# Colle 17 – Questions de cours

Question de cours n⁰1 — **Propriété**. Soient $A$ et $B$ deux parties d'un même ensemble fini $E$.
Alors : $\text{Card}(E\backslash A) = \text{Card}(E) - \text{Card}(A)$, et $\text{Card}\,(A \cup B) = \text{Card}\,(A) + \text{Card}\,(B) - \text{Card}(A \cap B)$

Observons que : $E = (E\backslash A) \cup A$. Cette union étant disjointe, on a : $\text{Card}(E) = \text{Card}(E\backslash A) + \text{Card}(A)$. On en déduit la première égalité.

Dans le même registre : $A \cup B = (A\backslash B) \cup B$.
Cette union étant disjointe, on a : $\text{Card}(A \cup B) = \text{Card}\,(A\backslash B) + \text{Card}(B) \qquad (\spadesuit)$.
Par ailleurs : $A = (A\backslash B) \cup (A \cap B)$.
Cette nouvelle union étant disjointe, on a : $\text{Card}(A) = \text{Card}\,(A\backslash B) + \text{Card}(A \cap B)$.
Par suite : $\text{Card}\,(A\backslash B) = \text{Card}(A) - \text{Card}(A \cap B) \qquad (\clubsuit)$.

D'après $(\spadesuit)$ et $(\clubsuit)$ : $\text{Card}\,(A \cup B) = \text{Card}\,(A) + \text{Card}\,(B) - \text{Card}(A \cap B)$.

---

Question de cours n⁰2 — **Propriété**. Soient $E$ et $F$ deux ensembles finis, et $f : E \longrightarrow F$ une application. On suppose $\textbf{Card}\,(E) = \textbf{Card}\,(F)$. LASSE (les assertions suivantes sont équivalentes) :
$1/\ f$ est bijective $\qquad 2/\ f$ est injective $\qquad 3/\ f$ est surjective

Montrons $1) \Longrightarrow 2) \Longrightarrow 3) \Longrightarrow 1)$ ; la boucle sera ainsi bouclée !

Supposons $E$ et $F$ finis de même cardinal $n \in \mathbb{N}^*$.

- $\underline{1) \Longrightarrow 2)}$ : trivial.

- $\underline{2) \Longrightarrow 3)}$ : supposons $f$ injective. On peut commencer par noter que $f(E)$ est une partie de $F$. En outre, puisque $f$ est injective, $f(E)$ est un ensemble fini, de cardinal égal à celui de $E$ (cours). Or $\text{Card}\,(E) = \text{Card}\,(F)$ (par hypothèse). Donc l'ensemble $f(E)$ est une partie de $F$, de cardinal égal à celui de $F$ ; il s'ensuit que $f(E) = F$ (cours). Donc $f$ est surjective, ce qui prouve l'implication.
- $\underline{3) \Longrightarrow 1)}$ : supposons à présent $f$ surjective. Alors $f(E) = F$, donc $\text{Card}\,(f(E)) = \text{Card}\,(F)$, et par conséquent $\text{Card}\,(f(E)) = \text{Card}\,(E)$ (puisque $\text{Card}\,(E) = \text{Card}\,(F)$ par hypothèse). On en déduit (cours) que $f$ est injective, et donc bijective. Ce qui prouve l'implication, et achève la preuve de la propriété.

---

Question de cours n⁰3 — **Théorème**. Si $E$ est un ensemble fini de cardinal $n$, alors $(S_E, \circ)$ est un groupe fini de cardinal $n!$.

Un élément de $S_E$ est une bijection de $E$ dans $E$. En vertu de la question de cours 2, il existe autant de bijections de $E$ dans $E$ que d'injections de $E$ dans $E$ (puisque $E$ est fini). Or le nombre d'injections de $E$ dans $E$ est : $\dfrac{n!}{(n-n)!} = n!$.*

Par suite, il existe $n!$ bijections de $E$ dans $E$, ce qui assure déjà que : $\boxed{\text{Card}\,(S_E) = n!}$

En outre, la loi de composition ("$o$") est une *loi de composition interne* dans $S_E$ (la composée de deux bijections est une bijection). Cette lci est *associative* car plus généralement la composition des applications l'est. Elle possède un *élément neutre* qui est l'identité de $E$. Enfin, tout élément $f$ de $S_E$ est *inversible* (pour la loi "$o$") dans $S_E$, car si $f$ est bijective de $E$ dans $E$, sa réciproque $f^{-1}$ est elle aussi une bijection de $E$ dans $E$.

$\boxed{\text{Ce qui prouve que } (S_E, \circ) \text{ est un groupe, de cardinal } n!.}$

---

Question de cours n⁰4 — **Propriété**. Pour tout entier $n \geqslant 3$, le groupe $(S_n, \circ)$ est non-abélien.

Soit $n$ un entier $\geqslant 3$. Les transpositions $(12)$ et $(13)$ appartiennent à $S_n$, puisque $n \geqslant 3$...

