11.1 ΘΕΩΡΗΜΑΤΑ ΤΟΥ SYLOW

Τα θεωρήματα αυτά (τρία τον αριθμό) απεδείχθησαν αρχικώς από τον Νορβηγό μαθηματικό L. Sylow (1832-1918), δημοσιεύθησαν το έτος[1] 1872 και διαδραμάτισαν έκτοτε έναν καθοριστικό ρόλο στην ανάπτυξη τής Θεωρίας Πεπερασμένων Ομάδων. Το 1ο θεώρημα τού Sylow 11.1.2 γενικεύει το θεώρημα 5.7.1 τού Cauchy και το πόρισμα 5.6.6 (και αποτελεί ένα *μερικό αντίστροφο* τού θεωρήματος 4.1.22 τού Lagrange), καθώς διασφαλίζει *την ύπαρξη υποομάδων τάξεως* p^{ξ}, $\xi \in \{1,...,\nu\}$, οιασδήποτε πεπερασμένης ομάδας G τάξεως $n = p^{\nu}m$, όπου $\nu, m \in \mathbb{N}$ και p ένας πρώτος αριθμός με $p \nmid m$. Εναλλακτικές αποδείξεις αυτού τού θεωρήματος[2] επροτάθησαν το 1878 από τους E. Netto[3] (1846-1919), ο οποίος χρησιμοποίησε συνδυαστικά επιχειρήματα από τη θεωρία των μετατάξεων, και A. Capelli[4] (1855-1910), ο οποίος ακολούθησε μια διαφορετική τεχνική εμπεριέχουσα εν σπέρματι την έννοια τής *δράσεως* τής ομάδας αναφοράς επί ενός κατάλληλου διαμελισμού τού υποκειμένου συνόλου της σε υποσύνολα, καθένα των οποίων έχει p στοιχεία. Το 1887 ο F.G. Frobenius (1849-1917) προσέθεσε μία ακόμη απόδειξη[5], η οποία έκανε χρήση τού θεωρήματος 4.4.21 και τής εξισώσεως κλάσεων συζυγίας (5.64). Η (πολύ κομψή) απόδειξη τού Frobenius επέζησε κατ' ουσίαν μέχρι των ημερών μας (με ελάχιστες παραλλαγές και προσθήκες, και αφού είχε συμπεριληφθεί στα συγγράμματα Άλγεβρας των H. Weber[6] (1842-1913), E. Netto[7], και R. Fricke[8] (1860-1930) τα εμφανισθέντα στα τέλη τού 19ου και στις αρχές τού 20ου αιώνα). Από την άλλη μεριά, η (κατά τι περίπλοκη) τεχνική τού Capelli έτυχε κάποιας βελτιώσεως σε ένα άρθρο τού G.A. Miller[9] (1863-1951) δημοσιευθέν το 1915. Ωστόσο, η (τότε διαθέσιμη) απόδειξη παρέμενε μακροσκελής. Η πρώτη *σύντομη* απόδειξη που στηρίζεται μόνον στο θεώρημα τροχιών και σταθεροποιητών 10.2.5 ως προς μια καταλλήλως επιλεγμένη δράση τής G και σε κάποια αριθμητική ιδιότητα τού διωνυμικού συντελεστή $\binom{n}{p^{\xi}}$, χωρίς να καταφεύγει σε επαγωγικά επιχειρήματα ή στη χρήση των θεωρημάτων 4.4.21 ή 5.7.1, είδε το φως τής δημοσιότητας το 1959 και οφείλεται στον H. Wielandt[10] (1910-2001). Στην παρούσα ενότητα παραθέτουμε τόσον την απόδειξη τού Frobenius όσον και εκείνην τού Wielandt.

Για το 2ο και το 3ο θεώρημα τού Sylow, τα οποία αφορούν στις ιδιότητες των μεγιστικών p-υποομάδων μιας πεπερασμένης ομάδας, όπου p είναι ένας πρώτος αριθμός που διαιρεί την τάξη της, παραθέτουμε αποδείξεις στις οποίες υπεισέρχονται εκ νέου κατάλληλες δράσεις τής ομάδας. Αυτές ακολουθούν εν πολλοίς

[1]Βλ. L. Sylow: *Théorèmes sur les groupes de substitutions*, Math. Ann. **5**, (1872), 584-594.

[2]Βλ. W.C. Waterhouse: *Early Proofs of Sylow's Theorem*, Archive for History of Ex. Sc., Vol. **21** (1980), 279-290.

[3]E. Netto: *Neuer Beweis eines Fundamentaltheorems aus der Theorie der Substitutionenlehre*, Math. Ann. **13** (1878), 249-250.

[4]A. Capelli: *Sopra l'isomorphismo dei gruppi di sostituzioni*, Giornale di Math. **16** (1878), 32-87.

[5]F.G. Frobenius: *Neuer Beweis des Sylowschen Satzes*, Jour. reine angew. Math. **100** (1887), 179-181.

[6]H. Weber: *Lehrbuch der Algebra*, Bd. **II**, Braunschweig, 1889, σελ. 135-136.

[7]E. Netto: *Gruppen- und Substitutionentheorie*, Leipzig, 1908.

[8]R. Fricke: *Lehrbuch der Algebra*, Bd. **I**, Braunschweig, 1924, σελ. 291-293.

[9]G.A. Miller: *New Proof of Sylow's Theorem*, The Annals of Mathematics, Second Series, Vol. **16**, (1915), 169-171.

[10]H. Wielandt: *Ein Beweis für die Existenz der Sylowgruppen*, Archiv der Math. (Basel) **10** (1959), 401-402.

τη μέθοδο τού Wielandt, με κάποιες συμπληρώσεις οφειλόμενες στους W. Krull[11] (1899-1971) και P.X. Gallagher[12].

Προτάσσουμε το αριθμοθεωρητικό λήμμα 11.1.1 στο οποίο βασίζεται η δεύτερη απόδειξη τού θεωρήματος 11.1.2.

