Groupes symétriques et alternés. Générateurs, simplicité

Références : [P] : D. Perrin, cours d'algèbre [D] : J. Dekont, théorie des groupes
[U] : F. Ulmer, théorie des groupes

1) Rappels et notations (Voir par exemple [P], I.0, I.1, [D], 2.4)

- S_n désigne le groupe symétrique sur $\{1, \dots, n\}$. $|S_n| = n!$

Plus généralement, si E est un ensemble, on note S_E le groupe symétrique de E, i.e le groupe des bijections de E dans E.

- Le support d'une permutation $\sigma \in S_n$ est $\mathrm{supp}(\sigma) = \{ i \in [\![1, n]\!] \mid \sigma(i) \neq i \}$ (on peut vérifier que $\sigma(\mathrm{supp}(\sigma)) = \mathrm{supp}(\sigma)$ et que 2 permutations à supports disjoints commutent)
- Un k-cycle (ou cycle de longueur k) est une permutation σ telle que

$$\mathrm{supp}(\sigma) = \{a_1, \dots, a_k\}, \quad \sigma(a_i) = a_{i+1}, \ 1 \leq i \leq k-1, \quad \sigma(a_k) = a_1$$

et noté $(a_1\ a_2\ \dots\ a_k)$. En particulier, σ est d'ordre k.

Remarque : on a $(a_1\ a_2 \dots a_k) = (a_2\ a_3 \dots a_k\ a_1)$, etc.... Il y a donc $(k-1)!$ k-cycles à support fixé et par conséquent $(k-1)!\binom{n}{k} = \dfrac{n!}{k(n-k)!}$ k-cycles dans S_n

- On peut vérifier que $\forall \sigma \in S_n$, $\sigma(a_1\ a_2 \dots a_k)\sigma^{-1} = (\sigma(a_1)\ \sigma(a_2) \dots \sigma(a_k))$ (*)

L'ensemble des k-cycles forment donc une classe de conjugaison

Exercice (1) : Soit $\sigma \in S_n$ un k-cycle. Calculer l'ordre de son centralisateur $C_{S_n}(\sigma)$ et en déduire que $C_{S_n}(\sigma) = \langle \sigma \rangle \simeq \mathbb{Z}/n\mathbb{Z}$ lorsque σ est un n-cycle.

Théorème 1.1 (Décomposition en cycles disjoints) : toute permutation σ s'écrit sous la forme $\sigma = c_1 \dots c_p$ où les c_i sont des cycles à supp 2 à 2 disjoints. Cette écriture est unique à permutation près des facteurs.

De plus $o(\sigma) = \mathrm{ppcm}(\ell(c_i), i = 1, \dots, p)$ ($\ell(c_i)$ = Longueur de c_i)

~

(1)

Exercice : Soit $\sigma \in S_n$ un k-cycle. Calculer l'ordre de son centralisateur $C_{S_n}(\sigma)$ et en déduire que $C_{S_n}(\sigma) = \langle \sigma \rangle \simeq \mathbb{Z}/n\mathbb{Z}$ lorsque σ est n-cycle.

$\sim$

$$C_{S_n}(\sigma) = \{\sigma' \in S_n \quad \sigma' \sigma \sigma'^{-1} = \sigma\}$$

σ k-cycle

$$|C_{S_n}(\sigma)| = \frac{|S_n|}{\#\{k\text{-cycles}\}} = k(n-k)!$$

(relation orbite stabilisateur pour l'action $S_n \curvearrowright S_n$ par conjugaison).

Remarques : si σ est un n-cycle, on obtient que

$\langle \sigma \rangle$ est bien maximal

en effet : $|C_{S_n}(\sigma)| = n = |\langle \sigma \rangle|$

• on peut aussi calculer l'ordre du centralisateur d'une permutation quelconque en termes de sa décomposition en cycle, cf [D], exercice 2.4.13

t

un

Principe de calcul de la décomposition : orbites de $\{1, \dots, n\}$ sous $\langle \sigma \rangle$ (voir par exemple [U], th 5.4)

De (*) et de l'unicité de la décomposition, on déduit que σ_1 et $\sigma_2 \in S_n$ sont conjuguées ssi elles ont le même nombre de cycles de longueur identiques dans leur décomposition.

Application, exercice : Noter que $\sigma_1, \sigma_2 \in S_7$ définies par (1) bis

$$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 4 & 5 & 6 & 7 & 2 & 1 \end{pmatrix}, \quad \sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 3 & 1 & 5 & 6 & 7 & 4 \end{pmatrix}$$

sont conjuguées dans S_7 et trouver une permutation qui les conjugue.

+ Description des classes de conjugaison dans S_5.

- **Signature** : $\varepsilon : S_n \longmapsto \{-1, 1\}$ $(\simeq \mathbb{Z}/2\mathbb{Z})$

Déf formelle (peu utilisée) : $\varepsilon(\sigma) = \prod_{1 \leq i < j \leq n} \frac{\sigma(i) - \sigma(j)}{i - j}$

Dans la pratique, on utilise que a) ε est un morphisme

b) $\varepsilon((a_1 \cdots a_p)) = (-1)^{p+1}$

(cf par exemple [U], 5.3)

Exemple : $\varepsilon(\sigma_1) \overset{(2)}{=} \dots = (-1)^4 \cdot (-1)^5 = -1$

Définition 1.2 (groupe alterné)

$A_n = \ker \varepsilon$. (et donc $A_n \lhd S_n$)

Remarquer que $|A_n| = \frac{n!}{2}$ si $n \geq 2$ (ε est surjective)

2) Générations

Théorème 2.1 : S_n est engendré par les transpositions (i.e les cycles de longueur 2)

preuve : $(a_1 \cdots a_p) = (a_1\ a_p)(a_1\ a_{p-1}) \cdots (a_1\ a_2)$ + déc en cycles (th 1.1)

Exercices d'application :

- ($n \geq 2$) Noter que ε est le seul morphisme non trivial $S_n \longmapsto \mathbb{C}^*$ et en déduire que A_n est le seul sous-groupe d'indice 2 de S_n. (3)
- Soit V un $\mathbb{K}$ e.v de dim $= n$, $(e_i)_{1 \leq i \leq n}$ une base et Ψ le plongement de S_n dans $GL(V)$ défini par

(1) bis Exercice : Montrer que $\sigma_1, \sigma_2 \in S_7$ définies par $\sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 4 & 5 & 6 & 7 & 2 & 1 \end{pmatrix}$, $\sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 3 & 1 & 5 & 6 & 7 & 4 \end{pmatrix}$ sont conjuguées dans S_7 et trouver une permutation les conjugue.

+ Description des classes de conjugaison dans S_5.

