Leçon 190 - Méthodes combinatoires, problèmes de dénombrement.

Extrait du rapport de jury

Il est nécessaire de dégager clairement différentes méthodes de dénombrement et de les illustrer d'exemples significatifs. De nombreux domaines de mathématiques sont concernés par des problèmes de dénombrement, cet aspect varié du thème de la leçon doit être mis en avant. L'utilisation de séries génératrices est un outil puissant pour le calcul de certains cardinaux. De plus, il est naturel de calculer des cardinaux classiques et certaines probabilités. Il est important de connaître l'interprétation ensembliste de la somme des coefficients binomiaux et ne pas se contenter d'une justification par le binôme de Newton. L'introduction des corps finis (même en se limitant aux cardinaux premiers) permet de créer un lien avec l'algèbre linéaire. Les actions de groupes peuvent également conduire à des résultats remarquables.
Pour aller plus loin, les candidates et candidats peuvent aussi présenter des applications de la formule d'inversion de Möebius ou de la formule de Burnside. Des candidats ayant un bagage probabiliste pourront explorer le champ des permutations aléatoires, en présentant des algorithmes pour générer la loi uniforme sur le groupe symétrique $\mathfrak{S}_n$ et analyser certaines propriétés de cette loi uniforme (points fixes, cycles, limite en ∞, ...)

Présentation de la leçon

Je vais vous présenter la leçon 190 intitulée : "Méthodes combinatoires, problèmes de dénombrement.". Le nombre apparaissant comme la structure abstraite la plus primitive de l'esprit, la plus familière également, il est naturel de chercher à saisir l'étendue d'un domaine, d'un problème, d'un objet en en condensant la complexité en un nombre : c'est tout l'enjeu de la combinatoire, quasiment omniprésente dans les problèmes mathématiques. L'intérêt pour la combinatoire et le dénombrement explose avec l'étude des jeux de hasard, motivés par le chevalier de Méré et étudiés par Fermat et Pascal, et trouvant de nombreuses applications modernes en théorie des jeux combinatoires et en informatique. Nous allons donner dans cette leçon différentes utilisations de la combinatoire aussi bien en algèbre qu'en analyse.
Dans un premier temps on s'intéresse au dénombrement et à la combinatoire. Dans un premier point on fait quelques rappels sur les ensembles finis et les cardinaux, notamment avec les relations d'inclusion ainsi que d'union d'ensembles et de produit cartésien d'ensembles. Dans un deuxième point, on étudie plus spécifiquement les relations entre fonctions et cardinaux. On commence tout d'abord par énoncer la proposition 8 qui nous permet ensuite de démontrer que lorsqu'on a une application entre deux ensembles finis, alors il y a équivalence entre l'injectivité, la surjectivité et la bijectivité. On continue ensuite en donnant le cardinal des applications de E dans F ainsi que le nombre de parties de E et des exemples. Enfin dans une dernière sous-partie, on s'intéresse à la combinatoire avec les notions d'arrangement et de combinaison qui font apparaître la notion de coefficient binomial ainsi que plusieurs relations parfois utiles dans les calculs comme on peut le voir dans l'exemple 28.
Dans un deuxième temps, on s'intéresse au dénombrement en algèbre. Tout d'abord, on s'attarde sur l'indicatrice d'Euler où l'on donne sa définition, ainsi qu'un moyen de calculer $\varphi(n)$ en fonction de sa décomposition en facteurs premiers puis différentes interprétations de ce nombre. Dans un deuxième point on étudie la combinatoire du côté des groupes et des actions de groupes avec tout d'abord un rappel sur l'ordre d'un groupe et d'un élément puis sur le théorème de Lagrange et le premier théorème d'isomorphisme qui permettent de donner des informations sur le cardinal d'un sous-groupe dans le cas d'un groupe fini comme par exemple dans le cas de $\mathfrak{S}_n$. On continue avec les actions de groupes en donnant quelques résultats remarquables comme le théorème de Cayley ainsi que l'équation aux classes et la formule de Burnside et on donne des applications avec le groupe des isométries du cube et le dénombrement des endomorphismes nilpotents de E grâce à la décomposition de Fitting. On conclut cette sous-partie avec les théorèmes de Sylow qui nous sont souvent utiles pour montrer qu'un groupe est simple en dénombrant ses p-Sylows. On termine enfin cette partie avec le dénombrement des polynômes unitaires irréductibles sur $\mathbb{F}_q$. Pour cela on introduit la fonction de Möbius ainsi que deux de ses propriétés avant d'en arriver au nombre de polynômes unitaires irréductibles sur $\mathbb{F}_q$ (ce qui redémontre au passage qu'il existe toujours un corps à p^n éléments).
Finalement, on conclut cette leçon par une dernière partie consacrée aux séries

