Chapitre 15

Ensembles finis et groupe symétrique

15.1 Ensembles finis

Notation. Soit n un entier naturel non nul. On note $\mathbb{N}_n = [\![1, n]\!]$. Par convention : $\mathbb{N}_0 = \emptyset$.

Définition 1 - Soient E et F deux ensembles.

On dit que E **est équipotent à** F s'il existe une bijection de E dans F.

Remarque. La relation binaire "être équipotent à" (équipotence) est une **relation d'équivalence** (pour mémoire : réflexive, symétrique, transitive) sur les ensembles. Cette observation faite, nous pourrons dire par la suite que deux ensembles E et F sont équipotents s'il existe une bijection entre E et F.

Lemme 1 - La relation binaire d'équipotence est une relation d'équivalence.

Preuve. Ecrivons $E \sim F$ lorsque E est équipotent à F.

➤ Réflexivité : pour tout ensemble E, l'application id_E est une bijection de E dans E. Donc $\boxed{E \sim E}$.

➤ Symétrie : soient E et F deux ensembles équipotents. Il existe donc une bijection $f : E \longrightarrow F$. Dans ce cas, la bijection réciproque f^{-1} est une bijection de F dans E. Par suite : $\boxed{(E \sim F) \Longrightarrow (F \sim E)}$.

➤ Transitivité : soient E, F et G trois ensembles tels que $E \sim F$ et $F \sim G$. Alors il existe une bijection $f : E \longrightarrow F$ et une bijection $g : F \longrightarrow G$. La composée $g \circ f$ est une bijection de E dans G, puisque la composée de deux bijections en est encore une (cf colle 6). D'où $E \sim G$. En résumé : $\boxed{[(E \sim F) \wedge (F \sim G)] \Longrightarrow (E \sim G)}$

Conclusion. La relation d'équipotence est une relation d'équivalence. △

Exemples : les ensembles $E = \{1, 2, 3\}$ et $F = \{a, b, c\}$ sont équipotents ; $\mathbb{N}$ et $\mathbb{N}^*$ sont équipotents ; plus surprenant $\mathbb{N}$ et $\mathbb{Z}$ sont équipotents ; encore plus surprenant, $\mathbb{N}$ et $\mathbb{Q}$ sont équipotents (Cantor-Bernstein...). En revanche, $\mathbb{N}$ et $\mathbb{R}$ ne le sont pas (vous verrez l'an prochain que le premier est *dénombrable*, mais pas le second).

Propriété 1 - (Exercice classique). $\mathbb{N}$ est équipotent à $\mathbb{N}^*$ et à $\mathbb{Z}$.

Preuve. ➤ Pour le premier point : l'application $f : k \in \mathbb{N} \longmapsto k+1 \in \mathbb{N}^*$ est clairement bijective, de bijection réciproque $f^{-1} : k \in \mathbb{N}^* \longmapsto k-1 \in \mathbb{N}$. Ainsi : $\boxed{\mathbb{N} \sim \mathbb{N}^*}$.

➤ Pour le second point : on construit une application $f : \mathbb{N} \longrightarrow \mathbb{Z}$ en posant :

$$\forall\, n \in \mathbb{N},\ f(n) = \begin{cases} \dfrac{n}{2} & \text{si } n \text{ est pair} \\ -\dfrac{n+1}{2} & \text{si } n \text{ est impair} \end{cases}$$

Montrons l'injectivité de f : soient n et n' deux entiers naturels tels que : $f(n) = f(n')$ (♠) .
Si $f(n)$ et $f(n')$ sont tous deux positifs ou nuls, alors n et n' sont pairs, et $f(n) = n/2$ et $f(n') = n'/2$. D'où (♠) implique $n = n'$.
Si $f(n)$ et $f(n')$ sont tous deux strictement négatifs, alors n et n' sont impairs, et $f(n) = -(n+1)/2$ et $f(n') = -(n'+1)/2$. D'où (♠) implique encore $n = n'$.

Dans les deux cas : $f(n) = f(n') \Longrightarrow n = n'$, ce qui prouve que f est injective.

Montrons la surjectivité de f : soit N un entier relatif. Si N est positif ou nul, alors N admet pour antécédent $2N$ par f. Et si N est strictement négatif, alors il admet pour antécédent $(-2N-1)$ par f. On a donc établi que : $\forall\, N \in \mathbb{N},\ \exists\, n \in \mathbb{N},\ f(n) = N$. Ce qui assure que f est surjective.

Par suite, l'application f est bijective, d'où : $\boxed{\mathbb{N} \sim \mathbb{Z}}$. △

Définition 2 - Un ensemble E est **fini** s'il existe un entier naturel n tel que E et $\mathbb{N}_n$ soient équipotents.

Lemme 2 - Soient n et m deux entiers naturels.

1) S'il existe une injection de $\mathbb{N}_n$ dans $\mathbb{N}_m$, alors $n \leqslant m$.

2) S'il existe une surjection de $\mathbb{N}_n$ dans $\mathbb{N}_m$, alors $n \geqslant m$.

3) S'il existe une bijection de $\mathbb{N}_n$ dans $\mathbb{N}_m$, alors $n = m$.

Preuve. ➤ Montrons le 1). Raisonnons par récurrence sur l'entier naturel n en posant :

$$\mathscr{P}(n) : \text{“s'il existe une injection de } \mathbb{N}_n \text{ dans } \mathbb{N}_m, \text{ alors } n \geqslant m\text{”}$$

➥ Initialisation $(n = 0)$: OK. [1]

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

Considérons $f : \mathbb{N}_{n+1} \longrightarrow \mathbb{N}_m$ une application injective. Deux cas peuvent alors se présenter ; soit $f(n+1) = m$, soit $f(n+1) \neq m$.

Premier cas — Si $f(n+1) = m$: on introduit alors la restriction de f à $\mathbb{N}_n$, que nous noterons g. Pour mémoire, il s'agit de l'application $g = f_{|\mathbb{N}_n} : \mathbb{N}_n \longrightarrow \mathbb{N}_m$ définie en posant : $\forall\, k \in \mathbb{N}_n,\ g(k) = f(k)$. [2]

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

1. On pourra puissamment observer que tout entier naturel est supérieur ou égal à zéro.
2. “g est définie par la même formule que f, sur un ensemble de définition plus petit”.

En outre g est à valeurs dans $\mathbb{N}_{m-1}$, puisque m ne peut avoir d'antécédent par g. En effet, s'il existait un entier $k \in \mathbb{N}_n$ tel que $g(k) = m$, alors on aurait $f(k) = m$ (par définition de g) et $f(n+1) = m$ (par hypothèse). L'injectivité de f impliquerait alors $k = n+1$, ce qui serait absurde puisque $k < n+1$.

