forall g \in G, gHg^{-1} = H$ και συνεπώς η H είναι μια ορθόθετη υποομάδα τής G.

Πρόταση 2.2.10. *Κάθε ομάδα $(G, \star)$ τάξης 30 διαθέτει μια ορθόθετη υποομάδα τάξης 5 και μια ορθόθετη υποομάδα τάξης 3.*

Απόδειξη. Από την Πρόταση 2.2.7 γνωρίζουμε ότι η G διαθέτει μια ορθόθετη υποομάδα K τάξης 15. Η K είναι κυκλική και κάθε υποομάδα της είναι χαρακτηριστική. Σε κάθε διαιρέτη d τής τάξης υπάρχει μια υποομάδα τάξης d, που όπως έχουμε διαπιστώσει είναι χαρακτηριστική υποομάδα τής K, άρα ορθόθετη υποομάδα τής G. Η K έχει υποομάδες τάξης 5 και 3. Αυτές είναι ορθόθετες υποομάδες τής G. □

2.2.2 Η εναλλάσσουσα ομάδα $\mathbb{A}_5$ είναι απλή

Υπενθυμίζουμε ότι

Ορισμός 2.2.3. Μια ομάδα $(G, \star)$ με $[G : 1] > 1$, ονομάζεται *απλή* αν, διαθέτει ως ορθόθετες υποομάδες μόνο τις $\{e_G\}$ και G.

Πρόταση 2.2.11. *Οι απλές αβελιανές ομάδες είναι οι κυκλικές ομάδες πρώτης τάξης.*

Απόδειξη. Έστω ότι η G είναι μια απλή αβελιανή ομάδα. Η G διαθέτει κάποιο $x \in G$ με $x \neq e_G$, επειδή $[G : 1] > 1$.
Η κυκλική υποομάδα $\langle x \rangle$ οφείλει να συμπίπτει με την G, αφού $\{e_G\} \subsetneq \langle x \rangle$ και $\langle x \rangle \trianglelefteq G$.
Θεωρούμε το στοιχείο $x^2 \in G$.
Αν $x^2 = e_G$, τότε η G είναι κυκλική υποομάδα με τάξη τον πρώτο αριθμό 2.
Αν $x^2 \neq e_G$, τότε $\langle x^2 \rangle = G = \langle x \rangle$. Επομένως, $x \in \langle x^2 \rangle$ και γι' αυτό $x = x^{2r}$. Έτσι συμπεραίνουμε ότι το x πεπερασμένης τάξης, έστω $n > 1$. Αφού η $\langle x \rangle = G$ είναι κυκλική σε κάθε διαιρέτη m τού n υπάρχει κυκλική υποομάδα $\langle y \rangle$ τής G τάξης m. Έστω p ένας πρώτος διαιρέτης τού n. Τότε η κυκλική υποομάδα $\langle y \rangle$ έχει τάξη p και αφού $\langle y \rangle \neq \{e_G\}$ και $\langle y \rangle \trianglelefteq G$, έπεται ότι η G ισούται με την κυκλική ομάδα $\langle y \rangle$ τής G. Ώστε η ομάδα G είναι κυκλική πρώτης τάξης. □

Πρόταση 2.2.12. *Κάθε ομάδα $(G, \star)$ τάξης 60 που έχει περισσότερες από μία 5–Sylow υποομάδες είναι απλή.*

Απόδειξη. Παρατηρούμε ότι το πλήθος n_5 των 5–Sylow υποομάδων τής G ισούται με 6, επειδή $n_5 \equiv 1 \mathrm{mod} 5$, $n_5 \mid 12$ και αφού έχουμε υποθέσει ότι $n_5 \geq 2$.

Έστω ότι η G δεν είναι απλή και ότι $H \trianglelefteq G$ είναι μια μη τετριμμένη ορθόθετη υποομάδα της.

