Thm/Def 1 : L'unicité découle du Lemme suivant :

Lemme 0 : 1▸ $n \leq m \iff \exists f : [\![1,n]\!] \hookrightarrow [\![1,m]\!]$

2▸ $n \geq m \iff \exists f : [\![1,n]\!] \twoheadrightarrow [\![1,m]\!]$

3▸ $n = m \iff \exists f : [\![1,n]\!] \hookrightarrow\!\!\!\!\rightarrow [\![1,m]\!]$

4▸ $f : [\![1,n]\!] \longrightarrow [\![1,n]\!]$ est une injection ssi c'est une bijection.

(notation : $f : A \hookrightarrow B$ (resp. $f : A \twoheadrightarrow B$, resp. $f : A \hookrightarrow\!\!\!\!\rightarrow B$) signifie que f est une injection (resp. surjection), resp. bijection) de A dans B)

Preuve : 1▸ ▸ Si $n \leq m$, alors l'inclusion convient.

▸ Soit $m \in \mathbb{N}$. Pour $k \in [\![1,p]\!]$, il existe $\theta_k : [\![1,p]\!] \hookrightarrow\!\!\!\!\rightarrow [\![1,p]\!]$ telle que $\theta_k(k) = p$ (la transposition (k,p) par exemple). Sachant cela, montrons le résultat par récurrence sur n :

• $n = 0$: $0 \leq m$, c'est immédiat.

• Soit $n \in \mathbb{N}$ rendant vraie l'implication. Soit $f : [\![1,n+1]\!] \hookrightarrow [\![1,m]\!]$. Remarquons que nécessairement $m \geq 1$ puisque $[\![1,n+1]\!] \neq \emptyset$. Quitte à remplacer f par $\theta \circ f$ où $\theta : [\![1,m]\!] \hookrightarrow\!\!\!\!\rightarrow [\![1,m]\!]$ telle que $\theta(f(n+1)) = m$, supposons que $f(n+1) = m$. Alors $f_{|[\![1,n]\!]} : [\![1,n]\!] \hookrightarrow [\![1,m-1]\!]$, donc par hypothèse de récurrence, $n \leq m-1$, donc $n+1 \leq m$.

2▸ Montrons le résultat par récurrence sur m :

• $m = 0$: $n \geq 0$, c'est immédiat.

• Soit $m \in \mathbb{N}$ rendant vraie l'implication. Soit $f : [\![1,n]\!] \twoheadrightarrow [\![1,m+1]\!]$. Remarquons que nécessairement $n \geq 1$ puisque $[\![1,m+1]\!] \neq \emptyset$ (la surjectivité de f s'écrit $\forall y \in [\![1,m+1]\!], \exists x \in [\![1,n]\!] : f(x) = y$. Comme $[\![1,m+1]\!] \neq 0$, il faut que $[\![1,n]\!] \neq \emptyset$ pour que cette proposition soit vraie). Quitte à remplacer f par $f \circ \theta$ où $\theta : [\![1,n]\!] \hookrightarrow\!\!\!\!\rightarrow [\![1,n]\!]$, supposons que $f^{-1}(\{m+1\}) = [\![p,n]\!]$ ($p \in [\![1,n]\!]$). Alors $f_{|[\![1,p-1]\!]} : [\![1,p-1]\!] \twoheadrightarrow [\![1,m]\!]$, donc par par hypothèse de récurrence, $n-1 \geq p-1 \geq m$, donc $n \geq m+1$.

3▸ ▸ On applique 1▸ à f et f^{-1} pour montrer que $n \leq m \leq n$.

▸ Si $n = m$, alors l'identité convient.

4▸ La réciproque est évidente. Montrons l'implication directe par récurrence sur n :

• $n = 0$: Soit $f : [\![1,0]\!] = \emptyset \hookrightarrow [\![1,0]\!] = 0$. Alors $\forall y \in \emptyset, \exists! x \in \emptyset : f(x) = y$, i.e. f est bijective (NB : $\forall x \in \emptyset$, $\mathcal{P}$ est toujours vraie, qu'importe $\mathcal{P}$).

