Soit E un ensemble non vide, $n \in \mathbb{N}^*$.

I Méthodes ensemblistes et dénombrement élémentaire.

A Cardinal d'un ensemble fini Sab 1.1 1.2 1.3 1.4

Définition 1 : On dit que E est fini de cardinal n s'il existe une bijection de E sur $[\![1, n]\!]$. On note $\mathrm{card}(E) = n$ ou encore $|E| = n$.

Remarque 2 : Si E est vide alors $|E| = 0$ par convention.

Proposition 3 : Soient A, B deux ensembles finis ;
Alors $|A \cup B| = |A| + |B| - |A \cap B|$

Corollaire 4 : Soit $(E_i)_{i \in [\![1,n]\!]}$ n ensembles finis deux à deux disjoints. Alors
$$\left|\bigcup_{i=1}^{n} E_i\right| = \sum_{i=1}^{n} |E_i|$$

Corollaire 5 : Soit $(E_i)_{i \in [\![1,n]\!]}$ n ensembles finis, alors :
$$\left|\bigcup_{i=1}^{n} E_i\right| = \sum |E_i| - \sum_{1 \leq i < j \leq n} |E_i \cap E_j| + \sum_{1 \leq i < j < k \leq n} |E_i \cap E_j \cap E_k| + \dots + (-1)^n \left|\bigcap_{1 \leq i \leq n} E_i\right|$$
(Formule du crible ou de Sylvester).

Application 6 : Il y a 684 nombres contenant au moins 0, 3, 6 ou 9.

Théorème 7 : Soit $(A_i)_{i \in [\![1,p]\!]}$ p ensembles finis, alors $|A_1 \times \dots \times A_p| = \prod_{k=1}^{p} |A_k|$.

Application 8 : Le cardinal de l'ensemble des applications d'un n ensemble dans un p ensemble est p^n.

Exemple 9 : Il y a 64 signes possibles différents dans l'alphabet de Braille.

B Arrangements, permutations, combinaisons Sab 2.1 2.2 2.3 2.5 2.6

Définition 10 : Soit E un ensemble à n éléments, $p \in [\![1, n]\!]$. Un arrangement p à p de E est un p-uplet $(e_1, \dots, e_p)$ formé de p éléments de E deux à deux distincts.

Théorème 11 : Le nombre d'arrangements d'un n ensemble p à p est
$$A^p_n = n(n-1)\cdots(n-p+1) = \frac{n!}{(n-p)!}$$

Application 12 : Le nombre de tirages ordonnés sans remise de p boules parmi n boules est A^p_n.

Définition 13 : On appelle permutation d'un n ensemble E, tout arrangement de E à n. On note $S(E)$ leur ensemble

Proposition 14 : $|S(E)| = n! = A^n_n$.

Définition 15 : Soit $p \in [\![1, n]\!]$. On appelle combinaison toute partie à p éléments d'un ensemble à n éléments. On note C^p_n ou $\binom{n}{p}$ le nombre de combinaisons de n éléments p à p.

Proposition 16 : $\binom{n}{p} = \frac{n(n-1)\times\cdots\times(n-p+1)}{1\times 2\times\cdots\times p} = \frac{n!}{p!(n-p)!}$

Proposition 17 : i) $\binom{n}{p} = \binom{n}{n-p}$ ii) $\binom{n}{p} = \binom{n-1}{p} + \binom{n-1}{p-1}$
iii) $\binom{n}{p} = \frac{n}{p}\binom{n-1}{p-1}$ iv) $\binom{n}{p} = \frac{n}{n-p}\binom{n-1}{p} = \frac{n-p+1}{p}\binom{n}{p-1}$

Application 18 : Une course à 20 chevaux a 1140 tiercés.

Théorème 19 : Soit A un anneau, a et $b \in A$ tels que $ab = ba$. Alors
$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$ (Formule du binôme de Newton).

Application 20 : $(1+1)^n = \sum_{i=0}^{n} \binom{n}{i} 1^i$, on déduit $\sum_{0}^{n} k = \frac{n(n+1)}{2}$ $\sum_{0}^{n} k^2 = \frac{n(n+1)(2n+1)}{6}$.