11.1.1 Λήμμα. *Εάν $n = p^{\nu} m$, όπου $\nu, m \in \mathbb{N}$ και p ένας πρώτος αριθμός με $p \nmid m$, τότε για κάθε $\xi \in \{1,...,\nu\}$ υπάρχει κάποιος $k \in \mathbb{N}$ με $k \equiv 1 (\operatorname{mod} p)$, ούτως ώστε να ισχύει*

$$\binom{n}{p^{\xi}} = p^{\nu-\xi} m k.$$

ΑΠΟΔΕΙΞΗ. Προφανώς,

$$\begin{aligned}\binom{n}{p^{\xi}} &= \frac{n(n-1)\,\cdots\,(n-p^{\xi}+1)}{p^{\xi}!}\\ &= \frac{n}{p^{\xi}} \cdot \frac{(n-1)(n-2)\,\cdots\,((n-1)-(p^{\xi}-1)+1)}{(p^{\xi}-1)!}\\ &= \frac{n}{p^{\xi}}\binom{n-1}{p^{\xi}-1} = p^{\nu-\xi} m \binom{n-1}{p^{\xi}-1} = p^{\nu-\xi} m k,\end{aligned}$$

όπου $k := \binom{n-1}{p^{\xi}-1} \in \mathbb{N}$. Εν συνεχεία, παρατηρούμε ότι

$$k = \frac{(n-1)(n-2)\,\cdots\,((n-1)-(p^{\xi}-1)+1)}{(p^{\xi}-1)(p^{\xi}-2)\,\cdots\,(p^{\xi}-(p^{\xi}-1))} = \prod_{j=1}^{p^{\xi}-1} \frac{p^{\nu} m - j}{p^{\xi} - j}.$$

Κάθε $j \in \{1,...,p^{\xi}-1\}$ γράφεται υπό τη μορφή $j = p^{\lambda_j} t_j$, όπου

$$\lambda_j := \max\{\kappa \in \mathbb{N}_0 \,|p^{\kappa} \mid j\} \quad \text{και} \quad t_j := \frac{j}{p^{\lambda_j}}.$$

Κατά συνέπειαν,

$$k = \prod_{j=1}^{p^{\xi}-1} \frac{p^{\nu-\lambda_j} m - t_j}{p^{\xi-\lambda_j} - t_j}, \tag{11.1}$$

όπου $\nu - \lambda_j > 0$ και $\xi - \lambda_j > 0$ για κάθε $j \in \{1,...,p^{\xi}-1\}$. Κατόπιν υπολογισμού τού γινομένου τού δεξιού μέλους τής (11.1) λαμβάνουμε

$$k = \frac{bp + a}{cp + a}, \tag{11.2}$$

[11]W. Krull: *Über die p-Untergruppen endlicher Gruppen*, Archiv der Math. (Basel) **12** (1961), 1-6.

[12]P.X. Gallagher: *On the p-subgroups of finite groups*, Archiv der Math. (Basel) **18** (1967), 469.

για κατάλληλους ακεραίους αριθμούς a, b, c, όπου

$$a = \prod_{j=1}^{p^{\xi}-1} (-t_j) = (-1)^{p^{\xi}-1} \prod_{j=1}^{p^{\xi}-1} t_j. \tag{11.3}$$

Η (11.2) γράφεται ως εξής:

$$a(k-1) = p(b-kc). \tag{11.4}$$

Επειδή (εξ ορισμού) μκδ$(p, t_j) = 1$, $\forall j \in \{1,..., p^{\xi} - 1\}$, έχουμε (λόγω τής (11.3) και τού λήμματος 7.3.1) μκδ$(p, a) = 1$. Από την (11.4) έπεται ότι

$$\left.\begin{array}{r} p \mid a(k-1) \\ \text{μκδ}(p,a) = 1 \end{array}\right\} \underset{\text{B.2.9}}{\Longrightarrow} p \mid k-1,$$

δηλαδή ότι $k \equiv 1 (\operatorname{mod} p)$. □

11.1.2 Πρώτο θεώρημα τού Sylow. *Έστω $(G, \cdot)$ μια ομάδα τάξεως $n = p^{\nu} m$, όπου $\nu, m \in \mathbb{N}$ και p ένας πρώτος αριθμός με $p \nmid m$. Τότε για κάθε $\xi \in \{1,..., \nu\}$ υπάρχει τουλάχιστον μία υποομάδα H τής G τάξεως p^{ξ}.*

Πρωτη αποδειξη. Εάν η G είναι αβελιανή, τότε ο ισχυρισμός είναι αληθής (βλ. θεώρημα 4.4.22). Ας υποθέσουμε λοιπόν ότι η G είναι μη αβελιανή και ότι τα $x_1,..., x_l$ είναι εκπρόσωποι εκείνων των σαφώς διακεκριμένων κλάσεων συζυγίας που δεν περιέχονται στο κέντρο $Z(G)$. Τότε η (5.64) γράφεται ως εξής:

$$|G| = |Z(G)| + \sum_{j=1}^{l} |G : \mathrm{C}_G(x_j)| = |Z(G)| + \sum_{j=1}^{l} \frac{|G|}{|\mathrm{C}_G(x_j)|}.$$

Θα χρησιμοποιήσουμε τη δεύτερη μορφή τής μαθηματικής επαγωγής ως προς την τάξη τής G. Η επαγωγή ξεκινά από το 6, καθώς η $\mathfrak{S}_3$ είναι η μοναδική (μέχρις ισομορφισμού) μη αβελιανή ομάδα με τη μικρότερη δυνατή τάξη. Επειδή οι 2 και 3 είναι οι μόνοι πρώτοι διαιρέτες τού 6, αρκεί η υπόμνηση τού ότι η $\mathfrak{S}_3$ διαθέτει τρία στοιχεία τάξεως 2 και δύο στοιχεία τάξεως 3. (Πρβλ. 3.2.2 και 4.1.42.) Θεωρούμε οιαδήποτε μη αβελιανή ομάδα G τάξεως $|G| = n = p^{\nu} m > 6$ και υποθέτουμε ότι για *όλες τις μη αβελιανές ομάδες τάξεως $< |G|$ ο ισχυρισμός είναι αληθής*. Διακρίνουμε δύο περιπτώσεις:

Περίπτωση πρώτη. Εάν

$$p \mid |G : \mathrm{C}_G(x_j)|\,, \ \ \forall j \in \{1,..., l\},$$

τότε $p \mid |Z(G)|$ (διότι εξ υποθέσεως $p \mid |G|$). Όμως το κέντρο $Z(G)$, ως αβελιανή ομάδα, περιέχει κάποιο $g \in Z(G) \smallsetminus \{e_G\}$ τάξεως p *εντός τού* $Z(G)$ (βλ. 4.4.21). Η κυκλική ομάδα $\langle g \rangle$ είναι υποομάδα τού κέντρου $Z(G)$ τάξεως $|\langle g \rangle| = p$. Κατά το (i) τής προτάσεως 5.4.19, $\langle g \rangle \trianglelefteq G$. Ως εκ τούτου, ορίζεται η πηλικοομάδα $G/\langle g \rangle$ τάξεως $|G/\langle g \rangle| = p^{\nu-1} m$. Εξ αυτού συνάγουμε ότι για κάθε $\xi \in \{1,..., \nu\}$ υπάρχει κάποια υποομάδα L τής $G/\langle g\rangle$ τάξεως[13] $p^{\xi-1}$. (Πράγματι· για $\xi>1$, εάν η $G/\langle g\rangle$ είναι αβελιανή, τούτο έπεται από το θεώρημα 4.4.22, ενώ εάν η $G/\langle g\rangle$ είναι μη αβελιανή, τούτο έπεται από την επαγωγική μας υπόθεση, καθόσον $|G/\langle g\rangle|<|G|$.) Το πόρισμα 4.4.15 μας πληροφορεί ότι η L οφείλει να είναι τής μορφής $L=H/\langle g\rangle$, για κάποια υποομάδα H τής G που περιέχει την $\langle g\rangle$. Επομένως,

$$p^{\xi-1}=|L|=|H/\langle g\rangle|=\frac{|H|}{|\langle g\rangle|}=\frac{|H|}{p}\Rightarrow |H|=p^{\xi}$$

και ο ισχυρισμός είναι αληθής και για την ίδια την G.