• Soit $n \in \mathbb{N}$ rendant l'implication vraie. Soit $f : [\![1,n+1]\!] \hookrightarrow [\![1,n+1]\!]$. Il existe $\theta : [\![1,n+1]\!] \hookrightarrow\!\!\!\!\rightarrow [\![1,n+1]\!]$ telle que $\theta \circ f(n+1) = n+1$. De là, $\theta \circ f$ induit une injection de $[\![1,n]\!]$ dans $[\![1,n]\!]$ (par restriction à $[\![1,n]\!]$, $\theta \circ f$ étant injective, $n+1 \notin \theta \circ f([\![1,n]\!])$). Par hypothèse de récurrence, $\theta \circ f$ est bijective, donc $f = \theta^{-1} \circ (\theta \circ f)$ aussi. ■

Pour conclure la preuve de Thm/Def 1 : si $f : [\![1,n]\!] \hookrightarrow\!\!\!\!\rightarrow E$ et $g : E \hookrightarrow\!\!\!\!\rightarrow [\![1,m]\!]$, alors $g \circ f : [\![1,n]\!] \hookrightarrow\!\!\!\!\rightarrow [\![1,m]\!]$, donc $n = m$. ■

Thm 2 : Il existe $g : [\![1,n]\!] \hookrightarrow\!\!\!\!\rightarrow E$ et $f : [\![1,p]\!] \hookrightarrow\!\!\!\!\rightarrow F$.

▸ • Si E et F sont équipotents, alors $\exists \varphi : E \hookrightarrow\!\!\!\!\rightarrow F$, donc $g \circ \varphi \circ f^{-1} : [\![1,n]\!] \hookrightarrow\!\!\!\!\rightarrow E \hookrightarrow\!\!\!\!\rightarrow F \hookrightarrow\!\!\!\!\rightarrow [\![1,p]\!]$ donc $n = p$.

• Si $n = p$, alors $\exists \psi : [\![1,n]\!] \hookrightarrow\!\!\!\!\rightarrow [\![1,p]\!]$, donc $g^{-1} \circ \psi \circ f : E \hookrightarrow\!\!\!\!\rightarrow [\![1,n]\!] \hookrightarrow\!\!\!\!\rightarrow [\![1,p]\!] \hookrightarrow\!\!\!\!\rightarrow F$, donc E et F sont équipotents.

▸ $\forall n \geq 1$, $[\![1,n]\!] \neq \emptyset$. ■

Prop 3 : Montrons un résultat un peu plus fort : une partie d'un ensemble fini est finie, et le cardinal est croissant pour l'inclusion.

Preuve : Soit E fini de cardinal n. Procédons par récurrence sur n :

• $n = 0$: Si $F \subseteq E = \emptyset$, alors $F = \emptyset$, et c'est bon.

• Soit $n \in \mathbb{N}^*$, supposons la propriété vraie pour les ensembles de cardinal $n-1$. Soit $F \subseteq E$. Si $F = E$, alors il n'y a rien à faire. Supposons $F \neq E$. On peut alors considérer $x \in E \setminus F \neq \emptyset$. Dès lors, $F \subseteq E \setminus \{x\}$, mais $\# E \setminus \{x\} = n-1$ (en effet, on utilise θ comme dans Lemme 0.1▸ sur une numérotation de E pour faire correspondre n et x), donc F est fini de cardinal $\# F \leq \# E \setminus \{x\} = n-1 < \# E$.

