I - Dénombrement par mise en évidence d'une bijection explicite

a) Notion de cardinal d'un ensemble

Déf 1: L'ensemble E est dit fini et de cardinal n, soit s'il est vide et dans ce cas $n=0$, soit, si $n>0$, s'il existe une bijection de E sur un intervalle d'entier $[\![1,n]\!]$; on dit alors que E est un n-ensemble et on écrit $\mathrm{Card}E=n$ (ou $|E|=n$)

Rmq 2: $|\emptyset|=0$

Prop 3: Soit E un ensemble de cardinal n et F un autre ensemble. Il existe une bijection entre E et F ssi F est de cardinal n

Prop 4: Soit E un ensemble fini. Soit F une partie de E. L'ensemble F est fini et $|F|\leqslant|E|$
En particulier, $|F|=|E|$ ssi $F=E$.

Prop 5: Soit E et E' deux ensembles. Soit $f: E\to E'$ une fonction
1) Si E' est fini et f injective alors E est fini et $|E|\leqslant|E'|$
2) Si E est fini et f surjective alors E' est fini et $|E'|\leqslant|E|$

Rmq 6: $|E|=|E'|$ ssi f est bijective

Thm 7: (Principe des tiroirs de Dirichlet) On possède p chaussettes que l'on veut ranger dans n tiroirs. Soit f l'application qui à une chaussette associe le tiroir dans lequel on la range
1) Si $p>n$, alors il y a forcément un tiroir qui contient plusieurs chaussettes: l'application ne peut pas être injective
2) Si $p<n$, alors il y a forcément un tiroir qui ne contient pas de chaussettes: l'application n'est pas surjective.

b) Opérations ensemblistes

Thm 8: (Formule du Crible) Soient $(E_k)_{k\in[\![1,n]\!]}$ n ensembles finis. Alors:
$$\left|\bigcup_{k=1}^{n}E_k\right|=\sum_{k=1}^{n}\left[(-1)^{k+1}\sum_{1\leqslant i_1<\dots<i_k\leqslant n}|E_{i_1}\cap\dots\cap E_{i_k}|\right]$$

Rmq 9: Si les $(E_k)_{k\in[\![1,n]\!]}$ sont deux à deux disjoints, alors
$$\left|\bigcup_{k=1}^{n}E_k\right|=\sum_{k=1}^{n}|E_k|$$

Application 10: En notant pour tout $n\geqslant1$, $p_1,\dots p_k$ les nombres premiers inférieurs à n et $U_i=\{(a,b)\in[\![1,n]\!]^2,\ p_i|a \text{ et } p_i|b\}$ pour tout $i\in[\![1,k]\!]$, on peut calculer $\left|\bigcup_{i=1}^{k}U_i\right|$ avec la formule du crible

Prop 11: (Principe des bergers: version 1): Soit E un ensemble fini. On suppose que E admet une partition constituée de p sous-ensemble de même cardinal x. Alors $|E|=x\times p$

Rmq 12: permet de compter le nombre de pattes d'un troupeau constitué de n moutons.

Prop 13: (Principe des bergers: version 2): Soient E et F deux ensemble non vides. Soit $p\in\mathbb{N}^*$. Soit $f: E\to F$ une application. On suppose que $\forall y\in F$, $|f^{-1}(\{y\})|=p$, alors $|E|=p|F|$

Ex 14: Considérons un troupeau de moutons T et P l'ensemble des pattes de moutons. On considère l'application f qui à une patte P associe le mouton possédant cette patte, $\forall m\in T$, $|f^{-1}(\{m\})|=4$

Déf 15: Soient p ensembles finis $A_1,\dots A_p$ tout élément de la forme $(x_1,\dots x_p)$, où, pour tout $k\in[\![1,p]\!]$, $x_k\in A_k$ est appelé p-liste ou p-uplet. L'ensemble de ces p-listes, noté $A_1\times\dots\times A_p$ est le produit cartésien de ces ensembles.

Ex 16: Pour $E=[\![1,20]\!]$, $(19,1,2,1,3)$ et $(1,19,2,1,9)$ sont des 5-uplets de E différents.

Thm 17: $|A_1\times\dots\times A_p|=\prod_{i=1}^{p}|A_i|$

Thm 18: Soit $p\in\mathbb{N}^*$. Soit E un ensemble fini tel que $|E|=n$. Le nombre de p-liste de E est n^p.

c) Arrangement d'un ensemble

Déf 19: On appelle p-arrangement de E toute p-liste d'éléments de E deux à deux distincts

Thm 20: Soit $p\in\mathbb{N}^*$. Soit E un ensemble fini tel que $|E|=n$. Le nombre de p-arrangements de E est $\frac{n!}{(n-p)!}$ si $p\leqslant n$. Sinon, il n'en existe pas.

