

## Modèles standards des entiers naturels.

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

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

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

$$\left\{ \begin{array}{l} \forall n \in \mathbb{N} \ n + 0 = n \\ \forall a, b \in \mathbb{N} \ a + s(b) = s(a + b) \end{array} \right.$$

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

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

$$\left\{ \begin{array}{l} \mathbb{N} \neq \emptyset \\ \leq \text{ ordre total sur } \mathbb{N} \\ \forall A \subseteq \mathbb{N} | A \neq \emptyset \ A \text{ admet un minimum pour } \leq \\ \forall A \subseteq \mathbb{N} | A \neq \emptyset \ A \text{ majorée pour } \leq \Rightarrow A \text{ admet un maximum pour } \leq \\ \mathbb{N} \text{ non majorée pour } \leq \end{array} \right.$$

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

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

Si  $(\mathbb{N}, 0, s)$  est un modèle de Péano des entiers naturels alors  $(\mathbb{N}, \leq_{(\mathbb{N}, 0, s)})$  est un modèle ordinal des entiers naturels.

Si  $(\mathbb{N}, \leq)$  est un modèle ordinal des entiers naturels alors  $(\mathbb{N}, 0_{(\mathbb{N}, \leq)}, s_{(\mathbb{N}, \leq)})$  est un modèle de Péano des entiers naturels.

Ces deux modèles fournissent donc deux points de départ 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  $\left\{ \begin{array}{l} \emptyset \in A \\ \forall x \in A \ x \cup \{x\} \in A \end{array} \right.$

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

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

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

On pose  $0 = \emptyset$ , et on pose  $s: \mathbb{N} \rightarrow \mathbb{N}: x \mapsto x \cup \{x\}$ . 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.

$a \leq b \leq c$  signifie  $a \leq b$  et  $b \leq c$

$a < b$  signifie  $a \leq b$  et  $a \neq b$ .

$a < b < c$  signifie  $a < b$  et  $b < c$

$$\mathbb{N}^* = \mathbb{N} \setminus \{0\}$$

$$\text{Pour } a \in \mathbb{N}^* \quad p(a) = a - 1 = s^{-1}(a)$$

$$\text{Pour } a, b \in \mathbb{N} \quad \llbracket a, b \rrbracket = \{k \in \mathbb{N}, a \leq k \leq b\}$$

$$\text{Pour } a \in \mathbb{N} \quad \llbracket a, \infty \rrbracket = \{k \in \mathbb{N}, a \leq k\}$$

### 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 éventuellement être nul auquel cas il n'y a pas de  $u_i$ . Grâce à la notation set-builder le principe de récurrence se réécrit.

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

$$\text{Récurrence d'ordre } N \in \mathbb{N}^*. \begin{cases} \forall k \in \llbracket 0, N-1 \rrbracket \quad P(n_0 + k) \\ \forall n \geq n_0 \quad (\forall k \in \llbracket 0, N-1 \rrbracket \quad P(n+k)) \Rightarrow P(n+N) \end{cases} \Rightarrow \forall n \geq n_0 \quad P(n)$$

$$\text{Récurrence forte. } \begin{cases} P(n_0) \\ \forall n \geq n_0 \quad (\forall k \in \llbracket n_0, n \rrbracket \quad P(k)) \Rightarrow P(n+1) \end{cases} \Rightarrow \forall n \geq n_0 \quad P(n)$$

### Propriétés élémentaires de $\mathbb{N}$ .

$(\mathbb{N}, 0, s, \leq)$  vérifie le modèle de Peano, vérifie le modèle ordinal, et les récurrences.

$$\{0\} \cup s(\mathbb{N}) = \mathbb{N}$$

$s: \mathbb{N} \rightarrow \mathbb{N}^*$  est bijective.

