Chap. J1 : dénombrement et probabilités dans un univers fini

Jouons un peu : *alea* en latin et *az zahr* en arabe : le dé.

§0 Préliminaire : une différence de point de vue pour l'introduction des probabilités entre le lycée et le cours de prépa. :

Au lycée, vous avez parlé de probabilité essentiellement sans parler de dénombrement. Les notions de probabilités, de variables aléatoires, étaient en quelque sorte *premières*, c'est-à-dire non définies à partir d'autre. Par exemple, pour plusieurs tirages à pile ou face successifs, disons 3, d'une pièce équilibrée, vous avez évalué la probabilité d'obtenir trois fois « pile » comme $1/2\times1/2\times1/2$ en voyant ces tirages comme trois tirages de Bernoulli indépendants, et en dessinant un arbre. Cette probabilité 1/2 pour un lancer était un fait non déduit d'autre chose et de même pour la notion d'indépendance. Vous avez aussi parlé de loi binomiale de la même façon.

Nous retrouverons ce type de calcul au chapitre J2 qui sera centré sur la notion de *variable aléatoire*. Dans ce chapitre J1, nous nous concentrons d'abord sur les fondements mathématiques de ce qu'est une probabilité sur un ensemble (univers) fini Ω. Par exemple on dira, pour trois lancers de pièces, que l'univers de possibles est celui des triplets (r_1, r_2, r_3) où chaque résultat r_i est un élément d'un ensemble à deux éléments $\{P, F\}$. De la sorte $\Omega = \{P, F\}^3$ est un ensemble à 8 éléments. En supposant que chaque issue est équiprobable (en quelque sorte nous sommes des dieux qui contemplons toutes les réalisations possibles et qui leur attribuons un poids), on définit une probabilité sur cet univers et on retrouve la probabilité $1/(2^3)$ (plutôt que $(1/2)^3$ suivant le calcul de terminale, noter la nuance).

Certains exercices vous paraîtront plus difficiles avec ce point de vue par rapport à des méthodes vues au lycée, mais rassurez-vous, nous retrouverons ces méthodes, mieux comprises, dès le chapitre J2. Il n'est en effet pas toujours nécessaire, dans les exercices, de connaître tout l'univers des possibles pour calculer des probabilités. De même, la notion d'indépendance est une notion cruciale en probabilité qui peut parfois être considérée comme première dans la modélisation probabiliste d'un phénomène. Mais le cadre mathématique des univers est :

• indispensable du point de vue théorique, pour la construction ensuite des variables aléatoires qui vérifient ce qu'on attend d'elles du point de vue pratique,

• incontournable aussi pour certains calculs de probabilités, souvent plus difficiles, qu'on ne peut faire que par dénombrement.

I Ensembles finis et dénombrement :

Enjeu : l'essentiel est la *pratique* du dénombrement qu'on développe à partir du § 3) et les résultats et formules qui s'y trouvent. Le 1), après avoir abordé quelques problèmes théoriques, veut surtout insister sur le fait que c'est le concept de *bijection* qui est au coeur du dénombrement. Le 2) rappelle des formules *déjà connues* de calcul de cardinaux, cruciales pour la suite, en expliquant comment on peut, si on en ressent le besoin, les déduire rigoureusement du 1).

1) Théorie : Le point commun entre 4 bananes et 4 carottes, cardinaux.

Avertissement : *Beaucoup d'énoncés de ce paragraphe sembleront « évidents » : tant mieux, et qu'ils le restent. Mais pour ceux et celles qui aimeraient quand même comprendre ou sentir comment ils s'articulent avec une construction mathématique, on donne quelque détails ici. Aucune démonstration du 1) n'est demandée pour le programme de colle*

Point de départ : Au chapitre **(A2)** on a défini l'ensemble $\mathbb{N}$ des entiers naturels (axiomes de $\mathbb{N}$), avec son ordre. Pour un élément $n \in \mathbb{N}$, on sait donc ce qu'est l'ensemble $[\![1, n]\!]$ par exemple.

a) Lemme (admis) : Les sous-ensembles $[\![1, n]\!]$ et $[\![1, m]\!]$ de $\mathbb{N}$ sont en bijection ssi $n = m$.

Ce résultat intuitivement évident est à la base de ce qu'on appelle compter ou encore de notre intuition des nombres ! On peut le prouver à l'aide de la déf. axiomatique de $\mathbb{N}$ i.e. du principe de récurrence, mais cette dém. n'est pas exigible (cf. appendice).

b) (i) Déf. $E \neq \varnothing$ est fini s'il existe un $n \in \mathbb{N}^*$ tel que E soit en bijection avec $[\![1, n]\!]$.

Ce nombre n, défini de façon unique par le a), s'appelle cardinal de E.

Convention : on convient que $\varnothing$ est fini aussi et $\mathrm{Card}(\varnothing) = 0$,

(ii) Lemme : deux ensembles finis sont en bijection si, et seulement si, ils ont même cardinaux.

c) Lemme (admis) Si E fini et $A \subset E$ alors $\mathrm{Card}(A) \leq \mathrm{Card}(E)$ et si en plus $A \subset E$ est différent de E alors $\mathrm{Card}(A) < \mathrm{Card}(E)$ (dém. par réc. admise).

d) Prop (*se démontre seulement à partir de ce qui précède*) Soient E et F deux ensembles finis :

(i) s'il existe une injection de E dans F alors $\mathrm{Card}(E) \leq \mathrm{Card}(F)$.
(ii) s'il existe une surjection de E dans F alors $\mathrm{Card}(E) \geq \mathrm{Card}(F)$.

e) Prop. Soient E et F deux ensembles finis et $f : E \to F$.

(i) f est injective ssi $\mathrm{Card}(f(E)) = \mathrm{Card}(E)$.
(ii) f est surjective ssi $\mathrm{Card}(f(E)) = \mathrm{Card}(F)$.
(iii) Si E et F ont le même cardinal :
$f : E \to F$ est bijective ssi elle est injective ssi elle est surjective

2) Résultats déjà connus sur les cardinaux

a) Cardinal d'une réunion : *dém. de* $\mathrm{Card}(A \cup B) = \mathrm{Card}\ (A) + \mathrm{Card}\ (B) - \mathrm{Card}(A \cap B)$.

(i) Pourquoi ce résultat est intuitivement "évident" ?
(ii) On le déduit quand même des notions précédentes à partir du cas où A et B disjoints.
(iii) Rem. : Pour $A_1, \ldots, A_n$ *deux à deux disjoints*, on a par réc. immédiate :

$$\mathrm{Card}(\bigcup_{i=1}^{n} A_i) = \sum_{i=1}^{n} \mathrm{Card}(A_i).$$

b) Lemme des bergers : Si $f : E \to F$ est telle que tout élément de F a exactement p antécédents par f, alors $\mathrm{Card}(E) = p\,\mathrm{Card}(F)$.

c) Cardinal d'un produit : $\mathrm{Card}\ (A \times B) = \mathrm{Card}(A).\mathrm{Card}(B)$.

Corollaire (réc.) : pour tout $n \in \mathbb{N}^*$, $\mathrm{Card}(E^n) = \mathrm{Card}(E)^n$.

d) Cardinal pour une arborescence (généralise le calcul du cardinal d'un produit) :
Soit E un ensemble de p-uplets $(x_1, \ldots, x_p)$ tels que :
• x_1 peut prendre n_1 valeurs,
• *pour chaque valeur de l'entrée* x_1, l'entrée x_2 peut prendre n_2 valeurs,
⋮
• *pour chaque valeur de* $(x_1, \ldots, x_{p-1})$, l'entrée x_p peut prendre n_p valeurs.

Représentation de E comme l'ensemble des chemins de la racine aux feuilles d'une arborescence. Alors, le lemme des bergers permet de montrer par récurrence que :

$$\mathrm{Card}(E) = n_1 \times \cdots \times n_p.$$

3) Résultats nouveaux : dénombrement d'ensembles d'applications

Méthodes pour dénombrer :
• par bijection, se ramener à un ensemble de cardinal connu (du type du § 2),
• parfois, quand le problème se ramène par bijection à une arborescence, on n'explicite pas la bijection, mais on se contente de « multiplier les choix » (rédaction moins rigoureuse mais plus rapide : faire seulement attention que les choix ne se recoupent pas, i.e. qu'on a bien une arborescence. Cette rédaction passe bien pour les exercices d'oraux. Aux écrits ce seraient des récurrences.)

a) Dénombrement de l'ensemble $\mathcal{A}(E,F)$ des applications de E dans F :

Idée : si $p = \mathrm{Card}(E)$, si F est un ensemble quelconque ; et si on indice les éléments de E de sorte que $E = \{a_1, \dots, a_p\}$, on code une application $f : E \to F$ par la donnée d'un p-uplet $(y_1, \dots, y_p) \in F^p$ avec la convention que $y_1 = f(a_1), \dots, y_p = f(a_p)$.

On en déduit une bijection entre $\mathcal{A}(E,F)$ et F^p.