En résumé, l'application g induit une application injective de $\mathbb{N}_n$ dans $\mathbb{N}_{m-1}$. Par hypothèse de récurrence, on en déduit que $\boxed{n \leqslant m-1, \text{ d'où } n+1 \leqslant m}$.

Second cas — Si $f(n+1) \neq m$: on introduit alors l'application :

$$\begin{aligned} \tau : \mathbb{N}_m &\longrightarrow \mathbb{N}_m \\ m &\longmapsto f(n+1) \\ f(n+1) &\longmapsto m \\ k &\longmapsto k \text{ si } k \neq f(n+1) \text{ et } k \neq m \end{aligned}$$

L'application τ est bijective, car c'est clairement une involution (Toronto est l'identité de $\mathbb{N}_m$!). [3]

Cette remarque faite, on introduit l'application : $F = \tau \circ f : \mathbb{N}_n \longrightarrow \mathbb{N}_m$. L'application F est injective, car c'est la composée de τ (injective car bijective) et de f (injective par hypothèse).

De plus, $F(n+1) = \tau(f(n+1)) = m$. On est ainsi ramenés au premier cas, et on peut donc conclure que $n+1 \leqslant m$.

Dans les deux cas, on a établi (sous l'hypothèse que $\mathscr{P}(n)$ est vraie) que s'il existe une application injective de $\mathbb{N}_{n+1}$ dans $\mathbb{N}_m$, alors $n+1 \leqslant m$. Ce qui prouve que la propriété $\mathscr{P}(n+1)$ est vraie. La propriété est donc initialisée et héréditaire, et on peut donc conclure.

Conclusion. S'il existe une injection de $\mathbb{N}_n$ dans $\mathbb{N}_m$, alors $n \leqslant m$.

➤ Montrons le 2). Soient n et m deux entiers naturels, et supposons qu'il existe une surjection de $\mathbb{N}_n$ dans $\mathbb{N}_m$. Notons alors $f : \mathbb{N}_n \longrightarrow \mathbb{N}_m$ une application surjective.

Soit $k \in \mathbb{N}_m$. Puisque f est surjective, $f^{-1}(\{k\})$ est non vide. Plus précisément, c'est une partie non vide de $\mathbb{N}_n$, et à ce titre elle admet un plus petit élément, disons N_k. Ce procédé, qui consiste à associer à un entier $k \in \mathbb{N}_m$ le plus petit de ses antécédents par f, donne lieu à une application :

$$\begin{aligned} g : \mathbb{N}_m &\longrightarrow \mathbb{N}_n \\ k &\longmapsto N_k \end{aligned}$$

Par construction même, on a : $f \circ g = \mathrm{id}_{\mathbb{N}_m}$. Il s'ensuit que $f \circ g$ est injective (car bijective), et donc que g est injective [4].

D'après le point 1), puisque $g : \mathbb{N}_m \longrightarrow \mathbb{N}_n$ est injective, on peut conclure que $m \leqslant n$.

Conclusion. S'il existe une surjection de $\mathbb{N}_n$ dans $\mathbb{N}_m$, alors $n \geqslant m$.

3. Nous verrons plus tard que τ est un exemple de **transposition**.

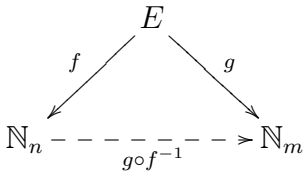
4. Car : $f \circ g$ injective implique g injective. Preuve : supposons $f \circ g$ injective. Soient x et x' tels que $g(x) = g(x')$. Alors $f(g(x)) = f(g(x'))$ d'où $x = x'$ puisque $f \circ g$ est injective. En résumé : $g(x) = g(x')$ implique $x = x'$, ce qui prouve que g est injective.

➤ Montrons le 3) (enfin un peu de repos). Soient n et m deux entiers naturels, et supposons qu'il existe une bijection de $f : \mathbb{N}_n \longrightarrow \mathbb{N}_m$. Puisque f est en particulier injective, on a $n \leqslant m$; et puisque f est en particulier surjective, on a $n \geqslant m$. Donc : $n = m$.

Conclusion. S'il existe une bijection de $\mathbb{N}_n$ dans $\mathbb{N}_m$, alors $n = m$. △

Remarque : cette propriété est particulièrement importante, puisqu'elle permet de définir (de manière unique !) le cardinal d'un ensemble fini E. En effet, un ensemble fini E est un ensemble pour lequel il existe un entier n tel que E et $\mathbb{N}_n$ sont équipotents. Le "3)" de la propriété assure l'unicité de cet entier n, ce qui autorise à l'appeler cardinal de l'ensemble E.

En effet, supposons qu'il existe deux entiers naturels n et m et deux bijections $f : E \longrightarrow \mathbb{N}_n$ et $g : E \longrightarrow \mathbb{N}_m$:



Alors l'application $g \circ f^{-1}$ est bijective (composée de deux bijections) de $\mathbb{N}_n$ dans $\mathbb{N}_m$, d'où $n = m$ d'après la propriété.

Définition 3 - Soit E un ensemble fini. On appelle **cardinal de** E l'unique entier naturel n tel que E et $\mathbb{N}_n$ sont équipotents.

Notation. On note $\mathrm{Card}\,(E)$, ou $\sharp E$ ou encore $|E|$ le cardinal d'un ensemble fini E.

Lemme 3 - Soient E un ensemble fini de cardinal $n \in \mathbb{N}^*$, et $a \in E$. Alors $E \setminus \{a\}$ 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 $E \setminus \{a\}$, que nous noterons g : $E \setminus \{a\} \longrightarrow \mathbb{N}_n$.

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 :

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

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

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 τ 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 $E \setminus \{a\} \sim \mathbb{N}_{n-1}$.

Dans les deux cas, on a établi que $E \setminus \{a\}$ 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 $E \setminus \{a\}$ est un ensemble fini de cardinal $n-1$. △

Théorème 1 - Soient E un ensemble fini, et $A \in \mathscr{P}(E)$.
Alors A est un ensemble fini, et $\text{Card}(A) \leqslant \text{Card}(E)$ (avec égalité SSI $A = E$).

