190

Méthodes Combinatoires, Problèmes de Dénombrement

I) Définitions et propriétés élémentaires

1) Cardinalité

def 1: Soient E et F deux ensembles et $f: E \to F$ une application. On dit que :
- f injective ssi $\forall x, y \in E$, $f(x) = f(y) \Rightarrow x = y$
- f surjective ssi $\forall y \in F$, $\exists x \in E$ tq $f(x) = y$
- f bijective ssi f injective et surjective

def 2. Soit E un ensemble. On dit que E est fini s'il existe $n \in \mathbb{N}$ et $\varphi : E \to [\![1, n]\!]$ une bijection. L'entier n est unique et on pose $\mathrm{Card}E = \# E = |E| = n$

Prop 3:
- Si $f: E \to F$ injective et F fini, alors E fini et $|E| \leqslant |F|$
- Si f surjective et E fini, alors F fini et $|E| \geqslant |F|$
- Si f bijective, et E ou F est fini alors E et F sont finis et $|E| = |F|$.

Prop 4: Soient E et F deux ensembles finis. Alors on a :
- $E \times F$ est fini et $|E \times F| = |E| \cdot |F|$
- $E \cup F$ et $E \cap F$ sont finis et $|E \cup F| + |E \cap F| = |E| + |F|$

App 5: Si E est un ens. fini et $n \in \mathbb{N}^*$, alors E^n est fini et $|E^n| = |E|^n$.

Prop 6: [Principe de la somme des parties]
Si E un ens. fini et $E = A_1 \sqcup \dots \sqcup A_n$ est une partition de E, alors les A_i sont finis et
$|E| = |A_1| + \dots + |A_n|$.

Rem 7: Tous les ensembles à partir de maintenant seront supposés finis. On fixe E et F deux ens. finis

App 8: Soient E et F deux ensembles. Alors on a :
- $E^F := \{f : F \to E\}$ vérifie $|E^F| = |E|^{|F|}$
- $\mathcal{P}(E)$ est fini et $|\mathcal{P}(E)| = 2^{|E|}$
- $\mathfrak{S}_E := \{f : E \to E \text{ bijective}\}$ est fini et $|\mathfrak{S}_E| = |E|!$

2) Propriétés élémentaires

Prop 9: [Principe des tiroirs] Si $|E| > |F|$, Alors $f : E \to F$ n'est pas injective

App 10:
- Si on choisit 101 entiers parmi $[\![1, 200]\!]$, alors il y en a au moins 1 qui divise un autre
- (Approximation d'un réel). Soit $x \in \mathbb{R}$, et $n \in \mathbb{N}^*$
$\exists \frac{p}{q} \in \mathbb{Q}$ tq $\left|x - \frac{p}{q}\right| < \frac{1}{nq}$

Prop 11: [Principe des bergers]: Soit $f : E \to F$ telle que $\forall x \in F$, $|f^{-1}(\{x\})| = n$, alors $|E| = n|F|$

Methode 12: Pour compter ses moutons, le berger peut compter le nombre de pattes puis diviser par 4.

App 13: Si on définit $\binom{n}{k} := \#\{A \in \mathcal{P}(E), |A| = k\}$
Alors $\binom{n}{k} = \frac{n!}{k!(n-k)!} \mathbb{1}_{0 \leq k \leq n}$ dits coefficients binomiaux

3) Résultats sur les coefficients

Prop 14: [Formule de Pascal] $\forall n \in \mathbb{N}, \forall k \in [\![0, n-1]\!]$
$$\binom{n+1}{k+1} = \binom{n}{k+1} + \binom{n}{k}$$

App 15: Si A est un anneau et $a, b \in A$, tq $ab = ba$, alors $\forall n \in \mathbb{N}$,
$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$$

