Groupes des permutations d'un ensemble fini. Applications.

105

I. Groupe des permutations

1. Définitions

Def 1 : Le groupe des permutations d'un ensemble E est le groupe des bijections de E sur lui-même, noté $S(E)$.

Notation 2 : Si $E = \{1, \dots, n\} \subset \mathbb{N}$, on note $S(E) = \mathfrak{S}_n$.

Prop 3 : Si E et F sont deux ensembles non vides et φ une bijection de E sur F alors $S(E)$ et $S(F)$ sont isomorphes.

On ne va donc étudier que le cas du groupe $\mathfrak{S}_n$.

Prop 4 : $\mathfrak{S}_n$ agit naturellement sur $X = \{1, \dots, n\}$ par la relation $\sigma \cdot i = \sigma(i)$ pour tout $\sigma \in \mathfrak{S}_n$ et $i \in X$.
Cette action est transitive.

Rmq 5 : Soit $x \in \mathfrak{S}_n$, $\mathrm{Stab}_{\mathfrak{S}_n}(x) = \mathfrak{S}_{n-1}$

Cor 6 : $\mathrm{Card}(\mathfrak{S}_n) = n!$

Thm 7 (Cayley) : Tout groupe fini d'ordre n est isomorphe à un sous-groupe de $\mathfrak{S}_n$.

2. Cycles et générateurs

Def 8 : Un cycle d'ordre k noté $\sigma = (x_1, \dots, x_k)$, avec $x_i \in \{1, \dots, n\}$ signifie que
$$\begin{cases} \sigma(x_i) = x_i & \text{si } i \notin \{1, \dots, k\} \\ \sigma(x_k) = x_1 \\ \sigma(x_i) = x_{i+1} & \text{si } i \in \{1, \dots, k\} \end{cases}$$

Rmq 9 : Un 2-cycle est une transposition.

Def 10 : On définit $\mathrm{supp}(\sigma) = \{x \in E \mid \sigma(x) \neq x\}$ le support de la permutation σ.

Def 11 : On dit que 2 cycles σ et σ' sont disjoints dans $\mathfrak{S}_n$ ssi leurs supports sont disjoints dans E.

Théorème 12 : Toute permutation $\sigma \in \mathfrak{S}_n \setminus \{id\}$ se décompose en produit de cycle 2 à 2 disjoints

Ex 13 : $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 4 & 5 & 1 & 7 & 6 & 8 \end{pmatrix} = (1\,2\,3\,4\,5)\,(6\,7)$

Prop 14 : $\mathfrak{S}_n$ est engendré par les transpositions.

Lemme 15 : $\mathfrak{S}_n$ est engendré par $(1\,2)$ et $(1\,2 \dots n)$

Prop 16 : Soit $\sigma = (x_1, \dots, x_k)$ un k-cycle de $\mathfrak{S}_n$ et $\tau \in \mathfrak{S}_n$.
alors $\tau\sigma\tau^{-1} = (\tau(x_1), \dots, \tau(x_k))$

Prop 17 : $\forall \sigma \in \mathfrak{S}_n$ et $j \in [\![1, n]\!]$, soit a_j le nombre de cycles de longueur j de la décomposition de σ. On a $n = \sum_{j=1}^{n} j a_j(\sigma)$
Alors σ est conjugué à σ' ssi $a_j(\sigma) = a_j(\sigma')$ $\forall j \in [\![1, n]\!]$.

Cor 18 : Le nombre de classes de conjugaison de $\mathfrak{S}_n$ est le nombre de partitions de n.

II. Morphismes et sous-groupes

1. Morphisme signature

Def 19 : Soit $\sigma \in \mathfrak{S}_n$, on définit $\varepsilon(\sigma)$, la signature de σ, par
$$\varepsilon(\sigma) = \prod_{1 \leq i < j \leq n} \frac{\sigma(j) - \sigma(i)}{j - i}$$

Prop 20 : ε est l'unique morphisme surjectif de $\mathfrak{S}_n$ dans $\{\pm 1\}$

Prop 21 : Si $\sigma \in \mathfrak{S}_n$ est un k-cycle, $\varepsilon(\sigma) = (-1)^{k-1}$.

