XX Dénombrement

3 juin 2016

Soient E, F et G trois ensembles.

Définition 0.0.1.
On dit que E et F sont *équipotents* s'il existe une bijection de E dans F. Dans ce cas, on notera $E \cong F$ (notation non officielle), et si φ est une bijection de E dans F, on notera $\varphi : E \xrightarrow{\sim} F$.

Proposition 0.0.2.
La relation d'équipotence est une relation d'équivalence.

1 Cardinal d'un ensemble fini

Le programme stipule que parmi les propriétés de la partie 1, les plus intuitives seront admises sans démonstration ; il stipule également que l'utilisation systématique de bijections dans les problèmes de dénombrement n'est pas un attendu du programme.

Définition 1.0.1.
On dit que E est *fini* s'il est vide ou s'il existe $n \in \mathbb{N}^*$ tel que $E \cong [\![1, n]\!]$.
Dans le cas contraire, E est dit *infini*.

Le résultat qui donne un sens à ce que l'on appelle intuitivement *le nombre d'éléments d'un ensemble fini* est alors le suivant :

Théorème 1.0.2.
(i) Soient n, m deux entiers naturels non nuls. Si $[\![1, n]\!] \cong [\![1, m]\!]$, alors $n = m$.
(ii) Cela assure que si un ensemble est fini et équipotent à $[\![1, n]\!]$ pour un certain $n \in \mathbb{N}^*$, alors ce n est unique et est appelé le *cardinal* de E, et est noté $\operatorname{Card} E$, $\#E$ ou $|E|$. Par convention, $\operatorname{Card} \varnothing = 0$.

Démonstration.
La démonstration du premier point se fait par récurrence sur n en posant l'hypothèse (P_n) : pour tout $m \in \mathbb{N}^*$, si $[\![1, m]\!] \cong [\![1, n]\!]$, alors $m = n$.
La démonstration est tout à fait du même style que les démonstrations des résultats 1.0.5 et 1.0.6, et est laissée en exercice. $\square$

Exemple 1.0.3.
1. Pour tout $n \in \mathbb{N}$, $[\![1, n]\!]$ est évidemment fini et de cardinal n.
2. Soient $n, m \in \mathbb{N}$, $n < m$.
   Alors $\operatorname{Card}[\![n, m]\!] = m - n + 1$. En effet, l'application $[\![1, m-n+1]\!] \to [\![n, m]\!]$, $a \mapsto a+n-1$ est une bijection.

Dans toute la suite on supposera que E est fini de cardinal n.

Théorème 1.0.4.
E est équipotent à F si et seulement si (F est aussi fini et $\operatorname{Card} E = \operatorname{Card} F$).

Démonstration.
Si E est vide, F aussi.
Sinon, soit $\varphi : [\![1, n]\!] \xrightarrow{\sim} E$, et $\psi : E \xrightarrow{\sim} F$. Alors $\psi \circ \varphi : [\![1, n]\!] \xrightarrow{\sim} F$. $\square$

Lemme 1.0.5.
Supposons E non vide, et $a \in E$. Alors $E \backslash \{a\}$ est fini de cardinal $n - 1$.

Démonstration.
Le cas où $E = \{a\}$ est évident. Supposons donc que $E \backslash \{a\}$ est non vide.
Soit $\varphi : [\![1, n]\!] \xrightarrow{\sim} E$.
Si $\varphi(n) = a$, posons $\psi = \varphi$.
Si $\varphi(n) = b$ pour b un élément de E différent de a, notons p l'antécédent de a. Donc $p < n$. Posons alors $\psi = \varphi \circ \tau_{p,n}$, où $\tau_{p,n}$ est la transposition de S_n échangeant p et n.
Alors dans tous les cas, $\psi : [\![1, n]\!] \xrightarrow{\sim} E$, et $\psi(n) = a$.
Ainsi, $\psi|_{[\![1,n-1]\!]} : [\![1, n-1]\!] \xrightarrow{\sim} E \backslash \{a\}$, d'où le résultat. $\square$

Théorème 1.0.6.
Soit $A \subset E$. Alors A est fini et $\operatorname{Card} A \leqslant \operatorname{Card} E$. De plus, $\operatorname{Card} A = \operatorname{Card} E$ si et seulement si $A = E$.