Il reste à observer que $(12)(13) = (132)$ tandis que $(13)(12) = (123)$ pour conclure.

**Conclusion**. Pour tout entier $n \geqslant 3$, le groupe $(S_n, \circ)$ est non-abélien.

*Remarque :* de fait, le groupe $(S_n, \circ)$ est abélien SSI $n < 3$, d'après ce qui précède, et car les groupes $S_1$ (groupe trivial) et $S_2 = \{\text{id}, (12)\}$ sont commutatifs.

---

*. Plus généralement, le nombre d'applications injectives de $E$ dans $F$ est $\dfrac{n!}{(n-p)!}$ si $\text{Card}(E) = p \leqslant n = \text{Card}(F)$.

Question de cours n$^0$5 — **Propriété**. Deux permutations à supports disjoints commutent.

➤ On commence par prouver que si un entier $k$ appartient au support d'une permutation $\sigma$, alors $\sigma(k)$ appartient également au support de $\sigma$.

Considérons donc un entier $k \in \operatorname{supp}(\sigma)$. Par l'absurde, supposons que $\sigma(k)$ n'appartienne pas au support de $\sigma$. Alors :

$$\sigma(\sigma(k)) = \sigma(k) \text{ d'où } (\sigma \text{ étant injective}) : \sigma(k) = k$$

Ce qui contredit l'hypothèse "$k \in \operatorname{supp}(\sigma)$". Donc $\sigma(k) \in \operatorname{supp}(\sigma)$.

En résumé : $\forall \sigma \in S_n, \forall k \in \mathbb{N}_n,\ [k \in \operatorname{supp}(\sigma)] \Longrightarrow [\sigma(k) \in \operatorname{supp}(\sigma)] \qquad (\spadesuit)$

➤ La preuve du lemme est à présent une formalité. Soient $\varphi$ et $\rho$ deux éléments de $S_n$, à supports disjoints.

Soit $k$ un entier de $\mathbb{N}_n$. Puisque $\operatorname{supp}(\varphi) \cap \operatorname{supp}(\rho) = \emptyset \quad (\clubsuit)$, on peut distinguer 3 cas :

➢ *Premier cas :* $k \in \operatorname{supp}(\varphi)$. Alors on a : $k \notin \operatorname{supp}(\rho)$ (selon $(\clubsuit)$), et $\varphi(k) \in \operatorname{supp}(\varphi)$ (selon $(\spadesuit)$), donc $\varphi(k) \notin \operatorname{supp}(\rho)$ (re-$(\clubsuit)$).

On en déduit que : $\quad \varphi(\rho(k)) = \varphi(k)$ et $\rho(\varphi(k)) = \varphi(k)$. Donc : $\varphi(\rho(k)) = \rho(\varphi(k))$.

➢ *Second cas :* $k \in \operatorname{supp}(\rho)$. D'après le premier cas : $\varphi(\rho(k)) = \rho(\varphi(k))$.

➢ *Troisième cas :* $k \notin (\operatorname{supp}(\rho) \cup \operatorname{supp}(\varphi))$. Alors : $\varphi(\rho(k)) = \rho(\varphi(k)) = k$.

➢ *Conclusion :* $\forall k \in \mathbb{N}_n,\ \varphi(\rho(k)) = \rho(\varphi(k)) = k$. Ainsi : $\varphi \circ \rho = \rho \circ \varphi$.

**Conclusion**. Deux permutations à supports disjoints commutent.

---

Question de cours n$^0$6 — **(sur le principe du volontariat) Théorème**. Les transpositions engendrent $S_n$.

**Preuve**. Raisonnons par récurrence sur l'entier naturel $n$ en posant pour tout $n \in \mathbb{N} \setminus \{0, 1\}$ :

$\mathscr{P}(n)$ : "Pour toute permutation $\sigma \in S_n$ il existe un entier $k$ et $k$ transpositions $\tau_1, \ldots, \tau_k$ de $S_n$ tels que : $\sigma = \displaystyle\prod_{i=1}^{k} \tau_i$"

➡ <u>Initialisation ($n = 2$)</u> : les permutations de $S_2$ sont l'identité (produit de 0 transposition) et $(12)$ (produit d'une transposition), ce qui assure que $\mathscr{P}(2)$ est vraie.

➡ <u>Hérédité</u> : supposons la propriété établie jusqu'à un certain entier naturel $n$, et montrons que $\mathscr{P}(n+1)$ est vraie.

Soit $\sigma \in S_{n+1}$. On peut distinguer deux cas : $\sigma(n+1) = n+1$ et $\sigma(n+1) \neq n+1$.

<u>Premier cas — Si $\sigma(n+1) = n+1$</u> : dans ce cas, la restriction $\sigma_{|\mathbb{N}_n}$ est une permutation de $\mathbb{N}_n$. Par hypothèse de récurrence, il existe un entier $k$ et $k$ transpositions $\tau_1, \ldots, \tau_k$ de $S_n$ tels que : $\sigma_{|\mathbb{N}_n} = \displaystyle\prod_{i=1}^{k} \tau_i$.

