ΘΕΩΡΗΜΑ 1. (Galois) Η A_n είναι απλή, για $n \geq 5$.

Απόδειξη: Έστω $1 \neq K \lhd A_n$. Επειδή η A_n παράγεται από τους κύκλους μήκους 3, αρκεί να δείξουμε ότι κάθε τέτοιος κύκλος ανήκει στην K. Πράγματι, αν η K περιέχει τον κύκλο, ας πούμε τον (123), τότε περιέχει κάθε άλλο κύκλο $(\alpha_1\alpha_2\alpha_3)$. Θεωρούμε τη μετάθεση

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & \cdots \\ \alpha_1 & \alpha_2 & \alpha_3 & \kappa & \lambda & \cdots \end{pmatrix}$$

Αν η σ είναι άρτια έχει καλώς. Αν είναι περιττή, τότε θεωρούμε τη μετάθεση

$$\sigma' = (\kappa\lambda)\sigma = (\kappa\lambda)\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & \cdots \\ \alpha_1 & \alpha_2 & \alpha_3 & \kappa & \lambda & \cdots \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & \cdots \\ \alpha_1 & \alpha_2 & \alpha_3 & \lambda & \kappa & \cdots \end{pmatrix}$$

που είναι άρτια. Άρα ευθύς εξ αρχής μπορούμε να υποθέσουμε ότι η σ είναι άρτια.
Τότε $\sigma(123)\sigma^{-1} = (\sigma(1)\sigma(2)\sigma(3)) = (\alpha_1\alpha_2\alpha_3)$.
Συνεπώς, αν η K περιέχει έναν 3-κύκλο, τότε περιέχει όλους τους 3-κύκλους και επομένως $K = A_n$. Υποθέτουμε ότι αυτό δεν συμβαίνει, δηλαδή η K δεν περιέχει κανέναν 3-κύκλο. Θα καταλήξουμε σε άτοπο.
Από όλα τα μη τετριμμένα στοιχεία της K $\big($και έχει, γιατί $K \neq 1\big)$ θεωρούμε κάποιο, το οποίο σταθεροποιεί τον μέγιστο αριθμό συμβόλων από το $\{1, 2, \ldots, n\}$. Έστω αυτό το α. Πώς γράφεται το α ως γινόμενο ξένων κύκλων, **παραλείποντας φυσικά τους κύκλους μήκους** 1**;**

1) Έστω ότι το α γράφεται στη μορφή $\alpha = (j_1j_2j_3\cdots)\gamma$, όπου γ γινόμενο ξένων κύκλων μήκους ≥ 2 και ξένων προς τον $(j_1j_2j_3\cdots)$. Είναι όμως δυνατόν $\gamma = 1$. Το α μετακινεί 3 τουλάχιστον σύμβολα, τα j_1, j_2 και j_3. Επειδή το α δεν είναι 3-κύκλος θα μετακινεί περισσότερα, γιατί αλλιώς $\gamma = 1$ και $\alpha = (j_1j_2j_3)$. Δεν μπορεί να μετακινεί μόνον 4, πχ. τα j_1, j_2, j_3, j_4 γιατί τότε $\gamma = 1$ $\big($αλλιώς ο γ θα μετακινεί τουλάχιστον 2 σύμβολα$\big)$ και επομένως $\alpha = (j_1j_2j_3j_4) = (j_1j_4)(j_1j_3)(j_1j_2)$ περιττή μετάθεση. Επομένως το α μετακινεί τουλάχιστον 5 σύμβολα, έστω τα j_1, j_2, j_3, j_4 και j_5. Έστω $\beta = (j_3j_4j_5)$ και $\alpha_1 = \beta\alpha\beta^{-1} = (j_1j_2j_4\cdots)\beta\gamma\beta^{-1} \in K$. Επειδή οι $(j_1j_2j_3\cdots)$ και γ είναι ξένες μεταθέσεις και οι $\beta(j_1j_2j_3\cdots)\beta^{-1}$ και $\beta\gamma\beta^{-1}$ είναι ξένες. Επειδή $\alpha(j_2) = j_3$ και $\alpha_1(j_2) = j_4$, έπεται ότι $\alpha \neq \alpha_1$ και επομένως $\alpha_1\alpha^{-1} = \beta\alpha\beta^{-1}\alpha^{-1} \neq 1$. Τώρα, το β σταθεροποιεί όλους τους αριθμούς j_i με $i > 5$. Επίσης, όσα j_i με $i > 5$ σταθεροποιούνται και από το α, τότε αυτοί σταθεροποιούνται και από το $\beta\alpha\beta^{-1}\alpha^{-1} \in K$. Είδαμε ότι το α μετακινεί τους j_1, j_2, j_3, j_4 και j_5. Αλλά $\beta\alpha\beta^{-1}\alpha^{-1}(j_2) = \beta\alpha\beta^{-1}(j_1) = \beta\alpha(j_1) = \beta(j_2) = j_2$. Επομένως το $\beta\alpha\beta^{-1}\alpha^{-1}$ σταθεροποιεί περισσότερους $\big($κατά έναν$\big)$ αριθμούς απ᾽ ότι το α, άτοπο λόγω της εκλογής του α.

