CH 0) Structures algébriques

1. Relations d'ordre, d'équivalence : rappels

1.1. **Relation binaire.** Soit E un ensemble. Une relation binaire sur E est la donnée d'une partie $\mathcal{R}$ de $E \times E$. On note $x\mathcal{R}y$ pour signifier $(x, y) \in \mathcal{R}$.

Définition 1.1.
- *$\mathcal{R}$ est réflexive si et seulement si :* $\forall x \in E, x\mathcal{R}x$,
- *$\mathcal{R}$ est symétrique si et seulement si :* $\forall x, y \in E, x\mathcal{R}y \implies y\mathcal{R}x$,
- *$\mathcal{R}$ est transitive si et seulement si :* $\forall x, y, z \in E, (x\mathcal{R}y \text{ et } y\mathcal{R}z) \implies (x\mathcal{R}z)$,
- *$\mathcal{R}$ est antisymétrique si et seulement si :*
  $\forall x, y \in E, (x\mathcal{R}y \text{ et } y\mathcal{R}x) \implies (x = y)$,

Définition 1.2. *Une application $f : E \to F$ est compatible avec une relation binaire $\mathcal{R}$ sur E si :*

$$\forall x, y \in E,\ x\mathcal{R}y \implies f(x) = f(y)$$

1.2. **Relation d'ordre.**

Définition 1.3. *Une relation binaire sur un ensemble est une **relation d'ordre** si elle est **réflexive, antisymétrique et transitive.** Un ensemble muni d'une relation d'ordre est dit **ensemble ordonné.***

Il est pratique et usuel de noter $\preceq$ une relation d'ordre.

Exemple 1.4.
- ***Ordre usuel de*** $\mathbb{R}$ ***:*** *il s'agit de l'ordre $\leq$ usuel.*
- ***Divisibilité :*** *c'est la relation sur $\mathbb{N}^*$ définie par $x\mathcal{R}y$ si et seulement si x divise y. On la note $/$.*
- ***Inclusion :*** *C'est la relation $\subset$ définie sur E, où E est l'ensemble $\mathcal{P}(X)$ des parties d'un ensemble X.*

Soit $(E, \preceq)$ un ensemble ordonné. Deux éléments x et y de E sont dits **comparables** (pour $\preceq$) si on a $x \preceq y$ ou $y \preceq x$.

Si toute paire d'éléments est comparable, l'ordre est dit **total**. Sinon, il est dit **partiel**.

1.3. **Relation d'équivalence.** Un *relation d'équivalence* est une relation binaire qui est **réflexive, symétrique** et **transitive**.

1.3.1. *Égalité :* C'est la relation binaire définie par $x\mathcal{R}y \Leftrightarrow x = y$. C'est une relation d'équivalence.

1.3.2. *Relation induite par une application :* Soit $f : E \to F$ une application. La relation $x\mathcal{R}_f y \Leftrightarrow f(x) = f(y)$ est une relation d'équivalence sur E.

1.3.3. *Ensemble quotient :*

Définition 1.5. *Pour tout élément x de E la classe d'équivalence de x est la partie de E formée des éléments y de E tels que $x\mathcal{R}y$. On la note : $[x]$.*

$$[x] := \{y \in E/\ x\mathcal{R}y\}$$

Autres notations : $cl(x)$, $\bar{x}$.

Chaque classe d'équivalence est donc un sous-ensemble de $\mathcal{P}(E)$.

Définition 1.6. *L'ensemble des classes d'équivalences de $\mathcal{R}$ est appelé ensemble quotient de E par $\mathcal{R}$ (ou aussi quotient de E modulo $\mathcal{R}$). On le note $E_{/\mathcal{R}}$.*

Remarque 1.7. *On remarque que si $x\mathcal{R}y$, alors $[x] = [y]$. En effet, pour tout z dans $[x]$, on a $x\mathcal{R}z$. Or, comme $\mathcal{R}$ est symétrique, on a $y\mathcal{R}x$, et donc, par transitivité, que $y\mathcal{R}z$: z est dans la classe d'équivalence de y. En d'autre terme, on a montré $[x] \subset [y]$. Un argument analogue montre l'inclusion inverse $[y] \subset [x]$, d'où l'égalité $[x] = [y]$.*

Théorème 1.8. *L'ensemble quotient $E_{/\mathcal{R}}$ est une partition de E.* □

Rappelons qu'une partition de E est un ensemble de parties de E non-vides, deux-à-deux disjointes, et que leur union est E tout entier.