$\sim$

$\begin{cases} \sigma_1 = (1\,3\,5\,7)(2\,4\,6) \\ \sigma_2 = (1\,2\,3)(4\,5\,6\,7) \end{cases}$ de type $(3,4)$

On cherche $\sigma \in S_7$

$\sigma \sigma_1 \sigma^{-1} = \sigma_2$

$\| $

$(\sigma(1)\ \sigma(3)\ \sigma(5)\ \sigma(7))(\sigma(2)\ \sigma(4)\ \sigma(6))$

$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 1 & 5 & 2 & 6 & 3 & 7 \end{pmatrix}$

$\sim$

Classes de conjugaison dans S_5

$\{Id\}$, 2, 3, 4, 5 cycles

$(2,2)$: $\{(a\,b)(c\,d)\}$ à supp disjoints

$(2,3)$ (ppcm ordre est $2 \times 3 = 6$)

En tout $\underline{7}$ classes de conjugaisons ($=$ # partitions de 5)

(3)

Exercices d'application :

- ($n \geq 2$) Montrer que ε est le seul morphisme non trivial $S_n \to \mathbb{C}^*$ et en déduire que A_n est le seul sous-groupe d'indice 2 de S_n. (3)

Soit $\varphi : S_n \to \mathbb{C}^*$ un morphisme

τ transposition

on a $\varphi(\tau)^2 = \varphi(\tau^2) = \varphi(Id) = 1$

$\Rightarrow \varphi(\tau) = \pm 1$

Soit τ' une transposition

$\exists \sigma \in S_n \mid \tau' = \sigma \tau \sigma^{-1}$

on a donc $\varphi(\tau') = \varphi(\tau)$ (car $\mathbb{C}^*$ est abélien)

Puisque $S_n = \langle$ transpositions $\rangle$, on a donc

que φ ~~ε~~ $(S_n) = 1$ $(\varphi(\tau) = 1)$

ou

$\varphi = \varepsilon$ $(\varphi(\tau) = -1)$

Soit $H \subset S_n$, $[S_n : H] = 2$. On a donc $H \lhd S_n$ et on peut identifier le groupe quotient à $\{-1, 1\} \subset \mathbb{C}^*$

on a un morphisme non trivial (projection canonique)

$\Pi : S_n \to \frac{S_n}{H} = \{-1, 1\}$, nécessairement donné par la signature d'après le 1er point. Par suite $H = \ker \Pi = \ker \varepsilon = A_n$.

Remarque : on peut aussi utiliser que $D(S_n) = A_n$ (cf Th 3.2 ci-dessus : en effet puisque $\frac{S_n}{H} \simeq \mathbb{Z}/2\mathbb{Z}$ est abélien, on a $D(S_n) = A_n \subset H$ (D le groupe dérivé). Donc $A_n = H$ par des raisons évidentes d'indice.

$\Psi(\sigma)(e_i) = e_{\sigma(i)}$. Vérifier que $\varepsilon(\sigma) = \det \Psi(\sigma)$ ($k = \mathbb{C}$) (4)

Remarque : Soit G un groupe fini ; via le plongement de Cayley $G \hookrightarrow S_G \simeq S_{|G|}$ et Ψ, on peut plonger G dans $GL(V)$ $\dim_k V = |G|$ (représentation régulière, [U] p 145). Voir aussi l'utilité de cette construction dans la preuve du 1er théorème de Sylow ([P], I.5 p 19).

- $S_n = \langle (1\,2), (1\,2\,3 \ldots n) \rangle$ ([U], ex 5.5) (5)

Théorème 2.2

$A_n = \langle$ 3-cycles $\rangle$

Preuve : A_n st engendré par les $(a\,b)(c\,d)$ = produit d'au plus deux 3-cycles (cf [P] I.1 p 11)

∨

3) Centre et groupe dérivé

Théorème 3.1 (centre)

a) $Z(S_n) = \{Id\}$ si $n \geq 3$

b) $Z(A_n) = \{Id\}$ si $n \geq 4$ (Rque : $A_3 = \langle (1\,2\,3) \rangle \simeq \mathbb{Z}/3\mathbb{Z}$ et donc $Z(A_3) = A_3$)

Preuve a) Soit $\sigma \in S_n \setminus \{Id\}$ et $i \neq j$ / $\sigma(i) = j$. On a $\tau\sigma \neq \sigma\tau$ où $\tau = (j\,k)$, $k \neq i, j$ (cf [P], I.3, Exemples 3.2)

b) Même principe en remplaçant τ par un 3-cycle approprié

∨

Théorème 3.2 (groupes dérivés) (voir [P], I.8, th 8.1)

a) $D(S_n) = A_n$

b) $D(A_n) = A_n$ pour $n \geq 5$

Preuve : a) $D(S_n) \subset A_n$ car $\varepsilon([\sigma_1, \sigma_2]) = 1$, tout 3-cycle est un commutateur (les 3-cycles sont conjugués dans S_n) + th. 2.2 (on explique : astuce du commutateur) (6)

b) Même idée en exploitant que les 3-cycles sont conjugués dans A_n, $n \geq 5$. (pourquoi ? (7))

(4) $\varepsilon(\sigma) = \det(\Psi(\sigma))$?

$\det : \Psi(S_n) \xrightarrow{\sim} \mathbb{C}^*$ morphisme

$\Psi(S_n) \subset S_n$

D'après B) on a soit $\det \equiv 1$

soit $\forall \sigma \in S_n$, $\det(\Psi(\sigma)) = \varepsilon(\sigma)$

c'est le cas :

$$\det \Psi((1\,2)) = \det \left(\begin{array}{cc|c} 0 & 1 & \\ 1 & 0 & 0 \\ \hline & 0 & I_{n-2} \end{array} \right)$$

$= -1$

et on conclut par (3).

(5) $H = \langle (1\ 2), (1\ 2\ 3\ \dots\ n) \rangle = S_n$?

τ " $\sim$ " σ

on a $\sigma \tau \sigma^{-1} = (\sigma(1)\ \sigma(2)) = (2\ 3) \in H$

De même, $(3,4) = \sigma (2\ 3) \sigma^{-1} \in H$

etc...

$\blacktriangleright$ $(i\ i+1) \in H \quad 1 \le i \le n-1$

De plus $(i+1\ i+2)(i\ i+1)(i+1\ i+2) = (i+2\ \ i) \in H$

on a de même $(1\ i+3) \in H$

etc. et finalement, $(i\ j) \in H \quad \forall\ 1 \le i < j \le n$

D'où $H = S_n$ puisque $S_n = \langle$ transpositions $\rangle$

(6) + (7) : $\sim$ **Astuce du commutateur** $\sim$ (Voir aussi [P], IV.3) c) dans le contexte des groupes linéaires)

(6) : σ 3-cycle. On veut écrire $\sigma = [\sigma_1, \sigma_2] = \sigma_1 \sigma_2 \sigma_1^{-1} \sigma_2^{-1}$?

on a σ^2 est un 3-cycle

$\sigma^2 = \sigma^{-1}$

Donc σ^2 et σ sont conjugués dans S_n

$\Rightarrow \exists\ \sigma_1 \in S_n \mid \sigma^2 = \sigma_1 \sigma \sigma_1^{-1}$

i.e. $\sigma = \sigma_1 \sigma \sigma_1^{-1} \sigma^{-1} = [\sigma_1, \sigma]$

(7) : Comme avant, on a $\sigma^2 = \sigma_1 \sigma \sigma_1^{-1}$

Si $\sigma_1 \in A_n$: OK

Si $\sigma_1 \in S_n \setminus A_n$, on considère τ une transposition telle que $\mathrm{Supp}\,\tau \cap \mathrm{Supp}\,\sigma = \emptyset$ (possible car $n \ge 5$). Posons $\sigma_2 = \sigma_1 \tau$; on a $\sigma_2 \in A_n$ et $\sigma^2 = \sigma_2 \sigma \sigma_2^{-1}$ (car $\tau \sigma = \sigma \tau$) et on se ramène ainsi au cas favorable.

4) Le cas particulier de S_4

Exercice : $\mathcal{D}(A_4) = V_4 = \{Id, (12)(34), (13)(24), (14)(23)\}$ [8]

A_4 et V_4 sont les seuls sous groupes normaux (non triviaux) de S_4

(éventuellement : $S_4 \simeq V_4 \rtimes S_3$) [8]

5) Simplicité

Théorème 5.1 (Galois, 1830), A_n est simple pour $n \geq 5$.

preuve : • $n = 5$, comptage des classes de conjugaison dans A_5 (cf argument donné dans le CCA du 13/1/2020, [P], I.8, [D], Ex 7.10, 7.11)

• $n > 5$ Récurrence sur n [9] ou on se ramène directement au cas $n = 5$ ([P], I.8), ou .....