2) Έστω ότι το α γράφεται ως γινόμενο αρτίου πλήθους ξένων αντιμεταθέσεων. Έστω πχ. ότι $\alpha = (j_1j_2)(j_3j_4)\gamma$. Θέτουμε πάλι $\beta = (j_3j_4j_5)$ και παίρνουμε $\alpha_1 = \beta\alpha\beta^{-1} = (j_1j_2)(j_4j_5)\beta\gamma\beta^{-1}$. Επειδή οι $(j_1j_2)(j_3j_4)$ και γ είναι ξένες μεταθέσεις και οι $\beta(j_1j_2)(j_3j_4)\beta^{-1} = (j_1j_2)(j_4j_5)$ και $\beta\gamma\beta^{-1}$ είναι ξένες. Επειδή $\alpha(j_4) = j_3$ και $\alpha_1(j_4) = (j_1j_2)(j_4j_5)\beta\gamma\beta^{-1}(j_4) = j_5$, άρα $\alpha_1 \neq \alpha \Leftrightarrow \Leftrightarrow \alpha_1\alpha^{-1} = \beta\alpha\beta^{-1}\alpha^{-1} \neq 1$. Και πάλι το ίδιο επιχείρημα: Το β σταθεροποιεί όλους τους αριθμούς j_i, με $i > 5$. Όσοι από αυτούς σταθεροποιούνται και από το α, τότε σταθεροποιούνται και από το $\beta\alpha\beta^{-1}\alpha^{-1}$. Από τους αριθμούς j_1, j_2, j_3, j_4 και j_5 το α μετακινεί τους j_1, j_2, j_3, j_4. Για το j_5 δεν ξέρουμε. Άρα το α σταθεροποιεί το πολύ έναν από τους j_1, j_2, j_3, j_4 και j_5. Αλλά $\beta\alpha\beta^{-1}\alpha^{-1}(j_1) = \beta\alpha\beta^{-1}(j_2) = \beta\alpha(j_2) = \beta(j_1) = j_1$ και $\beta\alpha\beta^{-1}\alpha^{-1}(j_2) = \beta\alpha\beta^{-1}(j_1) = \beta\alpha(j_1) = \beta(j_2) = j_2$. Επομένως το $\beta\alpha\beta^{-1}\alpha^{-1}$ σταθεροποιεί τουλάχιστον έναν παραπάνω απ᾽ ό,τι το α. Άτοπο λόγω της εκλογής του α. ■

ΠΟΡΙΣΜΑ 2. Η S_n και η A_n δεν είναι επιλύσιμες, για $n \geq 5$.

Απόδειξη: Αν η S_n ήταν επιλύσιμη, τότε θα ήταν και η $A_n \lhd S_n$ επιλύσιμη. Εφόσον η A_n είναι απλή, τότε θα έπρεπε να είναι αβελιανή. Προφανώς αυτό δεν συμβαίνει για $n \geq 4$.
Το ότι η A_n είναι μη επιλύσιμη, για $n \geq 5$ προκύπτει και από την ακόλουθη παρατήρηση:

Έστω $(\alpha\beta\gamma) \in A_n$. Εφόσον $n \geq 5$, υπάρχουν άλλα δύο σύμβολα δ, ε.
Τότε $(\alpha\beta\gamma) = [(\alpha\gamma\beta), (\beta\gamma)(\delta\varepsilon)] \in A'_n$. Επομένως $A'_n = A_n$, για $n \geq 5$ και η A_n μη αβελιανή. ■

