Modèles standards des entiers naturels.

$(\mathbb{N}, \mathbf{0}, \boldsymbol{s})$ **vérifie le modèle de Peano des entiers naturels** ssi

$$\begin{cases} 0 \in \mathbb{N} \\ s: \mathbb{N} \to \mathbb{N} \\ 0 \notin s(\mathbb{N}) \\ s \text{ injective} \\ \forall A \subseteq \mathbb{N} \left((0 \in A \text{ et } s(A) \subseteq A) \Rightarrow A = \mathbb{N}\right) \end{cases}$$

$(\mathbb{N}, \leq)$ **vérifie le modèle ordinal des entiers naturels** ssi

$$\begin{cases} \mathbb{N} \neq \emptyset \\ \leq \text{ ordre total sur } \mathbb{N} \\ \forall A \subseteq \mathbb{N} | A \neq \emptyset \;\; A \text{ admet un minimum pour } \leq \\ \forall A \subseteq \mathbb{N} | A \neq \emptyset \;\; A \text{ majorée pour } \leq \Rightarrow A \text{ admet un maximum pour } \leq \\ \mathbb{N} \text{ non majorée pour } \leq \end{cases}$$

Pour un modèle de Péano $(\mathbb{N}, 0, s)$, on peut définir $+_{(\mathbb{N},\mathbf{0},\boldsymbol{s})}$ comme l'unique $+: \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ tel que

$$\begin{cases} \forall n \in \mathbb{N} \; n + 0 = n \\ \forall a, b \in \mathbb{N} \;\; a + s(b) = s(a + b) \end{cases}$$

Pour un modèle de Péano $(\mathbb{N}, 0, s)$, on peut définir $\leq_{(\mathbb{N},\mathbf{0},\boldsymbol{s})}$ comme l'unique relation binaire sur $\mathbb{N}$ vérifiant $a \leq b \Leftrightarrow \exists d \in \mathbb{N} \; a + d = b$

Le modèle ordinal induit par un modèle de Péano $(\mathbb{N}, 0, s)$, correspond à $\left(\mathbb{N}, \leq_{(\mathbb{N},0,s)}\right)$

Pour un modèle ordinal $(\mathbb{N}, \leq)$, on peut définir $\mathbf{0}_{(\mathbb{N},\leq)} = \min_{\leq} \mathbb{N}$

Pour un modèle ordinal $(\mathbb{N}, \leq)$, on peut définir $\boldsymbol{s}_{(\mathbb{N},\leq)}$ comme l'unique $s: \mathbb{N} \to \mathbb{N}$ tel que $\forall n \in \mathbb{N} \; s(n) = \min_{\leq}\{k \in \mathbb{N} \mid k \geq n \text{ et } k \neq n\}$

Le modèle de Péano induit par un modèle ordinal $(\mathbb{N}, \leq)$, correspond à $\left(\mathbb{N}, 0_{(\mathbb{N},\leq)}, s_{(\mathbb{N},\leq)}\right)$

Equivalence des modèles.

Le modèle ordinal induit par un modèle de Péano est un modèle ordinal valide des entiers naturels et le modèle de Péano qu'il induit n'est autre que le modèle originel.

Le modèle de Péano induit par un modèle ordinal est un modèle de Péano valide des entiers naturels et le modèle ordinal qu'il induit n'est autre que le modèle originel.

Ces deux modèles fournissent donc deux points de départs équivalents.

Existence. Il existe un $(\mathbb{N}, 0, s)$ vérifiant le modèle de Peano.

Construction via ZFC. Un ensemble A vérifie l'axiome de l'infini AI ssi $\begin{cases} \emptyset \in A \\ \forall x \in A \;\; x \cup \{x\} \in A \end{cases}$

Un axiome de ZFC énonce qu'il existe au moins un tel ensemble A.

On pose $\mathbb{N} = \{x \in A \mid \forall X \text{ verifiant AI } \; x \in X\} = \{x \mid \forall X \text{ verifiant AI } \; x \in X\} = \bigcap\{X \text{ verifiant AI}\}$.

$\mathbb{N}$ est le plus petit ensemble pour $\subseteq$ vérifiant AI.

On pose $0 = \emptyset$, et on pose $s: \mathbb{N} \to \mathbb{N}: x \mapsto x \cup \{x\}$. Alors $(\mathbb{N}, 0, s)$ est un modèle de Peano.

Axiomatisations.

