

Chapitre 7 : Entiers, ensembles finis, dénombrement

Première partie

Les entiers naturels

I Propriétés fondamentales et principe de récurrence

L'ensemble $\mathbb{N}$ des entiers naturels vérifie les trois axiomes :

Propriétés fondamentales —

- Toute partie non vide de $\mathbb{N}$ admet un plus petit élément.
- Toute partie non vide et majorée de $\mathbb{N}$ admet un plus grand élément.
- $\mathbb{N}$ n'est pas majoré : il n'y a pas de plus grand élément dans $\mathbb{N}$.

De ces propriétés découle le principe de récurrence :

Principe de récurrence simple — pour $n \in \mathbb{N}$, soit $P(n)$ une assertion.

Si on a :

$$\begin{aligned} &P(0) \text{ est vraie} \\ &\forall n \in \mathbb{N}, (P(n) \text{ vraie} \implies P(n+1) \text{ vraie}) \end{aligned}$$

alors pour tout $n \in \mathbb{N}$, $P(n)$ est vraie.

En effet, considérons l'ensemble $A = \{n \in \mathbb{N} | P(n) \text{ est fausse}\}$. A est une partie de $\mathbb{N}$. Supposons que A soit non vide. A possède alors un plus petit élément que nous noterons n_0 . Ainsi $P(n_0)$ est fausse. Puisque $P(0)$ est vraie, on a $n_0 > 0$. On en déduit alors que $P(n_0 - 1)$ est fausse également, car sinon $P(n_0)$ serait vraie. Ainsi $n_0 - 1 \in A$, et $n_0 - 1 < n_0$. Or n_0 est le plus petit élément de A , donc ceci est impossible. L'hypothèse " A est non vide" est donc fausse, ce qui montre que pour tout $n \in \mathbb{N}$, $P(n)$ est vraie.

Il existe d'autres formes de récurrence :

Récurrence double : il peut arriver pour l'hérédité qu'on ait besoin de supposer la propriété vraie aux deux rangs précédents. Dans ce cas, on utilise le principe de récurrence double :

Principe de récurrence double — Si on a :

$$\begin{aligned} &P(0) \text{ est vraie} \\ &P(1) \text{ est vraie} \\ &\forall n \in \mathbb{N}, (P(n) \text{ et } P(n+1) \text{ vraies} \implies P(n+2) \text{ vraie}) \end{aligned}$$

alors pour tout $n \in \mathbb{N}$, $P(n)$ est vraie.

Cette récurrence est un cas particulier du principe dit de récurrence forte : dans celle-ci, pour l'hérédité, on suppose vraie la propriété à tous les rangs inférieurs :

Principe de récurrence forte — Si on a :

$$\begin{aligned} &P(0) \text{ est vraie} \\ &\forall n \in \mathbb{N}, (P(0), P(1), \dots, P(n) \text{ vraies} \implies P(n+1) \text{ vraie}) \end{aligned}$$

alors pour tout $n \in \mathbb{N}$, $P(n)$ est vraie.

II Un peu d'arithmétique

1 Multiples et diviseurs

Définition — Soit $a, b \in \mathbb{N}$.

On dit que a divise b et on note $a|b$ s'il existe $c \in \mathbb{N}$ tel que $b = ac$. On dit alors aussi que b est un multiple de a .

Propriétés/Exemples :

- $\forall n \in \mathbb{N}, n|0$ car $0 = n \times 0$
- $\forall n \in \mathbb{N}, 0|n \implies n = 0$
- $\forall n \in \mathbb{N}, 1|n$ car $n = 1 \times n$
- $\forall n \in \mathbb{N}, n|1 \implies n = 1$

Exemple : L'ensemble des diviseurs de 6 est $\{1, 2, 3, 6\}$.

Exercice d'application Montrer que pour tout entier positif impair n , $n^2 - 1$ est un multiple de 8.

Propriétés — La relation de divisibilité dans $\mathbb{N}$ est réflexive, antisymétrique et transitive :

- $\forall n \in \mathbb{N}, n|n$ (réflexivité)
- $\forall n, p \in \mathbb{N}$, si $n|p$ et $p|n$, alors $n = p$ (antisymétrie)
- $\forall n, p, q \in \mathbb{N}$, si $n|p$ et $p|q$ alors $n|q$ (transitivité)

Preuve :

1. Soit $a \in \mathbb{N}$, $a = a \times 1$ donc $a|a$: est réflexive.
2. Soit $a, b \in \mathbb{N}$. On suppose $a|b$ et $b|a$. Alors il existe $c \in \mathbb{N}$ tel que $b = ac$ et il existe $k \in \mathbb{N}$ tel que $a = kb$.
Alors $b = kcb$ donc $b = 0$ ou $kc = 1$.
 - Si $b = 0$ alors $a = 0$ car $b|a$. On a bien $a = b$.
 - Si $kc = 1$: $k, c \in \mathbb{N}$ donc $k = c = 1$ alors $b = a$.
 Dans les deux cas, on a prouvé que $a = b$: la relation de divisibilité est bien antisymétrique.
3. Soit $a, b, c \in \mathbb{N}$. On suppose $a|b$ et $b|c$. Alors il existe $k, \ell \in \mathbb{N}$ tels que $b = ka$ et $c = b\ell$. On a donc $c = ka\ell = (k\ell)a$ donc, comme $k\ell \in \mathbb{N}$, $a|c$, ce qui montre que la relation de divisibilité est transitive.

Proposition — Soit $a, b, c \in \mathbb{N}$. On suppose que $a|b$ et $a|c$. Alors pour tous $u, v \in \mathbb{N}$, $a|(bu + cv)$.

Preuve : Il existe $k, \ell \in \mathbb{N}$ tels que $b = ak$ et $c = a\ell$ alors $bu + cv = aku + a\ell v = a(ku + \ell v)$. Or comme $(ku + \ell v) \in \mathbb{N}$, alors $a|(bu + cv)$

Proposition — Soit $a, b \in \mathbb{N}$ et $b \neq 0$. Si $a|b$ alors $a \leq b$.

Preuve : Supposons $a|b$: alors il existe $c \in \mathbb{N}$, tel que $b = ac$, comme $b \neq 0$ alors $c \neq 0$, donc $c \geq 1$ donc $b \geq a$ (car $a \geq 0$!)

2 Division euclidienne

Théorème — Soit $a \in \mathbb{N}, b \in \mathbb{N}^*$. Alors il existe un unique couple $(q, r) \in \mathbb{N}^2$ vérifiant

$$a = bq + r \text{ et } 0 \leq r < b$$

C'est la division euclidienne de a par b , q étant le quotient et r le reste.

Preuve :

- **Unicité :** Supposons qu'il existe (q_1, r_1) et (q_2, r_2) vérifiant $a = bq_1 + r_1$ et $0 \leq r_1 < b$ et $a = bq_2 + r_2$ et $0 \leq r_2 < b$. Alors $0 = b(q_1 - q_2) + r_1 - r_2$, ou encore $r_1 - r_2 = b(q_2 - q_1)$. $q_1, q_2 \in \mathbb{N}$ donc $q_1 - q_2 \in \mathbb{Z}$. Donc $r_2 - r_1$ est donc un multiple de b . Or $-b < r_2 - r_1 < b$. Entre $-b$ et b exclus, il y a une unique multiple de b : 0. Donc $r_2 - r_1 = 0$ d'où $r_2 = r_1$. Ainsi $0 = b(q_1 - q_2)$ et comme $b \neq 0$ alors $q_1 - q_2 = 0$ i.e. $q_1 = q_2$. Ce qui prouve l'unicité d'un tel couple s'il existe.

- **Existence** : On considère $A = \{n \in \mathbb{N} \mid a - nb \geq 0\}$.

A est une partie de $\mathbb{N}$

- **non vide** : puisque $a \in \mathbb{N}$, alors $a - 0 \times b = a \geq 0$, ce qui montre que $0 \in A$.
- **majorée** : soit $n \in A$. Alors $a - nb \geq 0$, donc $nb \leq a$. Or, $b \neq 0$, donc $b \geq 1$. Ainsi, $n \leq nb$, donc $n \leq a$, ce qui montre que a est un majorant de A .

