REPUBLIQUE DU CAMEROUN
Paix – Travail – Patrie
****

UNIVERSITE DE YAOUNDE I
ECOLE NORMALE SUPERIEURE
DEPARTEMENT DE MATHEMATIQUES
****

REPUBLIC OF CAMEROUN
Peace – Work – Fatherland
****

UNIVERSITY OF YAOUNDE I
HIGHER TEACHER TRAINING COLLEGE
DEPARTMENT OF MATHEMATICS
****

UNE INTRODUCTION DES CLONES

Mémoire de DI.P.E.S II de mathématiques

Par :

KENGNE CHATUE Bethsaïda
Licencié en Mathématiques

Sous la direction
Dr TEMGOUA ALOMO Etienne Romuald
Chargée de Cours

Année Académique
2015-2016

Dédicace

À mon papa, Chatué Ernest, pour l'éducation qu'il m'a inculquée.

Remerciements

Tous mes remerciements à l'endroit des personnalités suivantes :
Tout d'abord, à mon encadreur, Dr TEMGOUA ALOMO Etienne Romuald pour les sacrifices consentis pour la réalisation de ce mémoire.
Ensuite, à tout le personnel enseignant du département de mathématiques de l'École Normale Supérieure de Yaoundé pour leur suivi indéfectible.
Enfin aux membres de ma famille, ma maman, Yvonne CHATUÉ, mon tuteur et sa femme, TAMOU CHATUÉ Alzafor et Marceline TAMOU, mes frères, DJOMMOU CHATUÉ Hachis, MOUTÉ CHATUÉ Sylvestre, KENGNE CHATUÉ Peter, TAMKO Olivier et ma sœur MOTIO CHATUÉ Rachel pour leur soutien inconditionnel. Sans oublier mes camarades de promotion pour leur solidarité et mes amis pour leur soutien sans contrepartie.

Déclaration sur l'honneur

Le présent travail est une œuvre originale du candidat et n'a été soumis nul part ailleurs, en partie ou en totalité, pour une autre évaluation académique. Les contributions externes ont été dument mentionnées et recensées en bibliographie.

Signature du candidat

KENGNE CHATUE Bethsaïda

Résumé

L'étude des clones a commencé en 1941 avec POST E.L qui décrivit le treillis des clones sur un ensemble à deux éléments. Le but de notre travail est de donner les outils qui permettront de mieux saisir la notion de clone. Pour le faire, nous procédons par deux approches à savoir : l'approche algébrique et l'approche catégorielle. Nous obtiendrons à partir de l'approche algébrique les théorèmes de Rosenberg caractérisant les clones maximaux et les clones minimaux.
Mots clés : clone, polymorphismes, relations invariantes, connexion de Galois, théorie de Lawvere.

Abstract

The study of the clones started in 1941 with POST E.L which described the lattice of the clones on a whole with two elements. The aim of our work is to give the tools which will make it possible to better seize the concept of clone. To do it, we proceed by two approaches namely : algebraic approach and category approach. We will obtain starting from the algebraic approach the theorems of Rosenberg characterizing the maximal clones and the minimal clones.

Keys words : clone, polymorphisms, invariant relationships, Galois connection, Lawvere theory.

Table des figures

Liste des tableaux

Table des matières

Introduction générale

En 1941, POST E.L présenta le treillis des clones sur un ensemble à deux éléments. Jablonskii en 1958 a caractérisé tous les clones maximaux pour un ensemble à trois éléments. En 1965, Rosenberg I.G. a généralisé les résultats de Jablonskii pour un ensemble fini d'éléments. Depuis 1941, certains mathématiciens cherchent à faire une généralisation des résultats de POST E.L sur un ensemble fini de cardinal supérieur ou égal à trois, ce qui permettra de mieux comprendre les algèbres universelles. Malheureusement, pour un ensemble à trois éléments, le treillis des clones contient $2^{\aleph_0}$ éléments et sa structure est complexe et peu connue. Bill Lawvere en 1963 dans sa thèse nous montre à partir de sa théorie (théorie de Lawvere) qu'on pouvait définir les clones à partir des catégories. Face à cette situation, on peut se poser les questions suivantes : qu'est ce qu'un clone du point de vue algébrique ? Qu'est ce qu'un clone du point de vue catégoriel ? Quels sont les outils qui permettrons de mieux saisir cette notion de clone ? Notre travail est organisé de la façon suivante : Dans le Chapitre 1, nous donnerons les notions nécessaires pour la compréhension de ce travail. Dans le chapitre 2, nous parlerons de la vision algébrique des clones ; nous présentons la notion de clone, de clone maximal, de clone minimal et nous donnerons les théorèmes caractérisant les clones maximaux et les clones minimaux. Le chapitre 3 sera consacré à l'approche catégorielle des clones : ici, nous introduirons la théorie de Lawvere et nous étudierons le lien entre cette théorie et celle des clones.

CHAPITRE UN

OPÉRATIONS, RELATIONS ET TREILLIS

Dans ce chapitre, nous donnerons les notions nécessaires pour la compréhension de ce travail.

1.1 Opérations et relations

1.1.1 Opérations

Soient n et k des entiers naturels. Désignons par E_k l'ensemble $E_k = \{0, 1, ..., k-1\}$ avec $k \geqslant 2$.

Définition 1.1.1. Une opération n-aire sur E_k est une application $f : E_k^n \to E_k$.

Notation 1.1.1. On la note $f^{(n)}$.

n est appelé arité de l'opération f.

Notation 1.1.2. L'ensemble des opérations n-aires sur E_k est noté $O_{E_k}^{(n)}$. L'ensemble des opérations sur E_k est noté O_{E_k} où $O_{E_k} = \bigcup_{n=1}^{+\infty} O_{E_k}^{(n)}$.