Démonstration.
Par récurrence sur $n = \operatorname{Card} E$.
Si $n = 0$, $E = A = \varnothing$, et le résultat est évident.
Soit $n \in \mathbb{N}$ tel que pour tout ensemble E de cardinal n, et pour tout $A \subset E$, on A soit fini et $\operatorname{Card} A \leqslant \operatorname{Card} E$.
Soit E de cardinal $n+1$, et $A \subset E$. Si $A = E$, alors A est fini et $\operatorname{Card} A = \operatorname{Card} E$.
Sinon, soit $a \in E \backslash A$. Posons $\tilde{E} = E \backslash \{a\}$. Alors $\operatorname{Card} \tilde{E} = n - 1$ d'après le lemme précédent, et $A \subset \tilde{E}$. Par hypothèse de récurrence, A est fini, et $\operatorname{Card} A \leqslant n - 1$. En particulier, $\operatorname{Card} A < \operatorname{Card} E$, donc $A \neq E$, ce qui prouve au passage que $\operatorname{Card} A = \operatorname{Card} E$ si et seulement si $A = E$. □

Remarque 1.0.7.
Grâce à ce résultat, pour montrer l'égalité de deux ensembles finis, on peut montrer la double inclusion, mais aussi se contenter d'une inclusion et montrer l'égalité des cardinaux.
Ce résultat est à rapprocher du résultat assurant que deux espaces vectoriels de dimension finie sont égaux si et seulement si l'un est inclus dans l'autre et ils ont même dimension.

Lemme 1.0.8.
Soit f une application surjective de F dans G. Alors il existe une injection de G dans F.

Démonstration.
Soit $y \in G$. Alors y a un (ou plusieurs) antécédent(s) par f. Choisissons un de ces antécédents, par exemple le plus petit, puisque $f^{-1}(\{y\})$ est une partie non vide de $\mathbb{N}$, et notons-le $g(y)$. On définit ainsi une application $g : G \to F$, tel que pour tout $y \in G$, $f(g(y)) = y$. Ainsi, $f \circ g$ est injective, et on sait alors que g est injective de G dans F. □

Exercice 1.0.9.
Montrer que s'il existe une injection $f : F \to G$, alors il existe une surjection $g : G \to F$.

Théorème 1.0.10.
Soit f une application de F dans G.

(i) Si G est fini et f est injective, alors F est fini également, et $\operatorname{Card} F \leqslant \operatorname{Card} G$.

(ii) Si F est fini et f est surjective, alors G est fini également, et $\operatorname{Card} F \geqslant \operatorname{Card} G$.

(iii) Si F et G sont finis et $\operatorname{Card} F = \operatorname{Card} G$, alors :

$$f \text{ est injective} \Leftrightarrow f \text{ est surjective} \Leftrightarrow f \text{ est bijective.}$$

Remarque 1.0.11.
La relation « F a moins d'éléments que G » correspond donc à « F s'injecte dans G » (au moins pour des ensembles finis).

De même, la relation « F a plus d'éléments que G » correspond donc à « F se surjecte sur G » (au moins pour des ensembles finis).

Concernant des ensembles quelconques, le lecteur intéressé pourra se étudier sur le théorème de Cantor-Bernstein.

Remarque 1.0.12.
Une fois encore, ce résultat est à rapprocher des résultats sur les espaces vectoriels et les applications linéaires en dimension finie.

Démonstration. (i) f étant injective, elle établit une bijection de F dans $f(F)$. Or $f(F) \subset G$, donc $f(F)$ est fini et $\operatorname{Card} f(F) \leqslant \operatorname{Card} G$. Ainsi, puisque $F \cong f(F)$, F est fini et $\operatorname{Card} F \leqslant \operatorname{Card} G$.

