Méthodes combinatoires, problèmes de dénombrement

I) Dénombrement élémentaires

1) Cardinal d'un ensemble fini

Déf 1 : Soit $n \in \mathbb{N}^*$, on note $\mathbb{N}_n = [\![1;n]\!]$, et on pose $\mathbb{N}_0 = \emptyset$.

Déf 2 : On dit qu'un ensemble X est fini si $\exists n \in \mathbb{N}$, et il existe une bijection de $\mathbb{N}_n$ dans X.

Lemme 3 : Soient $p, q \in \mathbb{N}$. S'il existe une injection de $\mathbb{N}_p$ dans $\mathbb{N}_q$, alors $p \leq q$.

Déf-Th 4 : Soit X un ensemble fini. $\exists! \, n \in \mathbb{N}$ tel que X est en bijection avec $\mathbb{N}_n$.
Cet unique entier n est appelé cardinal de X, noté $|X|$. On note alors $X = \{x_1, \dots, x_n\}$

Règle de la somme et du produit : On considère $A_1, \dots, A_r$ r actions avec $n_1, \dots, n_r$ façons de les effectuer.
alors le nombre de façon d'effectuer une de ces actions est $\sum_{i=1}^{r} n_i = n_1 + \dots + n_r$;
et le nombre de façon d'effectuer toutes ces actions est $\prod_{i=1}^{r} n_i = n_1 \times \dots \times n_r$.

Exple 6 : On veut régler 15 € avec des pièces de 1€, des billets de 5€ et 10€. Il y a 6 façon de régler.

Exple 7 : On veut compter le nombre de diviseurs de 180. Il y en a 18.

Prop : Principe des tiroirs : Soit $f : X \to Y$ avec $|X| > |Y|$ Il existe un élément de Y qui admet au moins 2 antécédents

2) Opérations sur les cardinaux

Prop 9 : Soient X, Y deux ensembles finis, alors $|X \cup Y| = |X| + |Y| - |X \cap Y|$. En particulier, si $X \cap Y = \emptyset$, $|X \sqcup Y| = |X| + |Y|$

Coro 10 : Formule du crible de Poincaré : Soient $X_1, \dots, X_n$ ensembles finis, $\left|\bigcup_{i=1}^{n} X_i\right| = \sum_{\substack{I \subset [\![1,n]\!] \\ I \neq \emptyset}} (-1)^{|I|+1} \cdot \left|\bigcap_{i \in I} X_i\right|$

Prop 11 : Soient $X_1, \dots, X_n$ ensembles finis, alors $\left|\prod_{i=1}^{n} X_i\right| = \prod_{i=1}^{n} |X_i|$.

Prop 12 : Soient X, Y deux ensembles finis. On note $\mathcal{F}(X,Y) = Y^X$. Alors $|Y^X| = |Y|^{|X|}$

Prop 13 : Soit X un ensemble fini. On note $\mathcal{P}(X)$ l'ensemble de ses parties. Alors $|\mathcal{P}(X)| = 2^{|X|}$.

3) Calcul combinatoire

Soit X un ensemble fini de cardinal n et $p \in [\![0;n]\!]$.

Déf 14 : On note $\mathfrak{S}(X)$ l'ensemble des bijections de X dans X, appelée permutations de X.

Prop 15 : On a $\mathfrak{S}(X) \simeq \mathfrak{S}_n$. De plus $|\mathfrak{S}(X)| = 1 \times 2 \times \dots \times n = n!$.

Déf 16 : On appelle p-arrangement de X tout p-uplet $(x_1, \dots, x_p) \in X^p$ formé d'élément 2 à 2 distincts

Prop 17 : Il y a exactement : $A_n^p = n \times (n-1) \times \dots \times (n-p+1) = \frac{n!}{(n-p)!}$ p-arrangements de X.

Coro 18 : Soient X, Y deux ensembles finis. On pose $|X| = p$ et $|Y| = n$. Si $|X| \leq |Y|$, il y a $\frac{n!}{(n-p)!}$ injections de X vers Y

Exple 19 : Un mot M de n lettres est constitué de r lettres distinctes et la j ème lettre apparait p_j fois.
Il y a $\frac{n!}{p_1! \cdots p_r!}$ anagrammes différents possibles

Déf 20 : On appelle combinaison à p éléments de X toute partie à p éléments.

Prop 21 : Il y a exactement $\binom{n}{p} = \frac{1}{p!} A_n^p = \frac{n!}{(n-p)!}$ combinaisons à p éléments de X.

Exple 22 : $\sum_{p=0}^{n} \binom{n}{p} = 2^n$. Plus généralement, $\forall x, y \in \mathbb{C}$, $\sum_{p=0}^{n} \binom{n}{p} x^p y^{n-p} = (x+y)^n$

Exple 23 : Formule du triangle de Pascal : $\forall n \in \mathbb{N}^*, \forall k \in [\![0, n-1]\!]$, $\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}$.