La partie A admet donc un plus grand élément : notons q ce plus grand élément, et posons $r = a - bq$. q et r sont alors deux entiers naturels. Supposons $r \geq b$. Alors $r - b \geq 0$. Or, $r - b = a - b(q + 1)$, ce qui montre que $q + 1 \in A$, ce qui contredit le fait que q est le plus grand élément de A . Ainsi, $r < b$.

On a donc montré l'existence de deux entiers naturels q et r tels que $a = bq + r$ et $0 \leq r < b$.

La démonstration donne un moyen d'obtenir le quotient et le reste : on soustrait successivement b de a tant que le résultat reste positif : le nombre de soustraction effectuées est le quotient, le nombre obtenu au final est le reste.

Exemple Division euclidienne de 27 par 7. On a $27 = 3 \times 7 + 6$ et $0 \leq 6 < 7$. Le nombre 27 est appelé le **dividende** de cette division euclidienne, 7 le **diviseur**, 3 est le quotient et 6 le reste.

3 Nombres premiers

Définition — Un entier naturel est dit premier s'il a **exactement** deux diviseurs : 1 et lui-même.
Attention! 1 n'est pas un nombre premier.

Théorème — Tout entier naturel, supérieur ou égal à 2, possède au moins un diviseur premier.

Preuve : On procède par récurrence forte. Pour $n \in \mathbb{N}$, notons H_n l'assertion " n possède un diviseur premier".

L'assertion H_2 est vraie car $2|2$ et 2 est premier.

Soit $n \geq 2$ un entier naturel. Supposons vraies les assertions H_k pour $k \in \llbracket 2; n \rrbracket$. Montrons que H_{n+1} est vraie : c'est bien sûr le cas si $n + 1$ est un nombre premier. Si maintenant, $n + 1$ n'est pas premier, il possède alors un diviseur d autre que 1 et lui-même; on peut donc écrire $n + 1 = d \times k$ et puisque $d \neq 1$ et $d \neq n + 1$, alors on a $2 \leq d \leq n$: l'assertion H_d est donc vraie par hypothèse, et d possède donc un diviseur premier que nous noterons p . p est alors aussi un diviseur premier de $n + 1$ ce qui montre que H_{n+1} est également vraie dans ce cas.

Par récurrence forte, l'assertion H_n est donc vraie pour tout $n \geq 2$.

Remarque — Tout entier n supérieur ou égal à 2 non premier possède un diviseur premier p tel que $p \leq \sqrt{n}$.

Preuve : Soit $n \in \mathbb{N}, n \geq 2$. Notons D l'ensemble de diviseurs premiers de n . D est une partie non vide de $\mathbb{N}$, donc admet un plus petit élément, noté p . n n'étant pas premier, $p < n$, et puisque $p|n$, alors il existe $k \in \mathbb{N}$ tel que $pk = n$. Puisque $p < n$, alors $k \geq 2$, donc k admet des diviseurs premiers, et k étant un diviseur de n , ses diviseurs premiers sont des diviseurs premiers de n . Si $k < p$, alors les diviseurs premiers de k sont inférieurs à p , ce qui contredit que p est le plus petit diviseur premier de n . Ainsi, $k \geq p$, et par conséquent, $pk \geq p^2$, c'est-à-dire $n \geq p^2$.

Crible d'Ératosthène —

Le crible d'Ératosthène permet d'obtenir les nombres premiers inférieurs à un entier N^2 donné :

- on écrit tous les entiers de 2 à N^2 dans un tableau de N lignes et N colonnes (en laissant la première case vide).

On parcourt ensuite la première ligne :

- le premier entier de cette ligne (c'est 2) est premier : on le conserve, et on raye tous ses multiples (autres que lui-même bien sûr) ;
- on recommence avec le premier entier non rayé suivant (c'est 3) : on le conserve, et on raye tous ses multiples ;
- on recommence avec le premier entier non rayé suivant (c'est 5) : on le conserve, et on raye tous ses multiples ;
- etc.
- arrivé au bout de la première ligne, tous les entiers figurant encore dans le tableau (ceux qui n'ont pas été rayés) sont premiers.

Exemple : mettre cet algorithme en œuvre pour trouver tous les nombres premiers inférieurs à 100.

	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Voici ce que vous devez obtenir :

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97

Théorème — L'ensemble des nombres premiers est infini.

Preuve : Par l'absurde.

Supposons qu'il y ait un nombre fini N de nombre premiers : $p_1, p_2, \dots, p_N$. Considérons $A = 1 + p_1 \times p_2 \times \dots \times p_N$. $A \in \mathbb{N}$ et $A \geq 2$ car $\forall i \in \{1, 2, \dots, N\}, p_i \geq 1$, donc A possède un diviseur premier. Quitte à renuméroter les p_i , supposons $p_1 | A$, or $p_1 | p_1 \times p_2 \times \dots \times p_N$.

Alors $p_1 | (A - p_1 \times p_2 \times \dots \times p_N)$ i.e $p_1 | 1$, ce qui absurde car $p_1 \neq 1$. Il y a donc une infinité de nombres premiers.

Théorème — Tout entier naturel supérieur ou égal à 2 peut s'écrire comme un produit de nombres premiers :

$$n = p_1 p_2 \dots p_N$$

avec $p_1, p_2, \dots, p_N$ premiers. L'écriture est unique, à l'ordre des facteurs près.

En regroupant les facteurs premiers identiques :

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_S^{\alpha_S}$$

avec $p_1, p_2, \dots, p_S$ premiers et 2 à 2 distincts et $\alpha_1, \alpha_2, \dots, \alpha_S \in \mathbb{N}^*$

Exemple : Déterminer la décomposition de 1848 en produit de facteurs premiers.

• 1848 est divisible par 8 (car 848 est un multiple de 8), et $1848 = 8 \times 231$. 231 est divisible par 3 : $231 = 3 \times 77 = 3 \times 7 \times 11$. Finalement $1848 = 2^3 \times 3 \times 7 \times 11$.

Exercice d'application Déterminer la décomposition en facteurs premiers de $n = 277\,200$.

4 PGCD

Définition — Soit $a, b \in \mathbb{N}$ tel que $(a, b) \neq (0, 0)$.

On appelle PGCD de a et de b le plus grand commun diviseur de a et b . On le note $\text{pgcd}(a, b)$.

Remarques :

- Si $(a, b) \neq (0, 0)$, l'ensemble des diviseurs communs de a et b est une partie de $\mathbb{N}$, non vide car $1|a$ et $1|b$ donc elle contient 1. Cette partie est de plus majorée : si d est un diviseur commun à a et b alors $d \leq a$ ou $d \leq b$ car a ou b est non nul.
Le pgcd de a et de b est donc correctement défini.
- Si $a = 0$, $\text{pgcd}(0, b) = b$ car $\forall n \in \mathbb{N}, n|0$ et le plus grand diviseur de b est b .

Convention — On convient que $\text{pgcd}(0, 0) = 0$.

Exemples :

- Trouver $\text{pgcd}(18, 48)$.
Les diviseurs de 18 sont : 1, 2, 3, 6, 9, 18 et ceux de 48 : 1, 2, 3, 4, 6, 8, 12, 16, 24, 48.
Donc $\text{pgcd}(18, 48) = 6$

- Trouver $\text{pgcd}(1848, 2016)$

$$1848 = 2^3 \times 3 \times 7 \times 11 \text{ et } 2016 = 2^5 \times 3^2 \times 7.$$

Les diviseurs communs à 1848 et 2016 s'écrivent : $2^a \times 3^b \times 7^c$ où $a \in \{0, 1, 2, 3\}$ et $b, c \in \{0, 1\}$. Le plus grand est $2^2 \times 3 \times 7 = 168$ d'où $\text{pgcd}(1848, 2016) = 168$

Déterminer le PGCD à l'aide de la décomposition en produit de facteurs premiers

On écrit la décomposition en produit de facteurs premiers de a et b :

$$a = p_1^{\alpha_1} \times p_2^{\alpha_2} \times \dots \times p_N^{\alpha_N}$$

$$b = p_1^{\beta_1} \times p_2^{\beta_2} \times \dots \times p_N^{\beta_N}$$

où $p_1, \dots, p_N$ sont premiers et $\alpha_i, \beta_i \in \mathbb{N}$. Alors $d = \text{pgcd}(a, b)$ a pour décomposition

$$d = p_1^{\delta_1} \times p_2^{\delta_2} \times \dots \times p_N^{\delta_N}$$

où $\delta_i = \min(\alpha_i, \beta_i)$.