Le cas d'égalité vient de la dernière inégalité ci-dessus, qui est stricte. ■

Cor 4 : Cela découle de Lemme 0.1▸

<u>Appli 5</u> : Il suffit de montrer que H est stable par inversion. Soit $x \in H$. Par stabilité, $\{x^n\}_{n\in\mathbb{N}^*} \subseteq H$, mais H est fini donc $\{x^n\}_{n\in\mathbb{N}^*}$ aussi, donc il existe $1 \leq n < m$ tels que $x^n = x^m$. De là, $1 = x^{\overbrace{m-n}^{\geq 1}} \in H$, donc $x^{-1} = x^{\overbrace{m-n-1}^{\geq 0}} \in H$. ■

<u>Prop 6</u> : Il existe $g : [\![1,n]\!] \hookrightarrow E$ et $f : [\![1,p]\!] \hookrightarrow F$. Quitte à composer f, supposons que $f : [\![n+1,n+p]\!] \hookrightarrow F$. Posons $\theta : [\![1,n+p]\!] \longrightarrow E \sqcup F$, $k \longmapsto \begin{cases} g(k) & \text{si } k \in [\![1,n]\!] \\ f(k) & \text{sinon.} \end{cases}$

- Soit $(k,\ell) \in [\![1,n+p]\!]^2$ tel que $\theta(k) = \theta(\ell)$.
  - Si $(k,\ell) \in [\![1,n]\!]^2$, alors $g(k) = \theta(k) = \theta(\ell) = g(\ell)$ donc $k = \ell$ par injectivité de g.
  - Si $(k,\ell) \in [\![n+1,n+p]\!]^2$, alors $f(k) = \theta(k) = \theta(\ell) = f(\ell)$ donc $k = \ell$ par injectivité de f.
  - Si $k \in [\![1,n]\!]$ et $\ell \in [\![n+1,n+p]\!]$, alors $g(k) = \theta(k) = \theta(\ell) = f(k) \in E \cap F = \emptyset$: impossible.
  - Si $\ell \in [\![1,n]\!]$ et $k \in [\![n+1,n+p]\!]$, alors c'est pareillement impossible.

Donc θ est injective.

- Soit $x \in E \sqcup F$. Si $x \in E$, alors $x = \theta(g^{-1}(x))$. Si $x \in F$, alors $x = \theta(n + f^{-1}(x))$.

Donc θ est bijective, donc $\#E \sqcup F = n+p = \#E + \#F$. ■

<u>Cor 7</u> : $E = \bigsqcup_{y\in F} f^{-1}(\{y\})$ (faire un dessin...), donc par hypothèse, $\#E = \sum_{y\in F} \#f^{-1}(\{y\}) = k\#F$. ■

<u>Cor 8</u> : $E = F \sqcup E \setminus F$

<u>Thm 9</u> : ▸ $E \cup F = E\setminus F \sqcup F \setminus E \sqcup E \cap F$.

- Deux démonstrations coexistent, selon le public qui leur est destiné :
  - Avec les fonctions indicatrices, pour un public plutôt aguerri :

La fonction $(1 - \mathbb{1}_{E_1}) \cdots (1 - \mathbb{1}_{E_m})$ est identiquement nulle sur $E = \bigcup_{i=1}^m E_i$. En développant le produit, on obtient $0 = 1 + \sum_{\emptyset \subsetneq I \subseteq [\![1,n]\!]} (-1)^{\#I} \prod_{i\in I} \mathbb{1}_{E_i}$, donc $1 = \sum_{k=1}^n (-1)^{k+1} \sum_{\substack{I \subseteq [\![1,n]\!] \\ \#I = k}} \mathbb{1}_{\bigcap_{i\in I} E_i}$.

Par conséquent, $\#E = \sum_{x\in E} 1 = \sum_{x\in E} \sum_{k=1}^n (-1)^{k+1} \sum_{\substack{I \subseteq [\![1,n]\!] \\ \#I = k}} \mathbb{1}_{\bigcap_{i\in I} E_i}(x) = \sum_{k=1}^n (-1)^{k-1} \sum_{\substack{I \subseteq [\![1,n]\!] \\ \#I = k}} \sum_{x\in E} \mathbb{1}_{\bigcap_{i\in I} E_i}(x)$

$\sum_{k=1}^n (-1)^{k-1} \sum_{\substack{I \subseteq [\![1,n]\!] \\ \#I = k}} \#\bigcap_{i\in I} E_i$.

