Chapitre 1 : Cardinalité

I. Ensembles finis

Généralités

1. Si il existe une surjection de $[\![1,n]\!]$ sur E, alors E est fini de card $\leq n$
2. Si il existe une injection de $[\![1,n]\!]$ sur E, alors E est de card $\geq n$

Si $|E|=n, |F|=m$:

- $|E\times F|=nm$
- $|E\cup F|=|E|+|F|-|E\cap F|$
- $|\mathscr{P}(E)|=2^n$,

Coefficients binomiaux

Identités :

- $$2^n=\sum_{k=0}^{n}\binom{n}{k}$$

  Idée clé : $\mathscr{P}(E)=\bigsqcup_{k=0}^{n}\{\text{parties de card } k\}$

- $$\binom{n}{k}=\binom{n}{n-k}$$

  Idée clé : passage au complémentaire.

- **Le triangle de Pascal** : si $n\in\mathbb{N}^*$:

$$\binom{n-1}{k}+\binom{n-1}{k-1}=\binom{n}{k}$$

Idée clé: deux types de parties de cardinal k : celles qui contiennent n et celles qui ne le contiennent pas.

- $$\binom{n}{k}=\sum_{j=k}^{n}\binom{j-1}{k-1}$$

  Idée clé : parties de card k selon leur plus grand élément $\in[\![k,n]\!]$

- **Identité de Vandermonde** :

$$\binom{m+n}{k}=\sum_{0\leq i\leq m, k-n\leq i\leq k}\binom{m}{i}\binom{n}{k-i}$$

Idée clé : parties de card k de $E\cup F=[\![1,m+n]\!]$ selon les cardinaux des traces sur E / sur F.

- $$k\binom{n}{k}=n\binom{n-1}{k-1}$$

  Idée clé: double comptage de $\{(i,\mathfrak{F})\mid\mathfrak{F}\subseteq F,|\mathfrak{F}|=k,1\leq i\leq k\}$
  Corollaire :

$$\binom{n}{k}=\frac{n!}{k!(n-k)!}$$

Principe des tiroirs

> **Principe des tiroirs** : Si $f:E\longrightarrow F$ et $|E|>|F|$, au moins deux éléments ont la même image.

Applications :

> **Pumping Lemma** :

> Soit L un langage rationnel :
>
> $\exists N \in \mathbb{N}; \forall \omega \in L,$
>
> $$|w| \geq N \Longrightarrow \exists x,y,z; \begin{cases} \omega \overset{\text{def}}{=} xyz \in L \\ |y| \leq N \end{cases} \wedge \forall n \in \mathbb{N}, xy^n z \in L$$

Lemme d'Erdös

> **Lemme d'Erdös** :
>
> Soit $(x_i)_{i \in [\![1, n^2+1]\!]}$ une famille d'entiers naturels.
>
> Alors il y a au moins une sous-famille croissante de card $n+1$ ou un sous-famille décroissante de card $n+1$.

Idée clé : card d'une plus grande sous-famille croissante/décroissante qui débute/termine en x_i, puis contradiction avec le principe des tiroirs.

Formule du crible / de Poincaré / Principe d'inclusion-exclusion

$E_1, \dots, E_n \subseteq X$

$$\left| \bigcup_1^n E_i \right| = \sum_{\substack{k \in [\![1,n]\!] \\ 1 \leq i_1 < \cdots < i_k \leq n}} (-1)^{k-1} \bigcap_j E_{i_j}$$

Idée clé : calcul de

$$1_X - 1_{\bigcup E_i} = \prod_1^n (1_X - 1_{E_i})$$

II. Ensembles Dénombrables

Ensemble dénombrable :

- *au sens strict* : en bijection avec $\mathbb{N}$
- *au sens large* : en bijection avec $\mathbb{N}$ OU fini

> **Proposition** : Tout ss-ensemble infini de $\mathbb{N}$ est dénombrable.

Idée clé :

$$f \overset{\text{def}}{=} \begin{cases} \mathbb{N} \longrightarrow E \\ 0 \mapsto \min(E) \\ n > 0 \mapsto \min(E \backslash \{f(0), \cdots, f(n-1)\}) \end{cases}$$

> **Corollaire** : Tout ensemble E tel qu'∃ une injection de E dans $\mathbb{N}$ est dénombrable au sens large.