génératrices. On donne tout d'abord des premiers exemples avec la définition d'une série génératrice ainsi que plusieurs exemples comme par exemple les nombres de Bell et de Catalan. On donne ensuite une application des séries formelles dans un deuxième point avec le dénombrement du nombre de dérangements de $\mathfrak{S}_n$ ainsi qu'une application aux probabilités avec le nombre de points fixes d'une permutation aléatoire.

Plan général

Cours détaillé

I Dénombrement et combinatoire

Dans toute cette sous-partie, on considère E un ensemble fini non vide.

I.1 Ensembles finis et cardinaux

Proposition 1 : [Deschamps (1), p.1369]
Soit F un sous-ensemble de E.
F est fini et $\text{Card}(F) \leq \text{Card}(E)$.
De plus, on a $\text{Card}(F) = \text{Card}(E)$ si, et seulement si, $F = E$.

Corollaire 2 : [Deschamps (1), p.1370]
Si F est inclus dans E et que F est infini, alors E est infini.

Proposition 3 : [Deschamps (1), p.1370 + 1371]
Soient A et B deux parties de E.
* $\text{Card}\left(\complement_E(A)\right) = \text{Card}(E) - \text{Card}(A)$.
* $\text{Card}(A \cup B) = \text{Card}(A) + \text{Card}(B) - \text{Card}(A \cap B)$.
* Si de plus $A \subseteq B$, alors $\text{Card}(B) = \text{Card}(A) + \text{Card}(B \backslash A)$.

Proposition 4 : Formule de crible de Poincaré [Deschamps (1), p.1371] :
Soient $E_1, ..., E_n$ des ensembles finis.

$$\text{Card}\left(\bigcup_{i=1}^{n} A_i\right) = \sum_{k=1}^{n} \left((-1)^{k-1} \sum_{1 \leq i_1 < i_2 < ... < i_n \leq n} \text{Card}(A_{i_1} \cap A_{i_2} \cap ... \cap A_{i_k}) \right)$$

Corollaire 5 : [Deschamps (1), p.1370]
Soient $E_1, ..., E_n$ une partition de E.

$$\text{Card}(E) = \text{Card}\left(\bigsqcup_{i=1}^{n} A_i\right) = \sum_{i=1}^{n} \text{Card}(E_i)$$

Proposition 6 : [Deschamps (1), p.1375]
Si $E_1, ..., E_n$ sont des ensembles finis, alors $\prod_{i=1}^{n} E_i$ est un ensemble fini et $\text{Card}\left(\prod_{i=1}^{n} E_i\right) = \prod_{i=1}^{n} \text{Card}(E_i)$.
En particulier, pour tout ensemble E fini et tout entier naturel non nul n, on a $\text{Card}(E^n) = \text{Card}(E)^n$.

Exemple 7 : [Deschamps (1), p.1375]
Il y a 16 777 216 couleurs codables en `RGB`.

