Algèbre 1 - SMP - S1

Groupes, anneaux et corps - Séquence 02

Pr. Hamza El Mahjour

Faculté
Polydisciplinaire
Larache
Université Abdelmalek Essaâdi

Objectifs principaux

- Manipuler des éléments du groupe symétrique

- Décrire un anneau et ses propriétés

- Définir un corps

Applications bijectives

Soit f une application de E dans F

- Injective $\longrightarrow \quad f(x) = f(y) \implies x = y$
- Surjective $\longrightarrow \quad \forall y \in F, \exists x \in E$
- Bijective $\rightarrow$ surj + inj

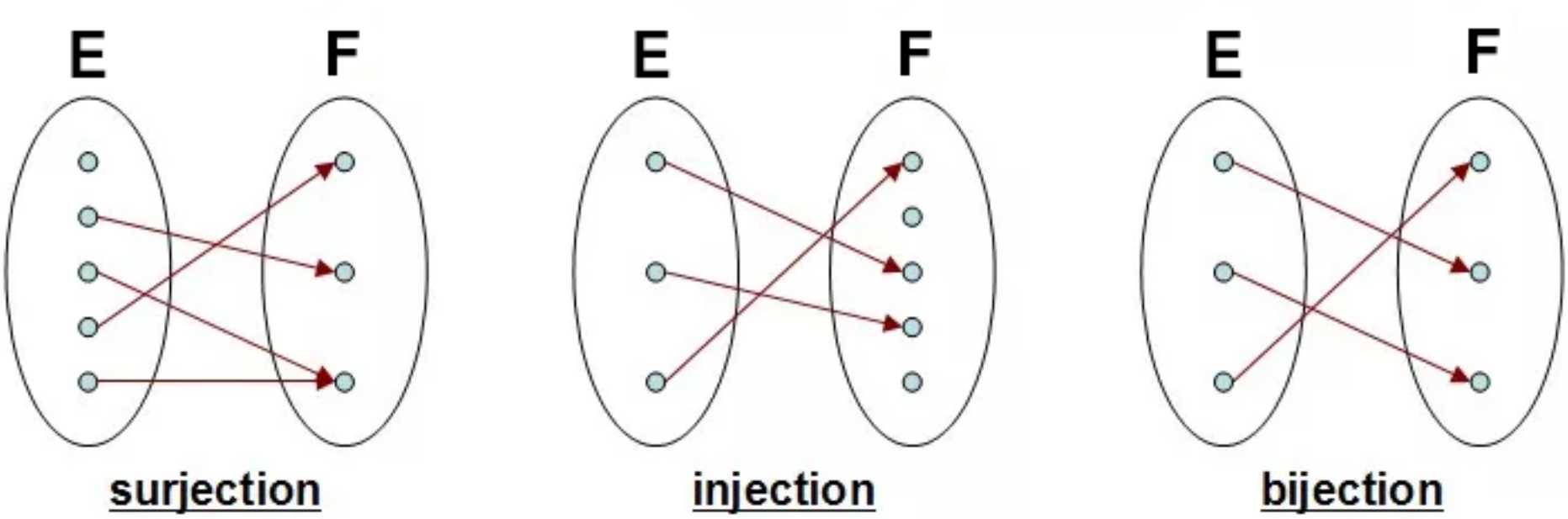

FIGURE – Injection, Surjection et Bijection

Groupe Symétrique

Définition

Soit Ω un ensemble fini ou infini. On définit

$$\mathrm{Perm}(\Omega) = \{f : \Omega \longrightarrow \Omega, \quad f \text{ est bijective}\}.$$

Une bijection d'un ensemble fini dans lui même n'est autre qu'une substitution de la position de ces éléments. On a le résultat suivant