Prop 16: Si $1 \leq k \leq n$, Alors $k\binom{n}{k} = n\binom{n-1}{k-1}$

App 17: Soit $\mathbb{F}_p$ corps fini à p éléments, p premier, et $\mathrm{Frob} : \begin{array}{l} \mathbb{F}_p \to \mathbb{F}_p \\ x \mapsto x^p \end{array}$. Alors Frob est un morphisme

Prop 18 : $\forall n \in \mathbb{N}$, on a : - $\sum_{k=0}^{n} \binom{n}{k} = 2^n$

- $\sum_{k=0}^{n} \binom{n}{k} (-1)^k = 0$ si $n \neq 0$
- (Formule de Vandermonde) $\forall p,q \in \mathbb{N}$, $\forall n \in [\![0,p+q]\!]$

$$\binom{p+q}{n} = \sum_{k=0}^{n} \binom{p}{k}\binom{q}{n-k}$$

Interprétation 19 : - $\# \bigsqcup_{k=0}^{n} \{F \subseteq E, |F| = k\} = \# \mathcal{P}(E)$

- $\# \{F \subset E, |F| \text{ impair}\} = \# \{F \subset E, |F| \text{ pair}\}$

II) Outils puissants de dénombrement

1) Crible de Poincaré

Prop 20 : [Formule du crible de Poincaré] : Soit $(A_i)_{1\leq i\leq n}$ une famille de sous-ensembles de E. Alors

$$\mathrm{Card}\left(\bigcup_{i=1}^{n} A_i\right) = \sum_{k=1}^{n} (-1)^{k-1} \sum_{1\leq i_1 < \dots < i_k \leq n} \mathrm{Card}\left(\bigcap_{j=1}^{k} A_{i_j}\right)$$

App 21 : Si $X_n, Y_n \sim \mathcal{U}([\![1,n]\!])$, et $X_n \perp\!\!\!\perp Y_n$

$$\mathbb{P}(X_n \wedge Y_n = 1) \xrightarrow[n\to+\infty]{} \frac{6}{\pi^2}$$

App 22 : Le nombre de permutations de $\mathfrak{S}_n$ sans point fixe est $D_n = n! \left(\sum_{k=0}^{n} \frac{(-1)^k}{k!} \right)$

2) Formules d'inversion

a) Inversion de Möbius

Def 23 : On appelle fonction de Möbius la fonction

$$\mu : \mathbb{N}^* \longrightarrow \{0,1,-1\}$$
$$n \longmapsto 0 \text{ si } n \text{ a un facteur carré}$$
$$p_1 \cdots p_r \longmapsto (-1)^r \quad p_i \text{ premiers distincts}$$

lemme 24 : - μ est multiplicative : si $m \wedge n = 1$
Alors $\mu(mn) = \mu(m)\mu(n)$

- $\sum_{d|n} \mu(d) = 0$ si $n > 1$.

thm 25 : [Inversion de Möbius]. Si $a_n = \sum_{d|n} b_d$

Alors $b_n = \sum_{d|n} \mu\left(\frac{n}{d}\right) a_d$

App 26 : On note $\forall n \in \mathbb{N}^*$, $\varphi(n) := \mathrm{Card}(\{m \in \mathbb{N}^* \mid m \leq n \text{ et } m\wedge n = 1\})$
alors $\varphi(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) d$

App 27 : Soit $I(n,q)$ le nombre de polynômes de $\mathbb{F}_q[X]$ irréductibles unitaires de degré n
On a $I(n,q) = \frac{1}{n} \sum_{d|n} \mu\left(\frac{n}{d}\right) q^d$

b) Inversion de Pascal

lemme 28 : $\sum_{k=0}^{p} (-1)^k \binom{n}{k}\binom{n-k}{p-k} = \begin{cases} 1 \text{ si } p = 0 \\ 0 \text{ si } p \geq 1 \end{cases}$

thm 29 : [Inversion de Pascal] Si $a_n = \sum_{k=0}^{n} \binom{n}{k} b_k$

Alors $b_n = \sum_{k=0}^{n} (-1)^k \binom{n}{k} a_{n-k}$

App 30. Soit $S_{n,p}$ le nombre de surjections de $\{1,\dots,n\}$ dans $\{1,\dots,p\}$. On a $S_{n,p} = (-1)^p \sum_{k=1}^{n} (-1)^k \binom{p}{k} k^n$