(ii) En utilisant 1.0.8, soit g injective de G dans F. En appliquant le premier point, G est donc fini et $\operatorname{Card} G \leqslant \operatorname{Card} F$.

(iii) Il suffit de démontrer : f est injective $\Leftrightarrow$ f est surjective, le reste étant alors facile.
Pour le sens direct, si f est injective, f est une bijection de F dans $f(F)$, donc $\operatorname{Card} F = \operatorname{Card} f(F)$. Mais $\operatorname{Card} G = \operatorname{Card} F$, donc $\operatorname{Card} f(F) = \operatorname{Card} G$, et comme $f(F) \subset G$, nous avons $f(F) = G$, ce qui signifie bien que f est surjective.
Pour le sens indirect, soient $x, y \in F$ tels que $f(x) = f(y)$ et $x \neq y$. Alors $f(y) \in f(F \backslash \{y\})$, et donc $f(F \backslash \{y\}) = G$. Par conséquent, $f|_{F \backslash \{y\}}$ est surjective à valeurs dans G, donc avec le point (ii), $\operatorname{Card} F \backslash \{y\} \geqslant \operatorname{Card} G$. Mais $\operatorname{Card} F \backslash \{y\} = \operatorname{Card} F - 1 = \operatorname{Card} G - 1$, ce qui est absurde. Par conséquent, f est aussi injective.

□

Exercice 1.0.13.
Soient $(G, \star)$ un groupe et A une partie ***finie*** non vide de G stable par $\star$. Soit $x \in A$.

1. Soit $\varphi : \mathbb{N}^* \to G$ l'application définie par $\varphi(n) = x^n$. Montrer que φ n'est pas injective.
2. En déduire que $x^{-1} \in A$, puis que A est un sous-groupe de $(G, \star)$.

Corollaire 1.0.14 (Principe des tiroirs, ou *Pigeonhole Principle* en anglais)**.**
Si $m < n$, il est impossible de ranger n paires de chaussettes dans m tiroirs sans en mettre au moins deux dans le même tiroir.

Exercice 1.0.15.
1. On prend un Rubik's Cube fini sur lequel on effectue la même manipulation encore et toujours. Démontrer que l'on finit par se retrouver avec ce Rubik's Cube de nouveau terminé[1].
2. Les membres d'une société internationale sont originaires de six pays différents. La liste des membres contient 1978 noms numérotés de 1 à 1978. Montrer qu'il y a un membre dont le numéro vaut la somme des numéros de deux autres membres venant du même pays ou le double du numéro d'un compatriote.

2 Dénombrement

2.1 Réunion, intersection et complémentaire

Définition 2.1.1.
Lorsque deux ensembles A et B sont disjoints, la réunion de A et B est appelée *union disjointe* de A et B, et est notée $A \sqcup B$.

Théorème 2.1.2.
Soient A et B deux parties de E.

(i) Si A et B sont disjoints, alors $\operatorname{Card}(A \sqcup B) = \operatorname{Card} A + \operatorname{Card} B$;

(ii) $\operatorname{Card}(A \backslash B) = \operatorname{Card} A - \operatorname{Card}(A \cap B)$;

(iii) $\operatorname{Card}(A \cup B) = \operatorname{Card} A + \operatorname{Card} B - \operatorname{Card}(A \cap B)$.

(iv) $\operatorname{Card}\left(\complement_E^A\right) = \operatorname{Card} E - \operatorname{Card} A$.