- Par récurrence, pour un public moins aguerri :

Soit $n \geq 2$, supposons la formule montrée pour une famille de n ensembles. D'après l'initialisation faite juste au-dessus,

$$\#\bigcup_{i=1}^{n+1} E_i = \#\bigcup_{i=1}^{n} E_i \cup E_{n+1} = \#\bigcup_{i=1}^{n} E_i + \#E_{n+1} - \#\left(\bigcup_{i=1}^{n} E_i\right) \cap E_{n+1}$$
$$= \#\bigcup_{i=1}^{n} E_i + \#E_{n+1} - \#\bigcup_{i=1}^{n} E_i \cap E_{n+1}$$

Par hypothèse de récurrence :

$$\#\bigcup_{i=1}^{n+1} E_i = \#E_{n+1} + \sum_{k=1}^{n} (-1)^{k+1} \sum_{\substack{I \subseteq [\![1,n]\!] \\ \#I = k}} \#\bigcap_{i\in I} E_i - \sum_{k=1}^{n} (-1)^{k+1} \sum_{\substack{I \subseteq [\![1,n]\!] \\ \#I = k}} \#\bigcap_{i\in I} E_i \cap E_{n+1}$$

$$= \#E_{n+1} + \sum_{k=1}^{n} (-1)^{k+1} \sum_{\substack{I \subseteq [\![1,n]\!] \\ \#I = k}} \#\bigcap_{i\in I} E_i - \sum_{k=1}^{n} (-1)^{k+1} \sum_{\substack{n+1 \in J \subseteq [\![1,n+1]\!] \\ \#J = k+1}} \#\bigcap_{j\in J} E_j$$

$$= \#E_{n+1} + \sum_{k=1}^{n} (-1)^{k+1} \sum_{\substack{I \subseteq [\![1,n]\!] \\ \#I = k}} \#\bigcap_{i\in I} E_i - \sum_{k=2}^{n+1} (-1)^{k} \sum_{\substack{n+1 \in J \subseteq [\![1,n+1]\!] \\ \#J = k}} \#\bigcap_{j\in J} E_j$$

si $k=1$, alors $J = \{n+1\}$, et $-(-1)^1 \#\bigcap_{j\in J} E_j = \#E_{n+1}$

$$= \sum_{k=1}^{n} (-1)^{k+1} \sum_{\substack{I \subseteq [\![1,n]\!] \\ \#I = k}} \#\bigcap_{i\in I} E_i + \sum_{k=1}^{n+1} (-1)^{k+1} \sum_{\substack{n+1 \in J \subseteq [\![1,n+1]\!] \\ \#J = k}} \#\bigcap_{j\in J} E_j$$

$$= \sum_{k=1}^{n+1} (-1)^{k+1} \sum_{\substack{I \subseteq [\![1,n+1]\!] \\ \#I = k \\ n+1 \notin I}} \#\bigcap_{i\in I} E_i + \sum_{k=1}^{n+1} (-1)^{k+1} \sum_{\substack{I \subseteq [\![1,n+1]\!] \\ \#I = k \\ n+1 \in I}} \#\bigcap_{i\in I} E_i$$

$$= \sum_{k=1}^{n+1} (-1)^{k+1} \sum_{\substack{I \subseteq [\![1,n+1]\!] \\ \#I = k}} \#\bigcap_{i\in I} E_i.$$ ■

<u>Prop 11</u> : On juste dire que $E \times F = \bigsqcup_{x\in E} \bigsqcup_{y\in F} \{(x,y)\}$, ou alors procéder par récurrence sur $\#E$ en écrivant $E \times F = (E \setminus \{x_0\}) \times F \sqcup \{x_0\} \times F$.

<u>Cor 12</u> : Montrons par récurrence sur $n = \#E$ que F^E est fini de cardinal $\#F^{\#E}$.

- $n = 0$: F^E est réduit à l'application vide.
- Soit $n \in \mathbb{N}$ rendant la proposition vraie pour E de cardinal n. Supposons que $\#E = n+1$. A fortiori, $E \neq \emptyset$, considérons $x \in E$. Justifions que F^E et $F^{E\setminus\{x\}} \times F$ sont équipotents : pour $f \in F^E$, posons $\varphi(f) = (f_{|E\setminus\{x\}}, f(x))$.
  - Si $(f_{|E\setminus\{x\}}, f(x)) = (g_{|E\setminus\{x\}}, g(x))$, alors $\forall y \in E\setminus\{x\}$, $f(y) = g(y)$ et $f(x) = g(x)$, donc $f = g$, donc φ est injective.