(Dans tous les cas, on montre que si $H \lhd A_n$ et $H \neq \{Id\}$, alors H contient un 3-cycle et donc $H = A_n$ en vertu du théorème 2.2 et le fait que les 3-cycles sont conjugués dans A_n)

Corollaire 5.2 ($n \geq 5$) Dans S_n, la liste des sous-groupes normaux est $\{Id\}, A_n, S_n\}$ ([P], I.8, corollaire 8.5)

Conséquence ($n \geq 5$) Soit $H \lhd S_n$. En regardant l'action

$S_n \curvearrowright \underbrace{S_n/H}_{\text{classes à gauche mod } H}$ par translations à gauche, on obtient que :

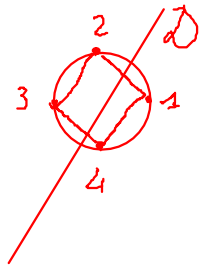
$$\begin{cases} [S_n : H] = 1 \text{ ou } [S_n : H] \geq n & [10] \\ H \simeq S_{n-1} \text{ si } [S_n : H] = n & \| \ (*), \text{ [P], corollaire 8.6} \end{cases}$$

(*) Vrai aussi pour $n \leq 5$, on le fait "à la main"

(8) avec une remarque préliminaire

on a $D(S_4) = A_4$

Rque : on peut plonger D_4 dans S_4 (et $D_n \hookrightarrow S_n$ en général)



$D_4 = \langle (2\,4), (1\,2\,3\,4) \rangle$

$(2\,4)$: $s_{/(Ox)}$; $(1\,2\,3\,4)$: $r_{(0, \pi/2)}$

on a facilement que

$V_4 = \{\sigma \in D_4 \mid \varepsilon(\sigma) = 1\}$ (et c'est donc un ss. groupe de S_4)

Ex $(1\,2)(3\,4)$ correspond à s_D

on a $V_4 \trianglelefteq S_4$

car $\begin{cases} V_4 \leq S_4 \\ V_4$ est une union de classes de conjugaisons

on a $A_4/V_4 \simeq \mathbb{Z}/3\mathbb{Z}$ (car est d'ordre 3)

donc abélien.

Donc $D(A_4) < V_4$ (I U du groupe dérivé)

Soit $D(A_4) = V_4$ ok

Soit $[V_4 : D(A_4)] = 2$ → exclu, sinon $|D(A_4)| = 2$

comme $D(A_4) \trianglelefteq A_4$, on aurait $D(A_4) < Z(A_4) = \{Id\}$

Soit $D(A_4) = \{Id\}$: exclu car A_4 n'est pas abélien ($Z(A_4) = \{Id\}$)

on peut aussi faire des calculs directs de commutateurs .....

Quelques mots sur la structure de produit semi-direct (PSD) sur S_4 :

on a $V_4 \triangleleft S_4$

et $S_3 \subset S_4$, en identifiant S_3 à $\{\sigma \in S_4 \mid \sigma(4) = 4\}$

on vérifie que $S_3 \cap V_4 = \{\mathrm{Id}\}$. Par suite $V_4 S_3 = S_4$

(puisque $|V_4 S_3| = |V_4|\,|S_3| = 4 \times 6 = |S_4|$)

on obtient donc une structure de PSD

$$S_4 \simeq V_4 \rtimes S_3$$

On peut de plus vérifier que le morphisme structurel $S_3 \to \mathrm{Aut}(V_4)$ associé à l'action $S_3 \curvearrowright V_4$ par conjugaison est un isomorphisme.

On dit alors que S_4 est l'holomorphe de V_4

(cf [D], exercice 3.3.12)

(9) On montre que A_n est simple, $n \geq 5$ par récurrence en admettant le résultat pour $n = 5$.

La stratégie est la suivante :

Soit $H \triangleleft A_n$, $n \geq 6$, $H \neq \{\mathrm{Id}\}$. On a aussi $A_{n-1} \subset A_n$ en voyant A_{n-1} comme $\{\sigma \in A_n \mid \sigma(n) = n\}$. Remarquons que $H \cap A_{n-1} \triangleleft A_{n-1}$

Il suffit alors de montrer que $H \cap A_{n-1} \neq \{\mathrm{Id}\}$. En effet, par récurrence, on peut conclure que $H \cap A_{n-1} = A_{n-1}$. En particulier, H contient un 3-cycle et puisque les 3-cycles sont conjugués dans A_n et engendrent A_n, il en résulte que $H = A_n$

Comment montrer que $H \cap A_{n-1} \neq \{Id\}$?

Soit $\sigma \in H$, $\{Id\}$.

1) Si $\sigma(n) = n$: ok

2) Si $\sigma(n) \neq n$, on trouve $\sigma_1 \in A_n$ tel que $\sigma_1 \sigma \sigma_1^{-1}(n) = \sigma(n)$, et $\sigma_1 \sigma \sigma_1^{-1} \neq \sigma$. En considérant $\sigma' = (\sigma_1 \sigma \sigma_1^{-1}) \sigma^{-1}$, on est ramené à 1).

Exercice : trouver σ_1 ! (si besoin, regarder Lemme 3.2 dans l'annexe)

Point culturel : On peut montrer qu'il n'y a pas de groupes simple ($\neq \mathbb{Z}/p\mathbb{Z}$ p premier) d'ordre $\in [\![1, 59]\!]$ et que A_5 est le seul groupe simple d'ordre 60 (cf [P] : chap I, Exercices E. 2) et F. 6))

$\downarrow$

(10)
on montre que pour $n \geq 5$ et $H < S_n$:
$$\begin{cases} [S_n : H] \mid 2 \text{ ou } [S_n : H] \geq n & (1) \\ H \simeq S_{n-1} \text{ si } [S_n : H] = n & (2) \end{cases}$$

Remarque : (1) n'est pas vérifié pour S_4 (considérer $D_4 < S_4$)

(1) : On considère l'action $S_n \curvearrowright S_n/H$ et le morphisme correspondant
$\phi : S_n \longrightarrow S_{S_n/H} \simeq S_{[S_n : H]}$ (Noter que ϕ est non trivial si $H \neq S_n$ puisque $\ker \phi < H$)
on a $\ker \phi \lhd S_n$. On déduit du cor 5.2 que ϕ est injectif si $[S_n : H] \geq 3$, ce qui n'est évidemment possible que si $[S_n : H] \geq n$

(2) si $[S_n : H] = n$, le raisonnement précédent montre qu'on a un isomorphisme $\phi : S_n \longrightarrow S_{n/H}$ et qui induit par restriction un isomorphisme entre $\underset{\hat{S}_n}{H}$ et $\{\sigma \in S_{n/H} \mid \sigma(H) = \underset{S_{n/H}}{\hat{H}}\} \simeq S_{n-1}$

Conséquences (de la conséquence)

Exercices

1) Soit K un corps et $n \geq 5$ et $f \in K[X_1, \dots, X_n]$. Montrer que le nombre de différents polynômes obtenus à partir de f en permutant les variables $X_1, \dots, X_n$ est a) $= 1$ ou b) $= 2$ (11) ou c) $\geq n$

2) Montrer que $\begin{cases} S_5 \simeq PGL(2, \mathbb{F}_5) \\ A_5 \simeq PSL(2, \mathbb{F}_5) \end{cases}$ (13), puis que ([P], IV Prop 5.3)

Dans ([P], loc. cit), on trouve aussi

$$\begin{cases} SL(2, \mathbb{F}_2) = PSL(2, \mathbb{F}_2) \simeq S_3 \\ PSL(2, \mathbb{F}_3) \simeq A_4 \\ PSL(2, \mathbb{F}_4) \simeq A_5 \end{cases} \quad (12)$$

(c'est une façon de voir que $PSL(2, \mathbb{F}_2)$ et $PSL(2, \mathbb{F}_3)$ ne sont pas simples (seules exceptions parmi les $PSL(n, k)$, $n \geq 2$)

On constate que $PSL(2, \mathbb{F}_4) \simeq PSL(2, \mathbb{F}_5)$ ($\simeq A_5$) : c'est un des cas exceptionnels d'isomorphisme (cf liste dans [P], fin du chap IV)

6) Point culturel

On connaît au moins une dizaine de démonstrations de la simplicité de A_n ($n \geq 5$). L'article joint en annexe (in english) en présente 5.

