Chapitre 2

Dénombrements

Référence pour ce chapitre : le module II.1 du L1, section 2.2.

2.1 Les bases

2.1.1 Principes de récurrence

Rappelons que l'ensemble $\mathbf{N}$ des entiers naturels est muni d'une relation d'ordre notée $\leq$ qui en fait un ensemble *bien ordonné*. En d'autres termes, $(\mathbf{N}, \leq)$ vérifie la propriété fondamentale : *Toute partie non vide de* $\mathbf{N}$ *admet un plus petit élément.*

Cette propriété est d'ailleurs équivalente à la conjonction des deux suivantes :
- L'ensemble $\mathbf{N}$ est totalement ordonné.
- Toute suite décroissante d'entiers est stationnaire. (De manière équivalente : il n'existe pas de suite infinie strictement décroissante dans $\mathbf{N}$.)

Le principe de récurrence. On en a déduit (page 35) un *principe de récurrence*. Dans la pratique, on considère ce principe comme une méthode de démonstration. Celle-ci admet au moins trois formes distinctes, que nous allons expliciter et illustrer.

La preuve par *récurrence simple* est celle qui a été décrite page 35.
Soit $P(n)$ un prédicat défini sur $\mathbf{N}$ et vérifiant les deux hypothèses suivantes :
- *Initialisation : $P(0)$ est vraie.*
- *Hérédité : $\forall n \in \mathbf{N}\ ,\ \big(P(n) \Rightarrow P(n+1)\big)$.*

Alors P est vraie sur $\mathbf{N}$ tout entier : $\forall n \in \mathbf{N}\ ,\ P(n)$.
On peut d'ailleurs aussi bien appliquer ce principe à $\mathbf{N}^*$ (qui est bien ordonné), ou à $\mathbf{N} \setminus \{0, 1\}$, etc. Il faut alors respectivement initialiser en vérifiant que $P(1)$ est vraie, ou que $P(2)$ est vraie, etc.

Exemple.
Montrons que, pour tout $n \in \mathbf{N}$, on a $2^n > n$. Nous notons donc, pour tout $n \in \mathbf{N}$:

$$P(n) := (2^n > n).$$

Initialisation : la propriété $P(0)$ dit que $2^0 > 0$, *i.e.* que $1 > 0$, qui est vraie.
Hérédité : supposons $P(n)$ vraie, *i.e.* $2^n > n$ (hypothèse de récurrence). Alors :

$$2^{n+1} = 2^n + 2^n \geq 2^n + 1 > (n+1) + 1.$$

La dernière inégalité utilisait l'hypothèse de récurrence. On a bien prouvé $P(n+1)$.
Du principe de récurrence (simple), on déduit que $\forall n \in \mathbf{N}\ ,\ P(n)$.

La preuve par *récurrence forte* est également conséquence du fait que $\mathbf{N}$ est bien ordonné. Elle découle du principe suivant.
Soit $P(n)$ un prédicat défini sur $\mathbf{N}$ et vérifiant l'hypothèse suivante :
Hérédité forte :

$$\forall n \in \mathbf{N}\ ,\ \Big(\big(\forall m < n\ ,\ P(m)\big) \Rightarrow P(n)\Big).$$

Alors P est vraie sur $\mathbf{N}$ tout entier : $\forall n \in \mathbf{N}\ ,\ P(n)$.
On peut d'ailleurs aussi bien appliquer ce principe à $\mathbf{N}^*$ ou à $\mathbf{N} \setminus \{0,1\}$, etc.

Exemple.
Disons qu'un entier $n \in \mathbf{N} \setminus \{0,1\}$ est *irréductible* s'il n'est pas le produit de deux entiers $p, q \in \mathbf{N} \setminus \{0,1\}$. Nous allons montrer que tout entier de $\mathbf{N} \setminus \{0,1\}$ est produit d'entiers irréductibles.
Nous notons donc, pour tout $n \in \mathbf{N} \setminus \{0,1\}$:

$$P(n) := (n \text{ est produit d'entiers irréductibles}).$$

Soit $n \in \mathbf{N} \setminus \{0,1\}$ et supposons (hypothèse de récurrence forte) que tout entier $m \in \mathbf{N} \setminus \{0,1\}$ tel que $m < n$ vérifie $P(m)$, autrement dit, qu'il est produit d'irréductibles. Il s'agit d'en déduire que n est lui-même produit d'irréductibles (hérédité forte). On distingue deux cas :

1. Si n est irréductible, il est bien entendu produit d'irréductibles !
2. Sinon, il est réductible et l'on peut écrire $n = pq$ avec $p, q \in \mathbf{N} \setminus \{0,1\}$. Comme $p, q > 1$, on a $p, q < n$. On peut donc leur appliquer l'hypothèse de récurrence forte : $P(p)$ et $P(q)$ sont vraies, *i.e.* p et q sont produits d'irréductibles, donc $n = pq$ aussi.

On a bien démontré $P(n)$, donc l'hérédité forte. Du principe de récurrence forte on tire la conclusion. (Cette démonstration remonte aux Éléments d'Euclide.)

La preuve par *récurrence double*, ou *récurrence à deux pas* [1] repose sur le principe suivant :
Soit $P(n)$ un prédicat défini sur $\mathbf{N}$ et vérifiant les deux hypothèses suivantes :

- *Initialisation : $P(0)$ et $P(1)$ sont vraies.*
- *Hérédité : $\forall n \in \mathbf{N}$, $\Big(\big(P(n)$ et $P(n+1)\big) \Rightarrow P(n+2)\Big)$.*

Alors P est vraie sur $\mathbf{N}$ tout entier : $\forall n \in \mathbf{N}$, $P(n)$.
On peut d'ailleurs aussi bien appliquer ce principe à $\mathbf{N}^*$, ou à $\mathbf{N} \setminus \{0,1\}$, etc. Il faut alors respectivement initialiser en vérifiant que $P(1)$ et $P(2)$ sont vraies, ou que $P(2)$ et $P(3)$ sont vraies, etc.

