Βασικό αποτέλεσμα: Αν $H \le G$ με $|G:H| = n$, τότε υπάρχει ομομορφισμός $\rho_H : G \to S_n$ με πυρήνα $N = \bigcap_{x \in G} xHx^{-1}$

Απόδειξη: Η G δρα από αριστερά στα αριστερά σύμπλοκα της H στην G. Η δράση είναι $g * (xH) = gxH$.

Αν $X = \{g_1H, g_2H, \dots, g_nH\}$ είναι το σύνολο των αριστερών συμπλόκων της H στην G, τότε $g*(g_iH) = gg_iH = g_jH$, για κάποιο $j \in \{1, 2, \dots, n\}$.

Θέτουμε $\tilde{\rho}_H : G \to \operatorname{Sym} X$ με $\tilde{\rho}_H(g)(xH) = gxH$.

Αν $a, b \in G$, τότε $\tilde{\rho}_H(ab)(xH) = abxH = \tilde{\rho}_H(a)(bxH) = \tilde{\rho}_H(a) \circ \tilde{\rho}_H(b)(xH)$. Άρα $\tilde{\rho}_H(ab) = \tilde{\rho}_H(a) \circ \tilde{\rho}_H(b)$. Άρα $\tilde{\rho}_H$ ομομορφισμός $G \to \operatorname{Sym}(X)$

Σταθεροποιούμε μια 1-1 και επί απεικόνιση $\tau : X = \{g_1H, g_2H, \dots, g_nH\} \to \{1, 2, \dots, n\}$ με $\tau(g_iH) = i \Rightarrow \tau^{-1}(i) = g_iH$. $\forall\, i = 1, 2, \dots, n$.

Τότε θέτουμε για κάθε $g \in G$
$\rho_H(g) = \tau \tilde{\rho}_H(g) \tau^{-1}$. Η $\tau \tilde{\rho}_H(g) \tau^{-1} \in S_n$.

Πράγματι $\tau \tilde{\rho}_H(g) \tau^{-1}(i) = \tau \tilde{\rho}_H(g)(g_iH) = \tau(gg_iH) = \tau(g_jH) = j \in \{1, 2, \dots, n\}$ γιατί $gg_iH = g_jH$ για κάποιο $j \in \{1, \dots, n\}$. Αν $\tau \tilde{\rho}_H(g) \tau^{-1}(i) = \tau \tilde{\rho}_H(g) \tau^{-1}(i') \Leftrightarrow$
$\Leftrightarrow \tau \tilde{\rho}_H(g)(g_iH) = \tau \rho_H(g)(g_{i'}H) = \tau(gg_iH) = \tau(gg_{i'}H)$
$\Leftrightarrow \tau(g_jH) = \tau(g_{j'}H) \Rightarrow j = j'$. Αλλά, αν $i \neq i'$, τότε $g_iH \neq g_{i'}H \Rightarrow gg_iH \neq gg_{i'}H \Leftrightarrow g_jH \neq g_{j'}H \Leftrightarrow j \neq j'$. Άρα $i = i'$ και η $\tau \tilde{\rho}_H(g) \tau^{-1} \in S_n$.

Έστω $\rho_H : G \to S_n$ με $\rho_H(g) = \tau \tilde{\rho}_H(g) \tau^{-1}$

Τότε $\rho_H(gg') = \tau \tilde{\rho}_H(gg')\tau^{-1} = \tau \tilde{\rho}_H(g)\tilde{\rho}_H(g')\tau^{-1} =$

$= \tau \tilde{\rho}_H(g)\tau^{-1}\tau\tilde{\rho}_H(g')\tau^{-1} = \rho_H(g)\rho_H(g')$

Άρα $\rho_H : G \to S_n$ ομομορφισμός.

<u>Πυρήνας της ρ_H:</u> $\rho_H(x) = 1 \Leftrightarrow \tau\tilde{\rho}_H(x)\tau^{-1} = 1 \Leftrightarrow$

$\Leftrightarrow \tau\tilde{\rho}_H(x)\tau^{-1}(i) = i \;\; \forall i = 1, \ldots, n \Leftrightarrow$

$\Leftrightarrow \tau\tilde{\rho}_H(x)(g_i H) = i \Leftrightarrow \tau(xg_i H) = i$.