Περίπτωση δεύτερη. Εάν $\exists j_0\in\{1,...,l\}: p\nmid |G:\mathrm{C}_G(x_{j_0})|$, τότε

$$\left.\begin{array}{r} p^{\nu}m=|G:\mathrm{C}_G(x_{j_0})|\,|\mathrm{C}_G(x_{j_0})| \\ \\ p\nmid |G:\mathrm{C}_G(x_{j_0})| \end{array}\right\}\Rightarrow p^{\xi}\mid |\mathrm{C}_G(x_{j_0})|,$$

για κάθε $\xi\in\{1,...,\nu\}$. Επειδή

$$x_{j_0}\notin Z(G)\Rightarrow |G:\mathrm{C}_G(x_{j_0})|>1\Rightarrow |\mathrm{C}_G(x_{j_0})|<|G|,$$

η $\mathrm{C}_G(x_{j_0})$ διαθέτει κάποια υποομάδα H τάξεως p^{ξ} για οιονδήποτε $\xi\in\{1,...,\nu\}$ (κάτι που έπεται εκ νέου από το θεώρημα 4.4.22 όταν η $\mathrm{C}_G(x_{j_0})$ είναι αβελιανή και από την επαγωγική μας υπόθεση όταν η $\mathrm{C}_G(x_{j_0})$ είναι μη αβελιανή). Επειδή

$$H\sqsubseteq \mathrm{C}_G(x_{j_0})\sqsubseteq G,$$

ο ισχυρισμός είναι και σε αυτήν την περίπτωση αληθής για την G. □

ΔΕΥΤΕΡΗ ΑΠΟΔΕΙΞΗ. Έστω $\xi\in\{1,...,\nu\}$ και έστω[14]

$$X:=\left\{A\in\mathfrak{P}(G)\,\middle|\,\mathrm{card}(A)=p^{\xi}\right\}\quad\left(\text{με card}\,(X)=\tbinom{n}{p^{\xi}}\right).$$

Επειδή για κάθε $g\in G$ και κάθε $A\in\mathfrak{P}(G)\smallsetminus\{\varnothing\}$ έχουμε $\mathrm{card}(A)=\mathrm{card}(gA)$, η G δρα επί τού X μέσω πολλαπλασιασμού εξ αριστερών:

$$G\times X\ni(g,A)\longmapsto g\bullet A:=gA=\{ga\,|a\in A\}\in X,$$

αφού $e_G\bullet A=A$ και $g_1\bullet(g_2\bullet A)=(g_1g_2)\bullet A$, για οιαδήποτε $g_1,g_2\in G$ και $A\in X$. Ας υποθέσουμε ότι το $\{A_1,...,A_s\}$ είναι ένα πλήρες σύστημα εκπροσώπων τού X ως προς την "$\asymp_G$". Τότε

$$X=\coprod_{i=1}^{s}\mathrm{Orb}_G(A_i)\Rightarrow \mathrm{card}\,(X)=\tbinom{n}{p^{\xi}}=\sum_{i=1}^{s}\mathrm{card}(\mathrm{Orb}_G(A_i)),$$

όπου, σύμφωνα με το λήμμα 11.1.1,

$$\exists k\in\mathbb{N}: k\equiv 1(\mathrm{mod}\,p)\ \text{ με }\ \tbinom{n}{p^{\xi}}=p^{\nu-\xi}mk.$$

[13] Για $\xi=1$ τούτο είναι προφανές.

[14] Η ισότητα $\mathrm{card}(X)=\binom{n}{p^{\xi}}$ έπεται άμεσα από το λήμμα 5.3.13.

Εάν ο πληθικός αριθμός καθεμιάς εκ των τροχιών των $A_1,\ldots,A_s$ ήταν διαιρετός διά τού $p^{\nu-\xi+1}$, τότε θα προέκυπτε αντίφαση, διότι

$$p^{\nu-\xi+1} \mid \binom{n}{p^\xi} \Longleftrightarrow p \mid mk \Longleftrightarrow \text{είτε } p \mid m \text{ είτε } p \mid k.$$

Κατά συνέπειαν, $\exists i_0 \in \{1,\ldots,s\}$, ούτως ώστε για τη μέγιστη δύναμη p^μ, $\mu \in \mathbb{N}_0$, τού p που διαιρεί τον πληθικό αριθμό $\mathrm{card}(\mathrm{Orb}_G(A_{i_0}))$ να έχουμε $\mu \leq \nu - \xi$. Έστω $H := \mathrm{Stab}_G(A_{i_0})$ ο σταθεροποιητής τού A_{i_0}. Κατά το θεώρημα τροχιών και σταθεροποιητών 10.2.5,

$$\mathrm{card}(\mathrm{Orb}_G(A_{i_0})) = |G : H| = p^\mu c,$$

για κάποιον $c \in \mathbb{N}$ με μκδ$(p,c) = 1$. Από το θεώρημα 4.1.22 τού Lagrange προκύπτει ότι

$$n = p^\nu m = |G : H|\,|H| = p^\mu c\,|H| \Rightarrow |H| = \frac{p^{\nu-\mu}m}{c} \ \ (\text{με } c \mid m).$$

Επομένως,

$$n = p^\nu m = p^\mu c\,|H| \leq p^{\nu-\xi}c\,|H| \Rightarrow |H| \geq \frac{p^\xi m}{c} \geq p^\xi. \tag{11.5}$$

Έστω τώρα τυχόν στοιχείο $a \in A_{i_0}$. Από τον ορισμό τού σταθεροποιητή και την πρόταση 4.1.12 συνάγουμε ότι

$$HA_{i_0} = A_{i_0} \Rightarrow Ha \subseteq A_{i_0} \Rightarrow |H| = \mathrm{card}(Ha) \leq \mathrm{card}(A_{i_0}) = p^\xi. \tag{11.6}$$

Οι (11.5) και (11.6) δίδουν $|H| = p^\xi$ (και η H είναι η ζητούμενη υποομάδα τής G τάξεως p^ξ). $\square$

11.1.3 Παρατήρηση. Επειδή η δεύτερη απόδειξη τού θεωρήματος 11.1.2 δεν χρησιμοποιεί τα θεωρήματα 4.4.21 ή 5.7.1, αυτά μπορούν να ιδωθούν και ως *πορίσματα* τού θεωρήματος 11.1.2!