Exercice d'application Déterminer PGCD(360, 336).

Théorème — Soit $a, b \in \mathbb{N}^*$. Soit r le reste de la division euclidienne de a par b . Alors $\text{pgcd}(a, b) = \text{pgcd}(b, r)$.

Preuve : Notons q le quotient de la division euclidienne de a par b :

$$a = bq + r \quad 0 \leq r < b$$

Soit d un diviseur commun à a et b . Alors $d|a$ et $d|b$, donc $d|(a - bq)$ i.e. $d|r$. Ainsi d est un diviseur commun à b et r . On a montré $\{\text{diviseurs communs de } a \text{ et } b\} \subset \{\text{diviseurs communs de } b \text{ et } r\}$, donc $\text{pgcd}(a, b) \leq \text{pgcd}(b, r)$.

Soit d un diviseur commun à b et r , alors $d|b$ et $d|r$ donc $d|(bq + r)$ i.e. $d|a$, donc d est un diviseur commun à a et b . Ainsi $\{\text{diviseurs communs de } b \text{ et } r\} \subset \{\text{diviseurs communs de } a \text{ et } b\}$ donc $\text{pgcd}(b, r) \leq \text{pgcd}(a, b)$

Finalement, $\text{pgcd}(a, b) = \text{pgcd}(b, r)$.

Ce résultat est à la base de l'**algorithme d'Euclide** pour le calcul du pgcd : on effectue la division euclidienne de a par b ; si le reste r est nul, alors $b|a$, donc $\text{pgcd}(a, b) = b$. Si le reste est non nul, on recommence avec b et r , etc. Le dernier reste non nul donne alors le pgcd de a et b .

Entrée : a, b .

Tant que $b > 0$, faire :

$r \leftarrow$ reste de la division euclidienne de a par b

$a \leftarrow b$

$b \leftarrow r$

Sortie : a

Exemple :

Calculer $\text{PGCD}(306, 758)$.

On a, avec l'algorithme d'Euclide

$$\begin{array}{rcl} 758 & = & 306 \times 2 + 146 \\ \text{puis } 306 & = & 146 \times 2 + 14 \\ \text{puis } 146 & = & 14 \times 10 + 6 \\ \text{puis } 14 & = & 6 \times 2 + 2 \\ \text{puis } 6 & = & 2 \times 3 + 0 \end{array}$$

Finalement, $\text{PGCD}(a, b)$ est le dernier reste non nul, à savoir 2.

5 PPCM

Définition — Soit $a, b \in \mathbb{N}^*$. On appelle PPCM de a et b , et on note $\text{ppcm}(a, b)$, le plus petit multiple non nul, commun à a et b .

Remarque : L'ensemble des multiples communs non nuls à a et b est une partie de $\mathbb{N}$, non vide car ab est un multiple de a et b non nul. Donc cette partie admet un plus petit élément : la définition est correcte.

Convention — Si a ou b est nul : on convient que $\text{ppcm}(a, b) = 0$.

Exemples : $\text{ppcm}(18, 48)$. Les multiples non nuls de 18 : 18, 36, 54, 72, 90, 108, 126, **144**, ... et ceux de 48 sont : 48, 96, **144**, Ainsi $\text{ppcm}(18, 48) = 144$.

Déterminer le PPCM à l'aide de la décomposition en produit de facteurs premiers

On écrit la décomposition en produit de facteurs premiers de a et b :

$$\begin{aligned} a &= p_1^{\alpha_1} \times p_2^{\alpha_2} \times \dots \times p_N^{\alpha_N} \\ b &= p_1^{\beta_1} \times p_2^{\beta_2} \times \dots \times p_N^{\beta_N} \end{aligned}$$

où $p_1, \dots, p_N$ sont premiers et $\alpha_i, \beta_i \in \mathbb{N}$. Alors $m = \text{ppcm}(a, b)$ a pour décomposition

$$m = p_1^{\mu_1} \times p_2^{\mu_2} \times \dots \times p_N^{\mu_N}$$

où $\mu_i = \max(\alpha_i, \beta_i)$.

Exemple : $1848 = 2^3 \times 3 \times 7 \times 11$ et $2016 = 2^5 \times 3^2 \times 7$ donc $\text{ppcm}(1848, 2016) = 2^5 \times 3^2 \times 7 \times 11$.

Exercice d'application Déterminer $\text{PPCM}(360, 336)$.

Proposition — Soit $a, b \in \mathbb{N}$. Alors $\text{ppcm}(a, b) \times \text{pgcd}(a, b) = ab$.

Exemple : Déterminer $\text{PPCM}(132, 72)$.

Commençons par déterminer $\text{PGCD}(132, 72)$. On a

$$\begin{array}{rcl} 132 & = & 72 \times 1 + 60 \\ \text{puis } 72 & = & 60 \times 1 + 12 \\ \text{puis } 60 & = & 12 \times 5 + 0 \end{array}$$

donc $\text{PGCD}(132, 72) = 12$. On en déduit

$$\text{PPCM}(132, 72) = \frac{132 \times 72}{12} = 132 \times 6 = 792.$$

Exercice d'application Calculer $A = \frac{11}{360} - \frac{5}{336}$.

Solution. Puisque $\text{PPCM}(360, 336) = 5040 = 2^4 \cdot 3^2 \cdot 5 \cdot 7$, on calcule :

$$A = \frac{11}{2^3 \cdot 3^2 \cdot 5} - \frac{5}{2^4 \cdot 3 \cdot 7} = \frac{11 \cdot 2 \cdot 7}{2^4 \cdot 3^2 \cdot 5 \cdot 7} - \frac{5^2 \cdot 3}{2^4 \cdot 3^2 \cdot 5 \cdot 7} = \frac{154 - 75}{2^4 \cdot 3^2 \cdot 5 \cdot 7} = \frac{79}{2^4 \cdot 3^2 \cdot 5 \cdot 7}.$$

Deuxième partie

Ensembles finis

I Ensemble fini, cardinal

Définition — Un ensemble E non vide est dit fini s'il existe un entier $n \in \mathbb{N}^*$ et une bijection de $\llbracket 1; n \rrbracket$ sur E . L'entier n est alors unique : c'est le **cardinal** de E , noté $\text{Card}(E)$.

Remarque : On trouve aussi les notations $\text{Card}(E) = |E| = \#E$. $\text{Card}(E)$ est bien sûr le nombre d'éléments de E . Par convention, l'ensemble vide est fini, de cardinal nul.

Exemples

- $\text{Card}(\{\emptyset, \{\emptyset\}, \{\emptyset, \emptyset\}, \{\emptyset, \{\emptyset\}\}\} = 4$.
- Soit $a, b \in \mathbb{Z}$ avec $a \leq b$. Alors $\llbracket a; b \rrbracket$ est fini de cardinal $b - a + 1$.
(prendre $\varphi: k \in \llbracket 1; b - a + 1 \rrbracket \mapsto k + a - 1$)
- Soit n un entier naturel non nul, et $\mathbb{U}_n$ l'ensemble des racines n -ième de l'unité.