$$\forall a \in \mathbb{N} \quad a \geq 0$$

$$\forall a \in \mathbb{N} \quad s(a) = a + 1$$

$$\forall a \in \mathbb{N} \quad s^{-1}(a+1) = a$$

$$\forall a, b \in \mathbb{N} \quad \neg(a \leq b) \Leftrightarrow a > b$$

$$\forall a, b \in \mathbb{N} \quad a \leq b \Leftrightarrow a < b + 1$$

$$\forall a, b \in \mathbb{N} \quad a + 1 \leq b \Leftrightarrow a < b$$

### Addition dans $\mathbb{N}$ .

$$\exists ! +: \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N} \text{ tel que } \begin{cases} \forall n \in \mathbb{N} \quad n + 0 = n \\ \forall a, b \in \mathbb{N} \quad a + s(b) = s(a + b) \end{cases}$$

$$\forall a, b, c \in \mathbb{N} \quad (a + b) + c = a + (b + c) \quad (+ \text{ est associative})$$

$$\forall a, b \in \mathbb{N} \quad a + b = b + a \quad (+ \text{ est commutative})$$

$$\forall a, b \in \mathbb{N} \quad a + b = 0 \Leftrightarrow a = b = 0 \quad (\text{somme de positifs nuls est nulle})$$

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.

$$\forall a, b \in \mathbb{N}^2 \mid a \leq b \quad \exists ! (b - a) \in \mathbb{N} \quad (b - a) + a = b$$

$$\forall a \in \mathbb{N}^* \quad s^{-1}(a) = a - 1$$

$$a \leq b \Rightarrow \begin{cases} a \leq b + c \\ (b - a) + c = (b + c) - a \end{cases}$$

$$\begin{cases} a + b \leq c \Leftrightarrow a \leq c \text{ et } b \leq c - a \\ \text{Dans ce cas } c - (a + b) = (c - a) - b \end{cases}$$

$$c \leq a \text{ et } c \leq b \Rightarrow (a = b \Leftrightarrow a - c = b - c)$$

$$c \leq a \text{ et } c \leq b \Rightarrow (a \leq b \Leftrightarrow a - c \leq b - c)$$

$$c \leq a \text{ et } c \leq b \Rightarrow (a < b \Leftrightarrow a - c < b - c)$$

### Multiplication dans $\mathbb{N}$

$$\exists ! \times : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N} \quad \begin{cases} \forall n \in \mathbb{N} \quad n \times 0 = 0 \\ \forall a, b \in \mathbb{N} \quad a \times (b + 1) = (a \times b) + a \end{cases}$$

$$a \times 0 = 0$$

$$a \times 1 = a$$

$$ab = ba \quad (\times \text{ est commutative})$$

$$a(b + c) = ab + ac \quad (\times \text{ est distributive sur } +)$$

$$b \geq c \Rightarrow ab \geq ac \text{ et } a(b - c) = ab - ac \quad (\times \text{ est distributive sur } -)$$

$$(ab)c = a(bc) \quad (\times \text{ est associative})$$

$$ab = 0 \Rightarrow a = 0 \text{ ou } b = 0 \quad (\text{intégrité})$$

$$\text{Si } a = b \text{ alors } ac = bc. \text{ Réciproque fausse si } c = 0.$$

$$\text{Si } ac = bc \text{ et } c \neq 0 \text{ alors } a = b$$

$$\text{Si } a \leq b \text{ et } c \geq 0 \text{ alors } ac \leq bc. \text{ Réciproque fausse si } c = 0.$$

$$\text{Si } ac \leq bc \text{ et } c > 0 \text{ alors } a \leq b.$$

$$\text{Si } a < b \text{ et } c > 0 \text{ alors } ac < bc.$$

$$\text{Si } ac < bc \text{ et } c > 0 \text{ alors } a < b.$$

### 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  **$b$  divise  $a$  /  $a$  multiple de  $b$  /  $b|a$  /  $\frac{a}{b} \in \mathbb{N}$  ssi  $\exists q \in \mathbb{N} \quad a = qb$**

Dans ce cas  $q$  est unique, est appelé **quotient de  $a$  par  $b$**  et noté  $q = \frac{a}{b}$

Pour  $a, c \in \mathbb{N}$ , et  $b, d \in \mathbb{N}^*$  :

$$a \neq 0 \Rightarrow \frac{a}{a} \in \mathbb{N} \text{ et } \frac{a}{a} = 1$$

$$\frac{a}{1} \in \mathbb{N} \text{ et } \frac{a}{1} = a$$

$$\frac{a}{b} \in \mathbb{N} \text{ et } \frac{a}{b} = 0 \text{ ssi } a = 0$$

$$\frac{a}{b} \in \mathbb{N}, \frac{c}{d} \in \mathbb{N} \Rightarrow \frac{ac}{bd} \in \mathbb{N}, \frac{ac}{bd} = \frac{a}{b} \times \frac{c}{d}$$

