190 — Méthodes combinatoires, problèmes de dénombrement

Soit $E$ un ensemble, $n \in \mathbb{N}$.

# I] Méthodes ensemblistes et dénombrement élémentaire

## 1] Cardinal d'un ensemble fini

I.1.1

**Définition 1 :** On dit que $E$ est fini et 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 :** Soit $A, B$ deux ensembles, finis.
Alors : $|A \cup B| = |A| + |B| - |A \cap B|$

**Corollaire 4 :** Soit $(E_i)_{i=1}^{n}$ $n$ ensembles finis 2 à 2 disjoints.
Alors : $\left|\bigcup_{i=1}^{n} E_i\right| = \sum_{i=1}^{n} |E_i|$

**Corollaire 5 :** (formule du crible) Soit $(E_i)_{i=1}^{n}$ $n$ ensembles finis.
Alors : $\left|\bigcup_{i=1}^{n} E_i\right| = \sum_{i=1}^{n} |E_i| - \sum_{1 \le i < j \le n} |E_i \cap E_j| + \sum_{1 \le i < j < k \le n} |E_i \cap E_j \cap E_k| + \dots + (-1)^{n-1} \left|\bigcap_{1 \le i \le n} E_i\right|$

I.1.2 I.1.4 [DeB.]

**Application 6 :** Il y a 684 nombres à 3 chiffres contenant au moins l'un des chiffres 0 ; 3 ; 6 ; 9.

**Théorème 7 :** Soit $(A_i)_{i=1}^{p}$ ensembles finis
Alors : $|A_1 \times \dots \times A_p| = \prod_{i=1}^{p} |A_i|$

**Application 8 :** Le cardinal de l'ensemble des applications d'un ensemble fini $X$ dans $Y$ un autre est : $|Y|^{|X|}$.

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

## 2] Arrangements, permutations, combinaisons

I.1.3 [DeB.]

**Définition 10 :** Soit $E$ ensemble à $n$ éléments, $p \in [\![1;n]\!]$. Un arrangement de $E$ $p$ à $p$ ou un $p$-arrangement 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 de $p$-arrangements d'un ensemble à $n$ éléments est : $A_n^p = (n) \times (n-1) \times \dots \times (n-p+1) = \frac{n!}{(n-p)!}$

**Application 12 :** Le nombre de tirages de $p$ boules parmi $n$ boules sans remise possibles est de $A_n^p$

**Définition 13 :** Soit $E$ ensemble à $n$ éléments. On appelle permutation de $E$ tout $n$-arrangement de $E$. Notés $S(E)$.

**Proposition 14 :** $|S(E)| = A_n^n = n!$

I.1.3 I.2 [DeB.]

**Définition 15 :** Toute partie à $p$ éléments d'un ensemble à $n$ éléments est appelée combinaison. On note $C_n^p$ ou $\binom{n}{p}$ ~~une telle partie~~ le nombre de $p$ combinaisons parmi $n$.

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

**Propriétés 17 :** (1) $\binom{n}{p} = \binom{n-1}{p} + \binom{n-1}{p-1}$
(2) $\binom{n}{p} = \binom{n}{n-p}$ (3) $\binom{n}{p} = \frac{n}{p}\binom{n-1}{p-1} = \frac{n}{n-p}\binom{n-1}{p} = \frac{n-p+1}{p}\binom{n}{p-1}$

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

**Théorème 19 :** Soit $\mathbb{A}$ un anneau, $a, b \in \mathbb{A}$ qui commutent.
Alors : $(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$

**Application 20 :** $(k+1)^n = \sum_{i=0}^{n} \binom{n}{i} k^i$ ce qui permet le calcul de $\sum_{k=1}^{n} k = \frac{n(n+1)}{2}$, $\sum_{k=1}^{n} k^2 = \frac{n(n+1)(2n+1)}{6}$, $\sum_{k=1}^{n} k^3 = \left[\frac{n(n+1)}{2}\right]^2$

# II] Méthodes en théorie des groupes

## 1] Dénombrement en théorie des groupes

I.6 [Ram.] I.1

**Définition 21 :** Soit $G$ un groupe. On dit que le groupe $G$ agit sur $E$ s'il existe un morphisme $\varphi : G \to \mathfrak{S}(E)$, $g \mapsto [E \to E, x \mapsto g.x]$

**Exemple 22 :** $G$ agit sur lui même par translation à gauche : pour tout $g \in G$, $h \in G$, $g.h = gh$.

**Théorème 23 :** Soit $G$ groupe fini d'ordre $n$, $H$ sous-groupe de $G$
Alors : $|H| \mid |G|$

I.6 [Rom]