Alors l'application $\varphi: \llbracket 1; n \rrbracket \longrightarrow \mathbb{U}_n$
 $k \longmapsto e^{i \frac{2(k-1)\pi}{n}}$ est bijective, donc $\mathbb{U}_n$ est fini de cardinal n .

Proposition — Soit E un ensemble fini et A une partie de E . Alors A est finie et $\text{Card}(A) \leq \text{Card}(E)$. De plus, $\text{Card}(A) = \text{Card}(E)$ si et seulement si $A = E$.

Remarque : Ainsi, si E et F sont deux ensembles finis de même cardinal, il suffit de prouver une inclusion pour avoir l'égalité.

II Applications entre ensembles finis

Proposition — Soit E, F deux ensembles finis et f une application de E dans F . Alors :

- si f est injective, alors $\text{Card}(E) \leq \text{Card}(F)$;
- si f est surjective, alors $\text{Card}(E) \geq \text{Card}(F)$;
- si f est bijective, alors $\text{Card}(E) = \text{Card}(F)$.

Petit travail à faire : illustrer cette proposition avec des diagrammes de Venn (quand on représente les ensembles par des patates). Donner des exemples montrant que les réciproques sont fausses.

Conséquence

Une application $f: E \longrightarrow F$ entre deux ensembles finis E et F tels que $\text{Card}(F) < \text{Card}(E)$ ne peut pas être injective : il existe donc nécessairement deux éléments qui ont la même image. C'est ce qu'on appelle le

Principe des tiroirs —

Si on range p chaussettes dans n tiroirs et qu'il y a strictement plus de chaussettes que de tiroirs ($p > n$), alors il y a un tiroir qui contient au moins deux chaussettes.

Exemples

1. Étant donné trois entiers, il y a en au moins deux de même parité (trois entiers à ranger dans deux tiroirs : celui des entiers pairs, et celui des impairs).
2. Soit n un entier naturel non nul. On considère un ensemble de $n + 1$ entiers choisis parmi $1, 2, 3, \dots, 2n$. Alors il existe deux entiers de cet ensemble dont la somme vaut $2n + 1$.
(exemple avec $n=5$: choisissez 6 entiers (distincts!) entre 1 et 10 ; il y en a deux dont la somme vaut 11)

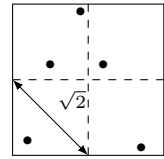
Preuve : avec les entiers compris entre 1 et $2n$, on peut former n tiroirs : ce sont les paires d'entiers dont la somme vaut $2n + 1 =$ les paires $\{1, 2n\}, \{2, 2n - 1\}, \dots, \{n, n + 1\}$. Si on range nos $n + 1$ entiers dans ces tiroirs, il y a un tiroir qui en contient deux (et comme ils sont distincts...)

3. Montrer que, parmi les Lorrains chevelus, il en existe au moins deux avec exactement le même nombre de cheveux. On considérera qu'un individu possède au plus 300 000 cheveux, et qu'il y a environ 2 300 000 d'habitants en Lorraine.

Solution. On considère 300 000 tiroirs, qui correspondent respectivement à 1 cheveux, 2 cheveux, etc. On place chaque Lorrain dans le tiroir correspondant à son nombre de cheveux sur la tête. Le principe des tiroirs assure alors qu'il y a au moins deux personnes ayant exactement le même nombre de cheveux sur la tête en Lorraine !

4. Etant donné cinq points dans un carré d'arête 2, montrer qu'on peut toujours en trouver deux distants d'au plus $\sqrt{2}$.

Solution. Coupons simplement notre carré en quatre carrés comme indiqué ci-contre, et prenons les quatre sous-carrés ainsi formés pour « tiroirs ». On doit ranger cinq points quelconques dans quatre tiroirs, nous sommes donc forcés d'en ranger deux dans le même tiroir. Au pire, ces points sont alors distants de $\sqrt{2}$, qui est la longueur de la diagonale de chaque sous-carré.



Proposition — Soit E et F deux ensembles finis non vides, et $f: E \rightarrow F$ une application. Alors :

- $\text{Card}(f(E)) \leq \text{Card}(F)$ avec égalité si et seulement si f est surjective ;
- $\text{Card}(f(E)) \leq \text{Card}(E)$ avec égalité si et seulement si f est injective.

Preuve : $f(E)$ est une partie de F , donc $f(E)$ est fini, et cardinal $\text{Card}(f(E)) \leq \text{Card}(F)$. Il y a égalité si et seulement si $f(E) = F$ ce qui équivaut à f surjective.

Notons $n = \text{Card}(E)$ et $e_1, \dots, e_n$ les éléments de E . Alors $f(E) = \{f(e_1), \dots, f(e_n)\}$ possède au plus n éléments, donc $\text{Card}(f(E)) \leq \text{Card}(E)$, avec égalité si et seulement si les $f(e_i)$ sont tous deux à deux distincts, ce qui équivaut à f injective.

Corollaire — Soit E et F deux ensembles finis non vides, de même cardinal : $\text{Card}(E) = \text{Card}(F)$.

Soit $f: E \rightarrow F$ une application. Alors les propositions suivantes sont équivalentes :

- f est injective ;
- f est surjective ;
- f est bijective.

Preuve : Supposons f injective. D'après la proposition précédente, $\text{Card}(f(E)) = \text{Card}(E)$. Or $\text{Card}(E) = \text{Card}(F)$, donc $\text{Card}(f(E)) = \text{Card}(F)$, ce qui montre que f est surjective.

Supposons f surjective. Alors $\text{Card}(f(E)) = \text{Card}(F)$, donc $\text{Card}(f(E)) = \text{Card}(E)$ puisque $\text{Card}(E) = \text{Card}(F)$. f est donc injective, donc bijective.

Supposons f bijective. Alors f est injective.

On a donc la chaîne d'implication : f injective $\implies f$ surjective $\implies f$ bijective $\implies f$ injective, ce qui montre l'équivalence des propositions.

III Opérations sur les cardinaux

Théorème — Soit E un ensemble, et A et B deux parties finies de E . Si A et B sont disjointes (i.e. $A \cap B = \emptyset$), alors $A \cup B$ est fini, de cardinal $\text{Card}(A \cup B) = \text{Card}(A) + \text{Card}(B)$.

Preuve : Notons $n = \text{Card}(A)$ et $p = \text{Card}(B)$. Il existe deux bijections $\varphi: A \rightarrow \llbracket 1; n \rrbracket$ et $\psi: B \rightarrow \llbracket 1; p \rrbracket$. Considérons l'application $f: A \cup B \rightarrow \llbracket 1; n + p \rrbracket$ définie par

$$f(x) = \begin{cases} \varphi(x) & \text{si } x \in A \\ n + \psi(x) & \text{si } x \in B \end{cases}$$

On peut vérifier facilement que f est bijective, ce qui prouve que $A \cup B$ est de cardinal $n + p$.

On en déduit :

Théorème — Soit E un ensemble, et A et B deux parties finies de E . Alors $A \setminus B$ et $A \cup B$ sont finis de cardinal

$$\text{Card}(A \setminus B) = \text{Card}(A) - \text{Card}(A \cap B)$$

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

En particulier, si E est fini, alors $\complement A$ est fini de cardinal $\text{Card}(\complement A) = \text{Card}(E) - \text{Card}(A)$.

Preuve : A est la réunion disjointe de $A \cap B$ et $A \setminus B$, donc, d'après le théorème précédent, $\text{Card}(A) = \text{Card}(A \cap B) + \text{Card}(A \setminus B)$, d'où l'on tire $\text{Card}(A \setminus B) = \text{Card}(A) - \text{Card}(A \cap B)$.

Ensuite, on remarque que $A \cup B$ est la réunion disjointe de $A \setminus B$ et B . Ainsi, $\text{Card}(A \cup B) = \text{Card}(A \setminus B) + \text{Card}(B) = \text{Card}(A) + \text{Card}(B) - \text{Card}(A \cap B)$.

