Leçon 190 : Méthodes combinatoires, problèmes de dénombrement.

1 Ensembles finis

Définition 1. Un ensemble E est fini si il existe un entier $n \in \mathbb{N}$ tel que E soit en bijection avec $\{1, \cdots, n\}$. On note alors $|E| = n$ son cardinal.

Théorème 2. *Si E est en bijection avec F alors $|E| = |F|$.*

Proposition 3. *Soient $N_1, \cdots, N_m$ des ensembles finis, alors $|N_1 \times \cdots \times N_m| = \prod_{i=1}^{m} |N_i|$.*

Application 4. *Si E et F sont deux ensembles, alors $|\mathcal{F}(E,F)| = |F|^{|E|}$, où $\mathcal{F}(E,F)$ désigne l'ensemble des applications de E dans F.*

Application 5. *Soit E un ensemble fini et $\mathcal{P}(E)$ l'ensemble des parties de E. Alors $|\mathcal{P}(E)| = 2^{|E|}$.*

Théorème 6 (Principe des tiroirs)**.** *Si E et F sont deux ensembles finis tels que $|E| > |F|$ et si $f : E \to F$ est une application de E dans F, alors il existe un élément de F qui admet au moins deux antécédents par f ; autrement dit il n'existe pas d'application injective de E dans F.*

Application 7. *L'équation $ax^2 + by^2 = 1$, où $a, b \neq 0$, admet au moins une solution dans $\mathbb{F}_q \times \mathbb{F}_q$.*

Proposition 8. *Soient A et B des ensembles finis tels que $A \cap B = \emptyset$. Alors $|A \cup B| = |A| + |B|$.*

Corollaire 9 (Lemme des bergers)**.** *Si un ensemble E possède une partition en p sous-ensembles ($E = \bigsqcup_{i=1}^{p} A_i$) contenant chacun r éléments, alors E contient $p \times r$ éléments.*

2 Arrangements et permutations

Définition 10. Un k-arrangement d'une partie fini E de cardinal n est une injection $\alpha : \{1, \cdots, k\} \to E$. On note $\mathcal{A}_k(E)$ l'ensemble des arrangements de N.

Proposition 11. $|\mathcal{A}_k(E)| = n(n-1)\cdots(n-k+1) = \frac{n!}{(n-k)!}$ *où* $n! = \prod_{k=1}^{n} k$ *et* $0! = 1$.

Application 12. *Notant $\mathfrak{S}_n$ l'ensemble des bijections de $\{1, \cdots, n\}$ dans lui même, on a $|\mathfrak{S}_n| = n!$.*

Définition 13. On note $\mathcal{P}_k(E)$ l'ensemble des sous-parties de E a k-éléments. On note aussi $\binom{n}{k} = |\mathcal{P}_k(E)|$ où $E = \{1, \cdots, n\}$.

Proposition 14. *Pour tout couple d'entiers positifs (k, n), on a :*

$$\binom{n}{k} = \begin{cases} \dfrac{n!}{k!(n-k)!} & \text{si } k \leqslant n \\ 0 & \text{sinon.} \end{cases}$$

Proposition 15 (Formule du Binôme)**.** *Soient $x, y \in A$ des éléments d'un anneau vérifiant $xy = yx$. Alors $(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}$.*

Application 16. *Soit K un corps de caractéristique p, alors pour tout $x \in K$, on a : $(x+y)^p = x^p + y^p$.*

3 Dénombrement en théorie des Groupes

Théorème 17 (Lagrange)**.** *Soit G un groupe fini de cardinal n, alors tout sous-groupe H de G est de cardinal divisant n.*

3.1 Action de groupe

Définition 18. On considère un groupe G opérant sur un ensemble X. pour tout $x \in X$, on note $\omega(x) = \{g.x,\ g \in G\}$ l'orbite de x et $Stab(x) = \{g \in G,\ g.x = x\}$ le stabilisateur de x.