Αν $xg_i H = g_j H$ με $j \neq i$, τότε $\tau(xg_i H) = \tau(g_j H) = j \neq i$.

άτοπο. Άρα $xg_i H = g_i H \;\; \forall i = 1, 2, \ldots, n \Leftrightarrow$

$\Leftrightarrow g_i^{-1} x g_i \in H \;\; \forall i = 1, \ldots, n \Leftrightarrow x \in g_i H g_i^{-1} \;\; \forall i = 1, \ldots, n$.

Αν $y \in G$, τότε $yH = g_i H$ για κάποιο i.

Τότε $g_i = yh$, όπου $h \in H$ και $g_i H g_i^{-1} = yhHh^{-1}y^{-1} =$

$= yHy^{-1}$. Άρα $x \in \bigcap_{y \in G} yHy^{-1}$. Αν $t \in G$, τότε

$$t\Big(\bigcap_{y \in G} yHy^{-1}\Big)t^{-1} = \bigcap_{y \in G} tyH(ty)^{-1} = \bigcap_{y \in G} yHy^{-1}$$

Άρα $\operatorname{Ker}\rho_H = \bigcap_{y \in G} yHy^{-1} \trianglelefteq G$ και $\operatorname{Ker}\rho_H \trianglelefteq H$.

<u>Εφαρμογή:</u> Έστω $|G| = 4p^n$, $n \geq 1$, όπου p πρώτος.

Είναι η G απλή;

<u>Απάντηση:</u> Αν $p = 2$, τότε $|G| = 2^{n+2}$ μια 2-ομάδα άρα όχι απλή γιατί έχει μη τετριμμένο κέντρο.

Αν $p \geq 5$, τότε το πλήθος των p-υποομάδων Sylow είναι $\equiv 1 \bmod p$ (άρα πρώτο προς τον p) και διαιρέτης της τάξης της ομάδας. Αν P μια p-υποομάδα Sylow της G τότε το πλήθος των p-υποομάδων Sylow είναι $1, 2$ ή 4.

Αν είναι 1, τότε η $P \triangleleft G$ (Όλες οι p-υποομάδες Sylow είναι συζυγείς): Οι περιπτώσεις 2 και 4 αποκλείονται γιατί $2 \not\equiv 1 \mod p$ και $4 \not\equiv 1 \mod p$.

Απομένει η περίπτωση $p=3$.

Αν δεν υπάρχει 1 3-υποομάδα Sylow τότε πρέπει να υπάρχουν 4. (Η περίπτωση να υπάρχουν 2 αποκλείεται γιατί $2 \not\equiv 1 \mod p$) και $\underline{4 \equiv 1 \mod 3}$

Από το προηγούμενο αποτέλεσμα υπάρχει ομομορφισμός $\rho_P : G \to S_4$ με πυρήνα $N = \bigcap_{x \in G} xPx^{-1}$.

$|S_4| = 4! = 24$. Αν $n \geq 2$, τότε $|G| \geq 4 \cdot 3^2 = 36 > 24 = |S_4|$. Άρα $\operatorname{Im}\rho_P \leq S_4 \Rightarrow |\operatorname{Im}\rho_P| \leq 24 < 36 \leq |G|$

Συνεπώς $N = \operatorname{Ker}\rho_P = \bigcap_{x \in G} xPx^{-1} > \frac{36}{24} > 1 \Rightarrow$

$\Rightarrow N \neq \{1\}$. Άρα N μη τετριμμένη κανονική υποομάδα της $G \Rightarrow G$ όχι απλή.

Αν $n=1$, δηλαδή $|G| = 4 \cdot 3 = 2^2 \cdot 3$, τότε ανάγεται στην περίπτωση $|G| = p^2 q$ (p, q διαφορετικοί πρώτοι) που δεν είναι απλή.

<u>Άσκηση:</u> Μια ομάδα G έχει τάξη $|G| = pqr$, όπου p, q, r διακεκριμένοι πρώτοι.

Τότε η G δεν είναι απλή.

<u>Απόδειξη:</u> Έστω $p > q > r$. Υποθέτουμε ότι καμία από τις p-Sylow, q-Sylow και r-Sylow δεν είναι κανονική.