Il reste à voir qu'une transposition dans $S_n$ est aussi une transposition dans $S_{n+1}$ ; en effet, une transposition de $S_n$ s'écrit $(ab)$ avec $a$ et $b$ deux entiers distincts dans $\mathbb{N}_n$ ; ce sont donc naturellement deux entiers distincts dans $\mathbb{N}_{n+1}$. Et puisque $\sigma(n+1) = n+1$, on a donc : $\sigma = \displaystyle\prod_{i=1}^{k} \tau_i$ (égalité dans $S_{n+1}$). Ainsi, sous l'hypothèse $\sigma(n+1) = n+1$, il existe un entier $k$ et $k$ transpositions $\tau_1, \ldots, \tau_k$ de $S_{n+1}$ tels que : $\sigma = \displaystyle\prod_{i=1}^{k} \tau_i$.

<u>Second cas — Si $\sigma(n+1) \neq n+1$</u> : dans ce cas, on introduit la permutation $\rho = (\sigma(n+1)\ \ n+1)\,\sigma$.[†]

$\rho$ est un élément de $S_{n+1}$, qui vérifie : $\rho(n+1) = n+1$. En vertu de l'étude faite dans le premier cas : il existe un entier $k$ et $k$ transpositions $\tau_1, \ldots, \tau_k$ de $S_{n+1}$ tels que : $\rho = \displaystyle\prod_{i=1}^{k} \tau_i$. Par suite, on a : $\sigma = (\sigma(n+1)\ \ n+1) \displaystyle\prod_{i=1}^{k} \tau_i$. La permutation $\sigma$ est ainsi écrite comme produit de $k+1$ transpositions.

<u>Synthèse</u> : dans les deux cas, on a montré que $\sigma \in S_{n+1}$ peut s'écrire comme produit de transpositions. Ce qui assure que $\mathscr{P}(n+1)$ est vraie, et achève la preuve de l'hérédité.

**Conclusion**. Pour tout entier naturel $n \geqslant 2$, et pour toute permutation $\sigma \in S_n$ il existe un entier $k$ et $k$ transpositions $\tau_1, \ldots, \tau_k$ de $S_n$ tels que : $\sigma = \displaystyle\prod_{i=1}^{k} \tau_i$. En d'autres termes, les transpositions engendrent le groupe symétrique.

---

†. La permutation $\rho$ est le produit de $\sigma$, et de la transposition échangeant $\sigma(n+1)$ et $n+1$.

## Compléments de cours (pour information, démos non exigibles en colle)

Lemme — Soient $E$ un ensemble fini de cardinal $n \in \mathbb{N}^*$, et $a \in E$. Alors $E \backslash \{a\}$ est un ensemble fini de cardinal $n-1$.

**Preuve**. Considérons $E$ un ensemble fini de cardinal non nul, et $a$ un élément de $E$.

Puisque $E$ est de cardinal $n$, il existe une bijection de $f : E \longrightarrow \mathbb{N}_n$. Deux cas peuvent alors se présenter ; soit $f(a) = n$, soit $f(a) \neq n$.

Premier cas — Si $f(a) = n$ : on introduit alors la restriction de $f$ à $E \backslash \{a\}$, que nous noterons $g : E \backslash \{a\} \longrightarrow \mathbb{N}_n$.

L'application $g$ est encore injective, puisque $f$ l'est et que la restriction d'une application injective l'est encore.

Par ailleurs : soit $k$ un élément de $\mathbb{N}_{n-1}$. Puisqu'alors $k$ appartient également à $\mathbb{N}_n$, $k$ admet un unique antécédent $x$ par $f$ dans $E$. Or cet unique antécédent ne peut être $a$, puisque $a$ est l'unique antécédent de $n$ et que $k \neq n$. Il s'ensuit que :

$$\forall\, k \in \mathbb{N}_{n-1},\ \exists!\, x \in E \backslash \{a\},\ g(x) = k$$

Par suite, l'application $g$ induit une bijection de $E \backslash \{a\}$ dans $\mathbb{N}_{n-1}$. D'où : $E \backslash \{a\} \sim \mathbb{N}_{n-1}$.

Second cas — Si $f(a) \neq n$ : on introduit alors l'application :

$$\begin{aligned} \tau : \mathbb{N}_n &\longrightarrow \mathbb{N}_n \\ n &\longmapsto f(a) \\ f(a) &\longmapsto n \\ k &\longmapsto k \text{ si } k \neq f(a) \text{ et } k \neq n \end{aligned}$$

L'application $\tau$ est bijective, car c'est une involution (Toronto...)

Donc l'application : $F = \tau \circ f : E \longrightarrow \mathbb{N}_n$ est bijective (c'est la composée de deux bijections) et a le bon goût de satisfaire la condition : $F(a) = n$. On est ainsi ramenés au premier cas, et on peut donc conclure que $E \backslash \{a\} \sim \mathbb{N}_{n-1}$.