Conséquence : si E et F sont finis, $\boxed{\mathrm{Card}(\mathcal{A}(E,F)) = \mathrm{Card}(F)^{\mathrm{Card}(E)}.}$

Notation générale : si E et F sont deux ensembles qcq, $\boxed{\mathcal{A}(E,F) \text{ est aussi noté } F^E}$.

(Notation déjà connue pour $\mathbb{R}^{\mathbb{N}} = \mathcal{F}(\mathbb{N},\mathbb{R})$ l'ensemble des suites réelles par exemple).

b) Détermination du nombre d'injections de E_p dans F_n :

(i) **Première partie :** le codage du a) donne encore une bijection entre l'ensemble $\mathcal{I}(E,F)$ des injections de E dans F et l'ensemble des p-uplets (ordonnés par déf. !) d'éléments de F *deux à deux distincts*.

Définition : Un p-uplet d'éléments de E *deux à deux distincts* s'appelle un *arrangement* de p éléments de E.

(ii) **Deuxième partie :** Dénombrement des arrangements par récurrence et lemme du berger (arborescence).

Avec la conclusion :

$$\boxed{\mathrm{Card}(\mathcal{I}(E_p,F_n)) = \mathrm{Card}(\mathfrak{a}_p(F)) = n(n-1)\dots(n-p+1)}$$

Preuve rédigée en appendice.

c) Corollaire :

$$\boxed{\begin{array}{l}\text{Si } E_n \text{ et } F_n \text{ sont deux ensembles de card. } n \text{ et si } \mathcal{B}(E_n,F_n) \text{ désigne l'ensemble des bijections}\\ \text{de } E_n \text{ dans } F_n \text{ alors } \mathrm{Card}(\mathcal{B}(E_n,F_n)) = n!\end{array}}$$

Cas particulier $E_n = F_n$: si on note $\mathcal{B}(E_n)$ l'ensemble des bijections de E_n dans lui-même, alors :

$$\boxed{\mathrm{Card}(\mathcal{B}(E_n)) = n!.}$$

Une telle bijection est aussi appelée *permutation* de E_n.

4) Dénombrement des parties d'un ensemble :

a) Calcul du cardinal de $\mathcal{P}(E)$, encore une bijection :

(i) Codage de sous-ensembles de E par des n-uplets de 0 et de 1 où $n = \mathrm{Card}(E)$:

Idée donnée pour $E = \{a_1, a_2, a_3\}$ un ensemble à trois éléments : A chaque sous-ensemble A de E on associe un triplet $c(A) \in \{0,1\}^3$, dont la première entrée vaut 1 si $a_1 \in A$, 0, sinon, et de même la deuxième entrée vaut 1 si $a_2 \in A$ et 0 sinon, et enfin la troisième entrée vaut 1 si $a_3 \in A$ et 0 sinon.

Ainsi si $A = \{a_1, a_3\}$, on aura $c(A) = (1,0,1)$. Si $A = \{a_2\}$, on aura $c(A) = (0,1,0)$ et si $A = \varnothing$, on aura $c(A) = (0,0,0)$.

On définit ainsi une application $c : \mathcal{P}(E) \to \{0,1\}^3$. Or si on se donne un triplet quelconque dans $\{0,1\}^3$, il code clairement un sous-ensemble de A et un seul. Par exemple $(1,1,0)$ code $\{a_1, a_2\}$.

Ainsi $c : \mathcal{P}(E) \to \{0,1\}^3$ est bijective et $\mathrm{Card}(\mathcal{P}(E)) = 2^3$.

La même construction s'applique à un ensemble E de cardinal n quelconque : on a ainsi une bijection de $\mathcal{P}(E)$ dans $\{0,1\}^n$, qui donne le résultat à retenir :

$$\boxed{\text{Si } E \text{ est de cardinal } n \text{ alors } \mathrm{Card}(\mathcal{P}(E)) = 2^n.}$$

(ii) Une façon plus snob de faire la même chose (si on aime) : on considère l'application

$$\chi : \mathcal{P}(E) \to \mathcal{F}(E, \{0,1\}), \quad A \mapsto \chi_A,$$

où χ_A notée aussi 1_A est la fonction caractéristique de A.

Par déf. $\forall\, x \in E,\ \chi_A(x) = \begin{cases} 1 \text{ si } \ x \in A, \\ 0 \quad \text{sinon.} \end{cases}$

De même cette application χ est bijective, ce qui donne que $\mathrm{Card}(\mathcal{P}(E)) = \mathrm{Card}(\{0,1\}^E) = 2^n$.

Le lien entre ces deux preuves est simplement l'identification d'une application de E dans $\{0,1\}$ à un n-uplet d'éléments de $\{0,1\}$, qu'on a mise en évidence au 3) a).

b) Calcul du $\mathrm{Card}(\mathcal{P}_p(E))$ où l'on note $\mathcal{P}_p(E)$ l'ensemble des parties à p éléments d'un ensemble E.

Prop. Si E est de cardinal n alors $\mathrm{Card}\,\mathcal{P}_p(E) = \dfrac{n!}{p!(n-p)!}$.

Preuve : en considérant l'application d'oubli de l'ordre : $\mathfrak{a}_p(E) \to \mathcal{P}_p(E)$, $(a_1, \ldots, a_p) \mapsto \{a_1, \ldots, a_p\}$.

Alors pour tout $A \in \mathcal{P}_p(E)$, cet ensemble A a exactement $p!$ antécédents par l'application F : tous les p uplets obtenus par permutation des éléments de A.

Le lemme des bergers donne alors que $p!\,\mathrm{Card}(P_p(E)) = \mathrm{Card}\,\mathfrak{a}_p(E)$ ce qui donne la conclusion :

$$\mathrm{Card}(P_p(E)) = \frac{\mathrm{Card}\,\mathfrak{a}_p(E)}{p!}$$

□

c) Obtention « naturelle » de la formule du binôme :

(i) Que sait-on des binomiaux depuis le chapitre A ?

• Pour en donner une définition mathématiquement irréprochable, au chapitre A, on a introduit le symbole $\binom{n}{p}$ avec une définition par récurrence double (convenablement initalisée). La formule de récurrence est la formule du triangle de Pascal

$$\binom{n+1}{p} = \binom{n}{p} + \binom{n}{p-1}. \tag{1}$$

• Avec cette formule de récurrence, on a prouvé que ces coefficients étaient ceux qui apparaissent dans le formule du binôme :

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}. \tag{2}$$

• Au chapitre A, on avait fait tomber du ciel la formule explicite :

$$\binom{n}{k} = \frac{n!}{k!(n-k)!} \tag{3}$$

qu' on avait néanmoins démontrée à l'aide de (1). Ce qui manquait était la façon de *trouver* cette formule.

• On vient de voir surgir au b), le second membre de (3) comme le nombre de parties à k éléments d'un ensemble à n éléments.

On a donc démontré que :

$\binom{n}{k}$ est le nombre de parties à k éléments d'un ensemble à n éléments,

mais le chemin qui nous a fait arriver à cette affirmation peut sembler un peu indirect. On voudrait donner au (ii) ci-dessous, un chemin direct qui suit davantage ce qu'on a pu vous dire au lycée sur le nombre de chemins dans un arbre. Mathématiquement, c'est moins facile à rédiger, mais pour l'intuition c'est essentiel !

(ii) Interprétation combinatoire de la formule du binôme : développer $(a+b)^n$ c'est faire une somme de 2^n termes où chaque terme correspond au choix de a ou b dans chacune des n parenthèses. On peut faire un arbre de ces choix. Pour une valeur de k donnée, les termes qui seront de la forme $a^k b^{n-k}$ sont exactement les termes où on aura choisi k parenthèses avec un a (et donc $n-k$ avec un b). Combien y-a-t-il de tels termes ? Exactement le nombre de façons de choisir k parenthèses parmi n, autrement dit, le nombre de parties à k éléments d'un ensemble à n éléments, d'où l'égalité :

$$\binom{n}{k} = \operatorname{Card} \mathcal{P}_k(E_n).$$

5) Exercices standards (dont les résultats ne sont pas des prop. au programme)

a) Compter les séparations :

Enoncé : soit $(n,p) \in \mathbb{N}^2$. Déterminer : Card $\{(x_1,\dots,x_p) \in \mathbb{N}^p,\ x_1+\cdots+x_p = n\}$.

Terminologie : un p-uplet $(x_1,\dots,x_p) \in \mathbb{N}^p$ tel que $x_1+x_2+\cdots+x_p = n$ s'appelle parfois une *partition* de l'entier n.

Une belle heuristique :

L'idée est de voir chaque n comme la somme $1+\cdots+1$ de n fois le chiffre 1 et de voir une partition $(x_1,\dots,x_p)$ comme une séparation de cette somme de 1 dans p tiroirs différents :

$$n = \underbrace{1+\cdots+1}_{x_1 \text{ fois } 1} + \cdots\cdots + \underbrace{1+\cdots+1}_{x_p \text{ fois } 1}.$$

Chaque 1 est un petit soldat et on met ces soldats dans p tiroirs. On va compter les séparations.