• Soit $(g,y) \in F^{E\setminus\{x\}} \times F$. Posons $f : z \in E \longmapsto \{ g(z) \text{ si } z \neq x,\ y \text{ sinon}$. Alors $(g,y) = \varphi(f)$, et φ est surjective.

Comme $\# F^{E\setminus\{x\}} \times F = \# F^{\# E - 1} \times \# F$ par hypothèse de récurrence et Cor 12, on a bien montré que F^E est fini de cardinal $\# F^{\# E}$. ■

<u>Cor 13</u> : Écrivons $E = \{x_1, \dots, x_n\}$, posons $f : \mathcal{P}(E) \longrightarrow \{0,1\}^n$, $A \longmapsto (\mathbb{1}_A(x_1), \dots, \mathbb{1}_A(x_n))$

▹ Soit $(A,B) \in \mathcal{P}(E)^2$ tel que $f(A) = f(B)$. Alors $\mathbb{1}_A = \mathbb{1}_B$, donc $A = B$.

▹ Soit $(\delta_1, \dots, \delta_n) \in \{0,1\}^n$. Alors $(\delta_1, \dots, \delta_n) = f(A)$ où $A = \{x_i : i \in [\![1,n]\!], \delta_i = 1\} \in \mathcal{P}(E)$.

Donc f est bijective, donc $\mathcal{P}(E)$ est fini de cardinal $\# \mathcal{P}(E) = \# \{0,1\}^n = 2^n$. ■

<u>Prop 15</u> : Choisir un k-arrangement ($k \in [\![0,n]\!]$) de E, c'est choisir le premier élément (n choix), choisir le deuxième élément distinct ($n-1$ choix), etc. jusqu'au k^e élément distinct des précédents ($n-(k-1)$ choix). Il y a donc $n(n-1)\cdots(n-(k-1)) = \frac{n!}{(n-k)!}$ possibilités. ■

Rq : Les démonstrations de ce genre, que l'on dit de type "protocole", sont très efficaces, et pas moins formelles qu'une démonstration plus classique.
Dans le cas de Prop 15, on aurait pu procéder par récurrence en écrivant $\mathcal{A}(E) = \bigsqcup_{x \in E} (x) \cdot \mathcal{A}(E \setminus \{x\})$, toutes notations sous-entendues.

<u>Prop 18</u> : Choisir un k-arrangement ($k \in [\![0,n]\!]$) de E, c'est choisir les éléments qui le composent ($\binom{n}{k}$ choix), et un ordre ($k!$ choix, puisque ça revient à choisir un k-arrangement de ces k éléments). On a donc $A_k^n = k! \binom{n}{k}$, a fortiori $\binom{n}{k} = \frac{n!}{k!(n-k)!}$. Si $k \notin [\![0,n]\!]$, alors $\binom{n}{k} = 0$ puisqu'il n'existe aucune manière de choisir k éléments parmi n. ■

<u>Prop 19</u> : ▸ Choisir k éléments parmi n, c'est aussi choisir $n-k$ éléments à ne pas prendre.

▸ Il n'y a qu'une manière de choisir aucun (ou tous les) élément(s).

▸ Il y a autant de manières de choisir 1 élément que d'éléments eux-même.

▸ Pour choisir $k+1$ éléments de $[\![1,n+1]\!]$, on peut :

▹ soit choisir $n+1$ et k éléments de $[\![1,n]\!]$: $\binom{n}{k}$ choix

▹ soit ne pas choisir $n+1$ puis choisir $k+1$ éléments de $[\![1,n]\!]$: $\binom{n}{k+1}$ choix

Il y a donc $\binom{n}{k} + \binom{n}{k+1}$ possibilités, d'où l'égalité.

