

GROUPE SYMÉTRIQUE

A. Compléments sur les groupes

♦ Exercice 1. [★]

Soient $(G, *)$ un groupe fini et x, y deux éléments de G .

1. Démontrer que x, x^{-1} et xyx^{-1} ont le même ordre.
2. Démontrer que xy et yx ont le même ordre.
3. Soit $k \in \mathbb{Z}$. Démontrer que l'ordre de x^k vaut $\omega(x)/(\omega(x) \wedge k)$.
4. On suppose que x et y commutent et que $\omega(x) \wedge \omega(y) = 1$. Démontrer que $\omega(xy) = \omega(x)\omega(y)$.

1. On a $(x^{-1})^{\omega(x)} = (x^{\omega(x)})^{-1} = e_G^{-1} = e_G$ donc $\omega(x^{-1})$ divise $\omega(x)$. En échangeant les rôles, on obtient que $\omega(x)$ divise $\omega(x^{-1})$. D'où

$$\omega(x^{-1}) = \omega(x).$$

On pose $z = yxy^{-1}$. On a $z^{\omega(x)} = (yxy^{-1})^{\omega(x)} = yx^{\omega(x)}y^{-1} = yy^{-1} = e_G$ donc $\omega(z)$ divise $\omega(x)$. Or $x = y^{-1}zy$ donc, en échangeant les rôles, on obtient que $\omega(x)$ divise $\omega(z)$. D'où

$$\omega(yxy^{-1}) = \omega(x).$$

2. On propose deux démonstrations :

▷ On a $xy = x(yx)x^{-1}$ donc, d'après la première question,

$$\omega(yx) = \omega(xy).$$

▷ On a $(xy)^{\omega(yx)+1} = x(yx)^{\omega(yx)}y = xy$, d'où $(xy)^{\omega(yx)} = e_G$ et donc $\omega(xy)$ divise $\omega(yx)$. En échangeant les rôles, on obtient que $\omega(yx)$ divise $\omega(xy)$. D'où

$$\omega(yx) = \omega(xy).$$

3. On a $(x^k)^{\omega(x)/(\omega(x) \wedge k)} = x^{k\omega(x)/(\omega(x) \wedge k)} = (x^{\omega(x)})^{k/(\omega(x) \wedge k)} = (e_G)^{k/(\omega(x) \wedge k)} = e_G$, donc $\omega(x^k)$ divise $\omega(x)/(\omega(x) \wedge k)$.

On a $(x^k)^{\omega(x^k)} = e_G$, c'est-à-dire $x^{k\omega(x^k)} = e_G$. Dès lors, $\omega(x)$ divise $k\omega(x^k)$. Cela entraîne que $\omega(x)/(\omega(x) \wedge k)$ divise $k\omega(x^k)/(\omega(x) \wedge k)$. Mézalors, comme $\omega(x)/(\omega(x) \wedge k)$ et $k/(\omega(x) \wedge k)$ sont premiers entre eux, le lemme de Gauss nous dit que $\omega(x)/(\omega(x) \wedge k)$ divise $\omega(x^k)$.

En conclusion,

$$\omega(x^k) = \frac{\omega(x)}{\omega(x) \wedge k}.$$

4. Comme x et y commutent, on a $(xy)^{\omega(x)\omega(y)} = (x^{\omega(x)})^{\omega(y)}(y^{\omega(y)})^{\omega(x)} = e_G$, d'où $\omega(xy)$ divise $\omega(x)\omega(y)$.

On a $(xy)^{\omega(xy)} = e_G$, c'est-à-dire $x^{\omega(xy)}y^{\omega(xy)} = e_G$ puisque x et y commutent. En élevant à la puissance $\omega(x)$, il s'ensuit que $x^{\omega(xy)\omega(x)}y^{\omega(xy)\omega(x)} = e_G$ (toujours parce que x et y commutent). On a donc $y^{\omega(xy)\omega(x)} = e_G$. Cela implique que $\omega(y)$ divise $\omega(xy)\omega(x)$. Comme $\omega(x) \wedge \omega(y) = 1$, le lemme de Gauß nous dit que $\omega(y)$ divise $\omega(x)$. On montre de même que $\omega(y)$ divise n . La propriété d'indépendance divisoriale (qui utilise l'hypothèse $\omega(x) \wedge \omega(y) = 1$) nous dit alors que $\omega(x)\omega(y)$ divise $\omega(xy)$.