Αν ο 5 είναι διαιρέτης τής $[H : 1]$, τότε η H περιέχει μια υποομάδα P τάξης 5, η οποία προφανώς είναι μια 5–Sylow υποομάδα τής G. Αφού όμως η H είναι ορθόθετη, περιέχει $\forall g \in G$ και κάθε συζυγή υποομάδα gPg^{-1} τής P, δηλαδή περιέχει και τις έξι 5–Sylow υποομάδες τής G. Επομένως, η H περιέχει $6 \times 4 = 24$ στοιχεία τάξης 5. Άρα $[H : 1] \geq 24$ και γι' αυτό $[H : 1] = 30$. Όμως σύμφωνα με την Πρόταση 2.2.10 μια ομάδα τάξης 30 διαθέτει ακριβώς μία 5–Sylow υποομάδα. Ώστε $5 \nmid [H : 1]$.

Αν ο 5 δεν είναι διαιρέτης τής $[H : 1]$, τότε η τάξη $[H : 1]$ είναι ένας διαιρέτης τού 12, δηλαδή 2, 3, 4, 6, ή 12. Σύμφωνα με την Πρόταση 2.2.3, μια ομάδα τάξης 12 έχει είτε μια ορθόθετη 3–Sylow υποομάδα K_1 τάξης 3 είτε μια ορθόθετη 2–Sylow υποομάδα K_2 τάξης 4. Από την Πρόταση 2.2.9 γνωρίζουμε ότι αυτή η K_i, $i = 1$ είτε 2, είναι χαρακτηριστική υποομάδα τής H και λόγω τής Παρατήρησης 2.2.2 είναι ορθόθετη υποομάδα τής G. Συνεπώς, μπορούμε να θεωρήσουμε ότι η G διαθέτει μια ορθόθετη υποομάδα H' τάξης 3 ή 4. Επιχειρηματολογώντας ανάλογα στην περίπτωση όπου $[H : 1] = 6$ μπορούμε να δεχθούμε και πάλι χωρίς περιορισμό τής γενικότητας ότι η G διαθέτει μια ορθόθετη υποομάδα H' τάξης 2 ή 3. Θεωρούμε την πηλικοομάδα G/H'. Η τάξη $[G/H' : 1]$ θα είναι είτε 30 είτε 20 είτε 15 και γι' αυτό η G/H' διαθέτει μια ορθόθετη υποομάδα $\overline{H}$ τάξης 5. (Αν η τάξη τής G/H' είναι 30 ή 15 το έχουμε ήδη αποδείξει. Στην περίπτωση που η τάξη είναι $20 = 2^2 \cdot 5$, τότε στην Πρόταση 2.2.4 αποδεικνύεται η ύπαρξη μιας ορθόθετης υποομάδας τάξης 5.) Θεωρούμε τον κανονικό επιμορφισμό $\pi : G \to G/H'$ και την αντίστροφη εικόνα $\pi^{-1}(\overline{H})$ τής ορθόθετης υποομάδας $\overline{H}$. Η $\pi^{-1}(\overline{H})$ είναι μια γνήσια ορθόθετη υποομάδα τής G που η τάξη της διαιρείται από τον αριθμό 5. Αυτό όμως οδηγεί σε άτοπο, όπως ήδη έχουμε διαπιστώσει. Συνεπώς, η G δεν διαθέτει μη τετριμμένες ορθόθετες υποομάδες, άρα πρόκειται για απλή ομάδα. □

Θεώρημα 2.2.1. *Η εναλλάσσουσα ομάδα $\mathbb{A}_5$ είναι απλή ομάδα.*

Απόδειξη. Η τάξη τής $\mathbb{A}_5$ είναι 60. Η $\mathbb{A}_5$ διαθέτει περισσότερα από 4 στοιχεία τάξης 5, δηλαδή περισσότερες από μία υποομάδες τάξης 5. Επομένως είναι μια απλή ομάδα. □

2.2.3 Πεπερασμένες Υποομάδες τής Ομάδας των αντιστρέψιμων Στοιχείων ενός Σώματος

Η τελευταία εφαρμογή τής Θεωρίας Sylow που θα παρουσιάσουμε συνδέεται με ένα πολύ ενδιαφέρον αποτέλεσμα τής Θεωρίας Σωμάτων.