I.2 Fonctions et cardinaux

Proposition 8 : [Deschamps (1), p.1372]
Soient E et F deux ensembles finis non vides et $f : E \longrightarrow F$.
$*$ 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 $\text{Card}(E) = \text{Card}(F)$.

Exemple 9 : Principe des tiroirs [Deschamps (1), p.1372] :
Soit $n \in \mathbb{N}^*$.
Parmi $n+1$ réels de l'intervalle $[0;1]$, il y en a au moins deux dont la distance est inférieure à $\frac{1}{n}$.

Théorème 10 : [Deschamps (1), p.1373]
Soient E et F deux ensembles finis de même cardinal et $f : E \longrightarrow F$.
Les assertions suivantes sont équivalentes :
$*$ f est injective. $*$ f est surjective. $*$ f est bijective.

Exemple 11 : [Deschamps (1), p.1373]
Si $(G, *)$est un groupe et H une partie finie non vide de G et stable pour la loi $*$, alors $(H, *|_H)$ est un sous-groupe de $(G, *)$.

Proposition 12 : [Deschamps (1), p.1375]
Soient E et F deux ensembles non vides de cardinaux respectifs n et p.
L'ensemble F^E est fini et $\text{Card}\left(F^E\right) = (\text{Card}(F))^{\text{Card}(E)} = n^p$.

Exemple 13 : [Deschamps (1), p.1376]
Soit $n \in \mathbb{N}^*$.
$*$ Pour $n \geq 2$, il y a $2^n - 2$ surjections de $[\![1; n]\!]$ dans $[\![1; 2]\!]$.
$*$ Pour $n \geq 3$, il y a $3^n - 3 \times 2^n + 3$ surjections de $[\![1; n]\!]$ dans $[\![1; 3]\!]$.

Proposition 14 : [Deschamps (1), p.1376]
Si E est un ensemble à n éléments, alors $\mathcal{P}(E)$ est fini et $\text{Card}(\mathcal{P}(E)) = 2^n$.

Exemple 15 : [Deschamps (1), p.1376]
Soit E un ensemble fini de cardinal n.
Le nombre de couples (A, B) de parties de E telles que $A \subseteq B$ est 3^n.

I.3 Combinatoire

Définition 16 : p-arrangement [Deschamps (1), p.1376] :
On considère p un entier naturel non nul et E un ensemble non vide.
On appelle **p-arrangement d'éléments de** E toute p-liste d'éléments de E deux à deux distincts.

Théorème 17 : [Deschamps (1), p.1376 + 1377]
Soient E un ensemble à n éléments et p un entier naturel non nul.
Le nombre de p-arrangements d'éléments de E est :

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

Exemple 18 : [Deschamps (1), p.1377]
$*$ Le nombre de mots de p lettres distinctes qu'on peut former avec un alphabet de n lettres est A_n^p.
$*$ Une course de chevaux comporte 20 partants. Le nombres de résultats possibles de tiercés dans l'ordre est $A_{20}^3 = 20 \times 19 \times 18 = 6840$.

Proposition 19 : [Deschamps (1), p.1377]
Le nombre d'injections d'un ensemble E de cardinal p dans un ensemble F de cardinal n est A_n^p.

Définition 20 : p-combinaison [Deschamps (1), p.1378] :
On considère un ensemble E de cardinal fini non vide.
On appelle **p-combinaison d'éléments de** E tout sous-ensemble fini de E de cardinal p.

Remarque 21 : [Deschamps (1), p.1379]
La différence entre arrangement et combinaison tient à ce que l'un est ordonné alors que l'autre pas.

Théorème 22 : [Deschamps (1), p.1378]
Soient E un ensemble non vide de cardinal n et p un entier naturel.
Le nombre de sous-ensemble de cardinal p de E est $C_n^p = \binom{n}{p} = \frac{A_n^p}{p!}$.