$$\frac{a}{b} \in \mathbb{N}, \frac{c}{d} \in \mathbb{N} \Rightarrow \left( \frac{a}{b} = \frac{c}{d} \Leftrightarrow ad = bc \right)$$

$$\frac{a}{b} \in \mathbb{N}, \frac{c}{d} \in \mathbb{N} \Rightarrow \left( \frac{a}{b} \leq \frac{c}{d} \Leftrightarrow ad \leq bc \right)$$

$$\frac{a}{b} \in \mathbb{N}, \frac{c}{d} \in \mathbb{N} \Rightarrow \left( \frac{a}{b} < \frac{c}{d} \Leftrightarrow ad < bc \right)$$

$$\frac{a}{b} \in \mathbb{N}, \frac{c}{d} \in \mathbb{N} \Rightarrow \frac{ad+bc}{bd} \in \mathbb{N}, \frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$$

$$\frac{a}{b} \in \mathbb{N}, \frac{c}{d} \in \mathbb{N}, \frac{a}{b} \geq \frac{c}{d} \Rightarrow ad \geq bc, \frac{ad-bc}{bd} \in \mathbb{N}, \frac{a}{b} - \frac{c}{d} = \frac{ad-bc}{bd}$$

$$\frac{a}{b} \in \mathbb{N}, \frac{c}{d} \in \mathbb{N}, c \neq 0, \frac{\frac{a}{b}}{\frac{c}{d}} \in \mathbb{N} \Rightarrow \frac{ad}{bc} \in \mathbb{N}, \frac{\frac{a}{b}}{\frac{c}{d}} = \frac{ad}{bc}$$

$$\forall d \in \mathbb{N}^* \quad \forall a, b, u, v \in \mathbb{N} \quad d|u \text{ et } d|v \Rightarrow d|au + bv$$

### Caractérisation des applications entre $\llbracket 1, p \rrbracket$ et $\llbracket 1, q \rrbracket$

**Lemme.**  $\forall n \in \mathbb{N}^* \quad \forall a \in \llbracket 1, n \rrbracket \quad \exists g: \llbracket 1, n \rrbracket \setminus \{a\} \rightarrow \llbracket 1, n - 1 \rrbracket \quad g$  bijective

$$\forall p, q \in \mathbb{N}^* \quad \exists f: \llbracket 1, p \rrbracket \rightarrow \llbracket 1, q \rrbracket \text{ injective} \Leftrightarrow p \leq q$$

$$\forall p, q \in \mathbb{N}^* \quad \exists f: \llbracket 1, p \rrbracket \rightarrow \llbracket 1, q \rrbracket \text{ surjective} \Leftrightarrow p \geq q$$

$$\forall p, q \in \mathbb{N}^* \quad \exists f: \llbracket 1, p \rrbracket \rightarrow \llbracket 1, q \rrbracket \text{ bijective} \Leftrightarrow p = q$$

$$\forall n \in \mathbb{N}^* \quad \forall f: \llbracket 1, n \rrbracket \rightarrow \llbracket 1, n \rrbracket, \quad f \text{ injective ssi } f \text{ surjective ssi } f \text{ bijective.}$$

### Ensembles finis et cardinaux.

Un ensemble  $E$  est fini ssi ( $E$  est vide ou il existe une bijection de  $\llbracket 1, n \rrbracket \rightarrow E$  avec  $n \geq 1$ )

Un ensemble  $E$  est infini, s'il n'est pas fini.

Le cardinal de l'ensemble vide est  $\text{card}(\emptyset) = 0 \in \mathbb{N}$ .

Le cardinal d'un ensemble  $E$  fini non vide noté  $\text{card}(E)$ , est l'unique entier  $n \geq 1$ , tel qu'il existe une bijection de  $\llbracket 1, n \rrbracket \rightarrow E$ .

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  $\text{card}(E) \in \mathbb{N}$

Un ensemble  $E$  est vide ssi  $\text{card}(E) = 0$

Entre 2 ensembles finis non vides  $E, F$ , il existe une application injective ssi  $\text{card}(E) \leq \text{card}(F)$

Entre 2 ensembles finis non vides  $E, F$ , il existe une application surjective ssi  $\text{card}(E) \geq \text{card}(F)$

Entre 2 ensembles finis non vides  $E, F$ , il existe une application bijective ssi  $\text{card}(E) = \text{card}(F)$

Entre 2 ensembles finis non vides  $E, F$  de même 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 finis, soit ils sont tous deux infinis.