Πρόταση 2.2.13. *Έστω ότι $(G, \star)$ είναι μια πεπερασμένη ομάδα με την ιδιότητα: Για κάθε $n \in \mathbb{N}$, υπάρχουν το πολύ n το πλήθος στοιχεία $g \in G$ με $g^n = e_G$. Τότε η G είναι μια κυκλική ομάδα.*

Απόδειξη. Έστω p ένας πρώτος αριθμός με $p \mid [G : 1]$ και P μια p–Sylow υποομάδα τής G με τάξη $[P : 1] = p^{\alpha}$. Παρατηρούμε ότι τα p^{α} στο πλήθος στοιχεία g τής P ικανοποιούν την ισότητα $g^{p^{\alpha}} = e_G$. Αν τώρα P' είναι μια p–Sylow υποομάδα τής G με $P' \neq P$, τότε υπάρχει κάποιο $\xi \in P'$, $\xi \notin P$ που ικανοποιεί την $\xi^{p^{\alpha}} = e_G$. Τότε όμως τουλάχιστον $p^{\alpha} + 1$ στο πλήθος στοιχεία τής G ικανοποιούν την $g^{p^{\alpha}} = e_G$. Αυτό αντίκειται στην υπόθεσή μας και γι' αυτό όλες οι p–Sylow υποομάδες τής G συμπίπτουν με την P. Συνεπώς, η P είναι μια ορθόθετη υποομάδα τής G.

Τώρα θα δείξουμε ότι η P είναι μια κυκλική υποομάδα τής G. Θεωρούμε το μέγιστο $m = \max\{\circ(g) \mid g \in P\}$ των τάξεων των στοιχείων τής P.

Επειδή η τάξη κάθε στοιχείου τής P είναι διαιρέτης τής $[P : 1] = p^{\alpha}$, έπεται ότι $m = p^{\beta}$. Θα δείξουμε ότι $\beta = \alpha$, από όπου προφανώς προκύπτει ότι η P είναι κυκλική.

Επειδή κάθε στοιχείο $g \in P$ έχει $\circ(g) = p^{\gamma}, \gamma \leq \beta$, έχουμε

$$g^{p^{\beta}} = \left(g^{p^{\gamma}}\right)^{p^{\beta-\gamma}} = (e_G)^{p^{\beta-\gamma}} = e_G.$$

Επομένως, τα p^{α} στο πλήθος στοιχεία g τής P ικανοποιούν την $g^{p^{\beta}} = e_G$. Αν όμως το β ήταν γνησίως μικρότερο τού α, τότε αυτό δεν θα συμφωνούσε με την υπόθεση τής πρότασής μας. Επομένως, $p^{\alpha} = p^{\beta}$ και γι' αυτό η P είναι κυκλική και ισόμορφη με την $\mathbb{Z}_{p^{\alpha}}$.

Θεωρούμε την ανάλυση τής τάξης τής $[G : 1]$ σε δυνάμεις διαφορετικών πρώτων αριθμών, ας πούμε $[G : 1] = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_s^{\alpha_s}$, όπουν οι $p_i, i = 1, \ldots, s$ είναι πρώτοι αριθμοί και οι $\alpha_i, i = 1, \ldots, s$ είναι φυσικοί.