Les deux modèles précédents énoncent des propriétés fondamentales de $\mathbb{N}$, mais ne sont pas de réelles axiomatisations des nombres entiers sur la logique, car ces modèles supposent une théorie des ensembles et des fonctions préexistante. Il est possible de donner une axiomatisation reposant uniquement sur la logique classique (calcul des propositions + prédicats), sans utiliser de concept de fonction ou d'ensemble mathématique a priori.

Une axiomatisation est **l'arithmétique de Peano** et est formulée sur $(\mathbb{N}, +, \times)$

Une axiomatisation plus faible est **l'arithmétique de Presburger** et est formulée sur $(\mathbb{N}, +)$, cependant est moins expressive.

Notations élémentaires.

$\boldsymbol{a \leq b \leq c}$ signifie $a \leq b$ et $b \leq c$
$\boldsymbol{a < b}$ signifie $a \leq b$ et $a \neq b$.
$\boldsymbol{a < b < c}$ signifie $a < b$ et $b < c$
$\mathbb{N}^* = \mathbb{N} \setminus \{0\}$
Pour $a \in \mathbb{N}^*$ $\boldsymbol{p(a) = a - 1} = s^{-1}(a)$
Pour $a, b \in \mathbb{N}$ $[\![a, b]\!] = \{k \in \mathbb{N}, a \leq k \leq b\}$
Pour $a \in \mathbb{N}$ $[\![a, \infty]\!] = \{k \in \mathbb{N}, a \leq k\}$

Formulations du principe de récurrence.

Soit $u_1, \dots, u_m$ des variables fixées, $P(n, u_1, \dots, u_m)$ un prédicat dont on abrège l'écriture en $P(n)$. m peut eventuellement etre nul auquel cas il n'y a pas de u_i. Grace à la notation set-builder le principe de récurrence se réénonce.

Récurrence simple. $\begin{cases} P(n_0) \\ \forall n \geq n_0 \ \ P(n) \Rightarrow P(n+1) \end{cases} \Rightarrow \forall n \geq n_0 \ P(n)$

Récurrence d'ordre $N \in \mathbb{N}^*$. $\begin{cases} \forall k \in [\![0, N-1]\!] \ \ P(n_0 + k) \\ \forall n \geq n_0 \ \left(\forall k \in [\![0, N-1]\!] \ \ P(n+k)\right) \Rightarrow P(n+N) \end{cases} \Rightarrow \forall n \geq n_0 \ P(n)$

Récurrence forte. $\begin{cases} P(n_0) \\ \forall n \geq n_0 \ \left(\forall k \in [\![n_0, n]\!] \ \ P(k)\right) \Rightarrow P(n+1) \end{cases} \Rightarrow \forall n \geq n_0 \ P(n)$

Propriétés élémentaires de $\mathbb{N}$.

$(\mathbb{N}, 0, s, \leq)$ vérifie le modèle de Peano, vérifie le modèle ordinal, et les récurrences.
$\{0\} \cup s(\mathbb{N}) = \mathbb{N}$
$s: \mathbb{N} \to \mathbb{N}^*$ est bijective.
$\forall a \in \mathbb{N} \ a \geq 0$
$\forall a \in \mathbb{N} \ s(a) = a + 1$
$\forall a \in \mathbb{N} \ s^{-1}(a+1) = a$
$\forall a, b \in \mathbb{N} \ \neg(a \leq b) \Leftrightarrow a > b$
$\forall a, b \in \mathbb{N} \ a \leq b \Leftrightarrow a < b + 1$
$\forall a, b \in \mathbb{N} \ a + 1 \leq b \Leftrightarrow a < b$

Addition dans $\mathbb{N}$.

$\exists! +: \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ tel que $\begin{cases} \forall n \in \mathbb{N} \ n + 0 = n \\ \forall a, b \in \mathbb{N} \ \ a + s(b) = s(a+b) \end{cases}$
$\forall a, b, c \in \mathbb{N} \ \ (a+b)+c = a+(b+c)$ (+ est associative)
$\forall a, b \in \mathbb{N} \ \ a + b = b + a$ (+ est commutative)
$\forall a, b \in \mathbb{N} \ \ a + b = 0 \Leftrightarrow a = b = 0$ (somme de positifs nuls est nulle)
Si $a = b$ alors $a + c = b + c$ et réciproquement. (+ est régulière)
Si $a \leq b$ alors $a + c \leq b + c$ et réciproquement.
Si $a < b$ alors $a + c < b + c$ et réciproquement.