Donc

$$xy \text{ est d'ordre } \omega(x)\omega(y).$$

♦ **Exercice 2.** [o] (Petit théorème de Fermat généralisé)

On rappelle que, pour tout $n \in \mathbb{N}^*$, on note $\varphi(n)$ le nombre d'entiers de $\llbracket 1; n \rrbracket$ premiers avec n . C'est l'indicatrice d'Euler.

Démontrer que, pour tout $n \in \mathbb{N}^*$ et tout $a \in \mathbb{Z}$ tel que $a \wedge n = 1$, on a $a^{\varphi(n)} \equiv 1 [n]$.

Soit $n \in \mathbb{N}^*$. On sait que le groupe $U(\mathbb{Z}/n\mathbb{Z})$ des unités de $\mathbb{Z}/n\mathbb{Z}$ est d'ordre $\varphi(n)$. Par conséquent, pour tout $a \in U(\mathbb{Z}/n\mathbb{Z})$, on a $a^{\varphi(n)} = 1$. Autrement dit,

$$\text{pour tout } a \in \mathbb{Z} \text{ tel que } a \wedge n = 1, \text{ on a } a^{\varphi(n)} \equiv 1 [n].$$

♦ **Exercice 3.** [★]

Démontrer que $x \in \mathbb{Z}/n\mathbb{Z}$ est un générateur de $(\mathbb{Z}/n\mathbb{Z}, +)$ si, et seulement si, $x \wedge n = 1$. En déduire le nombre de générateurs de $(\mathbb{Z}/n\mathbb{Z}, +)$.

On a

$$\begin{aligned} (x \in \mathbb{Z}/n\mathbb{Z} \text{ est un générateur de } (\mathbb{Z}/n\mathbb{Z}, +)) &\iff 1 \in \langle x \rangle \\ &\iff \exists u \in \mathbb{Z}, ux = 1 [n] \\ &\iff \exists u, v \in \mathbb{Z}, ux + vn = 1 \\ &\iff x \wedge n = 1, \end{aligned}$$

donc

$$x \in \mathbb{Z}/n\mathbb{Z} \text{ est un générateur de } (\mathbb{Z}/n\mathbb{Z}, +) \text{ si, et seulement si, } x \wedge n = 1.$$

On en déduit immédiatement que

$$\text{le nombre de générateurs de } (\mathbb{Z}/n\mathbb{Z}, +) \text{ vaut } \varphi(n) \text{ (l'indicatrice d'Euler).}$$

♦ **Exercice 4.** [★]

Démontrer que tout sous-groupe d'un groupe monogène est monogène.

Soit G un groupe monogène. On propose deux solutions.

▷ À la main :

Soient g un générateur de G et H un sous-groupe de G .

Notons b le plus petit entier naturel non nul tel que $g^b \in H$ et démontrons que $H = \langle g^b \rangle$.

Soit $h \in H$. Comme g est générateur de G , il existe $a \in \mathbb{N}$ tel que $h = g^a$. Effectuons la division euclidienne de a par b , ce qui donne $a = bq + r$ où $q \in \mathbb{N}$ et $r \in \llbracket 0; b-1 \rrbracket$. Alors $h = g^{bq+r} = (g^b)^q g^r$ ou encore $g^r = (g^b)^{-q} h$. Comme g^b et h sont des éléments de H , on en déduit que $g^r \in H$. La minimalité de b implique alors que $r = 0$. Donc $a = bq$ et $h = (g^b)^q$.

On a ainsi démontré que tout élément de H est une puissance de g^b , c'est-à-dire que $H = \langle g^b \rangle$. Donc H est monogène.

▷ Par isomorphie :

Si G est infini, on sait qu'il est isomorphe à $(\mathbb{Z}, +)$. Or tous les sous-groupes de \mathbb{Z} sont monogènes (puisque'ils sont de la forme $a\mathbb{Z}$) donc, par isomorphisme, tous les sous-groupes de G sont monogènes.

