Algèbre générale
2009/2010
S.P.

Dénombrements: fiche de rappels

Un ensemble E est dit fini s'il existe un entier $n \in \mathbf{N}$ tel que E soit en bijection avec $\{1, 2, \ldots, n\}$. Cet entier n est noté $card(E)$ ou encore $\mid E \mid$.

Tous les ensembles de cette fiche sont supposés finis.

L'ensemble $\{1, 2, \ldots, n\}$ est noté $[1, n]$.

Principes de dénombrements

(1) Somme: pour E et F disjoints: $\mid E \cup F \mid=\mid E \mid + \mid F \mid$.

Plus généralement, pour E_i, $i \in [1, n]$, deux à deux disjoints:

$$\mid \bigcup_{i=1}^{n} E_i \mid= \sum_{i=1}^{n} \mid E_i \mid$$

Démo: récurrence sur $n \geq 2$ à l'aide de l'associativité de la réunion.

(2) Produit: pour $E_i, i \in [1, n]$: $\mid E_1 \times \cdots \times E_n \mid=\mid E_1 \mid \cdots \mid E_n \mid$.
Démo: récurrence sur n en observant que le produit est la réunion disjointe

$$\bigcup_{x \in E_n} (E_1 \times \cdots \times E_{n-1}) \times \{x\}$$

et en utilisant (1).

(3) Principe des bergers: si $f : E \to F$ est une surjection on a

$$\mid E \mid= \sum_{y \in F} \mid f^{-1}(y) \mid .$$

Démo: observer que $E = \bigcup_{y \in F} f^{-1}(y)$ est une réunion de parties deux à deux disjointes.
Cas particulier très utilisé: s'il existe un entier m tel que pour tout $y \in F$, $\mid f^{-1}(y) \mid= m$ alors $\mid E \mid= m \mid F \mid$.

(4) Principe d'exclusion-inclusion:

$$\mid E \cup F \mid=\mid E \mid + \mid F \mid - \mid E \cap F \mid$$

Démo: observer

$$E \cup F = (E \setminus F) \cup (F \setminus E) \cup (E \cap F)$$

et utiliser (1).
Plus généralement, pour E_i, $i \in [1, n]$:

$$\mid \bigcup_{i=1}^{n} E_i \mid= \sum_{k=1}^{n} (-1)^{k-1} \sum_{1 \leq i_1 < i_2 < \cdots < i_k \leq n} \mid \bigcap_{l=1}^{k} E_{i_l} \mid$$

Démo: récurrence sur $n \geq 2$. Utiliser l'associativité de la réunion et la distributivité de l'intersection sur la réunion:

$$(\bigcup_{i=1}^{n} E_i) \bigcap E_{n+1} = \bigcup_{i=1}^{n} (E_i \bigcap E_{n+1})$$

(Cette démo est un exemple non trivial de récurrence. Faites la!)

L'énoncé qui suit résulte du principe des bergers.

(5) Soit A un ensemble et $m, n_1, \ldots, n_m \in \mathbf{N}^*$ des entiers.
Pour un entier $1 \leq k < m$ convenons d'appeler $(a_1, \ldots, a_k) \in A^k$ le début de longueur k de l'élément $(a_1, \ldots, a_k, a_{k+1}, \ldots, a_m) \in A^m$.

Soit $C \subset A^m$. Supposons que

- la première composante des $m-$uplets de C peut prendre n_1 valeurs distinctes

- quelquesoit $1 \leq k < m$, pour tout début $(a_1, \ldots, a_k)$ de longueur k d'un élément de C il y a exactement n_{k+1} éléments $a_{k+1} \in A$ pour lesquels $(a_1, \ldots, a_k, a_{k+1})$ est un début de longueur $k+1$ d'un élément de C.