Preuve. Prouvons par récurrence sur n que toute partie d'un ensemble fini à n éléments est elle-même finie, en posant :

$$\mathscr{P}(n) : \text{“si } E \text{ est fini de cardinal } n, \text{ alors toute partie } A \text{ de } E \text{ est finie et } \text{Card}(A) \leqslant \text{Card}(E)\text{”}.$$

➥ Initialisation $(n = 0)$: OK.[5]

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

Soit E un ensemble à $n+1$ éléments, et a un élément de E.

Soit A une partie de E. Deux cas peuvent alors se présenter : soit $a \in A$, soit $a \notin A$.

Premier cas — Si $a \in A$: alors l'ensemble $A \setminus \{a\}$ est une partie de l'ensemble $E \setminus \{a\}$. D'après la propriété précédente : $\text{Card}(E \setminus \{a\}) = \text{Card}(E) - 1 = n$. Ainsi $A \setminus \{a\}$ est une partie d'un ensemble à n éléments. Par hypothèse de récurrence, elle est donc finie, et : $\text{Card}(A \setminus \{a\}) \leqslant n$. Il s'ensuit que : $\text{Card}(A) \leqslant n+1$.

Second cas — Si $a \notin A$: alors l'ensemble A est une partie de l'ensemble $E \setminus \{a\}$, qui possède n éléments. Il s'ensuit, par hypothèse de récurrence, que A est finie, et que $\text{Card}(A) \leqslant n$. Puisque qui peut le plus peut le moins, on a aussi : $\text{Card}(A) \leqslant n+1$.

Dans les deux cas, on a établi que toute partie d'un ensemble à $n+1$ éléments est finie, de cardinal au plus égal à $n+1$, ce qui établit l'hérédité de la propriété.

Conclusion. Toute partie A d'un ensemble fini E est elle-même un ensemble fini, et $\text{Card}(A) \leqslant \text{Card}(E)$.

Cas d'égalité : montrons l'implication $[\text{Card}(A) = \text{Card}(E)] \Longrightarrow [A = E]$, en établissant la contraposée. Si $A \neq E$, alors il existerait $x \in E \setminus A$. On aurait donc $A \subset E \setminus \{x\}$, et par suite : $\text{Card}(A) \leqslant (n-1)$, d'où en particulier : $\text{Card}(A) \neq \text{Card}(E)$. En résumé : $[A \subsetneq E] \Longrightarrow [\text{Card}(A) \neq \text{Card}(E)]$, ce qui équivaut à : $[\text{Card}(A) = \text{Card}(E)] \Longrightarrow [A = E]$. Comme il est par ailleurs clair que : $[A = E] \Longrightarrow [\text{Card}(A) = \text{Card}(E)]$. En résumé : $[A = E] \Longleftrightarrow [\text{Card}(A) = \text{Card}(E)]$. △

5. La description des parties de l'ensemble vide étant relativement rapide.

15.2 Opérations sur les ensembles finis

Propriété 2 - Soient A et B deux parties disjointes d'un même ensemble fini E.

Alors $A \cup B$ est fini, et $\text{Card}\,(A \cup B) = \text{Card}\,(A) + \text{Card}\,(B)$

Preuve. Soient A et B deux parties disjointes d'un même ensemble fini E. On peut déjà affirmer que A et B sont des ensembles finis d'après la propriété précédente.

Débarrassons nous des cas extrêmes (et extrêmement triviaux) dans lesquels A et/ou B est vide. Si par exemple $A = \emptyset$, alors $A \cup B = B$ et $\text{Card}\,(A \cup B) = \text{Card}\,(B) = \text{Card}\,(A) + \text{Card}\,(B)$ puisque $\text{Card}\,(A) = 0\ldots$

Dans la suite des évènements, on suppose donc que A et B sont non vides. Puisque ce sont des ensembles finis (cf supra), il existe deux entiers naturels non nuls n et m et deux bijections $f : A \longrightarrow \mathbb{N}_n$ et $g : B \longrightarrow \mathbb{N}_m$.

On construit alors judicieusement une application

$$\begin{array}{rcll} F : A \cup B & \longrightarrow & \mathbb{N}_{n+m} & \\ x & \longmapsto & f(x) & \text{si } x \in A \\ x & \longmapsto & g(x) + n & \text{si } x \in B \end{array}$$

• L'application F est bien définie car A et B sont disjoints. Explicitement, si x appartient à $A \cup B$, alors $x \in A$ ou (exclusif) $x \in B$, et son image par F est donc définie de manière unique.

• Montrons l'injectivité de F : soient x et y deux éléments de $A \cup B$ tels que $F(x) = F(y)$ (♠). Trois cas peuvent se présenter :

➥ Si $x \in A$ et $y \in A$: alors (♠) implique $f(x) = f(y)$ d'où $x = y$ puisque f est injective.

➥ Si $x \in B$ et $y \in B$: alors (♠) implique $g(x) + n = g(y) + n$ d'où $g(x) = g(y)$ d'où $x = y$ puisque g est injective.

➥ Si $x \in A$ et $y \in B$: alors (♠) implique $f(x) = g(y) + n$. Or $f(x) \leqslant n$ (par construction de f) tandis que $g(y) + n > n$. L'égalité $f(x) = g(y) + n$ ne peut donc en aucun cas être vérifiée.

En résumé : $\forall\ (x, y) \in (A \cup B)^2,\ [F(x) = F(y)] \Longrightarrow [x = y]$. L'application F est donc injective.

• Montrons la surjectivité de F : soit N un entier de $\mathbb{N}_{n+m}$. Deux cas se présentent : soit $N \in \mathbb{N}_n$, soit $N \in [\![\, n+1, n+m \,]\!]$.

➥ Si $N \in \mathbb{N}_n$: l'application f étant bijective, il existe un élément $a \in A$ tel que $f(a) = N$, d'où $F(a) = N$.

➥ Si $N \in [\![\, n+1, n+m \,]\!]$: alors $N - n \in \mathbb{N}_m$. L'application g étant bijective, il existe un élément $b \in B$ tel que $g(b) = N - n$, d'où $g(b) + n = N$ d'où encore $F(b) = N$.

On a donc établi que : $\forall\, N \in \mathbb{N}_{n+m},\ \exists\, x \in A \cup B,\ F(x) = N$. Ce qui assure que F est surjective.

• Par suite, l'application F est bijective, donc $A \cup B$ et $\mathbb{N}_{n+m}$ sont équipotents, donc $\text{Card}\,(A \cup B) = n+m$.