Si G est fini, on sait qu'il est isomorphe à (\mathbb{U}_n, \times) . Si H désigne un sous-groupe de \mathbb{U}_n d'ordre d , on sait que tous les éléments de H ont un ordre qui divise d (c'est une conséquence du théorème de Lagrange) et donc que $\forall z \in H, z^d = 1$. Par suite, H est inclus dans \mathbb{U}_d . Comme ces deux ensembles ont le même cardinal, on en déduit que $H = \mathbb{U}_d$. En particulier, H est bien cyclique et, par isomorphisme, tout sous-groupe de G est cyclique.

En conclusion,

$$\text{tout sous-groupe d'un groupe monogène est monogène.}$$

Remarque : à bien y regarder, la démonstration par isomorphie en dit un peu plus sur les sous-groupes d'un groupe cyclique : si G est un groupe cyclique de cardinal n , alors pour tout diviseur d de n , il existe une unique sous-groupe de G d'ordre d . Par exemple, dans le cas du groupe cyclique $(\mathbb{Z}/n\mathbb{Z}, +)$, l'unique sous-groupe d'ordre d (où d divise n) est le sous-groupe cyclique engendré par la classe modulo n de n/d . Ce sous-groupe est évidemment isomorphe à $\mathbb{Z}/d\mathbb{Z}$.

B. Groupe symétrique

♦ Exercice 5. [o]

1. Calculer les puissances successives de $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 2 & 5 & 1 \end{pmatrix}$ et en déduire son ordre.
2. Même question avec $\sigma' = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 1 & 2 & 3 \end{pmatrix}$.
3. Déterminer $\sigma\sigma'$ et $\sigma'\sigma$.

A faire.

♦ Exercice 6. [o] (Centre de \mathfrak{S}_n)

Soit $n \geq 3$. On considère une permutation σ de \mathfrak{S}_n qui commute avec toutes les autres, autrement dit telle que $\forall s \in \mathfrak{S}_n, \sigma s = s\sigma$.

1. On considère une transposition $\tau = (a, b)$ de \mathfrak{S}_n . Calculer $\tau\sigma(a)$ et $\tau\sigma(b)$ et en déduire l'égalité entre ensembles $\{a, b\} = \{\sigma(a), \sigma(b)\}$.
2. Démontrer que $\sigma = \text{Id}$. On a ainsi démontré que le centre de \mathfrak{S}_n (c'est-à-dire le sous-groupe des éléments qui commutent avec tous les autres) est trivial.

1. On a clairement

$$\boxed{\tau\sigma(a) = \sigma(b) \quad \text{et} \quad \tau\sigma(b) = \sigma(a).}$$

2. Soit $b \in \llbracket 1; n \rrbracket$. On considère $a, c \in \llbracket 1; n \rrbracket$ tels que a, b, c soient distincts (ce qui est possible puisque $n \geq 3$). Alors $\{b\} = \{a, b\} \cap \{b, c\} = \{\sigma(a), \sigma(b)\} \cap \{\sigma(b), \sigma(c)\} = \{\sigma(b)\}$. Donc $\sigma(b) = b$. Cela démontre que $\sigma = \text{Id}$. Donc

$$\boxed{\text{le centre de } \mathfrak{S}_n \text{ est trivial.}}$$

♦ Exercice 7. [o]

Décomposer en produit de transpositions les permutations

$$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 5 & 2 & 4 \end{pmatrix} \quad \text{et} \quad \sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 5 & 1 & 6 & 2 & 4 \end{pmatrix}.$$

En déduire les signatures de ces deux permutations.