Exemple 23 : [Deschamps (1), p.1379 + 1380]
$*$ On désire organiser un match de foot entre $2n$ équipes de basket, chacune disputant un match. Il y a $u_n = \frac{(2n)!}{2^n n!}$ façons d'organiser ces matchs (c'est-à-dire d'apparier les équipes deux à deux).
$*$ Il y a 720 anagrammes du mot "orange" et 60 anagrammes du mot "ananas".

Proposition 24 : [Deschamps (1), p.1380]
Soient n et p deux entiers naturels avec n non nul.
$*$ $\binom{n}{0} = \binom{n}{n} = 1$. $*$ $\binom{n}{1} = \binom{n}{n-1} = n$.
$*$ Si $p \in [\![0; n]\!]$, alors $\binom{n}{p} = \binom{n}{n-p}$.
$*$ Si $p \in [\![1; n]\!]$, alors $\binom{n}{p} = \binom{n-1}{p-1} + \binom{n-1}{p}$ (Formule de Pascal).

Proposition 25 : Formule du binôme de Newton [Deschamps (1), p.1381] :
Soient $(A,+,\times)$ un anneau quelconque et $a,b\in A$.
Si a et b commutent, alors pour tout $n\in\mathbb{N}$, on a : $(a+b)^n=\sum_{k=0}^{n}\binom{n}{k}a^kb^{n-k}$.

Corollaire 26 : Formule de Vandermonde [Deschamps (1), p.1381] :
Soient m,m et p trois entiers naturels.
On a la relation :

$$\sum_{k=0}^{p}\binom{m}{k}\binom{n}{p-k}=\binom{m+n}{p}$$

En particulier, on a : $\sum_{k=0}^{n}\binom{n}{k}^2=\binom{2n}{n}$.

Proposition 27 : [Deschamps (1), p.1382]
Si n est un entier naturel non nul et $p\in[\![1;n]\!]$, alors on a $p\binom{n}{p}=n\binom{n-1}{p-1}$.

Exemple 28 : [Deschamps (1), p.1382]

$$\sum_{k=0}^{n}k\binom{n}{k}=n2^{n-1},\ \sum_{k=0}^{n}k(k-1)\binom{n}{k}=n(n-1)2^{n-2}\text{ et }\sum_{k=0}^{n}k^2\binom{n}{k}=n(n+1)2^{n-2}$$

II Dénombrement en algèbre

II.1 Indicatrice d'Euler

Définition 29 : Indicatrice d'Euler [Berhuy, p.156] :
Pour tout $n\geq 1$, on note $\varphi(n)$ le nombre d'entiers de l'ensemble $[\![1;n]\!]$ qui sont premiers avec n et on appelle **indicatrice d'Euler** la fonction $\varphi:\mathbb{N}^*\longrightarrow\mathbb{N}^*$.

Proposition 30 : [Deschamps (2), p.13]
Si $n=\prod_{i=1}^{r}p_i^{k_i}$ (décomposition en facteurs premiers), alors on a :

$$\varphi(n)=\prod_{i=1}^{r}(p_i-1)p_i^{k_i-1}=n\prod_{i=1}^{r}\left(1-\frac{1}{p_i}\right)$$

Proposition 31 : [Deschamps (2), p.12]
Pour tout entier naturel $n\geq 1$, on a $n=\sum_{d|n}\varphi(d)$.

Proposition 32 : [Deschamps (2), p.27]
Pour tout $n\geq 1$, $\varphi(n)$ est égal :
* Au nombre d'inversibles de l'anneau $\mathbb{Z}/n\mathbb{Z}$.
* Au nombre de générateurs de l'anneau $\mathbb{Z}/n\mathbb{Z}$.
* Au nombre de racines n-ièmes qui sont primitives sur $\mathbb{C}$.

II.2 Groupes et actions de groupes

Dans toute cette sous-partie, on considère un groupe $(G,*)$ (plus simplement noté G par la suite) de neutre noté "e_G", X un ensemble non vide, un corps $\mathbb{K}$ commutatif fini à $q=p^r$ éléments (avec p un nombre premier et $r\in\mathbb{N}^*$) et E un $\mathbb{K}$-espace vectoriel de dimension finie $n>0$.