Bijections classiques :

$$\begin{cases} \mathbb{Z} \longrightarrow \mathbb{N} \\ n \mapsto \begin{cases} 2n \text{ si } n \geq 0 \\ -2n-1 \text{ sinon.} \end{cases} \end{cases}$$

$$\begin{cases} \mathbb{N}^n \longrightarrow \mathbb{N} \\ (a_1, \cdots, a_n) \mapsto 2^{a_1} 3^{a_2} \cdots \underbrace{p_n^{a_n}}_{p_n : n\text{-ième nombre premier}} \end{cases}$$

$$\begin{cases} \mathbb{Q} \longrightarrow \mathbb{N} \\ x = \underbrace{\varepsilon \frac{p}{q}}_{\varepsilon = \pm 1,\ p \wedge q = 1} \mapsto \begin{cases} 2^p 3^q \text{ si } \varepsilon = 1 \\ 2^p 5^q \text{ si } \varepsilon = -1 \text{ et } p \neq 0 \end{cases} \end{cases}$$

> **Proposition**: Une réunion d'ensembles dénombrables est dénombrable.

Idée clé :

$$\begin{cases} \bigcup E_i \longrightarrow \mathbb{N} \times \mathbb{N} \\ x \mapsto (i, f_i(x)) \end{cases}$$

où $i = \min\{j | x \in E_j\}$

Ensembles non dénombrables :

- $\mathbb{R}$: *Idée clé* : argument diagonal de Cantor.

III. Equipotence

Ensembles équipotents :
ensembles en bijection.

> **Théorème de Cantor** : E et $\mathscr{P}(E)$ ne sont pas équipotents.

Idée clé : par l'absurde, avec $X \overset{\text{def}}{=} \{x \in E | x \notin f(x)\}$

Chapitre 2 : Relations

I. Relations binaires

Relation binaire sur une ensemble E :
une partie $R \subseteq E \times E$

Notation: $xRy \iff (x, y) \in R$

Clôture transitive R^{**} de R :

$$\forall x, y \in E, xR^{**}y \iff \exists n \geq 1, x_1, \cdots, x_n \in E;$$
$$(x_0 = x) \wedge (x_i R x_{i+1} \forall i \in [\![0, n-1]\!]) \wedge (x_n = y)$$

Relation d'équivalence R :
relation binaire réflexive, symétrique et transitive.

- $x \in \mathscr{C}(x)$
- $\forall x, y \in E, xRy \iff \mathscr{C}(x) = \mathscr{C}(y)$
- $\forall x, y \in E, xRy \iff \mathscr{C}(x) \cap \mathscr{C}(y) \neq \emptyset$

> **Corollaire** :

- L'ensemble des classes d'équivalence de la relation d'éq R sur E définit une partition de E.
- Réciproquement : toute partition de E définit une relation d'éq dont les classes d'éq sont les éléments de la partition.

Ensemble quotient E/R :
ensemble des classes d'éq de R sur E.

Surjection canonique :
L'application

$$\pi : \begin{cases} E \longrightarrow E/R \\ x \mapsto \mathscr{C}(x) \overset{\text{def}}{=} \{y \in E; xRy\} \end{cases}$$

> **Proposition** : Soit $f : E \longrightarrow F$ compatible avec R, i.e
>
> $$\forall x, y \in E, xRy \Longrightarrow f(x) = f(y)$$
>
> Alors il existe $\bar{f} : E/R \longrightarrow F$ tq le diagramme suivant est commutatif :
>
> $$\begin{array}{ccc} E & \overset{f}{\longrightarrow} & F \\ \pi \downarrow & \nearrow \bar{f} & \\ E/R & & \end{array}$$

Relation d'ordre $\leq$:
Relation binaire réflexive, antisymétrique, transitive.

Exs :

- $(\mathbb{N}, \leq), (\mathbb{R}, \leq)$ (ordres totaux)

- ordre lexicographique
- Dans $\mathbb{N}^k$: $(m_1, \cdots, m_k) \leq (n_1, \cdots, n_k)$ si c'est le cas pour toutes les composantes (ordre partiel).
- L'inclusion dans $\mathscr{P}(E)$ (ordre partiel).
- La divisibilité dans $\mathbb{N}^*$ (ordre partiel).

Chaîne :

Ensemble totalement ordonné.

Antichaîne :

Ensemble où deux éléments distincts ne sont pas comparables.

Successeur :

Soient $x, y \in E$ (muni de $\leq$). y est le successeur de x ssi :

$$(y > x) \wedge \forall z \in E, y \geq z \geq x \Longrightarrow y = z$$

(y est plus grand que x, et il n'y a rien entre les deux).