3) Séries génératrices

a) Série génératrice classique

def 31 : On appelle série génératrice d'une suite $(a_n)_{n\in\mathbb{N}}$ la série formelle $\sum_{n=0}^{\infty} a_n X^n$

App 32 [Nombre de Catalan] C_n est défini comme le nombre de chemins entre 0 et $2n$ positifs (cf schéma annexe). Alors

$$C_n = \frac{1}{n+1}\binom{2n}{n}$$

b) Série génératrice exponentielle

def 33 : On appelle série génératrice exponentielle d'une suite $(a_n)_{n\in\mathbb{N}}$ la série formelle

$$\sum_{n=0}^{\infty} \frac{a_n}{n!} X^n$$

App 34 : [Nombres de Bell] . B_n est défini comme le nombre de partition de $\{1,..,n\}$. Alors [DEV1]

$$B_n = \frac{1}{e}\sum_{k=0}^{\infty}\frac{k^n}{k!}$$

App 35 : [Nombre de dérangements] $D_n := \#\{\tau \in \mathfrak{S}_n, \tau(i) \neq i \ \forall i \in [\![1,n]\!]\}$

Alors $D_n = E\left[\frac{n!}{e} + \frac{1}{2}\right]$

c) série génératrice de Dirichlet

def 36 : On appelle série génératrice de Direchlet une série de la forme $\sum_{n=1}^{\infty}\frac{a_n}{n^s}$ pour une suite $(a_n)_n$ donnée, où s peut être réel ou complexe.

thm 37 : [Unicité] Si $\sum_{n=1}^{\infty}\frac{a_n}{n^s} = \sum_{n=1}^{\infty}\frac{b_n}{n^s}$, $\forall Re(s) > Re(s_0)$

Alors $a_n = b_n \quad \forall n \in \mathbb{N}^*$

prop 38 : Soit $\zeta(s) = \sum_{n=1}^{\infty}\frac{1}{n^s}$ la fonction ζ de Riemann on a :

- $\frac{1}{\zeta(s)} = \sum_{n=1}^{\infty}\frac{\mu(n)}{n^s}$ pour $Re(s) > 1$
- $\sum_{n=1}^{\infty}\frac{\varphi(n)}{n^s} = \frac{\zeta(s-1)}{\zeta(s)}$.

App 39 : . $\sum_{d|n}\varphi(n) = n$

III) Applications aux structures algébriques

1) Combinatoire en théorie des groupes et géométrie

Soit G un groupe fini.

Thm 40 : [Lagrange] Si $H \leq G$, Alors

$|G| = |H||G/H|$

App 41 : $\mathrm{Card}\,\mathcal{A}_n = \frac{\mathrm{Card}\,\mathfrak{S}_n}{2} = \frac{n!}{2}$

Prop 42 : Si $G \curvearrowright X$ (G agit sur X). $\forall x \in X$, on a

$|\mathrm{Stab}(x)||\mathrm{Orb}(x)| = |G|$

App 43 : Si $G \curvearrowright X$ transitivement, alors $|G| = |\mathrm{Orb}(x)|$, $\forall x \in G$

Prop 44 : [Formule des Classes] Si $G \curvearrowright X$, et si $X = \bigcup_{i=1}^{r}\mathrm{Orb}(x_i)$ la partition de X en obites sous l'action de G. On a $|X| = \sum_{i=1}^{r}|\mathrm{Orb}(x_i)| = \sum_{i=1}^{r}\frac{|G|}{|\mathrm{Stab}(x_i)|}$