Thm 22 : Si $\sigma \in \mathfrak{S}_n$ est produit de p transpositions $\varepsilon(\sigma) = (-1)^p$

Cor 23 : Soit $\sigma \in \mathfrak{S}_n$, $\varepsilon(\sigma) = (-1)^{\mathrm{Inv}(\sigma)}$ avec $\mathrm{Inv}(\sigma)$ le nombre d'inversions de σ.

Ex 24 : $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 4 & 5 & 1 & 7 & 6 & 8 \end{pmatrix}$, $\varepsilon(\sigma) = -1$.

Thm 25 (lemme de Zolotarev) : Soit $a \in \mathbb{F}_p^*$, on note $m_a : \mathbb{F}_p^* \to \mathbb{F}_p^*$, $x \mapsto ax$
Alors $\varepsilon(m_a) = \left(\frac{a}{p}\right)$.

App 26: $\left(\frac{a}{p}\right) = (-1)^{\frac{p^2-1}{8}}$

2. Sous-groupes de $\mathfrak{S}_n$

Def 27: $\mathcal{A}_n = \mathrm{Ker}(\varepsilon)$.

Prop 28: $\mathcal{A}_n$ est engendré par les 3-cycles.

Prop 29: Le centre de $\mathfrak{S}_n$ est $Z(\mathfrak{S}_n) = \begin{cases} \mathfrak{S}_n \text{ si } n=2 \\ \{id\} \text{ si } n \geq 3 \end{cases}$

Thm 30: Pour $n \geq 5$, les seuls sous-groupes distingués de $\mathfrak{S}_n$ sont $\{id\}$, $\mathcal{A}_n$ et $\mathfrak{S}_n$.

Prop 31: Si $n \geq 2$, $D(\mathfrak{S}_n) = \mathcal{A}_n$
Si $n \geq 5$, $D(\mathcal{A}_n) = \mathcal{A}_n$

Prop 32: $\mathcal{A}_n$ est simple pour $n \geq 5$.

Cor 33: $\mathcal{A}_5$ est le seul groupe simple d'ordre 60.

DEV 2

III. Applications

Soit $\mathbb{K}$ un corps.

1. Matrices de permutation

Def 34: Soit $\mathcal{B} = (e_1, \dots, e_n)$ la base canonique de $\mathbb{K}^n$. Soit $\sigma \in \mathfrak{S}_n$, on définit l'endomorphisme $u_\sigma \in \mathcal{L}(\mathbb{K}^n)$ par : $\forall i \in [\![1,n]\!] \quad u_\sigma(e_i) = e_{\sigma(i)}$.
On appelle matrice de permutation associée à $\sigma \in \mathfrak{S}_n$ la matrice $P_\sigma \in \mathcal{M}_n(\mathbb{K})$ représentant u_σ dans la base canonique. On a ainsi $P_\sigma = \left(\delta_{i,\sigma(j)}\right)_{i,j \in [\![1,n]\!]}$

Prop 35: Soient $\sigma_1, \sigma_2 \in \mathfrak{S}_n$, $P_{\sigma_1\sigma_2} = P_{\sigma_1} P_{\sigma_2}$.
Soit $\sigma \in \mathfrak{S}_n$, P_σ est inversible et $P_\sigma^{-1} = P_{\sigma^{-1}}$.

Thm 36: Le morphisme $\varphi : \begin{array}{ccc} \mathfrak{S}_n & \to & GL_n(\mathbb{K}) \\ \sigma & \mapsto & P_\sigma \end{array}$ est injectif et $\det(P_\sigma) = \varepsilon(\sigma)$.

Thm 37 (Brauer) : Si σ et σ' sont deux permutations conjuguées, alors P_σ et $P_{\sigma'}$ sont semblables.

Thm 38: Soit A une matrice de $GL_n(\mathbb{K})$. Il existe une matrice de permutation P telle que $P^{-1}A$ admette une décomposition LU.

2. Déterminant

Def 39: Soit $A = (a_{ij}) \in \mathcal{M}_n(\mathbb{K})$. On a :

$$\det A = \sum_{\sigma \in \mathfrak{S}_n} \varepsilon(\sigma) \prod_{i=1}^{n} a_{\sigma(i),i}$$

Ex 40: $A = \begin{pmatrix} 1 & 2 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}$ $\quad \mathfrak{S}_3 = \{id, (1,2), (1,3), (2,3), (1,2,3), (1,3,2)\}$
$\det A = 1$.