On a

$$\begin{aligned} \sigma_1 &= (4, 5) \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 4 & 2 & 5 \end{pmatrix} \\ &= (4, 5)(2, 4) \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 2 & 4 & 5 \end{pmatrix} \\ &= (4, 5)(2, 4)(2, 3) \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 4 & 5 \end{pmatrix} \\ &= (4, 5)(2, 4)(2, 3)(1, 2). \end{aligned}$$

et

$$\begin{aligned} \sigma_2 &= (4, 6) \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 5 & 1 & 4 & 2 & 6 \end{pmatrix} \\ &= (4, 6)(2, 5) \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 1 & 4 & 5 & 6 \end{pmatrix} \\ &= (4, 6)(2, 5)(1, 3). \end{aligned}$$

On en déduit que

$$\boxed{\varepsilon(\sigma_1) = 1 \quad \text{et} \quad \varepsilon(\sigma_2) = -1.}$$

♦ **Exercice 8.** [★] (Les transpositions à pivot engendrent \mathfrak{S}_n)

Démontrer que \mathfrak{S}_n est engendré par les transpositions $(1, 2), (1, 3), (1, 4), \dots, (1, n)$.

Comme \mathfrak{S}_n est engendré par les transpositions, il suffit de démontrer que toute transposition (i, j) se décompose à l'aide des $(1, i)$.

Si $n = 2$, la seule transposition est $(1, 2)$.

Si $n \geq 3$, pour $1 < i < j$, on veut écrire (i, j) en fonction de $(1, i)$ et $(1, j)$. On se souvient pour cela de la formule de conjugaison des cycles (dans le cas d'une transposition) :

$$\rho(i, j)\rho^{-1} = (\rho(i), \rho(j)),$$

ce qui incite à prendre pour ρ une transposition qui envoie i sur 1 et laisse fixe j , c'est-à-dire $\rho = (1, i)$. On obtient $(1, i)(i, j)(1, i) = (1, j)$, d'où $(i, j) = (1, i)(1, j)(1, i)$.

En conclusion,

\mathfrak{S}_n est engendré par les transpositions $(1, 2), (1, 3), (1, 4), \dots, (1, n)$.

♦ **Exercice 9.** [○]

Décomposer en produit de cycles à supports disjoints les permutations

$$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 5 & 2 & 4 \end{pmatrix} \quad \text{et} \quad \sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 5 & 1 & 6 & 2 & 4 \end{pmatrix}.$$

En déduire les signatures de ces deux permutations.

On a

$$\sigma_1 = (2, 3, 5, 4) \text{ est de signature } -1$$

et

$$\sigma_2 = (1, 3)(2, 5)(4, 6) \text{ est de signature } -1.$$

♦ **Exercice 10.** [★] (Ordre d'une permutation)

Démontrer que l'ordre d'une permutation est le ppcm de l'ordre des cycles de sa décomposition en cycles à supports disjoints.

Soit σ une permutation de $\llbracket 1; n \rrbracket$ et $\sigma = c_k c_{k-1} \dots c_2 c_1$ sa décomposition en cycles à supports disjoints. Posons μ le ppcm des longueurs des cycles c_1, \dots, c_k .

Alors $\sigma^\mu = c_k^\mu c_{k-1}^\mu \dots c_2^\mu c_1^\mu = \text{Id}$ car les c_i commutent. Donc $\omega(\sigma)$ divise μ .

Si $\omega(\sigma)$ était un diviseur strict de μ , l'un des facteurs $c_i^{\omega(\sigma)}$ serait différent de Id . Le support de ce facteur ne serait donc pas vide et, comme les c_i sont à supports disjoints, on aurait $\text{supp}(c_i^{\omega(\sigma)}) \subset \text{supp}(\sigma^{\omega(\sigma)})$, ce qui impliquerait que le support de Id n'est pas vide : absurde ! Donc $\omega(\sigma) = \mu$.

En conclusion,

l'ordre d'une permutation est le ppcm de l'ordre des cycles de sa décomposition en cycles à supports disjoints.

♦ **Exercice 11.** [○]

On mélange un jeu de 32 cartes de la façon suivante : on sépare le jeu en deux moitiés puis on intercale une carte de chaque paquet en commençant par le second. Ainsi l'ordre 1 2 3 4 5 6 ... devient 17 1 18 2 19 3 ...

Déterminer le nombre de battues nécessaires pour que le jeu retrouve son état initial.