Entre les p tiroirs, on a $p-1$ séparation. Pour se donner une partition de l'entier n, il (faut et) il suffit de se donner la place des $p-1$ séparations.

On considère donc qu'on a deux signes 1 et 0 et qu'on code les séparations avec des 0 qu'on va mettre entre les 1.

Par exemple pour $n=9$, la partition de n qui vaut $(x_1,x_2,x_3) = (3,1,5)$, sera codée par $(1,1,1,0,1,0,1,1,1,1,1)$.

Bien sûr on peut avoir des tiroirs vides par exemple $(7,0,2)$ sera codé par $(1,1,1,1,1,1,1,0,0,1,1)$.

Ce codage est bien bijectif sur l'ensemble des $n+(p-1)$ -uplets de 1 et de 0 ayant exactement $p-1$ entrée égale à 0 : par exemple avec l'exemple précédent, si on se donne le 11-uplet $(1,1,1,0,1,1,1,1,0,1,1)$ il code $(3,4,2)$ et seulement $(3,4,2)$.

Or il y a $\binom{n+p-1}{p-1}$ tels uplets (le nombre de choix possibles pour placer les $p-1$ zéros parmi les $n+p-1$ entrées).

Conclusion : le cardinal cherché vaut $\binom{n+p-1}{p-1} = \binom{n+p-1}{n}$.

La preuve précédente est-elle rigoureuse mathématiquement ? oui car on a remplacé les petits soldats et les tiroirs par des objets bien mathématiques, les 0 et les 1. Néanmoins, on peut la reformuler de manière plus concise, en construisant d'autres bijections plus commode à formuler mathématiquement.

b) Nombre d'applications strictement croissantes : entre $E = [\![1,n]\!]$ et $F = [\![1,p]\!]$. Cf. notes manuscrites.

c) Exercice (où on raisonne plutôt avec une arborescence) Déterminer le nombre de surjections de $[\![1,n+1]\!]$ dans $[\![1,n]\!]$.

Choisir une surjection f de E_{n+1} dans F_n c'est :

• choisir b l'élément de F qui a 2 antécédents : n choix.

• le choix précédent ayant été fait, choisir l'ensemble A formé de ces deux antécédents : $\binom{n+1}{2}$ choix.

• définir $f_{|E\setminus A} : E \setminus A \to F \setminus \{b\}$ qui est une bijection quelconque entre ces deux ensembles à $n-1$ éléments : $(n-1)!$ choix.

Le nombre total de ces surjections est alors de $n.\binom{n+1}{2}(n-1)! = n!\binom{n+1}{2}$.

Vous n'aimez pas cette preuve ? Méditez sur la multiplication des choix ici, qui vient du lemme des bergers. Voir aussi exercice de la planche qui donne sinon une formule de récurrence pour le nombre de surjections en toute généralité !

6) Exercices de dénombrements d'objets plus concrets : boules dans des urnes etc

Voir planche et partie suivante avec le langage des proba.

II Introduction aux probabilités dans un univers fini :

0) La notion d'expérience aléatoire :

Des *expériences aléatoires que nous connaissons* : lancer des dés, tirer une carte, jouer à pile ou face pour ce qui est des jeux, mais aussi, pour la vie courante : attendre un autobus à 18 heures, observer la transmission des caractères génétiques dans une famille.

Le résultat de *chaque* expérience est *imprévisible* avec les données dont nous disposons. Mais l'idée *d'expérience* contient implicitement ici (comme cela doit toujours être le cas en science) l'idée d'*expérience reproductible* dans des conditions *identiques pour autant que l'observateur puisse les mesurer*. Ces conditions ne sont pas vraiment identiques en réalité : on ne lance pas les dés de la même façon, mais on ne contrôle pas ce lancer.

En réalité, il faudrait distinguer ce *hasard déterministe* qui intervient dans les phénomènes en principe parfaitement décrit par la physique classique, mais où l'imprécision de notre connaissance des conditions initiales tient lieu de hasard, et le hasard de la physique quantique, qui est un *vrai hasard* qui ne provient pas d'une ignorance des conditions, mais est intrinsèque à la description théorique.

La théorie des probabilités s'intéresse à un modèle qui pourra décrire les résultats de ces expériences renouvelées un grand nombre de fois.

1) Univers et événements associés à une expérience aléatoire :

a) L'univers :

Pour représenter une *expérience aléatoire*, on considère qu'on peut définir l'ensemble Ω de tous les résultats possibles de l'expérience. L'ensemble Ω s'appelle *l'univers* associé à notre expérience.

• Si on lance un dé : $\Omega =$

• Si on lance un dé rouge et un dé vert : $\Omega =$

• Si on tire 2 fois à la suite une pièce à pile ou face (et on note successivement les résultats des deux lancers) : $\Omega =$

Dans tout ce cours de première année, l'univers Ω sera un ensemble **finie**.

Remarque : le choix de l'univers pour représenter notre expérience n'est pas toujours aussi évident. On verra plus tard (cf. **III et J2**) qu'on pourra aussi raisonner en proba. sans *expliciter* l'univers de l'expérience, mais cet univers sera toujours *là, derrière*.

Terminologie : Un élément de l'univers peut être appelé *un résultat, une issue, une réalisation...*

Exercice/exple : trois univers différents pour modéliser des tirages de boules

On dispose d'une boite avec N boules supposées discernables (par exemples des boules de loto avec un numéro dessus). On va tirer n boules de la boîte de plusieurs façons différentes.

Donner un univers mathématique Ω modélisant les résultats dans les cas suivants, et préciser son cardinal :

(i) On tire les n boules en même temps, sans s'occuper de mettre un ordre dans les boules tirées.

(ii) On tire les n boules l'une après l'autre en les rangeant sur un rail dans l'ordre du tirage (l'ordre compte)

(iii) On tire les n boules avec remise : à chaque fois qu'on sort une boule, on note son numéro, puis on la remet dans la boîte. On s'intéresse à la suite (dans l'ordre du tirage) des numéros obtenus.

b) Le langage des événements :

(i) Exemple : pour le tirage de deux pièces à pile ou face, on s'intéresse à l'« événement » : « on obtient deux fois le même résultat ». Cet événement est réalisé pour les deux tirages (P,P) et (F,F).

On va appeler *événement* ce sous-ensemble $\{(P,P),(F,F)\}$ de Ω.

(ii) **Définition générale :** on appelle *événement* E tout sous-ensemble de notre univers fini Ω.

Exercice : On tire un dé rouge et un dé vert. Décrire l'événement : « la somme des dés fait 8 ».

(iii) **Evénements particuliers :** on appelle
- événement *certain* l'événement $E =$
- événement *impossible* l'événement $E =$
- événement *élémentaires* tous les événements de la forme $E = \{\omega\}$ où $\omega \in \Omega$.

(iv) **Opérations sur les événements :**

Terminologie : soit Ω un univers fini et A et B deux événements de cet univers.
- on appelle *événement contraire de* A, l'événement $E =$
- on appelle *événement « A ou B »*, l'événement $E =$
- on appelle *événement « A et B »*, l'événement $E =$

Scholie : on se permet en proba. ce que je vous avais très précisément interdit au chapitre A1. Je n'acceptais pas et continue à ne pas accepter, si A et B sont des ensembles que l'on parle de l'ensemble « A ou B », (le ou étant réservé aux prop. logiques), mais je l'accepte dans le cadre du langage des *événements*.

N.B. De la même façon, un langage informatique n'acceptera pas une syntaxe du style :
`a==3 or 4`
car le `or` relie deux booléens, et la phrase correcte sera : `a==3 or a==4`.

(v) **Relation entre des événements :**

Soit A et B deux événements d'un univers Ω. On dit que :
- A et B sont *incompatibles* ssi
- A entraîne B ssi

Exple : l'événement A « obtenir deux fois piles » entraîne l'événement B « obtenir deux fois de suite le même résultat ».

(vi) **Système complet d'événements :**

Déf. : Soit Ω un univers fini. On appelle *système complet d'événements* (incompatibles) de Ω toute famille $(E_i)_{i\in[\![1,n]\!]}$ telle que :
- $\forall\,(i,j) \in [\![1,n]\!]^2,\ i \neq j \Rightarrow E_i \cap E_j = \varnothing$,
- $\bigcup_{i=1}^{n} E_i = \Omega$.

2) Probabilités :

a) Qu'est-ce qu'intuitivement une probabilité ? Deux types de réponses

(i) Réponse de l'homme de la rue : la probabilité d'un événement A est la « chance » qu'on a que A arrive *parmi* tous les événements concurrents possibles.

(ii) Une première façon de considérer cette « chance » (celle qui sera le plus souvent la nôtre) : embrasser du regard tout l'univers des possibles.

> "The probability of an event is greater or less, according to the number of chances by which it may happen, compared with the whole number of chances by which it may happen or fail". Abraham De Moivre, The doctrine of Chances, London 1718.