App 45 : Si G non abélien. On note $n(G)$ la proportion de couples $(x,y) \in G^2$ commutant. Alors $n(G) \leq \frac{5}{8}$

Prop 46 : [Formule de Burnside] Si $G \curvearrowright X$, Alors $\forall g \in G$: le nombre d'orbite dans X sous G ($|\mathrm{Orb}_X(G)|$) est

$$|\mathrm{Orb}_X(G)| = \frac{1}{|G|}\sum_{g \in G}|\mathrm{Fix}_X(g)|$$

App 47 : Le nombre moyen de points fixes d'une permutation de $\mathfrak{S}_n$ est 1.

2) Dénombrement sur les corps finis.

Soit p un nombre premier et $q = p^r$, on a :

Ex 48. - $\mathrm{Card}(GL_n(\mathbb{F}_q)) = (q^n-1)\dots(q-1).q^{\frac{n(n-1)}{2}}$

- $\mathrm{Card}(SL_n(\mathbb{F}_q)) = (q^n-1)\dots(q^2-1)q^{\frac{n(n-1)}{2}}$
- $\mathrm{Card}(\mathcal{N}_d(\mathbb{F}_q)) = q^{d(d-1)}$ où $\mathcal{N}_d(\mathbb{F}_q)$ est l'ensemble des matrices nilpotentes à coefficients dans $\mathbb{F}_q$. [DEV2]

Nombres de Bell

Le but de ce développement est de calculer les nombres B_n, appelés nombres de Bell et définis comme étant le nombre de partition possible d'un ensemble à n éléments, à permutation près.
Par exemple, $B_0 = 1,\ B_1 = 1,\ B_2 = 2$ et $B_3 = 5$ car les partitions de $\{1,2,3\}$ sont les suivantes :

$$\{1,2,3\},\ \{1,2\}\cup\{3\},\ \{1,3\}\cup\{2\},\ \{2,3\}\cup\{2\},\ \text{et } \{1\}\cup\{2\}\cup\{3\}.$$

Le résultat final est le suivant :

Théorème 0.1.

$$\forall n \in \mathbb{N},\ B_n = \frac{1}{e}\sum_{k=0}^{\infty}\frac{k^n}{k!}$$

Étape 1 : Commençons par prouver ce lemme grâce à un argument combinatoire :

Lemme 0.2.

$$\forall n \in \mathbb{N}^*, B_{n+1} = \sum_{k=0}^{n}\binom{n}{k}B_k$$

Démonstration. Ce résultat se voit bien si on compte les partitions de $\{1,\dots,n+1\}$ de la manière suivante :
- Si $A_1 \sqcup \ldots \sqcup A_r = \{1,\dots,n+1\}$ est une partition, supposons que $1 \in A_1$. En fixant $1 \in A_1$, nous sommes sûrs de ne pas compter plusieurs fois une seule partition, comme la permutation des A_i n'est pas prise en compte.
- Fixons donc le cardinal de A_1 entre 1 et $n+1$, disons $k+1$, et calculons le nombre de partitions de $\{1,\dots,n+1\}$ sous cette condition.
- Un seul élément de A_1 est fixé (1), nous avons donc exactement $\binom{n}{k}$ choix pour les k autres.
- De là, il reste $n+1-(k+1)$ éléments à partitioner : il y a exactement B_{n-k} choix par définition.