Une battue correspond à la permutation σ de $\llbracket 1; 32 \rrbracket$ donnée par

$$\sigma(k) = \begin{cases} k/2 & \text{si } k \text{ est pair} \\ (33+k)/2 & \text{si } k \text{ est impair} \end{cases}$$

La décomposition en cycles de σ donne

$$\begin{aligned}\sigma &= (1\ 17\ 25\ 29\ 29\ 31\ 32\ 16\ 8\ 4\ 2) \\ &\quad (3\ 18\ 9\ 21\ 27\ 30\ 15\ 24\ 12\ 6) \\ &\quad (5\ 19\ 26\ 13\ 23\ 28\ 14\ 7\ 20\ 10) \\ &\quad (11\ 22)\end{aligned}$$

L'ordre de σ est alors donné par

$$\omega(\sigma) = 10 \vee 10 \vee 10 \vee 2 = 10.$$

Donc

le jeu retrouve son état initial après 10 battues.

♦ **Exercice 12.** [o] (Nombres de p -cycles)

Déterminer le nombre de p -cycles dans \mathfrak{S}_n .

Pour déterminer un p -cycle de \mathfrak{S}_n , il faut commencer par choisir une p -liste d'éléments distincts de $\llbracket 1; n \rrbracket$, ce qui laisse $n(n-1) \cdots (n-p+1)$ choix. Comme un p -cycle possède p écritures différentes, on a compté chaque p -cycle p fois ce qui donne $n(n-1) \cdots (n-p+1)/p$ cycles de longueur p . En conclusion,

$$\text{il y a } (p-1)! \binom{n}{p} \text{ } p\text{-cycles dans } \mathfrak{S}_n.$$

♦ **Exercice 13.** [o]

On souhaite démontrer que \mathfrak{S}_n peut être engendré par une transposition et une permutation circulaire.

1. a) Soient $a < b$ deux éléments de $\llbracket 1; n \rrbracket$. Calculer

$$(b-1, b) \cdots (a+2, a+3)(a+1, a+2)(a, a+1)(a+1, a+2)(a+2, a+3) \cdots (b-1, b).$$

En déduire que \mathfrak{S}_n est engendré par les transpositions $(1, 2), (2, 3), \dots, (n-1, n)$.

- b) Pour $k \in \llbracket 0; n-2 \rrbracket$, calculer

$$(1, 2, \dots, n)^k (1, 2) (1, 2, \dots, n)^{-k}.$$

En déduire que \mathfrak{S}_n est engendré par les deux éléments $\tau = (1, 2)$ et $c = (1, 2, \dots, n)$.

2. Décomposer $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}$ en un produit de τ , c , c^{-1} et de leurs puissances.

1. a) On trouve que

$$(b-1, b) \cdots (a+2, a+3)(a+1, a+2)(a, a+1)(a+1, a+2)(a+2, a+3) \cdots (b-1, b) = (a, b).$$

Comme les transpositions engendrent \mathfrak{S}_n , on en déduit que

$$\mathfrak{S}_n \text{ est engendré par les transpositions } (1, 2), (2, 3), \dots, (n-1, n).$$

- b) On a

$$(1, 2, \dots, n)^k (1, 2) (1, 2, \dots, n)^{-k} = (k+1, k+2).$$

Cela implique que les transpositions $(1, 2), (2, 3), \dots, (n-1, n)$ (qui engendrent \mathfrak{S}_n d'après a)) s'écrivent chacune comme un produit de $(1, 2)$ et $(1, 2, \dots, n)$. Par conséquent,

$$\mathfrak{S}_n \text{ est engendré par les deux éléments } \tau = (1, 2) \text{ et } c = (1, 2, \dots, n).$$

2. On décompose σ en produit de transpositions :

$$\sigma = (2, 4) \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix} = (2, 4)(2, 3) \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix} = (2, 4)(2, 3)(1, 2)$$

et l'on applique les formules des questions précédentes à chacune des transpositions :

$$(1, 2) = \tau, \quad (2, 3) = c^1 \tau c^1, \quad (2, 4) = (3, 4)(2, 3)(3, 4) = c^2 \tau c^{-2} c^1 \tau c^{-1} c^2 \tau c^{-2} = c^2 \tau c^{-1} \tau c^1 \tau c^{-2}$$

d'où

$$\sigma = c^2 \tau c \tau c \tau c^{-2} c \tau c \tau,$$

ce qui donne

$$\boxed{\sigma = c^2 \tau c \tau c \tau c^{-1} \tau c \tau.}$$

♦ **Exercice 14.** [★] (Les 3-cycles engendrent \mathfrak{A}_n)

Soit $n \geq 3$. Démontrer que tout produit de deux transpositions s'écrit comme le produit de cycles de longueur 3. En déduire que \mathfrak{A}_n est engendré par les 3-cycles.