• Sur l'exemple du lancer de deux dés équilibrés : $\Omega = [\![1,6]\!]^2$, et on associe à chaque couple $(1,1)$, $(1,2),\ldots$ la même *probabilité* de $1/36$. On définit la probabilité d'un événement comme la somme des probabilités des événements élémentaires qui le constitue.

Exercice : trouver la probabilité des événements : « la somme des deux dés vaut k » suivant les valeurs de k.

• Sur l'exemple du lancer d'un seul dé non équilibré : on va attribuer à chaque face une certaine *probabilité*.

(iii) Une deuxième façon de considérer cette chance : l'approche fréquentiste.

Pour évaluer la « chance » qu'un événement E se réalise dans une expérience aléatoire, on peut répéter n fois cette expérience et considérer la fréquence $F_n(E)$ qui est le nombre de fois où E a été obtenu divisé par n.

Les fréquences ont beaucoup de point commun avec les proba. qu'on va définir : elles sont entre 0 et 1, et s'ajoute pour des événements disjoints. Elles ont l'inconvénient de dépendre de n. D'un certain point de vue les proba. vont être des *fréquences idéalisées*.

Remarque : le lien entre les deux points de vue du (ii) et (iii) est souvent *implicite* dans notre compréhension des probabilités. Expérimentalement (par exemple pour le dé non équilibré) ce seront souvent les fréquences qui vont donner le modèle (mais pas toujours : on peut savoir au départ comment le dé est construit). Il n'est pas clair *a priori* que le modèle global donne un résultat en terme de fréquence. (C'est un théorème, pas évident, des probabilités : la loi des grands nombres, nous en reparlerons).

b) Définition axiomatique d'une probabilité sur un univers fini :

(i) **Déf.** Soit Ω un univers **FINI** non vide.
Une probabilité sur Ω est une application $P : \mathcal{P}(\Omega) \to [0,1]$ telle que :
- $P(\Omega) = 1$,
- pour toutes parties disjointes A et B de Ω, $P(A \cup B) = P(A) + P(B)$.

(ii) **Rem.** Bien sûr le même univers Ω peut être muni de différentes probabilités P. Penser à l'exemple du dé pipé ou non.

Terminologie : on appelle *espace probabilisé* un couple (Ω, P) où Ω est un ensemble (pour nous fini) et P est une probabilité sur Ω.

c) Conséquences de la déf. axiomatique d'une probabilité sur un univers fini :

Prop. Soit (Ω, P) un espace probabilisé fini, alors pour tous les événements A et B dans Ω :
(i) Pour tout $A \in \mathcal{P}(\Omega)$, $P(A^c) =$
(ii) $P(\varnothing) =$
(iii) si $A \subset B$ alors $P(A) \leq P(B)$ (on dit que P est croissante)
(iv) $P(A \cup B) = P(A) + P(B) - P(A \cap B)$.

N.B. Ce n'est PAS parce que le (iv) ressemble à la formule des quatre cardinaux que ces proba. ont un lien quelconque avec un cardinal ! Preuve *axiomatique*.

d) Probabilité d'une réunion de n événements :

(i) **Le cas des réunions disjointes :** si $A_1, \dots, A_n$ sont des événements deux à deux incompatibles dans un espace probabilisé (Ω, P) alors :

$$P\left(\bigcup_{i=1}^{n} A_i\right) =$$

En particulier, si $(A_i)_{i \in [\![1,n]\!]}$ est un *système complet* d'événements de Ω alors : $\sum_{i=1}^{n} P(A_i) =$

(ii)**Dans le cas d'une réunion quelconque une inégalité :** si $A_1, \dots, A_n$ sont des événements quelconques d'un univers Ω alors :

$$P(A_1 \cup \dots \cup A_n) \leq P(A_1) + \dots + P(A_n).$$

(iii) Exercice standard : sous les hyp. du (ii) montrer que :
$P(A_1 \cup A_2 \cup A_3) = P(A_1) + P(A_2) + P(A_3) - P(A_1 \cap A_2) - P(A_1 \cap A_3) - P(A_2 \cap A_3) + P(A_1 \cap A_2 \cap A_3)$.

e) Partition par un système complet d'événements :

Prop. (facile) Si $(E_i)_{i \in [\![1,n]\!]}$ est un système complet d'événements d'un univers Ω alors

$$\boxed{\forall\, A \in \mathcal{P}(\Omega),\ P(A) = \sum_{i=1}^{n} P(A \cap E_i).}$$

f) Le retour du point de vue des proba. des événements élémentaires : (cf. a) (ii))

(i) **Prop.** Soit $\Omega = \{\omega_1, \dots, \omega_n\}$ un univers fini non vide.
Pour toute famille $(p_i)_{i\in[\![1,n]\!]}$ de nombres dans $[0,1]$ tels que $\sum_{i=1}^{n} p_i = 1$, il existe une unique probabilité P sur Ω telle que $P(\{\omega_i\}) = p_i$ pour tout $i \in [\![1,n]\!]$.

(ii) **Cas particulier :** si tous les p_i sont égaux à $1/n$ on dit que la proba. est uniforme.

(iii) **Lien proba/cardinaux dans le cas uniforme :** Si P est une proba. uniforme sur un univers fini Ω alors :

$$\text{pour tout événement } A \text{ de } \Omega,\ P(A) = \frac{\mathrm{Card}(A)}{\mathrm{Card}(\Omega)}.$$

Dans ce cas uniforme, les calculs de proba. peuvent se ramener à un calcul de dénombrement.
Un cas typique de proba. uniforme : les tirages de boules, cf. planche pour les méthodes.

III Probabilités conditionnelles :

Le roi est issu d'une famille de deux enfants. Quelle est la probabilité que le roi ait une soeur ?

1) Motivation double

a) Dans le cadre des proba. uniformes : Soit (Ω, P) un espace probabilisé fini avec P la probabilité uniforme sur Ω.

Si on considère deux événements A et B, et si on sait que B est réalisé, et qu'on veut évaluer la probabilité de l'événement A, on va considérer *parmi les* $\mathrm{Card}(B)$ *éléments de* B, ceux qui sont dans A, et on a envie d'appeler « la probabilité de A sachant B » le rapport :

$$P(A|B) := \frac{\mathrm{Card}(A \cap B)}{\mathrm{Card}(B)} \quad (1).$$

Mais en divisant numérateur et dénominateur par $\mathrm{Card}(\Omega)$, on a donc considéré :

$$P(A|B) := \frac{P(A \cap B)}{P(B)} \quad (2)$$

La formule (1) a l'avantage de faire comprendre que calculer $P(A|B)$ c'est changer d'univers et se placer dans l'univers B.

La formule (2) permet de relier cette probabilité $P(A|B)$ avec les probabilités dans Ω.

b) Dans le cadre de l'approche fréquentiste : On reprend le point de vue fréquentiste du II 2) a) (iii).

On répète n fois une expérience aléatoire et on considère le nombre n_A (resp. n_B) de réalisations de l'événement A (resp. B). On a défini les fréquences : $F_n(A) = n_A/n$, et $F_n(B) = n_B/n$.

Si on suppose $n_B > 0$ (autrement dit B s'est réalisé au moins une fois), alors on peut définir la *fréquence relative* de A par rapport à B :

$$F_n(A|B) = \frac{n_{A\cap B}}{n_B},$$

où $n_{A\cap B}$ est bien sûr le nombre de réalisations de $A \cap B$.

On remarque alors que :

$$F_n(A|B) = \frac{F_n(A \cap B)}{F_n(B)}$$

Avec l'idée donnée au 2) a) (iii) que les proba. sont des fréquences idéalisées, il n'est pas surprenant d'introduire la déf. suivante : [1]

2) Définition générale :

a) **Déf.** Soit (Ω, P) un espace probabilisé. Soit B un événement de probabilité non nulle. Pour tout événement A on définit la *probabilité de A sachant B* notée $P(A|B)$ ou $P_B(A)$ par :

$$\boxed{P(A|B) = P_B(A) = \frac{P(A \cap B)}{P(B)}.}$$

b) **Prop.** Avec les notations du a), l'application : $P_B : \mathcal{P}(\Omega) \to [0,1]$, $A \mapsto P_B(A)$ est une probabilité sur Ω appelée *probabilité conditionnelle à B*.

N.B. Malgré la notation $P(A|B)$, l'événement $A|B$ n'existe pas ! Il ne s'agit pas de la probabilité P appliquée à un événement. C'est pour cela que la notation $P_B(A)$ serait la « meilleure ». Toutefois l'autre à l'avantage de suivre la dénomination orale.

c) **Calculer P_B c'est changer d'univers :** Dans le cas particulier du 1) a) (formule (1)) on a vu que le calcul de $P(A|B)$ revient à « changer d'univers » en se plaçant dans l'univers B.

Ceci se généralise à un espace probabilisé fini (Ω, P) quelconque, en voyant la probabilité de chaque événement comme la somme des probabilités des événements élémentaires qui le composent, on obtient la :

Remarque : $P(A|B) = \dfrac{\sum\limits_{x \in A \cap B} p_x}{\sum\limits_{x \in B} p_x}$ où pour tout $x \in \Omega$, on note $p_x = P(\{x\})$.