11) 1) Soit K un corps et $n \geq 5$ et $f \in K[X_1, \dots, X_n]$. Montrer que le nombre de différents polynômes obtenus à partir de f en permutant les variables $X_1, \dots, X_n$ est a) $= 1$ ou b) $= 2$ ou c) $\geq n$

Application immédiate du point (1) :

on regarde l'action

$$S_n \curvearrowright K[X_1, \dots, X_n]$$
$$\sigma \cdot (P(X_1, \dots, X_n)) := P(X_{\sigma^{-1}(1)}, \dots, X_{\sigma^{-1}(n)})$$

(on met σ^{-1} pour avoir une action à gauche)

avec $H = Stab_{S_n}(P)$ et en remarquant que ce qu'on cherche est le cardinal de l'orbite de P sous S_n, qui vaut $\frac{|S_n|}{H} = [S_n : H]$.

$\curvearrowright$

12) Remarque préliminaire : on considère la droite projective $\mathbb{P}(\mathbb{F}_q^2)$ sur $\mathbb{F}_q$ (ie : l'ensemble des droites vectorielles du $\mathbb{F}_q$ ev $\mathbb{F}_q^2$).

On a une partition $\mathbb{F}_q^2 - \{0\} = \coprod_{D \in \mathbb{P}(\mathbb{F}_q^2)} D - \{0\}$

Comme $\# D = q$, on a donc

$\frac{q^2 - 1}{q - 1} = q + 1$ éléments dans $\mathbb{P}(\mathbb{F}_q^2)$

De plus le morphisme structurel

$\phi : GL(2, \mathbb{F}_q) \longrightarrow S_{\mathbb{P}(\mathbb{F}_q^2)} \simeq S_{q+1}$ de l'action naturelle de l'action naturelle $GL(2, \mathbb{F}_q) \curvearrowright \mathbb{P}(\mathbb{F}_q^2)$ a pour noyau $\{ \mathrm{Id}, \lambda \in \mathbb{F}_q^* \}$ et induit donc des morphismes injectifs

$\phi_1 : PGL(2, \mathbb{F}_q) \hookrightarrow S_{\mathbb{P}(\mathbb{F}_q^2)}$

$\phi_2 : PSL(2, \mathbb{F}_q) \hookrightarrow S_{\mathbb{P}(\mathbb{F}_q^2)}$

En particulier on a un morphisme injectif

$PSL(2,\mathbb{F}_2) \hookrightarrow S_3$ qui en fait un isomorphisme puisque $|PSL(2,\mathbb{F}_2)| = |S_3| = 6$ (voir [P], chap IV, prop 5.1 pour le calcul des cardinaux de $GL(n,\mathbb{F}_q)$, $SL(n,\mathbb{F}_q)$, $PGL(n,\mathbb{F}_q)$, $PSL(n,\mathbb{F}_q)$)

$\wr$

13) On veut montrer $\begin{cases} PGL(2,\mathbb{F}_5) \simeq S_5 & (1') \\ PSL(2,\mathbb{F}_5) = A_5 & (2') \end{cases}$

$\wr$

(1') D'après la remarque préliminaire, on a un morphisme injectif défini par l'action sur les droites

$\phi_1 : PGL(2,\mathbb{F}_5) \hookrightarrow S_{|\mathbb{P}(\mathbb{F}_5^2)|} \simeq S_6$

Puisque $\frac{|S_6|}{|PGL(2,\mathbb{F}_5)|} = \frac{6!}{120} = 6$, on obtient (1') par le point (2) de la conséquence.

(2') on a $PSL(2,\mathbb{F}_5) \lhd PGL(2,\mathbb{F}_5)$ (induit par l'inclusion $SL(n,k) \lhd GL(n,k)$). De plus $|PSL(2,\mathbb{F}_5)| = 60$ en conséquence de quoi $PSL(2,\mathbb{F}_5)$ s'identifie (via ϕ_1) à un sous-groupe d'indice 2 de S_5, donc à A_5 (c.q.f.d.).

$\wr$

Remarque (relative au point (1'))

L'action de $PSL(2,\mathbb{F}_5)$ sur $\mathbb{P}(\mathbb{F}_5^2)$ est transitive et en particulier ne fixe aucune droite. On a ainsi exhibé via ϕ_1 un sous-groupe de S_6 isomorphe à S_5 mais ne fixant aucun élément de $\{1,\dots,6\}$. Cette situation est exceptionnelle et est liée au fait que $Aut(S_6) \neq Int(S_6)$ (alors qu'on a l'égalité pour les autres S_n). Voir [P], chap I, Proposition 8.11

Annexe (culturelle)

SIMPLICITY OF A_n

KEITH CONRAD

1. Introduction

A finite group is called *simple* when it is nontrivial and its only normal subgroups are the trivial subgroup and the whole group.

For instance, a finite group of prime size is simple, since it in fact has no non-trivial proper subgroups at all (normal or not). A finite abelian group G not of prime size, is not simple: let p be a prime factor of $|G|$, so G contains a subgroup of order p, which is a normal since G is abelian and is proper since $|G| > p$. Thus, the abelian finite simple groups are the groups of prime size.

When $n \geq 3$ the group S_n is not simple because it has a nontrivial normal subgroup A_n. But the groups A_n are simple, provided $n \geq 5$.

Theorem 1.1 (C. Jordan, 1875)**.** *For $n \geq 5$, the group A_n is simple.*

The restriction $n \geq 5$ is optimal, since A_4 is not simple: it has a normal subgroup of size 4, namely $\{(1), (12)(34), (13)(24), (14)(23)\}$. The group A_3 is simple, since it has size 3, and the groups A_1 and A_2 are trivial.

We will give five proofs of Theorem 1.1. Section 2 includes some preparatory material and later sections give the proofs of Theorem 1.1. In the final section, we give a quick application of the simplicity of alternating groups and give references for further proofs not treated here.

2. Preliminaries

We give two lemmas about alternating groups A_n for $n \geq 5$ and then two results on symmetric groups S_n for $n \geq 5$.

Lemma 2.1. *For $n \geq 3$, A_n is generated by 3-cycles. For $n \geq 5$, A_n is generated by permutations of type $(2, 2)$.*

Proof. That the 3-cycles generate A_n for $n \geq 3$ has been seen earlier in the course. To show permutations of type $(2, 2)$ generate A_n for $n \geq 5$, it suffices to write any 3-cycle (abc) in terms of such permutations. Pick $d, e \notin \{a, b, c\}$. Then note

$$(abc) = (ab)(de)(de)(bc).$$

□

The 3-cycles in S_n are all conjugate in S_n, since permutations of the same cycle type in S_n are conjugate. Are 3-cycles conjugate in A_n? Not when $n = 4$: (123) and (132) are not conjugate in A_4. But for $n \geq 5$ we do have conjugacy in A_n.