Proposition 19. *Pour tout $x \in X$, on a $|\omega(x)| = \frac{|G|}{|Stab(x)|}$.*

Application 20. *Soit G un groupe fini non abélien. On note $n(G)$ la proportion des couples d'éléments de G qui commutent parmi tous les couples de G. Alors $n(G) \leqslant \frac{5}{8}$.*

Corollaire 21 (Équation aux classes)**.** *Si $y \in \omega(x)$ alors $Stab(x)$ et $Stab(y)$ sont conjugués, donc $|Stab(x)| = |Stab(y)|$ et notant Ω l'ensemble des orbites de X, on a : $|X| = \sum_{w \in \Omega} \frac{|G|}{|Stab(\omega)|}$.*

Application 22. *Le centre d'un p-groupe non trivial est non trivial, et tout groupe de cardinal p^2 est abélien.*

Application 23 (Lemme de Cauchy)**.** *Soit G un groupe de cardinal n et p un diviseur premier de n. Alors G contient au moins un élément d'ordre p.*

Proposition 24 (Formule de Burnside)**.** *On note $Fix(g) = \{x \in X,\ g.x = x\}$ et r le nombre d'orbites de X, alors $r = \frac{1}{|G|}\sum_{g\in G}|Fix(g)|$.*

Application 25. *Le nombre moyen de points fixes d'une permutation de $\mathfrak{S}_n$ est 1.*

3.2 Théorèmes de Sylow

Définition 26. Soit G un groupe fini de cardinal $p^\alpha m$ avec p ne divisant pas m. Un $p-$Sylow de G est un sous-groupe de G de cardinal p^α.

Exemple 27. $P = \{A \in M_n(\mathbb{F}_p),\ a_{ij} = 0 \text{ si } i > j,\ a_{ii} = 1\}$ est un p-Sylow de $GL_n(\mathbb{F}_p)$.

Lemme 28. *Soit G un groupe avec $|G| = p^\alpha m$, p ne divisant pas m et soit H un sous-groupe de G. Soit 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 29. *Soit G comme précédemment, alors :*
(i) G contient au moins un p-Sylow.
(ii) Si H est un p-sous-groupe de G, alors il existe un p-Sylow S de G avec $H \subset S$.
(iii) Les p-Sylow sont tous conjugués (et donc leur nombre n_p divise n).
(iv) On a $n_p \equiv 1\ mod(p)$ (donc n_p divise m).

4 Dénombrement et Corps finis

4.1 Fonction d'Euler

Définition 30. On appelle fonction d'Euler et on note $\phi(n)$ le nombre d'entier $1 \leqslant k \leqslant n$ premier avec n.

Exemple 31. Pour tout nombre premier p et pour tout $\alpha \in \mathbb{N}^*$, on a : $\phi(p^\alpha) = p^{\alpha-1}(p-1)$.

Lemme 32. *Pour tout $n \in \mathbb{N}$, on a $n = \sum_{d|n}\phi(d)$.*

Application 33. *Tout sous-groupe fini du groupe multiplicatif d'un corps est cyclique.*

4.2 Fonction de Möbius

Définition 34. On définit la fonction de Möbius $\mu : \mathbb{N}^* \to \mathbb{Z}$ de la manière suivante : $\mu(1) = 1$, $\mu(n) = 0$ si n est divisible par le carré d'un nombre premier, et $\mu(p_1 \cdots p_r) = (-1)^r$, si les p_i sont des nombres premiers deux à deux distincts.

Proposition 35 (Formule d(inversion de Möbius)**.** *Soit $f : \mathbb{N}^* \to \mathbb{R}$. On pose alors $g : n \in \mathbb{N}^* \mapsto \sum_{d|n} f(d)$, alors on a pour tout $n \geqslant 1$: $f(n) = \sum_{d|n}\mu(\frac{d}{n})g(d) = \sum_{d|n}\mu(d)g(\frac{d}{n})$.*

Lemme 36. *Soit K un corps fini, alors il existe un nombre premier p et un entier $n \in \mathbb{N}$ tels que $|K| = p^n$.*

Définition 37. Pour $n \in \mathbb{N}^*$, on note $A(n,q)$ l'ensemble des polynômes de $\mathbb{F}_q[X]$ (où $q = p^n$) irréductibles unitaires de degré n et $I(n,q) = |A(n,q)|$.

Proposition 38 (DEV 1). *Pour tout $n \leqslant 1$, on a $X^{q^n} - X = \prod_{d|n}\prod_{P\in A(d,q)} P$. On en déduit que $nI(n,q) = \sum_{d|n}\mu(\frac{n}{d})q^d$. En particulier, $I(n,q) \sim \frac{q^n}{n}$.*

4.3 Symbole de Legendre

Définition 39. Soit $q = p^n$ où p est un nombre premier impair. On note $(\mathbb{F}_q^*)^2 = \{x \in \mathbb{F}_q^*,\ \exists y \in \mathbb{F}_q,\ x = y^2\}$.