L'intérêt des proba. conditionnelles, c'est que P_B est souvent plus facile à calculer, car l'univers est « réduit ». On va le voir très vite en exercice, cf. 3) b).

3) Formule « en sens inverse » :

a) Une simple inversion de la formule de la déf. qui a des applications cruciales :

Prop. Si A et B sont deux événements d'un espace probabilisé (Ω, P) alors :

$$\boxed{P(A \cap B) = P(A|B).P(B), \text{ à la condition bien sûr que : } P(B) \neq 0.}$$

Raison d'être de la formule précédente :

Parfois, dans la pratique, il est plus facile de connaître $P(A|B)$ que $P(A \cap B)$!

b) **Illustration sur un problème de boules dans une urne :**

Exercice : On considère une urne contenant dix boules, six rouges et quatre noires. Les boules sont de même taille et convenablement mélangées. On tire une première boule et on note sa couleur. Puis sans remettre la première, on tire une seconde boule et on note sa couleur. On note A_1 (resp. A_2) l'événement « la première (resp. la deuxième) boule est rouge ».

(0) A quoi sert la phrase : « les boules sont de même taille et convenablement mélangées » ?

Pour chacune des questions suivantes, expliciter l'espace probabilisé considéré (univers, proba.).

(1) Calculer $P(A_1)$

(2) Calculer $P(A_2|A_1)$

(3) En déduire $P(A_1 \cap A_2)$.

(4) Comparer la méthode précédente au calcul direct de $P(A_1 \cap A_2)$ avec un dénombrement.

1. Si tout ce qui précède peut rassurer comme motivation, il ne faut pas se méprendre : il ne s'agit nullement de « prouver » la déf. du 2) a) : on ne prouve pas une définition. En revanche, cette définition entraîne des théorèmes, en lien avec ce qui précède.

En outre, il ne faut pas penser qu'il y a un ordre *chronologique* entre les deux événements A et B.. puisqu'on pourra considérer $P(A|B)$ et $P(B|A)$

Le calcul avec les proba. conditionnelles est ici plus simple que le calcul par dénombrement.

4) Formule des probabilités composées :

a) Prop. Soit $n \in \mathbb{N}_{\geq 2}$ et soit (Ω, P) un espace probabilisé fini. Pour toute famille $(A_1, \dots, A_n)$ d'événements tels que $P(A_1 \cap \dots A_{n-1}) \neq 0$ on a :

$$\boxed{P(A_1 \cap \dots \cap A_{n-1} \cap A_n) = P(A_1).P(A_2|A_1).P(A_3|A_1 \cap A_2) \dots P(A_n|A_1 \cap \dots \cap A_{n-1}).}$$

Remarque :

C'est la formule du lycée pour le calcul de la probabilité d'un chemin dans un arbre.

b) Exercice d'application : Anatole[2] a le dimanche soir u chemises unies et r chemises rayées dans son armoire. Chaque matin, levé à l'aurore, il choisit une chemise à l'aveugle, dans son armoire (ce qui signifie que toutes les chemises peuvent être choisies avec la même probabilité) et le soir, il met cette chemise au sale. Quelle est la probabilité pour qu'il choisisse (le lundi, mardi, mercredi) successivement deux chemises à rayures suivies d'une chemise unie ?

On comparera la rédaction « arbre » du lycée, et la formule des proba. composées.

5) Formule des probabilités totales :

a) Un cas particulier simple mais important :

Prop. Pour tout couple (A, B) d'événements d'un espace probabilisé (Ω, P) :

$$P(A) = P(A \cap B) + P(A \cap B^c).$$

Si en outre $P(B) \neq 0$ et $P(B) \neq 1$, alors on peut écrire :

$$\boxed{P(A) = P(A|B)P(B) + P(A|B^c).P(B^c)}$$

b) Exercice : On reprend l'exercice du 3) b). Calculer $P(A_2)$ en utilisant cette formule. Commentez le résultat obtenu.

c) La formule générale :

Prop. Soit $(A_1, \dots, A_n)$ un système complet d'événements d'un espace probabilisé (Ω, P). On a déjà dit que pour tout événement B :

$$P(B) = \sum_{i=1}^{n} P(B \cap A_i).$$

Si en plus chaque A_i est de probabilité non nulle, on peut écrire :

$$\boxed{P(B) = \sum_{i=1}^{n} P(B|A_i)P(A_i), \text{ (formule des probabilités totales).}}$$

La formule des proba. totales est celle que vous utilisiez au lycée quand vous ajoutiez des proba. associées à plusieurs chemins dans un arbre.

d) Exercice : Soit $n \in \mathbb{N}^*$. On dispose d'une urne $\mathcal{J}$ qui contient un jeton marqué avec un 1, deux jetons marqués avec un 2, jusqu'à..., n jetons marqués avec un n.

On dispose par ailleurs de n autres urnes $\mathcal{U}_1, \dots, \mathcal{U}_n$, telles que dans $\mathcal{U}_i$ il y a i boules blanches et $n - i$ boules noires.

On fait l'expérience suivante : on tire un jeton dans $\mathcal{J}$ et si le jeton tiré porte le numéro i, on tire une boule dans l'urne $\mathcal{U}_i$. Quelle est la probabilité d'obtenir une boule blanche ?

6) Formule de Bayes

a) Lien entre les deux probabilités conditionnelles :

Prop. Soient A et B deux événements de probabilité non nulle d'un même espace probabilisé (Ω, P). Alors :

2. Que veut dire Anatole en grec ?

$$\boxed{P(A|B) = \frac{P(B|A).P(A)}{P(B)}}$$

b) Un exemple qui explique que cette formule s'appelle parfois « probabilité des causes » :

Exercice : Les montres kwatch ont une probabilité de tomber en panne estimée à 1%. Mais sur le marché, elles sont mélangées à des contrefaçons, qui occupent 20% du marché, et ont, elles, une proba. de tomber en panne de 10%.

(i) Vous achetez une montre : quelle est la probabilité qu'elle tombe en panne ?

(ii) En sens inverse (probabilité des causes) : votre montre tombe en panne. Quelle est la probabilité que ce soit une contrefaçon ?

N.B. Attention : Les notions de « cause » et de « chronologie » sont absentes de la théorie des probabilités. Les proba. conditionnelles sont définies pour deux événements sans considérer un éventuel « ordre » Donc il ne faut pas réduire la formule du a) à une *probabilité des causes, car il peut ne pas avoir de cause (cf. ex.pl.)*

c) La formule de Bayes plus générale : juste un peu plus d'algèbre

Prop. Soit $(A_1, \dots, A_n)$ un système complet d'événements d'un espace probabilisé (Ω, P) tel que pour tout $i \in [\![1, n]\!]$, $P(A_i) \neq 0$. Pour tout événement B de Ω tel que $P(B) \neq 0$, on a :

$$\boxed{P(A_i|B) = \frac{P(B|A_i).P(A_i)}{\sum_{j=1}^{n} P(B|A_j).P(A_j)}}$$

d) Remarque : c'est exactement cette formule qu'on a utilisée sans le dire au b) (ii).

IV L'indépendance des événements :

1) L'indépendance de deux événements :

a) Déf. Deux événements A et B d'un espace probabilisé (Ω, P) sont dits *indépendants* ssi :

$$P(A \cap B) = P(A).P(B)$$

b) Remarque : La déf. est symétrique en A et B.

c) Caractérisation : Soient A et B deux événements de probabilités non nulles.
Alors A et B sont indépendants ssi $P(A|B) = P(A)$ ssi $P(B|A) = P(B)$.

d) Attention :

(i) Ne pas confondre la notion d'*événements indépendants* et celle d'*événements incompatibles*.

Des événements de proba. non nulles, s'ils sont indép., ne seront pas incompatibles : pourquoi ?

(ii) Parfois on a une *intuition* que deux événements sont indépendants. Par exemple si on lance deux dés un événement portant sur le résultat du premier dé et un événement portant sur le résultat du second dé seront indépendants dans l'espace probabilisé standard pour deux dés ($\Omega = [\![1, 6]\!]^2$ avec proba. uniforme).

(iii) Mais en général :

l'indépendance de deux événements ne se détermine pas forcément a priori mais demandera un *calcul*.

Exercice : On tire trois fois à pile ou face une pièce équilibrée. On considère l'événement A « les trois lancers donnent le même résultat », et l'événement B « on obtient au plus un pile ».

(1) Ces événements vous paraissent-ils « intuitivement » indépendants ?

(2) Etudier, par le calcul cette indépendance.

(iv) Parfois au contraire : l'indépendance des événements fait partie du modèle probabiliste que l'on fixe pour étudier notre situation (cf. pl. : paradoxe du prisonnier).

(v) **N.B.** Contrairement à la notion d'événement *incompatible* qui est une notion *ensembliste*, la notion d'événement *indépendant* dépend du choix de la probabilité sur notre univers (par exemple un événement de proba. nulle est indépendant de tous les autres).

e) Prop. Si A et B sont deux événements indépendants alors A^c et B, A et B^c, A^c et B^c sont indépendants.