Exple 24 : On considère l'équation $x_1 + \dots + x_p = n$ avec $(x_1, \dots, x_p) \in \mathbb{N}$. Il y a exactement $\binom{n+p+1}{p-1}$ solutions.

Exple 25 : Soient X, Y deux ensembles finis. On pose $|X| = p$ et $|Y| = n$. Si $|X| \leq |Y|$ il y a $\sum_{k=0}^{n} (-1)^{n-k} \binom{n}{k} k^p$ surjections

Exple 26 : Formule de Chu-Vandermonde : $\forall p, q \in \mathbb{N}$, $n \in [\![0, p+q]\!]$, $\binom{p+q}{n} = \sum_{i+j=n} \binom{p}{i} \binom{q}{j}$

4) Dénombrement en algèbre linéaire

Soit $p \in \mathcal{P}$ et $q = p^r$. Soit $n \in \mathbb{N}^*$.

Prop 27 : On a $|GL_n(\mathbb{F}_q)| = \prod_{k=0}^{n-1} (q^n - q^k) = q^{\frac{n(n-1)}{2}} \cdot \prod_{k=1}^{n} (q^k - 1)$.

Coro 28 : $|SL_n(\mathbb{F}_q)| = |PGL_n(\mathbb{F}_q)| = q^{\frac{n(n-1)}{2}} \cdot \prod_{k=2}^{n} (q^k - 1)$.

Appli : Isomorphismes exceptionnels : on a $GL_2(\mathbb{F}_2) = SL_2(\mathbb{F}_2) \simeq \mathfrak{S}_3$

II) Méthodes arithmétiques de dénombrement

Déf 30 : On dit qu'une fonction $f : \mathbb{N}^* \to \mathbb{C}$ est multiplicative si $\forall m, n \in \mathbb{N}^*$, $m \wedge n = 1 \Rightarrow f(mn) = f(m)f(n)$

1) La fonction indicatrice d'Euler

Déf° 31 : Soit $n \in \mathbb{N}^*$. On pose $\varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^\times| = |\{k \in [\![1, n]\!] : k \wedge n = 1\}|$

Prop 32 : φ est multiplicative et $\forall p \in \mathbb{P}, \forall \alpha \in \mathbb{N}^*$, $\varphi(p^\alpha) = (p-1)p^{\alpha-1}$.

Prop 33 : $\forall n \in \mathbb{N}^*$, $\varphi(n) = n \cdot \prod_{\substack{p \in \mathbb{P} \\ p | n}} \left(1 - \frac{1}{p}\right)$ et $n = \sum_{d|n} \varphi(d)$.

Appli 34 : $\forall p \in \mathbb{P}$, $(\mathbb{Z}/p\mathbb{Z})^\times$ est cyclique.

2) La fonction de Moëbius

Déf 35 : On définit la fonction de Moëbius par $\mu : \mathbb{N}^* \to \{-1, 0, 1\}$

$$n \longmapsto \begin{cases} 0 & \text{si } \exists p \in \mathbb{P} \text{ tq } p^2 | n \\ (-1)^r & \text{si } n = p_1 \cdots p_r \end{cases}$$

Prop 36 : μ est multiplicative.

DVPT

Prop 37 : Soit $n \in \mathbb{N}^*$, $\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{si } n = 1 \\ 0 & \text{si } n \geq 2 \end{cases}$

Exple 38 : Soit $n \in \mathbb{N}^*$, on note r_n la probabilité pour que 2 entiers choisis aléatoirement de $[\![1, n]\!]^2$ soient premiers entre eux. Alors $r_n = \frac{1}{n^2} \cdot \sum_{d=1}^{n} \mu(d) \cdot \left\lfloor \frac{n}{d} \right\rfloor^2$. De plus, $\lim_{n \to \infty} r_n = \frac{6}{\pi^2}$.

①

Exple 39 : $\forall s \in \mathbb{C}$, $\mathrm{Re}(s) > 1$, on a $\left(\sum_{n=1}^{\infty} \frac{1}{n^s}\right) \times \left(\sum_{n=1}^{\infty} \frac{\mu(n)}{n^s}\right) = \zeta(s) \cdot \sum_{n=1}^{\infty} \frac{\mu(n)}{n^s} = 1$

Déf 40 : Soient $u, v : \mathbb{N}^* \to \mathbb{C}$. On pose $\forall n \in \mathbb{N}^*$, $(u * v)(n) = \sum_{d|n} u_d \, v_{\frac{n}{d}}$ le pd de convolution arithmétique.

Th 41 : $(\mathbb{C}^{\mathbb{N}^*}, +, *)$ est un anneau commutatif et μ est inversible d'inverse 1.