Prop 41: Le déterminant est une forme multilinéaire alternée.

Thm 42: Toute application multilinéaire alternée est le déterminant d'une matrice dans une certaine base.

Prop 43: $\det({}^tA) = \det(A)$.

Prop 44: Une permutation de deux colonnes change le signe du déterminant.
En fait, on a $\det(P_\sigma A) = \varepsilon(\sigma) A \quad \forall A \in \mathcal{M}_n(\mathbb{K})$ $\forall \sigma \in \mathfrak{S}_n$.

3. Isométries.

Soit T un tétraèdre régulier (plein).

Def 45: Un point $S \in T$ est dit extremal si
$\forall M, N \in T, \quad S \in [M,N] \Rightarrow S = M$ ou $S = N$

313

Prop 46 : Soit $g \in Is(T)$, le groupe des isométries du tétraèdre. alors g envoie un point extremal de T sur un point extremal de T.

DEV 3

Thm 47 : Les groupes d'isométries d'un tétraèdre régulier sont $Is(T) \simeq \mathfrak{S}_4$ et $Is^+(T) \simeq \mathcal{A}_4$.

App 48 : (Table de caractères de $\mathfrak{S}_4$).

$\mathfrak{S}_4$	id	(1,2)	(1,2)(3,4)	(1,2,3)	(1,2,3,4)
χ_{triv}	1	1	1	1	1
χ_ε	1	-1	1	1	-1
χ_{std}	3	1	-1	0	-1
$\varepsilon\chi_{std}$	3	-1	-1	0	1
ϕ	2	0	2	-1	0

Références :

- Mathématiques pour l'agrégation : Algèbre & Géométrie, Rombaldi.
- Cours d'algèbre, Perrin
- Algèbre linéaire, Grifone.
- H2G2
- CVA

Lemme de Zolotarev

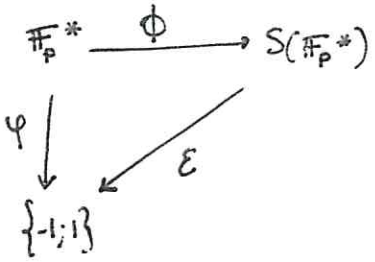
CVA p 197

leçon: 105

Théorème:
Soit p un nombre premier impair. La multiplication par a dans $\mathbb{F}_p^*$, notée m_a, est une permutation et on a:

$\left(\frac{a}{p}\right) = \varepsilon(m_a)$. Ce qui permet de calculer $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$

Démonstration:



On va montrer:

#1: Si $\psi: \mathbb{F}_p^* \to \{-1;1\}$ est un morphisme non trivial alors c'est le morphisme $a \mapsto \left(\frac{a}{p}\right)$

#2: $\phi: \mathbb{F}_p^* \to S(\mathbb{F}_p^*)$, $a \mapsto m_a$ est un morphisme de groupe

#3: Pour tout $a \in \mathbb{F}_p^*$, $\varepsilon(m_a) = \left(\frac{a}{p}\right)$
d'où $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$

#1: Soit ψ un morphisme de groupe non trivial $\mathbb{F}_p^* \to \{-1;1\}$ et z un carré de $\mathbb{F}_p^*$. On a $z = y^2$ pour $y \in \mathbb{F}_p^*$.
Donc $\psi(z) = \psi(y^2) = \psi(y)^2 = 1$
On note K l'ensemble des carrés de $\mathbb{F}_p^*$. On a donc $K \subset \ker\psi$
On $|\ker\psi| = \frac{|\mathbb{F}_p^*|}{|\mathrm{Im}\,\psi|} = \frac{p-1}{2}$

De plus, on a $|K| = \frac{p-1}{2}$. En effet, $f: \mathbb{F}_p^* \to \mathbb{F}_p^*$, $x \mapsto x^2$ est un morphisme de groupe. De plus, $|\ker f| = 2$.
Soit $a \in \ker f$, $f(a) = a^2 = 1$ donc $(a+1)(a-1) = 0$. Or $\mathbb{F}_p$ est un corps, il est donc intègre. Donc $a = 1$ ou $a = -1$. Or $p \neq 2$ donc $1 \neq -1$.
L'équation a donc deux solutions distinctes. donc $\ker f$ est d'ordre 2.
Comme l'ensemble des carrés est égale à $\mathrm{Im}(f)$, qui est isomorphe à $\mathbb{F}_p^*/\ker\phi$, on a $|K| = \frac{p-1}{2}$.