Theorem

L'ensemble $Perm(\Omega)$ *muni de la composition* $\circ$ *est un groupe.*

Permutation,cycle et orbite

Voici un exemple de $\{1,2,3\} \longrightarrow \{1,2,3\}$

$$Id = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \quad \sigma_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \quad \sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$
$$\rho_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \quad \rho_2 = 1 \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \quad \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

Définition

Soit $\sigma \in \mathfrak{S}_n$ et soit $a \in S_n$ fixé. On appelle **orbite** de a par σ l'ensemble

$$\mathcal{O}_{a,\sigma} = \{\sigma^n(a), \quad n \in \mathbb{N}\}.$$

Anneau

Définition

Un **anneau** (aussi appelé anneau unitaire) est un triplet $(\mathbb{A}, +, \cdot)$ où $(A, +)$ est un groupe commutatif et $\cdot$ est une loi de composition interne qui vérifie

1. $\forall x, y, z \in \mathbb{A}, \quad x \cdot (y + z) = x \cdot y + x \cdot z.$ (distributivité)
2. $\exists \mathbb{1}_{\mathbb{A}}, \forall x \in \mathbb{A}, \quad \mathbb{1}_{\mathbb{A}} \cdot x = x \cdot \mathbb{1}_{\mathbb{A}} = x.$ (élément neutre pour $\cdot$)

Si de plus la loi $\cdot$ est commutative dans $\mathbb{A}$ alors l'**anneau est commutatif**.

1. Les triplets $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$,$(\mathbb{R}, +, \cdot)$sont des anneaux.
2. $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ est un anneau commutatif.

Anneau intègre

Définition

On dit que $(\mathbb{A}, +, \cdot)$ est un anneau **intègre** si le seul élément absorbant est $0_{\mathbb{A}}$. Autrement dit

$$x \cdot y = 0_{\mathbb{A}} \quad \Longrightarrow \quad x = 0_{\mathbb{A}} \quad \text{ou} \quad y = 0_{\mathbb{A}}.$$

1. Les anneaux usuels sont intègres.
2. Par contre, $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ n'est pas intègre !

Sous-anneau

un sous-anneau $\mathbb{B}$ d'un anneau $\mathbb{A}$ est tout simplement un anneau tel que $\mathbb{B} \subset \mathbb{A}$. plus précisément

Définition

Un sous-anneau d'un anneau commutatif $(\mathbb{A}, +, \cdot)$ est une partie de $\mathbb{A}$ stable par addition, par multiplication et contenant l'élément unité de $\mathbb{A}$; c'est un sous- groupe de $(A, +)$ et c'est un anneau.

Par exemple on a les sous-anneaux suivants

$$(\mathbb{Z}, +, \cdot) \subset (\mathbb{Q}, +, \cdot) \subset (\mathbb{R}, +, \cdot) \subset (\mathbb{C}, +, \cdot)$$

Caractérisation : $a + (-b) \in \mathbb{B}$ et $a \cdot b \in \mathbb{B}$

Morphismes et idéaux

Définition

Un **idéal** d'un anneau $\mathbb{A}$ est un sou-groupe I de $\mathbb{A}$ tel que :

$$\forall x \in I, \forall x \in \mathbb{A}, \qquad a \cdot x \in I.$$

Un idéal d'un anneau n'est pas un sous-anneau sauf s'il contient l'élément $\mathbb{1}_{\mathbb{A}}$.

Exemple : $2\mathbb{Z}$ est un idéal de l'anneau $\mathbb{Z}$

On est habitué à l'utilisation de $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$. En effet ce sont ces deux structures il y a quelque chose qui les distingue. C'est le fait que tous ces éléments non nuls admettent un inverse.

Définition

Un corps est un anneau où tous les éléments admettent un inverse pour la multiplication.

- Les corps infinis usuels sont : $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ et $(\mathbb{C}, +, \cdot)$.
- Un exemple d'un corps fini est $\mathbb{F}_p = (\mathbb{Z}/p\mathbb{Z}, +, \cdot)$ où p est un nombre premier