II Le dénombrement en algèbre et en théorie des corps.

A Actions de groupes Rom 1.1 1.6+exo Per 3.4

Définition 21 : Soit G un groupe. On dit que G opère à gauche sur E si on a une application : $G \times E \to E$ $(g, x) \mapsto g \cdot x$ telle que :
$\begin{cases} \forall x \in E,\ 1 \cdot x = x \\ \forall (g, g', x) \in G^2 \times E,\ g \cdot (g' \cdot x) = (gg') \cdot x \end{cases}$

Exemple 22 : G agit sur lui-même par translation à gauche : $\begin{matrix} G \times G \to G \\ (g, h) \mapsto gh \end{matrix}$

Théorème 23 : Soit G un groupe fini d'ordre n, H un groupe de G.
Alors $|H| \mid |G|$.

Application 24 : (Lemme des bergers) Soit A, B deux ensembles finis, $\varphi : A \to B$ application telle que pour tout $x \in B$, $|\varphi^{-1}(x)| = n$. Alors $|A| = n|B|$

Définition 25 : Soit G opérant sur E, $x \in E$. L'orbite de x sous l'action de G est $O(x) = \{g \cdot x,\ g \in G\}$. Le stabilisateur de x sous l'action de G est le sous-groupe $G_x = \{g \in G,\ g \cdot x = x\}$.

Théorème 26 : Soit G agissant sur E, $x \in E$. Alors $|O(x)| = \frac{|G|}{|G_x|}$

Corollaire 27 (équation des classes) : Soit G opérant sur E.
On note $O(x_1), \dots, O(x_n)$ toutes les orbites deux à deux distinctes.
Alors $|E| = \sum_{i=1}^{n} |O(x_i)| = \sum_{i=1}^{n} \frac{|G|}{|G_{x_i}|}$

Application 28 : Soit G opérant sur E. Pour tout $g \in G$ on note $\mathrm{Fix}(g) = \{x \in E,\ g \cdot x = x\}$
Alors le nombre d'orbite est $n = \frac{1}{|G|} \sum_{g \in G} |\mathrm{Fix}(g)|$. (Formule de Burnside).

Développement (Théorème de Wedderburn)

Tout corps fini est commutatif.

B Théorie des corps Per 3.2 4.5 1.5 Rom 13.6 13.7

Proposition 29 : Le cardinal d'un corps fini est une puissance d'un nombre premier : sa caractéristique.

Théorème 30 : Soit $p \in \mathcal{P}$. On pose $q = p^n$.
i) Il existe un corps $\mathbb{K}$ à q éléments, c'est le corps de décomposition du polynôme $X^q - X$ sur $\mathbb{F}_p$.
ii) En particulier, $\mathbb{K}$ est unique, à isomorphisme près. On le note $\mathbb{F}_q$.

Théorème 31 : Soit $m \in \mathbb{N}^*$. On a alors :
i) $|GL_n(\mathbb{F}_q)| = (q^n - 1)\cdot(q^n - q^{n-1})$
ii) $|SL_n(\mathbb{F}_q)| = (q^n-1)\dots(q^n - q^{n-2})q^{n-1} = N$
iii) $|PGL_n(\mathbb{F}_q)| = |SL_n(\mathbb{F}_q)| = N$
iv) $|PSL_n(\mathbb{F}_q)| = N/d$ où $d = n \wedge q-1$.

Développement Soit G un groupe fini et p un diviseur premier de $|G|$. Alors G contient au moins un p sous groupe de Sylow.

Corollaire 32 : Si $|G| = p^\alpha m$, $p \nmid m$ alors G contient des sous groupes d'ordre p^i $\forall i \leq \alpha$.

Application 33 : Les p Sylow sont tous conjugués (et donc leur nombre k divise m) et on a $k \equiv 1 \ [p]$ (donc k divise m).

Définition 34 : On pose $\mathbb{F}_q^2 = \{x \in \mathbb{F}_q, \exists y \in \mathbb{F}_q, x = y^2\}$ les carrés de $\mathbb{F}_q$.