Lemma 2.2. *For $n \geq 5$, any two 3-cycles in A_n are conjugate in A_n.*

Proof. We show every 3-cycle in A_n is conjugate within A_n to (123). Let σ be a 3-cycle in A_n. It can be conjugated to (123) in S_n:

$$(123) = \pi\sigma\pi^{-1}$$

for some $\pi \in S_n$. If $\pi \in A_n$ we're done. Otherwise, let $\pi' = (45)\pi$, so $\pi' \in A_n$ and

$$\pi'\sigma\pi'^{-1} = (45)\pi\sigma\pi^{-1}(45) = (45)(123)(45) = (123).$$

□

Example 2.3. The 3-cycles (123) and (132) are not conjugate in A_4. But in A_5 we have

$$(132) = \pi(123)\pi^{-1}$$

for $\pi = (45)(12) \in A_5$.

Most proofs of the simplicity of the groups A_n are based on Lemmas 2.1 and 2.2. The basic argument is this: show any non-trivial normal subgroup $N \lhd A_n$ contains a 3-cycle, so N contains every 3-cycle by Lemma 2.2, and therefore N is A_n by Lemma 2.1.

The next lemma will be used in our fifth proof of the simplicity of alternating groups.

Lemma 2.4. *For $n \geq 5$, the only nontrivial proper normal subgroup of S_n is A_n. In particular, the only subgroup of S_n with index 2 is A_n.*

Proof. The last statement follows from the first since any subgroup of index 2 is normal.

Let $N \lhd S_n$ with $N \neq \{(1)\}$. We will show $A_n \subset N$, so $N = A_n$ or S_n.

Pick $\sigma \in N$ with $\sigma \neq (1)$. That means there is an i with $\sigma(i) \neq i$. Pick $j \in \{1, 2, \ldots, n\}$ so $j \neq i$ and $j \neq \sigma(i)$. Let $\tau = (ij)$. Then

$$\sigma\tau\sigma^{-1}\tau^{-1} = (\sigma(i)\ \sigma(j))(ij).$$

Since $\sigma(i) \neq i$ or j and $\sigma(i) \neq \sigma(j)$ (why?), the 2-cycles $(\sigma(i)\ \sigma(j))$ and (ij) are unequal, so their product is not the identity. That shows $\sigma\tau \neq \tau\sigma$.

Since $N \lhd S_n$, $\sigma\tau\sigma^{-1}\tau^{-1}$ lies in N. By construction, $\sigma(i) \neq i$ or j. If $\sigma(j) \neq i$ or j, then $(\sigma(i)\ \sigma(j))(ij)$ has type $(2, 2)$. If $\sigma(j) = i$ or j, $(\sigma(i)\ \sigma(j))(ij)$ is a 3-cycle. Thus N contains a permutation of type $(2, 2)$ or a 3-cycle. Since $N \lhd S_n$, N contains all permutations of type $(2, 2)$ or all 3-cycles. In either case, this shows (by Lemma 2.1) that $N \supset A_n$. □

Remark 2.5. There is an analogue of Lemma 2.4 for the "countable" symmetric group S_∞ consisting of all permutations of $\{1, 2, 3, \ldots\}$. A theorem of Schreier and Ulam (1933) says the only nontrivial proper normal subgroups of S_∞ are $\cup_{n\geq 1} S_n$ and $\cup_{n\geq 1} A_n$, which are the subgroup of permutations fixing all but a finite number of terms and its subgroup of even permutations.

Remark 2.6. From Lemma 2.4, any homomorphic image of S_n which is not an isomorphism has size 1 or 2. In particular, there is no surjective homomorphism $S_n \to \mathbf{Z}/(m)$ for $m > 2$.

Theorem 2.7. *For $n \geq 5$, any proper subgroup of S_n other than A_n has index at least n. Moreover, any subgroup of index n is isomorphic to S_{n-1}.*

Proof. Let H be a proper subgroup of S_n other than A_n, and let $m > 1$ be the index of H in S_n. We want to show $m \geq n$. Assume $m < n$. The left multiplication action of S_n on S_n/H gives a group homomorphism

$$\varphi\colon S_n \to \mathrm{Sym}(S_n/H) \cong S_m.$$

By hypothesis, $m < n$, so φ is not injective. Let K be the kernel of φ, so $K \subset H$ and K is non-trivial. Since $K \lhd S_n$, Lemma 2.4 says $K = A_n$ or S_n. Since $K \subset H$, we get $H = A_n$ or S_n, which contradicts our initial assumption about H. Therefore $m \geq n$.

Now let H be a subgroup of S_n with index n. Consider the left multiplication action of S_n on S_n/H. This is a homomorphism $\ell\colon S_n \to \mathrm{Sym}(S_n/H)$. Since S_n/H has size n, $\mathrm{Sym}(S_n/H)$ is isomorphic to S_n. The kernel of ℓ is a normal subgroup of S_n which lies in H (why?). Therefore the kernel has index at least n in S_n. Since the only normal subgroups of S_n are 1, A_n, and S_n, the kernel of ℓ is trivial, so ℓ is an isomorphism. What is the image $\ell(H)$ in $\mathrm{Sym}(S_n/H)$? Since $gH = H$ if and only if $g \in H$, $\ell(H)$ is the group of permutations of S_n/H which fixes the "point" H in S_n/H. The subgroup fixing a point in a symmetric group isomorphic to S_n is isomorphic to S_{n-1}. Therefore $H \cong \ell(H) \cong S_{n-1}$. □

Theorem 2.7 is false for $n = 4$: S_4 contains the dihedral group of size 8 as a subgroup of index 3. An analogue of Theorem 2.7 for alternating groups will be given in Section 8; its proof uses the simplicity of alternating groups.

Corollary 2.8. *Let F be a field. If $f \in F[X_1, \ldots, X_n]$ and $n \geq 5$, the number of different polynomials we get from f by permuting its variables is either 1, 2, or at least n.*

Proof. Letting S_n act on $F[X_1, \ldots, X_n]$ by permutations of the variables, the polynomials we get by permuting the variables of f is the S_n-orbit of f. The size of this orbit is $[S_n : H]$, where $H = \mathrm{Stab}_f = \{\sigma \in S_n : \sigma f = f\}$. By Theorem 2.7, this index is either 1, 2, or at least n. □

3. First proof

Our first proof of Theorem 1.1 is based on the one in [2, pp. 149–150].

We begin by showing A_5 is simple.

Theorem 3.1. *The group A_5 is simple.*

Proof. We want to show the only normal subgroups of A_5 are $\{(1)\}$ and A_5. This will be done in two ways.

Our first method involves counting the sizes of the conjugacy classes. There are 5 conjugacy classes in A_5, with representatives and sizes as indicated in the following table.

Rep.	(1)	(12345)	(21345)	(12)(34)	(123)
Size	1	12	12	15	20

If A_5 has a normal subgroup N, then N is a union of conjugacy classes – including $\{(1)\}$ – whose total size divides 60. However, no sum of the above numbers which includes 1 is a factor of 60 except for 1 and 60. Therefore N is trivial or A_5.

For the second proof, let $N \lhd A_5$ with $|N| > 1$. We will show N contains a 3-cycle. It follows that $N = A_n$ by Lemmas 2.1 and 2.2.

Pick $\sigma \in N$ with $\sigma \neq (1)$. The cycle structure of σ is $(abc), (ab)(cd)$, or $(abcde)$, where different letters represent different numbers. Since we want to show N contains a 3-cycle, we may suppose σ has the second or third cycle type. In the second case, N contains

$$((abe)(ab)(cd)(abe)^{-1})(ab)(cd) = (be)(cd)(ab)(cd) = (aeb).$$

In the third case, N contains

$$((abc)(abcde)(abc)^{-1})(abcde)^{-1} = (adebc)(aedcb) = (abd).$$

Therefore N contains a 3-cycle, so $N = A_5$. □

Lemma 3.2. *When $n \geq 5$, any $\sigma \neq (1)$ in A_n has a conjugate $\sigma' \neq \sigma$ such that $\sigma(i) = \sigma'(i)$ for some i.*

For example, if $\sigma = (12345)$ in A_5 then $\sigma' = (345)\sigma(345)^{-1} = (12453)$ has the same value at $i = 1$ as σ does.