Coro 42 : Formule d'inversion de Moëbius : $\forall f, g : \mathbb{N}^* \to \mathbb{C}$, on a $\forall n \in \mathbb{N}^*$, $g(n) = \sum_{d|n} f(d) \iff f(n) = \sum_{d|n} \mu(d) g\left(\frac{n}{d}\right)$

Exple 43 : On a $\varphi(n) = \sum_{d|n} \mu(d) \cdot \frac{n}{d}$.

Exple 44 : On note $I(n, q)$ l'ensemble des polynômes irréductibles de degré n sur $\mathbb{F}_q$.
alors $|I(n,q)| = \sum_{d|n} \mu\left(\frac{n}{d}\right) q^d$. En particulier, $|I(n,q)| \underset{+\infty}{\sim} \frac{q^n}{n}$.

3) Symbole de Legendre

Déf 45 : $\forall x \in \mathbb{F}_p$, on pose $\left(\frac{x}{p}\right) = \begin{cases} 0 & \text{si } x = 0 \\ 1 & \text{si } x \in (\mathbb{F}_p^*)^2 \\ -1 & \text{sinon} \end{cases}$

Prop 46 : $\forall p \in \mathbb{P}$ impair, $\left(\frac{\cdot}{p}\right)$ est multiplicatif et $\forall a \in \mathbb{F}_p$, $\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}}$.

Corollaire 47 : $\forall a \in \mathbb{F}_p^*$, $|\{x \in \mathbb{F}_p : ax^2 = 1\}| = 1 + \left(\frac{a}{p}\right)$

III) Méthode analytiques de dénombrement

1) Série génératrice

Déf 48 : Soit $(a_n) \in \mathbb{C}^{\mathbb{N}}$. On appelle série génératrice exponentielle de (a_n) la SE $\sum_{n \geq 0} a_n x^n$

DV

Exple 49 : $\forall n \in \mathbb{N}^*$, le nombre de partitions de $[\![1, n]\!]$ est $B_n = \frac{1}{e} \sum_{k=0}^{\infty} \frac{k^n}{k!}$.

②

Déf 50 : On appelle dérangement de $[\![1, n]\!]$ toute permutation de σ_n sans points fixes

Exple 51 : $\forall n \in \mathbb{N}^*$, le nombre de dérangements de $[\![1, n]\!]$ est $D_n = n! \sum_{k=0}^{n} \frac{(-1)^k}{k!}$

Exple 52 : n enfants envoient leur lettre au père noël mais il distribue les cadeaux au hasard.
La probabilité qu'aucun enfant n'ait le bon cadeau est $r_n = \sum_{k=0}^{n} \frac{(-1)^k}{k!}$. De plus, $\lim_{n \to \infty} r_n = \frac{1}{e}$.

Exple 53 : Soient $a_1, \dots, a_k \in \mathbb{Z}$ mutuellement 1^{ers} entre eux.
On pose $u_n = |\{(x_1, \dots, x_k) \in \mathbb{N}^k : a_1 x_1 + \dots + a_k x_k = n\}|$, alors $u_n \underset{+\infty}{\sim} \frac{1}{a_1 \cdots a_k} \cdot \frac{n^{k-1}}{(k-1)!}$.

2) Divergence de séries

Exple 54 : La série des inverses des nombre 1^{ers} $\sum_{n \geq 1} \frac{1}{p_n}$ diverge. Ainsi, il y a une infinité de nbs 1^{ers}

Th de la progression arithmétique de Dirichlet : Soient $a, D \in \mathbb{N}$ avec $a \wedge D = 1$,
alors il y a une infinité de nombres 1^{ers} de la forme $a + nD$, $n \in \mathbb{N}$.

IV) Utilisation des groupes et dénombrements en théorie des groupes

1) Action de groupes

Soit X un ensemble fini et $(G,\cdot)$ un groupe fini

Déf 56 : On dit que G opère à gauche sur X, noté $G \curvearrowright X$, si on a une application $\phi : G \to \mathfrak{S}(X)$, $g \mapsto [g \mapsto g\cdot x]$

Déf 57 : Si $G \curvearrowright X$. On note $\forall x \in X, \forall g \in G$:

- $G\cdot x = \{g\cdot x,\ g \in G\} \subset X$ l'orbite de x sous l'action de G
- $G_x = Stab_G(x) = \{g \in G,\ g\cdot x = x\} < G$, le stabilisateur de x
- $X^G = \{x \in X : G\cdot x = \{x\}\} \subset P(X)$ l'ensemble des orbites triviales
- $Fix(g) = \{x \in X : g\cdot x = x\} \subset X$ l'ensemble des points fixés par g.

Th 58 : Soit $G \curvearrowright X$. $\forall x \in X$, l'application $\varphi_x : G/G_x \to G\cdot x$, $gG_x \mapsto g\cdot x$ est bijective

De plus, $|G\cdot x| = [G:G_x] = \dfrac{|G|}{|G_x|}$. En particulier, on a $|G\cdot x|$ divise $|G|$.