Donc $\psi = \left(\frac{\cdot}{p}\right)$

#2: Soit $a \in \mathbb{F}_p^*$. Mq $m_a: \mathbb{F}_p^* \to \mathbb{F}_p^*$ est une bijection
Comme a est inversible, $(m_a)^{-1} = m_{a^{-1}}$ et, en particulier, m_a est bijective.
De plus, $m_a \circ m_b(z) = ab(z) = m_{ab}(z)$ pour $z \in \mathbb{F}_p^*$
donc $m_a \circ m_b = m_{ab}$
donc ϕ est bien un morphisme de $\mathbb{F}_p^*$ dans $S(\mathbb{F}_p^*)$.

#3 : D'après #1, il nous suffit de mq $a \mapsto \left(\frac{a}{p}\right)$ et $a \mapsto \varepsilon(m_a)$ définissent deux morphismes non triviaux de $\mathbb{F}_p^*$ vers $\{1;-1\}$

$a \mapsto \left(\frac{a}{p}\right)$ vaut -1 sur les non carrés et il en existe $\left(\frac{p-1}{2}\right.$ exactement)

$a \mapsto \varepsilon(m_a)$?

Le groupe multiplicatif $\mathbb{F}_p^*$ est cyclique. Soit donc a un générateur de $\mathbb{F}_p^*$. Le morphisme m_a envoie a^m sur a^{m+1} et sa décomposition en cycle disjoints est donc : $m_a := (1 \; a \; a^2 \; \dots \; a^{p-2})$

de signature $\varepsilon(m_a) = (-1)^{p-1+1} = (-1)$. Le morphisme est donc non triviae

Les deux morphismes sont donc non triviaux. De plus, ce sont des morphismes

$a \mapsto \left(\frac{a}{p}\right)$

$a \mapsto \varepsilon(m_a)$ par #2

Donc, ce sont les mêmes.

Il nous suffit désormais de calculer $\varepsilon(m_2)$. Si l'on ordonne $\mathbb{F}_p^*$ par

$0 < 1 < \dots < p-1$

on sait que $\varepsilon(m_2) = (-1)^{\mathrm{Inv}(m_2)}$ où $\mathrm{Inv}(m_2)$ est le nombre d'inversion de la permutation m_2, càd le nombre de couples (i,j) de $\mathbb{F}_p$ tq $i<j$ et $m_2(i) > m_2(j)$

La permutation m_2 envoie :

$1 \mapsto 2 \quad 2 \mapsto 3 \quad \dots \quad \frac{p-1}{2} \mapsto p-1$

$\frac{p+1}{2} \mapsto 1 \quad \frac{p+3}{2} \mapsto 3 \quad \dots \quad \frac{p+(p-2)}{2} = p-1 \mapsto p-2$

On voit que 1 possède une inversion avec $\frac{p+1}{2}$

2 possède deux inversions avec $\frac{p+1}{2}$ et $\frac{p+3}{2}$

$\vdots$

$\frac{p-1}{2}$ possède $\frac{p-1}{2}$ inversions avec tous ceux qui lui précède

donc $\mathrm{Inv}(m_2) = 1+2+3+\dots+\frac{p-1}{2} = \frac{1}{2} \times \frac{p-1}{2} \times \frac{p+1}{2} = \frac{p^2-1}{8}$

□

Leçons: 101, 105, 191, 161,

CVA p135

Détermination des groupes d'isométries du tétraèdre

Théorème:

Les groupes d'isométries du tétraèdre régulier sont : $Is(T) \simeq \mathfrak{S}_4$ et $Is^+(T) \simeq \mathfrak{A}_4$

Démonstration:

On note T le tétraèdre régulier (plein). On note S_1, S_2, S_3 et S_4 les sommets de T.

Étape 1: Mq une isométrie du tétraèdre stabilise l'ensemble de ses points extremaux.

On sait qu'une application affine envoie un segment sur un segment, donc, sur un segment [AB], les points extremaux sont A et B.

Soit S un point extrémal de T et $g \in Is(T)$. Notons $S' = g(S)$. Mq S' est extremal

Soit $M', N' \in T$ tq $M' \neq N'$ et $S' \in [M'N']$.