Plus généralement :

Théorème — Si $A_1, A_2, \dots, A_n$ sont des ensembles finis deux à deux disjoints, alors $\bigcup_{k=1}^n A_k$ est fini de cardinal :

$$\text{Card}\left(\bigcup_{k=1}^n A_k\right) = \sum_{k=1}^n \text{Card}(A_k)$$

Exemple Déterminer le nombre d'entiers compris entre 1 et 1000 dont la somme des chiffres vaut 3.

On va représenter un entier entre 1 et 999 par un triplet (a, b, c) où a est le chiffre des centaines, b celui des dizaines et c celui des unités. On cherche donc le nombre de triplets (a, b, c) d'entiers de $\llbracket 0; 9 \rrbracket$ tels que $a + b + c = 3$.

Notons $E = \{(a, b, c) \in \llbracket 0; 9 \rrbracket^3 \mid a + b + c = 3\}$. Distinguons suivant la valeur prise par a : a peut valoir au maximum 3, ainsi $E = A_0 \cup A_1 \cup A_2 \cup A_3$, où :

$$A_0 = \{(0, b, c) \mid b + c = 3\} \quad A_1 = \{(1, b, c) \mid b + c = 2\} \quad A_2 = \{(2, b, c) \mid b + c = 1\} \quad A_3 = \{(3, b, c) \mid b + c = 0\}$$

et les A_i sont clairement deux à deux disjoints. On a donc :

$$\text{Card}(E) = \sum_{k=0}^3 \text{Card}(A_k) = 4 + 3 + 2 + 1 = 10$$

Il y a 10 entiers compris entre 1 et 1000 dont la somme des chiffres vaut 3.

Théorème — Soit E et F deux ensembles finis non vides. Alors $E \times F$ est fini de cardinal

$$\text{Card}(E \times F) = \text{Card}(E) \times \text{Card}(F)$$

Preuve : Notons $n = \text{Card}(E)$ et $e_1, \dots, e_n$ les éléments de E : les e_i sont deux à deux distincts.

Remarquons que $E \times F = \bigcup_{i=1}^n (\{e_i\} \times F)$. Puisque pour $i, j \in \llbracket 1; n \rrbracket$ avec $i \neq j$, $e_i \neq e_j$, alors $\{e_i\} \times F \cap \{e_j\} \times F = \emptyset$.

Ainsi, $\text{Card}(E \times F) = \sum_{i=1}^n \text{Card}(\{e_i\} \times F)$.

Or l'application $\varphi: \{e_i\} \times F \rightarrow F$ qui à un élément x de F associe le couple (e_i, x) est clairement bijective, donc $\text{Card}(\{e_i\} \times F) = \text{Card}(F)$. Finalement, $\text{Card}(E \times F) = \sum_{i=1}^n \text{Card}(F) = \text{Card } E \times \text{Card}(F)$.

Plus généralement :

Théorème — Si $E_1, \dots, E_n$ sont des ensembles finis, alors $E_1 \times E_2 \times \dots \times E_n$ est fini de cardinal

$$\text{Card}(E_1) \times \text{Card}(E_2) \times \dots \times \text{Card}(E_n)$$

Troisième partie

Dénombrement

I Principes pour dénombrer

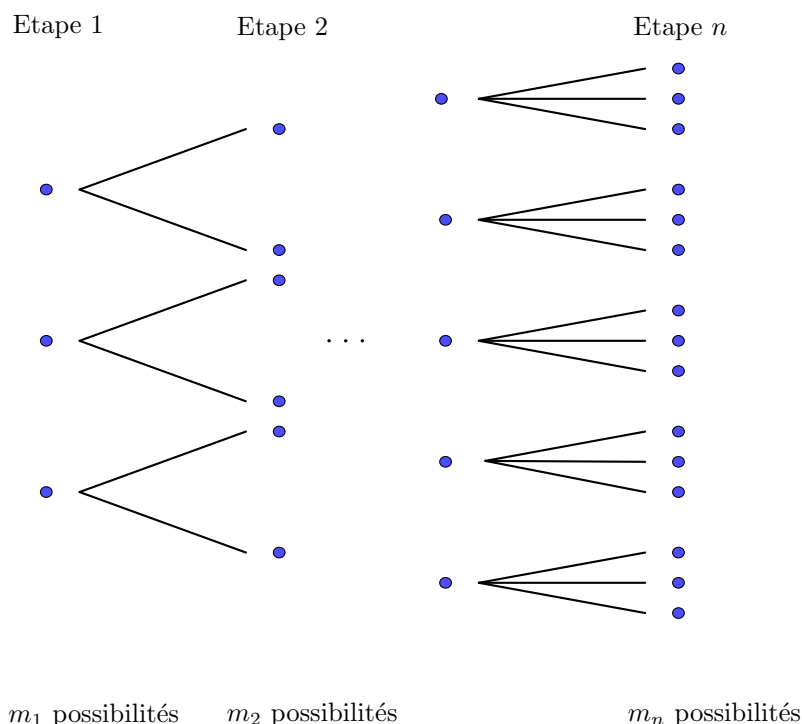
— Dénombrer, c'est déterminer le cardinal d'un ensemble. Il y a deux grands principes pour dénombrer :

- **Le principe de disjonction :**

si les éléments de l'ensemble E sont du type A **ou** du type B et qu'ils ne peuvent être à la fois du type A et du type B , alors le cardinal de E est égal à la **somme** du cardinal de l'ensemble des éléments de type A et du cardinal de l'ensemble des éléments du type B .

- **Le principe multiplicatif :**

si on cherche à dénombrer des objets construits en plusieurs étapes, on peut représenter ces objets comme les différentes branches d'un arbre simple :



s'il y a n étapes, et qu'à l'étape k , il y a m_k possibilités (m_k branches), alors le nombre total d'objet est $m_1 \times m_2 \times \dots \times m_n$.

Exemples de dénombrement

- **Combien y a-t-il de codes de 3 symboles commençant par 2 chiffres et se terminant par une lettre ?**

Un tel code est construit par étapes :

- choix d'un premier chiffre : 10 possibilités (c'est le nombre de chiffres entre 0 et 9) ;
- choix d'un deuxième chiffre : 10 possibilités ;
- choix d'une lettre : 26 possibilités.

Il y a donc $10 \times 10 \times 26$ codes possibles.

- **Combien y a-t-il de codes de trois chiffres deux à deux distincts ?**

Un tel code est construit par étapes :

- choix d'un premier chiffre : 10 possibilités ;
- choix d'un deuxième chiffre : 9 possibilités (car distinct du premier) ;
- choix d'un troisième chiffre : 8 possibilités (car distinct des deux premiers).

Il y a donc $10 \times 9 \times 8$ codes possibles.

• **Combien y a-t-il de codes de trois chiffres comportant au moins deux chiffres pairs ?**

Ces codes sont de deux types : ceux contenant exactement deux chiffres pairs (type 1), et ceux contenant exactement trois chiffres pairs (type 2).

Les codes du type 1 sont décrits par étapes :

- choix de la place du chiffre impair : 3 possibilités ;
- choix du chiffre impair : 5 possibilités ;
- choix du premier chiffre pair : 5 possibilités ;
- choix du deuxième chiffre pair : 5 possibilités.

Il y a donc 3×5^3 codes du type 1.

Les codes du type 2 sont eux aussi décrits par étape, chacune consistant à choisir un chiffre pair et comportant 5 possibilités ; il y a donc 5^3 codes du type 2.

Finalement, puisqu'il ne peut y avoir des codes de type 1 et 2 à la fois, il y a $3 \times 5^3 + 5^3$ codes de trois chiffres comportant au moins deux chiffres pairs.

Remarque : Il est parfois plus simple de dénombrer le complémentaire d'un ensemble plutôt que l'ensemble lui-même : on utilise alors la formule $\text{Card}(E \setminus A) = \text{Card}(E) - \text{Card}(A)$ valable si $A \subset E$.

Exemple : Dénombrer les codes de trois chiffres comportant au moins un chiffre pair.