Définition 33 : Ordre d'un groupe et d'un élément [Berhuy, p.128 + 149] :
On considère G fini et $x\in G$.
* On appelle **ordre du groupe** G le cardinal de G.
* On appelle **ordre de** x le cardinal de $<x>$ et on le note $o(x)$.

Théorème 34 : Théorème de Lagrange [Berhuy, p.148] :
Soit H un sous-groupe de G.
Si G est fini, alors on a $\mathrm{Card}(G)=\mathrm{Card}(G/H)\,\mathrm{Card}(H)$.
En particulier, l'ordre de tout sous-groupe de G divise le cardinal de G et il en est de même pour l'ordre de tout élément de G.

Théorème 35 : Premier théorème d'isomorphisme [Berhuy, p.241] :
Soient H et K deux groupes et $f:H\longrightarrow K$ un morphisme de groupes.
Le morphisme de groupes $\overline{f}:H/\mathrm{Ker}(f)\longrightarrow K$ induit un isomorphisme de groupes $G/\mathrm{Ker}(f)\cong\mathrm{Im}(f)$.

Exemple 36 : [Berhuy, p.200 + 215]
Pour tout $n\in\mathbb{N}^*$, on a $\mathrm{Card}(\mathfrak{S}_n)=n!$ et $\mathrm{Card}(\mathfrak{A}_n)=\frac{n!}{2}$.

Définition 37 : Action de groupe [Berhuy, p.169] :
On appelle **action (à gauche) de G sur X** toute application :

$$\cdot:\left|\begin{array}{ccc}G\times X&\longrightarrow&X\\(g,x)&\longmapsto&g\cdot x\end{array}\right.$$

telle que :
* Pour tout $x\in X$, $e_G\cdot x=x$.
* Pour tous $(g,g')\in G^2$ et $x\in X$, $g\cdot(g'\cdot x)=(gg')\cdot x$

Remarque 38 : [Berhuy, p.170]
La donnée d'une action de G sur X est équivalente à la donnée d'un morphisme de groupes de G dans $\mathfrak{S}_X$.
En effet, G agit sur X via $\cdot$ si, et seulement si, l'application

$$\Psi:\left|\begin{array}{ccc}G&\longrightarrow&\mathfrak{S}_X\\g&\longmapsto&\sigma_g:\left|\begin{array}{ccc}X&\longrightarrow&X\\x&\longmapsto&g\cdot x\end{array}\right.\end{array}\right.$$

est un morphisme de groupes.

On considère jusqu'à la fin de toute cette sous-partie que G agit sur X via une action notée "$\cdot$".

Théorème 39 : Théorème de Cayley [Berhuy, p.177] :
Si G est d'ordre n, alors G est isomorphe à un sous-groupe de $\mathfrak{S}_n$.

Définition 40 : Stabilisateur, orbite et points fixes [Berhuy, p.172 + 173] :
On considère $x \in X$ et $g \in G$.
On appelle :
* **stabilisateur de** x l'ensemble $\mathrm{Stab}_G(x) = \{g \in G \text{ tq } g \cdot x = x\}$.
* **orbite de** x l'ensemble $\mathrm{Orb}(x) = \{g \cdot x,\ x \in X\}$.
* **points fixes de** g l'ensemble $\mathrm{Fix}(g) = \{x \in X \text{ tq } g \cdot x = x\}$.

Lemme 41 : Équation aux classes [Berhuy, p.173] :
Si X est un ensemble fini et que Ω est un système de représentants de X, on a alors $\mathrm{Card}(X) = \sum_{\omega \in \Omega} \mathrm{Card}(\mathrm{Orb}(\omega))$.