Dans les deux cas, on a établi que $E \backslash \{a\}$ et $\mathbb{N}_{n-1}$ sont équipotents.

**Conclusion**. Si $E$ est un ensemble fini de cardinal $n \in \mathbb{N}^*$, et $a \in E$, alors $E \backslash \{a\}$ est un ensemble fini de cardinal $n-1$.

---

Lemme — Soient $E$ et $F$ deux ensembles finis, de cardinaux respectifs $p$ et $n$. Le nombre d'injections de $E$ dans $F$ est l'entier :

$$A_n^p = \frac{n!}{(n-p)!} \text{ si } p \in [\![ 0, n ]\!], \text{ et } A_n^p = 0 \text{ si } p > n.$$

**Preuve**. Commençons par observer que $f(E)$ étant une partie de $F$, on a $\text{Card}(f(E)) \leqslant n = \text{Card}(F)$. Par ailleurs, $f$ est injective si et seulement si $\text{Card}(f(E)) = \text{Card}(E) = p$. Il s'ensuit qu'il ne peut pas exister d'application injective de $E$ dans $F$ si $p > n$, ce qui prouve déjà la seconde partie de la proposition.

Supposons maintenant $p \leqslant n$, et notons $E = \{x_1, \dots, x_p\}$. Pour définir une application $f$, on peut choisir successivement les valeurs de $f(x_1)$,..., $f(x_p)$. Si l'on souhaite que l'application $f$ soit injective, on doit prendre ces éléments distincts dans $F$. On a alors $n$ choix pour $f(x_1)$, $n-1$ choix pour $f(x_2)$,..., $(n-p+1)$ choix pour $f(x_p)$. Il existe donc : $n(n-1)\cdots(n-p+1)$ injections de $E$ dans $F$, d'où : pour tout $p \in [\![ 0, n ]\!]$, il existe $\dfrac{n!}{(n-p)!}$ injections de $E$ dans $F$.

---

Propriété — Un $p$-cycle est une permutation. En outre, avec les notations usuelles :

$$(a_1 a_2 \cdots a_p)^{-1} = (a_p a_{p-1} \cdots a_1)$$

**Preuve**. Soit $k$ un élément de $\mathbb{N}_n$.

➥ Si $k \notin \{a_1, \dots, a_p\}$ : alors $[(a_p a_{p-1} \cdots a_1)(a_1 a_2 \cdots a_p)](k) = k$ puisque $k$ est laissé invariant par les $p$-cycles $(a_p a_{p-1} \cdots a_1)$ et $(a_1 a_2 \cdots a_p)$.

➥ Si $k \in \{a_1, \dots, a_{p-1}\}$ : il revient au même de dire qu'il existe $i \in \mathbb{N}_{p-1}$ tel que $k = a_i$. Alors :

$$[(a_p a_{p-1} \cdots a_1)(a_1 a_2 \cdots a_p)](k) = (a_p a_{p-1} \cdots a_1)((a_1 a_2 \cdots a_p)(a_i)) = (a_p a_{p-1} \cdots a_1)(a_{i+1}) = a_i$$

➥ Si $k = a_p$ : Alors :

$$[(a_p a_{p-1} \cdots a_1)(a_1 a_2 \cdots a_p)](a_p) = (a_p a_{p-1} \cdots a_1)(a_1) = a_p$$

**Conclusion intermédiaire** : $\forall k \in \mathbb{N}_n$,

$$[(a_p a_{p-1} \cdots a_1)(a_1 a_2 \cdots a_p)](k) = k, \text{ soit : } (a_p a_{p-1} \cdots a_1)(a_1 a_2 \cdots a_p) = \mathrm{id}_{\mathbb{N}_n}.$$

Dans l'autre sens :

➥ Si $k \notin \{a_1, \ldots, a_p\}$ : comme dans le cas précédent $[(a_1 a_2 \cdots a_p)(a_p a_{p-1} \cdots a_1)](k) = k$.

➥ Si $k \in \{a_2, \ldots, a_p\}$ : il revient au même de dire qu'il existe $i \in [\![ 2, p ]\!]$ tel que $k = a_i$. Alors :

$$[(a_1 a_2 \cdots a_p)(a_p a_{p-1} \cdots a_1)](k) = (a_1 a_2 \cdots a_p)(a_p a_{p-1} \cdots a_1)((a_i)) = (a_1 a_2 \cdots a_p)(a_{i-1}) = a_i$$

➥ Si $k = a_1$ : Alors :

$$[(a_1 a_2 \cdots a_p)(a_p a_{p-1} \cdots a_1)](k) = (a_1 a_2 \cdots a_p)(a_p a_{p-1} \cdots a_1)((a_1)) = (a_1 a_2 \cdots a_p)(a_p) = a_1$$