> **Proposition** : Si E est fini, $\leq$ est la clôture transitive de la relation "successeur".

Plus petit élément = minimum $\bot$ / Plus grand élément = maximum $\top$:

$$\forall x \in E, \bot \leq x \ / \ \forall x \in E, \top \geq x$$

Élément maximal / minimal x dans F :

$$\forall y \in F, y \geq x \Longrightarrow y = x \ / \ \forall y \in F, y \leq x \Longrightarrow y = x$$

> - Plus petit/grand élément $\Longrightarrow$ Élément minimal/maximal
>
> **MAIS**
>
> - Unique élément minimal/maximal $\not\Longrightarrow$ Plus petit/grand élément
>
> **À part pour les ensembles finis** :
>
> Si F fini admet un unique élément maximal, alors c'est un maximum.

Majorant / Minorant $y \in E \supset F$ de F :

$$\forall x \in F, y \geq x \ / \ \forall x \in F, y \leq x$$

Borne supérieure / inférieure :

Minimum / maximum de l'ensemble des majorants / minorants, s'il existe.

> - Plus grand / petit élément $\Longrightarrow$ Borne sup / inf
> - Borne supérieure appartenant à l'ensemble $\Longrightarrow$ maximum

Exs :

1. $(\mathbb{N}\backslash\{0\}, |)$, $F = \{a_1, \cdots, a_n\}$:

- les *majorants* : multiples communs aux a_i
  - borne sup : $ppcm(a_1, \cdots, a_n)$.
- les *minorants* : diviseurs communs aux a_i
  - borne inf : $pgcd(a_1, \cdots, a_n)$.

2. $(E, \leq) = (\mathscr{P}(X), \subseteq)$, $F = \{Y_1, \cdots, Y_n\}$:

- Borne sup : $\bigcup_i Y_i$
- Borne inf : $\bigcap_i Y_i$

Treillis

Treillis :

Ensemble ordonné dans lequel toute paire (d'éléments) admet une borne sup et une borne inf.

Treillis complet :

Si, de plus, pour toute partie $F \subseteq E$, F admet un borne sup et une borne inf.

NB : Un treillis complet a un plus grand / petit élément.

Exs:

1. $(\mathbb{N}\backslash\{0\}, |)$: treillis non complet
2. $(\mathscr{P}(X), \subseteq)$: treillis complet :

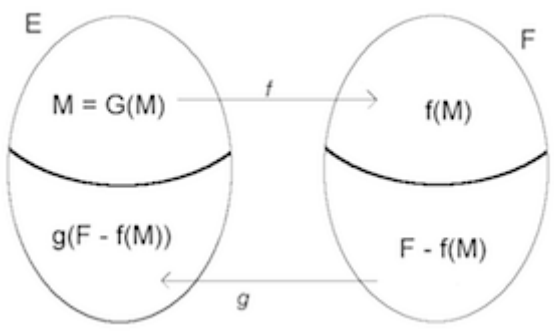
- Borne sup de $S \subseteq \mathscr{P}(X)$ = $\bigcup_{Y \in S} Y$
- Borne inf de $S \subseteq \mathscr{P}(X)$ = $\bigcap_{Y \in S} Y$

> **Th de Knaster-Tarski** : Soit $(E, \leq)$ un treillis complet, $f : E \longrightarrow E$ monotone.
>
> Alors f admet un plus petit / plus grand pt fixe.

Idée clé : c'est la borne inf / sup de $\{x \in E; x \geq f(x)\}$ / $\{x \in E; x \leq f(x)\}$

> **Théorème de Cantor-Bernstein** : *Si* il existe une injection de E dans F et une injection de F dans E, *alors* E et F sont équipotents.

Idée clé : Application de Knaster-Tarski



> **Théorème de Bourbaki-Witt** :
>
> Soit $(X, \leq)$ un ensemble ordonné tel que toute chaîne non vide admet une borne supérieure.
>
> Soit $f : X \longrightarrow X$ une application telle que $\forall x \in X, x \leq f(x)$.
>
> Alors f admet un point fixe.

> **Lemme de Zorn** : Soit X un ensemble ordonné dans lequel toute chaîne admet une borne supérieure. Alors X admet un élément maximal.

Idée clé : Appliquer Bourbaki-Witt à $\{\text{chaînes de } X\}$ en supposant par l'absurde qu'aucune chaîne n'est maximale.