▸ Remarquons que $\{C \subseteq [\![1,n+1]\!] \mid \# C = p+1\} = \bigsqcup_{k=1}^{n+1-p} \{C \subseteq [\![1,n+1]\!] \mid \# C = p+1, \min(C) = k\}$.
Or choisir une $p+1$ combinaison de $[\![1,n+1]\!]$ dont le minimum est k revient à choisir une p-combinaison de $[\![k+1,n+1]\!]$, et il y a $\binom{n+1-k}{p}$ possibilités. Finalement, $\binom{n+1}{p+1} = \sum_{k=1}^{n+1-p} \binom{n+1-k}{p} = \sum_{k=p}^{n} \binom{k}{p}$. (Sinon on peut faire une preuve non combinatoire avec la f^{ce} de PASCAL). ■

<u>Ex 20</u> :

▸ Choisir une permutation de $[\![1,n]\!]$, c'est fixer le nombre k de points fixes, et choisir un dérangement des $n-k$ éléments restant.

▸ Choisir une fonction de $[\![1,n]\!]$ dans $[\![1,p]\!]$, c'est fixer le nombre $k \in [\![0,p]\!]$ d'images distinctes, choisir ces k images ($\binom{p}{k}$ choix), puis choisir une surjection de $[\![1,n]\!]$ dans cet ensemble d'images ($S_{n,k}$ choix).

▸ Posons $E_{n,p} = \{(\alpha_1, \dots, \alpha_p) \in \mathbb{N}^p \mid \alpha_1 + \dots + \alpha_p = n\}$. Comme $E_{n,p} \subseteq [\![0,n]\!]^p$, $S_{E_{n,p}}$ est fini, et $\Gamma_p^n := \# E_{n,p} \leq (n+1)^p$. Montrons par récurrence sur $p \in \mathbb{N}^*$ que $\forall n \in \mathbb{N}$, $\Gamma_p^n = \binom{n+p-1}{p-1}$ $\left(= \binom{n+p-1}{n}\right)$.

▹ $p = 1$: $\forall n \in \mathbb{N}$, $E_{n,1} = \{(n)\}$ donc $\Gamma_1^p = 1 = \binom{n}{0}$.

▹ Soit $p \in \mathbb{N}^*$ tel que $\forall k \leq p$, $\forall n \in \mathbb{N}$, $\Gamma_k^n = \binom{n+k-1}{k-1}$. Soit $n \in \mathbb{N}$. Remarquons que $E_{n,p+1} = \bigsqcup_{k=0}^{n} E_{n,p}^{(k)}$ où $E_{n,p}^{(k)} = \{(\alpha_1, \dots, \alpha_{p+1}) \in E_{n,p+1} \mid \alpha_{p+1} = k\}$, donc $\Gamma_{p+1}^n = \sum_{k=0}^{n} \# E_{n,p}^{(k)}$. Comme $(\alpha_1, \dots, \alpha_{p+1}) \in E_{n,p+1} \iff (\alpha_1, \dots, \alpha_p) \in E_{n-\alpha_{p+1},p}$, les ensembles $E_{n,p}^{(k)}$ et $E_{n-k,p}$ sont équipotents, donc $\Gamma_{p+1}^n = \sum_{k=0}^{n} \Gamma_p^{n-k} = \sum_{k=0}^{n} \binom{n-k+p+1}{p-1} = \binom{n+p}{p}$ d'après la formule des colonnes. ■

<u>Prop 21</u> :

▸ D'après le théorème de LAGRANGE, $\forall \omega \in \mathbb{U}_n$, $\mathrm{ord}(\omega) \mid n$: on partitionne $\mathbb{U}_n = \bigsqcup_{d \mid n} \{\omega \in \mathbb{U}_n \mid \mathrm{ord}(\omega) = d\}$.

▸ $(a+b)^n = (a+b)\cdots(a+b)$: choisir un terme, c'est fixer le nombre k de facteurs a, puis choisir a dans k facteurs parmi les n.