**Conclusion intermédiaire bis** : $\forall k \in \mathbb{N}_n$,

$$[(a_1 a_2 \cdots a_p)(a_p a_{p-1} \cdots a_1)](k) = k, \text{ soit : } (a_1 a_2 \cdots a_p)(a_p a_{p-1} \cdots a_1) = \mathrm{id}_{\mathbb{N}_n}.$$

Conclusion. D'après les calculs précédents : $(a_p a_{p-1} \cdots a_1)(a_1 a_2 \cdots a_p) = \mathrm{id}_{\mathbb{N}_n}$ et $(a_1 a_2 \cdots a_p)(a_p a_{p-1} \cdots a_1) = \mathrm{id}_{\mathbb{N}_n}$. Par suite, l'application $(a_1 a_2 \cdots a_p)$ est une bijection de $\mathbb{N}_n$ dans $\mathbb{N}_n$ ; c'est donc une permutation, d'inverse $(a_p a_{p-1} \cdots a_1)$ dans $S_n$.

---

Propriété — Avec les notations usuelles :

$$(a_1 a_2 \cdots a_p) = \prod_{i=1}^{p-1} (a_i a_{i+1})$$

**Preuve**. Soit $k$ un élément de $\mathbb{N}_n$.

➥ Si $k \notin \{a_1, \ldots, a_p\}$ : alors $(a_1 a_2 \cdots a_p)(k) = k$ puisque $k$ n'appartient pas au support du cycle, et $\left[\prod_{i=1}^{p-1} (a_i a_{i+1})\right](k) = k$ puisque $k$ n'appartient au support d'aucune transposition $(a_i a_{i+1})$ du produit.

D'où : $\boxed{\forall k \in \mathbb{N}_n,\ k \notin \{a_1, \ldots, a_p\},\ \left[\prod_{i=1}^{p-1} (a_i a_{i+1})\right](k) = (a_1 a_2 \cdots a_p)(k)}$

➥ Si $k \in \{a_1, \ldots, a_{p-2}\}$ : il revient au même de dire qu'il existe $m \in \mathbb{N}_{p-1}$ tel que $k = a_m$. Alors d'une part :

$$(a_1 a_2 \cdots a_p)(k) = (a_1 a_2 \cdots a_p)(a_m) = a_{m+1}$$

Et d'autre part :

$$\begin{aligned}
\left[\prod_{i=1}^{p-1} (a_i a_{i+1})\right](a_m) &= \left[\left(\prod_{i=1}^{m-1} (a_i a_{i+1})\right)(a_m a_{m+1})\left(\prod_{i=m+1}^{p-1} (a_i a_{i+1})\right)\right](a_m) \\
&= \left[\left(\prod_{i=1}^{m-1} (a_i a_{i+1})\right)(a_m a_{m+1})\right]\left(\left(\prod_{i=m+1}^{p-1} (a_i a_{i+1})\right)(a_m)\right)
\end{aligned}$$

Puisque $a_m$ n'appartient au support d'aucune transposition $(a_i a_{i+1})$ pour $i \geqslant m+1$, on a :

$$\left(\prod_{i=m+1}^{p-1}(a_i a_{i+1})\right)(a_m) = a_m$$

Il s'ensuit que :

$$\left[\prod_{i=1}^{p-1}(a_i a_{i+1})\right](a_m) = \left[\left(\prod_{i=1}^{m-1}(a_i a_{i+1})\right)(a_m a_{m+1})\right](a_m) = \left[\left(\prod_{i=1}^{m-1}(a_i a_{i+1})\right)\right](a_{m+1})$$

De nouveau, puisque $a_{m+1}$ n'appartient au support d'aucune transposition $(a_i a_{i+1})$ pour $i \leqslant m-1$, on a :

$\left(\prod_{i=1}^{m-1}(a_i a_{i+1})\right)(a_{m+1}) = a_{m+1}$. D'où finalement : $\left[\prod_{i=1}^{p-1}(a_i a_{i+1})\right](a_m) = a_{m+1}$.

D'où : $\boxed{\forall k \in \{a_1, \ldots, a_{p-2}\},\ \left[\prod_{i=1}^{p-1}(a_i a_{i+1})\right](k) = (a_1 a_2 \cdots a_p)(k)}$

➥ Si $k = a_{p-1}$ : Alors d'une part : $(a_1 a_2 \cdots a_p)(a_{p-1}) = a_p$
Et d'autre part :

$$\left[\prod_{i=1}^{p-1}(a_i a_{i+1})\right](a_{p-1}) = \left[\left(\prod_{i=1}^{p-2}(a_i a_{i+1})\right)(a_{p-1} a_p)\right](a_{p-1}) = \left[\left(\prod_{i=1}^{p-2}(a_i a_{i+1})\right)\right](a_p) = a_p$$

La dernière égalité provenant de ce que $a_p$ n'appartient au support d'aucune transposition $(a_i a_{i+1})$ pour $i \leqslant p-2$.