Exemple 1.1.1. Soit $(G, +)$ un groupe fini. Soit $n \in \mathbb{N},\ n \geqslant 2$.

$$\begin{array}{rccl} f: & G^n & \to & G \\ & (x_1, x_2, ..., x_n) & \mapsto & f(x_1, x_2, ..., x_n) \quad = x_1 + x_2 + ... + x_n \end{array}$$

est une opération d'arité n sur G.

Définition 1.1.2. L'opération constante n-aire C_a est l'application de $E_k^n \to E_k$ définie par : $C_a(x_1, ..., x_n) = a$.

Définition 1.1.3. Pour $1 \leqslant i \leqslant n$, la i^{eme} projection n-aire sur E_k notée $P_i^{(n)}$ est l'application définie de E_k^n vers E_k par $P_i^{(n)}(x_1, ..., x_n) = x_i$.

Notation 1.1.3. L'ensemble des projections sur E_k est noté P_{E_k}.

Définition 1.1.4. Soient f une opération n-aire et $g_1, ..., g_n$ n opérations m-aires. On définit la composition de f et $g_1, ..., g_n$ par $f(g_1, ..., g_n)(h_1, ..., h_m) = f(g_1(h_1, ..., h_m), ..., g_n(h_1, ..., h_m))$ $\forall (h_1, ..., h_m) \in E_k^m$.

Exemple 1.1.2. L'application

$$\begin{array}{cccccc} f: & \mathbb{Z}_3^2 & \to & \mathbb{Z}_3 & \\ & (x_1, x_2) & \mapsto & f(x_1, x_2) & = x_1 + x_2 \end{array}$$

est une opération 2-aire et les applications

$$\begin{array}{cccccc} g_1: & \mathbb{Z}_3^3 & \to & \mathbb{Z}_3 & \\ & (a_1, a_2, a_3) & \mapsto & g_1(a_1, a_2, a_3) & = a_1a_2a_3 \end{array},$$

$$\begin{array}{cccccc} g_2: & \mathbb{Z}_3^3 & \to & \mathbb{Z}_3 & \\ & (b_1, b_2, b_3) & \mapsto & g_2(b_1, b_2, b_3) & = b_1b_2 + b_3 \end{array}$$

sont deux opérations 3-aires.
Soit $(h_1, h_2, h_3) \in \mathbb{Z}_3^3$.

$$\begin{array}{rcl} f(g_1, g_2)(h_1, h_2, h_3) & = & f(g_1(h_1, h_2, h_3), g_2(h_1, h_2, h_3)) \\ & = & f(h_1h_2h_3, h_1h_2 + h_3) \\ & = & h_1h_2h_3 + h_1h_2 + h_3 \end{array}$$

Exemple 1.1.3. L'application

$$\begin{array}{cccccc} f: & \mathbb{Z}_2^3 & \to & \mathbb{Z}_2 & \\ & (x_1, x_2, x_3) & \mapsto & f(x_1, x_2, x_3) & = x_1 + x_2x_3 \end{array}$$

est une opération 3-aire, et les applications

$$\begin{array}{cccccc} g_1: & \mathbb{Z}_2^2 & \to & \mathbb{Z}_2 & \\ & (a_1, a_2) & \mapsto & g_1(a_1, a_2,) & = a_1 + a_2 \end{array}, \quad \begin{array}{cccccc} g_2: & \mathbb{Z}_2^2 & \to & \mathbb{Z}_2 & \\ & (b_1, b_2) & \mapsto & g_2(b_1, b_2) & = b_1b_2 \end{array}$$

et

$$\begin{array}{cccccc} g_3: & \mathbb{Z}_2^2 & \to & \mathbb{Z}_2 & \\ & (c_1, c_2) & \mapsto & g_3(c_1, c_2) & = c_1 + c_2 \end{array}$$

sont trois opérations 2-aires.
Soit $(h_1, h_2) \in \mathbb{Z}_2^2$.

$$\begin{aligned} f(g_1, g_2, g_3)(h_1, h_2) &= f(g_1(h_1, h_2), g_2(h_1, h_2), g_3(h_1, h_2)) \\ &= f(h_1 + h_2, h_1 h_2, h_1 + h_2) \\ &= h_1 + h_2 + h_1 h_2 (h_1 + h_2) \\ &= h_1 + h_2 + h_1^2 h_2 + h_1 h_2^2 \end{aligned}$$

1.1.2 Relations

Définition 1.1.5. Une relation h-aire sur $E_k (h \in \mathbb{N})$ est une partie du produit cartésien E_k^h.
Une relation binaire (respectivement ternaire) est une relation 2-aire (respectivement 3-aire).

Notation 1.1.4. L'ensemble des relations h-aires sur E_k est noté $R_{E_k}^{(h)}$ et l'ensemble des relations sur E_k est noté R_{E_k} où $R_{E_k} = \bigcup\limits_{h=0}^{+\infty} R_{E_k}^{(h)}$.

Notation 1.1.5. Si ρ est une relation binaire sur E_k, on écrit parfois $x\rho y$ pour dire que $(x, y) \in \rho$.

Remarque 1.1.1. Une relation peut aussi être donnée sous forme matricielle où les colonnes de la matrice sont les éléments de la relation.

Notation 1.1.6. Si $\rho = \{(a_1, ..., a_h), (b_1, ..., b_h), (c_1, ..., c_h)\}$ est une relation d'arité h, alors on peut encore l'écrire :

$$\rho = \begin{pmatrix} a_1 & b_1 & c_1 \\ \vdots & \vdots & \vdots \\ a_h & b_h & c_h \end{pmatrix}$$

Définition 1.1.6. Une relation d'équivalence ρ sur E_k est une relation binaire vérifiant :
a) $\forall\, x \in E_k$, $(x, x) \in \rho$ (reflexivité)
b) $\forall\, x, y \in E_k$, $(x, y) \in \rho \Rightarrow (y, x) \in \rho$ (symétrique)
c) $\forall\, x, y, z \in E_k$, $(x, y) \in \rho$ et $(y, z) \in \rho \Rightarrow (x, z) \in \rho$ (transitivité).

