

Résumé de cours :
Semaine 8, du 3 au 7 novembre.

1 Injectivité et surjectivité (fin)

Propriété. Soit f une application de E dans F et g une application de F dans G .

Si $g \circ f$ est injective, alors f est injective.

Si $g \circ f$ est surjective, alors g est surjectif.

Définition et propriété :

- ◊ Soit f une bijection de E dans F . Pour tout $y \in F$, notons $f^{-1}(y)$ l'unique antécédent de y par f . Alors f^{-1} est une bijection de F dans E , appelée la bijection réciproque de f .
- ◊ On vérifie que $f \circ f^{-1} = Id_F$ et $f^{-1} \circ f = Id_E$.
- ◊ Réciproquement, s'il existe une application g de F dans E telle que $f \circ g = Id_F$ et $g \circ f = Id_E$, alors f et g sont des bijections et $g = f^{-1}$.
- ◊ $(f^{-1})^{-1} = f$.

Il faut savoir le démontrer.

Propriété. Si $f : E \rightarrow F$ et $g : F \rightarrow G$ sont bijectives, alors $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

Remarque. La notation f^{-1} , pour une application f , est utilisée selon deux sens *differents*, qu'il est important de bien distinguer :

- Lorsque f est une application *quelconque* de E dans F , si B est une partie de F , alors $f^{-1}(B) = \{x \in E / f(x) \in B\}$.
- Lorsque f est une *bijection* de E dans F , pour tout $y \in F$, $f^{-1}(y)$ est l'unique antécédent de y par f .

En particulier, dès que l'on utilise une expression de la forme $f^{-1}(y)$ où y est un élément de l'ensemble d'arrivée de f , on suppose nécessairement que f est une bijection.

Lorsque $y \in F$, il importe de bien distinguer $f^{-1}(y)$ qui représente, pour une bijection f , l'unique antécédent de y , et $f^{-1}(\{y\})$ qui représente, pour une application f quelconque, l'ensemble des antécédents de y . Cet ensemble peut être vide lorsque f n'est pas surjective, il peut contenir plus de deux éléments lorsque f n'est pas injective.

Propriété. Si f est une bijection de E dans F , alors pour tout $B \subset F$, $f(f^{-1}(B)) = B$ et, pour tout $A \subset E$, $f^{-1}(f(A)) = A$.

Propriété. (HP) Les applications injectives sont simplifiables à gauche et les applications surjectives sont simplifiables à droite.

Il faut savoir le démontrer.

Propriété. Si $E \neq \emptyset$, alors $f : E \rightarrow F$ est injective si et seulement si il existe $g : F \rightarrow E$ telle que $g \circ f = Id_E$.

Il faut savoir le démontrer.

Propriété. $f : E \rightarrow F$ est surjective si et seulement si il existe $g : F \rightarrow E$ telle que $f \circ g = Id_F$.

Il faut savoir le démontrer.

2 Lois internes

Définition. Une loi interne sur E est une application f de $E \times E$ dans E . Dans ce contexte la notation *préfixe* “ $f(x, y)$ ” est remplacée par la notation *infixe* “ $x f y$ ”, où $x, y \in E$. On dit que (E, f) est un magma (hors programme).

Définition. Soit Δ une loi interne sur E . Δ est associative si et seulement si pour tout $x, y, z \in E$, $(x \Delta y) \Delta z = x \Delta (y \Delta z)$. On dit alors que (E, Δ) est un magma associatif. Dans ce cas, si $x_1, \dots, x_p \in E$, la quantité $x_1 \Delta x_2 \Delta \dots \Delta x_p$ ne dépend pas des différentes façons de la parenthésier.

Définition. Soit Δ une loi interne sur E et soit $e \in E$. On dit que e est un élément neutre de (E, Δ) si et seulement si, pour tout $x \in E$, $x \Delta e = e \Delta x = x$. Si E possède un élément neutre, il est unique. On dit alors que (E, Δ) est un magma unitaire, ou bien unifère.

Définition. Un monoïde est un magma associatif unitaire. Il est commutatif, ou abélien, si et seulement si pour tout x, y , $x \Delta y = y \Delta x$.