▸ Idem

▸ Choisir k éléments de $[\![1,n+p]\!]$, c'est fixer le nombre i d'éléments qu'on prend dans $[\![1,n]\!]$, choisir i éléments de $[\![1,n]\!]$ ($\binom{n}{i}$ choix) et $k-i$ éléments de $[\![n+1,p]\!]$ ($\binom{p}{k-i}$ choix). ■

Thm 23 : Pour $n=0$, c'est évident. Supposons $n\geq 1$, posons $F={}^t(f_0\ f_1\ \cdots\ f_n)$, $G={}^t(g_0\ g_1\ \cdots\ g_n)$ et :

$$P=\begin{pmatrix}\binom{0}{0} & \binom{1}{0} & \cdots & \binom{n}{0}\\ & \binom{1}{1} & \binom{2}{1} & \vdots\\ & & \ddots & \\ 0 & & & \binom{n}{n}\end{pmatrix}$$

Par hypothèse, $F=PG$, il s'agit d'inverser P car $\det(P)=1$. Comme $(1+X)^k=\sum_{i=0}^{k}\binom{k}{i}X^i$, ${}^tP$ est la matrice de passage de $(X^k)_{k=0}^n$ à $((1+X)^k)_{k=0}^n$ dans $\mathbb{R}_n[X]$. Il suffit alors d'écrire $X^k=(1+X-1)^k=\sum_{i=0}^{k}\binom{k}{i}(-1)^{k-i}(1+X)^i$ pour voir que l'inverse de ${}^tP$, qui est la matrice de passage de $((1+X)^k)_{k=0}^n$ à $(X^k)_{k=0}^n$, est :

$$({}^tP)^{-1}=\begin{pmatrix}\binom{0}{0} & -\binom{1}{0} & \binom{2}{0} & \cdots & (-1)^n\binom{n}{0}\\ & \binom{1}{1} & -\binom{2}{1} & \cdots & (-1)^{n-1}\binom{n}{1}\\ & & \ddots & & \vdots\\ & & & & \binom{n}{n}\end{pmatrix}$$

d'où $g_n=\sum_{k=0}^{n}\binom{n}{k}(-1)^{n-k}f_k$. ■

Ex 27 : ▸ $e^X\sum_{n\geq 0}\frac{D_n}{n!}X^n=\sum_{n\geq 0}\sum_{k=0}^{n}\frac{D_k}{k!}\frac{1}{(n-k)!}X^n=\sum_{n\geq 0}\frac{1}{n!}\left(\sum_{k=0}^{n}\binom{n}{k}D_k\right)X^n=\sum_{n\geq 0}X^n=\frac{1}{1-X}$.

et $\frac{e^{-X}}{1-X}=\sum_{n\geq 0}\left(\sum_{k=0}^{n}\frac{(-1)^k}{k!}\right)X^n$

Ex 28 : DEV

Thm 29 : $h\mapsto gh$ est bijective donc $\#H=\#gH$. Ensuite, $G=\bigsqcup_{X\in G/H}X$, et $X=g_xH$.

Prop 30 : $G/\mathrm{Ker}(\varphi)\simeq \mathrm{Im}(\varphi)$ d'après le premier théorème d'isomorphisme.

Thm 32 : Soit $x\in E$. Posons $f:G\to \mathrm{Orb}(x)$, $g\mapsto g\cdot x$. Pour tout $g\in G$, $f(g)=x \iff g\in \mathrm{Stab}(x)$, donc $\bar{f}: G/\mathrm{Stab}(x)\to \mathrm{Orb}(x)$, $g\,\mathrm{Stab}(x)\mapsto g\cdot x$ est bien définie, et injective. Elle est clairement surjective car f l'est, donc f est bijective.

Prop 34 : ~DEV

Thm 35 : Posons $F=\{(g,x)\in G\times E \mid g\cdot x=x\}$, notons $(x_1,\dots,x_r)\in E^r$ un système complet de représentants pour les orbites. D'une part, $F=\bigsqcup_{g\in G}\{(g,x) : x\in \mathrm{Fix}(g)\}$, donc $\#F=\sum_{g\in G}\#\mathrm{Fix}(g)$.