11.1.4 Ορισμός. Έστω $(G,\cdot)$ μια ομάδα και έστω p ένας πρώτος αριθμός. Μια υποομάδα $H \sqsubseteq G$ καλείται **p-υποομάδα τού Sylow** όταν ισχύουν τα εξής:

(i) Η H είναι μια p-ομάδα (υπό την έννοια τού ορισμού 5.7.2).

(ii) Εάν η K είναι μια p-υποομάδα[15] τής G με $H \sqsubseteq K$, τότε $H = K$.

(Ως εκ τούτου, οι p-υποομάδες τού Sylow είναι μεγιστικά στοιχεία τού συνόλου όλων των p-υποομάδων τής G ως προς την "$\sqsubseteq$".) Το σύνολο όλων των p-υποομάδων τού Sylow συμβολίζεται ως εξής:

$$\boxed{\mathrm{Syl}_p(G) := \{H \in \mathbf{Subg}(G) \mid H \ p\text{-υποομάδα τού Sylow}\}.}$$

[15] Αυτό σημαίνει ότι $K \sqsubseteq G$ και ότι η K είναι αφ' εαυτής μια p-ομάδα.

11.1.5 Πρόταση. *Έστω $(G,\cdot)$ μια πεπερασμένη ομάδα και έστω p ένας πρώτος αριθμός. Τότε*

$$H \in \mathrm{Syl}_p(G) \Longleftrightarrow \exists \nu \in \mathbb{N}_0 : |H| = p^\nu \text{ και } \text{μκδ}\,(|G:H|\,,p) = 1$$

ΑΠΟΔΕΙΞΗ. "$\Rightarrow$" Εάν $H \in \mathrm{Syl}_p(G)$, τότε η υποομάδα H είναι μια p-ομάδα, οπότε $\exists \nu \in \mathbb{N}_0 : |H| = p^\nu$ (επί τη βάσει τού πορίσματος 5.7.3). Ας υποθέσουμε ότι μκδ$(|G:H|\,,p) > 1$. Κατ' ανάγκην,

$$\text{μκδ}\,(|G:H|\,,p) = p \Rightarrow \exists \mu, m \in \mathbb{N} : \mu > \nu \text{ και } |G| = p^\mu m,\ p \nmid m.$$

Κατά το 1ο θεώρημα τού Sylow 11.1.2 $\exists K \sqsubseteq G : |K| = p^\mu$. Η K είναι μια p-υποομάδα τής G (εκ νέου λόγω τού πορίσματος 5.7.3) και $H \sqsubset K$, κάτι που αντιφάσκει προς την 11.1.4 (ii). Άρα μκδ$(|G:H|\,,p) = 1$.

"$\Leftarrow$" Εάν $\exists \nu \in \mathbb{N}_0 : |H| = p^\nu$ και μκδ$(|G:H|\,,p) = 1$, τότε σύμφωνα με το πόρισμα 5.7.3 η H είναι μια p-ομάδα· επιπροσθέτως, εάν η K είναι μια p-υποομάδα τής G με $H \sqsubseteq K \sqsubseteq G$, τότε (εκ νέου λόγω τού πορίσματος 5.7.3) $\exists l \in \mathbb{N}_0 : |K| = p^l$, οπότε (βάσει τού θεωρήματος 4.1.22 τού Lagrange)

$$|K| = p^l \mid n = p^\nu m \Rightarrow l \leq \nu \Rightarrow |K| = p^l \mid p^\nu = |H| \Rightarrow |K| \leq |H|\,,$$

απ' όπου έπεται ότι $K \subseteq H \Rightarrow K = H$. Άρα $H \in \mathrm{Syl}_p(G)$. □

11.1.6 Πόρισμα. *Έστω $(G,\cdot)$ μια ομάδα τάξεως $n = p^\nu m$, όπου $\nu \in \mathbb{N}_0, m \in \mathbb{N}$ και p ένας πρώτος αριθμός με $p \nmid m$. Τότε*

$$\mathrm{Syl}_p(G) = \{H \in \mathbf{Subg}(G) : |H| = p^\nu\}\,.$$

11.1.7 Πόρισμα. *Έστω $(G,\cdot)$ μια ομάδα τάξεως $n = p^\nu m$, όπου $\nu \in \mathbb{N}_0, m \in \mathbb{N}$ και p ένας πρώτος αριθμός με $p \nmid m$. Τότε $\mathrm{Syl}_p(G) \neq \varnothing$, ήτοι η G διαθέτει τουλάχιστον μία p-υποομάδα τού Sylow.*

ΑΠΟΔΕΙΞΗ. Εάν $\nu = 0$, τότε $\mathrm{Syl}_p(G) = \{e_G\} \neq \varnothing$. Εάν $\nu \geq 1$, τότε σύμφωνα με το 1ο θεώρημα τού Sylow 11.1.2 $\exists H \sqsubseteq G : |H| = p^\nu$. Αυτή η H είναι p-υποομάδα τού Sylow επί τη βάσει τού πορίσματος 11.1.6. □

11.1.8 Θεώρημα. *Έστω $(G,\cdot)$ μια πεπερασμένη ομάδα και έστω p ένας πρώτος αριθμός. Εάν $H \in \mathrm{Syl}_p(G)$ και $K \trianglelefteq G$, τότε ισχύουν τα εξής:*

(i) $HK/K \in \mathrm{Syl}_p(G/K)$.

(ii) $\mathrm{Syl}_p(G/K) = \{QK/K \,|Q \in \mathrm{Syl}_p(G)\}\,.$

(iii) $H \cap K \in \mathrm{Syl}_p(K)$.