Théorème 1.9. *Soit Π une partition de l'ensemble. Il existe une et une seule relation d'équivalence $\mathcal{R}$ sur E telle que $\Pi = E_{/\mathcal{R}}$.* □

1.3.4. *Factorisation canonique.*

Définition 1.10. *Soit $\mathcal{R}$ une relation d'équivalence sur un ensemble E. L'application qui a un élément x de E associe sa classe d'équivalence $[x]$ est appelée surjection canonique. Elle est notée $p_{\mathcal{R}} : E \to E_{/\mathcal{R}}$.*

C'est bien une application, et elle bien surjective (puisque pour toute classe d'équivalence $[x]$ on a $p_{\mathcal{R}}(x) = [x]$ pour tout élément x de $[x]$).

Théorème 1.11. *Soit $\mathcal{R}$ une relation d'équivalence sur un ensemble E, et $f : E \to F$ une application quelconque. On note $p_{\mathcal{R}} : E \to E_{/\mathcal{R}}$ la surjection canonique.*

Alors, une condition nécessaire et suffisante pour que f soit compatible avec $\mathcal{R}$ est qu'il existe une application $g : E_{/\mathcal{R}} \to F$ telle que $f = g \circ p_{\mathcal{R}}$.

*Dans ce cas, g est unique et est appelé **passage au quotient de f modulo $\mathcal{R}$.***

Démonstration.

- *La condition est suffisante :* On suppose qu'il existe une application $g : E_{\mathcal{R}} \to F$ telle que $f = g \circ p_{\mathcal{R}}$. Alors, si x, y sont deux éléments de E tels que $x\mathcal{R}y$ on a :

$$\begin{aligned} f(x) = g(p_{\mathcal{R}}(x)) &= g([x]) \\ &= g([y]) \text{ car } [x] = [y] \text{ puisque } x\mathcal{R}y \\ &= g(p_{\mathcal{R}}(y)) \\ &= f(y) \end{aligned}$$

  Donc f est compatible avec $\mathcal{R}$.
- *La condition est nécessaire :* On suppose que f est compatible avec $\mathcal{R}$. Soit X un élément de $E_{/\mathcal{R}}$. Par définition, il existe un élément x de X (mais pas un seul en général !) tel que $X = [x]$. On a envie de définir $g(X)$ comme étant $f(x)$, mais celà ne définit peut-tre pas une application, puisqu'un autre choix de représentant y de X peut produire une autre valeur $f(y)$.

  Le point est qu'en fait la valeur $f(x)$ ne dépend pas du choix de x. En effet : soit y un élément de E tel que $y \in X$. Alors, $[y] = X = [x]$ et donc $x\mathcal{R}y$.

Comme f est compatible avec $\mathcal{R}$, on obtient $f(y) = f(x)$. On peut donc bien définir $g(X) = f(x)$ puisque ela ne dépend pas de x.

En outre :

$$\forall x \in E,\ g \circ p_{\mathcal{R}}(x) = g([x]) = f(x) \text{ (car } x \in [x])$$

Nous avons donc bien montré qu'il s'agit d'une condition nécessaire et suffisante.

Voyons pourquoi lorsque f est compatible avec $\mathcal{R}$, l'application g est unique :

Soit $g' : E_{\mathcal{R}} \to F$ une autre application telle que $f = g' \circ p_{\mathcal{R}}$. Alors, pour tout X dans $E_{\mathcal{R}}$, soit x un élément de E tel que $X = [x]$. Par définition, on a $g(X) = f(x)$. Par ailleurs, on doit avoir :

$$f(x) = g' \circ p_{\mathcal{R}}(x) = g'([x]) = g'(X)$$

Donc $g'(X) = g(X)$ quel que soit l'élément X de $E_{\mathcal{R}}$: les applications g et g' sont égales.

□

2. Structures algébriques

2.1. **Lois de composition.** Dans toute section, E, Λ désignent deux ensembles

Définition 2.1. *Une **loi de composition interne** sur E est une application $E \times E \to E$. On la note en général de la manière suivante : on choisit un symbole (par exemple $\top$) et pour tout x, y dans E, on écrit :*

$$x \top y$$

pour signifier l'image du couple (x, y) par la loi de composition interne.