Remarque 1.1.2. Une relation d'équivalence est dite non triviale si elle est distincte de E_k^2 et de Δ_{E_k} où $\Delta_{E_k} = \{(x, x), x \in E_k\}$. Δ_{E_k} est appelée la diagonale de E_k.

Exemple 1.1.4. Sur $E_4 = \{0, 1, 2, 3\}$, la relation ρ définie par :

$$\rho = \begin{pmatrix} 0 & 1 & 2 & 3 & 0 & 1 & 1 & 2 & 0 & 2 \\ 0 & 1 & 2 & 3 & 1 & 0 & 2 & 1 & 2 & 0 \end{pmatrix}$$

est une relation d'équivalence non triviale ayant pour classes d'équivalence $[0]_\rho = \{0, 1, 2\}$; $[3]_\rho = \{3\}$.

Définition 1.1.7. Une relation d'ordre ρ sur E_k est une relation binaire vérifiant a), c) de la Définition 1.1.6 et d) $\forall x, y \in E_k, ((x, y) \in \rho$ et $(y, x) \in \rho) \Rightarrow (x = y)$.
Si de plus il existe $m, M \in E_k$ tels que $\forall x \in E_k, (m, x) \in \rho$ et $(x, M) \in \rho$, alors on dit que ρ est une relation d'ordre bornée.

Exemple 1.1.5. Sur $E_4 = \{0, 1, 2, 3\}$, on définit les relations ρ_1 et ρ_2 par :

$$\rho_1 = \begin{pmatrix} 0 & 1 & 2 & 3 & 0 & 1 & 0 \\ 0 & 1 & 2 & 3 & 1 & 2 & 2 \end{pmatrix}$$

$$\rho_2 = \begin{pmatrix} 0 & 1 & 2 & 3 & 0 & 0 & 0 & 1 & 3 \\ 0 & 1 & 2 & 3 & 1 & 2 & 3 & 2 & 2 \end{pmatrix}$$

ρ_1 est une relation d'ordre sur E_4 et ρ_2 est une relation d'ordre bornée par 0 et 2 sur E_4.

Définition 1.1.8. Soit P un entier naturel premier. Un groupe abélien $(E_k, +, e)$ est dit P-groupe élémentaire si

$$P.x = \underbrace{x + x + \cdots + x}_{P \text{ fois}} = e$$

$\forall x \in E_k$. Par exemple, $(\mathbb{Z}_2, +, 0)$ est un 2-groupe élémentaire car $\forall x \in \mathbb{Z}_2$, $2.x = x + x = 0$.
Pour une opération binaire $+$ sur E_k, posons $\lambda_+ = \{(x, y, z, t) \in E_k^4 \mid x + y = z + t\}$.
ρ est une relation affine sur E_k s'il existe un P-groupe élémentaire $(E_k, +, e)$ tel que $\rho = \lambda_+$.

Exemple 1.1.6. $(\mathbb{Z}_2, +, 0)$ est un 2-groupe élémentaire.

$$\rho = \begin{pmatrix} 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix} = \lambda_+$$

est une relation affine sur $\mathbb{Z}_2$.

Définition 1.1.9. 1) Une permutation σ de E_k est une bijection de E_k vers E_k.
2) L'ordre de σ est le plus petit entier $r \geqslant 1$ tel que $\sigma^r = Id_{E_k}$.
3) Un point fixe de σ est un élément de E_k tel que $\sigma(x) = x$.
4) Le graphe de σ noté $gr(\sigma)$ est l'ensemble $gr(\sigma) = \{(x, \sigma(x)), x \in E_k\}$.
5) Une permutation est dite d'ordre premier si son ordre est un nombre premier.
Si σ est d'ordre premier, alors $gr(\sigma)$ est appelé le graphe d'une permutation d'ordre premier.

Exemple 1.1.7. Sur $E_4 = \{0, 1, 2, 3\}$, la permutation σ définie par $\sigma = (01)(23)$ est une permutation d'ordre 2 sans point fixe. Son graphe est

$$gr(\sigma) = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 1 & 0 & 3 & 2 \end{pmatrix}$$

$gr(\sigma)$ est donc le graphe d'une permutation d'ordre premier sans point fixe.

Définition 1.1.10. Une relation h-aire ρ $(h \geq 2)$ est :
- totalement réflexive (ou réflexive pour h = 2) si $\forall (a_1, ..., a_h) \in E_k^h, (a_1, ..., a_h) \in \rho$ dès qu'il existe $i, j \in \{1, ..., h\}, i \neq j$ tel que $a_i = a_j$ c'est-à-dire que ρ contient tous les h-uplets sur E_k avec au moins une répétition.
- totalement symétrique (ou symétrique pour h = 2) si $\forall (a_1, ..., a_h) \in \rho$ et toute permutation σ de $\{1, ..., h\}$, l'on a $(a_{\sigma(1)}, ..., a_{\sigma(h)}) \in \rho$.
Si ρ est totalement réflexive et totalement symétrique, on définit le centre de ρ par :
$C_\rho = \{x \in E_k : \forall x_2, ..., x_h \in E_k, (x, x_2, ..., x_h) \in \rho\}$.

Définition 1.1.11. Soit ρ une relation d'arité n sur E_k. On dit que ρ est une relation centrale lorsque ρ est un sous-ensemble propre de E_k^n ou bien ρ est totalement réflexive, totalement symétrique et C_ρ est un sous-ensemble propre non vide de E_k.