(iv) $\mathrm{Syl}_p(K) = \{Q \cap K \,|Q \in \mathrm{Syl}_p(G)\}\,.$

ΑΠΟΔΕΙΞΗ. Επειδή $K \trianglelefteq G \underset{4.2.19}{\Longrightarrow} K \trianglelefteq \langle H, K\rangle$, έχουμε $HK = \langle H, K\rangle = KH$ και $H \cap K \trianglelefteq K$ (βλ. λήμμα 4.5.12). Επίσης,

$$H \in \mathrm{Syl}_p(G) \underset{11.1.5}{\Longrightarrow} \exists \nu \in \mathbb{N}_0 : |H| = p^\nu \text{ και } \text{μκδ}\,(|G:H|\,,p) = 1.$$

(i) Σύμφωνα με το 2ο θεώρημα ισομορφισμών 4.5.13,

$$\begin{aligned} H/\,H\cap K \cong HK/\,K \Rightarrow p^{\nu} = |HK/\,K|\;|H\cap K| \\ \underset{\text{B.3.14}}{\Longrightarrow} \exists \xi \in \{0,1,...,\nu\} : |HK/\,K| = p^{\xi}. \end{aligned} \tag{11.7}$$

Το θεώρημα 4.1.50 δίδει αφ' ενός μεν

$$\left.\begin{aligned} |G:H| = |G:HK|\;|HK:H| \\ \text{μκδ}\,(|G:H|\,,p) = 1 \end{aligned}\right\} \Rightarrow \text{μκδ}\,(|G:HK|\,,p) = 1,$$

αφ' ετέρου δε

$$|G/K| = |G:K| = |G:HK|\;|HK:K| = |G:HK|\;|HK/\,K|\,,$$

οπότε

$$\text{μκδ}\,(|G/K:HK/K|\,,p) = \text{μκδ}\,(|G:HK|\,,p) = 1. \tag{11.8}$$

Από τις (11.7) και (11.8) προκύπτει ότι $HK/K \in \text{Syl}_p(G/K)$ (βλ. 11.1.5).

(ii) Λόγω τού (i) ο εγκλεισμός $\{QK/K\,|Q \in \text{Syl}_p(G)\} \subseteq \text{Syl}_p(G/K)$ είναι προφανής. Για την απόδειξη τής ισχύος τού αντιστρόφου εγκλεισμού θεωρούμε τυχούσα $L \in \text{Syl}_p(G/K)$ και τον φυσικό επιμορφισμό $\pi_K^G : G \to G/K$. Επειδή ισχύει $\left|G:(\pi_K^G)^{-1}(L)\right| = |G/K:L|$ (βλ. 4.4.15 (vi)), έχουμε προφανώς μκδ$\left(\left|G:(\pi_K^G)^{-1}(L)\right|,p\right) = 1$. Επιλέγουμε μια $Q \in \text{Syl}_p(\pi_K^{-1}(L))$ και παρατηρούμε ότι

$$\left.\begin{aligned} |G:Q| = \left|G:(\pi_K^G)^{-1}(L)\right|\;\left|(\pi_K^G)^{-1}(L):Q\right| \\ \text{μκδ}\left(\left|G:(\pi_K^G)^{-1}(L)\right|,p\right) = 1 \\ \text{μκδ}\left(\left|(\pi_K^G)^{-1}(L):Q\right|,p\right) = 1 \end{aligned}\right\} \Rightarrow \text{μκδ}\,(|G:Q|\,,p) = 1,$$

οπότε $Q \in \text{Syl}_p(G)$ (βάσει τής προτάσεως 11.1.5). Επειδή $QK/K \in \text{Syl}_p(G/K)$ (λόγω τού (i), με την Q στη θέση τής H) έχουμε κατ' ανάγκην

$$\left.\begin{aligned} \text{4.5.19 (ii)} \Rightarrow QK/K = \pi_K(Q) \sqsubseteq \pi_K(\pi_K^{-1}(L)) = L \in \text{Syl}_p(G/K) \\ QK/K \in \text{Syl}_p(G/K) \end{aligned}\right\} \Longrightarrow L = QK/K.$$

(iii) Επειδή $|H\cap K| = p^{\nu-\xi}$ (βλ. (11.7)) είναι αρκετό (λόγω τής προτάσεως 11.1.5) να αποδείξουμε ότι μκδ$(|K:H\cap K|\,,p) = 1$. Εφαρμόζοντας εκ νέου το θεώρημα 4.1.50 λαμβάνουμε

$$\left.\begin{aligned} |HK:K|\;|K:H\cap K| = |HK:H\cap K| \\ |HK:H|\;|H:H\cap K| = |HK:H\cap K| \\ |HK/\,K| = |H/\,H\cap K| \end{aligned}\right\} \Rightarrow |K:H\cap K| = |HK:H|\,,$$

απ' όπου έπεται ότι

$$\left.\begin{aligned} |G:H| = |G:HK|\;|HK:H| \\ \text{μκδ}\,(|G:H|\,,p) = 1 \end{aligned}\right\} \Rightarrow \text{μκδ}\,(|K:H\cap K|\,,p) = 1.$$

Άρα τελικώς $H \cap K \in \text{Syl}_p(K)$.

(iv) Λόγω τού (iii) ο εγκλεισμός $\{Q \cap K \,|Q \in \text{Syl}_p(G)\} \subseteq \text{Syl}_p(K)$ είναι προφανής. Για την απόδειξη τής ισχύος τού αντιστρόφου εγκλεισμού θεωρούμε τυχούσα υποομάδα $U \in \text{Syl}_p(K)$. Τότε η U είναι μια p-ομάδα, οπότε $\exists Q \in \text{Syl}_p(G) : U \sqsubseteq Q$. Άρα (λόγω τού (iii), με την Q στη θέση τής H)

$$[U \sqsubseteq Q \;\text{ και }\; U \sqsubseteq K] \Longrightarrow U \sqsubseteq Q \cap K \in \text{Syl}_p(K).$$

Επομένως,

$$\left.\begin{array}{r} U \in \text{Syl}_p(K) \;\text{ και }\; Q \cap K \in \text{Syl}_p(K) \\ U \sqsubseteq Q \cap K \sqsubseteq G \end{array}\right\} \Longrightarrow U = Q \cap K,$$

απ' όπου έπεται το ζητούμενο. □

11.1.9 Πρόταση. *Έστω $(G, \cdot)$ μια πεπερασμένη ομάδα και έστω p ένας πρώτος αριθμός. Εάν $H \in \text{Syl}_p(G)$, τότε $\text{Syl}_p(\text{N}_G(H)) = \{H\}$.*

ΑΠΟΔΕΙΞΗ. Η H έχει εξ ορισμού ως τάξη της μια δύναμη τού p. Επειδή $H \trianglelefteq \text{N}_G(H)$ (βλ. 5.2.4 (ii)) και

$$\left.\begin{array}{r} |G : H| = |G : \text{N}_G(H)|\; |\text{N}_G(H) : H| \\ \\ \text{μκδ}\,(|G : H|\,, p) = 1 \end{array}\right\} \Rightarrow \text{μκδ}\,(|\text{N}_G(H) : H|\,, p) = 1,$$