**Application 24 :** (lemme des bergers) Soit $A, B$ deux ensembles finis, $\varphi : A \to B$ application telle que pour tout $x \in B$, $|\varphi^{-1}(x)| = n$. appliquer Lagrange à $\varphi : G \to G/H$

**Alors :** $|A| = n|B|$

**Définition 25 :** Soit $G$ groupe agissant sur $E$, soit $x \in E$.
L'orbite de $x$ sous l'action de $G$ est : $Orb(x) = \{g.x \mid g \in G\}$.
Le stabilisateur de $x$ sous l'action de $G$ est : $Stab(x) = \{g \in G \mid g.x = x\}$.

**Théorème 26 :** Soit $G$ groupe agissant sur $E$, $x \in E$.
**Alors :** $|Orb(x)| = \dfrac{|G|}{|Stab(x)|}$

**Corollaire 27 :** (équation aux classes) Soit $G$ agissant sur $E$, soit $Orb(x_1), \dots, Orb(x_r)$ toutes les orbites 2 à 2 distinctes.
**Alors :** $|E| = \sum_{i=1}^{r} |Orb(x_i)| = \sum_{i=1}^{r} \dfrac{|G|}{Stab(x_i)}$

**Application 28 :** (formule de Burnside) Soit $G$ agissant sur $E$.
Pour tout $g \in G$, on note $Fix(g) = \{x \in E \mid g.x = x\}$.
**Alors :** Le nombres d'orbites sous l'action est : $\dfrac{1}{|G|} \sum_{g \in G} |Fix(g)|$
(*) (voir fin)

## 2) Dénombrement de cardinaux des groupes linéaires

Soit $p$ premier, $n \in \mathbb{N}^*$ et $q = p^\alpha$,

IV.5 [Rer]

**Proposition 29 :** (1) $|GL_n(\mathbb{F}_q)| = (q^n - 1) \times (q^n - q) \times \dots \times (q^n - q^{n-1})$
(2) $|SL_n(\mathbb{F}_q)| = (q^n - 1) \times (q^n - q) \times \dots \times (q^n - q^{n-2}) \times q^{n-1}$
(3) $|PGL_n(\mathbb{F}_q)| = |SL_n(\mathbb{F}_q)|$
(4) $|PSL_n(\mathbb{F}_q)| = \dfrac{|SL_n(\mathbb{F}_q)|}{PGCD(n; q-1)}$

**Application 30 :** On a les isomorphismes suivants :
(1) $GL_2(\mathbb{F}_2) = SL_2(\mathbb{F}_2) = PSL_2(\mathbb{F}_2) \simeq S_3$
(2) $PGL_2(\mathbb{F}_3) \simeq S_4$ et $PSL_2(\mathbb{F}_3) \simeq A_4$
(3) $PGL_2(\mathbb{F}_4) = PSL_2(\mathbb{F}_4) \simeq A_5$
(4) $PGL_2(\mathbb{F}_5) \simeq S_5$ et $PSL_2(\mathbb{F}_5) \simeq A_5$

## 3) Dénombrer pour simplifier

I.5 [Rer]

**Définition 31 :** Soit $G$ groupe de cardinal $n = p^\alpha m$ avec $p \nmid m$. On appelle $p$-sous-groupe de Sylow (ou $p$-Sylow) de $G$ tout sous-groupe de cardinal $p^\alpha$.

**Exemple 32 :** Soit $P = \{A = (a_{i,j}) \in GL_n(\mathbb{F}_q) \mid a_{i,j} = 0 \text{ si } i > j \text{ et } a_{i,i} = 1\}$
$P$ est un $p$-Sylow de $GL_n(\mathbb{F}_q)$ de cardinal $p^{\frac{n(n-1)}{2}}$.

**Lemme 33 :** Soit $G$ groupe tel que $|G| = n = p^\alpha m$ avec $p \nmid m$, soit $H$ un sous-groupe de $G$ et $S$ un $p$-Sylow de $G$.
**Alors :** il existe $a \in G$ tel que $aSa^{-1} \cap H$ soit un $p$-Sylow de $H$.