Voici les exemples à avoir en tête :
- L'addition dans $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$,
- La multiplication dans $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$,
- La soustraction dans $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ ou $\mathbb{C}$,
- La composition $\circ$ dans l'ensemble $S(X)$ des bijections (les permutations) d'un ensemble X.
- L'addition dans les entiers modulo p : $\mathbb{Z}/p\mathbb{Z}$.

Exercice 2.2. *La division est-elle une loi de composition interne dans $\mathbb{Q}$?*

Définition 2.3. *Une **loi de composition externe** sur E de **domaine d'opérateur** Λ, est une application $\Lambda \times E \to E$. On la note en général de la manière suivante : on choisit un symbole (par exemple $\clubsuit$) et pour tout x dans E, λ dans Λ, on écrit :*

$$\lambda \clubsuit x$$

pour signifier l'image du couple (λ, x) par la loi de composition externe.

l'exemple essentiel est celui d'un espace vectoriel E sur $\Lambda = \mathbb{R}$ ou $\mathbb{C}$: l'addition des vecteurs est une loi de composition interne, mais la multiplication par un scalaire est une loi de composition externe.

2.1.1. *Parties stables.* – Une partie A d'un ensemble E est stable pour une loi de composition interne $\top$ sur E si pour tout x, y dans A, le "produit" $x \top y$ est dans A. On peut alors restreindre la loi de composition interne à A : on obtient la **loi induite**.

– Une partie A d'un ensemble E est stable pour une loi de composition externe $\clubsuit$ sur E de domaine d'opérateurs Λ si pour tout x dans A et tout λ dans Λ, le "produit" $\lambda \clubsuit x$ est dans A. On peut alors restreindre la loi de composition externe à A : on obtient la **loi induite**.

2.1.2. *Propriétés éventuelles de lois de composition.* Une loi de composition interne $\top$ est :

Associative: si pour tout x, y, z dans E on a $(x\top y)\top z = x\top(y\top z)$. On peut alors écrire $x\top y\top z$.

Commutative: si pour tout x, y dans E on a $x\top y = y\top x$.

Un **élément neutre** de $(E,\top)$ est un élément e tel que :

$$\forall x \in E,\ x\top e = e\top x = x$$

Exercice 2.4. *Montrer que si un élément neutre existe, il est unique.*

Supposons que $(E,\top)$ admet un élément neutre e. Alors, un élément x de E est **symétrisable** s'il existe un élément x' de E tel que :

$$x\top x' = x'\top x = e$$

Ce x' est alors un *symétrique* de x.

Exercice 2.5. *Montrer que si $(E,\top)$ est associative et admet un élément neutre, alors pour tout x dans E, le symétrique de x, s'il existe, est unique.*

Soit $\top$, $\diamond$ deux lois de composition interne sur un même ensemble E. Alors $\top$ est **distributive** par rapport à $\diamond$ si :

$$\forall x,y,z \in E,\ \begin{cases} x\top(y\diamond z) = (x\top y)\diamond(x\top z) \\ \qquad\qquad\text{et} \\ (y\diamond z)\top x = (y\top x)\diamond(z\top x) \end{cases}$$

De même, une loi de composition externe $\clubsuit : \Lambda \times E \to E$ est **distributive** par rapport à une loi de composition interne $\top$ sur E si :

$$\forall x,y \in E\ \forall \lambda \in \Lambda,\ \lambda\clubsuit(x\top y) = (\lambda\clubsuit x)\top(\lambda\clubsuit y)$$

2.1.3. *Conventions de notations.*

– Si $\top$ est une loi de composition interne, on définit par récurrence la puissance n-ième d'un élément : $\top^1 x = x$, et $\top^{n+1}x = x\top(\top^n x)$. Si $\top$ admet un élément neutre e, par convention :

$$\top^0 x = e$$

Exercice 2.6. *On suppose que $\top$ est associative. Montrer que pour tout x dans E, et tout entier m, n :*

$$(\top^m x)\top(\top^n x) = \top^{m+n}x$$

– si en outre $(E,\top)$ admet un élément neutre, et si x est un élément de E admettant un symétrique x', on étend la notation $\top^n x$ aux entiers n négatifs en convenant :

$$\top^n x := \top^{|n|}x'$$

– en pratique, lorsqu'aucune confusion est à craindre, on utilise la **notation multiplicative** : on utilise le symbole . ou le symbole "vide" au lieu de $\top$: le produit $x\top y$ s'écrit alors $x.y$, ou encore xy. L'élément neutre, s'il existe, est alors noté 1, et les puissances $\top^n x$ sont notés x^n (en particulier, le symétrique, s'il existe, est noté x^{-1}).