Conclusion. Soient A et B deux parties disjointes d'un même ensemble fini E. Alors l'ensemble $A \cup B$ est fini et $\text{Card}\,(A \cup B) = \text{Card}\,(A) + \text{Card}\,(B)$. △

Corollaire 1 - Soit A une partie d'un ensemble fini E.
Alors $\bar{A}$ est un ensemble fini, et : $\text{Card}\,((E\backslash A)) = \text{Card}\,(E) - \text{Card}\,(A)$.

Preuve. Il résulte encore une fois du théorème 1 que les ensembles A et $(E\backslash A)$ sont finis.

Par ailleurs, on peut observer que A et $(E\backslash A)$ sont disjoints, et que $E = A \cup (E\backslash A)$. On déduit de la première observation que $\text{Card}\,(A \cup (E\backslash A)) = \text{Card}\,(A) + \text{Card}\,((E\backslash A))$ et de la seconde que $\text{Card}\,(A \cup (E\backslash A)) = \text{Card}\,(E)$. La conclusion provient directement de ces deux égalités. △

Corollaire 2 - Soient $n \in \mathbb{N}^*$ et $(A_i)_{i\in[\![1,n]\!]}$ une famille de parties de E, deux à deux disjointes (c'est à dire : $\forall\,(i,j) \in \mathbb{N}_n^2,\ (i \neq j) \Rightarrow (A_i \cap A_j = \emptyset)$). On a :

$$\text{Card}\left(\bigcup_{i=1}^{n} A_i\right) = \sum_{i=1}^{n} \text{Card}\,(A_i)$$

Preuve. Prouvons la propriété par récurrence sur n, en posant :

$\mathscr{P}(n)$: "si $(A_i)_{i\in[\![1,n]\!]}$ est une famille de parties de E deux à deux disjointes, alors : $\text{Card}\left(\bigcup_{i=1}^{n} A_i\right) = \sum_{i=1}^{n} \text{Card}\,(A_i)$".

➥ Initialisation $(n = 1)$: OK.

➥ Hérédité : supposons la propriété établie jusqu'à un certain entier naturel non nul n, et montrons que $\mathscr{P}(n+1)$ est vraie.

Soit $(A_i)_{i\in[\![1,n+1]\!]}$ une famille de parties de E deux à deux disjointes. On a : $\bigcup_{i=1}^{n+1} A_i = \left(\bigcup_{i=1}^{n} A_i\right) \cup A_{n+1}$.
Cette union est disjointe, car :

$$\left(\bigcup_{i=1}^{n} A_i\right) \cap A_{n+1} = \left(\bigcup_{i=1}^{n} \underbrace{A_i \cap A_{n+1}}_{=\emptyset \text{ (par H)}}\right) = \emptyset$$

On a donc : $\text{Card}\left(\left(\bigcup_{i=1}^{n} A_i\right) \cup A_{n+1}\right) = \text{Card}\left(\bigcup_{i=1}^{n} A_i\right) + \text{Card}\,(A_{n+1})$ (propriété 3) puis :

$$\text{Card}\left(\left(\bigcup_{i=1}^{n} A_i\right) \cup A_{n+1}\right) = \left[\sum_{i=1}^{n} \text{Card}\,(A_i)\right] + \text{Card}\,(A_{n+1})\ \text{(HR)}.$$

D'où : $\text{Card}\left(\bigcup_{i=1}^{n+1} A_i\right) = \sum_{i=1}^{n+1} \text{Card}\,(A_i)$, ce qui prouve que $\mathscr{P}(n+1)$ est vraie, et achève la preuve de l'hérédité.

Conclusion. Soient $n \in \mathbb{N}^*$ et $(A_i)_{i\in[\![1,n]\!]}$ une famille de parties de E, deux à deux disjointes.

On a : $\text{Card}\left(\bigcup_{i=1}^{n} A_i\right) = \sum_{i=1}^{n} \text{Card}\,(A_i)$ △

Corollaire 3 - Soient A et B deux parties d'un même ensemble E. On a :

$$\text{Card}\,(A\cup B)=\text{Card}\,(A)+\text{Card}\,(B)-\text{Card}\,(A\cap B)$$

Preuve. Soient A et B deux parties d'un ensemble fini. On a : $A\cup B=(A\backslash B)\cup B$. Dans le terme de droite de cette égalité, l'union est disjointe, et la propriété 3 permet donc d'affirmer que : $\text{Card}\,(A\cup B)=\text{Card}\,(A\backslash B)+\text{Card}\,(B)$ (♠).

Par ailleurs : $A=(A\backslash B)\cup(A\cap B)$, et puisque cette union est encore disjointe, une nouvelle application de la propriété 2 page 6 donne : $\text{Card}\,(A)=\text{Card}\,(A\backslash B)+\text{Card}\,(A\cap B)$ (♣)

On déduit de (♠) et (♣) que : $\boxed{\text{Card}\,(A\cup B)=\text{Card}(A)+\text{Card}(B)-\text{Card}\,(A\cap B)}$. △

Propriété 3 - Soient E et F deux ensembles finis. On a :

1/ $E\times F$ est fini, et $\text{Card}\,(E\times F)=\text{Card}\,(E)\times\text{Card}\,(F)$

2/ Pour tout $n\in\mathbb{N}^*$, E^n est fini et $\text{Card}\,(E^n)=[\text{Card}(E)]^n$

3/ F^E est fini, et $\text{Card}\left(F^E\right)=\text{Card}\,(F)^{\text{Card}(E)}$

Preuve. Preuve de 1/ : puisque nous sommes entre nous, on peut supposer que $E=\{x_1,\ldots,x_n\}$ et $F=\{y_1,\ldots,y_m\}$ où l'on a noté n et m les cardinaux respectifs de E et F.

Alors $E\times F$ est l'ensemble des couples (x_i,y_j) obtenus en faisant parcourir $\mathbb{N}_n$ à l'indice i, et $\mathbb{N}_m$ à l'indice j. Il est clair que l'on obtient ainsi nm éléments distincts. D'où $\text{Card}\,(E\times F)=nm$, c'est à dire : $\boxed{\text{Card}\,(E\times F)=\text{Card}\,(E)\times\text{Card}\,(F)}$.

Preuve de 2/ : la preuve peut s'obtenir via une récurrence aisée sur n, l'hérédité provenant du fait que $E^{n+1}=E^n\times E$ et du point 1/.

Preuve de 3/ : notons encore une fois n le cardinal de E et m celui de f. Une application f de E dans F est uniquement déterminée par les images des éléments de E. En d'autres termes, f est définie de manière unique par $f(x_i)$ (avec $i\in\mathbb{N}_n$). Or pour chacune de ces n valeurs (qui sont des éléments de F), on a m choix possibles. On obtiendra donc m^n façons différentes de définir une application de E dans F. D'où : $\text{Card}\left(F^E\right)=m^n$, c'est à dire : $\boxed{\text{Card}\left(F^E\right)=\text{Card}\,F^{\text{Card}\,E}}$. △

Théorème 2 - Soient E et F deux ensembles finis, et $f:E\longrightarrow F$ une application.