D'où on a l'égalité suivante :

$$B_{n+1} = \sum_{k=0}^{n}\binom{n}{k}B_{n-k}$$

puis en réindexant $k \longleftarrow n-k$ et en écrivant que $\binom{n}{k} = \binom{n}{n-k}$, on a l'égalité demandée. □

Étape 2 : Introduisons la série génératrice exponentielle des nombres de Bell :

$$f(z) = \sum_{n=0}^{\infty}\frac{B_n}{n!}z^n$$

Remarque 0.1. *f est définie au moins sur le disque unité d'après la formule de Hadamard $\frac{1}{R} = \limsup_{n\to\infty}\left(\frac{B_n}{n!}\right)^{\frac{1}{n}}$ car $B_n \leq n!$ pout tout n. En effet :*
- $B_0 = 1$

— *Si $B_k \leq k!$ pour tout $k \leq n$ où $n \in \mathbb{N}$ est fixé, alors*

$$\begin{aligned} B_{n+1} &= \sum_{k=0}^{n} \binom{n}{k} B_k \\ &\leq \sum_{k=0}^{n} \frac{n!}{k!(n-k)!} k! \\ &\leq n! \sum_{k=0}^{n} \frac{1}{k!} \\ B_{n+1} &\leq (n+1)! \end{aligned}$$

Pour z dans le disque unité, on peut dériver f et cela donne :

$$\begin{aligned} f'(z) &= \sum_{n=1}^{\infty} \frac{B_n}{(n-1)!} z^{n-1} \\ &= \sum_{n=0}^{\infty} \frac{B_{n+1}}{n!} z^n \\ &= \sum_{n=0}^{\infty} \frac{1}{n!} \sum_{k=0}^{n} \binom{n}{k} B_k z^n \\ &= \sum_{n=0}^{\infty} \sum_{k=0}^{n} \frac{B_k}{k!} \frac{1}{(n-k)!} z^n \quad \textit{on reconnaît un produit de Cauchy} \\ &= \left(\sum_{n=0}^{\infty} \frac{B_n}{n!} z^n \right) \left(\sum_{n=0}^{\infty} \frac{1}{n!} z^n \right) \\ f'(z) &= f(z) e^z \end{aligned}$$

On a donc un problème de Cauchy avec condition initiale $f(0) = B_0 = 1$.
Ce problème admet une unique solution qui est :

$$f(z) = \frac{1}{e} e^{e^z}$$

Étape 3 : De là, on peut écrire, pour z dans le disque unité :

$$\begin{aligned} ef(z) &= \sum_{k=0}^{\infty} \frac{e^{zk}}{k!} \\ &= \sum_{k=0}^{\infty} \frac{1}{k!} \sum_{n=0}^{\infty} \frac{(zk)^n}{n!} \end{aligned}$$

Pour intervertir les sommes, montrons que la famille $\left(\frac{(zk)^n}{k!n!} \right)_{(k,n) \in \mathbb{N}^2}$ est sommable :

$$\begin{aligned} \sum_{k=0}^{\infty} \sum_{n=0}^{\infty} \frac{|zk|^n}{k!n!} &\leq \sum_{k=0}^{\infty} \sum_{n=0}^{\infty} \frac{k^n}{k!n!} \\ &\leq \sum_{k=0}^{\infty} \frac{e^k}{k!} \\ &\leq e^e < \infty \end{aligned}$$

On peut intervertir les sommes et, en reprenant le calcul et d'après l'unicité des coefficients de f :

$$\begin{aligned} f(z) &= \frac{1}{e}\sum_{n=0}^{\infty}\sum_{k=0}^{\infty}\frac{1}{k!}\frac{(zk)^n}{n!} \\ &= \sum_{n=0}^{\infty}\underbrace{\frac{1}{e}\sum_{k=0}^{\infty}\frac{k^n}{k!}}_{=B_n}\frac{z^n}{n!} \end{aligned}$$

Cardinal du cône nilpotent sur un corps fini

Le but de ce développements est de dénombrer l'ensemble $\mathscr{N}_d(\mathbb{F}_q)$ des matrices nilpotentes de taille $d \times d$ sur un corps fini $\mathbb{F}_q$ de cardinal q. On fixe E un $\mathbb{F}_q$-espace vectoriel de dimension d. On note $\mathscr{N}(E)$ l'ensemble des endomorphismes nilpotents sur E et remarquons que $\mathscr{N}(E)$ muni d'une base est en bijection avec $\mathscr{N}_d(\mathbb{F}_q)$.