Exemple.
Nous allons démontrer que $(1+\sqrt{2})^n + (1-\sqrt{2})^n \in \mathbf{Z}$ pour tout entier $n \in \mathbf{N}$. C'est vrai pour $n = 0$ et $n = 1$ (calcul facile). De plus :

$$(1+\sqrt{2})^{n+2} + (1-\sqrt{2})^{n+2} = 2\big((1+\sqrt{2})^{n+1} + (1-\sqrt{2})^{n+1}\big) + \big((1+\sqrt{2})^n + (1-\sqrt{2})^n\big),$$

ce que l'on peut écrire $u_{n+2} = 2u_{n+1} + u_n$, en posant $u_n := (1+\sqrt{2})^n + (1-\sqrt{2})^n$. Il est alors clair que ($u_n \in \mathbf{Z}$ et $u_{n+1} \in \mathbf{Z}$) $\Rightarrow u_{n+2} \in \mathbf{Z}$, et l'on a bien l'hérédité, donc la conclusion par récurrence à deux pas.

L'hérédité dans cette démonstration, repose sur la relation (de récurrence à deux pas !) $u_{n+2} = 2u_{n+1} + u_n$. Notons qu'en posant $v_n := (1+\sqrt{2})^n - (1-\sqrt{2})^n$ on a la relation analogue : $v_{n+2} = 2v_{n+1} + v_n$, donc la même propriété d'hérédité pour l'assertion $v_n \in \mathbf{Z}$. De plus, cette dernière est vraie pour $n = 0$, mais fausse pour $n = 1$: l'initialisation en $n = 0$ est donc insuffisante dans une récurrence à deux pas.

Constructions par récurrence. On peut *définir* des objets par récurrence. Il y a, là encore, les récurrences simple, forte et à deux (ou k) pas. Nous allons illustrer chaque cas par un exemple.

Exemple.
On peut définir une suite numérique par récurrence simple ; par exemple la suite des *factorielles* :

$$0! := 1 \text{ et } \forall n \in \mathbf{N} \ , \ (n+1)! := (n+1)\, n!.$$

Ainsi, $1! = 1$, $2! = 2$, $3! = 6$, $4! = 24$, etc.

Exemple.
On peut définir une suite numérique par récurrence double ; par exemple, la suite de Fibonacci :

$$F_0 = 0, \ F_1 := 1 \text{ et } \forall n \in \mathbf{N} \ , \ F_{n+2} := F_{n+1} + F_n.$$

[1] Il existe aussi des récurrence à trois pas, et même à k pas, où $k \in \mathbf{N}^*$.

Exemple.
On peut définir une suite numérique par récurrence forte ; par exemple :

$$\forall n \in \mathbf{N}\ ,\ u_n := 1 + \sum_{i=0}^{n-1} u_i.$$

Par convention, pour $n = 0$, la "somme vide" $\sum_{i=0}^{n-1} u_i$ vaut 0. On a donc $u_0 = 1$, $u_1 = 2$, $u_2 = 4$ et $u_3 = 8$; et ensuite ?

Exercice.
Démontrer, par récurrence sur n, que $u_n = 2^n$.

Exercice.
On pose $v_0 := 0$, $v_1 := 1$ et $v_{n+2} := -v_{n+1} - v_n$. Calculer le terme général.

2.1.2 Comparaison de cardinaux finis.

Nous reprenons d'abord des théorèmes généraux sur les cardinaux et les appliquons ensuite de manière amusante.

Théorème.
Soit $f : E \to F$ une application.
(i) Si f est injective, card $E \leq$ card F.
(ii) On suppose que card $E =$ card F. Alors f injective si, et seulement si, elle est surjective. (Naturellement, elle est alors bijective.) □

Corollaire *(Principe des tiroirs de Dirichlet)*.
Soit $f : E \to F$ une application. Si card $E >$ card F, il existe $a \neq b \in E$ tels que $f(a) = f(b)$.

Exemples.
Dans un groupe de 27 personnes, il y en a certainement deux dont le nom commence par la même lettre.
Le nombre de cheveux normal d'une personne est de l'ordre de 100000 à 150000. Admettons qu'il soit toujours inférieur à 200000. Il y a donc à Toulouse deux personnes qui ont le même nombre de cheveux.

Exercice.
Dans un dé "polyédrique" (nombre quelconque de faces ayant chacune un nombre quelconque de côtés), il y a deux faces qui ont le même nombre de côtés.

2.1.3 Avec l'addition

Nous prendrons comme point de départ la propriété suivante :
Si A et B sont des ensembles finis disjoints, $\text{card}\ (A \cup B) = \text{card}\ A + \text{card}\ B$.

Un peu de théorie des ensembles. On peut définir l'addition des entiers de manière purement ensembliste, par la formule : $\text{card}\ A + \text{card}\ B := \text{card}\ (A \cup B)$, à condition bien entendu de choisir A et B disjoints. Voici une autre définition ... par récurrence ! Rappelons que l'on a déjà défini le successeur $m+1$ d'un cardinal m (page 34) et remarqué que le successeur d'un entier est un entier (page 35). On fixe alors $m \in \mathbf{N}$ et l'on définit $m+n$ par récurrence sur n :

$$m + 0 = m \text{ et } \forall n \in \mathbf{N}\ ,\ m + (n+1) := (m+n) + 1.$$

Dans un cas comme dans l'autre, on démontre alors par récurrence les propriétés bien connues : associativité, commutativité, soustraction, etc. Nous les admettrons et nous nous concentrerons sur celles relatives aux dénombrements.