Proof. Let σ be a non-identity element of A_n. Let r be the longest length of a disjoint cycle in σ. Relabelling, we may write

$$\sigma = (12\dots r)\pi,$$

where $(12\dots r)$ and π are disjoint.

If $r \geq 3$, let $\tau = (345)$ and $\sigma' = \tau\sigma\tau^{-1}$. Then $\sigma(1) = 2, \sigma'(1) = 2, \sigma(2) = 3$, and $\sigma'(2) = 4$. Thus $\sigma' \neq \sigma$ and both take the same value at 1.

If $r = 2$, then σ is a product of disjoint transpositions. If there are at least 3 disjoint transpositions involved, then $n \geq 6$ and we can write $\sigma = (12)(34)(56)(\dots)$ after relabelling. Let $\tau = (12)(35)$ and $\sigma' = \tau\sigma\tau^{-1}$. Then $\sigma(1) = 2, \sigma'(1) = 2, \sigma(3) = 4$, and $\sigma'(3) = 6$. Again, we see $\sigma' \neq \sigma$ and σ and σ' have the same value at 1.

If $r = 2$ and σ is a product of 2 disjoint transpositions, write $\sigma = (12)(34)$ after relabelling. Let $\tau = (132)$ and $\sigma' = \tau\sigma\tau^{-1} = (13)(24)$. Then $\sigma' \neq \sigma$ and they both fix 5. □

Now we prove Theorem 1.1.

Proof. We may suppose $n \geq 6$, by Theorem 3.1. For $1 \leq i \leq n$, let A_n act in the natural way on $\{1, 2, \dots, n\}$ and let $H_i \subset A_n$ be the subgroup fixing i, so $H_i \cong A_{n-1}$. By induction, each H_i is simple. Note each H_i contains a 3-cycle (build out of 3 numbers other than i).

Let $N \lhd A_n$ be a nontrivial normal subgroup. We want to show $N = A_n$. Pick $\sigma \in N$ with $\sigma \neq \{(1)\}$. By Lemma 3.2, there is a conjugate σ' of σ such that $\sigma' \neq \sigma$ and $\sigma(i) = \sigma'(i)$ for some i. Since N is normal in A_n, $\sigma' \in N$. Then $\sigma^{-1}\sigma'$ is a non-identity element of N which fixes i, so $N \cap H_i$ is a non-trivial subgroup of H_i. It is also a normal subgroup of H_i since $N \lhd A_n$. Since H_i is simple, $N \cap H_i = H_i$. Therefore $H_i \subset N$. Since H_i contains a 3-cycle, N contains a 3-cycle and we are done.

Alternatively, we can show $N = A_n$ when $N \cap H_i$ is non-trivial for some i as follows. As before, since $N \cap H_i$ is a non-trivial normal subgroup of H_i, $H_i \subset N$. Without referring to 3-cycles, we instead note that the different H_i's are conjugate subgroups of A_n: $\sigma H_i \sigma^{-1} = H_{\sigma(i)}$ for $\sigma \in A_n$ Since $N \lhd A_n$ and N contains H_i, N contains every $H_{\sigma(i)}$ for all $\sigma \in A_n$. Since $\sigma(i)$ can be any element of A_n as σ varies in A_n, N contains every H_i. Any permutation of type $(2, 2)$ is in some H_i since $n \geq 5$, so N contains all permutations of type $(2, 2)$. Every permutation in A_n is a product of permutations of type (2,2), so $N \supset A_n$. Therefore $N = A_n$. □

4. Second proof

Our next proof is taken from [6, p. 108]. It does not use induction on n, but we do need to know A_6 is simple at the start.

Theorem 4.1. *The group A_6 is simple.*

Proof. We follow the first method of proof of Theorem 3.1. Here is the table of conjugacy classes in A_6.

Rep.	(1)	(123)	(123)(456)	(12)(34)	(12345)	(23456)	(1234)(56)
Size	1	40	40	45	72	72	90

A tedious check shows no sum of these sizes, which includes 1, is a factor of $6!/2$ except for the sum of all the terms. Therefore the only non-trivial normal subgroup of A_6 is A_6. □

Now we prove the simplicity of A_n for larger n by reducing directly to the case of A_6.

Proof. Since A_5 and A_6 are known to be simple by Theorems 3.1 and 4.1, pick $n \geq 7$ and let $N \lhd A_n$ be a non-trivial subgroup. We will show N contains a 3-cycle.

Let σ be a non-identity element of N. It moves some number. By relabelling, we may suppose $\sigma(1) \neq 1$. Let $\tau = (ijk)$, where i, j, k are not 1 and $\sigma(1) \in \{i, j, k\}$. Then $\tau\sigma\tau^{-1}(1) = \tau(\sigma(1)) \neq \sigma(1)$, so $\tau\sigma\tau^{-1} \neq \sigma$. Let $\varphi = \tau\sigma\tau^{-1}\sigma^{-1}$, so $\varphi \neq (1)$. Writing

$$\varphi = (\tau\sigma\tau^{-1})\sigma^{-1},$$

we see $\varphi \in N$. Now write

$$\varphi = \tau(\sigma\tau^{-1}\sigma^{-1}),$$

Since τ^{-1} is a 3-cycle, $\sigma\tau^{-1}\sigma^{-1}$ is also a 3-cycle. Therefore φ is a product of two 3-cycles, so φ moves at most 6 numbers in $\{1, 2, \ldots, n\}$. Let H be the copy of A_6 inside A_n corresponding to the even permutations of those 6 numbers (possibly augmented to 6 arbitrarily if in fact φ moves fewer numbers). Then $N \cap H$ is non-trivial (it contains φ) and it is a normal subgroup of H. Since $H \cong A_6$, which is simple, $N \cap H = H$. Thus $H \subset N$, so N contains a 3-cycle. □

5. Third proof

Our next proof is by induction, and uses conjugacy classes instead of Lemma 3.2. It is based on [9, §2.3].

Lemma 5.1. *If $n \geq 6$ then every non-trivial conjugacy class in S_n and A_n has at least n elements.*

The lower bound n in Lemma 5.1 is actually quite weak as n grows. But it shows that the size of each non-trivial conjugacy class in S_n and A_n grows with n.

Proof. For $n \geq 6$, pick $\sigma \in S_n$ with $\sigma \neq (1)$. We want to look at the conjugacy class of σ in S_n, and if $\sigma \in A_n$ we also want to look at the conjugacy class of σ in A_n, and our goal in both cases is to find at least n elements in the conjugacy class.

Case 1: The disjoint cycle decomposition of σ includes a cycle with length greater than 2. Without loss of generality, $\sigma = (123\ldots)\ldots$.

For $3 \leq k \leq n$, fix a choice of $\ell \notin \{1, 2, 3, k\}$ (which is possible since $n \geq 5$) and let $\alpha_k = (2k\ell)$ and $\beta_k = (3k\ell)$. Then $\alpha_k\sigma\alpha_k^{-1}$ has the effect $1 \to 1 \to 2 \to k$ and $\beta_k\sigma\beta_k^{-1}$ has the effect $1 \to 1 \to 2 \to 2$ and $2 \to 2 \to 3 \to k$. This tells us that the conjugates

$$\alpha_3\sigma\alpha_3^{-1}, \ldots, \alpha_n\sigma\alpha_n^{-1}, \beta_3\sigma\beta_3^{-1}, \ldots, \beta_n\sigma\beta_n^{-1}$$

are all different from each other: the conjugates by the α's have different effects on 1, the conjugates by the β's have different effects on 2, and a conjugate by an α is not a conjugate by a β since they have different effects on 1. Since these conjugates are different, the number of conjugates of σ is at least $2(n-2) > n$. Because α_k and β_k are 3-cycles, if $\sigma \in A_n$ then these conjugates are in the A_n-conjugacy class of σ.