Alors $f(E)$ est un ensemble fini, et $\text{Card}\,(f(E))\leqslant\text{Card}\,(E)$.

En outre, f est injective SSI $\text{Card}\,(f(E))=\text{Card}\,(E)$.

Preuve. Notons $E=\{x_1,\ldots,x_n\}$ où $n\in\mathbb{N}^*$ désigne le cardinal de E (on pourra laisser de côté le cas extrême où $E=\emptyset$).

Alors $f(E)=\{f(x_1),\ldots,f(x_n)\}$ et il est clair que cet ensemble possède au plus n éléments, ce qui assure déjà que : $\text{Card}\,(f(E))\leqslant\text{Card}\,(E)$.

Plus précisément, $\text{Card}\,(f(E))=n$ si et seulement si les $f(x_i)$ sont deux à deux distincts, c'est à dire si et seulement si l'application f est injective, ce qui achève la preuve du théorème. △

Remarques : dans cet énoncé, seule la finitude de l'ensemble E intervient, et l'hypothèse "F fini" est donc superflue.

Par ailleurs, le théorème tient toujours dans le cas particulier où $E = \emptyset$, même si elle peut paraître un peu "étrange". Explicitement, un ensemble F étant donné il existe une unique application $f : \emptyset \longrightarrow F$ (parfois appelée application vide), l'application qui "n'associe rien à personne". Dans ce contexte, $f(\emptyset) = \emptyset$, et on a donc : $\text{Card}(f(\emptyset)) = \text{Card}(\emptyset) = 0$; ce qui ne doit pas nous surprendre, puisque l'application vide est injective. [6]

Corollaire 4 - Soient E et F deux ensembles finis, et $f : E \longrightarrow F$ une application. On suppose $\textbf{Card}(E) = \textbf{Card}(F)$. LASSE :

1/ f est bijective

2/ f est injective

3/ f est surjective

Remarque *: il est bon d'observer que l'énoncé ci-dessus est en général complètement faux sans l'hypothèse d'égalité des cardinaux.*

Preuve. 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, ça ne mange pas de pain. En outre, puisque f est injective, $f(E)$ est un ensemble fini, de cardinal égal à celui de E (en vertu du théorème 2). 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 $f(E) = F$ (théorème 1 page 5). 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 (grâce au théorème 2 page 8) que f est injective, et donc bijective. Ce qui prouve l'implication, et achève la preuve du théorème. △

15.3 Injections et permutations

Lemme 4 - 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.

6. En effet, pour tout couple (x, y) de $\emptyset \times \emptyset$, la condition $f(x) = f(y)$ implique $x = y$ est vérifiée...

Supposons maintenant $p \leqslant n$, et notons $E = \{x_1, \ldots, x_p\}$. Pour définir une application f, on peut choisir successivement les valeurs de $f(x_1), \ldots, f(x_p)$. 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 $f(x_2), \ldots, (n-p+1)$ 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. △

Définition 4 - Soient n un entier naturel non nul, $p \in [\![1, n]\!]$ et E un ensemble de cardinal n.

Un **arrangement** de p éléments de E est un p-uplet d'éléments distincts de E.

Exemples. Soit $E = \{1, 2, 3, 4\}$. Les triplets $(4, 2, 1)$ et $(1, 4, 2)$ sont des arrangements de E. Bien qu'ils contiennent les mêmes éléments, ils sont distincts, puisque dans un triplet l'ordre doit être pris en compte. Ici réside la différence fondamentale entre arrangements et combinaisons : les premiers sont ordonnés, tandis que les secondes ne le sont pas. Pour enfoncer le clou : les arrangements $(2, 3)$ et $(3, 2)$ sont distincts ; alors que $\{2, 3\}$ et $\{3, 2\}$ sont la même combinaison.

Définition 5 - Soit E un ensemble. Une **permutation** de E est une bijection de E dans E.

Exemples. L'application $x \longmapsto x^3$ est une permutation de $\mathbb{R}$. L'application $k \longmapsto 6-k$ est une permutation de $\mathbb{N}_5$. L'application qui à 1 associe 2, à 2 associe 3, et à 3 associe 1 est une permutation de $\mathbb{N}_3$.

Notation. Soit E un ensemble. On note S_E l'ensemble des permutations de E.

Théorème 3 - Si E est un ensemble fini de cardinal n, alors $(S_E, \circ)$ est un groupe fini de cardinal $n!$.

Preuve. Un élément de S_E est une bijection de E dans E. En vertu du corollaire 4 page 9, il existe autant de bijections de E dans E que d'injections de E dans E (puisque E est fini). Or d'après le lemme 4 page 9, il existe exactement $n!$ injections de E dans E.

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, puisque 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 une bijection de E dans E, sa réciproque f^{-1} est elle aussi une bijection de E dans E.

Ce qui prouve que $(S_E, \circ)$ est un groupe, et achève cette preuve. △

15.4 Groupe symétrique

15.4.1 Généralités

Définition 6 - Soit n un entier naturel non nul. On note S_n (ou $(S_n, \circ)$) et on appelle **groupe symétrique** l'ensemble des permutations de $\mathbb{N}_n$.

Une conséquence directe du théorème 3 est la :

Propriété 4 - Pour tout entier naturel non nul n, $(S_n, \circ)$ est un groupe fini de cardinal $n!$.

Preuve. C'est un cas particulier du théorème 3, appliqué à l'ensemble $E = \mathbb{N}_n$. △

Convention. *Dans la suite des évènements, on notera* ***multiplicativement*** *la lci de S_n. Explicitement, si σ et τ désignent deux permutations, on parlera du produit $\sigma\tau$ pour désigner la composée $\sigma \circ \tau$.*

Exemples. $S_1 = \{\mathrm{id}\}$ est le groupe à un élément ; $S_2 = \{\mathrm{id}_{\mathbb{N}_2}, (12)\}$ est le groupe à deux éléments. Tous deux sont abéliens.

En revanche, $S_3 = \{\mathrm{id}, (12), (13), (23), (123), (132)\}$ est un groupe à 6 éléments, non abélien (voir plus loin ou chapitre 11).

