Université Nice Côte d'Azur
Année 2020-2021

Fiche thématique : Les groupes symétrique et alterné

Table des matières

1. Aperçu des propriétés

◇ Ordre du groupe $\mathcal{S}_n$: $n!$

◇ Formule de conjugaison. On écrit les cycles sous la forme $(i_1 \ \dots \ i_k)$. Attention, il y a k écritures différentes pour le même cycle :

$$\sigma(i_1 \ \dots \ i_k)\sigma^{-1} = (\sigma(i_1) \ \dots \ \sigma(i_k)).$$

◇ Décomposition en cycles à supports disjoints. Exposant, Générateurs.

On a existence et unicité à permutation près de la décomposition en cycles. On en déduit que l'exposant du groupe est le ppcm de $\{1, 2, \dots, n\}$. Il en découle également que les cycles constituent un système de générateurs, puis, les transpositions, grâce à la formule $(i_1 \ i_2 \ \dots \ i_k) = (i_1 \ i_2) \dots (i_{k-1} \ i_k)$. Les transpositions de type $(k \ k+1)$ forment un système de générateurs (avec relations de tresses). Pour finir, il faut noter le système de générateurs le plus petit possible (mais dont les relations sont compliquées) donné par $(1\ 2)$ et $(1\ 2 \ \dots \ n)$.

◇ Classes de conjugaison-paramétrisation, cardinal.

Grâce à la décomposition (unique) en cycles, on peut paramétrer les classes de conjugaison via les longueurs de cycles.

◇ Caractères (morphismes) de $\mathcal{S}_n$ dans le groupe multiplicatif $\mathbb{C}^*$.

En utilisant le système de générateurs donné par les transpositions, on montre qu'il y a au plus deux tels morphismes (dont un trivial). On peut

ensuite exhiber le morphisme [1]

$$\mathrm{sgn}(\sigma) = \prod_{1\leq i<j\leq n} \frac{\sigma(j)-\sigma(i)}{j-i} = \prod_{(i,j)\in\mathcal{P}_{2,n}} \frac{\sigma(j)-\sigma(i)}{j-i}$$

où $\mathcal{P}_{2,n}$ désigne l'ensemble des parties de $\{1,\ldots,n\}$ à 2 éléments. Notons que $\frac{\sigma(j)-\sigma(i)}{j-i}$ est bien défini pour $\{i,j\} \in \mathcal{P}_{2,n}$, car il ne dépend pas de l'ordre dans lequel on a choisi i et j. Du coup, on introduit le groupe alterné $\mathcal{A}_n := \ker \mathrm{sgn}$.

◇ Automorphismes de $\mathcal{S}_n$.

En utilisant le cardinal des classes de conjugaison d'éléments d'ordre 2, on obtient que tout automorphisme est intérieur (en montrant que toute transposition s'envoie sur une transposition, voir [Per82]), sauf pour $n = 6$ où l'on a une exception numérique entre transpositions et 3-transpositions :

$$\frac{6!}{4!2^1} = \frac{6!}{3!2^3}$$

Il n'est pas très difficile de prouver la présence d'un automorphisme extérieur de $\mathcal{S}_6$: on fait par exemple agir $\mathcal{S}_5$ sur ses six 5-Sylow. L'image de l'action est un sous-groupe transitif H de $\mathcal{S}_6$. On fait ensuite agir $\mathcal{S}_6$ sur $\mathcal{S}_6/\mathrm{H}$ qui possède 6 éléments (comme dans la démonstration de H d'indice n implique $\mathrm{H} \simeq \mathcal{S}_{n-1}$), et on obtient, par cette action, un morphisme de $\mathcal{S}_6$ dans lui-même qui en fait est un automorphisme de $\mathcal{S}_6$ et qui envoie H, qui est transitif, sur le stabilisateur de id, qui ne l'est pas.

Sous-groupes de $\mathcal{S}_n$

◇ Le centre.

Le centre de $\mathcal{S}_n$ est trivial pour $n \neq 2$. C'est juste une application de la formule de conjugaison.

◇ Le groupe dérivé = le groupe alterné, qui est engendré par les 3-cycles : $D(\mathcal{S}_n) = \mathcal{A}_n$. L'inclusion directe est évidente. Pour l'inclusion inverse, on le fait en deux temps : d'une part les 3-cycles engendrent $\mathcal{A}_n$ et d'autre part on vérifie qu'ils sont bien dans $D(\mathcal{S}_n)$. C'est très utile : on obtient souvent des morphismes qui partent de $\mathcal{S}_n$ (par des actions de groupes), puis, que l'on dérive.

◇ Le seul sous-groupe d'indice 2 de $\mathcal{S}_n$ est $\mathcal{A}_n$.

◇ Simplicité du groupe alterné.

---

1. La signature est bien un morphisme de $\mathcal{S}_n$ dans $\mathbb{C}^*$ puisque pour σ, τ dans $\mathcal{S}_n$ nous avons

$$\begin{aligned}
\mathrm{sgn}(\sigma\circ\tau) &= \prod_{\{i,\,j\}\in\mathcal{P}_{2,n}} \frac{\sigma(\tau(j))-\sigma(\tau(i))}{j-i} \\
&= \prod_{\{i,\,j\}\in\mathcal{P}_{2,n}} \frac{\sigma(\tau(j))-\sigma(\tau(i))}{\tau(j)-\tau(i)} \prod_{\{i,\,j\}\in\mathcal{P}_{2,n}} \frac{\tau(j)-\tau(i)}{j-i} \\
&= \prod_{\{k,\,\ell\}\in\mathcal{P}_{2,n}} \frac{\sigma(k)-\sigma(\ell)}{k-\ell} \prod_{\{i,\,j\}\in\mathcal{P}_{2,n}} \frac{\tau(j)-\tau(i)}{j-i} \\
&= \mathrm{sgn}(\sigma)\mathrm{sgn}(\tau).
\end{aligned}$$

On montre qu'un sous-groupe distingué contient un 3-cycle, puis, il les contient tous. C'est historique dans la non résolution par radicaux d'une équation de degré 5.

◇ Tout sous-groupe d'indice n de $\mathcal{S}_n$ est isomorphe à $\mathcal{S}_{n-1}$ (mais pour $n = 6$ il peut ne pas être le stabilisateur d'un élément). Bien connaître la démonstration qui passe par l'action d'un groupe G sur ses classes $^{\mathrm{G}}\!/_{\mathrm{H}}$.

◇ Groupe dérivé du groupe alterné. C'est toujours lui-même sauf pour $n = 3$ (groupe trivial) et $n = 4$ (le groupe de Klein).

Applications

◇ Actions du groupe symétrique.

Il faut remarquer que $\mathcal{S}_n$, à l'instar de $\mathrm{GL}(n, \Bbbk)$, arrive avec une action naturelle. Elle est n-transitive, ce qui constitue un record absolu, quand on sait à quel point la triple-transitivité est rare dans la nature.

- Théorème de Cayley.
- Polynômes symétriques. On a une action par automorphismes de $\mathcal{S}_n$ sur l'algèbre des polynômes à n indéterminées. La sous-algèbre des invariants est l'algèbre des polynômes symétriques. Parmi eux, il y a les polynômes symétriques élémentaires et les polynômes de Newton. Les premiers sont importants car ils engendrent la sous-algèbre des invariants (en toute caractéristique, et même sur $\mathbb{Z}$!) De plus, les fonctions symétriques élémentaires en les racines d'un polynôme unitaire sont les coefficients du polynôme.
- Représentations du groupe symétrique : la triviale, la signature, la naturelle (matrices de permutation), la standard (liée à la double transitivité de l'action naturelle de $\mathcal{S}_n$, ce qui constitue un joli développement). Il est bon de savoir calculer la table de caractères pour $n \leq 5$.
- La table des caractères de $\mathcal{S}_n$ est à coefficients dans $\mathbb{Z}$.

◇ Autres applications

- Le déterminant. Sans signature pas de déterminant. En fait, l'unicité d'une forme n-linéaire alternée à constante près sur un espace vectoriel de dimension n est assez claire, mais l'existence, pas du tout. Cela provient essentiellement de l'existence de la signature.
- Représentation du groupe du tétraèdre ou du groupe de l'icosaèdre.

◇ Exercices classiques :

- La formule de Wilson avec les p-Sylow de $\mathcal{S}_p$, p premier.
- Peut-on voir $\mathcal{S}_n$ comme produit semi-direct de $\mathcal{A}_n$?

2. Ordre du groupe

***Lemme* 2.1.** — *Soit $n \geq 0$ un entier. Soient X et Y deux ensembles de cardinal n.*

L'ensemble des bijections de X sur Y a pour cardinal $n!$.

En particulier (cas où $Y = X$) le groupe $\mathcal{S}_X$ a pour ordre $n!$.

Démonstration par récurrence sur n. Si $n = 0$, alors $X = Y = \emptyset$. Or si i est une application de l'ensemble vide dans lui-même, $i = \mathrm{id}$. Il y a donc une unique bijection de X sur Y (à savoir l'identité, et la propriété requise est démontrée puisque $0! = 1$.

Supposons $n > 0$ et la propriété vraie en rang $< n$. Comme $n > 0$ l'ensemble X est non vide ; on choisit $x \in X$. Pour tout y dans Y, on note B_y l'ensemble des bijections de X vers Y qui envoient x sur y. Le cardinal de B est alors égal à $\sum_{y\in Y} \mathrm{card}(B_y)$. Soit $y \in Y$. Se donner une bijection de X sur Y qui envoie x sur y revient à se donner une bijection de $X \smallsetminus \{x\}$ sur $Y \smallsetminus \{y\}$: une fois qu'on a imposé que l'image de x doit être égale à y, il reste à déterminer les images des autres éléments de X, nécessairement différentes de y. Comme $X \smallsetminus \{x\}$ et $Y \smallsetminus \{y\}$ sont de cardinal $n-1$, l'hypothèse de récurrence assure qu'il y a $(n-1)!$ bijections de $X \smallsetminus \{x\}$ sur $Y \smallsetminus \{y\}$; le cardinal de B_y est par conséquent égal à $(n-1)!$. Il vient

$$\mathrm{card}(B) = \sum_{y\in Y} \mathrm{card}(B_y) = \sum_{y\in Y} (n-1)! = \mathrm{card}(Y)(n-1)! = n \times (n-1)! = n!$$

□

3. Classes de conjugaison

***Proposition* 3.1.** — *Si $\sigma = (a_1\ a_2\ \ldots\ a_k) \in \mathcal{S}_n$ est un k-cycle et τ un élément de $\mathcal{S}_n$, nous avons*

$$\tau \circ \sigma \circ \tau^{-1} = \big(\tau(a_1)\ \tau(a_2)\ \ldots\ \tau(a_k)\big). \tag{1}$$

Tous les k-cycles sont conjugués dans $\mathcal{S}_n$.