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  $\forall i \in \llbracket 1, n-1 \rrbracket x_i \leq x_{i+1}$

Une famille  $(x_1, \dots, x_n)$  d'entiers est **strictement croissante** ssi  $\forall i \in \llbracket 1, n-1 \rrbracket x_i < x_{i+1}$

Pour  $n \geq 1$ ,  $S_n = \{\sigma: \llbracket 1, n \rrbracket \rightarrow \llbracket 1, n \rrbracket \mid \sigma \text{ bijective}\}$

Une famille finie d'entiers peut être permutée de sorte à la rendre croissante.

$\forall n \geq 1 \forall (x_i \in \mathbb{N})_{i \in \llbracket 1, n \rrbracket} \exists \sigma \in S_n \ x \circ \sigma$  croissante.

Un ensemble fini non vide d'entiers peut être décrit par une famille strictement croissante d'entiers unique.

$\forall n \geq 1 \forall X \subseteq \mathbb{N} \mid \text{Card}(X) = n \exists! (x_i \in \mathbb{N})_{i \in \llbracket 1, n \rrbracket} \ x$  strictement croissante et  $X = x(\llbracket 1, n \rrbracket) = \{x_1, \dots, x_n\}$

Une partie d'un ensemble fini, est finie et de cardinal inférieur.  $A \subseteq E \Rightarrow \text{card}(A) \leq \text{card}(E)$

Une partie de  $\mathbb{N}$  est finie ssi elle est majorée ssi elle est bornée.

L'intersection d'ensembles finis est finie, et  $\text{card}(E \cap F) \leq \min(\text{card}(E), \text{card}(F))$

L'union d'ensembles finis est finie, et  $\text{card}(E \cup F) = (\text{card}(E) + \text{card}(F)) - \text{card}(E \cap F)$

**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  $(x_k \in E)_{k \in D \supseteq \llbracket a, b \rrbracket}$  définie au moins sur les indices  $\llbracket a, b \rrbracket$ .

$\exists! \bigotimes_{k=a}^b x_k \in E \quad \bigotimes_{k=a}^b x_k = \begin{cases} x_a = x_b \text{ si } a = b \\ (\bigotimes_{k=a}^{b-1} x_k) * x_b \text{ si } a < b \end{cases}$

$\forall m \in \llbracket a, b-1 \rrbracket \quad \bigotimes_{k=a}^b x_k = (\bigotimes_{k=a}^m x_k) * (\bigotimes_{k=m+1}^b x_k)$

$b \geq a \geq c \geq 1 \Rightarrow \bigotimes_{k=a}^b x_k = \bigotimes_{k=a-c}^{b-c} x_k$  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  $h: D \supseteq A \rightarrow E$  définie au moins sur  $A$ .

$\exists! \bigotimes_{x \in A} h(x) \in E \quad \forall f: \llbracket 1, n \rrbracket \rightarrow A \text{ bijective}, \bigotimes_{x \in A} h(x) = \bigotimes_{k=1}^n h(f(k))$ .

On a en particulier  $\bigotimes_{k \in \llbracket a, b \rrbracket} x_k = \bigotimes_{k=a}^b x_k$

**Changement de variables.** Pour une bijection  $f$  vers  $A$  on a  $\bigotimes_{x \in A} h(x) = \bigotimes_{y \in f^{-1}(A)} h(f(y))$

Pour  $h: D \supseteq A \cup B \rightarrow E$ ,  $A \cap B = \emptyset \Rightarrow \bigotimes_{x \in A \cup B} h(x) = (\bigotimes_{x \in A} h(x)) * (\bigotimes_{x \in B} h(x))$

La somme itérée dans  $\mathbb{N}$  se note  $\Sigma$ . Le produit itéré dans  $\mathbb{N}$  se note  $\Pi$ .