15.4.2 Transpositions et p-cycles

Définition 7 - Soit $n \geqslant 2$ un entier, et soient i et j deux éléments distints de $\mathbb{N}_n$. On définit une application de $\mathbb{N}_n$ dans $\mathbb{N}_n$, que l'on note (ij) en posant :

$$\forall k \in \mathbb{N}_n,\ (ij)(k) = \begin{cases} j & \text{si } k = i \\ i & \text{si } k = j \\ k & \text{si } k \neq i \text{ et } k \neq j \end{cases}$$

Une telle application est appelée **transposition**.

Des exemples de transpositions de $\mathbb{N}_3$ ont déjà été utilisés dans le chapitre 11 sur les groupes, pour établir que le groupe S_3 (de cardinal 6) est non abélien.

Propriété 5 - Une transposition est une involution (et donc une permutation).

Preuve. Soient n un entier naturel supérieur ou égal à 2, et i et j deux entiers distincts de $\mathbb{N}_n$. Considérons la transposition (ij), c'est à dire pour mémoire l'application définie sur $\mathbb{N}_n$ et à valeurs dans $\mathbb{N}_n$ en posant :

$$\forall k \in \mathbb{N}_n,\ (ij)(k) = \begin{cases} j & \text{si } k = i \\ i & \text{si } k = j \\ k & \text{si } k \neq i \text{ et } k \neq j \end{cases}$$

Soit k un élément de $\mathbb{N}_n$.

➥ Si $k \neq i$ et $k \neq j$: alors $[(ij)(ij)](k) = (ij)((ij)(k)) = (ij)(k) = k$.

➥ Si $k = i$: alors $[(ij)(ij)](i) = (ij)((ij)(i)) = (ij)(j) = i$.

➥ Si $k = j$: alors $[(ij)(ij)](j) = (ij)((ij)(j)) = (ij)(i) = j$.

On a donc établi que : $\forall k \in \mathbb{N}_n,\ [(ij)(ij)](k) = k$, ce qui signifie que $(ij)(ij) = \mathrm{id}_{\mathbb{N}_n}$.

Ainsi la transposition (ij) est une involution, et par conséquent une permutation de $\mathbb{N}_n$ (donc un élément de S_n). △

Lemme 5 - Soient $n \geqslant 3$ un entier ; et i, j et k trois entiers distincts dans $\mathbb{N}_n$. Alors :

$$(ij)(jk) \neq (jk)(ij)$$

Preuve. Calculons l'image de i par chacune des deux permutations intervenant dans l'énoncé.

D'une part : $[(ij)(jk)](i) = (ij)(i) = j$ et d'autre part $[(jk)(ij)](i) = (jk)(j) = k$.

Puisque les images de i par $(ij)(jk)$ et $(jk)(ij)$ sont distinctes ($i \neq k$ par hyp), on peut affirmer que les applications $(ij)(jk)$ et $(jk)(ij)$ sont distinctes, ce qu'il fallait établir. △

Corollaire 5 - Le groupe symétrique S_n est non abélien dès que $n \geqslant 3$.

Preuve. Conséquence directe du lemme précédent. △

Définition 8 - Soient $n \geqslant 2$ un entier, et p un entier tel que $2 \leqslant p \leqslant n$. Soient encore $a_1, \ldots, a_p$ p éléments distincts de $\mathbb{N}_n$. On définit une application de $\mathbb{N}_n$ dans $\mathbb{N}_n$, que l'on note $(a_1 a_2 \cdots a_p)$ en posant :

$$\begin{cases} \forall\, i \in \mathbb{N}_{p-1},\ (a_1 a_2 \cdots a_p)(a_i) = a_{i+1} \\ (a_1 a_2 \cdots a_p)(a_p) = a_1 \\ \forall\, k \in \mathbb{N}_n \setminus \{a_1, \ldots, a_p\},\ (a_1 a_2 \cdots a_p)(k) = k \end{cases}$$

Une telle application est appelée un **p-cycle** ; l'ensemble $\{a_1, a_2, \ldots, a_p\}$ est appelé son **support**.

Propriété 6 - Un p-cycle est une permutation. En outre, avec les notations introduites plus haut :

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

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

➥ Si $k \notin \{a_1, \ldots, a_p\}$: 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 $k \in \{a_1, \ldots, a_{p-1}\}$: 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 : $\forall\, k \in \mathbb{N}_n$,

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

A'r'cominche, din l'aut'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 :

$$[(a_1a_2\cdots a_p)(a_pa_{p-1}\cdots a_1)](k) = (a_1a_2\cdots a_p)(a_pa_{p-1}\cdots a_1)((a_1)) = (a_1a_2\cdots a_p)(a_p) = a_1$$

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

$$[(a_1a_2\cdots a_p)(a_pa_{p-1}\cdots a_1)](k) = k, \text{ soit : } (a_1a_2\cdots a_p)(a_pa_{p-1}\cdots a_1) = \mathrm{id}_{\mathbb{N}_n}.$$

Conclusion. D'après les calculs précédents : $(a_pa_{p-1}\cdots a_1)(a_1a_2\cdots a_p) = \mathrm{id}_{\mathbb{N}_n}$ et $(a_1a_2\cdots a_p)(a_pa_{p-1}\cdots a_1) = \mathrm{id}_{\mathbb{N}_n}$. Par suite, l'application $(a_1a_2\cdots a_p)$ est une bijection de $\mathbb{N}_n$ dans $\mathbb{N}_n$; c'est donc une permutation, d'inverse $(a_pa_{p-1}\cdots a_1)$ dans S_n. △

Remarque. Deux cycles sont à **supports disjoints** lorsque... leurs supports sont disjoints (pas d'applaudissements !). Deux cycles à supports disjoints commutent.

Exemples. Une transposition est un 2-cycle. Tous les éléments (distincts de l'identité) du groupe S_3 sont des cycles. En revanche, dans S_4, il existe des permutations qui ne sont pas des cycles, comme par exemple le produit $(12)(34)$.

Propriété 7 - Mêmes notations que plus haut. On a :

$$(a_1a_2\cdots a_p) = \prod_{i=1}^{p-1}(a_ia_{i+1})$$

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

➥ Si $k \notin \{a_1, \ldots, a_p\}$: alors $(a_1a_2\cdots a_p)(k) = k$ puisque k n'appartient pas au support du cycle, et $\left[\prod_{i=1}^{p-1}(a_ia_{i+1})\right](k) = k$ puisque k n'appartient au support d'aucune transposition (a_ia_{i+1}) du produit.