N.B. La preuve est un *calcul* pas un blabla...

f) Un exemple avec trois événements : On lance deux dés équilibrés. On considère l'événement A « le premier dé donne 6 », l'événement B « le second dé donne 6 », et l'événement C »les résultats des deux dés sont différents ». Montrer que les trois événements sont *deux à deux indépendants*.

Remarque (transition avec le paragraphe suivant) : L'indép. de A, B, C deux à deux n'entraîne pas que C soit indépendant de $A \cap B$... On a besoin d'une relation d'indép. plus forte.

2) Indépendance d'une famille quelconque d'événements

a) Une notion insuffisante : l'indépendance deux à deux

(i) Déf. Des événements $A_1, \dots, A_n$ d'un espace probabilisé (Ω, P) sont dits *deux à deux* indépendants ssi pour tout $(i, j) \in [\![1, n]\!]^2$ tel que $i \neq j$, A_i et A_j sont indépendants.

(ii) Problème : la seule information que A, B, C sont deux à deux indép. ne permet pas de calculer $P(A \cap B \cap C)$ à partir de $P(A)$, $P(B)$, $P(C)$, cf. exple ci-dessus.

b) La bonne notion (plus forte) : l'indépendance *mutuelle*

(i) Déf. Des événements $A_1, \dots, A_n$ d'un espace probabilisé (Ω, P) sont dit *mutuellement indépendants* ssi pour tout sous-ensemble non vide I de $[\![1, n]\!]$:

$$P(\bigcap_{i \in I} A_i) = \prod_{i \in I} P(A_i).$$

(ii) **Remarque :** que donne la déf. pour trois événements, pour quatre événements ?

(iii) **Question :** Combien d'égalités doivent-elles être vérifiées pour vérifier la déf. du (i) ?

c) Lien entre indép. mutuelle et deux à deux :

(i) Si des événements sont mutuellement indép., ils sont en part. deux à deux indép.

(ii) La récip est fausse : contre-exemple ?

d) Prop. Soient $A_1, \dots, A_n$ une famille d'événements mutuellement indép. Pour tout $i \in [\![1, n]\!]$, on note $A'_i = A_i$ ou $A'_i = A_i^c$. Alors les événements $A'_1, \dots, A'_n$ sont encore mutuellement indép.

Preuve : Pas d'idée nouvelle, juste plus technique : récurrence. □

3) Et si on commençait par l'indépendance ?

(i) Remarque : L'indépendance est une notion cruciale des probabilités, qui les fait avancer bien au delà des raisonnements de dénombrement : jusqu'à maintenant nous avons fait des calculs dans un espace (Ω, P) donné, le plus souvent avec P uniforme, et constaté l'indépendances d'événements. Notamment pour deux dés ou deux lancers de pieces, cette indépendance était liée à l'écriture $\Omega = \Omega_1 \times \Omega_2$. Mais on peut aussi penser nos modèles autrement :

pour la répétition d'une même expérience aléatoire (lancers des dés, des pièces), on peut se demander comment *construire mathématiquement* un espace probabilisé dans lesquel les différentes répétitions seront *indépendantes*. Cette fois l'indépendance devient une *hypothèse a priori*, qui va induire la construction d'un espace probabilisé (Ω, P).

(ii) Exemple d'une telle construction : *pour n lancers d'une pièce de monnaie éventuellement biaisée.*

On considère n lancers d'une pièce, qui tombe sur pile avec probabilité $p \in [0, 1]$.

En notant 0 pour face et 1 pour pile, il est naturel de dire qu'une issue est un élément de $\{0,1\}^n$. Ce qui nous donne l'univers $\Omega = \{0,1\}^n$.

Pour chaque $k \in [\![1,n]\!]$, notons Π_k l'évenement « le k-ième lancer donne pile » et F_k l'événement « le k-ième lancer donne face ». La propriété suivante dit ce que nous voulons faire :

Prop. : Il existe une unique probabilité P sur Ω telle que
(1) pour tous $k \in [\![1,n]\!]$, $P(\Pi_k) = p$ et $P(F_k) = 1-p$,
(2) les résultat des différents lancers sont indépendants ce qui signifie que les événements $(\Pi_i)_{i\in[\![1,n]\!]}$ sont *mutuellement indépendants.*

Il faut déjà comprendre que cette propriété n'est pas *évidente.*

Démonstration par analyse-synthèse. Pour l'analyse, il suffit d'exprimer chaque événement élémentaire à l'aide des Π_k et F_ℓ. Synthèse laissée en exercice.

(iii) Généralisation :
D'une manière plus générale, si on dispose de n espaces probabilisés $(\Omega_1, P_1), \dots, (\Omega_n, P_n)$, les deux ingrédients de la construction du (i) sont :
• la considération de l'univers produit $\Omega = \Omega_1 \times \cdots \times \Omega_n$,
• l'existence et l'unicité d'une probabilité P sur Ω, dite probabilité produit, vérifiant :

$$\forall\, (A_1, \dots, A_n) \in \mathcal{P}(\Omega_1) \times \cdots \times \mathcal{P}(\Omega_n),\ P(A_1 \times \cdots \times A_n) = \prod_{i=1}^{n} P_i(A_i).$$

(iv) Exemple : si (Ω_1, P_1) est l'univers du lancer de un dé à six faces, (Ω_2, P_2) celui d'une pièce biaisée, etc.. et qu'on *veut* un modèle global d'un univers où les événements « ne portant que sur le dé d'un côté, et ceux ne portant que sur la pièce de l'autre » soient indépendants, alors la construction du (iii) est ce qu'il nous faut. En effet, on a la :

(iv) Propriété d'indépendance pour la probabilité produit :
Si P est la proba. du (iii), et si pour chaque $i \in [\![1,n]\!]$, E_i est un événement de la forme $E_i = \Omega_1 \times \cdots \times \Omega_{i-1} \times A_i \times \Omega_{i+1} \times \cdots \times \Omega_n$ avec $A_i \subset \Omega_i$ (i.e. « ne portant une contrainte que dans Ω_i) alors $(E_1, \dots, E_n)$ sont mutuellement indépendants.

(v) Remarque : cette décomposition de Ω en produit d'univers plus simples était implicite dans tous les calculs élémentaires des exercices du III (3) b) sur les boules, 4) b) sur Anatole etc... où l'on *changeait d'univers* suivant les questions.

Appendice : les démonstrations des prop. du paragraphe I . sur la théorie des cardinaux

(La numérotation des prop. renvoie à celle du § I. 1)

1 a), c) Des démonstrations par récurrences pas du tout dans l'esprit du programme :

Pour ceux qui se demandent à quoi peut ressembler la preuve de résultats aussi évidents, voici un preuve, qui n'est pas du tout exigible en prépa. :

Prop. 1.a) – *Pour tout $(m,n) \in (\mathbb{N}^*)^2$ si on a une bijection $f : [\![1,m]\!] \to [\![1,n]\!]$ alors $n = m$.*

Preuve – Pour tout $n \in \mathbb{N}^*$, notons H_n la prop. suivante :

$H(n)$: pour tout $m \in \mathbb{N}^*$, si on a une bijection entre $[\![1,m]\!]$ et $[\![1,n]\!]$ alors $m = n$.

Montrons par réc. que $H(n)$ est vraie pour tout $n \in \mathbb{N}^*$.

• Si $n = 1$. Soit f une bijection de $[\![1,m]\!]$ dans $\{1\}$. Alors tous les éléments ont la même image, donc l'injectivité force $m = 1$ et donc $H(1)$ est vraie.

Il faut bien comprendre que ce qu'on sait sur les entiers, ce sont les axiomes de Peano, et donc la notion de successeur *: l'entier n c'est le successeur de $n-1$ etc.*

• H.R. On suppose que pour un $n \in \mathbb{N}$ on a la propriété $H(n)$.

Soit alors $m \in \mathbb{N}$ et une bijection $f : [\![1,m]\!] \to [\![1,n+1]\!]$.

Cas 1 : Si $f(m) = n+1$ alors la restriction de f de $[\![1,m-1]\!]$ dans $[\![1,n]\!]$ est encore bijective. Par H.R. on conclut que $m-1 = n$ et donc $m = n+1$.

Cas 2 : Sinon, on considère k_0 l'unique antécédent de $n+1$ par f et $\varphi : [\![1,m]\!] \to [\![1,m]\!]$ telle que $m \mapsto k_0$ et $k_0 \mapsto m$ et qui est l'identité en dehors de $\{k_0, m\}$.

Alors $f \circ \varphi$ va de $[\![1,m]\!]$ dans $[\![1,n+1]\!]$ et envoie m sur $n+1$. Donc par le cas 1, on conclut encore $m = n+1$.

La récurrence est établie. □

La proposition suivante ressemble davantage à ce qu'on peut demander comme savoir faire à un élève de prépa. Rappellons qu'au (i), on a défini le cardinal de E comme l'unique entier n tel que E soit en bijection avec $[\![1,n]\!]$.