Les classes de conjugaison de $\mathcal{S}_n$ sont en bijection avec les partitions de n :

$$n = k_1 + k_2 + \ldots + k_r, \quad r \in \mathbb{N}, \quad 1 \leq k_1 \leq k_2 \leq \ldots \leq k_r.$$

Le nombre de classes de conjugaison est donc égal au nombre de « partages » de l'entier n, et si la décomposition d'une permutation contient k_1 1-cycles (les points fixes), k_2 2-cycles, …, k_m m-cycles, alors le nombre de ses conjugués vaut :

$$\frac{n!}{1^{k_1}k_1!\,2^{k_2}k_2!\,\ldots\,m^{k_m}k_m!}.$$

Démonstration. Si $x \notin \big\{\tau(a_1), \tau(a_2), \ldots, \tau(a_k)\big\}$, alors $\tau^{-1}(x) \notin \big\{a_1, a_2, \ldots, a_k\big\}$ donc $\tau \circ \sigma \circ \tau^{-1}(x) = x$. Si en revanche $x = \tau(a_i)$, alors $\tau \circ \sigma\tau^{-1}(x) = \tau \circ \sigma(a_i) = \tau(a_{i+1})$. D'où l'égalité (1).

Écrivons $\sigma = \sigma_1\sigma_2 \ldots \sigma_r$ comme produit de cycles à supports disjoints de longueurs k_1, k_2, …, k_r que nous pouvons ordonner de sorte que $1 \leq k_1 \leq k_2 \leq \ldots \leq k_r$. Alors

$$\tau \circ \sigma \circ \tau^{-1} = (\tau \circ \sigma_1 \circ \tau^{-1}) \circ (\tau \circ \sigma_2 \circ \tau^{-1}) \circ \ldots \circ (\tau \circ \sigma_r \circ \tau^{-1}) \tag{2}$$

est encore un produit de cycles disjoints de mêmes longueurs k_1, k_2, …, k_r que ceux de σ. Une classe de conjugaison détermine donc bien une partition de $n = k_1 + k_2 + \ldots + k_r$. Réciproquement compte tenu de (1) et (2) nous voyons que des permutations correspondant à la même partition sont conjuguées. □

4. Décomposition d'une permutation en produit de cycles disjoints

Le groupe $\mathcal{S}_n$ opère sur $E = \big\{1, 2, \ldots, n\big\}$. Soit $\sigma \in \mathcal{S}_n$ une permutation. Le groupe cyclique $\langle\sigma\rangle$ engendré par σ opère aussi sur E. Soient $\mathcal{O}_1$, $\mathcal{O}_2$, …, $\mathcal{O}_k$ les orbites de E sous l'action de $\langle\sigma\rangle$. Alors les permutations σ_i définies par

$$\sigma_i(x) = \begin{cases} x & \text{si } x \notin \mathcal{O}_i \\ \sigma(x) & \text{si } x \in \mathcal{O}_i \end{cases}$$

sont des cycles, d'ordre $|\mathcal{O}_i|$, deux à deux permutables. De plus $\sigma = \sigma_1\sigma_2 \dots \sigma_k$.

Par exemple si $E = \{1, 2, \dots, 8\}$ et

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 6 & 4 & 5 & 1 & 8 & 7 & 2 \end{pmatrix}$$

nous avons $\sigma = (1\ 3\ 4\ 5)(2\ 6\ 8)(7) = (1\ 3\ 4\ 5)(2\ 6\ 8)$; en général les cycles d'ordre 1 sont omis dans l'écriture de σ.

5. Le centre de $\mathcal{S}_n$

Soit $n \geq 3$. Le centre de $\mathcal{S}_n$ est réduit à $\{\mathrm{id}\}$.

Si $n \geq 3$, si a, b appartiennent à $\{1, 2, \dots, n\}$ et si σ appartient à $\mathcal{S}_n$, alors

$$\sigma \circ (a\ b) \circ \sigma^{-1} = (\sigma(a)\ \sigma(b)) \tag{3}$$

Soit σ un élément du centre de $\mathcal{S}_n$. En particulier $\sigma \circ (1\ 2) = (1\ 2) \circ \sigma$, *i.e.* $\sigma \circ (1\ 2) \circ \sigma^{-1} = (1\ 2)$. Par suite (3) entraîne

$$(\sigma(1)\ \sigma(2)) = (1\ 2).$$

Ainsi nécessairement $\sigma(1) = 1$ ou $\sigma(1) = 2$. De même $\sigma \circ (1\ 3) = (1\ 3) \circ \sigma$ et donc

$$(\sigma(1)\ \sigma(3)) = (1\ 3).$$

Il en résulte que $\sigma(1) = 1$. Ce qu'on a fait avec 1 peut être fait avec n'importe quel entier compris entre 2 et n. Il en résulte que $\sigma = \mathrm{id}$.

Réciproquement id commute avec toutes les permutations.

6. Les automorphismes de $\mathcal{S}_n$, $n \geq 3$

Puisque $n \geq 3$ le centre $Z(\mathcal{S}_n)$ de $\mathcal{S}_n$ est réduit à $\{\mathrm{id}\}$. Par suite $\mathcal{S}_n$ agit fidèlement sur lui-même par conjugaison. Autrement dit le groupe $\mathrm{Int}(\mathcal{S}_n)$ des automorphismes intérieurs de $\mathcal{S}_n$ est isomorphe à $\mathcal{S}_n$.

L'énoncé suivant assure que sauf dans le cas exceptionnel $n = 6$ les automorphismes intérieurs sont les seuls automorphismes.

On donne ensuite un automorphisme non intérieur de $\mathcal{S}_6$.

6.0.1. *Automorphismes de $\mathcal{S}_n$, $n \neq 6$.*

***Lemme* 6.1.** — *Soit $n \geq 3$. Soient a, b dans $\{1, 2, \dots, n\}$ et $\sigma \in \mathcal{S}_n$. Alors*

$$\sigma \circ (a\ b) \circ \sigma^{-1} = (\sigma(a)\ \sigma(b))$$

***Lemme* 6.2.** — *Soit $n \geq 3$. Le centre de $\mathcal{S}_n$ est réduit à $\{\mathrm{id}\}$.*

Démonstration. Soit σ un élément du centre de $\mathcal{S}_n$. En particulier $\sigma \circ (1\ 2) = (1\ 2) \circ \sigma$, *i.e.* $\sigma \circ (1\ 2) \circ \sigma^{-1} = (1\ 2)$. Par suite (Lemme 6.1)

$$(\sigma(1)\ \sigma(2)) = (1\ 2).$$

Ainsi nécessairement $\sigma(1) = 1$ ou $\sigma(1) = 2$. De même $\sigma \circ (1\ 3) = (1\ 3) \circ \sigma$ et donc

$$(\sigma(1)\ \sigma(3)) = (1\ 3).$$

Il en résulte que $\sigma(1) = 1$. Ce qu'on a fait avec 1 peut être fait avec n'importe quel entier compris entre 2 et n. Il en résulte que $\sigma = \mathrm{id}$.

Réciproquement id commute avec toutes les permutations. □

***Théorème* 6.3.** — *Soit $n \geq 3$. Supposons que $n \neq 6$; alors*

$$\mathrm{Aut}(\mathcal{S}_n) = \mathrm{Int}(\mathcal{S}_n) \simeq \mathcal{S}_n.$$

***Lemme* 6.4.** — *Soit φ un automorphisme de $\mathcal{S}_n$ qui envoie transpositions sur transpositions. Alors φ appartient à $\mathrm{Int}(\mathcal{S}_n)$.*

Démonstration. Les transpositions de la forme $(1\ i)$ où $2 \leq i \leq n$ engendrent $\mathcal{S}_n$. Posons $\tau_i = \varphi(1\ i)$. Remarquons que pour i et j distincts τ_i et τ_j ne commutent pas car $(1\ i)$ et $(1\ j)$ ne commutent pas. Il en résulte que les transpositions τ_i et τ_j ont exactement un élément en commun dans leur support. On peut donc écrire τ_2 et τ_3 sous la forme

$$\tau_2 = (\alpha_1\ \alpha_2) \qquad\qquad \tau_3 = (\alpha_1\ \alpha_3)$$

avec $\alpha_2 \neq \alpha_3$. Montrons que pour tout $k \geq 4$ on a $\tau_k = (\alpha_1\ \alpha_k)$ pour un certain $\alpha_k \in \{1, 2, \ldots, n\}$. En effet si α_1 n'était pas dans le support de τ_k on aurait $\tau_k = (\alpha_2\ \alpha_3)$ et

$$\tau_2 \circ \tau_k = (\alpha_1\ \alpha_2\ \alpha_3) \qquad\qquad \tau_3 \circ \tau_k = (\alpha_1\ \alpha_3\ \alpha_2)$$

seraient inverses l'un de l'autre. Mais

$$(1\ 2)(1\ k) = (2\ 1\ k)$$

n'est pas l'inverse de

$$(1\ 3)(1\ k) = (3\ 1\ k)$$

contradiction.

Notons que $\alpha\colon k \mapsto \alpha_k$ est un élément de $\mathcal{S}_n$.

L'automorphisme φ et la conjugaison par α coïncident sur les générateurs $(1\ j)$ de $\mathcal{S}_n$; ils coïncident donc sur $\mathcal{S}_n$ tout entier. □

Démonstration du Théorème 6.3. Soit φ un automorphisme non intérieur de $\mathcal{S}_n$. Montrons que $n = 6$.

D'après le Lemme 6.4 il existe une transposition τ telle que $\varphi(\tau)$ ne soit pas une transposition. Puisque $(\varphi(\tau))^2 = \mathrm{id}$, $\varphi(\tau)$ est un produit de $k \geq 2$ transpositions à supports disjoints. Désignons par $\mathrm{C}(\tau)$ le centralisateur de τ

$$\mathrm{C}(\tau) = \big\{ f \in \mathcal{S}_n \,|\, f \circ \tau = \tau \circ f \big\}.$$

On a

$$\mathrm{C}(\tau) = \underbrace{\mathbb{Z}/2\mathbb{Z}}_{\text{engendré par } \tau} \times \underbrace{\mathcal{S}_{n-2}}_{\text{permutations de support disjoint de celui de } \tau}$$

En particulier on a un morphisme surjectif

$$\psi\colon \mathrm{C}(\tau) \to \mathcal{S}_{n-2}$$

de noyau $\mathbb{Z}/2\mathbb{Z}$.

Posons $\mathrm{H} = \mathrm{C}(\varphi(\tau)) = \big\{ f \in \mathcal{S}_n \,|\, f \circ \varphi(\tau) = \varphi(\tau) \circ f \big\}$. Les groupes H et $\mathrm{C}(\tau)$ sont isomorphes via φ. Chacune des transpositions de la décomposition de $\varphi(\tau)$ commute avec $\varphi(\tau)$ donc H contient un sous-groupe N isomorphe à $\left(\mathbb{Z}/2\mathbb{Z}\right)^k$. De plus N est le noyau du morphisme

$$\begin{array}{ccl} \mathrm{H} & \to & \mathcal{S}_k \\ h & \mapsto & \text{permutation induite sur les } k \text{ transpositions de la décomposition de } \varphi(\tau) \end{array}$$

donc $\mathrm{N} \lhd \mathrm{H}$.