Equation des classes : Soit $G \curvearrowright X$. On note $G\cdot x_1, \dots, G\cdot x_r$ les orbites distinctes alors $|X| = \sum_{i=1}^{r} |G\cdot x_i| = \sum_{i=1}^{r} \dfrac{|G|}{|G_{x_i}|}$.

Exple 60 : $\forall n \in \mathbb{N}^*$, $n \neq 6$. Les automorphismes de $\mathfrak{S}_n$ sont tous intérieurs.

Corollaire 61 : Si G est un p-groupe et $G \curvearrowright X$, alors $|X| \equiv |X^G|\ [p]$

Exple 62 : Le centre d'un p-groupe n'est pas trivial : $|Z(G)| \geq p$.
En particulier, si G est un groupe d'ordre p^2, $G \simeq \mathbb{Z}/p^2\mathbb{Z}$ ou $G \simeq (\mathbb{Z}/p\mathbb{Z})^2$.

DV 3 **Exple 63 :** Soient $p, q \in \mathcal{P}$ impairs distincts, alors $\left(\frac{p}{q}\right)\cdot\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$

Formule de Burnside : Soit $G \curvearrowright X$. Le nombre d'orbites est $r = \dfrac{1}{|G|}\cdot\sum_{g\in G} |Fix(g)|$.

Exple 65 : On dispose d'un fil circulaire, 4 perles bleues, 3 blanches, 3 rouges. On peut faire 76 colliers différents

2) Dénombrement des p-Sylow et simplicité

Dans cette section, $|G| = n = p^\alpha m$ avec $p \in \mathcal{P}$, $\alpha \in \mathbb{N}^*$, $p \wedge m = 1$.

Déf 66 : On appelle p-sous-groupe de Sylow de G tout sous groupe de cardinal p^α.

Exple 67 : Soit $G = GL_n(\mathbb{F}_p)$, alors $UT_n(\mathbb{F}_p) = \{A = (a_{i,j}) : \forall i > j, a_{i,j} = 0 \text{ et } a_{i,i} = 1\}$ est un p-Sylow de G

Lemme 68 : Soit $H < G$ et S un p-Sylow de G alors $\exists a \in G$ tq $aSa^{-1} \cap H$ soit un p-Sylow de H.

DV 4 **Théorèmes de Sylow :** (1) G contient au moins un p-Sylow
(2) Tout les p-Sylow de G sont conjugués
(3) Soit n_p le nb de p-Sylow de G, alors $\begin{cases} n_p \equiv 1\ [p] \\ n_p \mid m \end{cases}$

Coro 70 : Soit S un p-Sylow de G. $S \trianglelefteq G \iff S$ est l'unique p-Sylow de G.

Exple 71 : Soient $p, q \in \mathcal{P}$, $p < q$. Un groupe d'ordre $p^2 q$ n'est pas simple

DV 5 **Exple 72 :** A_5 est simple. On a ainsi $\forall n \geq 5$, A_n est simple

DV 6 **Exple 73 :** Soient $p, q \in \mathcal{P}$, $p < q$ et G un groupe d'ordre pq

- Si $q \not\equiv 1\ [p]$ (ie $p \nmid q-1$) alors $G \simeq \mathbb{Z}/pq\mathbb{Z}$,
- Si $q \equiv 1\ [p]$ (ie $p \mid q-1$) alors $G \simeq \mathbb{Z}/pq\mathbb{Z}$ ou $G \simeq \mathbb{Z}/q\mathbb{Z} \rtimes_\alpha \mathbb{Z}/p\mathbb{Z}$

3) Dénombrement des classes de conjugaison

Déf 74 : Soit G un groupe fini. On note $\widehat{G}$ le groupe dual de G, ie l'ensemble des caractères linéaires

Th : Orthogonalité des caractères : Soient $\chi_1, \chi_2 \in \widehat{G}$, $\langle \chi_1, \chi_2 \rangle = \dfrac{1}{|G|}\cdot\sum_{g\in G} \chi_1(g)\overline{\chi_2(g)} = \begin{cases} 1 & \text{si } \chi_1 = \chi_2 \\ 0 & \text{si } \chi_1 \neq \chi_2 \end{cases}$

Coro : Le nombre de caractères irréductibles de G est égal au nombre de classes de conjugaisons
De plus, si $G = V_1^{\oplus \alpha_1} \oplus \dots \oplus V_r^{\oplus \alpha_r}$, on a $|G| = (\dim V_1)^2 + \dots + (\dim V_r)^2$.

Exple : Dans $\mathfrak{S}_3$, il y a 3 classes de conjugaison. Dans D_4 et H_8, il y en a 5.