Remarque 1.1.3. Une relation 1-aire centrale sur E_k est un sous-ensemble propre non vide de E_k.

Exemple 1.1.8. $\rho = \begin{pmatrix} 0 & 1 & 2 & 3 & 0 & 0 & 0 & 1 & 2 & 3 \\ 0 & 1 & 2 & 3 & 1 & 2 & 3 & 0 & 0 & 0 \end{pmatrix}$
est une relation binaire centrale sur E_4 et 0 est l'élément central de cette relation.

Définition 1.1.12. Soit $l \in \mathbb{N}^*$. Une famille T = $\{\rho_1, ..., \rho_l\}$ de relations d'équivalence sur E_k est dite u-régulière avec $u \geqslant 3$ et $u^l \leq k$ si

- $\forall i \in \{1, ..., l\}$, la relation ρ_i possède exactement u classes d'équivalences.
- $\bigcap_{i=1}^{l} C_i \neq \emptyset$ où C_i est une classe d'équivalence de $\rho_i, \forall i \in \{1, ..., l\}$.

La relation λ_T donnée par une famille u-régulière T est définie par :

$$\lambda_T = \{(x_1, ..., x_u) : \forall\, i = 1, ..., l \ \ \exists\, m, n \in \{1, ..., u\} \text{ avec } m \neq n \text{ tel que } (x_m, x_n) \in \rho_i\}.$$

Une relation est dite régulière si elle est de la forme λ_T.

Exemple 1.1.9. Sur $E_4 = \{0, 1, 2, 3\}$, prenons $u = 3$ et $l = 1$. La relation d'équivalence définie par :

$$\rho = \begin{pmatrix} 0 & 1 & 2 & 3 & 0 & 1 \\ 0 & 1 & 2 & 3 & 1 & 0 \end{pmatrix}$$

a pour classes d'équivalence $[0]_\rho = \{0, 1\}; [2]_\rho = \{2\}; [3]_\rho = \{3\}$. $T = \{\rho\}$ est 3-régulière. La relation ρ_1 définie par

$$\rho_1 = \{(x_1, x_2, x_3) \in E_4^3 \mid (x_1, x_2) \in \rho \text{ ou } (x_1, x_3) \in \rho \text{ ou } (x_2, x_3) \in \rho\}$$

est de la forme λ_T. Donc c'est une relation régulière.

Remarque 1.1.4. Les relations régulières sont totalement symétriques et totalement réflexives.

1.2 Treillis

Définition 1.2.1. Un ensemble non vide L muni de deux opérations binaires $\vee$ et $\wedge$ est appelé treillis si $\vee$ et $\wedge$ satisfont les conditions suivantes : $\forall\, x, y, z \in L$

$L_1)$ $x \vee y = y \vee x$ et $x \wedge y = y \wedge x$ (commutativité des lois)

$L_2)$ $x \vee (y \vee z) = (x \vee y) \vee z$ et $x \wedge (y \wedge z) = (x \wedge y) \wedge z$ (associativité des lois)

$L_3)$ $x \vee x = x$ et $x \wedge x = x$ (idempotence des lois)

$L_4)$ $x = x \vee (x \wedge y)$ et $x = x \wedge (x \vee y)$ (absorption des lois).

Exemple 1.2.1. Soit P l'ensemble des propositions. Soit $\vee$ le connecteur "ou" et $\wedge$ le connecteur "et". $(P, \vee, \wedge)$ est un treillis.

Exemple 1.2.2. Soit L l'ensemble des nombres naturels. Soit $\vee$ le plus petit commun multiple et $\wedge$ le plus grand commun diviseur. $(L, \vee, \wedge)$ est un treillis.

Exemple 1.2.3. Soient G un groupe et $N(G)$ l'ensemble des sous groupes normaux de G. On définit les opérations $\vee$ et $\wedge$ dans $N(G)$ par $N_1 \vee N_2 = N_1N_2 = \{n_1n_2 : n_1 \in N_1, n_2 \in N_2\}$, et $N_1 \wedge N_2 = N_1 \cap N_2$. Alors, $(N(G), \vee, \wedge)$ est un treillis.

Exemple 1.2.4. Soient A un anneau et $I(A)$ l'ensemble des idéaux de A. On définit les opérations $\vee$ et $\wedge$ dans $I(A)$ par $I_1 \vee I_2 = \{i_1 + i_2 : i_1 \in I_1, i_2 \in I_2\}$ et $I_1 \wedge I_2 = I_1 \cap I_2$. Alors $(I(A), \vee, \wedge)$ est un treillis.

Théorème 1.2.1. L est un treillis si et seulement si L est un ensemble partiellement ordonné tel que $\forall x, y \in L, sup\{x, y\}$ et $inf\{x, y\}$ existent dans L.