Από τα προηγούμενα γνωρίζουμε ότι κάθε p_i–Sylow υποομάδα P_i είναι κυκλική τάξης $p_i^{\alpha_i}$ και ορθόθετη. Θεωρούμε την απεικόνιση

$$\phi : P_1 \times P_2 \times \cdots \times P_s \to G, (x_1, x_2, \ldots, x_s) \quad \mapsto x_1 x_2 \ldots x_s.$$

Παρατηρούμε ότι $\forall i = 1, 2, \ldots, s, P_i \cap (P_1 P_2 \ldots P_{i-1} P_{i+1} \ldots P_s) = \{e_G\}$, επειδή η τάξη τής P_i είναι $p_i^{\alpha_i}$ ενώ η τάξη τής $P_1 P_2 \ldots P_{i-1} P_{i+1} \ldots P_s$ είναι $p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_{i-1}{}^{\alpha_{i-1}} p_{i+1}{}^{\alpha_{i+1}} \ldots p_s^{\alpha_s}$. Επιπλέον παρατηρούμε ότι γινόμενα στοιχείων από διαφορετικές υποομάδες P_i και P_j μετατίθενται μεταξύ τους. Γι' αυτό η ϕ είναι ένας ομομορφισμός ομάδων, ο οποίος μάλιστα είναι και μονομορφισμός. Επιπλέον, επειδή το πλήθος των στοιχείων τού γινομένου $P_1 \times P_2 \times \cdots \times P_s$ είναι ίδιο με την τάξη $[G : 1]$ έπεται ότι ο ϕ είναι ισομορφισμός.

Έτσι

$$G \cong \mathbb{Z}_{p_1^{\alpha_1}} \times \mathbb{Z}_{p_2^{\alpha_2}} \times \cdots \times \mathbb{Z}_{p_s^{\alpha_s}} \cong \mathbb{Z}_{p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_s^{\alpha_s}}.$$

Ώστε η G είναι μια κυκλική ομάδα. □

Θεώρημα 2.2.2. *Έστω K ένα σώμα και $(K^\star, \cdot)$ η πολλαπλασιαστική ομάδα των αντιστρέψιμων στοιχείων του. Κάθε πεπερασμένη ομάδα G τής $K^\star$ είναι κυκλική.*

Απόδειξη. Παρατηρούμε ότι $\forall n \in \mathbb{N}$, το πολυώνυμο $x^n - 1_K \in K[x]$ έχει το πολύ n το πλήθος θέσεις μηδενισμού στο K. Συνεπώς, $\forall n \in \mathbb{N}$, υπάρχουν το πολύ n το πλήθος στοιχεία g τής G που ικανοποιούν την $g^n = 1_K$. Σύμφωνα με την προηγούμενη πρόταση, η G είναι μια κυκλική ομάδα. □

Παρατηρήσεις 2.2.3. Το προηγούμενο θεώρημα εφαρμόζεται άμεσα στο σύνολο των n–οστών ριζών τής μονάδας ενός σώματος K, δηλαδή στο σύνολο

$$\Omega_n = \{\omega \in K \mid \omega^n = 1_K\}.$$

Το σύνολο Ω_n είναι μια πεπερασμένη υποομάδα τής πολλαπλασιαστικής ομάδας $(K^*, \cdot)$ των αντιστρέψιμων στοιχείων τού K. Σύμφωνα με το Θεώρημα 2.2.2, η Ω_n είναι κυκλική.

Οι γεννήτορες τής Ω_n είναι οι λεγόμενες *πρωταρχικές n–οστές ρίζες τής μονάδας* που περιέχονται στο σώμα K.

Ανοικτά Ακαδημαϊκά Μαθήματα

Πανεπιστήμιο Ιωαννίνων

Τέλος Ενότητας

Χρηματοδότηση

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

Με τη συγχρηματοδότηση της Ελλάδας και της Ευρωπαϊκής Ένωσης

Σημειώματα

Σημείωμα Αναφοράς

Copyright Πανεπιστήμιο Ιωαννίνων, Διδάσκων: Καθηγητής Νικόλαος Μαρμαρίδης «Θεωρία Ομάδων». Έκδοση: 1.0. Ιωάννινα 2014. Διαθέσιμο από τη δικτυακή διεύθυνση: http://ecourse.uoi.gr/course/view.php?id=1250.

Σημείωμα Αδειοδότησης