D'où : $\boxed{\left[\prod_{i=1}^{p-1}(a_i a_{i+1})\right](a_{p-1}) = (a_1 a_2 \cdots a_p)(a_{p-1})}$

➥ Si $k = a_p$ : Alors d'une part : $(a_1 a_2 \cdots a_p)(a_p) = a_1$
Et d'autre part :

$$\left[\prod_{i=1}^{p-1}(a_i a_{i+1})\right](a_p) = \left[\left(\prod_{i=1}^{p-2}(a_i a_{i+1})\right)(a_{p-1} a_p)\right](a_p) = \left[\left(\prod_{i=1}^{p-2}(a_i a_{i+1})\right)\right](a_{p-1}) = \left[\left(\prod_{i=1}^{p-3}(a_i a_{i+1})\right)\right](a_{p-2})$$

$$= \cdots = \left[\left(\prod_{i=1}^{2}(a_i a_{i+1})\right)\right](a_3) = (a_1 a_2)(a_2) = a_1$$

D'où : $\boxed{\left[\prod_{i=1}^{p-1}(a_i a_{i+1})\right](a_p) = (a_1 a_2 \cdots a_p)(a_p)}$

**Conclusion**. $\forall k \in \mathbb{N}_n$, $\left[\prod_{i=1}^{p-1}(a_i a_{i+1})\right](k) = (a_1 a_2 \cdots a_p)(k)$ soit : $\prod_{i=1}^{p-1}(a_i a_{i+1}) = (a_1 a_2 \cdots a_p)$

**Cette dernière propriété signifie que tout $p$-cycle s'écrit comme un produit d'exactement $(p-1)$ transpositions.**

---

Théorème — Toute permutation peut s'écrire comme un produit de cycles à supports disjoints.

**Preuve**. Preuve par récurrence sur $n \in \mathbb{N}$, $n \geqslant 2$. On pose $P(n)$ : "Dans $S_n$, toute permutation de $S_n$ s'écrit comme produit de cycles à supports disjoints".

➤ **Initialisation (pour $n = 2$)**. Les éléments de $S_2$ sont $\mathrm{id}_{\mathbb{N}_2}$ (produit de zéro cycle) et $(12)$ (produit d'un cycle).

➤ **Hérédité**. Supposons $P(n)$ vraie pour un entier naturel $n \geqslant 2$. Soit $\sigma \in S_{n+1}$ ; on distingue deux cas.

Premier cas : si $\sigma(n+1) = n+1$. Alors $\sigma_{|\mathbb{N}_n}$ est une permutation de $S_n$. Par hypothèse de récurrence, il existe $k$ cycles $c_1, \ldots, c_k$ à supports disjoints tels que : $\sigma_{|\mathbb{N}_n} = \prod_{i=1}^{k} c_i$. Or ces $k$-cycles $c_i$ peuvent être vus comme des éléments de $S_{n+1}$, et puisque $\sigma$ laisse $(n+1)$ invariant, l'égalité $\sigma = \prod_{i=1}^{k} c_i$ est valide dans $S_{n+1}$.

Second cas : si $\sigma(n+1) \neq n+1$. On considère alors la transposition $\tau = ((n+1), \sigma(n+1))$. Alors $\tau\sigma$ est un élément de $S_{n+1}$ tel que : $\tau\sigma(n+1) = n+1$.

D'après l'étude faite dans le premier cas, il existe $k$-cycles $c_1,\ldots, c_k$ de $S_{n+1}$ tels que : $\tau\sigma = \prod_{i=1}^{k} c_i$.

Par suite ‡ : $\sigma = \tau c_1 \cdots c_k$.

Si $\sigma(n+1) \notin \bigcup_{i=1}^{k} \mathrm{supp}(c_i)$, alors $\tau$, $c_1,\ldots, c_k$ sont à supports disjoints, et c'est gagné.

Sinon : $\exists!\, j \in [\![ 1, k ]\!],\ c_j = (\sigma(n+1), x_1, \ldots, x_p)$.

L'entier $x_p$ est alors l'unique antécédent de $n+1$ par $\sigma$.

On pose alors : $\widehat{c_j} = (\sigma(n+1), x_1, \ldots, x_p, n+1)$.

Les cycles $c_1,\ldots, \widehat{c_j},\ldots, c_k$ sont à supports disjoints, et par construction : $\sigma = c_1 \cdots \widehat{c_j} \cdots c_k$.

On en déduit que dans les deux cas, tout élément de $S_{n+1}$ est produit de cycles à supports disjoints, d'où $P(n+1)$ est vraie.

**Conclusion**. Pour tout entier $n \geqslant 2$, tout élément de $S_n$ est produit de cycles à supports disjoints.

---

Théorème — $\forall\, (\sigma, \tau) \in S_n^2,\ \varepsilon(\sigma\tau) = \varepsilon(\sigma)\,\varepsilon(\tau)$

**Preuve**. Soient $\sigma$ et $\tau$ deux éléments de $S_n$.

Soit $(i, j)$ un couple d'entiers de $\mathbb{N}_n$ avec : $1 \leqslant i < j \leqslant n$.