On pose $M := g^{-1}(M')$ $N := g^{-1}(N')$

Comme g^{-1} est, tout comme g, une application affine, elle envoie le segment $[M'N']$ vers le segment $[g^{-1}(M')\, g^{-1}(N')] = [MN] \subset T$

Vu que S est extremal, $S = M$ ou $S = N$ et donc $S' = M'$ ou N'.

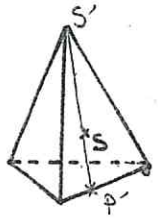
Donc S' est extremal.

Ccl: Si $g \in Is(T)$, g envoie un point extrémal de T sur un point extremal de T.

Étape 2: S est un sommet du tétraèdre ssi S est extrémal

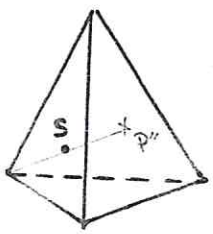
$\Leftarrow$ • Si S est sur une arête, il est en particulier extrémal sur l'arête. Donc, par l'étape 1, c'est un sommet.

• Si S est sur une face F. Projetons S à partir d'un sommet S' de F, sur l'arête opposé à S'.



On note P' le point ainsi obtenu.
Le tétraèdre étant convexe, le segment $[S'P']$ ainsi obtenu reste dans le tétraèdre. Comme S est extremal sur ce segment, $S = S'$ ou $S = P'$.
Si $S = S'$ c'est un sommet, sinon si $S = P'$, on se ramène au cas précédent.
Donc S est un sommet.

• Si S est un point intérieur au tétraèdre, on projete S à partir d'un sommet S'' sur la face opposé F''
On obtient ainsi un point noté P''.
Par convexité, le segment reste dans le tétraèdre.
Donc $S = S''$ ou $S = P''$.
On peut alors appliqué le raisonnement précédent. S''



Donc, si S est un point extremal, c'est un sommet du tétraèdre.

⇒ Comme les quatres sommets de T ne sont pas coplanaires, la famille (S_1, S_2, S_3, S_4) constitue un repère de l'espace affine $\mathbb{R}^3$. Dans ce repère, le tétraèdre T est l'ensemble des points M de coord (x_1, x_2, x_3) avec $x_i \geq 0$ et $\sum x_i \leq 1$.

Supposons que l'origine S_1 soit dans $[MM']$ avec $M = (x_i)$ et $M' = (x_i')$ sur le tétraèdre
Alors S_1 est barycentre à coeff positifs de $(M,\alpha), (M',\alpha')$.

On peut supposer que les coefficients sont tous positifs strictement (sinon $S_1 = M$ ou M')

Or, $\alpha(x_1, x_2, x_3) + \alpha'(x_1', x_2', x_3') = (0,0,0)$. avec $\alpha > 0$, $\alpha' > 0$ et $\alpha + \alpha' = 1$ et les x_i, x_i' positifs.

Donc $(x_1, x_2, x_3) = (x_1', x_2', x_3') = (0,0,0)$

Donc $M = M' = S_1$.

Le sommet S_1 est donc bien un point extrémal.

On peut enfin envoyer un sommet sur un autre sommet par une application affine (ex: rotation d'ordre 3). On en déduit par l'étape 1 que tous les S_i sont extremaux.

Donc: si $g \in Is(T)$ alors g permute les quatres sommets de T.

Étape 3: Mq $Is(T) \simeq \mathfrak{S}_4$

Notons $\mathcal{E}$ l'ensemble des sommets (et donc des points extremaux) de T. Mq $Is(T) \simeq \mathfrak{S}(\mathcal{E})$

Considérons $\Phi : Is(T) \longrightarrow \mathfrak{S}(\mathcal{E}) \simeq \mathfrak{S}_4$. L'application Φ envoie l'isométrie

$$g \longmapsto \Phi(g) : \mathcal{E} \to \mathcal{E}, \quad S \mapsto g(S)$$

g qui est une application de l'espace affine vers lui-même, sur la permutation que g induit sur l'ensemble des sommets de T.
Il s'agit donc d'un morphisme de groupe.