Ainsi comme $\mathrm{C}(\tau) \simeq \mathrm{H}$, $\mathrm{C}(\tau)$ contient un sous-groupe N' avec les deux propriétés suivantes :

$$\begin{cases} \mathrm{N}' \lhd \mathrm{C}(\tau) \\ \mathrm{N}' \simeq \left(\mathbb{Z}/2\mathbb{Z}\right)^k \end{cases}$$

Via ψ on obtient que $\mathcal{S}_{n-2}$ contient un sous-groupe distingué isomorphe à $\left(\mathbb{Z}/2\mathbb{Z}\right)^k$ ou $\left(\mathbb{Z}/2\mathbb{Z}\right)^{k-1}$ suivant que $\tau \in \mathrm{N}'$ ou $\tau \notin \mathrm{N}'$.

Or les sous-groupes distingués de $\mathcal{S}_n$ sont

- $\diamond$ $\{\mathrm{id}\}$, $\mathcal{A}_n$, $\mathcal{S}_n$ si $n \neq 4$;
- $\diamond$ $\{\mathrm{id}\}$, $\mathcal{K} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, $\mathcal{A}_4$, $\mathcal{S}_4$.

On en déduit les deux possibilités suivantes

- $\diamond$ $n = 4$ car $\mathcal{S}_2 \simeq \mathbb{Z}/2\mathbb{Z}$ peut alors correspondre à $\left(\mathbb{Z}/2\mathbb{Z}\right)^{k-1}$ avec $k = 2$;
- $\diamond$ $n = 6$ car $\mathcal{S}_4$ contient $\mathcal{K} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Supposons que $n = 4$. Le centralisateur d'une transposition dans $\mathcal{S}_4$ est de cardinal 4 (c'est le groupe $\mathcal{K}$) alors que le centralisateur d'une double transposition est de cardinal 8 (en effet il divise strictement 24, est multiple strict de 4 car contient $\mathcal{K}$ mais aussi au moins un 4-cycle) : contradiction.

Ainsi $n = 6$. □

6.0.2. *Automorphismes extérieurs de $\mathcal{S}_6$, version* 1. Étudions désormais les automorphismes extérieurs de $\mathcal{S}_6$.

Rappelons l'énoncé suivant :

***Théorème* 6.5.** — *Soit $n \geq 5$. Les sous-groupes distingués de $\mathcal{S}_n$ sont* $\{\mathrm{id}\}$, $\mathcal{A}_n$ *et* $\mathcal{S}_n$.

***Lemme* 6.6.** — *L'ensemble* $\mathrm{Syl}_5(\mathcal{S}_5)$ *des* 5*-sous-groupes de* Sylow *de* $\mathcal{S}_5$ *est de cardinal* 6.

***Lemme* 6.7.** — *Numérotons arbitrairement de* 1 à 6 *les éléments de* $\mathrm{Syl}_5(\mathcal{S}_5)$. *Faisons opérer* $\mathcal{S}_5$ *sur* $\mathrm{Syl}_5(\mathcal{S}_5) \simeq \{1, 2, 3, 4, 5, 6\}$ *par conjugaison. La morphisme* $\mathcal{S}_5 \to \mathcal{S}_6$ *associé est injectif. Notons* G *son image.*

***Lemme* 6.8.** — *Numérotons arbitrairement de* 1 à 6 *les éléments de* $\mathcal{S}_6/\mathrm{G}$. *Faisons opérer* $\mathcal{S}_6$ *sur* $\mathcal{S}_6/\mathrm{G} \simeq \{1, 2, 3, 4, 5, 6\}$ *par translations.*

Le morphisme $\varphi\colon \mathcal{S}_6 \to \mathcal{S}_6$ *associé est un automorphisme.*

***Lemme* 6.9.** — *Le groupe* G *n'a pas de points fixes sur* $\{1, 2, 3, 4, 5, 6\}$.

Le groupe $\varphi(\mathrm{G})$ *admet un point fixe.*

L'automorphisme φ *n'est pas intérieur.*

Démonstration du Lemme 6.6. On a $|\mathcal{S}_5| = 5! = 120 = 2^3 \cdot 3 \cdot 5$. L'ordre d'un élément de $\mathrm{Syl}_5(\mathcal{S}_5)$ est donc 5. Or 5 est premier donc tout élément de $\mathrm{Syl}_5(\mathcal{S}_5)$ est isomorphe à $\mathbb{Z}/5\mathbb{Z}$. Posons $n_5 = \#\mathrm{Syl}_5(\mathcal{S}_5)$. Les théorèmes de Sylow assurent que

$$\begin{cases} n_5 \equiv 1 \bmod 5 \\ n_5 \text{ divise } 2^3 \cdot 3 = 24 \end{cases}$$

Par conséquent n_5 appartient à $\{1, 6\}$.

Supposons que $n_5 = 1$. Alors $\mathcal{S}_5$ a un unique 5-Sylow qui est distingué : contradiction avec le fait que les sous-groupes distingués de $\mathcal{S}_5$ sont $\{\mathrm{id}\}$, $\mathcal{A}_5$ et $\mathcal{S}_5$. Par suite $n_5 = 6$. □

Démonstration du Lemme 6.7. Soit K le noyau du morphisme de $\mathcal{S}_5$ vers $\mathcal{S}_\mathrm{G}$. Il est contenu dans le stabilisateur de chacun des éléments de $\mathrm{Syl}_5(\mathcal{S}_5)$. L'action de G sur $\mathrm{Syl}_5(\mathcal{S}_5)$ est transitive (théorème de Sylow). Il en résulte que le stabilisateur de chaque élément de $\mathrm{Syl}_5(\mathcal{S}_5)$ a pour cardinal $\frac{120}{6} = 20$. Donc $|\mathrm{K}|$ divise 20. Puisque K est distingué dans $\mathcal{S}_5$, que $|\mathrm{K}|$ divise 20 et que les sous-groupes distingués de $\mathcal{S}_5$ sont $\{\mathrm{id}\}$, $\mathcal{A}_5$ et $\mathcal{S}_5$, on obtient que $\mathrm{K} = \{\mathrm{id}\}$. □

Démonstration du Lemme 6.8. Soit K′ le noyau du morphisme naturel de $\mathcal{S}_6$ dans $\mathcal{S}_{\mathcal{S}_6/\mathrm{G}}$. Il est contenu dans le stabilisateur des éléments de $\mathcal{S}_6/\mathrm{G}$ et en particulier dans celui de la classe triviale G qui n'est autre que G. Ainsi $|\mathrm{K}'|$ divise $|\mathrm{G}| = 120$. On a donc

$$\begin{cases} \mathrm{K}' \lhd \mathcal{S}_6 \\ |\mathrm{K}'| \text{ divise } 120 \\ \text{les sous-groupes distingués de } \mathcal{S}_6 \text{ sont } \{\mathrm{id}, \mathcal{A}_6, \mathcal{S}_6\} \end{cases}$$

d'où $\mathrm{K}' = \{\mathrm{id}\}$. Autrement dit le morphisme φ est injectif. Pour des raisons de cardinalité φ est bijectif. □

Démonstration du Lemme 6.9. Si G avait un point fixe sur $\{1, 2, 3, 4, 5, 6\} \simeq \mathcal{S}$ cela signifierait qu'il existe un 5-sous-groupe de Sylow invariant par conjugaison, *i.e.* distingué, ce qui est absurde. Par contre $\varphi(\mathrm{G})$ a un point fixe, celui qui correspond à la classe triviale G, invariante sous l'action de G par translation.

Supposons que φ soit intérieur donc de la forme

$$\sigma \mapsto \sigma_0 \circ \sigma \circ \sigma_0^{-1}$$

pour un certain σ_0. Soit p un point fixe de $\varphi(\mathrm{G})$. On aurait alors pour tout $g \in \mathrm{G}$

$$\begin{aligned} g(\sigma_0^{-1}p) &= \sigma_0^{-1}(\sigma_0(g(\sigma_0^{-1}(p)))) \\ &= \sigma_0^{-1}((\sigma_0 \circ g \circ \sigma_0^{-1})(p)) \\ &= \sigma_0^{-1}(\varphi(g)(p)) \\ &= \sigma_0^{-1}(p) \end{aligned}$$

car p est fixe sous $\varphi(\mathrm{G})$. On aboutit alors à une contradiction. □

6.0.3. *Automorphismes extérieurs de $\mathcal{S}_6$, version* 2. Rappel : soit G un groupe. Si H est un sous-groupe de G d'incide r, nous obtenons un morphisme de G dans $\mathcal{S}_r$ en faisant agir G sur les classes à gauche modulo H. Plus précisément si $g_1\mathrm{H}$, …, $g_r\mathrm{H}$ désignent les r classes à gauche, nous associons une permutation $\sigma \in \mathcal{S}_r$ à un élément $g \in \mathrm{G}$ en posant

$$(gg_i)\mathrm{H} = g_{\sigma(i)}\mathrm{H}$$

Notons que $i \mapsto \sigma(i)$ est une bijection : l'inverse est donné par l'action de g^{-1}.

***Lemme* 6.10.** — *Soit $n \geq 5$. Si* H *est un sous-groupe de $\mathcal{S}_n$ d'indice n qui agit transitivement sur $\{1, 2, \ldots, n\}$, alors le morphisme $\psi\colon \mathcal{S}_n \to \mathcal{S}_n$ associé à l'action de $\mathcal{S}_n$ sur les classes de $\mathcal{S}_n$ modulo* H *est un automorphisme non intérieur.*

Démonstration. Considérons l'action

$$\mathcal{S}_n \times \mathcal{S}_n/\mathrm{H} \to \mathcal{S}_n/\mathrm{H} \qquad\qquad (g, g_i\mathrm{H}) \mapsto g_{\sigma(i)}\mathrm{H} := (gg_i)\mathrm{H}$$

Par définition un élément g appartient à $\ker\psi$ si et seulement si

$$g \in \bigcap_{i=1}^{n} \mathrm{Stab}(g_i\mathrm{H}).$$

En particulier $\ker\psi$ est contenu dans H. Comme H est d'indice $n \geq 3$ et comme les seuls sous-groupes distingués de $\mathcal{S}_n$ sont d'indice 1 ou 2 ou n on a $\ker\psi = \{\mathrm{id}\}$. Par suite ψ est un automorphisme.