Chapitre 3 : Structures algébriques

0. Catégories

Catégorie :

Il y a des :

- objets : $E, F, G...$
- flèches : $Hom(E, F)$: on y manipule des applications $E \longrightarrow F$ qui sont compatibles avec la structure.

$F : \mathscr{C} \longrightarrow \mathscr{C}'$ foncteur.

Si E est un objet, $F(E)$ objet.

Si $f \in Hom_{\mathscr{C}}(E, G)$, $F(f) \in Hom_{\mathscr{C}}(F(E), F(G))$

Problème universel : objet libre

$L(X)$ est libre sur X si pour tout E dans $\mathscr{C}$, pour tout $f : X \longrightarrow E$, il existe un unique $\widehat{f}$ unique dans $Hom_{\mathscr{C}}(L(X), E)$ qui prolonge f.

I. Semi-groupes et monoïdes

Partie génératrice du monoïde M :

$X \subseteq M$, telle que $\langle X \rangle = M$. (X engendre M)

Congruence :

Une relation d'éq $\sim$ telle que

$$m_1 \sim m_2 \Longrightarrow \forall u, v \in M, um_1v \sim um_2v$$

> **Prop** : Une congruence $\sim$ sur M est compatible avec la loi de monoïde, i.e :
>
> $$m_1 \sim m_2 \wedge n_1 \sim n_2 \Longrightarrow m_1n_1 \sim m_2n_2$$

> **Propriété universelle** : Soit $f : M \longrightarrow N$ un morphisme de monoïdes, $\sim$ une congruence sur M compatible avec f, i.e tq $m_1 \sim m_2 \Longrightarrow f(m_1) = f(m_2)$
>
> *Alors* : il existe un morphisme de monoïdes f de $M/\sim$ dans N tq
>
> $$f = \widehat{f} \circ \pi$$

Cas particulier : si :

$$m_1 \sim m_2 \Longleftrightarrow f(m_1) = f(m_2)$$

$\widehat{f}$ est injectif.

2. Monoïdes libres

> **Prop** : Pour un monoïde M, et une application $f : \Sigma \longrightarrow M$, il existe un unique morphisme de monoïdes $\widehat{f}$ de Σ^* dans M tq
>
> $$f = \widehat{f} \circ i$$
>
> (i : injection de Σ dans Σ^*)

Application "longueur" :

C'est l'unique prolongement de

$$\begin{cases} \Sigma \longrightarrow \mathbb{N} \\ a \mapsto 1 \end{cases}$$

en un morphisme de Σ^* dans $\mathbb{N}$ (on le note $|\cdot|$).

Base $X \subseteq M$:

tout élément de M se décompose de façon unique comme un produit d'éléments de X.

Monoïde libre :

Monoïde isomorphe à un ss-monoïde de Σ^* qui admet une base.

Code :

une partie $X \subseteq M$ tq

$$\forall u_i, v_i \in X, u_1 \cdots u_n = v_1 \cdots v_p \Longrightarrow (n = p) \wedge (\forall i, u_i = v_i)$$

NB : Soit L un ss-monoïde de Σ^* :

- si on note X les mots qui se décomposent de façon non triviale dans L : alors $L = \langle X \rangle$
- > L est libre ssi
  >
  > $$\forall w \in \Sigma^*, \exists u, v \in L; uw \in L \wedge wv \in L$$
  >
  > alors $w \in L$

Corollaire : Ss-mon. libres de Σ^* : stables par intersection

Corollaire : Si $X \subseteq \Sigma^*$, existence d'un plus petit ss-mon. libre contenant X : enveloppe libre de X.

> **Th de défaut** : Si $X \subseteq \Sigma^*$ et on suppose X fini. Soit L l'enveloppe libre de X, Y le code de L.
>
> Alors si X n'est pas code, $|Y| < |X|$

3. Monoïdes finis

Si $M = \langle x \rangle$, si $m + p$ est le plus petit possible tel que $x^{m+p} = x^m$, la structure de M est donnée par :

$$M = \{\varepsilon, x, \cdots, x^m = x^{m+p}, \cdots, x^{m+p-1}\}$$

Groupes

Sous-groupe distingué/normal $H \subseteq G$:

Une des conditions équivalentes suivantes est vraie :

- $\forall g \in G, gH = Hg$
- $\forall g \in G, gHg^{-1} = H$
- stable par automorphismes intérieurs

Une relation d'équivalence "compatible" est de la forme : "$\exists$ H ss-groupe distingué" ssi :

$$g_1 \sim g_2 \iff g_1 H = g_2 H$$

Alors $H = \overline{1}$ est un sous-groupe distingué.