ΑΣΚΗΣΗ 3. Έστω $|G| = 8p^n$, όπου n θετικός ακέραιος και p πρώτος. Τότε η G είναι επιλύσιμη.
Απόδειξη: Προσπερνάμε τις απλές περιπτώσεις $p = 2$ ή $P \lhd G$, όπου $|P| = p^n$. (γιατί;) Έχουμε δύο επιλογές: **1)** $p = 3$ και τέσσερις 3-υποομάδες του Sylow και **2)** $p = 7$ και οκτώ 7-υποομάδες του Sylow.
1) $|G| = 8 \cdot 3^n$. Η αναπαράσταση με τα σύμπλοκα της 3-υποομάδας μας πάει στην S_8. Αντ' αυτού παίρνουμε τη δράση μέσω συζυγίας της G στις 4 υποομάδες $P = P_1, P_2, P_3, P_4$ τάξης 3^n. Η δράση είναι μεταβατική, άρα ο επαγόμενος ομομορφισμός $\varphi : G \to S_4$ μη τετριμμένος. Πυρήνας είναι η υποομάδα $H = \bigcap_{i=1}^{4} N_G(P_i)$. Αν $H = 1$, τότε η φ είναι μονομορφισμός και άρα $G \cong \mathrm{Im}\varphi \leqslant S_4$, άρα επιλύσιμη γιατί η S_4 είναι επιλύσιμη. (Σε αυτή την περίπτωση $G \cong S_4$, γιατί $|G| \geq 8 \cdot 3 = |S_4|$). Έστω $H \neq 1$. Επειδή έχουμε μία G-τροχιά, $4 = |G : \mathrm{Stab}_G(P_1)| = |G : N_G(P_i)|$, άρα $|N_G(P_i)| = 2 \cdot 3^n$, άρα επιλύσιμη (επειδή $2 \not\equiv 1 \mod 3$ έχουμε μία μόνο 3-υποομάδα του Sylow στην $N_G(P_i)$, άρα κανονική δείκτου 2 στην $N_G(P_i)$) για κάθε $i = 1, 2, 3, 4$. $H \leqslant N_G(P_1)$ και επειδή η $N_G(P_1)$ είναι επιλύσιμη και η H είναι επιλύσιμη. Επομένως $H = \mathrm{Ker}\varphi$ και $G/H \cong \mathrm{Im}\varphi$ επιλύσιμες, συνεπώς και η G επιλύσιμη.
2) $|G| = 8 \cdot 7^n$. Αν $n \geq 2$, τότε ο ομομορφισμός $\varphi : G \to S_8$ που προκύπτει από τη δράση της G στα αριστερά σύμπλοκα της P, όπου $|P| = 7^n$ (P μια 7-υποομάδα του Sylow της G) έχει πυρήνα μια μη τετριμμένη υποομάδα της P, γιατί αν $G \cong \varphi(G) \leqslant S_8$, τότε επειδή $7^2 \mid |G|$ θα έχουμε $7^2 \mid |S_8| = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot 7 \cdot 8$, άτοπο. Επειδή οι μόνες δυνάμεις του 7 που διαιρούν την τάξη της $\varphi(G) \leqslant S_8$ είναι το $7^0 = 1$ ή το 7 και επειδή $\mathrm{Ker}\varphi \leqslant P$, έπεται ότι $|\mathrm{Ker}\varphi| = 7^n$ ή 7^{n-1}. Σε κάθε περίπτωση ο πυρήνας $\mathrm{Ker}\varphi$ είναι επιλύσιμος. Επομένως η τάξη της $G_1 = G/\mathrm{Ker}\varphi \cong \varphi(G)$ είναι 8 ή $8 \cdot 7$. Στην πρώτη περίπτωση η G_1 είναι επιλύσιμη. Στη δεύτερη περίπτωση, αν $P_1 \lhd G_1$, όπου $|P_1| = 7$, τότε G_1 επιλύσιμη. Αλλιώς έχουμε 8 το πλήθος 7-υποομάδες του Sylow στην G_1, άρα $8 \cdot (7-1) = 48$ στοιχεία τάξεως 7. Επειδή $|G_1| = 8 \cdot 7 = 56$, απομένουν 8 στοιχεία που αποτελούν τη μοναδική 2-υποομάδα του Sylow, ας την πούμε Q. Επομένως $Q \lhd G_1$ και η G_1 πάλι επιλύσιμη. Σε κάθε περίπτωση η $G_1 = G/\mathrm{Ker}\varphi$ είναι επιλύσιμη. Άρα και η G επιλύσιμη. ■

ΑΣΚΗΣΗ 4. Η S_n εμφυτεύεται στην A_{n+2}, για κάθε n, αλλά όχι στην A_{n+1}, για $n \geq 2$.
Απόδειξη: Ορίζουμε την απεικόνιση $\varphi : S_n \to A_{n+2}$ ως εξής:

$$\varphi(\alpha) = \begin{cases} \alpha, & \text{αν } \alpha \text{ άρτια}, \\ \alpha \cdot (n, n+1), & \text{αν } \alpha \text{ περιττή}. \end{cases}$$