Le complémentaire est formé par les codes ne comportant aucun chiffre pair, c'est-à-dire les codes de trois chiffres impairs. Un tel code est construit par étapes :

- choix d'un premier chiffre impair : 5 possibilités ;
- choix d'un deuxième chiffre impair : 5 possibilités ;
- choix d'un troisième chiffre impair : 5 possibilités.

Il y a donc 5^3 codes ne comportant aucun chiffre pair. De même, on dénombre 10^3 codes de trois chiffres. Ainsi, il y a $10^3 - 5^3$ codes de trois chiffres comportant au moins un chiffre pair.

D'autres exemples :

• **Soit $n \in \mathbb{N}^*$. Dans une salle ayant n places, de combien de manières peut-on placer n élèves ?**

Imaginons (artificiellement) que les élèves arrivent l'un après l'autre (ce qui revient à les numéroté). Le placement peut être décrit par les étapes suivantes :

- choix de la place pour le premier élève : n possibilités ;
- choix de la place pour le deuxième élève : $n - 1$ possibilités (il n'y a plus que $n - 1$ places libres) ;
- choix de la place pour le troisième élève : $n - 2$ possibilités ;
- $\vdots$
- choix de la place pour l'avant-dernier élève : 2 possibilités ;
- choix de la place pour le dernier élève : 1 possibilité.

Au total, il y a donc $n!$ placements possibles.

On a utilisé le principe multiplicatif en numérotant artificiellement les élèves ; on aurait pu également raisonner sur les tables et non sur les élèves :

- choix de l'élève pour la première table : n possibilités ;
- choix de l'élève pour la deuxième table : $n - 1$ possibilités ;
- $\vdots$
- choix de l'élève pour l'avant-dernière table : 2 possibilités ;
- choix de l'élève pour la dernière table : 1 possibilité.

• **Dans une classe de 47 places, de combien de manières peut-on placer 41 élèves ?**

Raisonnons sur les élèves que l'on numérote artificiellement :

- choix de la table pour le premier élève : 47 possibilités ;
- choix de la table pour le deuxième élève : 46 possibilités ;
- $\vdots$
- choix de la table pour l'avant-dernier élève : 8 possibilités ;
- choix de la table pour le dernier élève : 7 possibilités.

Il y a donc $47 \times 46 \times \cdots \times 8 \times 7 = \frac{47!}{6!}$ façons de placer les élèves.

Aurait-on pu ici raisonner sur les tables ?

C'est possible, mais il faut commencer par choisir les 6 tables qui resteront inoccupées : appelons x le nombre de façons de choisir 6 tables parmi 47.

Le nombre de manières de placer les 41 élèves dans la salle est décrit par les étapes :

- choix des 6 places inoccupées : x possibilités ;
- choix de l'élève pour la première table non vide : 41 possibilités ;
- choix de l'élève pour la deuxième table non vide : 40 possibilités ;
- $\vdots$
- choix de l'élève pour l'avant-dernière table non vide : 2 possibilités ;
- choix de l'élève pour la dernière table non vide : 1 possibilité.

Au total, on obtient donc $x \times 41!$ façons de placer les élèves.

Puisqu'on a dénombré de deux manières le même ensemble, on en déduit que $x = \frac{47!}{6!41!}$. Il y a donc $\binom{47}{6}$ façons de choisir un ensemble de 6 tables dans une salle en contenant 47.

Exercices d'application

- Combien y a-t-il de couples (x, y) dans $\llbracket 1; n \rrbracket^2$ tels que $x \neq y$?
- En utilisant l'alphabet français (qui contient 26 lettres $\odot$), combien existe-t-il de mots de 3 lettres (successions de 3 lettres : le mot n'a pas forcément de sens) ne se terminant pas par la lettre e ?
- En utilisant l'alphabet français, donner le nombre de mots de trois lettres que l'on peut former en obéissant aux règles suivantes :
 - la première lettre du mot est l'une des voyelles A, E, I, O, U mais pas Y ;
 - la deuxième lettre du mot est l'une des 3 lettres suivant, dans l'alphabet, la voyelle précédente ;
 - la dernière lettre du mot est l'une des 6 voyelles A, E, I, O, U, Y, mais pas celle qui est la première lettre.
- À partir d'un alphabet de p lettres, combien de mots de n lettres peut-on former qui ne contiennent jamais deux lettres identiques consécutives ?
- Une urne contient $2n$ boules numérotées de 1 à $2n$ qu'on tire successivement sans remise. Combien de tirages peut-on faire pour lesquels un numéro pair est toujours suivi d'un numéro impair et un numéro impair d'un numéro pair ?

II Dénombrer des applications

Proposition — Soit E et F des ensembles finis. Posons $n = \text{Card}(E)$ et $p = \text{Card}(F)$.

- L'ensemble F^E des applications de E dans F est fini et $\text{Card}(F^E) = p^n$.
- L'ensemble des applications injectives de E dans F est de cardinal

$$\begin{cases} 0 & \text{si } n > p \\ \frac{p!}{(p-n)!} & \text{si } n \leq p \end{cases}$$

Preuve : Numérotions artificiellement les éléments de E .

Une application f de E dans F est construite par étapes :

- choix de l'image de l'élément 1 de E par f : p possibilités (on peut prendre n'importe quel élément de F) ;
- choix de l'image de l'élément 2 de E par f : p possibilités (idem) ;
- $\vdots$
- choix de l'élément n de E par f : p possibilités.

D'après le principe multiplicatif, il y a donc $p \times p \times \cdots \times p = p^n$ applications de E dans F .

On a déjà vu que si f est une application injective de E dans F , alors $\text{Card}(E) \leq \text{Card}(F)$. Donc, si $n > p$, il n'y a pas d'application injective de E dans F .

Supposons $n \leq p$. Une application injective f de E dans F peut être construite par étapes :

- choix de l'image de l'élément 1 de E par f : p possibilités (on peut choisir n'importe quel élément de F) ;
- choix de l'image de l'élément 2 de E par f : $p - 1$ possibilités (n'importe quel élément de F excepté celui choisi précédemment) ;

— :

- choix de l'image de l'élément n de E par f : $p - n + 1$ possibilités (n'importe quel élément de F excepté ceux choisis dans les $n - 1$ étapes précédentes).

Il y a donc $p \times (p - 1) \times \cdots \times (p - n + 1) = \frac{p!}{(p - n)!}$ applications injectives de E dans F .

Remarques :

1. On en déduit que le nombre de bijections d'un ensemble E de cardinal n dans lui-même, appelées aussi permutations de E , est $n!$.
(En effet, il y a $\frac{n!}{(n - n)!} = n!$ applications injectives de E dans lui-même, et une application de E dans E est injective ssi elle est bijective.)
2. Faire asseoir 41 élèves dans une salle de 47 places, c'est réaliser une injection de l'ensemble des élèves dans l'ensemble des places (injection car deux élèves ne peuvent s'asseoir à la même place). On retrouve donc le résultat de l'exemple précédent : il y a $\frac{47!}{(47 - 41)!} = \frac{47!}{6!}$ manières de placer les élèves.

III Dénombrer des parties

Proposition — Soit E un ensemble de cardinal n . L'ensemble $\mathcal{P}(E)$ des parties de E est de cardinal 2^n : $\text{Card}(\mathcal{P}(E)) = 2^n$.

Preuve : Numérotions artificiellement les éléments de E . Pour construire une partie A de E , on peut raisonner par étapes :

- considérer le premier élément de E et décider s'il appartient ou non à A : 2 possibilités ;
- :
- considérer le dernier élément de E et décider s'il appartient ou non à A : 2 possibilités.

Il y a donc $2 \times \cdots \times 2 = 2^n$ parties de E .

Définition — Soit E un ensemble de cardinal n . Soit $p \in \llbracket 0; n \rrbracket$.
On appelle **p -combinaison** de E toute partie de E de cardinal p .