Alors

$$\mid C \mid = n_1 \cdots n_m.$$

Démo: récurrence sur m. Pour $m = 1$ il n'y a rien à vérifier. Voici comment passer de m à $m+1$: soit $C \subset A^{m+1}$ une partie vérifiant les conditions de l'énoncé pour les entiers $n_1, \ldots, n_{m+1}$ et

$$p : A^{m+1} \to A^m : (a_1, \ldots, a_m, a_{m+1}) \to (a_1, \ldots, a_m)$$

l'application de projection. L'image $p(C) \subset A^m$ vérifie les conditions de l'énoncé pour les entiers $n_1, \ldots, n_m$. Par hypothèse $\mid p(C) \mid = n_1 n_2 \ldots n_m$. D'autrepart chaque $m-$ uplet de $p(C)$ admet n_{m+1} antécédents pour p. Le principe des bergers donne

$$\mid C \mid = \mid p(C) \mid n_{m+1} = n_1 n_2 \ldots n_m n_{m+1}.$$

Remarque: Une partie $C \subset A^m$ vérifiant les conditions de l'énoncé se représente par un arbre en disposant au niveau k les débuts de mots $(a_1, a_2, \ldots, a_k) \in A^k$ de la partie C. Il y a donc n_1 branches au niveau 1, $n_1 n_2$ branches au niveau 2, etc. (Faites-le, c'est instructif!)

Vocabulaire:

On appelle

- $m-$ liste d'éléments de A, tout $m-$ uplet $(a_1, \ldots, a_m) \in A^m$

- mot de longueur m en l'alphabet A, toute écriture $a_1 a_2 \ldots a_m$, $a_i \in A, i \in [1, m]$.

L'ensemble $D(m)$ des mots de longueur m en l'alphabet A est par définition même en bijection avec A^m.

Savoir compter

Soit $n, m \in \mathbf{N}^*$ et A un ensemble fini de cardinal n.

(1) Il y a n^m applications $f : [1, m] \to A$. En d'autres termes

$$\mid A^{[1,m]} \mid = \mid A \mid^m.$$

Démo: observer que l'application

$$\phi : A^{[1,m]} \to A^m : f \mapsto (f(1), f(2), \ldots, f(m))$$

est une bijection.

(2) A contient $2^{|A|}$ parties distinctes.
Démo: l'application

$$\chi : P(A) \to \{0,1\}^A$$

qui à toute partie $B \subset A$ associe sa fonction caractéristique χ_B est une bijection. D'où

$$| P(A) |=| \{0,1\}^A |= 2^{|A|}.$$

(3) Supposons $1 \leq m \leq n$. Il y a $\frac{n!}{(n-m)!}$ applications injectives $f : [1,m] \to A$.
- Démo: par récurrence finie sur $m \leq n$. C'est vrai pour $m = 1$. Pour $1 \leq m < n$ notons I_m l'ensemble des applications injectives de $[1,m]$ vers A. L'application

$$\phi : I_{m+1} \to I_m$$

qui à toute application $f \in I_{m+1}$ associe sa restriction à $[1,m]$ est une surjection pour laquelle toute $f' \in I_m$ admet exactement $n-m$ antécédents $f \in I_{m+1}$ obtenus en choisissant $f(m+1)$ dans la partie $A \setminus \{f'(1), \ldots, f'(m)\}$. Le principe des bergers donne alors

$$| I_{m+1} |= (n-m) \mid I_m |= (n-m)\frac{n!}{(n-m)!} = \frac{n!}{(n-(m+1))!}.$$

- Autre manière d'écrire la même démo: appliquer le principe (**5**) à la partie $C \subset A^m$ constituée des $m-$ uplets $(a_1, \ldots, a_m)$ de composantes deux à deux distinctes, pour les entiers $n_1 = n, n_2 = n-1, \ldots, n_m = n-(m-1)$.

(4) *Cas particulier important*: il y a $n!$ bijections $f : [1,n] \to [1,n]$.