Comme G est un groupe, et $\pi : G \longrightarrow G/\sim = G/H, g \mapsto gH$ surjective, G/H est un groupe, d'élément neutre $\pi(1) = H$.

> **Prop** : Soit $\varphi : G_1 \longrightarrow G_2$ un morphisme de monoïdes.
>
> $Ker(\varphi)$ est un ss-groupe distingué.
>
> φ se factorise :
>
> $$\begin{array}{ccc} G_1 & \xrightarrow{\varphi} & G_2 \\ \pi \downarrow & \nearrow \hat{g} & \\ G/\sim & & \end{array}$$

Groupes libres :

- Groupe libre à un générateur $\simeq \mathbb{Z}$
- $\mathbb{Z}/n\mathbb{Z} = \langle x | x^n = 1 \rangle$
- Groupe diédral $D_{2n} \simeq \langle \rho, \sigma | \rho^n = 1, \sigma^2 = 1, \sigma\rho\sigma^{-1} = \rho^{-1} \rangle$:
  - rotation d'angle $\pm 2\pi/3$
  - 3 symétries

Groupes abéliens libres de type fini :

Groupes isomorphes à $\mathbb{Z}^n$

Groupes finis

> **Thm de Lagrange** : si H est un sg de G, $|H|/|G|$

3. Groupe opérant sur un ensemble.

Opération de de G sur l'ensemble E :

c'est la donnée d'une application

$$\begin{cases} G \times E \longrightarrow E \\ (g, x) \mapsto g \cdot x \end{cases}$$

telle que :

- $\forall x \in E, 1 \cdot x = x$ (1 opère comme id sur E)
- $\forall g, g' \in E, \forall x \in G, g \cdot (g' \cdot x) = (gg') \cdot x$

Alors :

$$\varphi \overset{\text{def}}{=} \begin{cases} G \longrightarrow \mathfrak{S}(E) \\ g \mapsto g \cdot \bullet \end{cases}$$

est un morphisme de groupes.

Réciproquement : tout morphisme φ de G dans $\mathfrak{S}(E)$ définit une opération de G sur E.

Orbites :

classes d'équivalence pour la relation

$$\forall x, y \in E, x \sim y \iff \exists g \in G; x = g \cdot y$$

Stabilisateur de x :

le sous-groupe :

$$H_x \stackrel{\text{def}}{=} \{g \in G | g \cdot x = x\}$$

$$\begin{cases} G \longrightarrow \omega_x \\ g \mapsto g \cdot x \end{cases}$$

est une application surjective telle que :

$$\forall g, g' \in G, g \cdot x = g' \cdot x \iff \exists h \in H_x; g = g'h$$

d'où :

$$|G| = |H_x||\omega_x|$$

Fixateur $Fix(g)$ de $g \in G$ agissant sur E :

ensemble des points fixes de g dans E.

Formule (qui n'est pas) de Burnside : Soit G un groupe fini opérant sur un ensemble fini E.

Soit $k = |E/G|$ le nombre d'orbites de E sous l'opération de G.

$$k = |E/G| = \frac{1}{|G|} \sum_{g \in G} |Fix(g)|$$

Idée clé : Double comptage de $\{(g, x) | g \in G \wedge x \in E \wedge g \cdot x = x\}$

Anneaux

Idéal I d'un anneau A :

sous-groupe additif tel que :

$$\forall a \in A, \forall x \in I, ax \in I$$

NB : A/I est muni d'une structure d'anneau.

Séries formelles

$$\mathbb{K}[[X]] \stackrel{\text{def}}{=} \{\sum_{n \geq 0} a_n X^n, (a_n) \in \mathbb{K}^{\mathbb{N}}\}$$

- addition usuelle, produit de Cauchy

Valuation $v : \mathbb{K}[[X]] \longrightarrow \mathbb{N} \cup \{\pm\infty\}$ d'une série formelle :

$$v(\sum_{n \geq 0} a_n X^n) = \begin{cases} +\infty \text{ si } \forall n, a_n \neq 0 \\ \min(i, a_i \neq 0) \text{ sinon} \end{cases}$$

d distance ultramétrique :

$$d(\sum_{n \geq 0} a_n X^n, \sum_{n \geq 0} b_n X^n) = \exp(-v(\sum_{n \geq 0} a_n X^n - \sum_{n \geq 0} b_n X^n))$$