**Propriétés spécifiques à  $\Sigma$ .**

$$\forall \alpha \in \mathbb{N} \quad \Sigma_{x \in A} \alpha h(x) = \alpha \Sigma_{x \in A} h(x)$$

$$\forall \alpha \in \mathbb{N} \quad \Sigma_{x \in A} \alpha = \alpha \times \text{card}(A), \text{ en particulier } \Sigma_{x \in A} 1 = \text{card}(A)$$

**Combinatoire.**

**Fonction puissance.**  $\exists ! \hat{\cdot} : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N} : (a, b) \mapsto a^b = \begin{cases} 1 & \text{si } b = 0 \\ \prod_{k=1}^b a & \text{si } b \geq 1 \end{cases}$

$$\forall a, b, c \in \mathbb{N} \quad a^{b+c} = a^b \times a^c$$

**Fonction factorielle.**  $\exists ! ! : \mathbb{N} \rightarrow \mathbb{N} : n \mapsto n! = \begin{cases} 1 & \text{si } n = 0 \\ \prod_{k=1}^n k & \text{si } n \geq 1 \end{cases}$

**Arrangement.**  $\forall n \in \mathbb{N} \quad \forall k \in \llbracket 0, n \rrbracket \quad \exists ! A_n^k \in \mathbb{N} \quad A_n^k = \frac{n!}{(n-k)!} = \begin{cases} 1 & \text{si } k = 0 \\ \prod_{k=n-k+1}^n k & \text{si } 1 \leq k \leq n \\ n! & \text{si } k = n \end{cases}$

**Coefficient binomial.**  $\forall n \in \mathbb{N} \quad \forall k \in \llbracket 0, n \rrbracket \quad \exists ! C_n^k \in \mathbb{N} \quad C_n^k = \binom{n}{k} = \begin{cases} 1 & \text{si } k = 0 \\ \binom{n-1}{k-1} + \binom{n-1}{k} & \text{si } 1 \leq k < n \\ 1 & \text{si } k = n \end{cases}$

$$\forall n \in \mathbb{N} \quad \forall k \in \llbracket 0, n \rrbracket \quad \frac{A_n^k}{k!} \in \mathbb{N} \text{ et } \binom{n}{k} = \frac{A_n^k}{k!} = \frac{n!}{k!(n-k)!}$$

$$\forall n \in \mathbb{N} \quad \binom{n}{0} = \binom{n}{n} = 1$$

$$\forall n \in \mathbb{N} \quad \forall k \in \llbracket 1, n-1 \rrbracket \quad \binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$$

$$\forall n \in \mathbb{N}^* \quad \binom{n}{1} = \binom{n}{n-1} = n$$

$$\forall n \in \mathbb{N} \quad \forall k \in \llbracket 0, n \rrbracket \quad \binom{n}{k} = \binom{n}{n-k}$$

Pour 2 ensemble finis  $E, F$ , le produit cartésien  $E \times F$  est fini,  $\text{card}(E \times F) = \text{card}(E) \times \text{card}(F)$

Pour 2 ensemble finis  $E, F$ , l'ensemble des applications de  $E$  vers  $F$  càd  $F^E = F(E, F)$  est fini, et  $\text{card}(F^E) = \text{card}(F)^{\text{card}(E)}$

Pour 2 ensemble finis  $E, F$ , l'ensemble des injections de  $E$  vers  $F$  a  $A_{\text{card}(F)}^{\text{card}(E)} = \frac{\text{card}(F)!}{(\text{card}(F) - \text{card}(E))!}$

éléments si  $\text{card}(E) \leq \text{card}(F)$ , exactement  $\text{card}(E)!$  si égalité, mais 0 éléments si  $\text{card}(E) > \text{card}(F)$ .

Pour 2 ensemble finis  $E, F$ , l'ensemble des bijections de  $E$  vers  $F$  a  $\text{card}(E)!$  éléments si  $\text{card}(E) = \text{card}(F)$ , mais 0 éléments si  $\text{card}(E) \neq \text{card}(F)$ .

Pour un ensemble fini  $E$ , l'ensemble des parties de  $E$  est fini de cardinal  $\text{card}(P(E)) = 2^{\text{card}(E)}$

Pour un ensemble fini  $E$  a  $n$  éléments, l'ensemble des parties de  $E$  a  $k \in \llbracket 0, n \rrbracket$  éléments est  $\binom{n}{k}$

Pour un ensemble fini  $E$  a  $n$  éléments, l'ensemble des familles de  $E$  a  $k \in \llbracket 0, n \rrbracket$  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.