Παρατηρούμε ότι $\alpha \cdot (n, n+1) = (n, n+1) \cdot \alpha$, για κάθε $\alpha \in S_n$. Εύκολα επαληθεύεται ότι $\varphi(\alpha\beta) = \varphi(\alpha)\varphi(\beta)$ για κάθε μία από τις περιπτώσεις: α και β άρτιες, α και β περιττές, α άρτια και β περιττή και α περιττή και β άρτια. Επίσης από τον ορισμό της φ προκύπτει ότι $\mathrm{Ker}\varphi = 1$. (Συμπληρώστε τις λεπτομέρειες).

Αν η S_n εμφυτευόταν στην A_{n+1} μέσω της εμφύτευσης $S_n \overset{\vartheta}{\hookrightarrow} A_{n+1}$, τότε $H = \vartheta(S_n) \cong S_n$ και $H \leqslant A_{n+1}$. Τότε $|A_{n+1} : H| = \dfrac{\frac{(n+1)!}{2}}{n!} = \dfrac{n+1}{2} \in \mathbb{Z}$, άρα $n+1$ άρτιος, δηλαδή n περιττός. Σε αυτή την περίπτωση θεωρούμε τη δράση της A_{n+1} επί των αριστερών συμπλόκων της H. Αυτή επάγεται έναν ομομορφισμό $\tau : A_{n+1} \to S_{\frac{n+1}{2}}$ με πυρήνα $K = \bigcap_{x \in A_{n+1}} xHx^{-1}$.

Έχουμε $\mathrm{Im}\tau \leqslant S_{\frac{n+1}{2}} \Rightarrow |\mathrm{Im}\tau| \leq |S_{\frac{n+1}{2}}| = \left(\dfrac{n+1}{2}\right)!$, άρα $\dfrac{|A_{n+1}|}{|K|} = \dfrac{(n+1)!}{2|K|} \leq \left(\dfrac{n+1}{2}\right)!$. Αλλά για $n \geq 4$ η A_{n+1} είναι απλή. Επομένως $K = 1$ και η τ είναι μονομορφισμός. Επομένως $\dfrac{(n+1)!}{2} \leq \left(\dfrac{n+1}{2}\right)! \Leftrightarrow (n+1)! \leq 2\left(\dfrac{n+1}{2}\right)!$. Όμως για κάθε περιττό $n \geq 3$ έχουμε $(n+1)! > 2 \cdot \left(\dfrac{n+1}{2}\right)!$. Πράγματι, για $n = 3$ έχουμε $(3+1)! = 4! > 4 = 2 \cdot 2! = 2 \cdot \left(\dfrac{3+1}{2}\right)!$. Αν για κάποιον περιττό n έχουμε $(n+1)! > 2 \cdot \left(\dfrac{n+1}{2}\right)!$, τότε ο επόμενος περιττός είναι ο $n+2$, οπότε $(n+3)! = (n+3)(n+2)(n+1)! > 2(n+2)\left(\dfrac{n+3}{2}\right)(n+1)! > \left(\dfrac{n+3}{2}\right)(n+1)! > \left(\dfrac{n+3}{2}\right) \cdot 2 \cdot \left(\dfrac{n+1}{2}\right)! = 2 \cdot \left(\dfrac{n+3}{2}\right)!$
Επομένως για $n \geq 5$ περιττό η S_n δεν εμφυτεύεται στην A_{n+1}.
Για $n = 3$, $|S_3| = 6$ και $|A_4| = 12$. Αν η S_3 εμφυτεύτετο στην A_4, τότε η A_4 θα είχε μια (κανονική) υποομάδα $H \cong S_3$ δείκτου 2. Πράγματι, σε μια τέτοια περίπτωση η A_4/H θα ήταν κυκλική τάξης 2. Επομένως $\alpha^2 \in H$, για κάθε $\alpha \in A_4$. Αν α είναι ένας 3-κύκλος τότε $\alpha^2 \in H$, άρα και $\alpha^4 = (\alpha^2)^2 \in H$. Αλλά $\alpha^4 = \alpha^3\alpha = \alpha$. Συνεπώς $\alpha \in H$, για κάθε κύκλο μήκους 3. Επειδή η A_4 παράγεται από όλους τους κύκλους μήκους 3, θα είχαμε $H = A_4$, άτοπο. ■