Théorème.
Si A et B sont des ensembles finis quelconques :

$$\text{card}\ (A \cup B) = \text{card}\ A + \text{card}\ B - \text{card}\ (A \cap B).$$

Démonstration. On a d'abord, par application de la propriété de départ à la réunion disjointe $A = (A \cap B) \cup (A \setminus B)$:

$$\text{card}\ A = \text{card}\ (A \cap B) + \text{card}\ (A \setminus B) \Longrightarrow \text{card}\ A - \text{card}\ (A \cap B) = \text{card}\ (A \setminus B).$$

On remarque ensuite que $(A \cup B)$ est l'union disjointe de B et de $(A \setminus B)$, auxquels on applique à nouveau la propriété de départ :

$$\text{card}\ (A \cup B) = \text{card}\ B + \text{card}\ (A \setminus B) = \text{card}\ A + \text{card}\ B - \text{card}\ (A \cap B).$$

□

Pour comprendre ce qui va suivre, essayons le cas de trois ensembles finis A, B, C :

$$\text{card}\ (A \cup B \cup C) = \text{card}\ \big((A \cup B) \cup C\big) = \text{card}\ (A \cup B) + \text{card}\ (C) - \text{card}\ \big((A \cup B) \cap C\big).$$

On calcule donc $\text{card}\ (A \cup B) = \text{card}\ A + \text{card}\ B - \text{card}\ (A \cap B)$ et :

$$\begin{aligned} \text{card}\ \big((A \cup B) \cap C\big) &= \text{card}\ \big((A \cap C) \cup (B \cap C)\big) \\ &= \text{card}\ (A \cap C) + \text{card}\ (B \cap C) - \text{card}\ \big((A \cap C) \cap (B \cap C)\big) \\ &= \text{card}\ (A \cap C) + \text{card}\ (B \cap C) - \text{card}\ (A \cap B \cap C). \end{aligned}$$

En reportant dans la première égalité, on trouve enfin :

$$\text{card}\ (A \cup B \cup C) = \text{card}\ A + \text{card}\ B + \text{card}\ C - \text{card}\ (A \cap B) - \text{card}\ (A \cap C) - \text{card}\ (B \cap C) + \text{card}\ (A \cap B \cap C).$$

Théorème *(Formule d'inclusion-exclusion ou formule du crible).*
Soient $A_1, \ldots, A_n$ des ensembles finis quelconques. Alors :

$$\begin{aligned}
\text{card}\,(A_1 \cup \cdots \cup A_n) &= \sum_{i=1}^{n} \text{card}\, A_i - \sum_{1\le i<j\le n} \text{card}\,(A_i \cap A_j) \\
&+ \sum_{1\le i<j<k\le n} \text{card}\,(A_i \cap A_j \cap A_k) \\
&- \sum_{1\le i<j<k<\ell\le n} \text{card}\,(A_i \cap A_j \cap A_k \cap A_\ell) + \cdots \\
&+ (-1)^{n-1} \text{card}\,(A_1 \cap \cdots \cap A_n) \\
&= \sum_{k=1}^{n} (-1)^{k-1} \sum_{1\le i_1<\cdots<i_k\le n} \text{card}\,(A_{i_1} \cap \cdots \cap A_{i_k}).
\end{aligned}$$

Démonstration. Par récurrence sur n ; réservé aux courageux ! □

Exemple.
Anticipant sur le cours d'arithmétique, nous allons calculer le nombre d'entiers dans $[\![1, 900]\!]$ ayant un facteur commun avec 900. Ces entiers sont nécessairement divisibles par l'un des facteurs premiers de 900, lesquels sont 2, 3 et 5. On pose donc :

$$A := \{n \in [\![1,900]\!] \mid 2|n\}, \quad B := \{n \in [\![1,900]\!] \mid 3|n\} \text{ et } C := \{n \in [\![1,900]\!] \mid 5|n\}.$$

Les éléments de A sont les $2k$ tels que $1 \le k \le 900/2$, il y en a donc 450 ; avec le même raisonnement pour B et C, on trouve :

$$\text{card}\, A = 450, \quad \text{card}\, B = 300 \text{ et } \text{card}\, C = 180.$$

Les éléments de $A \cap B$ sont les $6k$ tels que $1 \le k \le 900/6$, il y en a donc 150 ; avec le même raisonnement pour $A \cap C$ et $B \cap C$, on trouve :

$$\text{card}\,(A \cap B) = 150, \quad \text{card}\,(A \cap C) = 90 \text{ et } \text{card}\,(B \cap C) = 60.$$

Enfin, les éléments de $A \cap B \cap C$ sont les $30k$ tels que $1 \le k \le 900/30$, il y en a donc 30. Finalement, le nombre cherché est :

$$\begin{aligned}
\text{card}\,(A \cup B \cup C) &= \text{card}\, A + \text{card}\, B + \text{card}\, C \\
&- \text{card}\,(A \cap B) - \text{card}\,(A \cap C) - \text{card}\,(B \cap C) \\
&+ \text{card}\,(A \cap B \cap C) \\
&= 450 + 300 + 180 - 150 - 90 - 60 + 30 = 660.
\end{aligned}$$

Exercice.
Combien d'entiers de $[\![100, 999]\!]$ ont au moins un chiffre 7 en écriture décimale ?

2.1.4 Avec la multiplication

Nous prendrons comme point de départ la propriété suivante :
Si A et B sont des ensembles finis quelconques, card $(A \times B) =$ card $A \times$ card B.