Coefficients binomiaux
Soit $\binom{n}{m}$ le nombre de parties de cardinal $m \leq n$ de A. On a

$$\binom{n}{m} = \frac{n!}{m!(n-m)!}$$

Démo: Notons $P_m \subset P(A)$ l'ensemble des parties de cardinal m et I_m l'ensemble des applications injectives de $[1,m]$ vers A. L'application

$$\phi : I_m \to P_m$$

qui à $f \in I_m$ associe la partie $\phi(f) = \{f(1), f(2), \ldots, f(m)\} \in P_m$ est une surjection. Observer ensuite que

$$\phi(f) = \phi(f') \Leftrightarrow f^{-1} \circ f' : [1,m] \to [1,m] \text{ est une bijection }.$$

Dès lors pour toute partie $P \in P_m$ il y a exactement $m!$ applications $f \in I_m$ pour lesquelles $\phi(f) = P$. Le principe des bergers donne

$$\binom{n}{m} = \mid P_m \mid = \frac{\mid I_m \mid}{m!}.$$

Propriétés immédiates
$\sum_{m=0}^{n} \binom{n}{m} = 2^n$ (le membre de gauche calcule $\mid P(A) \mid$)
pour $m \leq n$, $\binom{n}{m} = \binom{n}{n-m}$ (toute partie $P \in P_m$ admet un unique complémentaire $A \setminus P \in P_{n-m}$)
pour $1 \leq m < n$, $\binom{n}{m} = \binom{n-1}{m} + \binom{n-1}{m-1}$ (pour $a \in A$ fixé dénombrer séparément les parties $P \in P_m$ t.q. $a \in P$ et celles t.q. $a \notin P$)

Exercice 0
Soit $m \leq n$. Montrer sans calcul que

$$\binom{m}{m} + \binom{m+1}{m} + \cdots + \binom{n}{m} = \binom{n+1}{m+1}$$

Formule du binôme
Quels que soient $x_1, x_2 \in \mathbf{C}$,

$$(x_1 + x_2)^n = \sum_{k=0}^{n} \binom{n}{k} x_1^k x_2^{n-k}.$$

Démo: récurrence sur n.

Cas particuliers: pour $x_1 = 1 = x_2$ on retrouve $2^n = \sum_{k=0}^{n} \binom{n}{k}$, pour $x_1 = -1, x_2 = 1$ on a $0 = \sum_{k=0}^{n} (-1)^k \binom{n}{k}$.

Formule multinomiale
Quels que soient $x_1, \ldots, x_m \in \mathbf{C}$,

$$(x_1 + x_2 + \ldots + x_m)^n = \sum_{n_1 + n_2 + \ldots + n_m = n} \frac{n!}{n_1! n_2! \cdots n_m!} x_1^{n_1} x_2^{n_2} \cdots x_m^{n_m}.$$

Démo: récurrence sur $m \geq 2$.

Fonction génératrice
Soit $I \subset \mathbf{R}$ un intervalle tel que $0 \in I$, $(a_k)_{k \in \mathbf{N}}$ une suite d'entiers naturels et $f : I \to \mathbf{R}$ une application de classe C^∞. f est dite fonction génératrice de la suite $(a_k)_{k \in \mathbf{N}}$ si

$$\frac{f^{(k)}(0)}{k!} = a_k, \qquad \text{pour tout } k \in \mathbf{N},$$

où $f^{(k)}(0)$ désigne la dérivée $k-$ ième de f en 0. Une autre manière de dire cela est d'écrire

$$\sum_{k=0}^{\infty} \frac{f^{(k)}(0)}{k!} x^k = \sum_{k=0}^{\infty} a_k x^k \qquad \text{(égalité entre séries formelles)}$$

Exemples:

- le polynôme $(1+x)^n$ est fonction génératrice de la suite finie $(\binom{n}{0}, \binom{n}{1}, \ldots, \binom{n}{n})$
- sur l'intervalle $I =]-1,1[$, $f(x) = \frac{1}{1-x}$ est fonction génératrice de la suite $(1,1,1,\ldots)$ et $f'(x) = \frac{1}{(1-x)^2}$ est génératrice de la suite $(1,2,3,\ldots)$.