Corollaire 42 : Équation aux classes pour les p-groupes [Berhuy, p.181] :
Si G un p-groupe non trivial, alors $Z(G)$ est non trivial.

Développement 1 : [cf. COMBES]

Théorème 43 : [Combes, p.175]
On a $\mathrm{Isom}^+(\mathcal{C}) \cong \mathfrak{S}_4$ et $\mathrm{Isom}(\mathcal{C}) \cong \mathfrak{S}_4 \times \mathbb{Z}/2\mathbb{Z}$.

Proposition 44 : [Rombaldi, p.156]

$$\mathrm{Card}(\mathrm{GL}_n(\mathbb{F}_q)) = \prod_{k=0}^{n-1} \left(q^n - q^k\right) \text{ et } \mathrm{Card}(\mathrm{SL}_n(\mathbb{F}_q)) = \frac{1}{q-1} \prod_{k=0}^{n-1} \left(q^n - q^k\right)$$

Lemme 45 : [Caldero (1), p.74]
Les suites $\left(\mathrm{Ker}\left(u^k\right)\right)_{k\in\mathbb{N}}$ et $\left(\mathrm{Im}\left(u^k\right)\right)_{k\in\mathbb{N}}$ sont respectivement croissante et décroissante au sens de l'inclusion.
De plus, ces deux suites sont stationnaires à partir d'un certain rang $n_0 \in \mathbb{N}$.

Lemme 46 : Lemme de Fitting [Caldero (1), p.74] :
Avec les notations du lemme précédent, on a $E = \mathrm{Ker}\left(u^{n_0}\right) \oplus \mathrm{Im}\left(u^{n_0}\right)$.
De plus, u induit un endomorphisme nilpotent sur $\mathrm{Ker}\left(u^{n_0}\right)$ et un automorphisme sur $\mathrm{Im}\left(u^{n_0}\right)$.

Définition 47 : Décomposition de Fitting [Caldero (1), p.74] :
La donnée de $((F,G),v,w)$ où $F = \mathrm{Ker}\left(u^{n_0}\right)$, $G = \mathrm{Im}\left(u^{n_0}\right)$, $v = u|_F$ et $w = u|_G$ avec $E = F \oplus G$, v nilpotent et w un automorphisme est appelée **décomposition de Fitting**.

Théorème 48 : [Caldero (1), p.74]
Il y a exactement $n_d = q^{d(d-1)}$ matrices nilpotentes de taille $d \times d$ à coefficients dans $\mathbb{K}$.

Exemple 49 :
En appliquant la formule à l'espace vectoriel $E = \mathbb{F}_2^2$ sur le corps $\mathbb{F}_2$, on trouve qu'il y a 4 matrices nilpotentes dans $\mathcal{M}_2(\mathbb{F}_2)$. Par un calcul direct, on trouve que ce sont les matrices :

$$\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \text{ et } \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$$

Proposition 50 : Formule de Burnside [Berhuy, p.176] :
Si G et X sont finis, que l'on note $\mathrm{Fix}(g) = \{x \in X \text{ tq } g \cdot x = x\}$ et Ω l'ensemble des orbites de X sous l'action de G, alors on a l'égalité :

$$\mathrm{Card}(\Omega) = \frac{1}{\mathrm{Card}(G)} \sum_{g \in G} \mathrm{Card}(\mathrm{Fix}(g))$$

Corollaire 51 : [Caldero (2), p.240]
Si G est un groupe non abélien d'ordre n possédant k classes de conjugaison, alors la probabilité p que deux éléments commutent est égale à $\frac{k}{n}$.

On suppose jusqu'à la fin de cette sous-partie que G est de cardinal fini.

Définition 52 : p-sous-groupe de G [Berhuy, p.311] :
On appelle **p-sous-groupe de** G tout sous-groupe de G de cardinal une puissance de p.

Désormais, on écrit $\mathrm{Card}(G) = p^m q$ où $p \nmid q$ et $m \in \mathbb{N}^*$.