έχουμε (λόγω τής προτάσεως 11.1.5) $H \in \text{Syl}_p(\text{N}_G(H))$. Εν συνεχεία θεωρούμε *τυχούσα* $U \in \text{Syl}_p(\text{N}_G(H))$. Ο τύπος τού γινομένου 4.5.9 δίδει

$$\text{card}(HU) = \frac{|H|\,|U|}{|H \cap U|}.$$

Επειδή αμφότερες οι τάξεις $|H|$ και $|U|$ είναι δυνάμεις τού πρώτου αριθμού p, ο πληθικός αριθμός $\text{card}(HU)$ είναι ωσαύτως μια δύναμη τού p. Από την άλλη μεριά, η τάξη $|H|$ τής H ισούται με τη μεγίστη δύναμη τού p που διαιρεί την τάξη $|G|$ τής G. Κατά συνέπειαν, $\text{card}(HU) = |H| \Rightarrow H = U$. □

11.1.10 Πόρισμα. *Έστω $(G, \cdot)$ μια πεπερασμένη αβελιανή ομάδα και έστω p ένας πρώτος αριθμός. Τότε η G έχει μία και μόνον p-υποομάδα τού Sylow.*

ΑΠΟΔΕΙΞΗ. Προφανής (βάσει τής προτάσεως 11.1.9) αφού για οιαδήποτε υποομάδα $H \in \text{Syl}_p(G)$ έχουμε $\text{N}_G(H) = G$. □

11.1.11 Πρόταση. *Έστω $(G, \cdot)$ μια πεπερασμένη ομάδα και έστω p ένας πρώτος αριθμός. Τότε ισχύουν τα εξής:*

(i) *Εάν η H είναι μια p-υποομάδα τής G, τότε κάθε υποομάδα τής G που είναι συζυγής προς την H (υπό την έννοια τού ορισμού 5.1.4) είναι μια p-υποομάδα τής G.*

(ii) *Εάν $H \in \text{Syl}_p(G)$, τότε για κάθε υποομάδα K τής G, η οποία είναι συζυγής προς την H, έχουμε $K \in \text{Syl}_p(G)$.*

ΑΠΟΔΕΙΞΗ. Έστω ότι $H, K \in \mathbf{Subg}(G)$ με $(H,K) \in \mathcal{R}^G_{\text{συζ.}}\Big|_{\mathbf{Subg}(G)\times\mathbf{Subg}(G)}$. Τότε υπάρχει κάποιο $g \in G$, τέτοιο ώστε να ισχύει $K = gHg^{-1}$.

(i) Ας υποθέσουμε ότι η H είναι μια p-υποομάδα τής ομάδας G. Τότε κάθε στοιχείο της έχει ως τάξη του μια (μη αρνητική ακεραία) δύναμη τού p. Θεωρούμε τυχόν στοιχείο $y \in K$. Τότε $\exists x \in H : y = gxg^{-1}$. Κατά το (ii) τής προτάσεως 2.3.9 έχουμε $\text{ord}(y) = \text{ord}(x)$. Άρα η τάξη τού y είναι μια (μη αρνητική ακεραία) δύναμη τού p. Ως εκ τούτου, η K είναι μια p-υποομάδα τής G.

(ii) Ας υποθέσουμε ότι $H \in \text{Syl}_p(G)$. Τότε η K (λόγω τού (i)) είναι μια p-υποομάδα τής G. Έστω L μια p-υποομάδα τής G με $K \sqsubseteq L$. Τότε

$$K = gHg^{-1} \sqsubseteq L \Rightarrow H \sqsubseteq g^{-1}Lg = g^{-1}L\left(g^{-1}\right)^{-1}.$$

Η $g^{-1}L\left(g^{-1}\right)^{-1}$, ούσα συζυγής προς την L, είναι μια p-υποομάδα τής G (λόγω τού (i)). Επειδή $H \in \text{Syl}_p(G)$, έχουμε κατ' ανάγκην

$$H = g^{-1}Lg \Rightarrow K = gHg^{-1} = g(g^{-1}Lg)g^{-1} = L,$$

οπότε $K \in \text{Syl}_p(G)$. □

11.1.12 Συμβολισμός. Έστω $(G,\cdot)$ μια πεπερασμένη ομάδα και έστω p ένας πρώτος αριθμός. Τότε συμβολίζουμε ως

$$\boxed{\mathfrak{s}_p(G) := \text{card}(\text{Syl}_p(G))}$$

το πλήθος των p-υποομάδων τού Sylow τής G.

11.1.13 Δεύτερο θεώρημα τού Sylow. *Έστω $(G,\cdot)$ μια ομάδα τάξεως $n = p^\nu m$, όπου $\nu, m \in \mathbb{N}$ και p ένας πρώτος αριθμός με $p \nmid m$. Τότε ισχύουν τα ακόλουθα:*

(i) *Εάν $K \in \text{Syl}_p(G)$, τότε για κάθε p-υποομάδα H τής G έχουμε $L \sqsubseteq K$, όπου η L είναι μια υποομάδα τής G συζυγής προς την H.*

(ii) *Στην G όλες οι p-υποομάδες τού Sylow είναι συζυγείς (και, ως εκ τούτου, ισόμορφες), έχουσες (σύμφωνα με το πόρισμα* 11.1.6) *τάξη p^ν. Εξ αυτού έπεται ότι*

$$\boxed{\mathfrak{s}_p(G) \mid m.} \tag{11.9}$$

ΑΠΟΔΕΙΞΗ. (i) Έστω $K \in \text{Syl}_p(G)$. Τότε $|K| = p^\nu$ (βλ. 11.1.6). Ας υποθέσουμε ότι η H είναι μια p-υποομάδα τής G κι ας θεωρήσουμε το σύνολο

$$X := G/_K\mathcal{R} = \{\, gK \mid g \in G\}$$

των αριστερών πλευρικών κλάσεων τής K εντός τής G. Η απεικόνιση

$$H \times X \ni (h, gK) \longmapsto h \bullet (gK) := (hg)K \in X,$$

ορίζει μια δράση τής H επί τού X, αφού $e_G \bullet (gK) = e_H \bullet (gK) = gK$ και

$$h_1 \bullet (h_2 \bullet (gK)) = h_1 \bullet ((h_2 g)K) = (h_1 h_2 g)K = (h_1 h_2) \bullet (gK)\,,$$

για οιαδήποτε $h_1, h_2 \in H$ και $gK \in X$. Έστω $\{g_1 K, ..., g_l K\}$ ένα πλήρες σύστημα εκπροσώπων τού X ως προς την "$\asymp_H$". Ύστερα από εφαρμογή τού πορίσματος 10.2.10 για την H συνάγουμε ότι

$$\left.\begin{array}{r} \text{card}(X) \equiv \text{card}(\text{Fix}_H(X))(\text{mod}\, p) \\ p \nmid m = \frac{n}{p^\nu} = \frac{|G|}{|K|} = |G:K| = \text{card}\,(X) \end{array}\right\} \Rightarrow \text{Fix}_H(X) \neq \varnothing.$$

Άρα $\exists i_0 \in \{1, ..., l\} : g_{i_0} K \in \text{Fix}_H(X)$, απ' όπου έπεται ότι

$$\begin{aligned} \text{Orb}_H(g_{i_0} K) = \{g_{i_0} K\} &\Rightarrow (h g_{i_0})\, K = h \bullet (g_{i_0} K) = g_{i_0} K, \; \forall h \in H \\ &\Rightarrow g_{i_0} h g_{i_0}^{-1} \in K, \; \forall h \in H \Rightarrow g_{i_0} H g_{i_0}^{-1} \sqsubseteq K. \end{aligned}$$

Αρκεί λοιπόν να θέσουμε $L := g_{i_0} H g_{i_0}^{-1}$.