Raisonnons par l'absurde : supposons que ψ soit un automorphisme intérieur. Alors il existe $a \in \mathcal{S}_n$ tel que $\psi(\mathrm{H}) = a\mathrm{H}a^{-1}$. Ainsi $\psi(\mathrm{H})$ agit transitivement sur $\{1, 2, \ldots, n\}$. En effet soient i, j dans $\{1, 2, \ldots, n\}$; il existe par hypothèse un élément h de H tel que $h(a^{-1}(i)) = a^{-1}(j)$, donc aha^{-1} est un élément de $a\mathrm{H}a^{-1}$ qui envoie i sur j. Remarquons que si $g_i\mathrm{H} = \mathrm{H}$ est la classe de l'élément neutre modulo H, alors $\psi(\mathrm{H})$ fixe i ; en effet si $h \in \mathrm{H}$, alors

$$hg_i\mathrm{H} = h\mathrm{H} = \mathrm{H} = g_i\mathrm{H}$$

et donc n'agit pas transitivement. □

***Proposition* 6.11.** — *Il existe un sous-groupe* H *de* $\mathcal{S}_6$ *d'indice* 6 *qui agit transitivement sur*

$$\{1, 2, 3, 4, 5, 6\}.$$

Démonstration. Considérons l'action de $\mathrm{GL}(2, \mathbb{F}_5)$ sur les six droites du plan $(\mathbb{F}_5)^2$. Cette action est transitive. Elle devient fidèle après avoir quotienté par le sous-groupe des homothéties qui est d'ordre 4. Autrement dit cette action induit un morphisme injectif de $\mathrm{PGL}(2, \mathbb{F}_5)$ dans $\mathcal{S}_6$; l'image H de ce morphisme agit transitivement sur $\{1, 2, 3, 4, 5, 6\}$. L'ordre de $\mathrm{GL}(2, \mathbb{F}_5)$ est $24 \cdot 20 = 5! \cdot 4$. Par conséquent

$$|\mathrm{H}| = |\mathrm{PGL}(2, \mathbb{F}_5)| = 5!$$

Ainsi H est un sous-groupe d'indice 6 dans $\mathcal{S}_6$. □

7. La simplicité de $\mathcal{S}_n$

***Théorème* 7.1.** — *Le groupe* $\mathcal{A}_n$ *est simple dès que* $n \geq 5$.

Nous allons donner deux démonstrations de ce résultat.

7.0.1. *Le groupe* $\mathcal{A}_n$ *est simple dès que* $n \geq 5$, *version* 1.

***Corollaire* 7.2.** — *Dès que* $n \geq 5$, *on a* $D(\mathcal{A}_n) = \mathcal{A}_n$.
Dès que $n \geq 2$, *on a* $D(\mathcal{S}_n) = \mathcal{A}_n$.

Remarque 7.1. Le Corollaire est une conséquence évidente du Théorème 7.1 mais il peut se montrer directement. Donnons quelques détails. On a les inclusions suivantes :

$$D(\mathcal{A}_n) \subset D(\mathcal{S}_n) \subset \mathcal{A}_n$$

***Lemme* 7.3.** — *Soit* $n \geq 5$.

(1) *Le groupe $\mathcal{A}_n$ est $(n-2)$ fois transitif sur $\{1, 2, \ldots, n\}$; autrement dit si $a_1, a_2, \ldots, a_{n-2}$ sont des éléments distincts de $\{1, 2, \ldots, n\}$, si $b_1, b_2, \ldots, b_{n-2}$ sont des éléments distincts de $\{1, 2, \ldots, n\}$, alors il existe $\sigma \in \mathcal{A}_n$ tel que $\sigma(a_i) = b_i$.*

(2) *Les 3-cycles sont conjugués dans $\mathcal{A}_n$.*

Démonstration. (1) Nous écrivons

$$\{1, 2, \ldots, n\} = \{a_1, a_2, \ldots, a_{n-2}, a_{n-1}, a_n\} = \{b_1, b_2, \ldots, b_{n-2}, b_{n-1}, b_n\}$$

et considérons $\rho \in \mathcal{S}_n$ telle que $\rho(a_i) = b_i$ pour tout $i = 1, \ldots, n$. Si σ est paire, alors $\sigma = \rho$ convient. Si σ est impaire, alors $\rho = \sigma(a_{n-1}\ a_n)$ convient.

(2) Soient $\sigma = (a_1\ a_2\ a_3)$ et $\tau = (b_1\ b_2\ b_3)$ deux 3-cycles dans $\mathcal{S}_n$. Comme d'après ce qui précède $\mathcal{A}_n$ est $(n-2)$ transitif il existe g dans $\mathcal{A}_n$ tel que $g(a_i) = b_i$ pour tout $i = 1, 2, 3$. De plus $\tau = g\sigma g^{-1}$.

□

Lemme 7.4. — *Dès que $n \geq 3$ les 3-cycles engendrent $\mathcal{A}_n$.*

Démonstration. Puisque le groupe $\mathcal{S}_n$ est engendré par les produits de transpositions, le groupe $\mathcal{A}_n$ est engendré par les produits pairs de transpositions et on a

$$(a\ b)(b\ c) = (a\ b\ c)$$

$$(a\ b)(a\ c) = (a\ c\ b)$$

(notons au passage que tous les 3-cycles sont dans $\mathcal{A}_n$) et

$$(a\ b)(c\ d) = (a\ b)(a\ c)(a\ c)(c\ d) = (a\ c\ b)(a\ c\ d)$$

□

Il suffit donc de montrer que tout 3-cycle est dans $\mathcal{A}_n$ un commutateur. Soit $\sigma = (a\ b\ c)$ un 3-cycle, $\sigma^2 = (a\ c\ b)$ en est un autre donc σ et σ^2 sont conjugués dans $\mathcal{A}_n$ (Lemme 7.3) : il existe τ dans $\mathcal{A}_n$ tel que $\sigma^2 = \tau^{-1}\sigma\tau$ d'où $\sigma = \sigma^{-1}\tau^{-1}\sigma\tau = [\sigma^{-1}, \tau^{-1}]$.

On montre de manière "analogue" que $D(\mathcal{S}_n) = \mathcal{A}_n$ dès que $n \geq 2$.

Remarques 7.2. Soit H un sous-groupe distingué de G.

— La classe de conjugaison d'un élément $h \in$ H est contenue dans H, c'est-à-dire

$$\forall\, g \in \mathrm{G} \qquad ghg^{-1} \in \mathrm{H}$$

— Si $h \in$ H et $g \in$ G le commutateur $ghg^{-1}h^{-1} = (ghg^{-1})h^{-1}$ appartient à H et n'est pas, en général, un conjugué de h ; on obtient donc une nouvelle classe de conjugaison, le but étant de montrer qu'un système générateur de G est tout entier dans H.

Démonstration du théorème 7.1 pour $n = 5$. Le groupe $\mathcal{A}_5$ a 60 éléments :

— le neutre ;
— 15 éléments d'ordre 2 (produit de deux transpositions disjointes) ;
— 20 éléments d'ordre 3 (3-cycles) ;
— 24 éléments d'ordre 5 (5-cycles).

Les 3-cycles sont conjugués dans $\mathcal{A}_5$ (Lemme 7.3). Les éléments d'ordre 2 le sont aussi : si $\tau = (a\ b)(c\ d)(e)$ et $\tau' = (a'\ b')(c'\ d')(e')$ on définit $\sigma \in \mathcal{A}_n$ tel que $\sigma(a) = a'$, $\sigma(b) = b'$ et $\sigma(e) = e'$ alors $\sigma\tau\sigma^{-1} = \tau'$.

Soit H un sous-groupe distingué non trivial de $\mathcal{A}_5$. Si H contient un élément d'ordre 3 (respectivement 2), alors il les contient tous d'après ce qui précède. Si H contient un élément d'ordre 5, il contient le 5-SYLOW engendré par cet élément donc tous les 5-sous-groupes de SYLOW puisqu'ils sont conjugués ainsi tous les éléments d'ordre 5.

Le groupe H ne peut pas contenir un seul des trois types d'éléments précédents en plus du neutre car ni $25 = 24 + 1$, ni $21 = 20 + 1$, ni $16 = 15 + 1$ ne divisent 60 (rappel : $|\mathrm{H}|$ divise $|\mathcal{A}_5| = 60$). Par conséquent H contient au moins deux des trois types d'où

$$|\mathrm{H}| \geq 15 + 20 + 1 = 36.$$

Comme $|\mathrm{H}|$ divise $|\mathcal{A}_5| = 60$ on obtient $|\mathrm{H}| = 60$ et $\mathrm{H} = \mathcal{A}_5$. □

Remarque 7.3. Les 25 éléments d'ordre 5 de $\mathcal{A}_5$ ne sont pas conjugués dans $\mathcal{A}_5$ sinon ils formeraient une orbite et 24 diviserait 60. Nous pouvons cependant éviter le recours à SYLOW dans la démonstration précédente en remarquant que si a et b sont d'ordre 5, alors b est conjugué à a ou a^2 dans $\mathcal{S}_5$.

Démonstration du théorème 7.1 pour $n > 5$. Posons $E = \{1, 2, \ldots, n\}$. Soit $\{\mathrm{id}\} \neq \mathrm{H} \triangleleft \mathcal{A}_n$. Soit $\sigma \in \mathrm{H} \smallsetminus \{\mathrm{id}\}$. On se ramène au cas $n = 5$; pour ce faire on va fabriquer à partir de σ un élément non trivial de H qui n'agit que sur un ensemble à 5 éléments donc qui a $n - 5$ points fixes.

Comme $\sigma \neq \mathrm{id}$ il existe $a \in E$ tel que $b = \sigma(a) \neq a$. Soit $c \in E$ tel que $c \notin \{a, b, \sigma(b)\}$ (un tel c existe puisque $n \geq 5$). Soit τ le 3-cycle donné par $\tau = (a\ c\ b)$. Alors $\tau^{-1} = (a\ b\ c)$. Considérons ρ défini par

$$\rho = \tau\sigma\tau^{-1}\sigma^{-1} = (a\ c\ b)(\sigma(a)\ \sigma(b)\ \sigma(c)).$$

Comme $b = \sigma(a)$ l'ensemble $F = \{a, b, \sigma(a), \sigma(b), \sigma(c)\}$ a au plus 5 éléments et $\rho(F) = F$, $\rho_{|E \smallsetminus F} = \mathrm{id}_{|E \smallsetminus F}$. Quitte à ajouter au besoin des éléments à F on peut supposer que $|F| = 5$. Notons que $\rho(b) = \tau(\sigma(b)) \neq b$ (en effet $\sigma(b) \neq \tau^{-1}(b) = c$) donc $\rho \neq \mathrm{id}$.

Considérons $\mathcal{A}(F)$ l'ensemble des permutations paires de F. Il satisfait les deux propriétés suivantes

— $\mathcal{A}(F)$ est isomorphe à $\mathcal{A}_5$;
— $\mathcal{A}(F)$ se plonge dans $\mathcal{A}_n$ via $u \mapsto \overline{u}$ où

$$\begin{cases} \overline{u}_{|F} = u \\ \overline{u}_{|E \smallsetminus F} = \mathrm{id}_{|E \smallsetminus F} \end{cases}$$

Soit $\mathrm{H}_0 = \{u \in \mathcal{A}(F) \mid \overline{u} \in \mathrm{H}\} = \mathrm{H} \cap \mathcal{A}(F)$. Alors
— $\mathrm{H}_0 \triangleleft \mathcal{A}(F)$;
— $\rho_{|F} \in \mathrm{H}_0$;
— $\rho_{|F} \neq \mathrm{id}_F$.