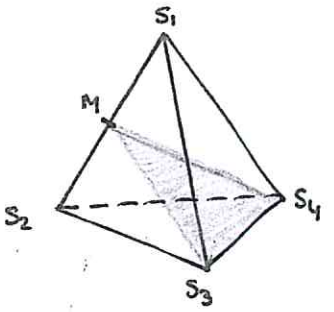
- Mq Φ est injectif:

Soit $g \in Is(T)$ telle que $\Phi(g) = Id_{\mathcal{E}}$, càd g laisse fixes les 4 sommets. Or, (S_1, S_2, S_3, S_4) constitue un repère affine de $\mathbb{R}^3$. Ainsi g fixe un repère de $\mathbb{R}^3$: c'est donc l'identité.
Donc $\ker \Phi = \{Id_T\}$
Donc Φ est injectif.

- Mq Φ est surjectif:

On montre que $\operatorname{Im} \Phi$ contient un système de générateur de $\mathfrak{S}_4$: les transpositions.
Pour cela, il nous suffit de mq $\operatorname{Im} \Phi$ contient $(1\ 2)$; les autres transpositions s'y trouveront alors par symétrie.
On cherche donc une (unique) isométrie qui laisse fixe S_3 et S_4 et qui échange S_1 et S_2.

Il s'agit de la symétrie orthogonale par rapport au plan médiateur $[S_1S_2]$, cf figure ci-contre.



Il faut vérifier que cette symétrie est bien une isométrie du tétraèdre.
En effet, c'est bien une isométrie et comme elle stabilise l'ensemble des sommets, elle envoie l'enveloppe convexe des sommets sur elle-même : c'est donc une isométrie qui stabilise le tétraèdre.

<u>ccl</u> : ϕ est donc un isomorphisme, donc $Is(T) \simeq \mathcal{S}(\mathcal{E}) \simeq \mathcal{S}_4$

<u>Étape 4</u> : Mq $Is^+(T) \simeq \mathcal{A}_4$

On remarque que tout sous-groupe affine qui fixe un point peut-être assimilé à un sous-groupe du groupe linéaire ; on peut par exemple lui appliquer le déterminant.

Le sous-groupe $Is^+(T)$ est alors le noyau du déterminant restreint à $Is(T)$.

Comme l'image du déterminant restreint à $Is(T)$ prend exactement deux valeurs 1 et -1, il vient que le sous-groupe $Is^+(T)$ est d'indice 2 dans $Is(T)$.

Via l'isomorphisme de l'étape 3, entre $Is(T)$ et $\mathcal{S}_4$, le sous-groupe $Is^+(T)$ est donc isomorphe à un sous-groupe d'indice 2 de $\mathcal{S}_4$.

Or, il n'y a qu'un seul tel sous-groupe : le sous-groupe alterné $\mathcal{A}_4$.

On a donc $Is^+(T) \simeq \mathcal{A}_4$.

Classification des groupes simples d'ordre 60.

Thm: Soit G un groupe simple d'ordre 60. Alors G est isomorphe au groupe alterné A_5.

Démo: (On admet que le groupe alterné A_5 est un groupe simple d'ordre 60).

Lemme: Soient deux groupes G et H. Soit ϕ un morphisme de G vers H. Alors ϕ envoie $D(G)$ dans $D(H)$.

Démo:

Par définition, le groupe dérivé de G $D(G)$ est le sous-groupe de G engendré par les commutateurs $[g,g'] := gg'g^{-1}g'^{-1}$, $g,g' \in G$.
Or, comme ϕ est un morphisme de groupes, il envoie $[g,g']$ sur $[\phi(g),\phi(g')]$. Il envoie donc les générateurs de $D(G)$ sur des éléments de $D(H)$ donc ϕ envoie $D(G)$ sur $D(H)$. □

Soit n_5 le nombre de 5-Sylow de G. Par les théorèmes de Sylow, on a:
$\begin{cases} n_5 \mid 12 \\ n_5 \equiv 1 \ [5] \end{cases}$ donc $n_5 = 1$ ou $n_5 = 6$. Or G est simple, donc ses seuls sous-groupes distingués sont $\{e\}$ et G tout entier, donc $n_5 \neq 1$.
On en déduit donc que G possède 6 5-Sylow.