La permutation $\sigma\tau$ réalise une inversion si et seulement si :

- ➥ $\tau$ réalise une inversion sur le couple $(i, j)$, et $\sigma$ ne réalise pas d'inversion sur le couple $(\tau(i), \tau(j))$ ;
- ➥ $\tau$ ne réalise pas d'inversion sur le couple $(i, j)$, et $\sigma$ réalise une inversion sur le couple $(\tau(i), \tau(j))$

En sommant $U(\sigma)$ et $U(\tau)$, on compte les inversions décrites ci-dessus, ainsi que deux fois les cas où $\tau$ réalise une inversion sur le couple $(i, j)$ et $\sigma$ réalise une inversion sur le couple $(\tau(i), \tau(j))$.
Il s'ensuit que $U(\sigma\tau)$ et $U(\sigma) + U(\tau)$ ont même parité. Donc :

$$(-1)^{U(\sigma\tau)} = (-1)^{U(\sigma)+U(\tau)} \Longleftrightarrow (-1)^{U(\sigma\tau)} = (-1)^{U(\sigma)}(-1)^{U(\tau)} \Longleftrightarrow \boxed{\varepsilon(\sigma\tau) = \varepsilon(\sigma)\,\varepsilon(\tau)}$$

**Remarque**. Le théorème ci-dessus signifie que l'application $\varepsilon : (S_n, \circ) \longrightarrow (\{\pm 1\}, \times)$ est un morphisme de groupes : l'image par $\varepsilon$ de $\sigma \circ \tau$ est égal au produit des images $\varepsilon(\sigma) \times \varepsilon(\tau)$.

---

‡. En multipliant à gauche par $\tau$ les deux termes de l'égalité précédente.

# Banque d'exercices

**Exercice 1.** — Soit $E$ fini de cardinal $n$. Etablir que $\text{Card}(\mathscr{P}(E)) = 2^n$.

**Exercice 2.** — Soient $n$ et $p$ deux entiers naturels, avec $p \leqslant n$. Combien existe t-il d'applications $f : \mathbb{N}_p \longrightarrow \mathbb{N}_n$ strictement croissantes ?

**Exercice 3.** — Dans $S_5$, combien existe t-il de transpositions ?

**Exercice 4.** — Dans $S_5$, combien existe t-il de 3-cycles ?

**Exercice 5.** — Dans $S_5$, combien existe t-il de produits de 2 transpositions à supports disjoints ?

**Exercice 6.** — Soit $n$ un entier $\geqslant 2$. On considère :

$$H = \{\sigma \in S_n,\ \sigma(n) = n\}$$

$H$ est donc l'ensemble des permutations de $\mathbb{N}_n$ laissant $n$ invariant.
Montrer que $H$ est un sous-groupe de $S_n$. Quel est son cardinal ?

**Exercice 7.** — Soit $n$ un entier $\geqslant 2$. Combien existe t-il d'éléments de $S_n$ qui échangent 1 et 2 ?

**Exercice 8.** — Dans $S_8$ on considère le 6-cycle $c_1 = (135246)$ et le 3-cycle $c_2 = (154)$.
Existe t-il un élément $\sigma$ de $S_8$ tel que : $c_1 = \sigma^{-1} c_2 \sigma$ ?

## Banque d'exercices - Indications (seulement pour le TD de lundi 9/02)

**Exercice 1.** — Commencez par répondre aux 2 questions suivantes :

1/ Quelles sont les valeurs possibles pour le cardinal d'une partie de $E$ ?

2/ Pour une valeur $k$ possible, combien existe t-il de parties de cardinal $k$ ?

**Exercice 2.** — A la main, commencez par construire 2 ou 3 applications strictement croissantes de $\mathbb{N}_3$ dans $\mathbb{N}_5$. De quoi avez-vous besoin pour construire ces exemples ?

**Exercice 3.** — Commencez par compter le nombre de supports possibles, puis, une fois le support choisi, comptez le nombre de permutations ayant ce support qui répondent à la question.

**Exercice 4.** — Commencez par compter le nombre de supports possibles, puis, une fois le support choisi, comptez le nombre de permutations ayant ce support qui répondent à la question.

**Exercice 5.** — Commencez par compter le nombre de supports possibles, puis, une fois le support choisi, comptez le nombre de permutations ayant ce support qui répondent à la question.

**Exercice 6.** — Méthode des "$(SGx)$" pour montrer que $H$ est un sous-groupe.

**Exercice 7.** — ...

**Exercice 8.** — Signature.

# Banque d'exercices - Corrigés

**Exercice 1.** — Soit $E$ fini de cardinal $n$. Etablir que $\text{Card}(\mathscr{P}(E)) = 2^n$.

Pour tout entier $k \in [\![ 0, n ]\!]$, notons : $\mathscr{P}_k(E) = \{A \subset E,\ \text{Card}(A) = k\}$.

On a : $\mathscr{P}(E) = \displaystyle\bigcup_{k=0}^{n} \mathscr{P}_k(E)$.