Démonstration. (i) Soient m, p les cardinaux de A et B, et $\varphi : [\![1, m]\!] \xrightarrow{\sim} A$ et $\psi : [\![1, p]\!] \xrightarrow{\sim} B$.
Soit $\chi : \begin{array}{ccc} [\![1, m+p]\!] & \to & A \sqcup B \\ x & \mapsto & \begin{cases} \varphi(x) & \text{si } x \leqslant m \\ \psi(x-m) & \text{si } x > m \end{cases} \end{array}$.
Cette application est bien définie et il est facile de voir qu'elle est surjective. De plus, A et B étant disjoints, elle est injective, donc $A \sqcup B \cong [\![1, m+p]\!]$, donc $\operatorname{Card}(A \sqcup B) = m + p = \operatorname{Card} A + \operatorname{Card} B$.

(ii) Il suffit d'écrire que $A = (A \cap B) \sqcup (A \backslash B)$ et d'utiliser le premier point.

(iii) Là encore, on remarque que $A \cup B = B \sqcup (A \backslash B)$ et on utilise les deux premiers points.

(iv) Remarquer que $\complement_E^A = E \backslash A$.

□

Remarque 2.1.3.
Il existe une formule qui généralise le résultat précédent à la réunion d'une famille finie d'ensembles finis : c'est la *formule de Poincaré*, aussi appelée *formule du crible*. Elle est hors-programme et sera vue en TD.

2.2 Produit cartésien

Théorème 2.2.1.
Soient E et F deux ensembles finis. Alors $E \times F$ est fini et

$$\operatorname{Card}(E \times F) = (\operatorname{Card} E) \times (\operatorname{Card} F).$$

⚠ Il existe beaucoup d'analogies entre la dimension d'un espace vectoriel et le cardinal d'un ensemble, mais $\dim(E \times F) = \dim E + \dim F$.

Démonstration.
On note :

$$n = \operatorname{Card} E,\ p = \operatorname{Card} F,$$
$$E = \{ e_1, \cdots, e_n \},\ F = \{ f_1, \cdots, f_p \}.$$

[1] Pour mémoire, il y a plus de 43.10^{12} combinaisons possibles sur un Rubik's Cube classique.

Donc $E \times F = \{ (e_i, f_j),\ i \in [\![1, n]\!],\ j \in [\![1, p]\!] \}$.
Donc en notant $A_i = \{ e_i \} \times F$ pour $i \in [\![1, n]\!]$, on a :

$$E \times F = \bigsqcup_{i=1}^{n} A_i,$$

ainsi

$$\begin{aligned}\operatorname{Card} E \times F &= \sum_{i=1}^{n} \operatorname{Card} A_i \\ &= \sum_{i=1}^{n} \operatorname{Card} F \\ &= n \operatorname{Card} F \\ &= \operatorname{Card} E \times \operatorname{Card} F.\end{aligned}$$

□

Remarque 2.2.2.
Ce résultat se généralise facilement par récurrence à un produit de q ensembles finis, $q \in \mathbb{N}^*$:

$$\operatorname{Card}\left(\prod_{i=1}^{q} E_i\right) = \prod_{i=1}^{q} \operatorname{Card} E_i.$$

Exercice 2.2.3.
Combien y a-t'il de possibilités de tirer neuf cartes avec remise dans un jeu de 32 cartes ?

2.3 Applications entre ensembles finis

Théorème 2.3.1.
Soient E et F deux ensembles finis. Alors F^E est fini et

$$\operatorname{Card}\left(F^E\right) = (\operatorname{Card} F)^{\operatorname{Card} E}.$$

Démonstration.
On pose $\varphi : [\![1, n]\!] \xrightarrow{\sim} E$, et :

$$\mu : \begin{array}{ccc} F^E & \to & F^n \\ f & \mapsto & (f \circ \varphi(1), \cdots, f \circ \varphi(n)) = (f \circ \varphi(i))_{i \in [\![1,n]\!]} \end{array}$$

$$\nu : \begin{array}{ccc} F^n & \to & F^E \\ (f_1, \cdots, f_n) = (f_i)_{i \in [\![1,n]\!]} & \mapsto & \left\{ \begin{array}{ccc} E & \to & F \\ x & \mapsto & f_{\varphi^{-1}(x)} \end{array} \right. \end{array}.$$