Rmq 21: des p-arrangements sont utilisés pour modéliser les tirages successifs sans remise

Ex 22:
- Le nombre de mots de 3 lettres distinctes est $26\times25\times24$
- $|S_n|=n!$

Déf 23: Soit $p \in \mathbb{N}^*$. On appelle p-combinaison de E toute partie de cardinal p.

Déf 24: On appelle coefficient binomial, p parmi n, $\binom{n}{p} = \frac{n!}{p!(n-p)!}$

Thm 25: Soit $p \in \mathbb{N}^*$. Soit E un ensemble fini tel que $|E| = n$ le nombre de p-combinaison de E est $\binom{n}{p}$

Ex 26: Le nombre de tirages possibles au loto est $\binom{49}{6}$

Prop 27: Soit $n \in \mathbb{N}^*$, $p \in [\![0, n]\!]$

1) Symétrie des coefficients binomiaux $\binom{n}{p} = \binom{n}{n-p}$

2) Formule de pascal $\binom{n}{p} + \binom{n}{p+1} = \binom{n+1}{p+1}$ pour $p \leq n-1$

App 28: (Formule du binome de Newton) Soient $(a,b) \in \mathbb{K}^2$ où $\mathbb{K}$ est un corps commutatif, soit $n \in \mathbb{N}^*$ alors

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

App 29: Soit E un ensemble fini. Alors $\mathcal{P}(E)$ l'ensemble des parties de E est fini et vérifie $|\mathcal{P}(E)| = 2^{|E|}$

II - Utilisations des méthodes algébriques pour dénombrer

a) Dénombrement de $\mathbb{Z}/n\mathbb{Z}$

Déf 30: Soit n un entier non nul. On appelle indicatrice d'Euler de n l'entier $\phi(n) := |(\mathbb{Z}/n\mathbb{Z})^\times|$

Prop 31: Soit $n \in \mathbb{N}^*$, $n \geq 2$ soit $k \in \mathbb{N}$. $\bar{k}$ l'élément $\bar{k}$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$ ssi $k \wedge n = 1$.

Rmq 32: $\phi(n)$ est donc le nombre d'entier $k \in [\![1, n]\!]$ premier avec n. Si n est un nombre premier alors $\phi(n) = n-1$.

Prop 33: Soit $n \geq 2$, on écrit sa décomposition en facteurs premiers $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$. Alors $\phi(n) = n \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right)$

Conséquence 34: Pour tout $n \geq 2$, $n = \sum_{d|n} \phi(d)$

Thm 35 (d'Euler): Soit $n \in \mathbb{N}^*$, $k \in \mathbb{N}$. Si $k \wedge n = 1$ alors $k^{\phi(n)} \equiv 1 \ [n]$

Rmq 36: Ce théorème généralise le petit théorème de Fermat

b) Par inversion

Déf 37: On définit la fonction de Möbius $\mu : \mathbb{N}^* \to \{0, 1, -1\}$ comme suivant $\mu(1) = 1$, $\mu(n) = 0$ si n contient un facteur carré et $\mu(p_1 \cdots p_r) = (-1)^r$ si $p_1, \ldots, p_r$ sont des nombres premiers distincts.

Prop 38: Pour tout $n \in \mathbb{N}^*$, $\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{si } n = 1 \\ 0 & \text{si } n \geq 2 \end{cases}$.

App 39: (Théorème de Césaro) La probabilité pour que deux entiers choisis aléatoirement dans $[\![1, n]\!]^2$ $n \in \mathbb{N}^*$, soient premier entre eux tend lorsque $n \to +\infty$ vers $\frac{6}{\pi^2}$

Rmq 40: Pour tout $n \in \mathbb{N}$ $\phi(n) = n \sum_{d|n} \frac{\mu(d)}{d}$

Prop 41: La fonction indicatrice d'Euler ϕ et la fonction de Möbius μ sont inversibles dans $(\mathbb{R}^{\mathbb{N}^*}, +, *)$

Thm 42: (Formule d'inversion de Möbius) Pour toutes suites u et v dans $\mathbb{R}^{\mathbb{N}^*}$, les assertions suivantes sont équivalentes : i) $\forall n \in \mathbb{N}^*$, $u(n) = \sum_{d|n} v(d)$

ii) $\forall n \in \mathbb{N}^*$, $v(n) = \sum_{d|n} \mu(d)\, u\left(\frac{n}{d}\right)$

App 43: Pour tout entier naturel $n \in \mathbb{N}^*$, pour tout nombre premier p, il existe dans $\mathbb{F}_p$ des polynomes irréductibles de degré n et leur nombre vérifie $I_n^p \underset{n \to +\infty}{\sim} \frac{p^n}{n}$ dev ①

c) Fonction génératrices

Déf 44: Soit $(a_n)_{n \in \mathbb{N}}$ une suite de nombres complexes, la fonction génératrice ordinaire de (a_n) est définie pour $f(x) = \sum_{n=0}^{+\infty} a_n x^n$, à condition que cette série entière ait un rayon de convergence non nul.