**Théorème 34 :** (de Sylow) Soit $G$ groupe tel que $|G| = p^\alpha m$ avec $p \nmid m$
**Alors :** (1) Si $H$ est un $p$-groupe de $G$, alors il existe un $p$-Sylow $S$ tel que $H \subset S$
(2) Les $p$-Sylow sont tous conjugués
(3) $n_p \equiv 1 \mod (p)$ et $n_p \mid m$

**Corollaire 35 :** Soit $S$ $p$-Sylow de $G$.
**Alors :** $S \triangleleft G$ ssi $S$ est l'unique $p$-Sylow de $G$ ssi $n_p = 1$

**Application 36 :** Un groupe d'ordre 63 n'est pas simple.

# III) Méthodes utilisant des fonctions remarquables et partition d'un entier à parts fixées

## 1) Fonction indicatrice d'Euler

X.2 [Rom]

**Définition 37 :** On appelle fonction indicatrice d'Euler la fonction qui associe à tout entier naturel non-nul $n$, le nombre $\varphi(n)$ d'entiers compris entre 1 et $n$ qui sont premiers avec $n$.

**Théorème 38 :** Soit $a \in \mathbb{Z}$.
**Alors :** $\bar{a} \in (\mathbb{Z}/n\mathbb{Z})^\times$ ssi $a \wedge n = 1$ ssi $\mathbb{Z}/n\mathbb{Z} = \langle \bar{a} \rangle$

X.2

**Théorème 39 :** (d'Euler) Pour tout entier $a$ tel que $a \wedge n = 1$, on a : $a^{\varphi(n)} \equiv 1 \mod (n)$

[Rom]

**Corollaire 40 :** (petit théorème de Fermat) Pour $p$ premier, avec $a$ on a : $a^{p-1} \equiv 1 \mod (p)$

**Théorème 41 :** Pour $n \geq 2$, $n = \sum_{d \in \mathcal{D}_n} \varphi(d)$ $\mathcal{D}_n$ diviseurs de $n$

## 2) Fonction de Möbius

XI.7

**Définition 42 :** En notant $n = \prod^{r} p_i^{\alpha_i}$ la décomposition en facteurs premiers de $n$, on définit la fonction de Möbius par : pour tout $n \in \mathbb{N}^*$, $\mu(n) = \begin{cases} 1 & \text{si } n = 1 \\ (-1)^r & \text{si } n = \prod^{r} p_i \\ 0 & \text{sinon} \end{cases}$

**Lemme 43 :** Pour tout $n \in \mathbb{N}^*$, $\sum_{d \mid n} \mu(d) = \begin{cases} 1 & \text{si } n = 1 \\ 0 & \text{si } n \geq 2 \end{cases}$

[Rom]

**Théorème 44 :** (formule d'inversion de Möbius) Soit $u, v \in \mathbb{R}^{\mathbb{N}^*}$.
Alors pour tout $n \in \mathbb{N}^*$, $u(n) = \sum_{d \mid n} v(d)$ ssi pour tout $n \in \mathbb{N}^*$, $v(n) = \sum_{d \mid n} \mu(d) u\left(\frac{n}{d}\right)$

**Application 45 :** Pour $u = \mathbb{1}$ et $v = \varphi$, on a la formule : pour tout $n \in \mathbb{N}^*$, $\varphi(n) = \sum_{d \mid n} \mu(d) \frac{n}{d}$

## 3) Utilisation des séries entières pour dénombrer

[FGN An 2]

**Théorème 46 :** (partition d'un entier à parts fixées)
Soit $(a_1, \dots, a_k) \in \mathbb{N} \setminus \{0\}$ premiers entre eux, soit $n \in \mathbb{N}^*$ et $\left(u_n := \operatorname{card} \{(x_1, \dots, x_k) \in \mathbb{N}^k \mid a_1 x_1 + \dots + a_k x_k = n\}\right)_{n \in \mathbb{N}}$
Alors : $u_n \sim \frac{1}{a_1 \times \dots \times a_k} \times \frac{n^{k-1}}{(k-1)!}$

(*) A rajouter :

**Théorème :** (de Dixon) Soit $G$ groupe non-abélien fini.
Alors : la probabilité $p(G)$ pour que deux éléments de $G$ tirés uniformément et indépendamment comme tout vérifie : $p(G) \leq \frac{5}{8}$.

[Les]

**Application :** Soit $\mathbb{D}_8$ groupe diédral à 8 éléments.
Alors : $p(\mathbb{D}_8) = \frac{5}{8}$.

Références :


[DeBi] Mathématiques pour le CAPES et l'Agrégation Interne – de Biasi

[Rom] Mathématiques pour l'agrégation Algèbre et Géométrie – Rombaldi

[Per] Cours d'Algèbre – Perrin

[FGN An2] Exercices de mathématiques Oraux X-ENS Analyse 2 – Francinou

[Les] 131 développements pour l'oral – Lesesvre