évidence très utile : toute identité satisfaite par la fonction génératrice f ou entre fonctions génératrices de suites différentes induit une suite de relations algébriques portant sur les coefficients $(a_k)_{k\in\mathbf{N}}$.

Voici un exemple simple:

- $(1+x)^m(1+x)^n = (1+x)^{m+n}$ est équivalente à

$$\sum_{p\le m, q\le n, p+q=k} \binom{m}{p}\binom{n}{q} = \binom{m+n}{k}, \text{ pour tout } k \le n+m.$$

Pouvez-vous justifier cette identité *sans calcul*?

Quelques exemples classiques

Exercice 1

On se donne un ensemble E, une partition $(A_j)_{1\le j\le m}$ de E et des entiers $p_1, \ldots, p_m$ tels que $p_j \le \mid A_j \mid$ pour tout j.

Notons $P_{p_1,p_2,\ldots,p_m} \subset P(E)$ l'ensemble des parties qui contiennent p_j éléments de A_j pour tout j. On a

$$\mid P_{p_1,\ldots,p_m} \mid = \binom{\mid A_1 \mid}{p_1}\binom{\mid A_2 \mid}{p_2}\cdots\binom{\mid A_m \mid}{p_m}$$

Solution 1: c'est le produit: on note P_{p_j} l'ensemble des parties de cardinal p_j de A_j. Il suffit d'observer que l'application

$$P_{p_1} \times P_{p_2} \times \cdots \times P_{p_m} \to P_{p_1,p_2,\ldots,p_m} : (P_1, P_2, \ldots P_m) \mapsto \bigcup_{j=1}^{m} P_j$$

est une bijection.

Solution 2: si on ne pense pas au produit, on peut par exemple procéder par récurrence sur m. Pour $m=1$ c'est vrai pour tout ensemble E par définition de $\binom{|A_1|}{p_1}$. Voici comment passer de m à $m+1$: l'application

$$P_{p_1,\ldots,p_{m+1}} \to P_{p_1,\ldots,p_m} \subset P(\bigcup_{j=1}^{m} A_j) : P \mapsto P \setminus A_{m+1}$$

est une surjection pour laquelle chaque partie $Q \in P_{p_1,\ldots,p_m}$ admet $\binom{|A_{m+1}|}{p_{m+1}}$ antécédents. Le principe des bergers donne

$$\mid P_{p_1,\ldots,p_{m+1}} \mid = \mid P_{p_1,\ldots,p_m} \mid \binom{\mid A_{m+1} \mid}{p_{m+1}}.$$

Exercice 2

Soit un alphabet $\{a_1, \ldots, a_m\}$ et des entiers $n, n_1, \ldots n_m$ tels que $\sum_{j=1}^m n_j = n$.
On demande de dénombrer les mots de longueur n dans lesquels chaque lettre a_j figure exactement n_j fois.

Solution 1: pour $j \in [1, m]$ on repère la position de la lettre a_j dans un mot en considérant l'ensemble

$$A_j = \{a_{ji}, i \in [1, n]\}$$

où

$$a_{ji} \text{ signifie } \textit{la lettre } a_j \textit{ apparait en position } i \textit{ dans le mot}$$

On prend ensuite

$$E = \bigcup_{j=1}^m A_j$$

et on applique (**5**) à l'ensemble $A = P(E)$ en prenant pour C l'ensemble des parties

$$(P_1, P_2, \ldots, P_m) \in P(A_1) \times P(A_2) \times \cdots \times P(A_m) \subset P(E)^m$$

telles que
(i) $| P_j |= n_j$ (la lettre a_j apparait n_j fois)