Un peu plus de théorie des ensembles. On peut définir la multiplication des entiers de manière purement ensembliste, par la formule : card $A \times$ card $B :=$ card $(A \times B)$. Voici une autre définition, par récurrence. On fixe $m \in \mathbf{N}$ et l'on définit $m.n$ par récurrence sur n : $m.0 = 0$ et, pour tout $n \in \mathbf{N}$, $m.(n+1) := m.n + m$. Dans un cas comme dans l'autre, on démontre alors par récurrence les propriétés bien connues : associativité, commutativité, simplifiabilité (*i.e.* $ab = ac \Rightarrow b = c$ si $a \neq 0$), etc. Nous les admettrons et nous nous concentrerons sur celles relatives aux dénombrements.

Théorème *(Principe des bergers).*
Soit $f : E \to F$ une application. On suppose que toutes les images réciproques $f^{-1}(\{y\})$, $y \in F$, ont le même nombre d'éléments q. Alors card $E = q$ card F.
Démonstration. Fixons un ensemble G à q éléments (par exemple $[\![1, q]\!]$). Pour tout $y \in F$, soit ϕ_y une bijection de G sur $f^{-1}(\{y\})$. L'application $(y, i) \mapsto \phi_y(i)$ est alors une bijection de $F \times G$ sur E. □

Exemple.
Pour compter des moutons, il suffit de compter les pattes et de diviser par 4. (Des applications plus significatives suivront !)

Puissances. Fixons $a \in \mathbf{N}$. On définit a^n par récurrence sur n : $a^0 = 1$ et, pour tout $n \in \mathbf{N}$, $a.(n+1) := a.a^n$. On démontre (par récurrence !) les formules classiques : $a^{m+n} = a^m.a^n$, $(ab)^m = a^m b^m$ et $(a^m)^n = a^{mn}$.

Théorème.
Soit E un ensemble fini. On a : card $\mathcal{P}(E) = 2^{\text{card } E}$.
Démonstration. Elle se fait par récurrence sur $n :=$ card E. Pour $n = 0$, on a card $\mathcal{P}(\emptyset) =$ card $\{\emptyset\} = 1 = 2^0$, comme escompté.
Supposons la propriété vérifiée pour un ensemble à n éléments et considérons E tel que card $E = n + 1$. Soient $x \in E$ et $E' := E \setminus \{x\}$, d'où card $E' = n$. par hypothèse de récurrence, card $\mathcal{P}(E') = 2^n$. Considérons maintenant l'application $F \mapsto F \cap E'$ de $\mathcal{P}(E)$ dans $\mathcal{P}(E')$. Pour tout $F' \in \mathcal{P}(E')$, l'image réciproque de F' dans $\mathcal{P}(E)$ a exactement 2 éléments : F' et $F' \cup \{x\}$. D'après le principe des bergers, card $\mathcal{P}(E) = 2$ card $\mathcal{P}(E') = 2.2^n = 2^{n+1}$ (c'est la définition des puissances), ce qui achève la récurrence. □

Rappelons que $\mathcal{F}(E, F)$ désigne l'ensemble des applications de E dans F. On le note également F^E, ce qui se peut se justifier par la formule card $\mathcal{F}(E, F) = (\text{card } F)^{\text{card } E}$, que nous allons maintenant démontrer.

Théorème.
Soient E et F des ensembles finis. On a : card $\mathcal{F}(E,F) = (\text{card } F)^{\text{card } E}$.
Démonstration. Elle se fait par récurrence sur $n := \text{card } E$. Nous noterons $q := \text{card } F$. Pour $n = 0$, il faut admettre que card $\mathcal{F}(\emptyset, F) = 1$. Si l'on trouve cette affirmation trop étrange (elle est pourtant rigoureusement exacte), on n'a qu'à l'admettre comme une pure convention et entamer la récurrence avec $n = 1$. Dans ce cas, E est un singleton : $E = \{x\}$ et on vérifie sans peine que l'application $f \mapsto f(x)$ de $\mathcal{F}(\{x\}, F)$ sur F est une bijection.
Supposons l'affirmation vraie pour card $E = n$ et prouvons la pour card $E = n + 1$. On écrit $E = E' \cup \{x\}$, où card $E' = n$ et où $x \notin E'$. L'hypothèse de récurrence nous dit que card $\mathcal{F}(E', F) = q^n$. Nous allons prouver, que card $\mathcal{F}(E,F) = q \,\text{card } \mathcal{F}(E', F)$. Considérons en effet l'application de restriction $f \mapsto f_{|F'}$ de $\mathcal{F}(E,F)$ dans $\mathcal{F}(E', F)$. L'image réciproque de $g \in \mathcal{F}(E', F)$ est formée des $f \in \mathcal{F}(E,F)$ qui prennent sur F' les mêmes valeurs que g et qui prennent en x une valeur arbitraire dans F. Il y a donc q telles applications f et le principe des bergers nous donne la conclusion. On a donc : card $\mathcal{F}(E,F) = q.q^n = q^{n+1}$, vue la définition par récurrence des puissances, ce qui achève la démonstration. □

Rappelons qu'à l'aide des fonctions caractéristiques (page 16), on avait construit une bijection de $\mathcal{P}(E)$ sur $\mathcal{F}(E, \{0,1\})$. Le théorème que nous venons de démontrer fournit donc une nouvelle preuve de l'égalité card $\mathcal{P}(E) = 2^{\text{card } E}$.