Théorème 0.1.0.1. *Pour tout corps fini $\mathbb{F}_q$ de cardinal q et tout entier d, on a :*

$$n_d := |\mathscr{N}_d(\mathbb{F}_q)| = q^{d(d-1)}$$

Lemme 0.1.0.1. *Soient $N \in \mathscr{N}(E)$ et e un vecteur non nul de E. On note r le nombre maximal tel que $\mathscr{E} = (e, Ne, N^2e, ..., N^{r-1}e)$ est une famille libre. On a alors : $N^re = 0$.*

Preuve 0.1.0.1. *Soit $F = Vect(N^se,\ s \in \mathscr{N})$ le sous-espace de E engendré par e et N. Alors $\mathscr{E}$ est une base de F. En effet, elle est libre par construction. Montrons qu'elle est génératrice : c'est-à-dire que pour tout $s \geq r$, on a $N^se \in F$. Cela est vrai pour $s = r$ car par construction la famille $(e, Ne, ..., N^{r-1}e, N^re)$ est liée et donc il existe des scalaires $a_0, ..., a_{r-1}$ tels que $N^re = \sum_{i=0}^{r-1} a_iN^ie$. C'est finalement vrai par récurrence pour tout $s \geq r$, car $N^se = \sum_{i=0}^{r-1} a_iN^{s-r+i}e$.*

Par construction, N stabilise F, on note N_F l'endomorphisme induit par la restriction de N à F. Sa matrice dans la base $\mathscr{E}$ est donc

$$\begin{pmatrix} 0 & \cdots & 0 & a_0 \\ 1 & \ddots & \vdots & \vdots \\ 0 & \ddots & 0 & \vdots \\ 0 & 0 & 1 & a_{r-1} \end{pmatrix}$$

On reconnaît alors la matrice compagnon du polynôme $P = X^r - \sum_{i=0}^{d} a_iX^i$ dont le polynôme caratéristique est justement le polynôme P (qui est également polynôme minimal). Comme N_F est nilpotente alors, pour tout i, $a_i = 0$, d'où $N^re = 0$.

Prouvons à présent le théorème. Pour cela, on note $L_{r,d}$ l'ensemble des parties libres dans E à r éléments. De plus, on dit que $N \in \mathscr{N}(E)$ *respecte* une famille $\mathscr{E} = (e_1, e_2, ..., e_r)$ de $L_{r,d}$ si, pour tout entier s compris entre 1 et r, on a : $Ne_s = e_{s+1}$, où l'on convient que $e_{r+1} = 0$.

Démonstration du théorème 0.1.0.1. *Nous allons déterminer une formule de récurrence pour $n_d = \mathscr{N}_d(\mathbb{F}_q)$. Pour cela, calculons de deux manières différentes l'ensemble*

$$\tilde{\mathscr{N}_d} = \{(N, \mathscr{E}),\ N \in \mathscr{N}_d, \exists r \in \{1, ..., d\},\ \mathscr{E} \in L_{r,d} \text{ et } \mathscr{N} \text{ respecte } \mathscr{E}\}$$

On note π_1 (resp. π_2), la projection sur la première (resp. seconde) composante.