Démonstration. (A) Si $(L, \vee, \wedge)$ est un treillis, alors on définit la relation d'ordre $\leq$ sur L par $\forall x, y \in L, x \leq y \Leftrightarrow x = x \wedge y$.
(B) Si $(L, \leq)$ est un treillis, alors on définit les opérations binaires $\vee$ et $\wedge$ dans L par :
$x \vee y = sup\{x, y\}$ et $x \wedge y = inf\{x, y\}$ $\forall x, y \in L$.
Supposons que L est un treillis et $\leq$ la relation définie en (A)
$\rightarrow$ Soit $x \in L$. De $x \wedge x = x$, on a : $x \leq x$. Donc $\leq$ est réflexive.
$\rightarrow$ Soient $x, y \in L$ tels que $x \leq y$ et $y \leq x$. Alors $x = x \wedge y$ et $y = y \wedge x$. Puisque $x \wedge y = y \wedge x$ alors $x = y$. D'où $\leq$ est antisymétrique.
$\rightarrow$ Soient $x, y, z \in L$ tels que $x \leq y$ et $y \leq z$. Alors $x = x \wedge y$ et $y = y \wedge z$; donc $x = x \wedge y = x \wedge (y \wedge z) = (x \wedge y) \wedge z = x \wedge z$; ceci entraine $x \leq z$.
D'où $\leq$ est transitive.
Ce qui montre que $\leq$ est un ordre partiel sur L.
$\rightarrow$ Soient $x, y \in L$. Montrons que $sup\{x, y\}$ et $inf\{x, y\}$ existent dans L.
. On a : $x = x \wedge (x \vee y)$ et $y = y \wedge (y \vee x) = y \wedge (x \vee y)$; donc $x \leq x \vee y$ et $y \leq x \vee y$ et par suite, $x \vee y$ est un majorant de $\{x, y\}$.
Maintenant, si $x \leq u$ et $y \leq u$ alors $x \vee u = (x \wedge u) \vee u = u$ et $y \vee u = u$; donc $(x \vee u) \vee (y \vee u) = u \vee u = u$. $(x \vee y) \wedge u = (x \vee y) \wedge [(x \vee y) \vee u] = x \vee y$. D'où $x \vee y \leq u$ et donc $x \vee y = sup\{x, y\}$.
. On a $x \wedge y = (x \wedge y) \vee x$ et $x \wedge y = (x \wedge y) \vee y$; donc $x \wedge y \leq x$ et $x \wedge y \leq y$ et par suite, $x \wedge y$ est un minorant de $\{x, y\}$.
Maintenant, si $u \leq x$ et $u \leq y$ alors $u = u \wedge x = u \wedge y$; donc $u \wedge (x \wedge y) = (u \wedge x) \wedge y = u \wedge y = u$. D'où $u \leq x \wedge y$ et donc $x \wedge y = inf\{x, y\}$.
Donc L est un ensemble partiellement ordonné tel que $\forall x, y \in L, sup\{x, y\}$ et $inf\{x, y\}$ existent dans L.
Supposons que L est un ensemble partiellement ordonné tel que $\forall x, y \in L, sup\{x, y\}$ et $inf\{x, y\}$ existent dans L et supposons les opérations $\vee$ et $\wedge$ définies en (B).
$\rightarrow$ Soient $x, y \in L$. Alors $sup\{x, y\} = sup\{y, x\}$ et $inf\{x, y\} = inf\{y, x\}$. Donc $x \vee y = y \vee x$ et $x \wedge y = y \wedge x$.
$\rightarrow$ Soient $x, y, z \in L$. Alors $sup\{x, y \vee z\} = sup\{x, sup\{y, z\}\} = sup\{x, y, z\} = sup\{sup\{x, y\}, z\} = sup\{x \vee y, z\}$. Donc $x \vee (y \vee z) = (x \vee y) \vee z$. De même, on montre que $x \wedge (y \wedge z) = (x \wedge y) \wedge z$.
$\rightarrow$ Soit $x \in L$. Alors $sup\{x, x\} = x$ et $inf\{x, x\} = x$. Donc $x = x \vee x$ et $x = x \wedge x$.
$\rightarrow$ Soient $x, y \in L$. Alors on a $sup\{x, inf\{x, y\}\} = x$ et $inf\{x, sup\{x, y\}\} = x$.

Donc $x = x \vee (y \wedge z)$ et $x = x \wedge (y \vee z)$.
Donc L est un treillis. $\square$

Exemple 1.2.5. Soit X un ensemble non vide et $\mathcal{P}(X)$ l'ensemble des parties de X. Alors, $(\mathcal{P}(X), \subseteq)$ est un treillis. En effet pour tous A et B éléments de $\mathcal{P}(X)$, $A \cup B = sup\{A, B\}$ et $A \cap B = inf\{A, B\}$.

Exemple 1.2.6. Soit $\mathcal{C}([0,1])$ l'ensemble des fonctions continues de $[0,1]$ dans $\mathbb{R}$. On définit la relation $\mathcal{R}$ dans $\mathcal{C}([0,1])$ par $f\mathcal{R}g \Leftrightarrow f(a) \leq g(a)\ \forall a \in [0,1]$. Alors, $(\mathcal{C}([0,1]), \mathcal{R})$ est un treillis. En effet, soient f et g des éléments de $\mathcal{C}([0,1])$. Considérons les applications suivantes :

$$\begin{array}{rccl} M: & [0,1] & \rightarrow & \mathbb{R} \\ & a & \mapsto & M(a) = \frac{f(a)+g(a)+|f(a)-g(a)|}{2} \end{array}$$

et

$$\begin{array}{rccl} m: & [0,1] & \rightarrow & \mathbb{R} \\ & a & \mapsto & m(a) = \frac{f(a)+g(a)-|f(a)-g(a)|}{2} \end{array}$$

Posons $M(a) = max(f(a), g(a))$ et $m(a) = min(f(a), g(a))$. Alors $M = sup\{f, g\}$ et $m = inf\{f, g\}$.

Exemple 1.2.7. Soient G un groupe et $S(G)$ l'ensemble des sous groupes de G.
Alors $(S(G), \subseteq)$ est un treillis. En effet, soient H_1 et H_2 deux sous groupes de G. Alors,
$< H_1 \cup H_2 >= sup\{H_1, H_2\}$ et $< H_1 \cap H_2 >= inf\{H_1, H_2\}$.