Soustraction dans $\mathbb{N}$.

Le fait de définir une soustraction seulement dans $\mathbb{N}$ est maladroit car il faut toujours une précondition $a \leq b$. On préfère définir le groupe $\mathbb{Z}$ pour avoir une théorie plus élégante.
$\forall a, b \in \mathbb{N}^2 | a \leq b \ \ \exists! \, (\boldsymbol{b - a}) \in \mathbb{N} \ \ (b-a) + a = b$
$\forall a \in \mathbb{N}^* \ \ s^{-1}(a) = a - 1$
$a \leq b \Rightarrow \begin{cases} a \leq b + c \\ (b-a) + c = (b+c) - a \end{cases}$
$\begin{cases} a + b \leq c \Leftrightarrow a \leq c \text{ et } b \leq c - a \\ \text{Dans ce cas } c - (a+b) = (c-a) - b \end{cases}$
$c \leq a$ et $c \leq b \Rightarrow (a = b \Leftrightarrow a - c = b - c)$

$c \leq a$ et $c \leq b \Rightarrow (a \leq b \Leftrightarrow a - c \leq b - c)$
$c \leq a$ et $c \leq b \Rightarrow (a < b \Leftrightarrow a - c < b - c)$
Multiplication dans $\mathbb{N}$
$\exists! \times : \mathbb{N} \times \mathbb{N} \to \mathbb{N}\ \begin{cases} \forall n \in \mathbb{N}\ n \times 0 = 0 \\ \forall a, b \in \mathbb{N}\ \ a \times (b+1) = (a \times b) + a \end{cases}$
$a \times 0 = 0$
$a \times 1 = a$
$ab = ba$ ($\times$ est commutative)
$a(b+c) = ab + ac$ ($\times$ est distributive sur $+$)
$b \geq c \Rightarrow ab \geq ac$ et $a(b-c) = ab - ac$ ($\times$ est distributive sur $-$)
$(ab)c = a(bc)$ ($\times$ est associative)
$ab = 0 \Rightarrow a = 0$ ou $b = 0$ (intégrité)
Si $a = b$ alors $ac = bc$. Réciproque fausse si $c = 0$.
Si $ac = bc$ et $c \neq 0$ alors $a = b$
Si $a \leq b$ et $c \geq 0$ alors $ac \leq bc$. Réciproque fausse si $c = 0$.
Si $ac \leq bc$ et $c > 0$ alors $a \leq b$.
Si $a < b$ et $c > 0$ alors $ac < bc$.
Si $ac < bc$ et $c > 0$ alors $a < b$.
Division dans $\mathbb{N}$
Le fait de définir une division seulement dans $\mathbb{N}$ est encore très maladroit car il faut toujours une précondition de divisibilité. On préfère définir le corps $\mathbb{Q}$ pour avoir une théorie plus élégante.
Pour $a \in \mathbb{N}$ et $b \in \mathbb{N}^*$, on dit $\boldsymbol{b}$ **divise** $\boldsymbol{a}$ **/** $\boldsymbol{a}$ **multiple de** $\boldsymbol{b}$ **/** $\boldsymbol{b|a}$ **/** $\boldsymbol{\frac{a}{b}} \in \mathbb{N}$ ssi $\exists q \in \mathbb{N}\ a = qb$