Définition 53 : p-sous-groupe de Sylow de G [Berhuy, p.311] :
On appelle **p-sous-groupe de Sylow de** G (ou plus simplement p-Sylow) tout sous-groupe de G d'ordre p^m.

Théorème 54 : Théorème de Sylow [Berhuy, p.313] :
∗ Il existe des p-sous-groupes de Sylow de G et tout p-sous-groupe de G est contenu dans un p-Sylow.
∗ Le conjugué d'un p-Sylow est un p-Sylow et tous les p-Sylow de G sont conjugués entre eux. En particulier, si S est un p-Sylow de G, alors S est distingué dans G si, et seulement si, S est l'unique p-Sylow de G.
∗ Si n_p désigne le nombre de p-Sylow de G, alors $n_p \equiv 1\ [p]$ et $n_p | q$.

Exemple 55 : [Berhuy, p.315 + 328]
Tout groupe d'ordre 63 ou 255 n'est pas simple.

Corollaire 56 : [Berhuy, p.315]
Tout groupe d'ordre 33 cyclique.

Théorème 57 : Théorème de Cauchy [Berhuy, p.179] :
G possède au moins un élément d'ordre p.

II.3 Polynômes unitaires irréductibles sur $\mathbb{F}_q$

Définition 58 : Fonction de Möbius [Berhuy, p.151] :
On appelle **fonction de Möbius** la fonction μ définie par :

$$\mu : \left| \begin{array}{ccc} \mathbb{N}^* & \longrightarrow & \mathbb{Z} \\ n & \longmapsto & \begin{cases} (-1)^r & \text{si } n \text{ est produit de } r \text{ nombres premiers distincts} \\ 0 & \text{s'il existe un nombre premier } p \text{ tel que } p^2 \text{ divise } n \end{cases} \end{array} \right.$$

Développement 2 : [cf. FRANCINOU]

Lemme 59 : [Francinou, p.93]
Pour tout $n \in \mathbb{N}^*$, on a :

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{si } n = 1 \\ 0 & \text{si } n \geq 2 \end{cases}$$

Théorème 60 : Formule d'inversion de Möbius [Francinou, p.93] :
Soient A un groupe abélien et $f : \mathbb{N}^* \longrightarrow A$.
Si l'on pose $g(n) = \sum_{d|n} f(d)$, alors $f(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) g(d)$.

Théorème 61 : [Francinou, p.189]
Si l'on note $A(n,q)$ l'ensemble des polynômes irréductibles, unitaires et de degré n sur $\mathbb{F}_q$, alors $X^{q^n} - X = \prod_{d|n} \prod_{P \in A(d,q)} P(X)$

Corollaire 62 : [Francinou, p.189]
En notant $I(n,q) = \text{Card}(A(n,q))$, on a :

$$I(n,q) = \frac{1}{n} \sum_{d|n} \mu\left(\frac{n}{d}\right) q^d \text{ et } \forall q \geq 2,\ I(n,q) \underset{n \to +\infty}{\sim} \frac{q^n}{n}$$

Remarque 63 : [Berhuy, p.654]
On a donc en particulier pour tout $n, q \in \mathbb{N}^*$, $I(n,q) \geq 1$. Ainsi, il existe au moins un polynôme irréductible de degré quelconque n dans $\mathbb{F}_p$ (c'est-à-dire que $\mathbb{F}_{p^n}$ existe toujours en tant que corps).

III Séries génératrices

III.1 Premiers exemples

Définition 64 : Série génératrice :
On considère $\mathbb{K}$ un corps de caractéristique nulle et $(a_n)_{n \in \mathbb{N}} \in \mathbb{K}^{\mathbb{N}}$.
On appelle **série génératrice de** $(a_n)_{n \in \mathbb{N}}$ la série formelle $\sum_{n=0}^{+\infty} a_n X^n \in \mathbb{K}[[X]]$.