Exemple 1.2.8. Soient (X, T) un espace topologique, $\mathcal{F}_X$ l'ensemble des fermés de X et $\mathcal{O}_X$ l'ensemble des ouverts de X. Alors $(\mathcal{F}_X, \subseteq)$ et $(\mathcal{O}_X, \subseteq)$ sont des treillis. En effet, soient F_1 et F_2 des fermés de X, O_1 et O_2 des ouverts de X. Alors, $F_1 \cup F_2 = sup\{F_1, F_2\}$ et $F_1 \cap F_2 = inf\{F_1, F_2\}$. De même $O_1 \cup O_2 = sup\{O_1, O_2\}$ et $O_1 \cap O_2 = inf\{O_1, O_2\}$.

CHAPITRE DEUX

APPROCHE ALGÉBRIQUE DES CLONES

Dans ce chapitre, nous parlerons de la vision algébrique des clones. Nous définirons la notion de clone, de clone maximal, de clone minimal et nous donnerons les théorèmes caractérisant les clones maximaux et les clones minimaux.

2.1 Définitions

Définition 2.1.1. Soient $m, n \in \mathbb{N}$. Un ensemble F d'opérations sur E_k est fermé pour la composition si pour tout $f \in F \cap O_{E_k}^{(n)}$ et tous $g_1, ..., g_n \in F \cap O_{E_k}^{(m)}$, l'on a $f(g_1, ..., g_n) \in F \cap O_{E_k}^{(m)}$.

Définition 2.1.2. Un clone sur E_k est un sous-ensemble $\mathcal{C}$ de O_{E_k} qui contient les projections et qui est fermé pour la composition.

Exemple 2.1.1. P_{E_k} et O_{E_k} sont des clones.

Exemple 2.1.2. $F = \{f^{(n)} \in O_{E_k} \mid f(0, ..., 0) = 0,\ n \in \mathbb{N}^*\}$ est un clone.
En effet, soient $i \in \{1, ...n\}, n \geq 2, P_i^{(n)}$ la i-ème projection n-aire sur O_{E_k}. On a : $P_i^{(n)}(0, ...0) = 0$. Donc $P_i^{(n)} \in F$. Donc F contient toutes les projections.
Soient $f \in F \cap O_{E_k}^{(n)}$ et $g_1, ..., g_n \in F \cap O_{E_k}^{(m)}$. On a :

$$\begin{aligned} f(g_1, ..., g_n)(0, ..., 0) &= f(g_1(0, ..., 0), ..., g_n(0, ...0)) \\ &= f(0, ..., 0) \quad car\ \ g_1, ..., g_n \in F \cap O_{E_k}^{(m)} \\ &= 0 \quad car\ \ f \in F \cap O_{E_k}^{(n)} \end{aligned}$$

Donc F est fermé pour la composition. Donc F est un clone.

Exemple 2.1.3. $G = \{f^{(n)} \in O_{E_k} \mid f(\{0,1\}^n) \subseteq \{0,1\},\ n \in \mathbb{N}^*\}$ est un clone.
En effet, soient $i \in \{1, ...n\}, n \geq 2, P_i^{(n)}$ la i-ème projection n-aire sur O_{E_k}. On a :

$$\begin{aligned} P_i^{(n)}(\{0,1\}^n) &= P_i^{(n)}(\{0,1\} \times ... \times \{0,1\}) \\ &= \{0,1\} \\ &\subseteq \{0,1\} \end{aligned}$$

Donc G contient toutes les projections.
Soient $f \in G \cap O_{E_k}^{(n)}$ et $g_1, ..., g_n \in G \cap O_{E_k}^{(m)}$. On a :

$$\begin{aligned} f(g_1, ..., g_n)(\{0,1\}^m) &= f(g_1(\{0,1\}^m), ..., g_n(\{0,1\}^m)) \\ &\subseteq f(\{0,1\} \times ... \times \{0,1\}) \quad car \ \ g_1, ..., g_n \in G \cap O_{E_k}^{(m)} \\ &\subseteq f(\{0,1\}^n) \\ &\subseteq \{0,1\} \quad car \ \ f \in G \cap O_{E_k}^{(n)} \end{aligned}$$

Donc G est fermé pour la composition. Donc G est un clone.

Remarque 2.1.1. F et G ne sont pas comparables. En effet, considérons la fonction
$f : \{0,1,2\}^3 \to \{0,1,2\}$ définie par :

$$f(x,y,z) = \begin{cases} 0 & \text{si } x = y = z = 0 \\ 2 & \text{ailleurs} \end{cases}$$

$f(0,0,0) = 0$. Donc $f \in F$. $f(\{0,1\}^3) = f(\{0,1\} \times \{0,1\} \times \{0,1\}) = \{0,2\} \nsubseteq \{0,1\}$. Donc $f \notin G$. On conclut que $F \nsubseteq G$.
Considérons la fonction
$g : \{0,1\}^2 \to \{0,1\}$ définie par :

$$g(x,y) = \begin{cases} 1 & \text{si } x = y = 0 \\ 0 & \text{ailleurs} \end{cases}$$

$g(\{0,1\}^2) = g(\{0,1\} \times \{0,1\}) = \{0,1\}$. Donc $g \in G$. $g(0,0) = 1$. Donc $g \notin F$. On conclut que $G \nsubseteq F$.

Remarque 2.1.2. • L'intersection de clones sur E_k est un clone sur E_k.
• L'ensemble des clones sur E_k ordonné par la relation d'inclusion forme un treillis. Ce treillis contient un plus petit élément qui est P_{E_k} et un plus grand élément qui est O_{E_k}.

Définition 2.1.3. Soit $F \subseteq O_{E_k}$. On appelle clone engendré par F et on note $< F >$ le plus petit clone contenant F. On dit alors que les opérations dans F sont des générateurs du clone.