Comme $\mathcal{A}(F) \not\simeq \mathcal{A}_5$ est simple on a $\mathrm{H}_0 = \mathcal{A}(F)$. Soit alors $u \in \mathcal{A}(F)$ un 3-cycle. Il appartient à H_0 donc $\overline{u}$ qui est encore un 3-cycle appartient à H. Mais comme les 3-cycles sont tous conjugués dans $\mathcal{A}_n$ (Lemme 7.3) ils appartiennent tous à H et puisqu'ils engendrent $\mathcal{A}_n$ (Lemme 7.4) on a $\mathrm{H} = \mathcal{A}_n$. □

Remarque 7.4. Le groupe $\mathcal{A}_4$ n'est pas simple car

$$\big\{\mathrm{id},\ (1\ 2)(3\ 4),\ (1\ 3)(2\ 4),\ (1\ 4)(2\ 3)\big\}$$

est un sous-groupe distingué de $\mathcal{A}_4$ d'ordre 4.

***Corollaire* 7.5.** — *Dès que $n \geq 5$ les sous-groupes distingués de $\mathcal{S}_n$ sont* $\{\mathrm{id}\}$, *$\mathcal{A}_n$ et $\mathcal{S}_n$.*

Avant de démontrer ce résultat donnons quelques résultats intermédiaires.

***Lemme* 7.6.** — *Soit $n \geq 3$. Soient a, b dans $\{1, 2, \ldots, n\}$ et $\sigma \in \mathcal{S}_n$. Alors*

$$\sigma(a\ b)\sigma^{-1} = (\sigma(a)\ \sigma(b)).$$

***Lemme* 7.7.** — *Soit $n \geq 3$. Le centre de $\mathcal{S}_n$ est réduit à* $\{\mathrm{id}\}$.

Démonstration. Soit σ un élément du centre de $\mathcal{S}_n$. En particulier $\sigma(1\ 2) = (1\ 2)\sigma$, *i.e.* $\sigma(1\ 2)\sigma^{-1} = (1\ 2)$. Par suite (Lemme 7.6)

$$(\sigma(1)\ \sigma(2)) = (1\ 2).$$

Ainsi nécessairement $\sigma(1) = 1$ ou $\sigma(1) = 2$. De même $\sigma(1\ 3) = (1\ 3)\sigma$ et donc

$$(\sigma(1)\ \sigma(3)) = (1\ 3).$$

Il en résulte que $\sigma(1) = 1$. Ce qu'on a fait avec 1 peut être fait avec n'importe quel entier compris entre 2 et n. Il en résulte que $\sigma = \mathrm{id}$.

Réciproquement id commute avec toutes les permutations. □

Démonstration du Corollaire 7.5. Soit $\mathrm{H} \lhd \mathcal{S}_n$. Alors $\mathrm{H} \cap \mathcal{A}_n \lhd \mathcal{A}_n$ donc $\mathrm{H} \cap \mathcal{A}_n \in \big\{\mathrm{id}, \mathcal{A}_n\big\}$.

Si $\mathrm{H} \cap \mathcal{A}_n = \mathcal{A}_n$, alors $\mathrm{H} = \mathcal{A}_n$ ou $\mathrm{H} = \mathcal{S}_n$.

Si $\mathrm{H} \cap \mathcal{A}_n = \{\mathrm{id}\}$, alors la signature ε induit un isomorphisme de H sur $\varepsilon(\mathrm{H}) \subset \{1, -1\}$. Par suite $|\mathrm{H}| \leq 2$. Si $|\mathrm{H}| = 2$, alors $\mathrm{H} = \{\mathrm{id}, \sigma\}$. Mais si $\tau \in \mathcal{S}_n$ comme $\tau\sigma\tau^{-1}$ appartient à H et $\tau\sigma\tau^{-1} \neq \mathrm{id}$ on a $\tau\sigma\tau^{-1} = \sigma$. Autrement dit σ appartient au centre de $\mathcal{S}_n$ d'où $\sigma = \mathrm{id}$ (Lemme 7.7) : contradiction. Il en résulte que $\mathrm{H} = \{\mathrm{id}\}$. □

7.0.2. *Le groupe $\mathcal{A}_n$ est simple dès que $n \geq 5$, version* 2.

***Théorème* 7.8.** — *Le groupe $\mathcal{A}_5$ est simple.*

***Lemme* 7.9.** — *Tout p-*Sylow *distingué d'un groupe d'ordre fini est caractéristique.*

Démonstration. Soit G un groupe d'ordre fini. Soit H un p-Sylow de G qui est distingué. Soit φ un automorphisme de G. L'image de H par φ est un sous-groupe de même ordre que H, *i.e.* $\varphi(\mathrm{H})$ est un p-Sylow de G. Mais H est l'unique p-Sylow de G car H est distingué. Par conséquent $\varphi(\mathrm{H}) = \mathrm{H}$. □

***Lemme* 7.10.** — *Tout groupe d'ordre* 15 *est cyclique.*

Démonstration. Soit H un groupe d'ordre 15. Il a exactement un sous-groupe d'ordre 5 et un sous-groupe d'ordre 3. Ces deux sous-groupes sont distingués dans H. Par suite $\mathrm{H} \simeq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \simeq \mathbb{Z}/15\mathbb{Z}$ et est donc cyclique. □

***Lemme* 7.11.** — *Tout groupe d'ordre* 30 *contient un sous-groupe distingué d'ordre* 15.

Démonstration. Soit G un groupe d'ordre 30. Remarquons tout d'abord que tout sous-groupe d'ordre 15 de G est distingué dans G car il est d'indice 2 dans G.

Il suffit donc de démontrer l'existence d'un sous-groupe d'ordre 15 dans le groupe G.

— Supposons que G contienne plus d'un seul 5-Sylow, *i.e.* $n_5 > 1$. Puisque

$$n_5 \equiv 1 \pmod 5 \qquad\qquad n_5 \mid 6$$

on a $n_5 = 6$. Ainsi on a 6×4 éléments d'ordre 5, ce qui en ajoutant e fait 25 éléments de G. Il y a donc exactement un seul 3-Sylow que nous noterons K (sinon il y en aurait 10 donc 20 éléments d'ordre 3 soit 45 éléments au moins dans G). En particulier K est distingué dans G. Si H est l'un des sous-groupes d'ordre 5, $\mathrm{K} \cap \mathrm{H} = \{e\}$ et KH est un sous-groupe d'ordre 15 de G.

— Supposons que G contienne un seul 5-Sylow H ; il est alors distingué dans G. Si K est l'un des sous-groupes d'ordre 3 de G (il y en a au moins un) $K \cap \mathrm{H} = \{e\}$ et KH est un sous-groupe d'ordre 15 dans le groupe G.

□

***Lemme* 7.12.** — *Tout groupe d'ordre* 30 *ne contient qu'un seul* 5-*Sylow* (*d'ordre* 5).

Démonstration. Dans la démonstration du Lemme 7.11 nous avons vu d'une part que tout groupe G d'ordre 30 contient un sous-groupe K d'ordre 3 et un sous-groupe H d'ordre 5 et d'autre part que K ou H est distingué dans G.

Les groupes K et H sont distingués dans KH et sont donc caract éristiques dans le groupe cyclique KH (Lemme 7.9) qui est distingué dans G. Donc en fait K et H sont distingués dans G et G a un unique 5-Sylow. □

***Lemme* 7.13.** — *Tout groupe d'ordre* 20 *contient un seul sous-groupe d'ordre* 5.

Démonstration. Soit G un groupe d'ordre $20 = 4 \times 5$. Le groupe G contient un sous-groupe distingué d'ordre 5 : d'après les théorèmes de Sylow

$$n_5 \equiv 1 \bmod 5 \qquad\qquad n_5 \mid 4$$

d'où $n_5 = 1$. □

***Lemme* 7.14.** — *Tout groupe d'ordre* 12 *contient un sous-groupe caractéristique.*

Démonstration. Soit G un groupe d'ordre 12. Intéressons-nous aux 3-Sylow de G. Les théorèmes de Sylow assurent que

$$n_3 \equiv 1 \bmod 3 \qquad\qquad n_3 \mid 4$$

Il en résulte que $n_3 = 1$ ou $n_3 = 4$.

— Si $n_3 = 1$, alors ce sous-groupe est un sous-groupe caractéristique d'ordre 3 (Lemme 7.9).

— Si $n_3 = 4$, on dénombre $4 \times 2 = 8$ éléments d'ordre 3 ; en ajoutant le neutre on compte donc 9 éléments. Considérons maintenant les 2-Sylow de G. D'après les théorèmes de Sylow on a

$$n_2 \equiv 1 \bmod 2 \qquad\qquad n_2 \mid 3$$

Ainsi n_2 appartient à $\{1, 3\}$. Si $n_2 = 3$, on a trois sous-groupes d'ordre 4, soit trop d'éléments. Ainsi $n_2 = 1$, l'unique 2-Sylow est distingué et donc caractéristique (Lemme 7.10).

□

***Lemme* 7.15.** — *Tout groupe d'ordre* 6 *contient un sous-groupe caractéristique.*

Démonstration. Soit G un groupe d'ordre $6 = 2 \times 3$. Considérons ces 3-Sylow. Les théorèmes de Sylow assurent que

$$n_3 \equiv 1 \bmod 3 \qquad\qquad n_3 \mid 2$$

autrement dit que $n_3 = 1$. Ainsi G compte un unique 3-Sylow qui est donc distingué dans G et le Lemme 7.10 permet de conclure. □

***Lemme* 7.16.** — *Tout groupe d'ordre* 60 *qui contient plus qu'un seul* 5-*Sylow est simple.*

Démonstration. Soit G un groupe d'ordre 60. Supposons que $n_5 > 1$. D'après les théorèmes de Sylow

$$n_5 \equiv 1 \bmod 5 \qquad\qquad n_5 \mid 12$$

d'où $n_5 = 6$.

Raisonnons par l'absurde : supposons que G ne soit pas simple. Soit H un sous-groupe distingué propre de G.

Si |H| est divisible par 5 alors H contient au moins un 5-Sylow de G. Mais H est distingué et les 5-Sylow se déduisent les uns des autres par conjugaison ; ainsi H contient tous les 5-Sylow de G. On en d'éduit que H contient déjà 6×4 éléments d'ordre 5. Par ailleurs |H| divise 60 donc $|\mathrm{H}| = 30$ (rappelons que comme H est un sous-groupe propre de G, on a $|\mathrm{H}| < 60$. Mais dans ce cas H ne contient qu'un seul sous-groupe d'ordre 5 : contradiction avec le fait qu'il en contient 6. Par suite |H| n'est pas divisible par 5.

Si |H| appartient à {6, 12}, alors il existe un sous-groupe caractéristique de H d'ordre 2, 3 ou 4. Ce sous-groupe caractéristique de H, qui est lui-même distingué dans G, est distingué dans G. Nous pouvons donc maintenant supposer que H est d'ordre 2, 3 ou 4.

