I Outils basiques

Propriétés : Soit E un ensemble
i) Si $E_1, \dots, E_n$ est une partition de E (i.e $E = \bigcup_{i=1}^{n} E_i$ et $E_i \cap E_j = \emptyset$ si $i \neq j$) alors $|E| = \sum_{i=1}^{n} |E_i|$
ii) Si E est un ensemble de paires ordonnées (a,b) où $|\{a / \exists b, (a,b) \in E\}| = p$ et pour tout a $|\{b / (a,b) \in E\}| = q$ alors $|E| = pq$
iii) Si $E_1, \dots, E_n$ partition de E et $\forall i$ $|E_i| = |E_1| > 0$ alors $n = \frac{|E|}{|E_1|}$

Application 2 : $|E \times F| = |E| \cdot |F|$; si $|E| < +\infty$ et $A \subset E$ alors $|E \setminus A| = |E| - |A|$; $|E_1 \cup E_2| = |E_1| + |E_2| - |E_1 \cap E_2|$

Proposition 3 : Si $|E| = p$ et $|F| = n \geq p$ il y a $n \cdots (n-p+1) = \frac{n!}{(n-p)!}$ applications injectives de E dans F.
En particulier $|\mathfrak{S}_n| = n!$

Théorème 4 : de Lagrange
Soit G un groupe et $H \leq G$ un sous groupe de G alors $|H|$ divise $|G|$.

Proposition 5 (Formule du crible de Poincaré) :
Soient $E_1, \dots, E_n$ des ensembles finis alors
$$\left|\bigcup_{i=1}^{n} E_i\right| = \sum_{k=1}^{n} (-1)^{k+1} \sum_{1 \leq i_1 < \dots < i_k \leq n} |E_{i_1} \cap \dots \cap E_{i_k}|$$

Remarque 6 : Pour $n = 2$ on retrouve la formule
$|E_1 \cup E_2| = |E_1| + |E_2| - |E_1 \cap E_2|$

Lemme 7 : des tiroirs
Soient E et F deux ensembles finis tq $|E| > |F|$
alors pour toute application $f : E \to F$, il existe $x \in F$ tq $|f^{-1}(\{x\})| \geq 2$

Application 8 : Théorème de Weierstraß (cas réel)
Soient $a < b$ deux réels, et $(u_n)_{n \in \mathbb{N}} \in [a,b]^{\mathbb{N}}$ alors il possède une **valeur d'adhérence**.

Définition 9 : On définit :
- $\binom{n}{k}$ comme étant le nombre de parties à k éléments dans un ensemble à n éléments
- A_n^k le nombre d'arrangements de k éléments d'un ensemble de n éléments, c'est à dire le nombre de listes ordonnées de k éléments distincts pris dans un ensemble de n éléments.

Exemple 10 : (d'utilisation) On se fixe $n \in \mathbb{N}^*$
- **Binome de Newton :** si $x, y \in A$ anneau commutatif
$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}$$
- **Loi Binomiale :** Soit $p \in [0,1]$, une loi binomiale de paramètre (n,p) est une loi discrète réelle vérifiant $\mathbb{P}(X = k) = \binom{n}{k} p^k (1-p)^{n-k}$
La somme de n Bernoulli indépendantes de paramètre p est une **loi binomiale** de paramètre (n,p).

Proposition 11 : Soient $k, n \in \mathbb{N}$
- $A_n^k = \frac{n!}{(n-k)!}$ si $k \leq n$ $\quad A_n^k = 0$ sinon
- $\binom{n}{k} = \frac{n!}{k!(n-k)!}$ si $k \leq n$ $\quad \binom{n}{k} = 0$ sinon
- $\binom{n-1}{k} + \binom{n-1}{k-1} = \binom{n}{k}$ c'est la formule du triangle de Pascal.

II Formules d'inversions et séries formelles :

1) Formule d'inversion :

Proposition 12 : Formule d'inversion de Pascal
Soit A anneau commutatif et $a = (a_n)_{n \in \mathbb{N}} \in A^{\mathbb{N}}$
En posant $b_n = \sum_{k=0}^{n} \binom{n}{k} a_k$ alors $a_n = \sum_{k=0}^{n} (-1)^{n-k} \binom{n}{k} b_k$

Application 13 : Le nombre de surjection de $\{1,\dots,p\}$ dans $\{1,\dots,n\}$ est $\sum_{k=0}^{n} (-1)^{n-k}\binom{n}{k}k^p$

Définition 14 : Fonction de Mobius.

On définit la fonction de Mobius

$$\mu : \mathbb{N}^* \to \mathbb{Z}$$
$$n \mapsto \begin{cases} 0 \text{ si } n \text{ a un facteur carré} \\ (-1)^r \text{ si } n \text{ produit de } r \text{ nombres premiers distincts} \end{cases}$$

Théorème 15 : (Formule d'inversion de Mobius)

Si G est un groupe et $f, g : \mathbb{N}^* \to G$ vérifient $g(n) = \prod_{d|n} f(d)$ pour $n \geq 1$ alors $f(n) = \prod_{d|n} g\left(\frac{n}{d}\right)^{\mu(d)}$

Application 16 : Soit φ l'indicatrice d'Euler, on a $\sum_{d|n} \varphi(d) = n$ d'où $\varphi(n) = \sum_{d|n} \mu(d)\frac{n}{d}$.