Εφόσον υπάρχουν $1 + \lambda p$ p-υποομάδες του Sylow τότε επειδή $q \not\equiv 1 \mod p$ και $r \not\equiv 1 \mod p$ θα υπάρχουν 1 (άρα κανονική — το αποκλείσαμε) ή $qr \equiv 1 \mod p$ p-υποομάδες Sylow.

Άρα υπάρχουν $q r(p-1) = pqr - qr$ στοιχεία τάξης p.
Πόσες q-Sylow υποομάδες υπάρχουν;
(1 - το αποκλείσαμε), $r \not\equiv 1 \mod q$, p ή pr.
Αν υπήρχαν $pr \equiv 1 \mod q$ q-Sylow υποομάδες, τότε θα είχαμε $pr(q-1) = pqr - pr$ στοιχεία τάξης q.
Απομένουν $pqr - qr - pqr + pr = (p-q)r$ στοιχεία τάξης r ή 1. Τα στοιχεία αυτά αποτελούν την ένωση των r-υποομάδων του Sylow. Άρα το πλήθος των r-υποομάδων Sylow είναι της μορφής $1+\lambda r$.
Επειδή δύο (κυκλικές με τάξη πρώτο r) r-υποομάδες τέμνονται τετριμμένα, τότε $(p-q)r = 1$ στοιχεία. Ταυτόχρονα υπάρχουν $1+\lambda r - 1 = \lambda r$ έχουν τάξη r. στοιχεία τάξης r. Άρα $(p-q)r - 1 = \lambda r \Rightarrow r \mid 1$, άτοπο.

<u>Άσκηση:</u> Έστω ~~[illegible]~~ $G' = \langle [a,b] \mid a,b \in G \rangle$ η παράγωγος υποομάδα της G. Αν $G' \leq H \leq G$, τότε $H \triangleleft G$ και G/H αβελιανή.

<u>Απόδειξη:</u> Έστω $g \in G$ και $h \in H$. Τότε $g h g^{-1} h^{-1} = [g,h] \in G' \leq H \Rightarrow g h g^{-1} \in Hh = H$. Άρα $H \triangleleft G$.

Η G/G' είναι αβελιανή. ~~[illegible]~~ Πράγματι
Αν ~~[illegible]~~ Αν $x, y \in G$, τότε $[x,y] = xyx^{-1}y^{-1} G' = G' \Leftrightarrow (xG')(yG')(xG')^{-1}(yG')^{-1} = G' = 1_{G/G'} \Leftrightarrow xG'yG' = yG'xG'$

Η $H/G' \leq G/G'$ υποομάδα αβελιανής, άρα αβελιανή.

Άσκηση: $P \leq G$ Sylow υποομάδα. Αν $N_G(P) \leq H \leq G$ τότε $N_G(H) = H$.

Απόδειξη: Προφανώς $H \leq N_G(H)$. Έχουμε $P \leq N_G(P) \leq H$, άρα η $N_G(H)$ περιέχει κάποιες p-υποομάδες Sylow, συζυγείς στην $N_G(H)$ με την P. xPx^{-1} είναι μια τέτοια, $(x \in N_G(H))$. Άρα αν xPx^{-1}, τότε επειδή $x \in N_G(H)$, $xHx^{-1} = H$ και προφανώς $xPx^{-1} \subseteq xHx^{-1} = H$. Άρα $\exists\, h \in H$ με $xPx^{-1} = hPh^{-1} \Leftrightarrow h^{-1}xP(h^{-1}x)^{-1} = P \Rightarrow h^{-1}x \in N_G(P) \leq H$. Άρα $h^{-1}x \in H \Rightarrow$ ($h^{-1} \in H$) $x \in H$, και αυτό για κάθε $x \in N_G(H)$.

Άσκηση: Μια p-υποομάδα Sylow της G/K, όπου $K \triangleleft G$ είναι της μορφής KP/K, όπου P μια p-υποομάδα Sylow της G.