Dans ce cas G/H est d'ordre 30, 20 ou 15. Dans ces trois cas G/H contient un sous-groupe distingué d'ordre 5. Considérons la surjection canonique $\pi\colon \mathrm{G} \to \mathrm{G}/\mathrm{H}$. Le sous-groupe $\pi^{-1}(\mathrm{K})$ contient H et est distingué dans G. Or $\pi^{-1}(\mathrm{K})/\mathrm{H}$ est isomorphe à $K = \pi(\pi^{-1}(\mathrm{K}))$ donc $|\pi^{-1}(\mathrm{K})|$ est divisible par 5 : contradiction. □

Démonstration du Théorème 7.8. Le groupe $\mathcal{A}_5$ est d'ordre 60 et contient au moins deux 5-Sylow distincts engendrés par les 5-cycles (1 2 3 4 5) et (1 3 2 4 5). Le Lemme 7.16 assure donc que $\mathcal{A}_5$ est simple. □

***Lemme* 7.17.** — *Soit $n \geq 6$. Supposons que $\mathcal{A}_{n-1}$ soit simple. Soit* H *un sous-groupe distingué propre de $\mathcal{A}_n$. Il existe $\tau \in \mathrm{H}$ distincte de l'identité qui a au moins un point fixe.*

Démonstration. Supposons que $\mathrm{H} \neq \{\mathrm{id}\}$.

Remarque 7.5. Supposons que pour tout $\tau \in \mathrm{H} \smallsetminus \{\mathrm{id}\}$ et pour tout i on ait $\tau(i) \neq i$. Alors si τ_1 et τ_2 sont deux éléments de H qui coïncident en un point i, ils sont égaux. En effet si $\tau_1(i) = \tau_2(i)$ alors $\tau_2^{-1}\tau_1(i) = i$. De plus $\tau_2^{-1}\tau_1$ appartient à H donc par hypothèse $\tau_2^{-1}\tau_1 = \mathrm{id}$, *i.e.* $\tau_1 = \tau_2$.

Supposons que pour tout $\tau \in \mathrm{H} \setminus \{\mathrm{id}\}$ et pour tout i on ait $\tau(i) \neq i$. Considérons un élément τ de H. Si la décomposition ed τ en produit de cycles disjoints contient un cycle d'ordre ≥ 3 alors on peut écrire

$$\tau = (a_1\ a_2\ a_3\ \ldots)(b_1\ b_2\ \ldots)\ldots$$

Puisque $n \geq 6$ il existe σ dans $\mathcal{A}_n$ tel que $\sigma(a_1) = a_1$, $\sigma(a_2) = a_2$ et $\sigma(a_3) \neq a_3$. Alors

$$\sigma\tau\sigma^{-1} = (a_1\ a_2\ \sigma(a_3)\ \ldots)(\sigma(b_1)\ \sigma(b_2)\ \ldots)\ldots$$

Ainsi $\sigma\tau\sigma^{-1}(a_1) = \tau(a_1) = a_2$. À noter que $\sigma\tau\sigma^{-1}$ appartient à H car H est distingué. La Remarque 7.5 assure donc que $\sigma\tau\sigma^{-1} = \tau$. Mais $\sigma\tau\sigma^{-1}(a_2) = \sigma(a_3) \neq a_3$ et $a_3 = \tau(a_2)$ donc $\sigma\tau\sigma^{-1}(a_2) \neq \tau(a_2)$: contradiction. Ainsi aucun élément de H ne contient dans sa décomposition en cycles disjoints des cycles d'ordre ≥ 3. Les éléments de H sont donc des produits de transpositions disjointes.

Considérons un élément τ de H. D'après ce qui précède τ est un produit de transpositions disjointes. À noter que si τ contient une double transposition alors elle laisse fixe un élément ce qui est contraire à l'hypothèse. Ainsi τ s'écrit

$$\tau = (a_1\ a_2)(a_3\ a_4)(a_5\ a_6)\ldots$$

Soit $\sigma = (a_1\ a_2)(a_3\ a_5)$. Alors on a

$$\sigma\tau\sigma^{-1} = (a_1\ a_2)(a_5\ a_4)(a_3\ a_6)\ldots$$

D'une part $\sigma\tau\sigma^{-1}(a_2) = \tau(a_2)$ donc $\sigma\tau\sigma^{-1} = \tau$ (Remarque 7.5). D'autre part $\sigma\tau\sigma^{-1}(a_3) = \tau(a_3)$: contradiction. Il existe donc un élément τ dans $\mathrm{H} \setminus \{\mathrm{id}\}$ pour lequel $\tau(i) = i$ pour un certain $1 \leq i \leq n$. □

***Lemme* 7.18.** — *Soit $n \geq 6$. Supposons que $\mathcal{A}_{n-1}$ soit simple. Soit* H *un sous-groupe distingué propre de $\mathcal{A}_n$. Pour tout $1 \leq j \leq n$ le sous-groupe $\mathrm{G}_j = \mathrm{Stab}_{\mathcal{A}_n}(\{j\})$ est inclus dans* H.

Démonstration. Soit τ un élément de $\mathrm{H} \setminus \{\mathrm{id}\}$ pour lequel il existe $A \leq i \leq n$ tel que $\tau(i) \neq i$ (l'existence d'un tel τ est assurée par le Lemme 7.17). Ainsi τ appartient à $\mathrm{G}_i \cap \mathrm{H}$ qui est un sous-groupe distingué de G_i. Or G_i est isomorphe à $\mathcal{A}_{n-1}$ donc l'hypothèse de récurrence implique que G_i est simple. Or τ est non trivial donc $\mathrm{G}_i \cap \mathrm{H} = \mathrm{G}_i$, c'est-à-dire G_i est inclus dans H.

Par ailleurs pour tout σ dans $\mathcal{S}_n$ on a $\sigma\mathrm{G}_i\sigma^{-1} = G_{\sigma(i)}$. De plus $\mathrm{G}_i \subset \mathrm{H}$ donc $\sigma\mathrm{G}_i\sigma^{-1} \subset \sigma\mathrm{H}\sigma^{-1} = \mathrm{H}$. Il en résulte que pour tout $1 \leq j \leq n$ on a l'inclustion $\mathrm{G}_j \subset \mathrm{H}$. □

***Lemme* 7.19.** — *Soit $n \geq 6$. Supposons que $\mathcal{A}_{n-1}$ soit simple. Soit* H *un sous-groupe distingué propre de $\mathcal{A}_n$ non trivial. Alors $\mathcal{A}_n = \mathrm{H}$.*

Démonstration. Considérons un élément g de $\mathcal{A}_n$. C'est un produit d'un nombre pair de transpositions, il s'écrit donc

$$g = t_1 t_2 \ldots t_k$$

où chaque t_j est un produit de deux transpositions. Le support de chaque t_j contient au plus quatre éléments donc t_j appartient à G_i pour un i extérieur à ce support. Par suite $\mathcal{A}_n \subset \mathrm{G}_1\mathrm{G}_2\ldots\mathrm{G}_n$. Mais $\mathrm{G}_1\mathrm{G}_2\ldots\mathrm{G}_n \subset \mathrm{H}$ (Lemme 7.18). Il en résulte que $\mathcal{A}_n \subset \mathrm{H}$. Or $H \subset \mathcal{A}_n$ donc $\mathcal{A}_n = \mathrm{H}$. □

Démonstration du Théorème 7.1. Le groupe $\mathcal{A}_5$ est simple (Théorème 7.8). Pour $n \geq 6$ tout sous-groupe distingué de $\mathcal{A}_n$ différent de $\{\mathrm{id}\}$ est égal à $\mathcal{A}_n$ (Lemme 7.19). □

8. Décomposition d'une permutation en transpositions

***Théorème* 8.1.** — *Toute permutation $s \in \mathcal{S}_n$ est un produit de transpositions.*

***Proposition* 8.2.** — *Toute permutation $s \in \mathcal{S}_n$ s'écrit de manière unique (modulo l'ordre des termes) comme un produit de cycles disjoints*

$$s = c_1 c_2 \dots c_p.$$

L'ordre de s est le ppcm des ordres de c_1, c_2, …, c_p.

***Proposition* 8.3.** — *Soient* G *un groupe et $g \in \mathrm{G}$. L'application $f\colon k \mapsto a^k$ est un morphisme de $\mathbb{Z}$ sur le sous-groupe $\langle a\rangle$ engendré par a.*

Si f est injectif, alors $\langle a\rangle$ est isomorphe à $\mathbb{Z}$.

Si f n'est pas injectif, alors $\langle a\rangle$ est isomorphe à $\mathbb{Z}/n\mathbb{Z}$ où $n \in \mathbb{N}^*$ est le plus petit entier non nul tel que $a^n = e$. Dans ce cas, les entiers k tels que $a^k = e$ sont les multiples de n et $\langle a\rangle = \{e, a, \dots, a^{n-1}\}$.

***Proposition* 8.4.** — *Les sous-groupes de $(\mathbb{Z}, +)$ sont les sous-ensembles $n\mathbb{Z}$ où $n \in \mathbb{N}$.*

Démonstration. Notons que $0 \in n\mathbb{Z}$. Soient g, g' dans $n\mathbb{Z}$, *i.e.* $g = nk$ et $g' = nk'$ avec k et k dans $\mathbb{Z}$. Ainsi $g - g' = n(k - k')$ appartient à $n\mathbb{Z}$. Il en résulte que $n\mathbb{Z}$ est un sous-groupe de $\mathbb{Z}$.

Réciproquement soit G un sous-groupe de $\mathbb{Z}$. Si G est réduit à $\{0\}$, alors $\mathrm{G} = 0\mathbb{Z}$. Supposons désormais que $\mathrm{G} \neq \{0\}$; alors il existe $g \neq 0$ dans G. Remarquons que $-g \in \mathrm{G}$ donc $\mathrm{G} \cap \mathbb{N}^* \neq \emptyset$. Soit n le plus petit élément de $\mathrm{G} \cap \mathbb{N}^*$. Pour tout $k \in \mathbb{N}$ on a

$$nk = \underbrace{n + n + \ldots + n}_{k \text{ fois}} \in G$$

et $n(-k) = -(nk) \in \mathrm{G}$. Ainsi $n\mathbb{Z} \subset \mathrm{G}$. Soit $g \in \mathrm{G}$ positif. La division de g par n conduit à $g = nq + r$ avec $0 \leq r < n$ et $q \in \mathbb{N}$. Il en résulte que

$$r = g - \underbrace{n + n + \ldots + n}_{q \text{ fois}}$$

appartient à G. Supposons r non nul : alors n n'est pas le plus petit élément de $\mathrm{G} \cap \mathbb{N}$: contradiction. Par suite $r = 0$ et $g = nq \in n\mathbb{Z}$. Si $g \in \mathrm{G}$ est négatif, alors $-g \in \mathrm{G}$ est positif et appartient donc à $n\mathbb{Z}$. Il s'en suit que $\mathrm{G} \subset n\mathbb{Z}$ et donc $\mathrm{G} = n\mathbb{Z}$. □

Démonstration de la Proposition 8.3. L'application $f_0\colon \mathbb{N} \to \langle a\rangle$, $k \mapsto a^k$ vérifie

$$\forall\, k \in \mathbb{N} \qquad \forall\, k' \in \mathbb{N} \qquad f_0(k + k') = a^{k+k'} = a^k a^{k'} = f_0(k) f_0(k').$$

La propriété universelle du symétrisé $\mathbb{Z}$ de $\mathbb{N}$ permet de prolonger f_0 en un morphisme f de $\mathbb{Z}$ dans $\langle a\rangle$. Pour $k = -|k| < 0$, on a $f(-|k|) = f(|k|)^{-1} = (a^{|k|})^{-1} = a^k$. Par suite $\mathrm{im} f = \left\{a^k \mid k \in \mathbb{Z}\right\} = \langle a\rangle$.