Puisque le cardinal d'une partie de $E$ est unique, l'union ci-dessus est disjointe et :

$$\text{Card}\left(\mathscr{P}(E)\right) = \sum_{k=0}^{n} \text{Card}\left(\mathscr{P}_k(E)\right) = \sum_{k=0}^{n} \binom{n}{k} = 2^n$$

**Exercice 2.** — Soient $n$ et $p$ deux entiers naturels, avec $p \leqslant n$. Combien existe t-il d'applications $f : \mathbb{N}_p \longrightarrow \mathbb{N}_n$ strictement croissantes ?

Une application strictement croissante de $\mathbb{N}_p$ dans $\mathbb{N}_n$ est entièrement déterminée par son image, càd par une partie à $p$ éléments de $\mathbb{N}_n$.

**Conclusion.** Il existe $\binom{n}{p}$ applications strictement croissantes $\mathbb{N}_p$ dans $\mathbb{N}_n$.

**Exercice 3.** — Dans $S_5$, combien existe t-il de transpositions ?

Dans $S_5$, une transposition est uniquement déterminée par son support (les transpositions $(ij)$ et $(ji)$ étant égales), qui est une combinaison de 2 éléments parmi 5.

**Conclusion.** Il existe $\binom{5}{2} = 10$ transpositions dans $S_5$.

**Exercice 4.** — Dans $S_5$, combien existe t-il de 3-cycles ?

Dans $S_5$, un 3-cycle est uniquement déterminé par son support, disons $\{a_1, a_2, a_3\}$ ; et par l'image de $a_1$ (deux choix possibles).

**Conclusion.** Il existe $2 \times \binom{5}{3} = 20$ 3-cycles dans $S_5$.

**Exercice 5.** — Dans $S_5$, combien existe t-il de produits de 2 transpositions à supports disjoints ?

Dans $S_5$, une permutation qui est le produit de 2 transpositions à supports disjoints est uniquement déterminée par son support, disons $\{a_1, a_2, a_3, a_4\}$ ; et par l'image de $a_1$ (trois choix possibles).

**Conclusion.** Il existe $3 \times \binom{5}{4} = 15$ produits de 2 transpositions à supports disjoints dans $S_5$.

**Exercice 6.** — Soit $n$ un entier $\geqslant 2$. On considère :

$$H = \{\sigma \in S_n,\ \sigma(n) = n\}$$

$H$ est donc l'ensemble des permutations de $\mathbb{N}_n$ laissant $n$ invariant.

Montrer que $H$ est un sous-groupe de $S_n$. Quel est son cardinal ?

$H$ est inclus dans $S_n$ par définition (SG1) ; $\text{id}_{\mathbb{N}_n}$ appartient à $H$ ; on vérifie aisément que si $\sigma$ et $\rho$ sont deux éléments de $H$, alors $\sigma\rho$ et $\sigma^{-1}$ appartiennent à $H$ (SG3 et SG4).

On en déduit que $H$ est un sous-groupe de $S_n$.

Par ailleurs, $H$ est équipotent à l'ensemble des permutations de $[\![ 1, n-1 ]\!]$, qui est de cardinal $(n-1)!$ selon le cours.

**Conclusion.** $H$ est un sous-groupe de $S_n$, et $\text{Card}(H) = (n-1)!$.

**Exercice 7.** — Soit $n$ un entier $\geqslant 2$. Combien existe t-il d'éléments de $S_n$ qui échangent 1 et 2 ?

Autant que de permutations de $[\![ 3, n ]\!]$.

**Conclusion.** Il existe $(n-2)!$ éléments de $S_n$ qui échangent 1 et 2.

**Exercice 8.** — Dans $S_8$ on considère le 6-cycle $c_1 = (135246)$ et le 3-cycle $c_2 = (154)$.
Existe t-il un élément $\sigma$ de $S_8$ tel que : $c_1 = \sigma^{-1} c_2 \sigma$ ?

Supposons qu'il existe une permutation $\sigma$ telle que : $c_1 = \sigma^{-1} c_2 \sigma$.
Alors on aurait : $\varepsilon(c_1) = \varepsilon(\sigma^{-1} c_2 \sigma)$.

Or, selon les propriétés de la signature :

$$\varepsilon(\sigma^{-1} c_2 \sigma) = \varepsilon(\sigma^{-1})\varepsilon(c_2)\varepsilon(\sigma) = \underbrace{\varepsilon(\sigma^{-1})\varepsilon(\sigma)}_{=1}\varepsilon(c_2) = \varepsilon(c_2)$$

D'où : $\varepsilon(c_1) = \varepsilon(c_2)$. Or, selon le cours : $\varepsilon(c_1) = (-1)^{6-1} = -1$ et $\varepsilon(c_2) = (-1)^{3-1} = 1$. Contradiction.

**Conclusion.** Il n'existe aucune permutation $\sigma \in S_8$ telle que : $c_1 = \sigma^{-1} c_2 \sigma$.