Απόδειξη: Αν $|P| = p^{\kappa}$, τότε $|P \cap K| = p^{\lambda}$, όπου $\kappa \geq \lambda$. Προφανώς $P \cap K$ είναι μια p-υποομάδα Sylow της K. Άρα κάθε άλλη p-υποομάδα Sylow της K έχει τάξη p^{λ}.
Άρα θεωρούμε τον ισομορφισμό
$\varphi : KP/K \to P/K\cap P$, ο οποίος είναι καλά ορισμένος. Προφανώς $|P/K\cap P| = p^{\kappa-\lambda}$ και άρα και $|KP/K| = p^{\kappa-\lambda}$.

[Αν p^{κ} η τάξη μιας p-sylow στην G και p^{λ} η τάξη μιας p-sylow στην K, τότε $p^{\kappa-\lambda}$ είναι η τάξη μιας p-sylow στην G/K]

Κανονικές σειρές

Μια κανονική σειρά μιας ομάδας G είναι μια πεπερασμένη ακολουθία υποομάδων της της μορφής

$$G = A_0 > A_1 > A_2 > \dots > A_n = \{1\}$$

όπου $A_{i+1} \triangleleft A_i \ \forall i = 0, 1, \dots, n-1$.

Το n λέγεται μήκος της σειράς.

Επιλύσιμες ομάδες: Μια ομάδα G λέγεται επιλύσιμη αν έχει κανονική σειρά

$$G = A_0 \triangleright A_1 \triangleright A_2 \triangleright \dots \triangleright A_n = \{1\}$$

όπου τα πηλίκα A_i / A_{i+1} είναι αβελιανές ομάδες $\forall i = 0, 1, \dots, n-1$.

Η Παράγωγος σειρά: Έστω $G' = \langle [a, b] \mid a, b \in H \rangle \triangleleft G$

$G'' = (G')' \triangleleft G'$, και γενικά $G^{(i+1)} = (G^{(i)})'$.

Τότε οι $G^{(i)}$ είναι πλήρως αναλλοίωτες υποομάδες της G, άρα κανονικές στην G.

Πράγματι, έστω $\varphi : G \to G$ ομομορφισμός.

Τότε $\varphi([a, b]) = \varphi(a b a^{-1} b^{-1}) = \varphi(a)\varphi(b)\varphi(a)^{-1}\varphi(b)^{-1}$
$= [\varphi(a), \varphi(b)] \in G'$.

Άρα $\varphi(G') \subseteq G'$.

Συνεπώς ο $\varphi|_{G'} : G' \to G'$ είναι ομομορφισμός και σύμφωνα με τα παραπάνω επάγεται ομομορφισμός $\varphi|_{G''} : G'' \to G''$

Επαγωγικά, αν $\varphi(G^{(m)}) \subseteq G^{(m)}$, τότε ο φ επάγεται ομομορφισμό $\bar{\varphi} = \varphi|_{G^{(m+1)}} : G^{(m+1)} \to G^{(m+1)}$, γιατί $G^{(m+1)} = (G^{(m)})'$.

Κριτήριο επιλυσιμότητας:

Τα παρακάτω είναι ισοδύναμα:

1) G επιλύσιμη.

2) Υπάρχει όρος της παραγώγου σειράς $G^{(m)}$ με $G^{(m)}=\{1\}$.

$G=G^{(0)} \triangleright G^{(1)} \triangleright G^{(2)} \triangleright \cdots$

Απόδειξη: Έστω G επιλύσιμη. Τότε υπάρχει κανονική σειρά $G=A_0 \triangleright A_1 \triangleright \cdots \triangleright A_m=\{1\}$ με A_i/A_{i+1} αβελιανή, $\forall i=0,\dots,m-1$.

Έχουμε $G/A_1 = A_0/A_1$ αβελιανή, άρα $G' \leq A_0$.

Αν $a,b \in A_0 = G$ τότε $[a^{-1},b^{-1}]A_1 = A_1$.

Πράγματι αν a,b ... $a^{-1}b^{-1}ab\, A_1 = A_1 \Leftrightarrow$

δηλαδή $(aA_1)(bA_1) = (bA_1)(aA_1)$

$\Leftrightarrow abA_1 = baA_1$. Επειδή $x=(x^{-1})^{-1}$ $\forall x \in G$ έπεται ότι $[a,b]A_1 = A_1$

$\Rightarrow [a,b] \in A_1$ $\forall a,b \in G$. Άρα $G' \leq A_1$.