On vérifie que $\nu \circ \mu = \operatorname{Id}_{F^E}$ et $\mu \circ \nu = \operatorname{Id}_{F^n}$, donc ce sont des bijections. Ainsi $F^E \cong F^n$ et l'on peut conclure avec 1.0.4. □

Définition 2.3.2.
Soit $p \in [\![1, n]\!]$. On appelle *p-arrangement de E* toute injection de $[\![1, p]\!]$ dans E. Autrement dit, un p-arrangement est une manière de choisir p éléments distincts de E **en tenant compte de l'ordre dans lequel on choisit ces éléments** ; c'est donc aussi un p-uplet de E, ou encore une liste de p éléments de E.

Exemple 2.3.3.
Si $E = [\![1, 5]\!]$ et $p = 2$, les applications φ et ψ de $[\![1, 2]\!]$ dans E telles que $\varphi(1) = 3$, $\varphi(2) = 5$, $\psi(1) = 5$ et $\psi(2) = 3$, sont deux p-arrangements **différents** de E.

On peut aussi les identifier aux couples $(3, 5)$ et $(5, 3)$.

Théorème 2.3.4.
Si $\operatorname{Card} E = n$, il y a exactement $\dfrac{n!}{(n-p)!}$ p-arrangements de E.

Démonstration.
Pour construire une injection f de $[\![1, p]\!]$ dans E, il y a n choix possibles pour $f(1)$. Il reste alors $n-1$ choix possibles pour $f(2)$ et ainsi de suite, jusqu'aux $n - p + 1$ choix possibles pour $f(p)$: il y a donc $n \times (n-1) \times \cdots \times (n-p+1)$ injections possibles. □

Remarque 2.3.5.
Les arrangements sont utilisés pour modéliser des tirages **successifs** et **sans remise**.

Exercice 2.3.6.
Vous jouez « au hasard » au tiercé lors d'une course avec 10 partants : combien avez-vous de chance d'avoir le tiercé dans l'ordre ?

Corollaire 2.3.7.
Le groupe S_n des permutations sur n éléments est fini de cardinal $n!$.

Démonstration.
S_n correspond à l'ensemble des n-uplets de $[\![1, n]\!]$. □

2.4 Parties d'une ensemble fini

Définition 2.4.1.
Soit $p \in [\![1, n]\!]$. On appelle p-combinaison de E toute partie de E de cardinal p. Autrement dit, une p-combinaison est une manière de choisir p éléments distincts de E **sans tenir compte de l'ordre dans lequel on choisit ces éléments**. On note alors $\binom{n}{p}$ le nombre de p-combinaisons de E ; ce nombre se lit « p parmi n ».

Remarque 2.4.2.
Les combinaisons sont utilisées pour modéliser des tirages **simultanés**.

Remarque 2.4.3.
On étend cette définition à $p \in \mathbb{Z}$ par $\binom{n}{p} = 0$ lorsque $p \notin [\![0, n]\!]$.

Théorème 2.4.4.
Si $n \in \mathbb{N}$ et $p \in [\![0, n]\!]$, alors $\displaystyle\binom{n}{p} = \frac{n!}{(n-p)!p!}$.

Remarque 2.4.5.
Nous venons donc de donner une nouvelle définition du coefficient binomial $\binom{n}{p}$, défini en début d'année, et que nous avions interprétré comme le nombre de chemin réalisant p succès lors de n répétitions d'une même expérience aléatoire. Remarquons à nouveau qu'il s'agit d'un entier, ce qui n'est absolument pas évident avec la formule du théorème 2.4.4.