D'autre part, $F=\bigsqcup_{x\in E}\{(g,x) : g\in \mathrm{Stab}(x)\}$ donc $\#F=\sum_{x\in E}\#\mathrm{Stab}(x)=\sum_{i=1}^{r}\sum_{x\in \mathrm{Orb}(x_i)}\frac{\#G}{\#\mathrm{Orb}(x)}=\#G\times\sum_{i=1}^{r}\sum_{x\in \mathrm{Orb}(x_i)}\#\mathrm{Orb}(x_i)^{-1}=\#G\sum_{i=1}^{r}\#\mathrm{Orb}(x_i)\#\mathrm{Orb}(x_i)^{-1}=r\,\#G$. ■

Appli 36 : ~DEV

Prop 37 : $\varphi\circ\psi=\psi\circ\varphi\equiv 1$ donc $\mathrm{Im}(\varphi)\subseteq \mathrm{Ker}(\psi)$ et $\mathrm{Im}(\psi)\subseteq \mathrm{Ker}(\varphi)=\{\pm 1\}$. Pour tout $x\in \mathrm{Ker}(\psi)$, $x\in Z(X^{\frac{q-1}{2}}-1)$, donc $\#\mathrm{Ker}(\psi)\leq\frac{q-1}{2}$, mais $\#\mathbb{F}_q^\times=\#\mathrm{Ker}(\psi)\#\mathrm{Im}(\psi)$ donc $\#\mathrm{Im}(\psi)\geq 2$, donc $\mathrm{Im}(\psi)=\mathrm{Ker}(\varphi)=\{\pm 1\}$, et $\#\mathrm{Im}(\varphi)=\frac{q-1}{2}$ donc $\mathrm{Im}(\varphi)=\mathrm{Ker}(\psi)$. ■

Lemme 41, Thm 42 : Cor 38 + DEV

Ex 44 : Pour revenir en 0 partant de 0 en $2n$ étapes, on peut choisir les n instants où on fait un pas vers la droite, et faire des pas vers la gauche les instants restants.

Prop 45 : ▸ Immédiat avec l'étude précédente des dérangements.

Prop 46 : Choisir une permutation où k est un point fixe, c'est choisir une permutation de $[\![1,n]\!]\setminus\{k\}$: il y en a $(n-1)!$. Ainsi, $\mathbb{P}(X_k=1)=\frac{(n-1)!}{n!}=\frac{1}{n}$, d'où $X_k\sim\mathcal{B}(\frac{1}{n})$.
Choisir une permutation où $k\neq j$ sont des points fixes, c'est choisir une permutation de $[\![1,n]\!]\setminus\{k,j\}$: il y en a $(n-2)!$. Ainsi, $\mathbb{P}(X_k=X_j=1)=\frac{(n-2)!}{n!}=\frac{1}{n(n-1)}$. En particulier, $X_kX_j\sim\mathcal{B}(\frac{1}{n(n-1)})$.

De là, $\mathbb{E}[F_n]=\mathbb{E}[X_1]+\cdots+\mathbb{E}[X_n]=1$

$$\mathbb{V}[F_n]=\sum_{k=1}^{n}\mathbb{V}[X_k]+2\sum_{1\leq j<k\leq n}\mathrm{Cov}(X_k,X_j)=\sum_{k=1}^{n}\frac{1}{n}(1-\frac{1}{n})+2\sum_{1\leq j<k\leq n}\mathbb{E}[X_kX_j]-\mathbb{E}[X_k]\mathbb{E}[X_j]$$

$$=1-\frac{1}{n}+2\sum_{1\leq j<k\leq n}\frac{1}{n(n-1)}-\frac{1}{n^2}=1-\frac{1}{n}+\binom{n}{2}\left(\frac{1}{n(n-1)}-\frac{1}{n^2}\right)$$

$$=1-\frac{1}{n}+\frac{1}{2}-\frac{n-1}{2n}=1-\frac{1}{n}+\frac{1}{2}-\frac{1}{2}+\frac{1}{n}=1$$ ■