Exemple Dans $E = \{\text{I}, \text{II}, \text{III}, \text{IV}\}$, les ensembles $\{\text{I}, \text{II}, \text{III}\}$, $\{\text{III}, \text{I}, \text{II}\}$ et $\{\text{III}, \text{III}, \text{I}, \text{II}\}$ désignent les mêmes 3-combinaisons (l'ordre ne compte pas).

Proposition — Soit E un ensemble de cardinal n . Soit $p \in \llbracket 0; n \rrbracket$.

Le nombre de parties de E à p éléments, appelées aussi **p -combinaisons** de E , est $\binom{n}{p} = \frac{n!}{p!(n - p)!}$.

Preuve : En dénombrant de deux manières l'ensemble des façons de placer 41 élèves dans une salle de 47 places, on avait montré qu'il y a $x = \binom{47}{6}$ manières de choisir les 6 tables qui resteront inoccupées.

Suivons ici la même idée, et introduisons un ensemble F de cardinal $n - p$. Notons x le nombre de p -combinaisons de E .

Dénombrons de deux manières les injections de F dans E .

D'après une proposition précédente, il y en a $\frac{n!}{(n - (n - p))!} = \frac{n!}{p!}$.

Pour construire une injection f de F dans E , on peut également raisonner ainsi :

- choisir les éléments de E qui n'auront pas d'antécédents par f : il y a x possibilités ;
- déterminer une bijection de F dans E privé des p éléments précédemment choisis : il y a $(n - p)!$ possibilités.

Il y a donc $x \times (n - p)!$ injections de F dans E .

Par conséquent, $x \times (n - p)! = \frac{n!}{p!}$, donc $x = \frac{n!}{p!(n - p)!} = \binom{n}{p}$.

Remarque : On retrouve par des arguments de dénombrement les propriétés des coefficients binomiaux établis dans un précédent chapitre par le calcul :

- $\binom{n}{0} = 1$: il y a une seule partie à 0 élément dans un ensemble E à n éléments, c'est la partie vide.
- $\binom{n}{1} = n$: il y a n parties à un seul élément dans un ensemble E à n éléments, ce sont les singletons $\{a\}$, avec $a \in E$.
- $\binom{n}{k} = \binom{n}{n-k}$ pour tout $k \in \llbracket 0; n \rrbracket$: choisir une partie à k éléments de E revient à choisir son complémentaire qui est une partie à $n - k$ éléments de E .
- Montrons enfin par le dénombrement la formule du triangle de Pascal :

$$\text{pour tout } n \in \mathbb{N}^*, \text{ pour tout } k \in \llbracket 0; n-1 \rrbracket, \quad \binom{n}{k} + \binom{n}{k+1} = \binom{n+1}{k+1}$$

Soit $n \in \mathbb{N}^*$ et $k \in \llbracket 0; n-1 \rrbracket$. Posons $E = \{A \in \mathcal{P}(\llbracket 1; n+1 \rrbracket) \mid \text{Card}(A) = k+1\}$ et dénombrons E de deux manières :

1. E est l'ensemble des $k+1$ -combinaisons de $\llbracket 1; n+1 \rrbracket$, donc $\text{Card}(E) = \binom{n+1}{k+1}$.
2. D'autre part, les éléments de E sont de deux types :
 - les éléments contenant 1 : pour construire un tel élément de E , il suffit de prendre 1 et une partie de $\llbracket 2; n+1 \rrbracket$ à k éléments. Il y en a donc $\binom{n}{k}$.
 - les éléments ne contenant pas 1 : pour construire un tel élément de E , on choisit une partie de $\llbracket 2; n+1 \rrbracket$ à $k+1$ éléments. Il y en a donc $\binom{n}{k+1}$.

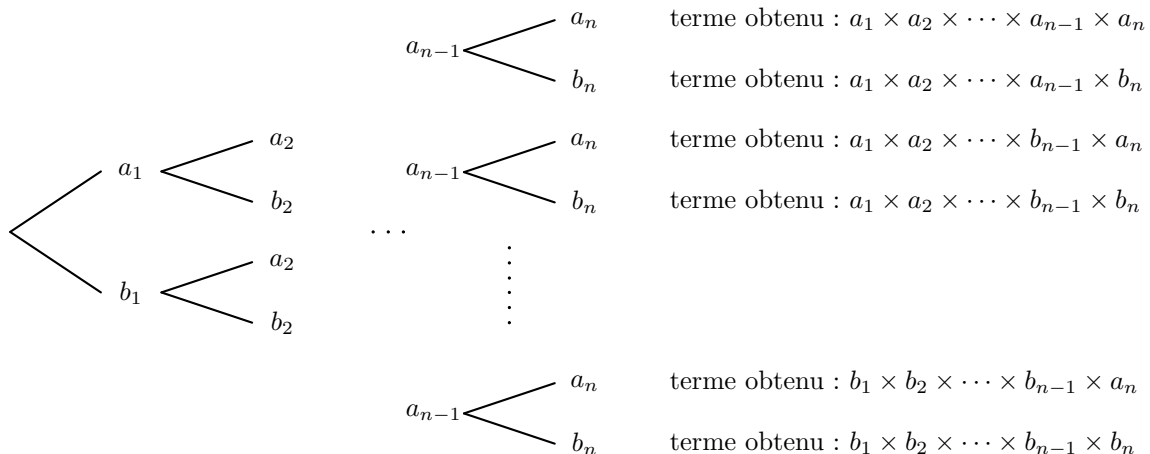
Un élément de E ne pouvant être des deux types simultanément, on en déduit que $\text{Card}(E) = \binom{n}{k} + \binom{n}{k+1}$.

Finalement, on a prouvé : $\binom{n+1}{k+1} = \binom{n}{k} + \binom{n}{k+1}$.

- On peut également retrouver la formule du binôme de Newton :

$$\text{pour tous } a, b \in \mathbb{C}, \text{ pour tout } n \in \mathbb{N}, \quad (a+b)^n = \sum_{k=0}^n \binom{n}{k} a^k b^{n-k}$$

Soit $a, b \in \mathbb{C}$, soit $n \in \mathbb{N}^*$ (la formule est clairement vraie pour $n = 0$). Posons pour $i \in \llbracket 1; n \rrbracket$, $a_i = a$ et $b_i = b$. Alors $(a+b)^n = (a_1+b_1)(a_2+b_2)\dots(a_n+b_n)$ et développer ce produit, c'est faire la somme de tous les termes obtenus en faisant les produits des éléments de chaque branche de l'arbre suivant :



Puisque tous les b_i sont égaux à b et tous les a_i sont égaux à a , les termes sont tous des produits de n facteurs égaux à a ou b , ils sont donc du type $a^k b^{n-k}$ avec $k \in \llbracket 0; n \rrbracket$.

Soit $k \in \llbracket 0; n \rrbracket$. Combien y a-t-il de termes du type $a^k b^{n-k}$? autant que de façons de choisir les k indices des facteurs a_i apparaissant dans ces produits (les indices des b_i sont alors les indices restants) : il y en a donc $\binom{n}{k}$ (il s'agit de choisir k indices parmi les n possibles).

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

Exercice d'application De combien de façons peut-on tirer cinq cartes simultanément dans un jeu de 52 cartes ?

IV Les p -listes

Définition — Soit E un ensemble et $p \in \mathbb{N}^*$. On appelle p -liste d'éléments de E tout p -uplet d'éléments de E , c'est-à-dire tout élément de E^p .

Remarque : L'ordre a une importance dans une liste ; il peut également y avoir des répétitions : $(2, 2, 1)$, $(1, 2, 2)$ et $(2, 1, 2)$ sont des 3-listes d'éléments de $\mathbb{N}$ deux à deux distinctes : $(2, 2, 1) \neq (1, 2, 2)$, $(2, 2, 1) \neq (2, 1, 2)$ et $(1, 2, 2) \neq (2, 1, 2)$.

Dans $E = \{\clubsuit, \heartsuit, \spadesuit, \diamondsuit\}$, le triplet $(\spadesuit, \heartsuit, \heartsuit)$ est une 3-liste. Le triplet $(\heartsuit, \spadesuit, \spadesuit)$ est une 3-liste différente.