D'après la Proposition 8.4 il existe $n \in \mathbb{N}$ tel que $\ker f = n\mathbb{Z}$. Si $n = 0$, alors f est injective ; c'est un isomorphisme f de $\mathbb{Z}$ dans $\langle a\rangle$. Si n est non nul, le théorème

d'isomorphisme assure l'existence d'un isomorphisme $\overline{f}$ entre $\mathbb{Z}/\ker f = \mathbb{Z}/n\mathbb{Z}$ et $\langle a\rangle$. Par définition le noyau de f est l'ensemble des $k \in \mathbb{Z}$ tels que $a^k = e$, c'est-à-dire l'ensemble $n\mathbb{Z}$ des multiples de n. Puisque $0, 1, \ldots, n-1$ sont des représentants des n classes modulo $n\mathbb{Z}$ leurs images $e = a^0, a, a^2, \ldots, a^{n-1}$ par $\overline{f}$ sont les éléments de $\mathrm{Im}(\overline{f}) = \mathrm{Im}(f) = \langle a\rangle$. □

***Proposition* 8.5.** — *Soit E un ensemble. Soit* G *un groupe. Considérons une action à gauche de* G *sur E.*

(i) La relation

$$x\mathcal{R}y \iff (\exists\, g \in \mathrm{G} \quad g \cdot x = y)$$

est une relation d'équivalence sur E.

(ii) Soit $x \in E$; alors

$$\mathrm{G}_x = \big\{g \in \mathrm{G} \,|\, g \cdot x = x\big\}$$

est un sous-groupe de G*.*

(iii) Soit $x \in E$, soit $g_0 \in \mathrm{G}$ et soit $y = g_0 \cdot x$. Alors

$$\mathrm{G}_y = g_0\mathrm{G}_x g_0^{-1} \qquad\qquad \big\{g \in \mathrm{G} \,|\, g \cdot x = y\big\} = g_0\mathrm{G}_x$$

Démonstration. (i) Pour tout $x \in E$ on a $x\mathcal{R}x$ car $e \cdot x = x$; la relation $\mathcal{R}$ est donc réflexive. Si $x\mathcal{R}y$ alors il existe $g \in \mathrm{G}$ tel que $g \cdot x = y$ d'où $x = g^{-1} \cdot y$, *i.e.* $y\mathcal{R}x$. Ainsi $\mathcal{R}$ est symétrique. Enfin elle est transitive car

$$(g \cdot x = y \text{ et } g' \cdot y = z) \Rightarrow g'g \cdot x = z$$

(ii) Direct.

(iii) Pour tout g dans G on a d'une part

$$\begin{aligned} g \in \mathrm{G}_y &\iff g \cdot (g_0 \cdot x) = g_0 \cdot x \\ &\iff (g_0^{-1} g g_0) \cdot x = x \\ &\iff g_0^{-1} g g_0 \in \mathrm{G}_x \\ &\iff g \in g_0 \mathrm{G}_x g_0^{-1} \end{aligned}$$

d'autre part

$$\begin{aligned} g \in \big\{g \in \mathrm{G} \,|\, g \cdot x = y\big\} &\iff g \cdot x = y \\ &\iff g \cdot x = g_0 \cdot x \\ &\iff g_0^{-1} g \cdot x = x \\ &\iff g_0^{-1} g \in \mathrm{G}_x \\ &\iff g \in g_0 \mathrm{G}_x \end{aligned}$$

□

Démonstration de la Proposition 8.2. La Proposition 8.4 assure que $k \mapsto s^k$ est un morphisme du groupe additif $\mathbb{Z}$ dans $\mathcal{S}_n$. C'est une action de $\mathbb{Z}$ sur l'ensemble $E = \{1, 2, \ldots, n\}$. Soient $\mathcal{O}_1, \mathcal{O}_2, \ldots, \mathcal{O}_p$ les orbites qui ne sont pas réduites à un point, *i.e.* les orbites des éléments du support de s. Soit i_1 dans $\mathcal{O}_1$. Son stabilisateur est un sous-groupe de $\mathbb{Z}$ donc de la forme $k\mathbb{Z}$ (Proposition 8.4). Les éléments de $\mathcal{O}_1$ sont

$$i_1,\ i_2 = s(i_1),\ i_3 = s(i_2) = s^2(i_1),\ \ldots,\ i_k = s(i_{k-1}) = s^{k-1}(i_1).$$

D'après la Proposition 8.5 (iii) ces éléments sont bijectivement associés aux classes de $\mathbb{Z}$ modulo le stabilisateur $k\mathbb{Z}$ et sont donc distincts. On a $s^k(i_1) = i_1$. L'action de s sur l'orbite $\mathcal{O}_1$ est la même que celle du cycle $c_1 = (i_1\ i_2\ \ldots\ i_k)$. De même il existe des cycles c_2, c_3, …, c_p ayant pour supports les orbites $\mathcal{O}_2$, $\mathcal{O}_3$, …, $\mathcal{O}_p$ ayant la même action que s sur ces orbites. Les cycles c_1, c_2, …, c_p commutent car ils sont disjoints et $(c_1c_2\ldots c_p)(i) = s(i)$ pour tout point i du support $\bigcup_{m=1}^{p} \mathcal{O}_m$ de s. Les autres éléments de E sont fixes par s et $c_1c_2\ldots c_p$ donc $s = c_1c_2\ldots c_p$.

Montrons l'unicité (modulo l'ordre des cycles) de l'expression $s = c_1c_2\ldots c_p$ par récurrence sur p. Si $p = 0$, *i.e.* si $s = \mathrm{id}$, l'unicité est évidente. Soit $p \geq 1$. Supposons que les permutations pouvant s'exprimer comme produit de moins de p cycles disjoints ont une écriture unique (modulo l'ordre des cycles). Considérons une permutation s qui est le produit de p cycles disjoints :

$$s = c_1c_2\ldots c_p$$

Soit $s = c'_1c'_2\ldots c'_q$ une autre décomposition de s en cycles disjoints. Soit i un élément du support $\mathcal{O}_1$ de c_1. Il appartient au support d'un des cycles c'_j et à un seul. Quitte à réindicer les c'_j on peut supposer que i appartient au support de c'_1. Pour tout r dans $\mathbb{Z}$ on a

$$s^{r(i)} = c_1^{r(i)} = (c'_1)^{r(i)}.$$

Ainsi $c_1 = c'_1$. Par conséquent $c_1c_2\ldots c_p = c'_1c'_2\ldots c'_q$ entraîne $c_2c_3\ldots c_p = c'_2c'_3\ldots c'_q$. D'après l'hypothèse de récurrence on obtient $p = q$ et $\{c_2, c_3, \ldots, c_p\} = \{c'_2, c'_3, \ldots, c'_p\}$.

Comme les cycles commutent on a pour tout entier n

$$s^n = c_1^n c_2^n \ldots c_p^n$$

Les supports des c_i étant disjoints, $s^n = \mathrm{id}$ si et seulement si $(c_1^n, c_2^n, \ldots, c_p^n) = (\mathrm{id}, \mathrm{id}, \ldots, \mathrm{id})$, *i.e.* si et seulement si n est multiple commun des ordres k_1, k_2, …, k_p de c_1, c_2, …, c_p. Le plus petit entier strictement positif n tel que $s^n = \mathrm{id}$ est donc $\mathrm{ppcm}(k_1, k_2, \ldots, k_p)$. □

Démonstration du Théorème 8.1. D'après la Proposition 8.2 il suffit de montrer que tout cycle $(i_1\ i_2\ \ldots\ i_p)$ est un produit de transpositions. Montrons par récurrence sur la longueur p du cycle que

$$(i_1\ i_2\ \ldots\ i_p) = (i_1\ i_2)(i_2\ i_3)\ldots(i_{p-1}\ i_p).$$

La formule est vraie pour $p = 2$.

Supposons que $p > 2$ et que la formule soit vraie pour $p - 1$, *i.e.*

$$(i_1\ i_2\ \ldots\ i_{p-1}) = (i_1\ i_2)(i_2\ i_3)\ldots(i_{p-1}\ i_{p-1});$$

alors

$$(i_1\ i_2)(i_2\ i_3)\ldots(i_{p-1}\ i_p) = (i_1\ i_2\ \ldots\ i_{p-1})(i_{p-1}\ i_p) = (i_1\ i_2\ \ldots\ i_p).$$

□

9. Formule de Wilson

a) Déterminons l'ordre d'un p-Sylow de $\mathcal{S}_p$.

L'ordre de $\mathcal{S}_p$ est $p! = p(p-1)!$. De plus p et $(p-1)!$ sont premiers entre eux. Par suite un p-Sylow de $\mathcal{S}_p$ est d'ordre p.

b) Dénombrons les p-Sylow dans $\mathcal{S}_p$.

Pour déterminer le nombre de p-Sylow de $\mathcal{S}_p$ on cherche combien il y a d'éléments d'ordre p de $\mathcal{S}_p$. Ce sont les p-cycles qui sont conjugués entre eux. Pour calculer leur nombre il suffit de calculer l'ordre du centralisateur C de l'un d'eux, par exemple du p-cycle $\sigma = (1\ 2\ \ldots\ p)$. Si s est une permutation, alors

$$s\sigma s^{-1} = (s(1)\ s(2)\ \ldots\ s(p))$$

Donc $s \in C$ si

$$(\sigma(1)\ \sigma(2)\ \ldots\ \sigma(p)) = (s(1)\ s(2)\ \ldots\ s(p))$$

c'est-à-dire si s est une puissance de la permutation circulaire d'ordre p. L'ordre de C est donc égal à p et il y a $\frac{p!}{p} = (p-1)!$ éléments d'ordre p dans $\mathcal{S}_p$ car $\mathcal{S}_p/C$ est en bijection avec les conjugués de σ.

Ces éléments d'ordre p se répartissent entre $\frac{(p-1)!}{p-1} = (p-2)!$ p-Sylow de $\mathcal{S}_p$ qui contiennent chacun $(p-1)$ éléments d'ordre p.

Autre rédaction possible : un p-Sylow est d'ordre p, p étant premier, un p-Sylow est donc un sous-groupe cyclique d'ordre p. Il y a $(p-1)!$ p-cycles dans $\mathcal{S}_p$ donc $\frac{(p-1)!}{p-1} = (p-2)!$ p-Sylow.

c) Montrons la formule de Wilson :

$$(p-1)! \equiv -1 \bmod p.$$

Notons n_p le nombre de p-Sylow. D'après b) on a $n_p = (p-2)!$. D'après les théorèmes de Sylow $n_p \equiv 1 \bmod p$. Donc $(p-2)! \equiv 1 \bmod p$ et $(p-1)! \equiv p-1 \bmod p$. Mais $p-1 \equiv -1 \bmod p$. Il en résulte que $(p-1)! \equiv -1 \bmod p$.