Démonstration.
Commençons par remarquer qu'ordonner (totalement) un ensemble à n éléments revient à numéroter ses éléments de 1 à n. Par conséquent, un ordre sur E peut être vu comme une bijection de $[\![1, n]\!]$ dans E, ou encore comme une permutation de E. Il y a donc $n!$ façons d'ordonner un ensemble à n éléments.
Ainsi, pour chaque choix de p éléments parmi n, il existe $p!$ p-arrangements contenant ces p-éléments : il y a donc exactement $p!$ fois plus de p-arrangements que de p-combinaisons. Ainsi, $\displaystyle\binom{n}{p} = \frac{1}{p!} \times \frac{n!}{(n-p)!}$. □

Exercice 2.4.6.
Vous jouez au hasard au tiercé lors d'une course avec 10 partants : combien avez-vous de chance d'avoir le tiercé dans le désordre ?

Proposition 2.4.7 (Formule du triangle de Pascal)**.**
Si $n \in \mathbb{N}$ et si $p \in \mathbb{N}$, $\displaystyle\binom{n}{p} = \binom{n-1}{p-1} + \binom{n-1}{p}$.

Démonstration.
On donne ici une preuve combinatoire. Le cas où $p \notin [\![1, n-1]\!]$ est évident. Sinon, soit E de cardinal n et $a \in E$. Notons F_p l'ensemble des parties de E a p éléments, alors

$$F_p = \underbrace{\{A \subset E \mid \#A = p \text{ et } a \in A\}}_{A_p} \sqcup \underbrace{\{A \subset E \mid \#A = p \text{ et } a \notin A\}}_{B_p}.$$

Il est évident *(sinon, détaillez le !)* que A_p est en correspondance bijective avec l'ensemble des parties de $E \setminus \{a\}$ ayant $p-1$ éléments (par $A \mapsto A \setminus \{a\}$) et possède donc $\binom{n-1}{p-1}$ éléments. De même, B_p est en correspondance bijective avec l'ensemble des parties de $E \setminus \{a\}$ ayant p éléments (par $A \mapsto A$) et possède donc $\binom{n-1}{p}$ éléments. Cela permet donc de conclure, car $\#F_p = \#A_p + \#B_p$. □

Proposition 2.4.8 (Formule du binôme de Newton)**.**
Soit x et y deux éléments d'un anneau $(A, +, \cdot)$ commutant l'un avec l'autre ($xy = yx$), soit $n \in \mathbb{N}$. Alors

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

Démonstration.
En voici une preuve combinatoire. On montre d'abord aisément par récurrence que toutes les puissances de x et de y commutent. Ensuite, lorsque l'on développe le produit

$$(x+y)^n = \underbrace{(x+y)\cdots(x+y)}_{n \text{ fois}}$$

on obtient des termes qui sont des produits de k facteurs valant x, et de $n-k$ facteurs valant y, pour k allant de 0 à n. Or, pour chacun de ces k, il y a k parmi n possibilités d'obtenir un produit de k facteurs valant x, et de $n-k$ facteurs valant y, d'où le résultat. □

Théorème 2.4.9.
Si E est fini, l'ensemble $\mathscr{P}(E)$ des parties l'est aussi et

$$\operatorname{Card} \mathscr{P}(E) = 2^{\operatorname{Card} E}.$$

Démonstration.
Pour tout $i \in [\![0, n]\!]$, notons P_i l'ensemble des parties de E ayant i éléments. Nous avons alors $\mathscr{P}(E) = \bigsqcup_{i=0}^{n} P_i$. Or chaque P_i est de cardinal $\binom{n}{i}$, donc $\mathscr{P}(E)$ est fini et :

$$\begin{aligned}\operatorname{Card} \mathscr{P}(E) &= \sum_{i=0}^{n} \binom{n}{i} \\ &= (1+1)^n \qquad \text{(binôme de Newton)} \\ &= 2^n.\end{aligned}$$

On peut aussi voir qu'il y a une correspondance bijective entre les parties de E et les applications à variables dans E et à valeurs dans $\{0,1\}$, par $\mathscr{P}(E) \to \{0,1\}^E$, $A \mapsto \mathbf{1}_A$. □