Un peu de surjections. Notons $n := \text{card } E$ et $p := \text{card } F$. Nous allons compter le nombre $S(n,p)$ d'applications surjectives de E dans F. Naturellement, on peut tout aussi bien supposer que $F = [\![1, p]\!]$, ce que nous ferons. Pour tout $i \in F$, soit $\mathcal{F}_i := \{f \in \mathcal{F}(E,F) \mid i \notin \text{Im} f\}$. Par définition, l'ensemble des surjections est égal à $\mathcal{F}(E,F) \setminus \bigcup_{i \in F} \mathcal{F}_i$, de sorte que $S(n,p) = p^n - \text{card } \bigcup_{i \in F} \mathcal{F}_i$. Nous allons calculer le cardinal de $\bigcup_{i \in F} \mathcal{F}_i$ à l'aide de la formule du crible :

$$\text{card } \bigcup_{i \in F} \mathcal{F}_i = \text{card } \bigcup_{i=1}^{p} \mathcal{F}_i = \sum_{k=1}^{p} (-1)^{k-1} \sum_{1 \le i_1 < \cdots < i_k \le p} \text{card } (\mathcal{F}_{i_1} \cap \cdots \cap \mathcal{F}_{i_k}).$$

L'ensemble $\mathcal{F}_{i_1} \cap \cdots \cap \mathcal{F}_{i_k}$ est formé des applications $f : E \to F$ telles que $i_1, \ldots, i_k \notin \text{Im} f$, autrement dit, des applications de E dans $F \setminus \{i_1, \ldots, i_k\}$. Comme ce dernier ensemble a $p - k$ éléments, on déduit du théorème : card $(\mathcal{F}_{i_1} \cap \cdots \cap \mathcal{F}_{i_k}) = (p-k)^n$. Anticipant sur la section 2.2 et notant $\binom{p}{k}$ le nombre de parties à k éléments $\{i_1, \ldots, i_k\} \subset F$:

$$S(n,p) = p^n - \sum_{k=1}^{p} (-1)^{k-1} \binom{p}{k} (p-k)^n = \sum_{k=0}^{p} (-1)^k \binom{p}{k} (p-k)^n.$$

Exercice.
Combien vaut 0^n ?

Exercice.
Soit $E \subset \mathbf{C}^*$ un ensemble à n éléments et soit $p \in \mathbf{C}^*$. Combien y a-t'il de complexes tels que $z^p \in E$?

2.2 Analyse combinatoire

2.2.1 Arrangements, permutations

Arrangements. Soient E et F deux ensembles finis ayant respectivement m et n éléments. Nous noterons $I(E,F)$ l'ensemble des applications injectives de E dans F. Si $m > n$, il n'y en a aucune et $I(E,F) = \emptyset$. Nous allons calculer card $I(E,F)$ lorsque $m \leq n$. Remarquons d'abord que, si card E = card E' et card F = card F', alors card $I(E,F)$ = card $I(E',F')$. (Argument : une bijection entre E et E' et une bijection entre F et F' donnent lieu à une bijection entre $I(E,F)$ et $I(E',F')$.) Le nombre recherché ne dépend donc que de m et de n. On le note A_n^m. (Donc $A_n^m = 0$ lorsque $m > n$.) Pour la même raison, on peut aussi bien supposer que $E = [\![1,m]\!]$. Dans ce cas, se donner une application injective f de E dans F revient à se donner une suite $(y_1,\ldots,y_m)$ de m éléments distincts de F : on pose $y_i := f(i)$. Une telle suite est appellée *arrangement de m objets pris parmi n.*

Lemme.
Si $0 \leq m \leq n-1$, on a : $A_n^{m+1} = (n-m)A_n^m$.
Démonstration. À toute suite $(y_1,\ldots,y_{m+1})$ de $(m+1)$ éléments distincts de F, associons la suite $(y_1,\ldots,y_m)$ de m éléments distincts de F. On obtient ainsi une application ϕ de $I([\![1,m+1]\!],F)$ dans $I([\![1,m]\!],F)$. L'image réciproque de $(y_1,\ldots,y_m)$ par ϕ est formée de toutes les suites $(y_1,\ldots,y_m,y)$ telles que $y \in F \setminus \{y_1,\ldots,y_m\}$: cette image réciproque a donc $(n-m)$ éléments. D'après le principe des bergers, card $I([\![1,m+1]\!],F) = (n-m)$ card $I([\![1,m]\!],F)$. □

Théorème.
Si $m \leq n$, on a $A_n^m = \dfrac{n!}{(n-m)!} = \prod_{i=0}^{m-1}(n-i)$.
Démonstration. Elle se fait par récurrence sur m. Pour $m = 0$, l'unique application de $\emptyset$ dans F est injective et l'on trouve $A_n^0 = 1 = \dfrac{n!}{n!}$, ce qui est correct. Si l'on trouve l'argument trop bizarre, on admet cette valeur comme une convention et l'on initialise la récurrence à $m := 1$. Dans ce cas, E est un singleton et les n applications de E dans F sont injectives : on a bien $A_n^1 = \dfrac{n!}{(n-1)!} = n$. On peut également dire que les arrangements de 1 objet pris parmi n sont ici les n suites (y) de 1 élément de F.
Supposons maintenant que $A_n^m = \dfrac{n!}{(n-m)!}\cdot$ pour un certain $m \in [\![0,n-1]\!]$. En combinant le lemme et l'hypothèse de récurrence, on trouve :

$$A_n^{m+1} = (n-m)A_n^m = (n-m)\frac{n!}{(n-m)!} = \frac{n!}{\big(n-(m+1)\big)!},$$

d'où la première égalité. L'égalité $\dfrac{n!}{(n-m)!} = \prod_{i=0}^{m-1}(n-i)$ est immédiate. □

Permutations. Lorsque $m = n$, toute application injective de E dans F est bijective. Le nombre A_n^n de ces bijections est égal au nombre des suites finies $(y_1, \ldots, y_n)$ formées des n éléments de F, chacun étant (bien entendu) présent une fois et une seule. Une telle suite est appelée *permutation* de F. Une définition essentiellement équivalente est celle-ci : une permutation de F est une bijection de F dans lui-même.

Théorème.
Le nombre de permutations d'un ensemble à n éléments est $n!$.