Remarque. l'usage est de confondre le monoïde (E, Δ) et l'ensemble sous-jacent E .

Notation. Si (E, Δ) est un monoïde d'élément neutre e , on convient que

$$x_1 \Delta x_2 \Delta \dots \Delta x_p = e, \text{ lorsque } p = 0.$$

Définition. Soit (E, \times) un monoïde d'élément neutre 1_E et $x \in E$. On dit que x est inversible à droite (resp : à gauche) si et seulement si il existe $y \in E$ tel que $yx = 1_E$ (resp : $xy = 1_E$).

Si x est inversible à gauche et à droite, il existe un unique $y \in E$ tel que $xy = yx = 1_E$. On note $y = x^{-1}$, c'est le symétrique de x .

Il faut savoir le démontrer.

Propriété.

Si x et y sont inversibles dans le monoïde (E, \times) , alors xy est aussi inversible et $(xy)^{-1} = y^{-1}x^{-1}$.

Définition. Un groupe est un monoïde dans lequel tout élément est inversible.

Définition. On appelle *anneau* tout triplet $(A, +, \cdot)$, où A est un ensemble et où “+” et “.” sont deux lois internes sur A telles que

- $(A, +)$ est un groupe abélien (l'élément neutre étant noté 0 ou 0_A),
- “.” est une loi associative, admettant un élément neutre noté 1 ou 1_A ,
- la loi “.” est *distributive* par rapport à la loi “+”, c'est-à-dire que
 $\forall (x, y, z) \in A^3 \quad x.(y + z) = (x.y) + (x.z) \text{ et } (x + y).z = (x.z) + (y.z)$.

3 Définition du cardinal d'un ensemble

Définition. Soit E un ensemble. S'il existe $n \in \mathbb{N}$ tel que \mathbb{N}_n est en bijection avec E , alors n est unique. On dit que n est le cardinal de E . Il est noté $\text{card}(E)$ ou bien $\#E$, ou encore $|E|$. En cas d'inexistence d'un tel entier n , on dit que E est infini.

Exemple. Pour tout $n, m \in \mathbb{Z}$, $\text{Card}(\llbracket n, m \rrbracket) = m - n + 1$.

Propriété. Soit A un ensemble de cardinal $n \in \mathbb{N}$ et soit B un ensemble quelconque. B est fini de cardinal n si et seulement si il existe une bijection de A sur B .

Propriété. Soit A un ensemble fini de cardinal $n \in \mathbb{N}$. Soit B une partie de A . Alors B est un ensemble fini et $|B| \leq |A|$, avec égalité si et seulement si $B = A$.

Propriété. Soit A une partie de \mathbb{N} . A est finie si et seulement si elle est majorée. En particulier, \mathbb{N} est infini.

4 Cardinaux d'ensembles usuels

Propriété. Pour tout $n \in \mathbb{N}^*$, une réunion disjointe de n ensembles finis est finie et son cardinal est égal à la somme des cardinaux de ces ensembles.

Propriété. Soit E un ensemble fini et A une partie de E . Alors $|E \setminus A| = |E| - |A|$.

Propriété. Soit E un ensemble fini et R une relation d'équivalence sur E . Alors E/R est aussi de cardinal fini, inférieur au cardinal de E .

Formule :

$$|A \cup B| = |A| + |B| - |A \cap B|.$$

Il faut savoir le démontrer.

Propriété. Formule du crible : (Hors programme)

$$\begin{aligned} \#\left(\bigcup_{i=1}^n E_i\right) &= \sum_{i=1}^n \#E_i - \sum_{1 \leq i < j \leq n} \#(E_i \cap E_j) + \cdots + (-1)^{k+1} \sum_{1 \leq i_1 < i_2 < \cdots < i_k \leq n} \#\left(\bigcap_{j=1}^k E_{i_j}\right) \\ &\quad + \cdots + (-1)^{n+1} \#\left(\bigcap_{i=1}^n E_i\right). \end{aligned}$$

Il faut savoir le démontrer.

Propriété. Le cardinal du produit cartésien de n ensembles finis est égal au produit des cardinaux de ces ensembles.