2) Séries formelles :

Définition 17 : On définit $\mathbb{Q}[[X]]$ l'anneau des séries entières sur $\mathbb{Q}$. Comme l'ensemble des suites à valeurs dans $\mathbb{Q}$ muni des opérations $(u_n)_n + (v_n)_n = (u_n + v_n)_n$ et $(u_n)_n \cdot (v_n)_n = \left(\sum_{k=0}^{n} u_k v_{n-k}\right)_n$ c'est un anneau commutatif et $u = (u_n)_{n\in\mathbb{N}} \in \mathbb{Q}[[X]]$ est inversible ssi $u_0 \neq 0$.

On note $X = (\delta_{1,n})_{n\in\mathbb{N}}$ et on a $X^k = (\delta_{k,n})_{n\in\mathbb{N}}$ ce qui motive la notation $(u_n)_{n\in\mathbb{N}} = \sum_{k=0}^{+\infty} u_k X^k$

Application 18 : Si on pose D_n le nombre de dérangements de $\mathfrak{S}_n$ alors $D_n = \sum_{k=0}^{n} (-1)^k \binom{n}{k}(n-k)!$

Application 19 : Si on pose C_n le n-ième nombre de Catalan qui est le nombre de mots de n parenthèses ouvrantes et n fermantes qui sont bien parenthésés on a $C_n = \frac{1}{n+1}\binom{2n}{n}$

Exemple 20 `()()` est bien parenthésé
`())(` n'est pas bien parenthésé

III Actions de groupe et colorations

1) Colorations

On se fixe E un ensemble

Définition 21 : Une coloration de E à q couleurs est une application $\chi : E \to \{1,\dots,q\}$.

Exemple 22 : Si E est l'ensemble des secteurs d'une roulette alors une coloration est : 

Théorème 22 : Soit $q \in \mathbb{N}$, il existe $N(r) \in \mathbb{N}$ tel que si $|E| \geq N(r)$ alors si on note $\mathcal{P}_2(E)$ l'ensemble des parties à 2 éléments de E, pour toute coloration χ à r couleurs de $\mathcal{P}_2(E)$, il existe $x, y, z \in E$ distincts tq $\chi(\{x;y\}) = \chi(\{y;z\}) = \chi(\{x;z\})$

Corollaire 23 : Soit $n \in \mathbb{N}$, il existe p premier tq $\forall q \geq p$ premier l'équation $x^n + y^n = z^n$ admet une solution non triviale dans $\mathbb{Z}/q\mathbb{Z}$.

DEV

2) Actions de groupe

On suppose ici E Fini et on se donne G un groupe Fini agissant sur E. On note Ω l'ensemble des orbites de E.

Lemme 24: Equation des classes

$$|E| = \sum_{\omega \in \Omega} |\omega|$$

Proposition 25: En notant $\mathcal{O}_x$ l'orbite de x et $Stab_G(x)$ son stabilisateur on a $|\mathcal{O}_x| = \frac{|G|}{Stab_G(x)}$

Proposition 26 : Formule de Burnside

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

Définition 27: Soient χ_1 ; χ_2 deux colorages de E ils sont dit equivalent si: il Existe $g \in G$ tq $\chi_2 g^{-1} = \chi_1$

Exemple 28: $E = \{1, \dots, n\}$ et $G = \mathfrak{S}_n$; deux colorages sont equivalents si: $\forall i \in \{1, \dots, q\}$ $|\chi_1^{-1}(\{i\})| = |\chi_2^{-1}(\{i\})|$

Proposition 29: Si on pose $C(E,q)$ le nombre de colorage à G-equivalence près on $C(E,q) = \frac{1}{|G|} \sum_{g \in G} q^{r(g)}$ où $r(g)$ est le nombre de g-orbite.

Exemple 30: Si E est l'ensemble des n secteurs d'une roulette et on identifie deux colorages si ils sont identiques à rotation près. alors $C(E,q) = \frac{1}{|G|} \sum_{i=0}^{n} q^{(n,i)}$

IV Dénombrement des Les corps Finis

1) Propriétés

On note F_q l'unique corps de cardinal q à isomorphisme près.

Proposition 31: F_q est de caractéristique première.

Proposition 32: Soit p la caractéristique de F_q. $\exists n \in \mathbb{N}^*$ tel que $q = p^n$

Proposition 33: $F_q^\times$ est cyclique

Proposition 34: Soit $n \in \mathbb{N}^*$. Soit $|B_n|$ le nombre de bases de $(F_q)^n$. Alors $|B_n| = \prod_{k=0}^{n-1} (q^n - q^k)$

2) Groupe linéaire

Proposition 35: $|GL_n(F_q)| = \prod_{k=0}^{n-1} (q^n - q^k)$

Proposition 36: $|SL_n(F_q)| = \frac{|GL_n(F_q)|}{q-1}$

Proposition 37: Le centre de $GL_n(F_q)$ est $Z_{n,q} = \{\lambda I_n, \lambda \in F_q^*\}$
Le centre de $SL_n(F_q)$ est $SZ_{n,q} = \{\lambda I_n, \lambda \in F_q^*, \lambda^n = 1\}$

Définition 38: $PGL_n(F_q) := GL_n(F_q)/Z_{n,q}$
$PSL_n(F_q) := SL_n(F_q)/SZ_{n,q}$

Proposition 39: $|PGL_n(F_q)| = \frac{|GL_n(F_q)|}{q-1}$

Proposition 40: $|PSL_n(F_q)| = \frac{|SL_n(F_q)|}{pgcd(q-1,n)}$

Proposition 41: Le nombre de matrices diagonalisables de $GL_n(F_q)$ est $|D_{n,q}| = \sum_{\substack{n_1, \dots, n_{q-1} \\ \sum n_i = n \\ n_i \geq 0}} \frac{|GL_n(F_q)|}{\prod_{k=1}^{q-1} |GL_{n_k}(F_q)|}$