Proposition — Soit E un ensemble de cardinal n . Soit $p \in \mathbb{N}^*$. Il y a n^p p -listes de E .

Preuve : Pour construire une p -liste, on procède par étapes :

- choix du premier élément de la p -liste : n possibilités ;
- choix du deuxième élément : n possibilités ;
- :
- choix du dernier élément : n possibilités.

Au final, il y a donc $n \times \dots \times n = n^p$ p -listes possibles.

On aurait aussi pu utiliser le résultat sur le cardinal d'un produit cartésien.

Exercice d'application De combien de façons peut-on tirer cinq cartes successivement avec remise dans un jeu de 52 cartes ?

Définition — Soit E un ensemble et $p \in \mathbb{N}^*$. On appelle p -liste d'éléments distincts de E , ou encore p -arrangement de E , tout p -uplet $(x_1, \dots, x_p) \in E^p$ tel que pour tout $i, j \in \llbracket 1; p \rrbracket$, $x_i \neq x_j$ si $i \neq j$.

Exemple Dans $E = \{\clubsuit, \heartsuit, \spadesuit, \diamondsuit\}$, les triplets $(\clubsuit, \heartsuit, \spadesuit)$ et $(\spadesuit, \clubsuit, \heartsuit)$ sont deux 3-arrangements de E différents (l'ordre compte).

Proposition — Soit E un ensemble fini de cardinal n et $p \in \mathbb{N}^*$. Alors :

- si $p > n$, il n'y a pas de p -listes d'éléments distincts de E ;
- si $p \leq n$, il y a $\frac{n!}{(n-p)!}$ p -listes d'éléments distincts de E .

Preuve : Si $p > n$: considérons une p -liste d'éléments distincts de E . Les n premiers éléments de cette p -liste sont tous distincts deux à deux, ils recouvrent donc tous les éléments de E (qui sont au nombre de n), il n'y a donc plus aucune possibilité pour l'élément suivant, une telle p -liste n'existe pas.

Supposons $p \leq n$. Définir une p -liste d'éléments distincts, c'est choisir successivement ses éléments parmi ceux de E :

- choix du premier élément : n possibilités ;
- choix du deuxième élément : $n - 1$ possibilités (on ne peut pas reprendre l'élément précédemment choisi) ;
- :
- choix du dernier élément : $n - (p - 1)$ possibilités (on doit choisir un élément distinct de ceux choisis au cours des $p - 1$ étapes précédentes).

Au final, il y a donc $n \times (n - 1) \times \dots \times (n - p + 1) = \frac{n!}{(n-p)!}$ p -listes d'éléments distincts.

Exemple Soit $n \in \mathbb{N}^*$. Il existe $n!$ façons exactement d'ordonner les n éléments de $\llbracket 1; n \rrbracket$.

Exercice d'application De combien de façon peut-on tirer cinq cartes successivement sans remise dans un jeu de 52 cartes ?

V À retenir

À retenir de ce cours —

- le principe de disjonction des cas : si E est la réunion disjointe de A et B , alors $\text{Card}(E) = \text{Card}(A) + \text{Card}(B)$.
- le principe multiplicatif : si les objets de E peuvent être décrits par étapes (attention ! la description doit être bi-univoque : la description permet d'obtenir tous les objets, et chaque objet n'est décrit qu'une fois)
- il y a $\binom{n}{k}$ parties à k éléments d'un ensemble à n éléments (dans une partie—qui est un ensemble— il n'y a pas d'ordre).

On devrait alors pouvoir retrouver rapidement les autres cardinaux énoncés :

- nombre de parties d'un ensemble à n éléments (2^n) ;
- nombre d'applications de E de cardinal n dans F de cardinal p (p^n) ;
- nombre d'applications injectives de E de cardinal n dans F de cardinal p (0 si $p < n$, $\frac{p!}{(p-n)!}$ si $p \geq n$) ;
- nombre de p -listes d'éléments de E de cardinal n (n^p) ;
- nombre de p -listes d'éléments distincts de E de cardinal n (0 si $p > n$, $\frac{n!}{(n-p)!}$ si $p \leq n$).

Tableau récapitulatif

Propriétés de l'objet à dénombrer		Modélisé par	Exemple fondamental	Écriture
Ordre	Éléments tous distincts			
Non	Oui	Parties d'un ensemble E : on utilise des combinaisons	Tirages simultanés	$\{...;...;...\}$
Oui	Non	p -uplets d'éléments d'un même ensemble E : on utilise des listes	Tirages successifs avec remise	$(...;...;...)$
Oui	Oui	p -uplets d'éléments d'un même ensemble E , sans répétition : on utilise des arrangements	Tirages successifs sans remise	$(...;...;...)$
Non	Non	On modifie la modélisation pour se ramener à l'un des trois cas précédents		

Exemples :

1. Combien peut-on former d'anagrammes, ayant un sens ou non, du mot MATH ?

Pour construire une telle anagramme :

- choix de la place du M : 4 possibilités ;
- choix de la place du A : 3 possibilités ;
- choix de la place du T : 2 possibilités ;
- choix de la place du H : 1 possibilité.

Au final, il y a $4 \times 3 \times 2 \times 1 = 4!$ anagrammes possibles.

Chaque anagramme est bien décrite de manière unique par cette construction, mais on aurait pu choisir une autre description, par exemple :

- choix de la lettre pour la première place : 4 possibilités ;
- choix de la lettre pour la deuxième place : 3 possibilités ;
- etc.

2. Même question pour le mot CHIMIE.

En choisissant la place de chaque lettre :

- choix de la place du C : 6 possibilités ;
- choix de la place du H : 5 possibilités ;
- choix de la place du M : 4 possibilités ;
- choix de la place du E : 3 possibilités ;
- les deux I occupent les deux dernières places.

Il y a donc $6 \times 5 \times 4 \times 3$ anagrammes possibles.

On aurait pu aussi commencer par choisir la place des deux I, puis la place de chacune des autres lettres :

- choix de la place des deux I : $\binom{6}{2}$ possibilités (on choisit 2 éléments dans un ensemble à 6 éléments) ;
- choix de la place du C : 4 possibilités (il reste 4 places libres une fois les deux I placés) ;
- choix de la place du H : 3 possibilités ;
- choix de la place du M : 2 possibilités ;
- choix de la place du E : 1 possibilité.

Je vous laisse vérifier que les deux résultats sont cohérents !

3. Tirages de boules dans une urne.

- (a) On considère 10 boules numérotées de 1 à 10. On tire successivement et sans remise 5 boules de l'urne. Combien de tirages peut-on obtenir ?

- choix de la première boule : 10 possibilités ;
- choix de la deuxième boule : 9 possibilités ;
- :
- choix de la cinquième boule : 6 possibilités.

Il y a donc $10 \times 9 \times \cdots \times 6 = \frac{10!}{5!}$ tirages possibles.

On peut aussi choisir de représenter un tirage par la liste des numéros obtenus. Un tirage est donc ici représenté par une 5-liste d'éléments distincts de l'ensemble des 10 boules de l'urne. Il y a donc $\frac{10!}{5!}$ tirages possibles.

- (b) Même question si les tirages ont lieu avec remise.

- choix de la première boule : 10 possibilités ;
- choix de la deuxième boule : 10 possibilités ;
- :
- choix de la cinquième boule : 10 possibilités.

Il y a donc $10 \times 10 \times \cdots \times 10 = 10^5$ tirages possibles.

On peut aussi choisir de représenter un tirage par la liste des numéros obtenus. Un tirage est donc ici représenté par une 5-liste d'éléments de l'ensemble des 10 boules de l'urne. Il y a donc 10^5 tirages possibles.

- (c) Même question si les tirages ont lieu simultanément.

Il faut alors reprérer qu'il n'y a pas d'ordre dans les boules tirées. Cela correspond simplement à choisir une partie à 5 éléments dans un ensemble à 10 éléments. Il y en a $\binom{10}{5}$.