Proposition 35 : i) pour $p = 2$ on a $\mathbb{F}_q^2 = \mathbb{F}_q$.
ii) Pour $p > 2$ on a $|\mathbb{F}_q^2| = \frac{q+1}{2}$.

Proposition 36 (caractérisation des carrés) On suppose $p > 2$, alors :
$x \in \mathbb{F}_q^{*2} \iff x^{\frac{q-1}{2}} = 1$.

Corollaire 37 : -1 est un carré dans $\mathbb{F}_q \iff q \equiv 1 \ [4]$.

Définition 38 : Pour tout $a \in \mathbb{F}_p^{*}$, le symbole de Legendre est l'entier :
$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{si } a \in \mathbb{F}_p^{*2} \\ -1 & \text{sinon} \end{cases}$

Proposition 39 : $|\{x \in \mathbb{F}_p, ax^2 = 1\}| = \begin{cases} 2 \text{ si } a \in \mathbb{F}_p^{*2} \\ 0 \text{ sinon} \end{cases}$

Théorème 40 (loi de réciprocité quadratique) Pour tout nombre premier impair $q \neq p$ on a : $\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$

III Fonctions arithmétiques multiplicatives

Définition 41 : $f : \mathbb{N}^* \to \mathbb{C}$ est dite multiplicative si $\forall m_1, m_2 \in \mathbb{N}$, $m_1 \wedge m_2 = 1 \Rightarrow f(m_1 m_2) = f(m_1) f(m_2)$. Per p 99

A Indicatrice d'Euler Rom 10.2

Définition 42 : On appelle fonction d'Euler et on note $\varphi(m)$ le nombre d'entiers x tels que $1 \leq x \leq m$ et $x \wedge m = 1$.

Remarque 43 : On a $\varphi(m) = |(\mathbb{Z}/m\mathbb{Z})^*|$.

Exemple 44 : Soit $p \in \mathcal{P}$, alors $\varphi(p) = p - 1$

Théorème 45 (Euler) Pour tout entier a tel que $a \wedge m = 1$, on a $a^{\varphi(m)} \equiv 1 \ [m]$.

Corollaire 46 (Fermat) Soit $p \in \mathcal{P}$ et $a \in \mathbb{N}$ tel que $a \wedge p = 1$. Alors $a^{p-1} \equiv 1 \ [p]$ et pour tout $a \in \mathbb{N}$, $a^p \equiv a \ [p]$

Théorème 47 : Pour tout $m \geq 2$ on a $m = \sum_{d \mid m} \varphi(d)$

B Fonction de Möbius Per 3.7 exo (p 85)

Définition 48 : On définit $\mu : \mathbb{N}^* \to \{0, 1, -1\}$ comme suit :
i) $\mu(1) = 1$
ii) $\mu(m) = 0$ si m contient un facteur carré
iii) $\mu(p_1 \dots p_n) = (-1)^n$ si $p_1, \dots, p_n$ sont des nombres premiers distincts

Proposition 49 : μ est multiplicative.

Proposition 50 : $\forall m \in \mathbb{N}^*$, $m \neq 1$, on a $\sum_{d \mid m} \mu(d) = 0$

Théorème 51 (formule d'inversion de Möbius)
Soit $f : \mathbb{N}^* \to A$ une application où A désigne un groupe abélien noté additivement.
On pose $g(m) = \sum_{d \mid m} f(d)$. Alors $f(m) = \sum_{d \mid m} \mu\left(\frac{m}{d}\right) g(d)$.

Application 52 : Pour $g = 1$ et $\alpha = \varphi$ on a pour tout $m \in \mathbb{N}^*$:
$\varphi(m) = \sum_{d \mid m} \mu\left(\frac{m}{d}\right) d$.

IV Séries génératrices

Lisses ?

Quoi mettre ? Lien avec les probas !

Références :

Mathématiques pour le CAPES et l'agrégation interne Jean de Biasi JdB
Daniel Perrin Cours d'Algèbre Per
Rombaldi Mathématiques pour l'agrégation Rom.