Démonstration. C'est $A_n^n = \dfrac{n!}{(n-n)!} = \dfrac{n!}{0!} = n!$. □

Un peu de dérangements. Soit $f : F \to F$ une application bijective (donc une permutation). On dit que c'est un *dérangement* si : $\forall y \in F\ ,\ f(y) \neq y$. De manière équivalente, la suite $(y_1, \ldots, y_n)$ de n éléments distincts de $\{1, \ldots, n\}$ est un dérangement si $\forall i \in [\![1, n]\!]\ ,\ y_i \neq i$. Nous allons calculer le nombre d_n de dérangements de F. Pour cela, nous prendrons $F := \{1, \ldots, n\}$. Nous noterons S_n l'ensemble de toutes les permutations de F et D_n l'ensemble de tous les dérangements de F. Pour tout $i \in F$, nous noterons $\mathcal{F}_i$ l'ensemble des bijections $f : F \to F$ telles que $f(i) = i$. L'ensemble des dérangements est donc égal à : $D_n = S_n \setminus \bigcup_{i=1}^n \mathcal{F}_i$, de sorte que : $d_n = n! - \text{card } \bigcup_{i=1}^n \mathcal{F}_i$. On applique la formule du crible :

$$\text{card } \bigcup_{i=1}^n \mathcal{F}_i = \sum_{k=1}^n (-1)^{k-1} \sum_{1 \leq i_1 < \cdots < i_k \leq n} \text{card } (\mathcal{F}_{i_1} \cap \cdots \cap \mathcal{F}_{i_k}).$$

Mais $\mathcal{F}_{i_1} \cap \cdots \cap \mathcal{F}_{i_k}$ est formé des permutations telles que $f(i_1) = i_1, \ldots, f(i_k) = i_k$. Leur nombre est celui des permutations de $F \setminus \{i_1, \ldots, i_k\}$, c'est-à-dire $(n-k)!$. Par ailleurs, le nombre des k-uplets $(i_1, \ldots, i_k)$ tels que $1 \leq i_1 < \cdots < i_k \leq n$ est noté $\binom{n}{k}$. Nous montrerons plus loin que $\binom{n}{k} = \dfrac{n!}{k!(n-k)!}$.
Il en découle :

$$\text{card } \bigcup_{i=1}^n \mathcal{F}_i = \sum_{k=1}^n (-1)^{k-1} \binom{n}{k} (n-k)! = \sum_{k=1}^n (-1)^{k-1} \frac{n!}{k!}.$$

Finalement :

$$d_n = n! - \sum_{k=1}^n (-1)^{k-1} \frac{n!}{k!} = n! \sum_{k=0}^n \frac{(-1)^k}{k!}.$$

On verra en cours d'analyse (une autre année !) que $\lim\limits_{n \to +\infty} \sum\limits_{k=0}^n \dfrac{(-1)^k}{k!} = \dfrac{1}{e}$. Donc $d_n \sim \dfrac{n!}{e}$.

Exercice.
Décrire tous les arrangements de 1, 2, 3 objets pris parmi les 4 éléments $\{1, 2, 3, 4\}$.

Exercice.
Décrire toutes les permutations de $F := \{1, 2, 3\}$ de deux manières (suites d'éléments de F ou bijections de F dans lui-même).

Exercice.
Décrire tous les dérangements de $\{1, 2, 3, 4\}$.

2.2.2 Combinaisons

Soit E un ensemble à n éléments. Lorsque $0 \leq m \leq n$, on appelle *combinaison de m objets pris parmi les n éléments de E* un sous-ensemble $\{y_1, \ldots, y_m\}$ formé de m éléments distincts de E : ce n'est donc rien d'autre qu'un sous-ensemble à m éléments de n. La différence entre une combinaison et un arrangement, c'est que l'ordre importe dans un arrangement mais pas dans une combinaison. Le nombre de ces combinaisons ne dépend évidemment que de m et de n. On le note traditionnellement C_n^m et, de manière plus moderne (influencée par l'univers anglo-saxon !) $\binom{n}{m}$, ce qui se lit : "choix de m parmi n". Les $C_n^m = \binom{n}{m}$ sont appelés *coefficients binomiaux* pour des raisons qui apparaitront à la section 2.2.4. Par convention, ou par raison, on a $\binom{n}{m} = 0$ lorsque $m > n$.

Théorème.
Lorsque $0 \leq m \leq n$, le nombre de combinaisons de m objets pris parmi n est donné par la formule :

$$C_n^m = \binom{n}{m} = \frac{n!}{m!\,(n-m)!}\cdot$$

Démonstration. À chaque arrangement $(y_1, \ldots, y_m)$ dans E, associons l'ensemble $\{y_1, \ldots, y_m\}$ sous-jacent, obtenu en oubliant l'ordre. Les arrangements ayant pour image une combinaison $\{y_1, \ldots, y_m\}$ donnée sont les $m!$ permutations de $(y_1, \ldots, y_m)$. D'après le principe des bergers, on a donc $A_n^m = m!\, C_n^m$, d'où la conclusion. □

Corollaire.
Le nombre d'applications strictement croissantes de $[\![1, m]\!]$ dans $[\![1, n]\!]$ est $\binom{n}{m}$.
Démonstration. Une application strictement croissante f de $[\![1, m]\!]$ dans $[\![1, n]\!]$ est totalement déterminée par son image $\{y_1, \ldots, y_m\} \subset [\![1, n]\!]$: le plus petit élément est $f(1)$, le suivant est $f(2)$, etc.