On a

$$(a, b)(a, c) = (a, c, b) \quad \text{et} \quad (a, b)(c, d) = (a, b)(b, c)(b, c)(c, d) = (a, b, c)(b, c, d),$$

donc

$$\boxed{\text{tout produit de deux transpositions s'écrit comme le produit de cycles de longueur 3.}}$$

Comme toute permutation paire est le produit d'un nombre pair de transpositions, on en déduit que toute permutation paire est le produit de cycles de longueur 3. Donc

$$\boxed{\mathfrak{A}_n \text{ est engendré par les 3-cycles.}}$$

♦ **Exercice 15.** [★]

Soit K un corps commutatif quelconque. Démontrer que $\mathcal{GL}_n(K)$ contient un sous-groupe isomorphe à \mathfrak{S}_n .

Pour toute permutation $\sigma \in \mathfrak{S}_n$, on introduit la matrice de permutation $P_\sigma \in \mathcal{M}_n(K)$ définie par

$$P_\sigma = (\delta_{i, \sigma(j)})_{i, j \in \llbracket 1; n \rrbracket},$$

c'est-à-dire la matrice obtenue en appliquant la permutation σ aux numéros des colonnes de I_n .

On introduit alors l'application

$$\varphi \begin{cases} \mathfrak{S}_n & \longrightarrow \mathcal{M}_n(K) \\ \sigma & \longmapsto P_\sigma \end{cases}$$

Vérifions que φ est un morphisme de groupes. Pour cela, pour toute permutation $\sigma \in \mathfrak{S}_n$, on considère l'endomorphisme $u_\sigma \in \mathcal{L}(K^n)$ canoniquement associé à P_σ , c'est-à-dire l'endomorphisme (c'est même un automorphisme) tel que $\forall k \in \llbracket 1; n \rrbracket$, $u_\sigma(\varepsilon_k) = \varepsilon_{\sigma(k)}$ où $\mathcal{B} = (\varepsilon_1, \dots, \varepsilon_n)$ désigne la base canonique de K^n . Si σ et ρ désignent deux permutations de $\llbracket 1; n \rrbracket$, on a alors

$$\varphi(\sigma\rho) = P_{\sigma\rho} = \text{Mat}_{\mathcal{B}}(u_{\sigma\rho}) = \text{Mat}_{\mathcal{B}}(u_\sigma u_\rho) = \text{Mat}_{\mathcal{B}}(u_\sigma) \text{Mat}_{\mathcal{B}}(u_\rho) = P_\sigma P_\rho = \varphi(\sigma)\varphi(\rho),$$

où l'égalité $u_{\sigma\rho} = u_\sigma u_\rho$ est justifiée par le fait que ces deux endomorphismes coïncident sur la base \mathcal{B} puisque

$$\forall k \in \llbracket 1; n \rrbracket, \quad u_{\sigma\rho}(\varepsilon_k) = \varepsilon_{\sigma\rho(k)} = u_\sigma(\varepsilon_{\rho(k)}) = u_\sigma(u_\rho(\varepsilon_k)).$$

On a donc bien démontré que φ est un morphisme de groupes.

Il est clair que ce morphisme est injectif (si $\sigma \in \mathfrak{S}_n$ est tel que $P_\sigma = I_n$, c'est que $\sigma = \text{Id}$) donc φ induit un isomorphisme entre \mathfrak{S}_n et $\varphi(\mathfrak{S}_n)$. Autrement dit,

$$\boxed{\text{le sous-groupe multiplicatif de } \mathcal{GL}_n(K), \text{ constituée des matrices de permutations } P_\sigma = (\delta_{i, \sigma(j)})_{i, j \in \llbracket 1; n \rrbracket} \text{ où } \sigma \in \mathfrak{S}_n, \text{ est isomorphe à } \mathfrak{S}_n.}$$