Proposition 40. *(i) On a $x \in (\mathbb{F}_q^*)^2 \iff x^{\frac{q-1}{2}} = 1$.*
(ii) $|(\mathbb{F}_q^*)^2| = \frac{q-1}{2}$.

Définition 41. On définit le symbole de Legendre $(\frac{x}{p})$ pour $x \in \mathbb{F}_p^*$ de la manière suivante :

$$\left(\frac{x}{p}\right) = \begin{cases} 1 \text{ si } x \in (\mathbb{F}_q^*)^2 \\ -1 \text{ si } x \notin (\mathbb{F}_q^*)^2 \end{cases} = x^{\frac{p-1}{2}}.$$

Proposition 42. *Pour tout x et y dans $\mathbb{F}_p^*$, on a : $(\frac{xy}{p}) = (\frac{x}{p})(\frac{y}{p})$*

Application 43. *Le produit de deux non-carré dans $\mathbb{F}_p^*$ est un carré, le produit d'un carré et d'un non-carré est un non-carré dans $\mathbb{F}_p^*$.*

Corollaire 44. *Soit p un nombre premier impair et soit a un élément de $\mathbb{F}_p^*$. Alors $|\{x \in \mathbb{F}_p,\ \ ax^2 = 1\}| = 1 + (\frac{a}{p})$.*

Théorème 45 (Loi de réciprocité quadratique **DEV 2**)**.** *Soient p et q deux nombres premiers impairs distincts. Alors :*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$$

5 Séries formelles

Définition 46. Soit K un corps de caractéristique nulle, on note $K[[X]]$ l'ensemble des suites (infinies) indexées par $\mathbb{N}$ à valeurs dans K, muni des deux opérations : $(x_i)_i + (y_i)_i = (x_i + y_i)_i$ et $(x_i)_i.(y_i)_i = \left(\sum_{i=0}^{n} x_i y_{n-i}\right)_n$. C'est un anneau commutatif intègre.

Remarque 47. Si l'on note $X = (0, 1, 0, \cdots)$, alors on a $X^k = (0, 0, \cdots, 0, 1, 0, \cdots)$ où l'unique 1 est à la $(k+1)$-ème position. Ainsi, tout élément $A \in K[[X]]$ s'écrit (de manière unique) sous forme d'un série : $A = (a_i)_i = \sum_{i\in\mathbb{N}} a_i X^i$. Cette série est la série génératrice de la suite A.

Exemple 48. $(1, 1, 1, \cdots) = \frac{1}{1-X}$

Application 49 (Nombres de Fibonacci)**.** *On considère la suite définie par $F_n = F_{n-1} + F_{n-2}$; $F_0 = F_1 = 1$. Alors $F_n = \frac{\beta^{n+1} - \alpha^{n+1}}{\sqrt{5}}$ où $\alpha = \frac{1-\sqrt{5}}{2}$ et $\beta = \frac{1+\sqrt{5}}{2}$.*

Application 50 (Nombre de Catalan)**.** *On considère un produit $P = X_1 ... X_n$ de n-nombres, et on veut déterminer le nombre a_n de parenthésage différents dont on peut munir P pour le calculer par des multiplication successives opérant toujours sur deux facteurs adjacents. Ainsi $a_2 = 1$, $a_3 = 2$, $a_4 = 5$. On pose $a_0 = 0$ et et $a_1 = 1$. On a alors pour $n \geqslant 1$, $a_n = \frac{1}{n}\binom{2n-2}{n-1}$*

Développements

1. Polynômes irréductibles de $\mathbb{F}_q[X]$ **[38]**

2. Loi de réciprocité quadratique **[45]**

Références

— **[C]** L.comptet, *Analyse combinatoire (tome 1 et 2.*
— **[FGN]** S.Francinou et H.Gianella et S.Nicolas, *Oraux X-ENS, algèbre 1.*
— **[FG]** S.Francinou et H.Gianella, *Exercice de mathématiques pour l'agrégation, algèbre 1.*
— **[NH2G2]** P.Caldero et J.Germoni, *Nouvelle histoires hédonistes de groupes et de géométries (tome 1).*
— **[P]** D.Perrin, *Cours d'algèbre.*
— **[S]** P.Saux Picart, *Cours de calcul formel, algorithmes fondamentaux.*