Case 2: The disjoint cycle decomposition of σ only has cycles with length 1 or 2. Therefore without loss of generality σ is a transposition or a product of at least 2 disjoint transpositions.

If σ is a transposition, then its S_n-conjugacy class is the set of all transpositions (ij) where $1 \leq i < j \leq n$, and the number of these permutations is $\binom{n}{2} = \frac{n^2-n}{2}$, which is greater than n for $n \geq 6$.

If σ is a product of at least 2 disjoint transpositions, then without loss of generality $\sigma = (12)(34)\cdots$, where the terms in $\cdots$ don't involve 1, 2, 3, or 4.

For $5 \leq k \leq n$, let $\alpha_k = (12)(3k)$, $\beta_k = (13)(2k)$, and $\gamma_k = (1k)(23)$. Then $\alpha_k\sigma\alpha_k^{-1}$ has the effect

$$1 \to 2 \to 1 \to 2, \quad 2 \to 1 \to 2 \to 1, \quad k \to 3 \to 4 \to 4,$$

$\beta_k\sigma\beta_k^{-1}$ has the effect

$$1 \to 3 \to 4 \to 4, \quad 3 \to 1 \to 2 \to k, \quad k \to 2 \to 1 \to 3,$$

and $\gamma_k\sigma\gamma_k^{-1}$ has the effect

$$2 \to 3 \to 4 \to 4, \quad 3 \to 2 \to 1 \to k, \quad k \to 1 \to 2 \to 3.$$

The conjugates of σ by the α's are different from each other since they take different elements to 4, the conjugates of σ by the β's are different from each other since they take different elements to 3, and the conjugates of σ by the γ's are different from each other since they take different elements to 3. Conjugates of σ by an α and a β are different since they send 1 to different places, conjugates of σ by an α and a γ are different since they send 2 to different places, and conjugates of σ by a β and a γ are different since they send different elements to 4 (1 for the β's and 2 for the γ's). In total the number of conjugates of σ we have written down (which are all conjugates by 3-cycles, hence they are conjugates in A_n if $\sigma \in A_n$) is $3(n-4)$, and $3(n-4) \geq n$ if $n \geq 6$. □

Now we prove Theorem 1.1.

Proof. We argue by induction on n, the case $n = 5$ having already been settled by Theorem 3.1. Say $n \geq 6$. Let $N \lhd A_n$ with $N \neq \{(1)\}$. Since N is normal and non-trivial, it contains non-identity conjugacy classes in A_n. By Lemma 5.1, any non-identity conjugacy class in A_n has size at least n when $n \geq 6$. Therefore, by counting the trivial conjugacy class and a non-trivial conjugacy class in N, we see $|N| \geq n + 1$.

Using a wholly different argument, we now show that $|N| \leq n$ if $N \neq A_n$, which will be a contradiction. Pick $1 \leq i \leq n$. Let $H_i \subset A_n$ be the subgroup fixing i, so $H_i \cong A_{n-1}$. In particular, H_i is a simple group by induction. Notice each H_i contains a 3-cycle.

The intersection $N \cap H_i$ is a normal subgroup of H_i, so simplicity of H_i implies $N \cap H_i$ is either $\{(1)\}$ or H_i. If $N \cap H_i = H_i$ for some i, then $H_i \subset N$. Since H_i contains a 3-cycle, N does as well, so $N = A_n$ by Lemmas 2.1 and 2.2. (This part resembles part of our first proof of simplicity of A_n, but we will now use Lemma 5.1 instead of Lemma 3.2 to show the possibility that $N \cap H_i = \{(1)\}$ for all i is absurd.)

Suppose $N \neq A_n$. Then, by the previous paragraph, $N \cap H_i = \{(1)\}$ for all i. Therefore each $\sigma \neq (1)$ in N acts on $\{1, 2, \ldots, n\}$ without fixed points (otherwise σ would be a non-identity element in some $N \cap H_i$). That implies each $\sigma \neq (1)$ in N is completely determined by the value $\sigma(1)$: if $\tau \neq (1)$ is in N and $\sigma(1) = \tau(1)$, then $\sigma\tau^{-1} \in N$ fixes 1, so $\sigma\tau^{-1}$ is the identity, so $\sigma = \tau$.

There are only $n - 1$ possible values for $\sigma(1) \in \{2, 3, \ldots, n\}$, so $N - \{(1)\}$ has size at most $n - 1$, hence $|N| \leq n$. We already saw from Lemma 5.1 that $|N| \geq n + 1$, so we have a contradiction. □

6. Fourth proof

Our next proof, based on [3, p. 50], is very computational.

Proof. Let $N \lhd A_n$ be a non-trivial normal subgroup. We will show N contains a 3-cycle.

Pick $\sigma \in N$, $\sigma \neq (1)$. Write

$$\sigma = \pi_1 \pi_2 \cdots \pi_k,$$

where the π_j's are disjoint cycles. In particular, they *commute*, so we can relabel them at our convenience. Eliminate any 1-cycles from the product.

Case 1: Some π_i has length at least 4. Relabelling, we can write

$$\pi_1 = (12 \cdots r)$$

with $r \geq 4$. Let $\varphi = (123)$. Then $\varphi\sigma\varphi^{-1} \in N$ and

$$\begin{aligned} \varphi\sigma\varphi^{-1} &= \varphi\pi_1\varphi^{-1}\pi_2 \cdots \pi_k \\ &= \varphi\pi_1\varphi^{-1}\pi_1^{-1}\sigma \\ &= (123)(123\cdots r)(132)(r\cdots 21)\sigma \\ &= (124)\sigma, \end{aligned}$$

so $(124) = \varphi\sigma\varphi^{-1}\sigma^{-1} \in N$.

Case 2: Each π_i has length ≤ 3, and at least two have length 3 (so $n \geq 6$). Without loss of generality, $\pi_1 = (123)$ and $\pi_2 = (456)$. Let $\varphi = (124)$. Then

$$\begin{aligned} \varphi\sigma\varphi^{-1} &= \varphi\pi_1\pi_2\varphi^{-1}\pi_3 \cdots \pi_k \\ &= \varphi\pi_1\pi_2\varphi^{-1}\pi_2^{-1}\pi_1^{-1}\sigma \\ &= (124)(123)(456)(142)(465)(132)\sigma \\ &= (12534)\sigma, \end{aligned}$$

so $\varphi\sigma\varphi^{-1}\sigma^{-1} = (12534) \in N$. Now run through Case 1 with this 5-cycle to find a 3-cycle in N.

Case 3: Exactly one π_i has length 3, and the rest have length ≤ 2. Without loss of generality, $\pi_1 = (123)$ and the other π_i's are 2-cycles. Then $\sigma^2 = \pi_1^2$ is in N, and $\pi_1^2 = (132)$.