Prop. 1. b) (ii) Deux ensembles finis sont en bijection si, et seulement si, ils ont le même cardinal.

Preuve : Soit E et F deux ensembles finis et $\varphi : E \to [\![1,m]\!]$ et $\psi : F \to [\![1,n]\!]$ des bijections, de sorte que $m = \mathrm{Card}(E)$ et $n = \mathrm{Card}(F)$.

Sens $\Rightarrow$: supposons qu'on ait une bijection $f : E \to F$ alors la composée $\psi \circ f \circ \varphi^{-1} : [\![1,m]\!] \to [\![1,n]\!]$ est bijective, et donc par le (i), $m = n$.

Sens $\Leftarrow$: si $m = n$ alors $\psi^{-1} \circ \varphi : E \to F$ est une bijection. □

La preuve suivante, H.P. en prépa, montre bien que "compter, c'est juste savoir faire +1" :

Prop. 1. c) – Si A est fini de cardinal n, toute partie de A est de cardinal au plus n.

Preuve – Il suffit de le faire pour $A = [\![1,n]\!]$ (en transportant la question par une bijection $\varphi : A \to [\![1,n]\!]$).

Soit H_n la prop. "tout sous-ensemble de $[\![1,n]\!]$ est de cardinal ou plus n". Montrons par réc. sur n que H_n est vraie pour tout $n \in \mathbb{N}^*$.

• Pour $n = 1$, les parties de $\{1\}$ sont $\varnothing$ et $\{1\}$ ok.

• On suppose la propriété vraie pour $[\![1,n]\!]$, montrons qu'elle l'est pour $[\![1,n+1]\!]$.

Soit $B \subset [\![1,n+1]\!]$. On considère $B \cap [\![1,n]\!] = B_1$. Par H.R., il est de cardinal au plus n.

Et suivant que $(n+1) \in B$ ou pas, B a au plus un élément de plus que B_1 donc est de cardinal au plus $n+1$. La récurrence est établie. □

Exercice : Modifier ce qui précède pour montrer que si $B \subset A$ et $B \neq A$ alors $\mathrm{Card}(B) < \mathrm{Card}(A)$.

1) d), e) des démonstrations plus importantes dans l'esprit des MPSI *Tous les ensembles considérés sont finis.*

Prop. du d) (i) Il existe une injection de E dans F ssi $\mathrm{Card}(E) \leq \mathrm{Card}(F)$

Sens $\Rightarrow$. On a une injection $f : E \to F$. On en déduit que $f : E \to f(E)$ est une bijection. Donc par a), $\mathrm{Card}(E) = \mathrm{Card}(f(E))$. Or comme $f(E) \subset F$, par c), on a $\mathrm{Card}(f(E)) \leq \mathrm{Card}\, F$. On conclut bien que $\mathrm{Card}(E) \leq \mathrm{Card}(F)$.

Sens $\Leftarrow$. On note $m = \mathrm{Card}(E)$ et $n = \mathrm{Card}(F)$. On a $m \leq n$.

Par déf. du cardinal, on a une bijection φ de E dans $[\![1, m]\!]$ et une bijection ψ de F dans $[\![1, n]\!]$.

Or pour $m \leq n$, on a $[\![1, m]\!] \subset [\![1, n]\!]$ ce qui donne une injection naturelle de $[\![1, m]\!]$ dans $[\![1, n]\!]$, qu'on notera $i : x \in [\![1, m]\!] \mapsto x$.

On peut alors faire le diagramme suivant :

$$\begin{array}{ccc} E & \overset{\varphi}{\to} & [\![1, m]\!] \\ ? & & \downarrow i \\ F & \overset{\psi}{\to} & [\![1, n]\!] \end{array}$$

Pour fabriquer une injection de E dans F, il suffit de considérer l'application $\psi^{-1} \circ i \circ \phi$, qui est bien injective comme composée d'injections. □

Prop. du d) (ii) *Il existe une surjection de E dans F ssi* $\mathrm{Card}(E) \geq \mathrm{Card}(F)$

Sens $\Rightarrow$. On a une surjection $f : E \to F$. Comme E est un ensemble fini, on peut choisir d'indexer ses éléments $E = \{x_1, \ldots, x_m\}$ (ce qui revient à fixer une bijection avec $[\![1, m]\!]$).

On peut définir un ordre dans E en disant que $x_i \leq x_j \Leftrightarrow i \leq j$.

Pour chaque élément $y \in F$, on peut choisir, dans l'ensemble, fini,non vide, de ses antécédents, le plus petit, que l'on note $g(y)$.

La déf. de l'ordre dans E sert à se donner une méthode pour choisir l'antécédent de y.

On a ainsi défini une application $g : F \to E$ telle que pour tout $y \in F$, $f(g(y)) = y$.

Donc $f \circ g = \mathrm{id}_F$ et en part. g est injective. Par le (i), on en déduit que $\mathrm{Card}(F) \leq \mathrm{Card}(E)$.

Sens $\Leftarrow$. Tout à fait analogue au sens $\Leftarrow$ du (i), en considérant cette fois, si $m \geq n$, une surjection de $[\![1, m]\!]$ dans $[\![1, n]\!]$ par exemple l'application s qui est l'identité sur $[\![1n]\!]$ et qui envoie tous les $k \geq n + 1$ sur n.

Prop. du e) (i) *$f : E \to F$ est injective ssi* $\mathrm{Card}(f(E)) = \mathrm{Card}(E)$.

Sens $\Rightarrow$. On a f injective, donc $f : E \to f(E)$ est bijective, et donc par la rem. du b), $\mathrm{Card}(E) = \mathrm{Card}(f(E))$.

Sens $\Leftarrow$. Par contraposée : on suppose f non injective, montrons que $\mathrm{Card}(f(E)) \neq \mathrm{Card}(E)$.

(Remarquons qu'on a toujours $\mathrm{Card}(f(E)) \leq \mathrm{Card}(E)$).

On a donc deux éléments $(x_1, x_2) \in E^2$ tels que $x_1 \neq x_2$ et $f(x_1) = f(x_2)$.

Alors en notant $E_1 = E \setminus \{x_1\}$, on a $f(E) = f(E_1)$.

Mais $\mathrm{Card}(f(E_1)) \leq \mathrm{Card}(E_1)$ (car f est surjective de E_1 sur $f(E_1)$).

Donc $\mathrm{Card}(f(E)) \leq \mathrm{Card}(E_1) = \mathrm{Card}(E) - 1$. □

Prop. du e) (ii) *f est surjective ssi* $\mathrm{Card}(f(E)) = \mathrm{Card}(F)$.

Preuve très facile : f est surjective ssi $f(E) = F$. Or $f(E)$ étant un sous-ensemble de F, il est égal à F si, et seulement si, il a le même cardinal que F. □

Prop. du e) (iii)

Si E et F ont le même cardinal, $f : E \to F$ est bijective ssi elle est injective ssi elle est surjective.

On se donne donc E et F de même cardinal et $f : E \to F$. Il s'agit de montrer que f est injective si, et seulement si, elle est surjective.

Or f injective équivaut par (i) à $\mathrm{Card}(f(E)) = \mathrm{Card}(E)$. Par hyp. sur E et F, ceci équivaut à $\mathrm{Card}(f(E)) = \mathrm{Card}(F)$. Ceci équivaut par (ii) à f surjective. □

Prop. du 2) a) Formule des quatre cardinaux

Il est essentiel d'avoir compris la preuve "évidente" de cette formule : quand on compte $\mathrm{Card}(A)+\mathrm{Card}(B)$ *on compte deux fois les éléments de* $A\cap B$*. Voici une preuve plus formelle, avec la déf. des cardinaux.*

(i) Cas d'une réunion disjointe. Si $A\cap B=\varnothing$, on peut facilement, à partir d'une bijection entre A et $[\![1,m]\!]$ et d'une bijection entre B et $[\![1,n]\!]$, exhiber une bijection entre $A\cup B$ et $[\![1,m+n]\!]$.

On a donc si A et B disjoints $\mathrm{Card}(A\cup B)=\mathrm{Card}(A)+\mathrm{Card}(B)$.

(ii) Conséquence aussi : Si $C\subset A$ alors $\mathrm{Card}(A\setminus C)=\mathrm{Card}(A)-\mathrm{Card}(C)$.

En effet, il suffit d'écrire $A=C\cup(A\setminus C)$ et d'appliquer le (i).

(iii) Cas général où A et B ne sont pas nécessairement disjoints.

Pour prouver la formule des quatre cardinaux, on se ramène à une union disjointe :

Il suffit d'écrire $A\cup B=((A\setminus(A\cap B))\cup B$ réunion disjointe, et on applique le (i) et le (iii) pour avoir la conclusion. □

Prop. du 2) b) Lemme des bergers : Si $f:E\to F$ est telle que tout élément de F a exactement p antécédents par f, alors $\mathrm{Card}(E)=p\,\mathrm{Card}(F)$.