Dans ce cas q est unique, est appelé **quotient de $\boldsymbol{a}$ par $\boldsymbol{b}$** et noté $q = \frac{a}{b}$
Pour $a, c \in \mathbb{N}$, et $b, d \in \mathbb{N}^*$:
$a \neq 0 \Rightarrow \frac{a}{a} \in \mathbb{N}$ et $\frac{a}{a} = 1$
$\frac{a}{1} \in \mathbb{N}$ et $\frac{a}{1} = a$
$\frac{a}{b} \in \mathbb{N}$ et $\frac{a}{b} = 0$ ssi $a = 0$
$\frac{a}{b} \in \mathbb{N}, \frac{c}{d} \in \mathbb{N} \Rightarrow \frac{ac}{bd} \in \mathbb{N}, \frac{ac}{bd} = \frac{a}{b} \times \frac{c}{d}$
$\frac{a}{b} \in \mathbb{N}, \frac{c}{d} \in \mathbb{N} \Rightarrow \left(\frac{a}{b} = \frac{c}{d} \Leftrightarrow ad = bc\right)$
$\frac{a}{b} \in \mathbb{N}, \frac{c}{d} \in \mathbb{N} \Rightarrow \left(\frac{a}{b} \leq \frac{c}{d} \Leftrightarrow ad \leq bc\right)$
$\frac{a}{b} \in \mathbb{N}, \frac{c}{d} \in \mathbb{N} \Rightarrow \left(\frac{a}{b} < \frac{c}{d} \Leftrightarrow ad < bc\right)$
$\frac{a}{b} \in \mathbb{N}, \frac{c}{d} \in \mathbb{N} \Rightarrow \frac{ad+bc}{bd} \in \mathbb{N}, \frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$
$\frac{a}{b} \in \mathbb{N}, \frac{c}{d} \in \mathbb{N}, \frac{a}{b} \geq \frac{c}{d} \Rightarrow ad \geq bc, \frac{ad-bc}{bd} \in \mathbb{N}, \frac{a}{b} + \frac{c}{d} = \frac{ad-bc}{bd}$
$\frac{a}{b} \in \mathbb{N}, \frac{c}{d} \in \mathbb{N}, c \neq 0, \frac{\frac{a}{b}}{\frac{c}{d}} \in \mathbb{N} \Rightarrow \frac{ad}{bc} \in \mathbb{N}, \frac{\frac{a}{b}}{\frac{c}{d}} = \frac{ad}{bc}$
$\forall d \in \mathbb{N}^*\ \ \forall a, b, u, v \in \mathbb{N}\ \ d|u$ et $d|v \Rightarrow d|au + bv$
Caractérisation des applications entre $\boldsymbol{[\![1, p]\!]}$ et $\boldsymbol{[\![1, q]\!]}$
Lemme. $\forall n \in \mathbb{N}^*\ \ \forall a \in [\![1, n]\!]\ \ \exists g : [\![1, n]\!] \setminus \{a\} \to [\![1, n-1]\!]\ \ g$ bijective
$\forall p, q \in \mathbb{N}^*\ \ \exists f : [\![1, p]\!] \to [\![1, q]\!]$ injective $\Leftrightarrow p \leq q$
$\forall p, q \in \mathbb{N}^*\ \ \exists f : [\![1, p]\!] \to [\![1, q]\!]$ surjective $\Leftrightarrow p \geq q$
$\forall p, q \in \mathbb{N}^*\ \ \exists f : [\![1, p]\!] \to [\![1, q]\!]$ bijective $\Leftrightarrow p = q$
$\forall n \in \mathbb{N}^*\ \ \forall f : [\![1, n]\!] \to [\![1, n]\!]$, f injective ssi f surjective ssi f bijective.