Case 4: All π_i's are 2-cycles, so necessarily $k > 1$. Write $\pi_1 = (12)$ and $\pi_2 = (34)$. Let $\varphi = (123)$. Then

$$\begin{aligned} \varphi\sigma\varphi^{-1} &= \varphi\pi_1\pi_2\varphi^{-1}\pi_3 \cdots \pi_k \\ &= \varphi\pi_1\pi_2\varphi^{-1}\pi_2^{-1}\pi_1^{-1}\sigma \\ &= (123)(12)(34)(132)(34)(12)\sigma \\ &= (13)(24)\sigma, \end{aligned}$$

so

$$\varphi\sigma\varphi^{-1}\sigma^{-1} = (13)(24) \in N.$$

Let $\psi = (135)$. Then

$$\begin{aligned} (13)(24)\psi(13)(24)\psi^{-1} &= (13)(24)(135)(13)(24)(153) \\ &= (13)(135)(13)(153) \\ &= (135), \end{aligned}$$

so N contains a 3-cycle. □

7. Fifth proof

Our final proof is taken from [8, p. 295].

Let $N \lhd A_n$ with N not $\{(1)\}$ or A_n. We will study N as a subgroup of S_n. By Lemma 2.4, N is not a normal subgroup of S_n. This means the normalizer of N inside S_n is a proper subgroup, which contains A_n, so

$$A_n = \mathrm{N}_{S_n}(N). \tag{7.1}$$

For any transposition τ in S_n, $\tau \notin \mathrm{N}_{S_n}(N)$ by (7.1), so $\tau N\tau^{-1} \neq N$. Since $N \lhd A_n$ and $\tau N\tau^{-1}$ is a subgroup of A_n, the product set $N \cdot \tau N\tau^{-1}$ is a subgroup of A_n. We have the chain of inclusions

$$N \cap \tau N\tau^{-1} \subset N \subset N \cdot \tau N\tau^{-1} \subset A_n,$$

where the first and second are strict.

We will now show, for any transposition τ in S_n, that

$$N \cap \tau N\tau^{-1} \lhd S_n, \quad N \cdot \tau N\tau^{-1} \lhd S_n. \tag{7.2}$$

The proof of (7.2) is a bit tedious , so first let's see why (7.2) leads to a contradiction.

It follows from (7.2) and Lemma 2.4 that

$$N \cap \tau N\tau^{-1} = \{(1)\}, \quad N \cdot \tau N\tau^{-1} = A_n \tag{7.3}$$

for any transposition τ in S_n. By (7.3), $|A_n| = |N| \cdot |\tau N\tau^{-1}| = |N|^2$, so $n! = 2|N|^2$. This tells us $|N|$ must be even, so N has an element, say σ, of order 2. Then σ is a product of disjoint 2-cycles. There is a transposition ρ in S_n which commutes with σ: just take for ρ one of the transpositions in the disjoint cycle decomposition of σ. Then

$$\sigma = \rho\sigma\rho^{-1} \in N \cap \rho N\rho^{-1}.$$

From (7.3), using ρ for the arbitrary τ there, $N \cap \rho N\rho^{-1}$ is trivial, so we have a contradiction. (As another way of reaching a contradiction from the equation $n! = 2|N|^2$, we can use Bertrand's postulate – proved by Chebyshev – that there is always a prime strictly between m and $2m$ for any $m > 1$. That means, taking $m = n!/4$, the ratio $n!/2$ can't be a perfect square.)

It remains to check the two conditions in (7.2). In both cases, we show the subgroups are normalized by A_n and by τ, so the normalizer contains $\langle A_n, \tau\rangle = S_n$.

First consider $N \cap \tau N\tau^{-1}$. It is clearly normalized by τ. Now pick any $\pi \in A_n$. Then $\pi N\pi^{-1} = N$ since $N \lhd A_n$, and

$$\pi(\tau N\tau^{-1})\pi^{-1} = \tau(\tau^{-1}\pi\tau)N(\tau^{-1}\pi^{-1}\tau)\tau^{-1} = \tau N\tau^{-1} \tag{7.4}$$

since $\tau^{-1}\pi\tau \in A_n$. Therefore

$$\pi(N \cap \tau N\tau^{-1})\pi^{-1} = \pi N\pi^{-1} \cap \pi\tau N\tau^{-1}\pi^{-1} = N \cap \tau N\tau^{-1},$$

so A_n normalizes $N \cap \tau N\tau^{-1}$.

Now we look at $N \cdot \tau N\tau^{-1}$. Pick an element of this product, say

$$\sigma = \sigma_1\tau\sigma_2\tau^{-1},$$

where $\sigma_1, \sigma_2 \in N$. Then, since $N \lhd A_n$,

$$\tau\sigma\tau^{-1} = \tau\sigma_1\tau\sigma_2\tau^{-2} = \tau\sigma_1\tau\sigma_2 \in \tau N\tau^{-1} \cdot N = N \cdot \tau N\tau^{-1},$$

which shows τ normalizes $N \cdot \tau N\tau^{-1}$.

Now pick any $\pi \in A_n$. To see π normalizes $N \cdot \tau N \tau^{-1}$, pick σ as before. Then

$$\pi\sigma\pi^{-1} = \pi\sigma_1\pi^{-1} \cdot \pi(\tau\sigma_2\tau^{-1})\pi^{-1}.$$

The first factor $\pi\sigma_1\pi^{-1}$ is in N since $N \lhd A_n$. The second factor is in $\pi\tau N\tau^{-1}\pi^{-1}$, which equals $\tau N\tau^{-1}$ by (7.4).

8. Concluding Remarks

The standard counterexample to the converse of Lagrange's theorem is A_4: it has size 12 but no subgroup of index 2. For $n \geq 5$, the groups A_n also have no subgroup of index 2, since any index-2 subgroup of a group is normal and A_n is simple.

In fact, something stronger is true.

Corollary 8.1. *For $n \geq 5$, any proper subgroup of A_n has index at least n.*

This is an analogue of Theorem 2.7.

Proof. Let H be a proper subgroup of A_n, with index $m > 1$. Consider the left multiplication action of A_n on A_n/H. This gives a group homomorphism

$$\varphi\colon A_n \to \mathrm{Sym}(A_n/H) \cong S_m.$$

Let K be the kernel of φ, so $K \subset H$ (why?) and $K \lhd A_n$. By simplicity of A_n, K is trivial. Therefore A_n injects into S_m, so $(n!/2) \mid m!$, which implies $n \leq m$. □

The lower bound of n is sharp since $[A_n : A_{n-1}] = n$. Corollary 8.1 is false for $n = 4$: A_4 has a subgroup of index 3.

Remark 8.2. What the proof of Corollary 8.1 shows more generally is that if G is a finite simple group and H is a subgroup with index $m > 1$, then there is an embedding of G into S_m, so $|G| \mid m!$. With G fixed, this divisibility relation puts a lower bound on the index of any proper subgroup of G.

A reader who wants to see more proofs that A_n is simple for $n \geq 5$ can look at [4, pp. 247-248] or [5, pp. 32–33] for another way of showing a non-trivial normal subgroup contains a 3-cycle, or at [1, §1.7] or [7, pp. 295–296] for a proof based on the theory of highly transitive permutation groups.

References

[1] N. L. Biggs, A. T. White, "Permutation Groups and Combinatorial Structures," Cambridge Univ. Press, Cambridge, 1979.
[2] D. Dummit, R. Foote, "Abstract Algebra," 3rd ed., J. Wiley, 2004.
[3] T. Hungerford, "Algebra," Springer-Verlag, New York, 1980.
[4] N. Jacobson, "Basic Algebra I," 2nd ed., W. H. Freeman, New York, 1985.
[5] S. Lang, "Algebra," revised 3rd ed., Springer-Verlag, New York, 2002.
[6] J. Rotman, "Advanced Modern Algebra," Prentice-Hall, Upper Saddle River, 2002.
[7] W. R. Scott, "Group Theory," Dover, New York, 1987.
[8] M. Suzuki, "Group Theory I," Springer-Verlag, Berlin, 1982.
[9] R. Wilson, "The Finite Simple Groups," Springer-Verlag, New York, 2009,