D'où : $$\forall k \in \mathbb{N}_n,\ k \notin \{a_1, \ldots, a_p\},\ \left[\prod_{i=1}^{p-1}(a_ia_{i+1})\right](k) = (a_1a_2\cdots a_p)(k)$$

➥ 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 :

$$(a_1a_2\cdots a_p)(k) = (a_1a_2\cdots a_p)(a_m) = a_{m+1}$$

Et d'autre part :

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

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

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 :

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

$$= \cdots = \left[\left(\prod_{i=1}^{2}(a_i a_{i+1})\right)\right](a_3) = (a_1 a_2)(a_2) = a_1 \qquad \text{D'où : } \boxed{\left[\prod_{i=1}^{p-1}(a_i a_{i+1})\right](a_p) = (a_1 a_2 \cdots a_p)(a_p)}$$

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.

Les transpositions constituent donc les "briques élémentaires de S_n", dans un sens rendu plus précis par le théorème suivant :

Théorème 4 - (Version courte). Les transpositions engendrent le groupe symétrique.

Ou, le même en plus explicite :

Théorème 5 - (Version longue du théorème 4). Soit n un entier naturel supérieur ou égal à 2, et soit $\sigma \in S_n$.

Il existe un entier $k \leqslant n$, et k transpositions $\tau_1, \ldots, \tau_k$ de S_n tels que : $\sigma = \prod_{i=1}^{k} \tau_i$.

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 $k \leqslant n$ et k transpositions $\tau_1, \ldots, \tau_k$ de S_n tels que : $\sigma = \prod_{i=1}^{k} \tau_i$"

➥ Initialisation ($n = 2$) : 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.

➥ Hérédité : 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 $\sigma(n+1) \neq n+1$.

Premier cas — Si $\sigma(n+1) = n+1$: dans ce cas, la restriction $\sigma_{|\mathbb{N}_n}$ est une permutation de $\mathbb{N}_n$. Par hypothèse de récurrence, il existe un entier $k \leqslant n$ et k transpositions $\tau_1, \ldots, \tau_k$ de S_n tels que : $\sigma_{|\mathbb{N}_n} = \prod_{i=1}^{k} \tau_i$. 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 : $\sigma = \prod_{i=1}^{k} \tau_i$ (égalité dans S_{n+1}). Ainsi, sous l'hypothèse $\sigma(n+1) = n+1$, il existe un entier $k \leqslant n$ (en particulier $k \leqslant n+1$) et k transpositions $\tau_1, \ldots, \tau_k$ de S_{n+1} tels que : $\sigma = \prod_{i=1}^{k} \tau_i$.

Second cas — Si $\sigma(n+1) \neq n+1$: dans ce cas, on introduit la permutation $\rho = (\sigma(n+1)\ \ n+1)\,\sigma$.[7]

ρ 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 $k \leqslant n$ et k transpositions $\tau_1, \ldots, \tau_k$ de S_{n+1} tels que : $\rho = \prod_{i=1}^{k} \tau_i$. Par suite, on a : $\sigma = (\sigma(n+1)\ \ n+1) \prod_{i=1}^{k} \tau_i$. La permutation σ est ainsi écrite comme produit de $k+1$ transpositions (et $k+1 \leqslant n+1$).

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

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

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

Remarque *: le théorème est encore valable pour $n = 1$, puisque tout élément de S_1 (c'est à dire la seule identité) s'écrit comme produit de zéro transposition...*

Théorème 6 - 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 σ 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[8] : $\sigma = \tau c_1 \cdots c_k$.

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 σ.

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. △

8. En multipliant à gauche par τ les deux termes de l'égalité précédente.

15.4.3 Signature et groupe alterné

Définition 9 - Soit $n \geqslant 2$ un entier, et $(i,j) \in \mathbb{N}_n^2$ avec $i < j$. Une permutation $\sigma \in S_n$ réalise une **inversion** du couple (i,j) si $\sigma(i) > \sigma(j)$.

Notation. On note $\mathrm{I}(\sigma)$ le nombre de couples sur lesquels σ réalise une inversion.

Exemples. $\mathrm{I}(\mathrm{id}) = 0$.

Dans S_3, considérons la transposition $\tau(12)$. On a : $\tau(1) > \tau(2)$ (une inversion) ; $\tau(1) < \tau(3)$ (pas d'inversion) ; $\tau(2) < \tau(3)$ (pas d'inversion) ; par suite $\mathrm{I}((12)) = 1$.

Toujours dans S_3, considérons à présent la transposition $\tau(13)$. On a : $\tau(1) > \tau(2)$ (une inversion) ; $\tau(1) > \tau(3)$ (une inversion) ; $\tau(2) > \tau(3)$ (une inversion) ; par suite $\mathrm{I}((13)) = 3$.

Définition 10 - Soit $\sigma \in S_n$. La **signature de** σ est le réel $\varepsilon(\sigma) = (-1)^{\mathrm{I}(\sigma)}$

Définition 11 - Soit $\sigma \in S_n$. Il résulte de la définition précédente que la signature de σ vaut 1 ou (-1). La permutation σ sera dite **paire** (*resp.* **impaire**) lorsque $\varepsilon(\sigma) = 1$ (*resp.* $\varepsilon(\sigma) = -1$)

Théorème 7 - $\forall\, (\sigma,\tau) \in S_n^2,\ \varepsilon(\sigma\tau) = \varepsilon(\sigma)\varepsilon(\tau)$

Preuve. Soient σ et τ 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 :

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

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

$$(-1)^{\mathrm{I}(\sigma\tau)} = (-1)^{\mathrm{I}(\sigma)+\mathrm{I}(\tau)} \Longleftrightarrow (-1)^{\mathrm{I}(\sigma\tau)} = (-1)^{\mathrm{I}(\sigma)}(-1)^{\mathrm{I}(\tau)} \Longleftrightarrow \boxed{\varepsilon(\sigma\tau) = \varepsilon(\sigma)\varepsilon(\tau)}$$ △

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 ε de $\sigma \circ \tau$ est égal au produit des images $\varepsilon(\sigma) \times \varepsilon(\tau)$.

Propriété 8 - La signature d'une transposition vaut -1.