Il faut savoir le démontrer.

Formule : $|\mathcal{F}(E, F)| = |F|^{|E|}$.

Il faut savoir le démontrer.

Propriété. Si E est de cardinal n , alors $\mathcal{P}(E)$ est de cardinal 2^n .

Il faut savoir le démontrer.

5 Sommes et produits finis

Formules :

- Pour tout $a \in G$ et $n \in \mathbb{N}$, $\sum_{k=1}^n a = na$.
- Pour tout $n \in \mathbb{N}$, $\sum_{k=1}^n k = \frac{n(n+1)}{2}$.
- Pour tout $n \in \mathbb{N}$, $\sum_{k=1}^n k^2 = \frac{n(n+1)(2n+1)}{6}$.
- Pour tout $n \in \mathbb{N}$, $\sum_{k=1}^n k^3 = \left(\frac{n(n+1)}{2}\right)^2$.

Notation. Pour tout $n \in \mathbb{N}$, \mathcal{S}_n désigne l'ensemble des bijections de \mathbb{N}_n dans \mathbb{N}_n , que l'on appelle des permutations sur \mathbb{N}_n .

Commutativité généralisée : Soit $n \in \mathbb{N}$ et $x_1, \dots, x_n \in G$. Alors, $\forall \sigma \in \mathcal{S}_n$, $\sum_{i=1}^n x_i = \sum_{j=1}^n x_{\sigma(j)}$.

Définition. Soit A un ensemble fini et $(x_a)_{a \in A}$ une famille de G indexée par A .

Notons $n = |A|$. Il existe une bijection f de \mathbb{N}_n dans A . On pose $\sum_{a \in A} x_a \triangleq \sum_{i=1}^n x_{f(i)}$.

Cette quantité ne dépend pas de la bijection f .

Il faut savoir le démontrer.

Propriété d'additivité : Soit A un ensemble fini, $(x_a)_{a \in A}$ et $(y_a)_{a \in A}$ deux familles d'éléments de G indexées par A . Alors $\sum_{a \in A} (x_a + y_a) = \left(\sum_{a \in A} x_a \right) + \left(\sum_{a \in A} y_a \right)$.

Distributivité généralisée : Soit A un ensemble fini, $\lambda \in \mathbb{C}$ et $(x_a)_{a \in A}$ une famille de *complexes* indexée par A . Alors $\sum_{a \in A} (\lambda x_a) = \lambda \sum_{a \in A} x_a$.

Changement de variable dans une somme finie : Soit B un ensemble fini, $(x_b)_{b \in B}$ une famille d'éléments de G . Soit φ une bijection d'un ensemble A dans B . Alors $\sum_{b \in B} x_b = \sum_{a \in A} x_{\varphi(a)}$.

Il faut savoir le démontrer.

Formule : calcul d'une somme géométrique .

Soit $q \in \mathbb{C} \setminus \{1\}$, soit $m, n \in \mathbb{N}$ avec $m \leq n$. Alors $\sum_{k=m}^n q^k = \frac{q^m - q^{n+1}}{1 - q}$.

Il faut savoir le démontrer.

Théorème. Soit (G, \times) un groupe commutatif fini. Alors, pour tout $g \in G$, $g^{|G|} = 1_G$.

Il faut savoir le démontrer.

Remarque. Ce théorème est encore vrai lorsque G n'est pas commutatif (cf plus loin).

Sommation par paquets : Soit A un ensemble fini et $(x_a)_{a \in A}$ une famille d'éléments de G . On suppose qu'il existe un ensemble fini B et une famille $(A_b)_{b \in B}$ de parties de A telles que $A = \bigsqcup_{b \in B} A_b$.

Alors $\sum_{a \in A} x_a = \sum_{b \in B} \sum_{a \in A_b} x_a$.

Sommation par paquets, seconde formulation : Soit A un ensemble fini et $(x_a)_{a \in A}$ une famille d'éléments de G . Soit R une relation d'équivalence sur A . Alors $\sum_{a \in A} x_a = \sum_{c \in A/R} \sum_{a \in c} x_a$.