Ensembles finis et cardinaux.
Un **ensemble $\boldsymbol{E}$ est fini** ssi (E est vide ou il existe une bijection de $[\![1,n]\!] \to E$ avec $n \geq 1$)
Un **ensemble $\boldsymbol{E}$ est infini**, s'il n'est pas fini.
Le **cardinal de l'ensemble vide** est $\boldsymbol{card}(\emptyset) = 0 \in \mathbb{N}$.
Le **cardinal d'un ensemble $\boldsymbol{E}$ <u>fini non vide</u>** noté $\boldsymbol{card}(\boldsymbol{E})$, est l'unique entier $n \geq 1$, tel qu'il existe une bijection de $[\![1,n]\!] \to E$.
Le cardinal d'un ensemble fini est donc toujours un entier naturel.
Le cardinal d'un ensemble infini peut être défini, mais n'est jamais affecté à un entier naturel.
Un ensemble E est fini ssi $card(E) \in \mathbb{N}$
Un ensemble E est vide ssi $card(E) = 0$
Entre 2 ensembles finis non vides E, F, il existe une application injective ssi $card(E) \leq card(F)$
Entre 2 ensembles finis non vides E, F, il existe une application surjective ssi $card(E) \geq card(F)$
Entre 2 ensembles finis non vides E, F, il existe une application bijective ssi $card(E) = card(F)$
Entre 2 ensembles finis non vides E, F de meme cardinal, une application est injective ssi elle est surjective ssi elle est bijective.
D'un ensemble infini, on peut extraire une partie finie de taille un entier arbitraire fixé.
Une injection qui part d'un ensemble fini, arrive dans un ensemble fini.
Une surjection qui arrive d'un ensemble fini, part d'un ensemble fini.
Si deux ensembles sont en bijection, alors soit ils sont tous deux fini, soit ils sont tous deux infini.
Une application de domaine fini, a une image directe finie, car surjective dans son image.
Une famille $(x_1, \dots, x_n)$ d'entiers est **croissante** ssi $\forall i \in [\![1, n-1]\!]\ x_i \leq x_{i+1}$
Une famille $(x_1, \dots, x_n)$ d'entiers est **strictement croissante** ssi $\forall i \in [\![1, n-1]\!]\ x_i < x_{i+1}$
Pour $n \geq 1$, $\boldsymbol{S_n} = \{\sigma : [\![1,n]\!] \to [\![1,n]\!] \mid \sigma \text{ bijective}\}$
Une famille finie d'entiers peut être permutée de sorte à la rendre croissante.
$\forall n \geq 1\ \forall (x_i \in \mathbb{N})_{i \in [\![1,n]\!]}\ \exists \sigma \in S_n\ \ x \circ \sigma \text{ croissante.}$
Un <u>ensemble</u> fini non vide d'entiers peut être décrit par une famille strictement croissante d'entiers <u>unique</u>.
$\forall n \geq 1\ \ \forall X \subseteq \mathbb{N} \mid Card(X) = n\ \exists!\, (x_i \in \mathbb{N})_{i \in [\![1,n]\!]}\ x \text{ strictement croissante et } X = x([\![1,n]\!]) = \{x_1, \dots, x_n\}$
Une partie d'un ensemble fini, est finie et de cardinal inferieur. $A \subseteq E \Rightarrow card(A) \leq card(E)$
Une partie de $\mathbb{N}$ est finie ssi elle est majorée ssi elle est bornée.
L'intersection d'ensembles finis est finie, et $card(E \cap F) \leq \min\big(card(E), card(F)\big)$
L'union d'ensembles finis est finie, et $card(E \cup F) = \big(card(E) + card(F)\big) - card(E \cap F)$
Notation d'opérateur itéré, pour une l.c.i. associative et commutative.
Soit E ensemble muni d'une l.c.i. * associative et commutative. Soit $a, b \in \mathbb{N}$ tels que $a \leq b$ et soit une famille $(x_k \in E)_{k \in D \supseteq [\![a,b]\!]}$ définie au moins sur les indices $[\![a,b]\!]$.
$$\exists!\, \boldsymbol{\otimes_{k=a}^{b} x_k} \in E\ \ \otimes_{k=a}^{b} x_k = \begin{cases} x_a = x_b \text{ si } a = b \\ \big(\otimes_{k=a}^{b-1} x_k\big) * x_b \text{ si } a < b \end{cases}$$
$\forall m \in [\![a, b-1]\!]\ \otimes_{k=a}^{b} x_k = \left(\otimes_{k=a}^{m} x_k\right) * \left(\otimes_{k=m+1}^{b} x_k\right)$
$b \geq a \geq c \geq 1 \Rightarrow\ \otimes_{k=a}^{b} x_k = \otimes_{k=a-c}^{b-c} x_k$ donc on peut toujours ramener les indices entre 1 et n.
On peut définir l'opérateur pour un ensemble fini non vide A de cardinal $n \geq 1$, et une application $h : D \supseteq A \to E$ définie au moins sur A.
$\exists!\ \otimes_{x \in \boldsymbol{A}} \boldsymbol{h(x)} \in E\ \ \forall f : [\![1,n]\!] \to A$ bijective, $\otimes_{x \in A} h(x) = \otimes_{k=1}^{n} h\big(f(k)\big)$.
On a en particulier $\otimes_{k \in [\![a,b]\!]} x_k = \otimes_{k=a}^{b} x_k$