Preuve. Soient n un entier supérieur ou égal à 2, et τ une transposition dans S_n. Par définition de transposition, il existe deux entiers i et j tels que $1 \leqslant i < j \leqslant n$ et $\tau = (ij)$. On peut représenter τ de la manière suivante :

$$\begin{pmatrix} 1 & 2 & \cdots & i & \cdots & j & \cdots & n \\ 1 & 2 & \cdots & j & \cdots & i & \cdots & n \end{pmatrix}$$

On compte alors le nombre d'inversions réalisées sur les couples (k,m) où k allant de 1 à $n-1$ et $m>k$:

$$\mathrm{I}(\tau)=\underbrace{0}_{k=1}+\cdots+\underbrace{0}_{k=i-1}+\underbrace{j-i}_{k=i}+\underbrace{1}_{k=i+1}+\cdots+\underbrace{1}_{k=j-1}+\underbrace{0}_{k=j}+\cdots+\underbrace{0}_{k=n}$$

D'où : $\mathrm{I}(\tau)=j-i+j-i-1=2(j-i)-1$. Puisque $\mathrm{I}(\tau)$ est impair, on a $(-1)^{\mathrm{I}(\tau)}=-1$, càd $\varepsilon(\tau)=-1$.

Conclusion. La signature d'une transposition est égale à -1. △

Et puisque tout p-cycle est en particulier un produit de $p-1$ transpositions, on peut affirmer que :

Corollaire 6 - La signature d'un p-cycle vaut $(-1)^{p-1}$.

Preuve. Soit $C=(a_1a_2\cdots a_p)$ un p-cycle. D'après le théorème 4, C est produit de $p-1$ transpositions ; il existe $\tau_1,\ldots,\tau_{p-1}$ tels que $C=\prod_{i=1}^{p-1}\tau_i$.

Donc, d'après le théorème 7[9] : $\varepsilon(C)=\prod_{i=1}^{p-1}\varepsilon(\tau_i)$

D'où, d'après la propriété 8 $\varepsilon(C)=\prod_{i=1}^{p-1}(-1)$ soit : $\boxed{\varepsilon((a_1a_2\cdots a_p))=(-1)^{p-1}}$

△

Enfin :

Corollaire 7 - Pour toute permutation $\sigma\in S_n$, on a : $\varepsilon(\sigma^{-1})=\varepsilon(\sigma)$.

Preuve. Pour toute permutation σ de S_n, $\sigma^{-1}\sigma=\mathrm{id}_{\mathbb{N}_n}$. D'où : $\varepsilon(\sigma^{-1}\sigma)=\sigma(\mathrm{id}_{\mathbb{N}_n})$. Par suite : $\varepsilon(\sigma^{-1})\varepsilon(\sigma)=1$. On déduit de cette égalité que $\varepsilon(\sigma)$ et $\varepsilon(\sigma^{-1})$ sont simultanément égaux à 1 ou simultanément égaux à -1.

En tous les cas : $\boxed{\varepsilon(\sigma^{-1})=\varepsilon(\sigma)}$. △

La conséquence la plus importante de ce dernier corollaire étant l'énoncé ci-dessous.

Propriété 9 - (Propriété - Définition). On note A_n l'ensemble des permutations paires de S_n.
$(A_n,\circ)$ est un sous-groupe de $(S_n,\circ)$, appelé **groupe alterné**.
C'est en particulier un groupe fini, et : $\mathrm{Card}(A_n)=\dfrac{n!}{2}$.

Preuve. ➥ (SG1) : par définition même de A_n (c'est l'ensemble des permutations paires), on a $\boxed{A_n\subset S_n\ (\spadesuit)}$

➥ (SG2) : $\mathrm{id}_{\mathbb{N}_n}$, qui est l'élément neutre de $(S_n,\circ)$, est une permutation paire puisque $\varepsilon(\mathrm{id}_{\mathbb{N}_n})=1$. Ainsi : $\boxed{\mathrm{id}_{\mathbb{N}_n}\in A_n\ (\heartsuit)}$

9. Plus précisément, le théorème 7 permet d'établir par une récurrence facile sur n que pour une famille de n permutations $(\sigma_i)_{i\in\mathbb{N}_n}$, on a : $\varepsilon\left(\prod_{i=1}^{n}\sigma_i\right)=\prod_{i=1}^{n}\varepsilon(\sigma_i)$.

➥ **(SG3)** : soient σ et τ deux permutations paires. Alors $\varepsilon(\sigma\tau) \underbrace{=}_{\text{th. 7}} \underbrace{\varepsilon(\sigma)}_{=1 \text{ car } \sigma\in A_n} \underbrace{\varepsilon(\tau)}_{=1 \text{ car } \tau\in A_n} = 1$. D'où : $\sigma\tau \in A_n$.
Par conséquent : $\boxed{\forall\,(\sigma,\tau)\in A_n^2,\ \sigma\tau\in A_n\ \ (\diamondsuit)}$

➥ **(SG4)** : soit $\sigma \in A_n$. Alors $\varepsilon(\sigma)=1$, donc $\varepsilon(\sigma^{-1})=1$ en vertu du corollaire 7. Par suite : $\sigma^{-1}\in A_n$.

D'où : $\boxed{\forall\sigma\in A_n,\ \sigma^{-1}\in A_n\ \ (\clubsuit)}$

On déduit de ($\spadesuit$), ($\heartsuit$), ($\diamondsuit$) et ($\clubsuit$) que $\boxed{(A_n,\circ) \text{ est un sous-groupe de } (S_n,\circ)}$.

Assertion concernant le cardinal : par définition de A_n (et de S_n), l'ensemble S_n est la réunion disjointe de A_n et de $S_n\backslash A_n$. D'où : $\text{Card}(S_n) = \text{Card}(A_n)+\text{Card}(S_n\backslash A_n)$, ainsi : $\boxed{\text{Card}(A_n)+\text{Card}(S_n\backslash A_n)=n!\ \ (\spadesuit)}$.

D'autre part, l'application : $F : \sigma\in A_n \longmapsto (12)\,\sigma \in S_n\backslash A_n$ et l'application : $G : \sigma\in S_n\backslash A_n \longmapsto (12)\,\sigma\in A_n$ sont clairement réciproques l'une de l'autre. En particulier, elles sont bijectives ce qui implique : $\boxed{\text{Card}(A_n)=\text{Card}(S_n\backslash A_n)\ \ (\clubsuit)}$.

On déduit de ($\spadesuit$) et de ($\clubsuit$) que : $\boxed{\text{Card}(A_n)=\dfrac{n!}{2}}$. △

Remarque : une preuve plus rapide de la propriété précédente : A_n est l'ensemble des antécédents de l'élément neutre (1) par le morphisme de groupes $\varepsilon : (S_n,\circ) \longrightarrow (\{\pm 1\},\times)$. C'est (par définition) le noyau de ce morphisme. Or le noyau d'un morphisme de groupes est toujours un sous-groupe du groupe de départ. D'où la propriété.

Index