Exemple 2.1.4. Soit $f : E_k \to E_k$ une opération unaire. Montrons que $< \{f\} > = \{f^n \circ P_i^{(m)} : n \in \mathbb{N}, m \in \mathbb{N}^*, 1 \leq i \leq m\}$.
$\subseteq$) Posons $H = \{f^n \circ P_i^{(m)} : n \in \mathbb{N}, m \in \mathbb{N}^*, 1 \leq i \leq m\}$. Montrons que H est un clone.
$\forall m \in \mathbb{N}^*,\ \forall i \in \{1, ..., m\}$, $P_i^{(m)} = f^0 \circ P_i^{(m)} \in H$. Donc H contient les projections.
Soient $f^{(n)}, g_1^{(m)}, ..., g_n^{(m)} \in H$. Alors, il existe $n_0, e_1, ..., e_n \in \mathbb{N},\ j \in \{1, ..., n\},\ i_1, ..., i_n \in \{1, ..., m\}$ tels que $f = f^{n_0} \circ p_j^{(n)},\ \ g_1 = f^{e_1} \circ p_{i_1}^{(m)}, ..., g_n = f^{e_n} \circ p_{i_n}^{(m)}$. Soient $x_1, ..., x_m \in E_k$.

$$\begin{aligned}
f(g_1, ..., g_n)(x_1, ..., x_m) &= f(g_1(x_1, ..., x_m), ..., g_n(x_1, ..., x_m)) \\
&= f(f^{e_1} \circ p_{i_1}^{(m)}(x_1, ..., x_m), ..., f^{e_n} \circ p_{i_n}^{(m)}(x_1, ..., x_m)) \\
&= f(f^{e_1}(x_{i_1}), ..., f^{e_n}(x_{i_n})) \\
&= f^{n_0} \circ p_j^{(n)}(f^{e_1}(x_{i_1}), ..., f^{e_n}(x_{i_n})) \\
&= f^{n_0}(f^{e_j}(x_{i_j})) \\
&= f^{n_0+e_j}(x_{i_j}) \\
&= f^{n_0+e_j} \circ p_{i_j}^{(m)}(x_1, ..., x_m)
\end{aligned}$$

D'où $f(g_1, ..., g_n) = f^{n_0+e_j} \circ p_{i_j}^{(m)} \in H$. Donc H est un clone. Par suite, H est un clone contenant $\{f\}$. D'où $< \{f\} > \subseteq \{f^n \circ P_i^{(m)} : n \in \mathbb{N}, m \in \mathbb{N}^*, 1 \leq i \leq m\}$.
$\supseteq$) Soient $n \in \mathbb{N}, m \in \mathbb{N}^*$ et $i \in \{1, ..., m\}$. Montrons que $f^n \circ p_i^{(m)} \in < \{f\} >$. Puisque $< \{f\} >$ est un clone, alors $f^n, p_i^{(m)} \in < \{f\} >$. D'où $f^n \circ p_i^{(m)} \in < \{f\} >$.

Exemple 2.1.5. Dans E_2, $< \{\neg, \wedge\} >$ est l'ensemble des fonctions booléennes avec

x	0	1
$\neg x$	1	0

TABLE 2.1 – Table de définition de $\neg$ sur E_2

x	y	$x \wedge y$
0	0	0
0	1	0
1	0	0
1	1	1

TABLE 2.2 – Table de définition de $\wedge$ sur E_2

Définition 2.1.4. Soient $f \in O^{(n)}_{E_k}$ et $\rho \in R^{(h)}_{E_k}$. On dit que f préserve ρ si $\forall x_1, x_2, ..., x_n \in \rho$ avec

$$x_i = \begin{pmatrix} x_i^1 \\ x_i^2 \\ \vdots \\ x_i^h \end{pmatrix}$$

$\forall i \in \{1, ..., n\}$, on a

$$\begin{pmatrix} f(x_1^1, \cdots, x_n^1) \\ f(x_1^2, \cdots, x_n^2) \\ \vdots \\ f(x_1^h, \cdots, x_n^h) \end{pmatrix} \in \rho$$

Notation 2.1.1. On note $f \lhd \rho$ pour dire que f préserve ρ.

Définition 2.1.5. On dit aussi que f est un polymorphisme de ρ lorsque $f \lhd \rho$.

Notation 2.1.2. L'ensemble des opérations qui préservent ρ est noté $Pol\rho$.

Exemple 2.1.6. Déterminons $Pol\rho$ pour $\rho = \{0\}$ et $\rho = \{0, 1\}$.
Montrons que pour $\rho = \{0\}$, $Pol\rho = \{f^{(n)} \in O_{E_k} \mid f(0, ..., 0) = 0,\ n \in \mathbb{N}^*\} = Pol(\{0\})$.
Posons $F = \{f^{(n)} \in O_{E_k} \mid f(0, ..., 0) = 0,\ n \in \mathbb{N}^*\}$. Montrons que $Pol\rho = F$. Soit $f^{(n)} \in Pol(\{0\})$. Alors $f^{(n)}$ préserve $\{0\}$ c'est-à-dire comme $0, ..., 0 \in \{0\}$, $f(0, ..., 0) \in \{0\}$. Par suite, $f(0, ..., 0) = 0$ et donc $f^{(n)} \in F$. Donc $Pol(\{0\}) \subseteq \{f^{(n)} \in O_{E_k} \mid f(0, ..., 0) = 0,\ n \in \mathbb{N}^*\}$.
Soit $f^{(n)} \in F$. Alors, $f(0, ..., 0) = 0$. Or $0, ..., 0 \in \{0\}$ et $f(0, ..., 0) \in \{0\}$ entrainent que $f^{(n)}$ préserve $\{0\}$. Donc $f^{(n)} \in Pol(\{0\})$. Donc $\{f^{(n)} \in O_{E_k} \mid f(0, ..., 0) = 0,\ n \in \mathbb{N}^*\} \subseteq Pol(\{0\})$.