On fait agir G par conjugaison sur l'ensemble de ses 5-Sylow. Comme G a 6 5-Sylow, cette action fournit un morphisme de G dans $\mathfrak{S}_6$. Montrons que ce morphisme est injectif, c'est-à-dire que son noyau est trivial.
Soient $H_1, \dots, H_6$ les 6 5-Sylow de G, donc φ est défini par:

$$\varphi : G \to S(X) \simeq \mathfrak{S}_6$$
$$g \mapsto \begin{pmatrix} X \to X \\ H_i \mapsto gH_ig^{-1} \end{pmatrix}$$

$\ker\varphi$ étant un sous-groupe distingué de G et G simple, $\ker\varphi$ est soit trivial, soit G tout entier.
Par l'absurde, supposons que $\ker\varphi = G$. Dans ce cas, l'action est triviale, c'est-à-dire que, pour tout $g \in G$, $\forall i \in [\![1,6]\!]$, $gH_ig^{-1} = H_i$, ce qui contredit le théorème de Sylow qui assure la transitivité de l'action de G sur l'ensemble de ses 5-Sylow.

Donc $\ker\varphi$ est trivial et le morphisme d'action est injectif.

D'après le lemme, tout morphisme injectif de G dans $\mathfrak{S}_6$ envoie $D(G)$ dans $D(\mathfrak{S}_6)$. Montrons que $D(G) = G$ et que $D(\mathfrak{S}_6) \subset A_6$.

- $D(\mathfrak{S}_6) \subset \mathcal{A}_6$ car tous les commutateurs de $\mathfrak{S}_6$ vérifient
$$\varepsilon(gg'g^{-1}g'^{-1}) = \varepsilon(g)\,\varepsilon(g')\,\varepsilon(g^{-1})\,\varepsilon(g'^{-1}) = 1$$
- $D(G)$ est un sous-groupe distingué de G (en effet, $\forall g,h,k \in G$, $g[h,k]g^{-1} = [ghg^{-1}, gkg^{-1}]$)

Comme G est simple, il suffit donc de montrer que $D(G)$ n'est pas trivial

Par l'absurde, supposons que $D(G)$ est trivial. Alors $[g,g'] = e$ $\forall g \in G$ donc G est abélien. Or un groupe abélien est simple si et seulement si son ordre est premier. En effet, dans le cas abélien, tout sous-groupe est distingué donc tout élément non trivial engendre G tout entier. En particulier, G est cyclique (et simple) donc d'ordre premier.

Comme G est d'ordre 60, on a bien $D(G) = G$.

On a donc un morphisme injectif de G vers $\mathcal{A}_6$. On peut donc assimiler G à un sous-groupe de $\mathcal{A}_6$ d'indice $\frac{360}{60} = 6$.

Dans le cas général, si on a H un sous-groupe d'un groupe G alors on a une action de G sur l'ensemble G/H des classes à gauche, définie par $g \cdot (g'H) = (gg')\cdot H$, $\forall g,g' \in G$

Cette action est transitive car $g''g'^{-1}$ envoie $g'H$ sur $g''H$ $\forall g', g'' \in G$.

Ici, on obtient donc que $\mathcal{A}_6$ agit transitivement sur $\mathcal{A}_6/G$ (de cardinal 6) ce qui nous donne un morphisme de $\mathcal{A}_6$ dans $\mathfrak{S}_6$. Comme $\mathcal{A}_6$ est simple, pour montrer que ce morphisme est injectif, il suffit de montrer qu'il n'est pas trivial Or l'action est transitive donc le morphisme ne peut pas être trivial (sinon toute orbite serait singleton). On a donc $\varphi : \mathcal{A}_6 \longrightarrow \mathfrak{S}_6$ injectif. Or si $g \in G$, il fixe la classe de e : $\bar{e} = eG = G$.

$\varphi(g)(\bar{e}) = g \cdot (eG) = gG = G$.

Le morphisme φ envoie donc g sur $\varphi(g) \in \mathfrak{S}(\mathcal{A}_6/G) \simeq \mathfrak{S}_6$ qui, de plus, stabilise la classe $\bar{e}$. Or, le stabilisateur d'un élément de $\mathfrak{S}_n$ est $\mathfrak{S}_{n-1}$ donc φ envoie G injectivement dans $\mathfrak{S}_5$.

Comme dans le lemme, $D(G) = G$ s'envoie injectivement dans $D(\mathfrak{S}_5) \subset \mathcal{A}_5$.

On a un isomorphisme par égalité des cardinaux.

d'où $G \simeq \mathcal{A}_5$. □

Réf: CVA p 129