Ex 45: • Calcul du nombre de dérangement de $[\![1, n]\!]$ (permutation de S_n n'ayant pas de points fixes)

• Nombres de Bell : nombre de partitions de l'ensemble de $[\![1, n]\!]$.

III - Utilisation de la théorie des groupes

Soit G un groupe de X un ensemble.

Thm 46: (de Lagrange) Supposons que G soit un groupe fini et $H < G$ un sous groupe. Alors $|H| \mid |G|$

Déf 47: Considérons l'action de G à gauche sur l'ensemble X et $x \in X$. On appelle orbite de x sous G le sous ensemble $G.x = \{ g.x \mid g \in G \} \subset X$. On appelle stabilisateur de x dans G le sous groupe $G_x = \{ g \in G \mid g.x = x \} \subset G$.

Déf 48: Soit $H < G$ On appelle ensemble quotient de G par la relation d'équivalence $\sim_H$ et on note G/H, l'ensemble $\{gH \mid g \in G\}$ des classes à gauche de G modulo H.

Déf 49: On appelle indice de H dans G et on note $[G:H]$ le cardinal de l'ensemble quotient.

Ex 50: de cardinal du groupe alterné A_n, ou comme $S_n / \ker \varepsilon$ (ε est la signature d'une permutation) est $\frac{n!}{2}$.

Prop 51: Soit $x \in X$, l'application $f : G/G_x \longrightarrow G.x$ est une bijection

Cor 52: (Relation orbite / Stabilisateur) Soit $x \in X$. Alors
1) $|G.x| = [G : G_x]$
2) $|G| = |G_x| |G.x|$
3) Si G est fini alors $|G.x| = \frac{|G|}{|G_x|}$

Cor 53: Supposons G fini.
1) Formule aux classes : Si $X = \bigcup_{i=1}^{n} X_i$ est la partition de X en orbite sous l'action de G et si $x_i \in X_i$ est un élément de l'orbite de X_i, alors $|X| = \sum_{i=1}^{n} \frac{|G|}{|G_{x_i}|}$

2) Formule de Burnside : Etant donné $g \in G$, notons X^g l'ensemble des points fixes de X sous l'action de $\langle g \rangle$ de nombre r des orbites de X sous l'action de G est donné par
$$r = \frac{1}{|G|} \sum |X^g|$$

Thm 54: (de Cauchy) Soit G un groupe fini d'ordre divisible par un nombre premier p. Alors il existe dans G au moins un élément d'ordre p.

App 55: Soit p un nombre premier et G un p-groupe fini non trivial. Alors le centre $Z(G)$ de G ne se réduit pas à $\{e\}$. En particulier, un p-groupe fini d'ordre non premier n'est jamais un groupe simple. De plus, un groupe d'ordre p^2 est toujours abélien. dev ②

Déf 56: Soit G un groupe fini de cardinal n et p un diviseur premier de n. Si $n = p^\alpha m$ avec $p \nmid m$, on appelle p-sous-groupe de Sylow de G un sous groupe de cardinal p^α.

Ex 57: Soit $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ le corps fini à p éléments (p premier)
- $|Gl_n(\mathbb{F}_p)| = (p^n - 1)(p^n - p) \cdots (p^n - p^{n-1})$
- $|Sl_n(\mathbb{F}_p)| = p^{\frac{n(n-1)}{2}} (p^n - 1)(p^{n-1} - 1) \cdots (p^2 - 1)$
- $P = \{ A = (a_{ij}) \mid a_{ij} = 0 \text{ si } i > j \text{ et } a_{ii} = 1 \}$, $|P| = p^{\frac{n(n-1)}{2}}$

Thm 58: (de Sylow 1) Soit G un groupe fini et p un diviseur (premier) de $|G|$, alors G contient au moins un p-sous groupe de Sylow.

Thm 59: (de Sylow 2) : Soit G un groupe de cardinal $p^\alpha m$ avec $p \nmid m$
1) Si H est un sous groupe de G qui est un p-groupe, il existe un p-Sylow S avec $H \subset S$
2) les p-Sylow sont tous conjugués (et donc leur nombre n_p divise n)
3) On a $n_p \equiv 1 [p]$, donc $n_p \mid m$.