Attention ! Ne pas confondre ce 1, élément neutre, avec l'entier 1 !

– Si la loi de composition interne est commutative, on privilégie la **notation additive :** on utilise le symbole $+$, l'élément neutre éventuel est noté 0, l'éventuel symétrique est noté $(-x)$, la puissance n-ième est notée $n.x$.

2.2. **Morphismes.**

Définition 2.7. *Soient* $(E, \top)$ *et* $(E', \top')$ *deux ensembles munis de lois de composition internes. Une application* $f : (E, \top) \to (E', \top')$ *est un* ***morphisme*** *(ou* ***homomorphisme****) si :*

$$\forall x, y \in E,\ f(x \top y) = f(x) \top' f(y)$$

Définition 2.8. *Soient* $(E, \clubsuit)$ *et* $(E', \spadesuit)$ *deux ensembles munis de lois de composition externes de même domaine d'opérateurs* Λ*. Une application* $f : (E, \clubsuit) \to (E', \spadesuit)$ *est un* ***morphisme*** *(ou* ***homomorphisme****) si :*

$$\forall \lambda \in \Lambda,\ \forall x \in E,\ f(\lambda \clubsuit x) = \lambda \spadesuit f(x)$$

Remarque 2.9. *Il arrive qu'on considère des ensembles munis de plusieurs lois de composition interne ou externe. Une application entre tels ensembles est alors un (homo)morphisme si elle l'est pour chacune des lois de composition.*

Un morphisme est un **endomorphisme** si l'ensemble d'arrivée est égal à l'ensemble de départ. C'est un **isomorphisme** s'il est bijectif. Un endomorphisme bijectif est appelé **automorphisme**.

On rappelle que toute bijection admet une application réciproque.

Théorème 2.10. *La composée de deux morphismes est un morphisme.*

L'application réciproque d'un isomorphisme est un (iso)morphisme.

2.3. **Lois produits.** Soit $(E_i)_{i \in I}$ une famille d'ensembles. On suppose que chaque E_i est muni d'une loi de composition interne $\top_i$.

Définition 2.11. *Le produit des* $(E_i, \top_i)$ *est la loi de composition interne* $\top$ *sur le produit* $\prod_{i \in I} E_i$ *définie par :*

$$(x_i)_{i \in I} \top (y_i)_{i \in I} := (x_i \top_i y_i)_{i \in I}$$

Exemple 2.12. *On considère l'ensemble des suites* $(u_n)_{n \in \mathbb{N}}$ *de nombres réels (ici,* $I = \mathbb{N}$ *et chaque* $(E_i, \top_i)$ *est égal à* $(\mathbb{R}, +)$*). Alors :*

$$(u_n)_{n \in \mathbb{N}} + (v_n)_{n \in \mathbb{N}} = (u_n + v_n)_{n \in \mathbb{N}}$$

De même, si chaque E_i est muni d'une loi de composition externe $\clubsuit_i$ **- ayant toute le même domaine d'opérateurs** Λ**,** on définit :

Définition 2.13. *Le produit des* $(E_i, \clubsuit_i)$ *est la loi de composition externe* $\clubsuit$ *sur le produit* $\prod_{i \in I} E_i$ *définie par :*

$$\lambda \clubsuit (x_i)_{i \in I} := (\lambda \clubsuit_i x_i)_{i \in I}$$

Il est clair que l'opération "prendre le produit" préserve les propriétés observées par *tous* les $\top_i$. Par exemple, si tous les $\top_i$ sont associatifs (resp. commutatifs), il en est de même pour la loi produit.

Si chaque E_i est muni d'une loi de composition externe $\clubsuit_i$ distributive par rapport à $\top_i$, alors la loi de composition externe produit sur $\prod_{i \in I} E_i$ est distributive par rapport à loi de composition interne.