10. Produit semi-direct

Le groupe symétrique $\mathcal{S}_3$ compte six éléments

$$\text{id}, \quad (1\ 2), \quad (1\ 3), \quad (2\ 3), \quad \sigma = (1\ 2\ 3), \quad \sigma^2 = \sigma^{-1} = (1\ 3\ 2).$$

Il contient un sous-groupe distingué d'ordre 3

$$\langle\sigma\rangle = \{1, \sigma, \sigma^2\} = \mathcal{A}_3$$

isomorphe à $\mathbb{Z}/3\mathbb{Z}$ et on a la suite exacte suivante

$$1 \longrightarrow \mathcal{A}_3 \simeq \mathbb{Z}/3\mathbb{Z} \longrightarrow \mathcal{S}_3 \xrightarrow{\text{sgn}} \mathbb{Z}/2\mathbb{Z} \longrightarrow 1.$$

11. Exercices

Exercice 1

Dans le groupe symétrique $\mathcal{S}_5$, combien y a-t-il de 5-cycles distincts ? de 4-cycles distincts ?

Éléments de réponse 1

L'ensemble des 5-cycles est en bijection avec les 5-uplets (a, b, c, d, e) d'éléments distincts modulo permutation circulaire, c'est-à-dire :

$$(a, b, c, d, e) \sim (b, c, d, e, a) \sim (c, d, e, a, b) \sim (d, e, a, b, c) \sim (e, a, b, c, d)$$

de sorte que chaque classe est constituée de 5 éléments. On obtient alors $\binom{5}{5}(5-1)!$ tels cycles, où $\binom{5}{5}$ est le coefficient binomial.

Pour les 4-cycles le même raisonnement donne $\binom{4}{5}3!$.

Plus généralement le nombre de r-cycles dans $\mathcal{S}_n$ est $\binom{n}{r}(r-1)!$.

Exercice 2

Montrer que le groupe symétrique $\mathcal{S}_3$ est isomorphe à son groupe d'automorphisme $\mathrm{Aut}(\mathcal{S}_3)$.

Éléments de réponse 2

L'application qui à σ fait correspondre l'automorphisme intérieur $\sigma' \mapsto \sigma\sigma'\sigma^{-1}$ est un morphisme injectif de $\mathcal{S}_3$ dans $\mathrm{Aut}(\mathcal{S}_3)$, car le centre de $\mathcal{S}_3$ est trivial.

De plus un élément de $\mathrm{Aut}(\mathcal{S}_3)$ est déterminé par l'image des générateurs $(1\,2)$ et $(1\,3)$. Il y a donc au plus 6 choix possibles (choisir deux parmi les trois éléments d'ordre 2 de $\mathcal{S}_3$), donc en comparant les ordres nous obtenons que le morphisme ci-dessus est en fait un isomorphisme.

Exercice 3 Montrer que tout sous-groupe d'indice n dans $\mathcal{S}_n$ est isomorphe à $\mathcal{S}_{n-1}$.

Éléments de réponse 3 Soit H un sous-groupe d'indice n dans $\mathcal{S}_n$.

Si $n \geq 3$, on vérifie l'énoncé directement.

Si $n = 4$, alors si $\mathrm{H} \not\simeq \mathcal{S}_3$, alors H est cyclique (rappel : si p, q sont des nombres premiers tels que $p < q$ et p ne divise pas $q-1$ alors tout groupe d'ordre pq est cyclique) : contradiction avec le fait que $\mathcal{S}_4$ ne contient pas d'élément d'ordre 6.

Supposons $n \geq 5$. Le groupe $\mathcal{S}_n$, et donc aussi H, opère par translation à gauche sur $E = \mathcal{S}_n/\mathrm{H}$ d'où un homomorphisme

$$\varphi \colon \mathcal{S}_n \to \mathcal{S}_E \simeq \mathcal{S}_n.$$

Puisque $\ker\varphi = \bigcap_{a \in \mathcal{S}_n} a\mathrm{H}a^{-1}$, $\ker\varphi$ est distingué dans $\mathcal{S}_n$ et $\ker\varphi \subset \mathrm{H}$ on a $\ker\varphi = \{\mathrm{id}\}$ (rappel : pour $n \geq 5$ les sous-groupes distingués de $\mathcal{S}_n$ sont $\{\mathrm{id}\}$, $\mathcal{A}_n$ et $\mathcal{S}_n$). Pour des raisons de cardinalité ($|\mathcal{S}_n| = |\mathcal{S}_E \simeq \mathcal{S}_n|$), φ est un isomorphisme.

Comme H est le stabilisateur de la classe de idH on a : $\varphi(\mathrm{H}) \subset \mathcal{S}_n$ est le stabilisateur d'un point et c'est donc un sous-groupe isomorphe à $\mathcal{S}_{n-1}$.

Exercice 4

a) Déterminer les classes de conjugaison dans $\mathcal{S}_n$.

b) Déterminer les classes de conjugaison dans $\mathcal{A}_n$.

Éléments de réponse 4

a) Soit $c = (a_1 \ \dots \ a_k)$ un k-cycle de $\mathcal{S}_n$. Pour tout $\sigma \in \mathcal{S}_n$ on a

$$\sigma c \sigma^{-1} = (\sigma(a_1) \ \dots \ \sigma(a_k)).$$

Toute permutation se décompose de façon unique en produit de cycles à supports disjoints. Par suite les classes de conjugaison dans $\mathcal{S}_n$ sont paramétrées par les partitions de l'entier n. Rappelons qu'une partition de l'entier n est une famille finie d'entiers $m_i \geq 1$ tels que

$$m_1 \leq \ldots \leq m_r \qquad\qquad \sum m_i = n.$$

La classe de conjugaison correspondant à une telle partition est l'ensemble des permutations dont la décomposition en cycles fait intervenir exactement m_i cycles de longueur i pour tout i.

b) Puisque $\mathcal{A}_n$ est distingué dans $\mathcal{S}_n$ la classe de conjugaison dans $\mathcal{S}_n$ d'un élément de $\mathcal{A}_n$ est contenue dans $\mathcal{A}_n$. Comme $\mathcal{A}_n$ est d'indice 2 dans $\mathcal{S}_n$, la classe de conjugaison de σ dans $\mathcal{S}_n$ est soit égale à la classe de conjugaison de σ dans $\mathcal{A}_n$, soit réunion de deux classes de conjugaison dans $\mathcal{A}_n$.

Montrons que nous sommes dans le premier cas si et seulement si σ admet un cycle de longueur paire dans sa décomposition ou σ admet au moins deux cycles de même longueur impaire dans sa décomposition. Supposons que σ admette un cycle c de longueur paire, pour tout $\tau \in \mathcal{S}_n$ on a $\tau\sigma\tau^{-1} = (\tau c)\sigma(\tau c)^{-1}$; les classes de conjugaison dans $\mathcal{S}_n$ et $\mathcal{A}_n$ coïncident. Si σ admet deux cycles

$$c = (a_1 \ \dots \ a_{2k+1}) \qquad\qquad c' = (a'_1 \ \dots \ a'_{2k+1})$$

de même longueur impaire, alors si d désigne la permutation impaire

$$d = (a_1 \ a'_1) \ldots (a_{2k+1} \ a'_{2k+1})$$

nous avons pour tout $\tau \in \mathcal{S}_n$

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

et les classes de conjugaison dans $\mathcal{S}_n$ et $\mathcal{A}_n$ coïncident.

Réciproquement si σ n'a que des cycles de longueurs impaires deux à deux distinctes, alors on choisit deux entiers $1 \leq i < j \leq n$ apparaissant successivement dans un même cycle dans la décomposition de σ. On voit que $(i \ j)\sigma(i \ j)$ n'est pas conjuguée à σ dans $\mathcal{A}_n$ alors qu'elle l'est dans $\mathcal{S}_n$.

Exercice 5

Soit $n \in \mathbb{N}^*$. Montrer qu'il existe un morphisme injectif de $\mathcal{S}_n$ dans $\mathcal{A}_{n+2}$.

Éléments de réponse 5

Considérons l'application $\psi \colon \mathcal{S}_n \to \mathcal{A}_{n+2}$ définie par

$$\begin{cases} \psi(\sigma) = \sigma \text{ si } \sigma \text{ est une permutation paire} \\ \psi(\sigma) = \sigma \circ (n+1 \ n+2) \text{ si } \sigma \text{ est une permutation impaire} \end{cases}$$

L'application ψ est injective par unicité de la décomposition en cycles à supports disjoints.

On peut vérifier que ψ est un morphisme de groupes.

Exercice 6

Construire un morphisme surjectif de $\mathcal{S}_4$ sur $\mathcal{S}_3$.

Éléments de réponse 6

Faire agir $\mathcal{S}_4$ par conjugaison sur les éléments d'ordre 2 de $\mathcal{S}_4$ qui ne sont pas des transpositions.

Exercice 7

On rappelle que le groupe symétrique $\mathcal{S}_n$ agit par applications linéaires sur $\mathbb{R}^n$ muni de sa base canonique (e_i), en posant pour tout $\sigma \in \mathcal{S}_n$ et tout vecteur e_i de la base canonique $\sigma \cdot e_i = e_{\sigma(i)}$. Pour $\sigma = (1\ 2\ 3) \in \mathcal{S}_3$ expliciter la matrice associée et calculer $\sigma \cdot (x_1, x_2, x_3)$.

Éléments de réponse 7

L'action de $\mathcal{S}_3$ par applications linéaires sur $\mathbb{R}^3$ correspond à un morphisme de $\mathcal{S}_3$ vers le groupe $\mathrm{GL}(3, \mathbb{R})$ des bijections linéaires de $\mathbb{R}^3$. Il s'agit de trouver l'image de $\sigma = (1\ 2\ 3) \in \mathcal{S}_3$. L'application linéaire est entièrement déterminée par l'image d'une base : puisque $e_1 \mapsto e_2$, $e_2 \mapsto e_3$, $e_3 \mapsto e_1$ nous obtenons la matrice

$$\begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$$

et finalement l'image de (x_1, x_2, x_3) est (x_3, x_1, x_2) car

$$\begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} x_3 \\ x_1 \\ x_2 \end{pmatrix}.$$

Remarque : une erreur classique est de croire que l'action est donnée par

$$\sigma(x_1, x_2, x_3) = (x_{\sigma(1)}, x_{\sigma(2)}, x_{\sigma(3)}).$$

Ce n'est pas le cas, cette définition donnerait une action à droite, pas à gauche ! En fait on peut vérifier que la formule correcte pour l'action exprimée en coordonnées est

$$\sigma \cdot (x_1, x_2, x_3) = (x_{\sigma^{-1}(1)}, x_{\sigma^{-1}(2)}, x_{\sigma^{-1}(3)})$$

Références

[Per82] D. Perrin. *Cours d'algèbre*, volume 18 of *Collection de l'École Normale Supérieure de Jeunes Filles*. École Normale Supérieure de Jeunes Filles, Paris, 1982. Edited with the collaboration of Marc Cabanes and Martine Duchene.