Corollaire.
Pour $0 \leq m \leq n$, on a les formules :

$$\binom{n}{m} = \binom{n}{n-m} \text{ et } \sum_{m=0}^{n} \binom{n}{m} = 2^n.$$

Démonstration. La première formule est immédiate par calcul sur l'expression $\binom{n}{m} = \frac{n!}{m!\,(n-m)!}\cdot$ On peut également la justifier en remarquant que, si $\operatorname{card} E = n$, l'application $F \mapsto \complement_E F$ (passage au complémentaire) est une bijection de l'ensemble des parties à m éléments sur l'ensemble des parties à $(n-m)$ éléments.
La deuxième formule vient de ce que E a au total 2^n parties, dont $\binom{n}{0}$ à 0 éléments, $\binom{n}{1}$ à 1 élément, $\binom{n}{2}$ à 2 éléments, etc. □

Exemple.
Donnons une démonstration combinatoire de la formule :

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

Soient E et F deux ensembles disjoints ayant respectivement m et n éléments. L'ensemble $E \cup F$ a $(m+n)$ éléments, donc $\binom{m+n}{q}$ sous-ensembles à q éléments. Chacun de ces sous-ensemble est de la forme $E' \cup F'$, où $E' \subset E$ a p éléments (pour un p tel que $0 \leq p \leq q$) et où $F' \subset F$ a $(q-p)$ éléments. Pour chaque p, il y a $\binom{m}{p}\binom{n}{q-p}$ tels ensembles $E' \cup F'$, et leur nombre total est bien $\sum_{p=0}^{q} \binom{m}{p}\binom{n}{q-p}$. Une autre preuve, de nature algébrique, sera proposée en exercice à la section 2.2.4.

Exercice.
Décrire toutes les combinaisons de 1, 2, 3 objets pris parmi les 4 éléments $\{1, 2, 3, 4\}$.

Exercice.
Combien de poignées de main échangent n personnes qui se rencontrent ?

2.2.3 Étude des coefficients binomiaux

Théorème *(Formule de Pascal).*
Pour tous $m, n \in \mathbf{N}$ on a :

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

Démonstration. Si $m > n$, les deux membres de l'égalité sont nuls. Si $m = n$, $\binom{n+1}{m+1} = \binom{n}{m} = 1$ et $\binom{n}{m+1} = 0$, et les deux membres de l'égalité sont égaux à 1. On peut donc supposer que $0 \leq m < n$. Nous disposons dans ce cas de deux preuves tout à fait différentes.
La preuve calculatoire vient immédiatement à l'esprit :

$$\begin{aligned}
\binom{n}{m+1} + \binom{n}{m} &= \frac{n!}{(m+1)!\,\big(n-(m+1)\big)!} + \frac{n!}{m!\,(n-m)!} \\
&= (n-m)\frac{n!}{(m+1)!\,(n-m)!} + (m+1)\frac{n!}{(m+1)!\,(n-m)!} \\
&= (n+1)\frac{n!}{(m+1)!\,(n-m)!} \\
&= \frac{(n+1)!}{(m+1)!\,(n-m)!} \\
&= \binom{n+1}{m+1}.
\end{aligned}$$

La preuve combinatoire revient à montrer que les deux nombres comptent la même chose. Considérons un ensemble E à n éléments soit $E' := E \cup \{x\}$ avec $x \notin E$. Donc E' a $(n+1)$ éléments. L'entier $\binom{n+1}{m+1}$ est le nombre de parties de E' qui ont $(m+1)$ éléments. Il y en a de deux types :

1. Les parties à $(m+1)$ éléments de E : il y en a $\binom{n}{m+1}$.
2. Les $F \cup \{x\}$, où F est une partie à m éléments de E : il y en a $\binom{n}{m}$.

Au total, on a bien $\left(\binom{n}{m+1} + \binom{n}{m}\right)$ parties à $(m+1)$ éléments de E'. □

On peut calculer les coefficients binomiaux à l'aide du *triangle de Pascal* :

```
                    1
                  1   1
                1   2   1
              1   3   3   1
            1   4   6   4   1
          1   5  10  10   5   1
```

La règle de formation est la suivante : les côtés du triangle sont formés de 1 ; chaque coefficient du tableau est la somme de ceux qui lui sont supérieurs juste à gauche et juste à droite. Sur la n^{e} ligne on trouve alors de gauche à droite les $\binom{n}{m}$ pour $m = 0, 1, \ldots, n$.

La formule de Pascal permet également un calcul "récursif" des coefficients binomiaux par l'algorithme suivant :

```
Pasc(n,p)
si p = 0 alors rendre 1 sinon si n = 0 alors rendre 0
sinon rendre Pasc(n-1,p) + Pasc(n-1,p-1) ;;
```

Le lecteur intéressé pourra rechercher la "complexité" de cet algorithme ; par exemple, combien d'additions requiert-il ? Et dans quel mesure les calculs sont-ils redondants ?

Variations des coefficients binomiaux. Soient m, n tels que $0 \leq m \leq n-1$. De la formule :

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

on déduit que $\binom{n}{m+1} > \binom{n}{m}$ si, et seulement si, $2m \leq n$. On en tire les variations de la suite des $\binom{n}{m}$ à n fixé : si n est pair, cette suite croit strictement de 0 à $n/2$ (où elle prend sa valeur maximum) puis décroit strictement de $n/2$ à n ; si n est impair, cette suite croit strictement de 0 à $(n-1)/2$, prend la même valeur (son maximum) en $(n-1)/2$ et $(n+1)/2$, puis décroit strictement de $(n+1)/2$ à n.

Exercice.
Démontrer par récurrence la formule : $\sum_{n=p}^{q} \binom{n}{p} = \binom{q+1}{p+1}$, puis l'expliciter pour $p = 1, 2, 3$.