(ii) Έστω $K \in \text{Syl}_p(G)$. Εάν $H \in \text{Syl}_p(G)$, τότε $|K| = |H| = p^\nu$ (βλ. 11.1.6) και, βάσει των προαναφερθέντων στο (i), $\exists g_{i_0} \in G$, τέτοιο ώστε η $L := g_{i_0} H g_{i_0}^{-1}$ να είναι υποομάδα τής K. Επειδή $|L| = |K| = |H|$ (βλ. λήμμα 4.2.16), έχουμε κατ' ανάγκην $L = K$, οπότε οι K και H είναι συζυγείς υποομάδες τής G. Άρα το σύνολο $\text{Syl}_p(G)$ *ανήκει σε μία (και μόνον)* κλάση συζυγίας υποομάδων εντός τού $\mathbf{Subg}(G)$. Από την άλλη μεριά, σύμφωνα με το (ii) τής προτάσεως 11.1.11, κάθε υποομάδα τής G που είναι συζυγής προς κάποια p-υποομάδα τού Sylow οφείλει να ανήκει στο $\text{Syl}_p(G)$. Επομένως το σύνολο $\text{Syl}_p(G)$ *συγκροτεί αφ' εαυτού μία (και μόνον) κλάση συζυγίας υποομάδων* εντός τού $\mathbf{Subg}(G)$ και μπορούμε να εφαρμόσουμε το πόρισμα 5.2.9 και να λάβουμε

$$\left.\begin{array}{r} \mathfrak{s}_p(G) = |G : \text{N}_G(K)| \\ |G : \text{N}_G(K)|\, |\text{N}_G(K) : K| = |G : K| = m \end{array}\right\} \Rightarrow \mathfrak{s}_p(G) \mid m.$$

Άρα η συνθήκη διαιρετότητας (11.9) είναι αληθής. □

11.1.14 Πόρισμα. *Έστω $(G, \cdot)$ μια πεπερασμένη μη τετριμμένη ομάδα και έστω p ένας πρώτος αριθμός με $p \mid |G|$. Εάν $K \in \text{Syl}_p(G)$, τότε*

$$\boxed{\mathfrak{s}_p(G) = |G : \text{N}_G(K)|} \quad \textit{και} \quad \boxed{\mathfrak{s}_p(G) \mid |G : K|\,.} \tag{11.10}$$

Ιδιαιτέρως,

$$\boxed{\mathfrak{s}_p(G) \mid |G|\,.} \tag{11.11}$$

ΑΠΟΔΕΙΞΗ. Οι συνθήκες (11.10) είναι προφανείς από τα προαναφερθέντα στην απόδειξη τού 11.1.13 (ii). Επίσης, επειδή (κατά το πόρισμα 11.1.7) $\text{Syl}_p(G) \neq \varnothing$, υπάρχει *τουλάχιστον μία* $K \in \text{Syl}_p(G)$ (η οποία, βεβαίως, τις πληροί). Η (11.11) έπεται άμεσα από οιαδήποτε εκ των συνθηκών (11.10). □

11.1.15 Πόρισμα. *Έστω $(G,\cdot)$ μια πεπερασμένη μη τετριμμένη ομάδα και έστω p ένας πρώτος αριθμός με $p \mid |G|$. Εάν $H \in \mathrm{Syl}_p(G)$, τότε τα ακόλουθα είναι ισοδύναμα:*

(i) $H \trianglelefteq G$.

(ii) $\mathrm{Syl}_p(G) = \{H\}$.

ΑΠΟΔΕΙΞΗ. (i)⇒(ii) Τούτο έπεται από το (ii) τού θεωρήματος 11.1.13 και το γεγονός ότι η H, ως ορθόθετη υποομάδα τής G, ισούται με κάθε συζυγή της υποομάδα.

(ii)⇒(i) Έστω τυχόν $g \in G$. Η υποομάδα gHg^{-1} είναι συζυγής προς την H, οπότε, σύμφωνα με (ii) τής προτάσεως 11.1.11, $gHg^{-1} \in \mathrm{Syl}_p(G)$. Επειδή $\mathrm{Syl}_p(G) = \{H\}$ έχουμε $gHg^{-1} = H \Rightarrow H \trianglelefteq G$. □

11.1.16 Λήμμα. *Έστω $(G,\cdot)$ μια πεπερασμένη μη τετριμμένη ομάδα και έστω p ένας πρώτος αριθμός που είναι διαιρέτης τής τάξεώς της. Εάν $H \in \mathrm{Syl}_p(G)$ και εάν η τάξη μιας πλευρικής κλάσεως $gH \in \mathrm{N}_G(H)/H$ ισούται με μια (μη αρνητική ακεραία) δύναμη τού p, τότε $g \in H$.*

ΑΠΟΔΕΙΞΗ. Εξ υποθέσεως, $\exists \nu \in \mathbb{N} : |H| = p^{\nu}$ και $\exists \mu \in \mathbb{N}_0 : \mathrm{ord}(gH) = |\langle gH \rangle| = p^{\mu}$, οπότε η κυκλική ομάδα $\langle gH \rangle$ είναι μια p-υποομάδα τής πηλικοομάδας $\mathrm{N}_G(H)/H$. Το πόρισμα 4.4.15 μας πληροφορεί ότι η $\langle gH \rangle$ οφείλει να είναι τής μορφής $\langle gH \rangle = K/H$, για κάποια υποομάδα K τού ορθοθέτη $\mathrm{N}_G(H)$ που περιέχει την H. Επειδή

$$\left.\begin{array}{r} |K| = |K/H|\,|H| = |\langle gH \rangle|\,|H| = p^{\mu+\nu} \Rightarrow \text{ η } K \text{ είναι } p\text{-υποομάδα} \\ H \sqsubseteq K \end{array}\right\} \underset{11.1.4\,(ii)}{\Longrightarrow} H = K,$$