Υποθέτουμε ότι $G^{(i)} \leq A_i$. Εφόσον A_i/A_{i+1} αβελιανή $\Rightarrow$ ~~...~~

$G^{(i+1)} = (G^{(i)})' \leq A_i'$ και A_i/A_{i+1} αβελιανή

$\left[x,y \in A_i \text{ τότε } [x^{-1},y^{-1}]A_{i+1} = x^{-1}A_{i+1}\, y^{-1}A_{i+1}\, xA_{i+1}\, yA_{i+1} = (x^{-1}A_{i+1})(xA_{i+1})(y^{-1}A_{i+1})(yA_{i+1}) = A_{i+1} = 1_{A_i/A_{i+1}} \right]$

Άρα $G^{(i+1)} \leq A_{i+1}$.

Εφόσον $A_m=\{1\}$, έπεται ότι $G^{(m)}=\{1\}$

Αντιστρόφως, έστω $G^{(m)}=\{1\}$.

Η σειρά $G=G^{(0)} \triangleright G' \triangleright G'' \triangleright G^{(3)} \triangleright \cdots \triangleright G^{(m)}=\{1\}$ είναι επιλύσιμη γιατί $G^{(i)}/G^{(i+1)} = G^{(i)}/(G^{(i)})'$ είναι αβελιανή. Άρα η G είναι επιλύσιμη.

Πόρισμα 1: Κάθε υποομάδα και κάθε ομάδα πηλίκο μιας επιλύσιμης ομάδας G είναι επιλύσιμη.

Απόδειξη: Έστω $H \leq G$. Τότε $H^{(i)} \leq G^{(i)}$ $\forall i = 0, 1, 2, \dots$ Αν $G^{(m)} = 1$, τότε και $H^{(m)} = 1$ και άρα η H επιλύσιμη και G επιλύσιμη. Τότε G/K επιλύσιμη.

Έστω $K \triangleleft G$ και G επιλύσιμη. Τότε G/K επιλύσιμη.

$(G/K)' = G'K/K$, Πράγματι $[aK, bK] = aba^{-1}b^{-1}K = [a,b]K \in G'K/K$. ~~Άρα. Αντεστρόφως~~

Ομοίως $(G/K)^{(k)} = G^{(k)}K/K$ $\forall k = 1, 2, \dots$

και επειδή $G^{(m)} = 1$ για κάποιο m, έπεται ότι

$$(G/K)^{(m)} = G^{(m)}K/K = K/K = \{1\}$$

Πόρισμα 2: Έστω $K \triangleleft G$ και K και G/K επιλύσιμες. Τότε και η G είναι επιλύσιμη.

Απόδειξη: Εφόσον G/K επιλύσιμη, υπάρχει επιλύσιμη σειρά $(G/K)^{(0)} = G/K \triangleright G'K/K \triangleright G''K/K \triangleright \dots \triangleright G^{(n)}K/K = 1$. $G^{(n)}K \leq K \Rightarrow G^{(n)} \leq K$.

Επομένως ~~$G^{(n)}K \leq K \Rightarrow G^{(n)} \leq K$~~ εφόσον K επιλύσιμη, τότε και η υποομάδα της $G^{(n)}$ είναι επιλύσιμη. Άρα υπάρχει επιλύσιμη σειρά

$G^{(n)} \triangleright G^{(n+1)} \triangleright \dots \triangleright G^{(n+m)} = 1$

Άρα η σειρά $G = G^0 \triangleright G' \triangleright \dots \triangleright G^{(n)} \triangleright G^{(n+1)} \triangleright \dots \triangleright G^{(n+m)} = 1$ είναι επιλύσιμη.

Πόρισμα 3: Κάθε p-ομάδα (πεπερασμένη) είναι επιλύσιμη.

Απόδειξη: Έστω P μια πεπερασμ. p-ομάδα. Τότε η P έχει κέντρο $Z(P) \neq 1$ που είναι αβελιανή κανονική ομάδα, άρα επιλύσιμη.

Η $P/Z(P)$ είναι p-ομάδα με $|P/Z(P)| < |P|$

Με επαγωγή στην τάξη της ομάδας η $P/Z(P)$ είναι επιλύσιμη. Με βάση το προηγούμενο πόρισμα η P είναι επιλύσιμη.