(ii) si $a_{ji} \in P_j$ alors quelquesoit $k \neq j, a_{ki} \notin P_k$ (on ne peut placer deux lettres différentes en même position dans un mot).
Le nombre cherché est donc

$$\binom{n}{n_1}\binom{n-n_1}{n_2}\binom{n-(n_1+n_2)}{n_3}\cdots\binom{n-(n_1+\cdots+n_{m-1})}{n_m} = \frac{n!}{n_1!n_2!\cdots n_m!}$$

Solution 2: observer qu'on a déjà la réponse: en effet, dans la formule multinomiale le coefficient

$$\frac{n!}{n_1!\ldots n_m!}$$

compte précisément le nombre de mots en m lettres $x_j, j \in [1, m]$, comportant n_j fois la lettre x_j pour tout j.

Exercice 3

Soit $n, m \in \mathbf{N}^*$.
Déterminer le nombre de $m-$ uplets $(n_1, n_2, \ldots, n_m) \in \mathbf{N}^m$ tels que

(1) $\sum_{j=1}^m n_j \leq n$ (2) $\sum_{j=1}^m n_j = n$

Solution pour (1): pour $m = 2$ il s'agit de compter les points $(n_1, n_2) \in \mathbf{N} \times \mathbf{N}$ du plan affine situés sous la droite affine d'équation $x_1 + x_2 = n$. En commençant par le haut il y en a

$$1 + 2 + \ldots + n + 1 = \frac{(n+2)(n+1)}{2} = \binom{n+2}{2}.$$

Pour $m = 3$ il s'agit de compter les points $(n_1, n_2, n_3) \in \mathbf{N}^3$ situés sous le plan affine d'équation $x_1 + x_2 + x_3 = n$. On peut procéder comme suit: pour chaque $n_1 \in [0, n]$ compter les couples $(n_2, n_3) \in \mathbf{N}^2$ sous la droite d'équation $x_2 + x_3 = n - n_1$, le cas $m = 2$ donne alors

$$\binom{n+2}{2} + \binom{n+1}{2} + \cdots \binom{3}{2} + \binom{2}{2}$$

ce qui vaut $\binom{n+3}{3}$ par l'exercice 0.

On a donc une bonne hypothèse de récurrence: le nombre cherché vaut $\binom{n+m}{m}$. La preuve est identique à ce qui précède.

Voici une autre solution pour (1): on peut associer à toute solution $(n_1, \ldots, n_m)$ la suite strictement croissante d'entiers

$$1 + n_1 < 2 + n_1 + n_2 < \ldots < m + n_1 + n_2 + \ldots + n_m \in [1, m+n]$$

et à partir de cette suite définir une partie de cardinal m de $[1, m+n]$. On a donc une application

$$f : \{(n_1, \ldots, n_m), \sum_{j=1}^{m} n_j \leq n\} \to P_m([1, m+n])$$

qui est en fait une bijection. Conclusion: le nombre de solutions est

$$\mid P_m([1, m+n]) \mid = \binom{m+n}{m}.$$

Solution pour (2): Une solution consiste à observer que si $n_1 + n_2 + \ldots + n_m = n$ alors $n_1 + n_2 + \ldots + n_{m-1} \leq n$ ce qui, pour n fixé, donne une application de l'ensemble des $m-$ uplets solutions de (2) sur l'ensemble des $(m-1)-$ uplets solutions de (1). C' est une bijection de réciproque $(n_1, \ldots, n_{m-1}) \mapsto (n_1, \ldots, n_{m-1}, n - (n_1 + \ldots n_{m-1})$. Conclusion: le nombre cherché est $\binom{n+m-1}{m-1}$.

Une autre solution pour (2) consiste à observer qu'il suffit de faire (nombre de solutions de (1) pour n)-(nombre de solutions de (1) pour $n-1$). C'est donc

$$\binom{n+m}{m} - \binom{n-1+m}{m} = \binom{n+m-1}{m-1}$$