Changement de variables. Pour une bijection f vers A on a $\otimes_{x\in A} h(x) = \otimes_{y\in f^{-1}(A)} h\big(f(y)\big)$
Pour $h: D \supseteq A \cup B \to E,\ A \cap B = \emptyset \Rightarrow \otimes_{x\in A\cup B} h(x) = (\otimes_{x\in A} h(x)) * (\otimes_{x\in B} h(x))$
La somme itérée dans $\mathbb{N}$ se note $\sum$. Le produit itéré dans $\mathbb{N}$ se note $\boldsymbol{\Pi}$.
Propriétés spécifiques a $\sum$.
$\forall \alpha \in \mathbb{N}\ \ \sum_{x\in A} \alpha h(x) = \alpha \sum_{x\in A} h(x)$
$\forall \alpha \in \mathbb{N}\ \ \sum_{x\in A} \alpha = \alpha \times card(A)$, en particulier $\sum_{x\in A} 1 = card(A)$
Combinatoire.
Fonction puissance. $\exists!\ \widehat{}: \mathbb{N}\times\mathbb{N} \to \mathbb{N}: (a,b) \mapsto \boldsymbol{a^b} = \begin{cases} 1 \text{ si } b = 0 \\ \prod_{k=1}^{b} a \ \text{ si } b \geq 1 \end{cases}$
$\forall a,b,c \in \mathbb{N}\ a^{b+c} = a^b \times a^c$
Fonction factorielle. $\exists!\ !: \mathbb{N} \to \mathbb{N}: n \mapsto \boldsymbol{n}! = \begin{cases} 1 \text{ si } n = 0 \\ \prod_{k=1}^{n} k \ \text{ si } n \geq 1 \end{cases}$
Arrangement. $\forall n \in \mathbb{N}\ \forall k \in [\![0,n]\!]\ \ \exists!\, A_n^k \in \mathbb{N}\ \ \boldsymbol{A_n^k} = \frac{n!}{(n-k)!} = \begin{cases} 1 \text{ si } k = 0 \\ \prod_{k=n-k+1}^{n} k \ \text{ si } 1 \leq k \leq n \\ n! \text{ si } k = n \end{cases}$
Coefficient binomial. $\forall n \in \mathbb{N}\ \forall k \in [\![0,n]\!]\ \ \exists!\, C_n^k \in \mathbb{N}\ \ \boldsymbol{C_n^k} = \binom{\boldsymbol{n}}{\boldsymbol{k}} = \begin{cases} 1 \text{ si } k = 0 \\ \binom{n-1}{k-1} + \binom{n-1}{k} \text{ si } 1 \leq k < n \\ 1 \text{ si } k = n \end{cases}$
$\forall n \in \mathbb{N}\ \forall k \in [\![0,n]\!]\ \frac{A_n^k}{k!} \in \mathbb{N}$ et $\binom{n}{k} = \frac{A_n^k}{k!} = \frac{n!}{k!(n-k)!}$
$\forall n \in \mathbb{N}\ \binom{n}{0} = \binom{n}{n} = 1$
$\forall n \in \mathbb{N}\ \forall k \in [\![1,n-1]\!]\ \ \binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$
$\forall n \in \mathbb{N}^*\ \binom{n}{1} = \binom{n}{n-1} = n$
$\forall n \in \mathbb{N}\ \forall k \in [\![0,n]\!]\ \ \binom{n}{k} = \binom{n}{n-k}$
Pour 2 ensemble finis E, F, le produit cartésien $E \times F$ est fini, $card(E \times F) = card(E) \times card(F)$
Pour 2 ensemble finis E, F, l'ensemble des applications de E vers F càd $F^E = F(E,F)$ est fini, et $card(F^E) = card(F)^{card(E)}$
Pour 2 ensemble finis E, F, l'ensemble des injections de E vers F a $A_{card(F)}^{card(E)} = \frac{card(F)!}{(card(F)-card(E))!}$ éléments si $card(E) \leq card(F)$, exactement $card(E)!$ si égalité, mais 0 éléments si $card(E) > card(F)$.
Pour 2 ensemble finis E, F, l'ensemble des bijections de E vers F a $card(E)!$ éléments si $card(E) = card(F)$, mais 0 éléments si $card(E) \neq card(F)$.
Pour un ensemble fini E, l'ensemble des parties de E est fini de cardinal $card\big(P(E)\big) = 2^{card(E)}$
Pour un ensemble fini E a n éléments, l'ensemble des <u>parties</u> de E a $k \in [\![0,n]\!]$ éléments est $\binom{n}{k}$
Pour un ensemble fini E a n éléments, l'ensemble des <u>familles</u> de E a $k \in [\![0,n]\!]$ éléments est A_n^k puisque ce sont les injections.
Intuitivement le lien $\binom{n}{k} = \frac{A_n^k}{k!}$ peut se comprendre comme choisir une famille de k éléments mais ignorer l'ordre donc diviser par toutes les permutations possibles de cette famille.
Lemme des bergers. Si un ensemble E possède une partition en p parties contenant chacune r éléments alors E contient $p \times r$ éléments.