Preuve : Notons $F=b_1,\dots,b_n$. Alors $E=\bigcup_{i=1}^{n}f^{-1}(\{b_i\})$, et cette réunion est *disjointe*. Donc $\mathrm{Card}(E)=\sum_{i=1}^{n}\mathrm{Card}(f^{-1}(\{b_i\})=\sum_{i=1}^{n}p=np$.

Prop. du 2) c) Cardinal du produit :

En notant $A=\{a_1,\dots,a_m\}$, on a $A\times B=\bigcup_{i=1}^{m}\{a_i\}\times B$ réunion d'ensembles deux à deux disjoints.

Donc $\mathrm{Card}(A\times B)=\sum_{i=1}^{m}\mathrm{Card}(\{a_i\}\times B)=\sum_{i=1}^{m}n=m\times n$.

En effet chaque ensemble $\{a_i\}\times B$ est en bijection avec B.

On peut aussi appliquer le lemme des bergers à la projection $A\times B\to A$, $(a,b)\mapsto a$. □

3) b) Nombres d'injections, nombre d'arrangements :

On fixe un entier $n\in\mathbb{N}^*$, F un ensemble de cardinal n, et en notant $\mathfrak{a}_p(F)$ l'ensemble des arrangements de p éléments de F, on va montrer par récurrence (finie) sur $p\in[\![1,n]\!]$, la propriété $P(p)$ suivante :

$$P(p):\ \mathrm{Card}(\mathfrak{a}_p(F))=n(n-1)\dots(n-p+1).$$

(i) $P(1)$ est vraie car un arrangement de 1 élément de F est simplement la donnée d'un élément de F : il y a en n.

(ii) H.R. Supposons $P(p)$ vraie pour un $p\leq n-1$. Montrons que $P(p+1)$ est vraie.

On considère l'application $\Phi:\mathfrak{a}_{p+1}(F)\to\mathfrak{a}_p(F)$, $(x_1,\dots,x_{p+1})\mapsto(x_1,\dots,x_p)$.

Alors pour tout $(x_1,\dots,x_p)\in\mathfrak{a}_p(F)$ il a exactement $(n-p)$ antécédents dans $\mathfrak{a}_{p+1}(F)$: en effet pour compléter $(x_1,\dots,x_p)$ en un arrangement, il faut et il suffit de choisir un élément $x_{p+1}\in F\setminus\{x_1,\dots,x_p\}$.

Par le lemme des bergers appliqué à Φ, on conclut que $\mathrm{Card}(\mathfrak{a}_{p+1}(F))=(n-p)\,\mathrm{Card}(\mathfrak{a}_p(F))$.

Par H.R. $\mathrm{Card}(\mathfrak{a}_p(F))=n(n-1)\dots(n-p+1)$, donc $\mathrm{Card}(\mathfrak{a}_{p+1}(F))=n(n-1)\dots(n-p)$, la récurrence est établie. □

Une solution très formelle de l'exercice sur le nombre de partitions d'un entier

1) Montrer que, pour tout $N \in \mathbb{N}$, et tout $n \in \mathbb{N}$, $\sum_{i=0}^{n} \binom{N+i}{N} = \binom{N+n+1}{N+1}$.

2) Soit $(n,p) \in (\mathbb{N})^2$. On note $\mathcal{A}_{n,p} = \{(x_1,\dots,x_p) \in \mathbb{N}^p,\ x_1+\cdots+x_p = n\}$.

On se propose de donner une autre solution pour l'exercice fait en cours donnant le cardinal de $\mathcal{A}_{n,p}$, qu'on notera ici $P_{n,p}$.

a) Montrer que pour tout $p \geq 1$, $P_{n,p} = \sum_{k=0}^{n} P_{n-k,p-1}$.

b) Montrer alors la formule explicite donnant $P_{n,p}$ par récurrence.

Solution :

1) Montrons par récurrence sur $n \in \mathbb{N}$, la propriété $P(n)$ suivante ;

$P(n)$: $\forall N \in \mathbb{N}$, $\sum_{i=0}^{n} \binom{N+i}{N} = \binom{N+n+1}{N+1}$.

• Montrons que $P(0)$ est vraie.

Or $P(0)$: $\forall N \in \mathbb{N}$, $\binom{N}{N} = \binom{N+1}{N+1}$.

Cette propriété est vraie car les deux membres de l'égalité sont égaux à 1 pour tout $N \in \mathbb{N}$.

• H.R. on suppose que $P(n)$ est vraie pour un $n \in \mathbb{N}$. Montrons que $P(n+1)$ est vraie.

Soit $N \in \mathbb{N}$. On veut montrer que $\sum_{i=0}^{n+1} \binom{N+i}{N} = \binom{N+n+2}{N+1}$ $(*)$. Or :

$$\begin{aligned}
\sum_{i=0}^{n+1} \binom{N+i}{N} &= \sum_{i=0}^{n} \binom{N+i}{N} + \binom{N+n+1}{N}, \\
&= \binom{N+n+1}{N+1} + \binom{N+n+1}{N}, \quad \text{par H.R.,} \\
&= \binom{N+n+2}{N+1}, \quad \text{par la formule du triangle de Pascal.}
\end{aligned}$$

Ceci prouve exactement $(*)$. La récurrence est établie. □

2) a) Soit $n \in \mathbb{N}$ et $p \geq 1$.

On remarque que $\mathcal{A}_{n,p} = \bigcup_{k=0}^{n} \mathcal{B}_k$ (1), où $\mathcal{B}_k = \{(x_1,\dots,x_{p-1},k),\ (x_1,\dots,x_{p-1}) \in \mathcal{A}_{n-k,p-1}\}$.

En effet, pour un p-uplet $x = (x_1,\dots,x_p) \in \mathbb{N}^p$, en notant $k = x_p$:

$$x \in \mathcal{A}_{n,p} \Leftrightarrow x_1+\cdots+x_{p-1} = n-k \Leftrightarrow (x_1,\dots,x_{p-1}) \in \mathcal{B}_k,$$

La réunion des $(\mathcal{B}_k)_{k\in[\![0,n]\!]}$ qui apparaît dans l'égalité (1) est *disjointe*. En effet, si un p-uplet $(x_1,\dots,x_p)$ appartient à l'intersection $B_k \cap B_l$ alors $x_p = k$ et $x_p = l$ ce qui force $k = l$.

Donc (1) $\Rightarrow \mathrm{Card}(\mathcal{A}_{n,p}) = \sum_{k=0}^{n} \mathrm{Card}(\mathcal{B}_k)$ (2) (cardinal d'un réunion disjointe).

Or pour tout $k \in [\![0,n]\!]$, l'application $\varphi_k : \mathcal{B}_k \to \mathcal{A}_{n-k,p-1}$, $(x_1,\dots,x_{p-1},k) \mapsto (x_1,\dots,x_{p-1})$ est *bijective*, car elle admet comme application réciproque $\psi_k : (x_1,\dots,x_{p-1}) \mapsto (x_1,\dots,x_{p-1},k)$.

Donc, pour tout $k \in [\![0,n]\!]$, $\mathrm{Card}(\mathcal{B}_k) = \mathrm{Card}(\mathcal{A}_{n-k,p-1}) = P_{n-k,p-1}$.

Donc avec (2), on conclut bien que $P_{n,p} = \sum_{k=0}^{n} P_{n-k,p-1}$.

b) Montrons par récurrence sur $p \in \mathbb{N}^*$ la propriété $Q(p)$ suivante :

$Q(p)$: $\forall n \in \mathbb{N}$, $P_{n,p} = \binom{n+p-1}{p-1}$.

• Initialisation : $Q(1)$ s'écrit : $\forall n \in \mathbb{N}$, $P_{n,1} = \binom{n}{0} = 1$.

Or : soit $n \in \mathbb{N}$, $\mathcal{A}_{n,1} = \{x \in \mathbb{N}, x = n\} = \{n\}$ est bien de cardinal 1, ce qui établit $Q(1)$.

• H.R. : on suppose que $Q(p-1)$ est vraie pour un certain $p \in \mathbb{N}_{\geq 2}$ (de sorte que $p-1 \in \mathbb{N}^*$).

Soit $n \in \mathbb{N}$, on veut montrer que $P_{n,p} = \binom{n+p-1}{p-1}$.

Par a), on sait que $P_{n,p} = \sum_{k=0}^{n} P_{n-k,p-1}$.

Par H.R. on sait que $P_{n-k,p-1} = \binom{n-k+p-2}{p-2}$ pour tout $k \in [\![0,n]\!]$.

Donc on sait que $P_{n,p} = \sum_{k=0}^{n} \binom{n-k+p-2}{p-2} = \sum_{i=0}^{n} \binom{i+p-2}{p-2}$ $(*)$, par chgt. d'indice $i = n-k$.

Pour conclure que $Q(p)$ est vraie, il suffit donc d'appliquer la formule du 1) à $N = p-2$, on a :

$P_{n,p} = \binom{p-2+n+1}{p-1} = \binom{n+p-1}{p-1}$, *la récurrence est établie.* □