1.60. Tétel. Ha $n \geq 5$, akkor az A_n alternáló csoport egyszerű.

1.61. Tétel. Ha $n \geq 5$, akkor az S_n szimmetrikus csoport egyetlen valódi nemtriviális normálosztója A_n.

Bizonyítás. Legyen $\{\mathrm{id}\} < N \lhd S_n$; célunk belátni, hogy $N = A_n$ vagy $N = S_n$. Tekintsünk egy $\sigma \in N \backslash \{\mathrm{id}\}$ permutációt.

1. lépés: Létezik olyan $\tau \in S_n$ transzpozíció, amelyre $\sigma\tau \neq \tau\sigma$.
Mivel $\sigma \neq \mathrm{id}$, létezik olyan $i \in \{1, \ldots, n\}$, amelyre $j := i\sigma \neq i$. Legyen $k \in \{1, \ldots, n\} \setminus \{i, j\}$, és legyen $\tau = (jk)$. Ekkor $i(\sigma\tau) = (i\sigma)\tau = j\tau = k$ és $i(\tau\sigma) = (i\tau)\sigma = i\sigma = j$. Tehát az i elem képe $\sigma\tau$ és $\tau\sigma$ mellett különböző, és így $\sigma\tau \neq \tau\sigma$.

2. lépés: $\sigma^{-1}\tau^{-1}\sigma\tau \in N$.
Tudjuk, hogy $\sigma \in N$ és σ normálosztó, azaz zárt a konjugálásra, ezért $\tau^{-1}\sigma\tau \in N$. Másrészt $\sigma^{-1} \in N$ (mert N zárt az inverzképzésre), tehát $\sigma^{-1} \cdot \tau^{-1}\sigma\tau \in N$ (mert N zárt a szorzásra).

3. lépés: $\sigma^{-1}\tau^{-1}\sigma\tau$ vagy kettős transzpozíció (azaz két idegen transzpozíció szorzata) vagy pedig 3 hosszúságú ciklus.
A $\sigma^{-1}\tau^{-1}\sigma$ permutáció konjugáltja a $\tau^{-1} = \tau$ transzpozíciónak, ezért maga is transzpozíció (az 1.54. Tétel szerint). Tehát $\sigma^{-1}\tau^{-1}\sigma\tau$ két transzpozíció szorzata: $\sigma^{-1}\tau^{-1}\sigma \cdot \tau = (ab)(cd)$.[1] Három eset lehetséges aszerint, hogy az (ab) és (cd) transzpozícióknak hány közös mozgatott eleme van.

(a) $|\{a, b\} \cap \{c, d\}| = 0$: Ekkor (ab) és (cd) idegenek, ezért $\sigma^{-1}\tau^{-1}\sigma\tau$ kettős transzpozíció.

(b) $|\{a, b\} \cap \{c, d\}| = 1$: Tegyük fel például, hogy $b = c$ (de a, b, d páronként különbözőek). Ekkor $\sigma^{-1}\tau^{-1}\sigma\tau = (ab)(cd) = (ab)(bd) = (adb)$, ami egy három hosszúságú ciklus.

(c) $|\{a, b\} \cap \{c, d\}| = 2$: Ekkor $(ab) = (cd)$, ezért $\sigma^{-1}\tau^{-1}\sigma\tau = (ab)(cd) = (ab)(ab) = \mathrm{id}$. Node ez nem lehetséges, mert $\sigma^{-1}\tau^{-1}\sigma\tau = \mathrm{id} \iff \sigma\tau = \tau\sigma$, és az 1. lépésben a τ transzpozíciót úgy választottuk, hogy ne legyen felcserélhető σ-val.

4. lépés: N tartalmazza az összes 3 hosszúságú ciklust.
Az előző lépésben látott két esetet vizsgáljuk most is.

(a) Ha N tartalmaz egy kettős transzpozíciót, akkor minden kettős transzpozíciót tartalmaz, mert ezek mind egymás konjugáltjai (az 1.54. Tétel szerint), és N zárt a konjugálásra. Ha $a, b, c \in \{1, \ldots, n\}$ páronként különböző elemek, akkor az (abc) ciklus előáll két kettős transzpozíció szorzataként: $(abc) = (ab)(ac) = (ab)(de) \cdot (de)(ac)$. Itt a $d, e \in \{1, \ldots, n\}$ elemeket úgy kell megválasztani, hogy a, b, c, d, e páronként különbözőek legyenek (itt használjuk fel, hogy $n \geq 5$!). Az $(ab)(de)$ és $(de)(ac)$ kettős transzpozíciók a fentiek szerint N-ben vannak, így $(abc) \in N$ (mert N zárt a szorzásra).

(b) Ha N tartalmaz egy hármas ciklust, akkor minden hármas ciklust tartalmaz, mert ezek mind egymás konjugáltjai (az 1.54. Tétel szerint), és N zárt a konjugálásra.

5. lépés: $N = A_n$ vagy $N = S_n$.
Mivel a hármas ciklusok generálják az A_n csoportot (lásd a cserélgetős játékot), a 4. lépésből következik, hogy $N \geq A_n$. Ebből következik, hogy N indexe osztója A_n indexének, tehát $[S_n : N] = 1$ vagy $[S_n : N] = 2$. Az első esetben $N = S_n$, a második esetben $N = A_n$. □

Megjegyzés. A fenti két tétel $n = 3$ esetén is igaz (könnyű ellenőrizni), de $n = 4$ esetén nem: A_4 normálosztói $\{\mathrm{id}\}, V, A_4$, míg S_4 normálosztói $\{\mathrm{id}\}, V, A_4, S_4$.

Megjegyzés. Az 1.61. Tételt viszonylag könnyen le lehet vezetni az 1.60. Tételből (de azt nem bizonyítottuk). A másik irányban kézenfekvőnek tűnhet a következő gondolatmenettel levezetni az 1.60. Tételt az 1.61. Tételből: Ha $N \lhd A_n$, akkor $A_n \lhd S_n$ miatt $N \lhd A_n \lhd S_n$, TEHÁT $N \lhd S_n$. Az 1.61. Tétel szerint ekkor $N = \{\mathrm{id}\}$ vagy $N = A_n$ vagy $N = S_n$. A harmadik eset nem lehetséges, mert $N \subseteq A_n$, és ezzel meg is kaptuk, hogy A_n-nek csak két normálosztója van, mégpedig $\{\mathrm{id}\}$ és A_n. Ez a gondolatmenet azonban **hibás**! A hiba a „TEHÁT” szónál van: a normálosztóság nem tranzitív reláció. Például $\{\mathrm{id}, (12)(34)\} \lhd V$ (miért?) és $V \lhd S_4$ (órán láttuk), de ennek ellenére $\{\mathrm{id}, (12)(34)\} \not\lhd S_4$ (miért?). Valójában az 1.60. Tétel valamivel nehezebb az 1.61. Tételnél. A nehézség egyik oka, hogy az alternáló csoportban nem olyan szép a konjugáltsági reláció, mint a szimmetrikus csoportban: ha két permutáció egymás konjugáltja A_n-ben, akkor továbbra is azonos ciklusszerkezetűek, de két azonos ciklusszerkezetű permutáció nem mindig konjugált A_n-ben (S_n-ben persze igen, de a „konjugáló” permutáció nem biztos, hogy A_n-ben van). Ezt illusztrálják a feladatsorban a 34. és 35. feladatok (pluszpontért elmondható a megoldásuk gyakorlaton).

[1] A kellemesebb jelölés kedvéért $\tau = (jk)$ helyett $\tau = (cd)$ szerepel.