Etape 1 : *dénombrement sur la première coordonnée. On a*

$$|\tilde{\mathscr{N}_d}| = \sum_{N \in \mathscr{N}_d} |\pi_1^{-1}(N)|$$

Or, d'après le lemme, pour tout $N \in \mathscr{N}(E)$, *on a une bijection entre les éléments de* $E \setminus \{0\}$ *et l'ensemble des familles libres respectées par* N. *Par conséquent, on a*

$$|\tilde{\mathscr{N}_d}| = n_d(p^d - 1)$$

Etape 2 : *dénombrement sur la deuxième coordonnée.*

$$|\tilde{\mathscr{N}_d}| = \sum_{r=1}^{d} \sum_{\mathscr{E} \in L_{r,d}} |\pi_2^{-1}(\mathscr{E})|$$

Fixons r *entre* 1 *et* d *et notons* g_r *l'ordre du groupe* $\mathrm{GL}(k^r)$. *L'action naturelle de* $\mathrm{GL}(E)$ *sur* $L_{r,d}$ *est transitive d'après le théorème de la base incomplète. Pour* $\mathscr{E} \in L_{r,d}$,*on a donc* $|L_{r,d}| = |Orb(\mathscr{E})|$. *D'après les relations orbite-stabilisateur, on a donc :*

$$|L_{r,d}| = \frac{|\mathrm{GL}(E)|}{|Stab(\mathscr{E})|}$$

On complète $\mathscr{E}$ *en* $\tilde{\mathscr{E}}$ *une base de* E. *De plus,*

$$N \in Stab(\mathscr{E}) \iff Mat_{\tilde{\mathscr{E}}}(N) \in \left(\begin{array}{c|c} I_r & \mathscr{M}_{r,d-r}(\mathbb{F}_q) \\ \hline 0 & \mathrm{GL}_{d-r}(\mathbb{F}_q) \end{array}\right)$$

On en déduit donc que $|Stab(\mathscr{E})| = |\mathscr{M}_{r,d-r}(\mathbb{F}_q)||\mathrm{GL}_{d-r}(\mathbb{F}_q)| = q^{r(d-r)} g_{d-r}$. *Le nombre de familles libre à* r *éléments est donc :*

$$|L_{r,d}| = \frac{g_d}{q^{r(d-r)} g_{d-r}}$$

Remarquons que les matrices nilpotentes respectant $\mathscr{E}$ *sont de la forme :*

$$\left(\begin{array}{c|c} J_r & \mathscr{M}_{r,d-r}(\mathbb{F}_q) \\ \hline 0 & \mathscr{N}_{d-r}(\mathbb{F}_q) \end{array}\right)$$

où J_r *est le bloc de Jordan de taille* $r \times r$. *Ainsi, pour tout* $\mathscr{E} \in L_{r,d}$, *on a :* $|\pi_2^{-1}(\mathscr{E})| = q^{r(d-r)} n_{d-r}$. *On a donc :*

$$|\tilde{\mathscr{N}_d}| = \sum_{r=1}^{d} \frac{g_d}{g_{d-r}} n_{d-r}$$

Etape 3 : *Conclusion. En comparant les deux formules obtenues pour le cardinal de* $\tilde{\mathscr{N}_d}$, *on obtient :*

$$\frac{n_d}{g_d}(p^d - 1) = \sum_{r=1}^{d-1} \frac{n_{d-r}}{g_{d-r}} = \frac{n_{d-1}}{g_{d-1}} + \sum_{r=1}^{d-1} \frac{n_{d-r}}{g_{d-r}} = \frac{n_{d-1}}{g_{d-1}} + (q^{d-1} - 1)\frac{n_{d-1}}{g_{d-1}} = q^{d-1} \frac{n_{d-1}}{g_{d-1}}$$

On en déduit par récurrence, comme $n_1 = 1$ *et* $g_1 = q - 1$*, la formule suivante :*

$$\forall d \in \mathbb{N}^*, n_d = g_d \frac{q^{d(d-1)/2}}{\prod_{r=1}^{d}(q^r - 1)}$$

En utilisant que $g_d = |\operatorname{GL}_d(\mathbb{F}_q)| = \prod_{r=0}^{d-1}(q^d - q^r) = q^{d(d-1)/2}\prod_{r=1}^{d}(q^r - 1)$ *on obtient finalement que*

$$\forall d \in \mathbb{N}^*, n_d = q^{d(d-1)}$$