Proposition 65 : [Berhuy, p.707 + 712]
∗ L'ensemble $1 + X\mathbb{K}[[X]]$ est un sous-groupe de $\mathbb{K}[[X]]^\times$.
∗ Pour tous $\alpha \in \mathbb{K}^\times$ et $T_0 \in 1 + X\mathbb{K}[[X]]$, l'équation $T^\alpha = T_0$ (avec $T \in 1 + X\mathbb{K}[[X]]$) admet une unique solution.

Exemple 66 : [Gourdon, p.304 + 314 + Berhuy, p.719]
∗ Pour tous entiers naturel n et m, on a :

$$\sum_{\ell=0}^{n+m}\left(\sum_{k=0}^{n}\binom{n}{k}\binom{m}{\ell-k}\right)x^\ell=\sum_{\ell=0}^{m+n}\binom{n+m}{\ell}x^\ell$$

∗ Le nombre B_n de partitions de $[\![1;n]\!]$ est $B_n=\frac{1}{e}\sum_{k=0}^{+\infty}\frac{k^n}{k!}$ (nombres de Bell).
∗ Le nombre C_n de bons parenthésages du mot $a_0...a_n$ est $C_n=\frac{1}{n+1}\binom{2n}{n}$ (nombres de Catalan).

III.2 Utilisation des séries formelles

Théorème 67 : [Berhuy, p.714]
Soient $n\in\mathbb{N}$ et D_n le nombre de dérangements de $\mathfrak{S}_n$ (c'est-à-dire de permutations sans points fixes).
Pour tout entier naturel n, on a $n!=\sum_{k=0}^{n}\binom{n}{k}D_{n-k}$ et $D_n=n!\sum_{k=0}^{n}\frac{(-1)^k}{k!}$

Proposition 68 : [Caldero (2), p.303]
Soit $\mathbb{P}$ la probabilité uniforme sur $(\mathfrak{S}_n,\mathcal{P}(\mathfrak{S}_n))$.
Si F_n est la variable aléatoire réelle qui compte le nombre de points fixe de $\sigma\in\mathfrak{S}_n$, alors pour tout $r\in[\![0;n]\!]$ on a $\mathbb{P}(F_n=r)=\frac{\binom{n}{r}D_{n-r}}{\mathrm{Card}(\mathfrak{S}_n)}=\frac{1}{r!}\sum_{k=0}^{n-r}\frac{(-1)^k}{k!}$.
De plus, $(F_n)_{n\in\mathbb{N}^*}$ converge en loi vers la variable aléatoire Z qui suit une loi de Poisson de paramètre 1 et on a $\mathbb{E}(F_n)=\mathrm{Var}(F_n)=1$.

Remarques sur la leçon

— Les séries formelles jouent un rôle important en combinatoire et sont un outil puissant qu'il faut savoir maîtriser.

— On peut aussi parler du cas des carrés dans les corps finis et de parler de la loi de réciprocité quadratique.

Liste des développements possibles

— Dénombrement des endomorphismes nilpotents.

— Groupe des isométries du cube.

— Dénombrement des polynômes unitaires irréductibles sur $\mathbb{F}_q$.

Bibliographie

— Claude Deschamps, *Tout-en-un MPSI*.

— Grégory Berhuy, *Algèbre : le grand combat*.

— Claude Deschamps, *Tout-en-un MP/MP**.

— François Combes, *Algèbre et géométrie*.

— Jean-Étienne Rombaldi, *Mathématiques pour l'agrégation, Algèbre et géométrie*.

— Philippe Caldero, *Carnet de voyage en Algébrie*.

— Philippe Caldero, *Carnet de voyage en Analystan*.

— Serge Francinou, *Exercices de mathématiques pour l'agrégation, Algèbre 1*.

— Xavier Gourdon, *Les maths en tête, Algèbre et Probabilités*.