2.2.4 La formule du binôme de Newton

Théorème *(Formule du binôme de Newton).*
Soient a et b deux nombres complexes. On a alors, pour tout $n \in \mathbf{N}$:

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

Démonstration. Elle se fait par récurrence sur n. Pour $n = 0$, il s'agit de vérifier que $(a+b)^0 = \sum_{k=0}^{0} \binom{0}{k} a^k b^{0-k}$, autrement dit, que $1 = \binom{0}{0} a^0 b^0$, ce qui est bien vrai. Supposons la formule vraie au rang n. On calcule alors :

$$\begin{aligned}
(a+b)^{n+1} &= (a+b)(a+b)^n \\
&= (a+b)\sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k} \\
&= \sum_{k=0}^{n} \binom{n}{k} a^{k+1} b^{n-k} + \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k+1} \\
&= \sum_{j=1}^{n+1} \binom{n}{j-1} a^j b^{n-j+1} + \sum_{k=0}^{n+1} \binom{n}{k} a^k b^{n-k+1} \\
&= \sum_{j=1}^{n+1} \left(\binom{n}{j-1} + \binom{n}{j} \right) a^j b^{n-j+1} + b^{n+1} \\
&= \sum_{j=1}^{n+1} \binom{n+1}{j} a^j b^{n-j+1} + \binom{n}{0} a^0 b^{n-0+1} \\
&= \sum_{j=0}^{n+1} \binom{n+1}{j} a^j b^{n+1-j}.
\end{aligned}$$

□

Un peu d'algèbre combinatoire. Si l'on développe $(a+b)^n = (a+b)\cdots(a+b)$ (n facteurs), on voit apparaitre des termes de la forme $a^k b^{n-k}$. Chacun de ces termes apparait autant de fois qu'il y a de choix des k facteurs $(a+b)$ dans lesquels on prend a plutôt que b, donc, au total $\binom{n}{k}$ fois : c'est une autre preuve de la formule de Newton. Notons que les seules propriétés utilisées sont la commutativité et l'associativité de l'addition et de la multiplication, ainsi que la distributivité.

Exercice.
Calculer le terme en x^q dans $(1+x)^m(1+x)^n = (1+x)^{m+n}$, et en déduire l'égalité :

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

Module UE8 : Quatrième feuille de TD

Dénombrements

Exercice 1.
Soit $f : E \to E$ une application d'un ensemble E dans lui-même. On définit les *itérées* f^n de f par récurrence (simple) :

$$f^0 := \mathrm{Id}_E \text{ et } \forall n \in \mathbf{N}\ ,\ f^{n+1} := f \circ f^n.$$

Ce sont donc des applications de f dans lui-même. Par exemple, $f^1 = f \circ \mathrm{Id}_E = f$ et $f^2 = f \circ f^1 = f \circ f$.
(i) Prouver, par récurrence simple sur n, que $\forall n, p \in \mathbf{N}\ ,\ f^{n+p} = f^n \circ f^p$.
(ii) On prend $E := \mathbf{N}$ et $f(x) := x + 1$. Que vaut $f^n(x)$?
(iii) On prend $E := \mathbf{N}$ et $f(x) := x + p$. Que vaut $f^n(0)$?
(iv) On prend $E := \mathbf{N}$ et $f(x) := px$. Que vaut $f^n(1)$?
(v) On prend $E := \mathbf{N}$ et $f(x) := x^p$. Que vaut $f^n(x)$?

Exercice 2.
Interpréter à l'aide de bijections les trois "formules classiques" sur les puissances données page 45.

Exercice 3.
Un polyèdre régulier a f faces, qui ont toutes le même nombre n de côtés, a arêtes, dont chacune a deux extrémités et sépare deux faces, et s sommets, qui sont tous extremités du même nombre p d'arêtes (et donc sommets de p faces). Quelles relations y a-t'il entre ces 5 nombres ?

Exercice 4.
Les 30 étudiants d'un groupe de IMP-Maths II prennent chacun une copie au hasard dans le paquet de 30 copies de contrôle continu que leur rend le professeur. Quelle est la probabilité que tous se soient trompés de copie ?

Exercice 5.
(i) Calculer le nombre d'applications croissantes de $[\![1, m]\!]$ dans $[\![1, n]\!]$.
(Remarquer que $k \mapsto f(k)$ est croissante si, et seulement si, $k \mapsto f(k) + k - 1$ est strictement croissante.)
(ii) En déduire le nombre de solutions entières de l'équation : $x_1 + \cdots + x_n = p$. Vérifier la formule obtenue pour $p = 1, 2, 3$.
(Remarquer que, pour toute solution $(x_1, \ldots, x_p)$, l'application $k \mapsto \sum_{i=1}^{k} x_i$ est croissante de $[\![1, p]\!]$ dans $[\![1, n]\!]$.)

Exercice 6.

Démontrer la formule : $\sum_{p=0}^{n} \binom{n}{p}^2 = \binom{2n}{n}$.

Exercice 7.

Démontrer algébriquement la formule : $\sum_{p=0}^{n} \binom{n}{p} = 2^n$.
(Appliquer la formule du binôme à $a = b = 1$.)

Exercice 8.

Démontrer à l'aide de la formule du binôme :

$$\sum_{p=0}^{n} (-1)^p \binom{n}{p} = \delta_{n,0} = \begin{cases} 1 \text{ si } n = 0, \\ 0 \text{ sinon.} \end{cases}$$

Donner une interprétation combinatoire de cette égalité.
(Le "symbole de Kronecker" $\delta_{a,b}$ vaut 1 si $a = b$ et 0 sinon.)

Exercice 9.

Selon un préjugé célèbre, les hommes ont en moyenne plus de partenaires féminines que les femmes n'ont de partenaires masculins. Montrer que cette affirmation est incompatible avec l'égalité du nombre d'hommes et du nombre de femmes.

Exercice 10.

Dans les régions reculées du Volvestre, on attribue le temps baroque de 2007 au fait que c'est une année à 13 lunes. On voit en effet sur le calendrier qu'elle a 13 pleines lunes, la première le 3 janvier et la dernière le 24 décembre. Quelle est la fréquence moyenne des années à 13 lunes ?
(On admettra que toutes les années ont 365 jours.)