η K/H είναι τετριμμένη, οπότε $g \in H$. □

11.1.17 Λήμμα. *Έστω $(G,\cdot)$ μια πεπερασμένη μη τετριμμένη ομάδα και έστω p ένας πρώτος αριθμός που είναι διαιρέτης τής τάξεώς της. Εάν $H \in \mathrm{Syl}_p(G)$ και εάν το g είναι ένα στοιχείο τής G έχον ως τάξη του μια (μη αρνητική ακεραία) δύναμη τού p και $gHg^{-1} = H$, τότε $g \in H$.*

ΑΠΟΔΕΙΞΗ. Εξ υποθέσεως, $\exists \xi \in \mathbb{N}_0 : \mathrm{ord}(g) = p^{\xi}$. Ως γνωστόν, $H \trianglelefteq \mathrm{N}_G(H)$ (βλ. 5.2.4 (ii)), οπότε ορίζεται η πηλικοομάδα $\mathrm{N}_G(H)/H$ και ο φυσικός επιμορφισμός $\pi_H^{\mathrm{N}_G(H)} : \mathrm{N}_G(H) \longrightarrow \mathrm{N}_G(H)/H$. Επειδή $gHg^{-1} = H \Rightarrow g \in \mathrm{N}_G(H)$, έχουμε (λόγω τού 2.4.3 (iv))

$$\mathrm{ord}(\pi_H^{\mathrm{N}_G(H)}(g)) = \mathrm{ord}(gH) \mid \mathrm{ord}(g) = p^{\xi} \underset{B.3.14}{\Longrightarrow} \exists \mu \in \mathbb{N}_0,\ \mu \leq \xi : \mathrm{ord}(gH) = p^{\mu}.$$

Σύμφωνα με το προηγηθέν λήμμα 11.1.16 έχουμε $g \in H$. □

11.1.18 Τρίτο θεώρημα τού Sylow. *Έστω $(G,\cdot)$ μια πεπερασμένη μη τετριμμένη ομάδα και έστω p ένας πρώτος αριθμός με $p \mid |G|$. Τότε το πλήθος των p-υποομάδων τού Sylow αφήνει υπόλοιπο 1 διαιρούμενο διά τού p, δηλαδή*

$$\boxed{\mathfrak{s}_p(G) \equiv 1 (\mathrm{mod}\, p).} \tag{11.12}$$

ΑΠΟΔΕΙΞΗ. Ας υποθέσουμε ότι οι $H_0, H_1, \ldots, H_{\mathfrak{s}_p(G)-1}$ είναι οι (σαφώς διακεκριμένες) p-υποομάδες τού Sylow. (Αυτές, σύμφωνα με το (ii) τού θεωρήματος 11.1.13, είναι συζυγείς.) Παγιώνουμε μία εξ αυτών, ας πούμε την H_0, και θέτουμε από εδώ και στο εξής $H := H_0$. Η ομάδα H έχει τάξη $|H| = p^\kappa$ (για κάποιον $\kappa \in \mathbb{N}_0$) και δρα επί τού συνόλου

$$X := \mathrm{Syl}_p(G) = \{H_0, H_1, \ldots, H_{\mathfrak{s}_p(G)-1}\} = \{\, gHg^{-1} \mid g \in G\}$$

μέσω συζυγίας:

$$H \times X \ni (h, H_j) \longmapsto h \bullet H_j := hH_jh^{-1} \in X, \ \ \forall j \in \{0, 1, \ldots, \mathfrak{s}_p(G) - 1\},$$

αφού $e_G \bullet H_j = e_H \bullet H_j = H_j$ και

$$\begin{aligned} h_1 \bullet (h_2 \bullet H_j) &= h_1 \bullet (h_2H_jh_2^{-1}) = h_1(h_2H_jh_2^{-1})h_1^{-1} = (h_1h_2)\, H_j\, (h_1h_2)^{-1} \\ &= (h_1h_2) \bullet H_j, \ \ \forall j \in \{0, 1, \ldots, \mathfrak{s}_p(G) - 1\}. \end{aligned}$$

Ύστερα από εφαρμογή τού πορίσματος 10.2.10 για την H συνάγουμε ότι

$$\mathfrak{s}_p(G) = \mathrm{card}(X) \equiv \mathrm{card}(\mathrm{Fix}_H(X)) (\mathrm{mod}\, p). \tag{11.13}$$

Εν συνεχεία, παρατηρούμε ότι για $j \in \{0, 1, \ldots, \mathfrak{s}_p(G) - 1\}$ ισχύει η αμφίπλευρη συνεπαγωγή

$$\mathrm{Stab}_H(H_j) = H \Longleftrightarrow j = 0. \tag{11.14}$$

Πράγματι· εάν υπάρχει $j \in \{0, 1, \ldots, \mathfrak{s}_p(G) - 1\}$ με $\mathrm{Stab}_H(H_j) = H$, τότε[16]

$$[hH_jh^{-1} = H_j, \ \forall h \in H] \underset{11.1.17}{\Longrightarrow} [h \in H_j, \ \forall h \in H] \Rightarrow H_j \sqsubseteq H \underset{11.1.4\,(\mathrm{ii})}{\Longrightarrow} H_j = H \ (= H_0),$$

οπότε έχουμε κατ' ανάγκην ότι $j = 0$, επαληθεύοντας τη συνεπαγωγή "$\Rightarrow$" στην (11.14). Όμως ισχύει και η αντίστροφη συνεπαγωγή, καθότι για $j = 0$ έχουμε

$$\mathrm{Stab}_H(H_0) = \mathrm{Stab}_H(H) := \left\{ h \in H \ \middle| \ hHh^{-1} = H \right\} = H.$$

Κατά συνέπειαν, $H_j \in \mathrm{Fix}_H(X)$ (ή, ισοδυνάμως, $\mathrm{Stab}_H(H_j) = H$) *εάν και μόνον εάν* $j = 0$, οπότε

$$\mathrm{Fix}_H(X) = \{H_0\} = \{H\} \Rightarrow \mathrm{card}(\mathrm{Fix}_H(X)) = 1. \tag{11.15}$$

Η ισοτιμία (11.12) προκύπτει από τις (11.13) και (11.15). □

[16] Εν προκειμένω, εφαρμόζεται το λήμμα 11.1.17 με το h στη θέση τού (εκεί παρατεθέντος) g και την H στη θέση τής G (καθώς το h έχει προφανώς ως τάξη του μια δύναμη τού p). Εναλλακτικώς μπορεί να χρησιμοποιηθεί η συνεπαγωγή $[hH_jh^{-1} = H_j, \ \forall h \in H] \Rightarrow H \sqsubseteq \mathrm{N}_G(H_j)$, σε συνδυασμό με την πρόταση 11.1.9 (εφαρμοζόμενη με την H_j στη θέση τής εκεί παρατεθείσας H).