Montrons que pour $\rho = \{0,1\}$, $Pol\rho = \{f^{(n)} \in O_{E_k} \mid f(\{0,1\}^n) \subseteq \{0,1\},\ n \in \mathbb{N}^*\} = Pol(\{0,1\})$.
Posons $G = \{f^{(n)} \in O_{E_k} \mid f(\{0,1\}^n) \subseteq \{0,1\},\ n \in \mathbb{N}^*\} = Pol(\{0,1\})$. Montrons que $Pol\rho = G$.
$\subseteq$) Soit $f^{(n)} \in Pol\rho$. Montrons que $f^{(n)} \in G$. Soient $(x_1, ..., x_n) \in \{0,1\}^n$, alors $x_1, ..., x_n \in \{0,1\} = \rho$. Puisque $f \lhd \rho$, alors $f(x_1, ..., x_n) \in \{0,1\}$. D'où $f^{(n)} \in G$.
$\supseteq$) Soit $f^{(n)} \in G$. Montrons que $f^{(n)} \in Pol\rho$. Soient $x_1, ..., x_n \in \rho = \{0,1\}$. Alors $(x_1, ..., x_n) \in \{0,1\}^n$. Puisque $f^{(n)} \in G$, alors $f(x_1, ..., x_n) \in \{0,1\}$. D'où $f^{(n)} \in Pol\rho$.

Lemme 2.1.3. Pour toute relation ρ sur E_k, $Pol\rho$ est un clone sur E_k.

Démonstration. Soient ρ une relation h-aire sur E_k, $n \geq 1$, $i \in \{1, ..., n\}$ et $x_1, ..., x_n \in \rho$. Alors

$$\begin{aligned}
P_i^{(n)}\begin{pmatrix} x_1^1 & x_2^1 & \cdots & x_n^1 \\ x_1^2 & x_2^2 & \cdots & x_n^2 \\ \vdots & \vdots & \ddots & \vdots \\ x_1^h & x_2^h & \cdots & x_n^h \end{pmatrix} &= \begin{pmatrix} P_i^{(n)}(x_1^1, \cdots, x_n^1) \\ P_i^{(n)}(x_1^2, \cdots, x_n^2) \\ \vdots \\ P_i^{(n)}(x_1^h, \cdots, x_n^h) \end{pmatrix} \\
&= \begin{pmatrix} x_i^1 \\ x_i^2 \\ \vdots \\ x_i^h \end{pmatrix} \\
&= x_i \in \rho
\end{aligned}$$

Donc $Pol\rho$ contient toutes les projections.
Soient $f \in Pol\rho \cap O_{E_k}^{(n)}$ et $g_1, ..., g_n \in Pol\rho \cap O_{E_k}^{(m)}$. On a :

$$\begin{aligned}
f(g_1, ..., g_n)\begin{pmatrix} x_1^1 & x_2^1 & \cdots & x_m^1 \\ x_1^2 & x_2^2 & \cdots & x_m^2 \\ \vdots & \vdots & \ddots & \vdots \\ x_1^h & x_2^h & \cdots & x_m^h \end{pmatrix} &= \begin{pmatrix} f(g_1, \cdots, g_n)(x_1^1, \cdots, x_m^1) \\ f(g_1, \cdots, g_n)(x_1^2, \cdots, x_m^2) \\ \vdots \\ f(g_1, \cdots, g_n)(x_1^h, \cdots, x_m^h) \end{pmatrix} \\
&= \begin{pmatrix} f(g_1(x_1^1, \cdots, x_m^1), \cdots, g_n(x_1^1, \cdots, x_m^1)) \\ f(g_1(x_1^2, \cdots, x_m^2), \cdots, g_n(x_1^2, \cdots, x_m^2)) \\ \vdots \\ f(g_1(x_1^h, \cdots, x_m^h), \cdots, g_n(x_1^h, \cdots, x_m^h)) \end{pmatrix} \in \rho
\end{aligned}$$

Donc $Pol\rho$ est fermé pour la composition.
On conclut que $Pol\rho$ est un clone sur E_k. $\square$

Exemple 2.1.7. Pour $\theta = \{(0,0);(1,1);(2,2);(3,3);(0,1);(1,0)\}$, $Pol\theta$ est un clone sur E_4.

2.2 Polymorphismes et clones

2.2.1 Polymorphismes et relations invariantes

Notation 2.2.1. Soient A un ensemble non vide, $F \subseteq O_A$ et $\mathcal{R} \subseteq \mathcal{R}_A$. On note $Pol\mathcal{R}$ l'ensemble des opérations sur A qui préservent chaque relation de $\mathcal{R}$ et $InvF$ l'ensemble des relations sur A préservées par chaque opération de F c'est-à-dire $Pol\mathcal{R} = \{f \in O_A \mid \forall\sigma \in \mathcal{R},\ f \lhd \sigma\}$ et $InvF = \{\sigma \in \mathcal{R}_A \mid \forall f \in F,\ f \lhd \sigma\}$.

Définition 2.2.1. Soient A, I, J des ensembles non vides, $\mathcal{R} \subseteq A^J$ et $\sigma : I \to J$ une fonction. $\mathcal{R} * \sigma$ est le sous-ensemble de A^J défini par $\mathcal{R} * \sigma := \{v \circ \sigma \mid v \in \mathcal{R}\}$.

Définition 2.2.2. Soient A un ensemble non vide, I et J des ensembles, $\mathcal{S} \subseteq A^I$ et $\sigma : J \to I$. $(\mathcal{S} : \sigma)_I$ est le sous-ensemble de A^I défini par $(\mathcal{S} : \sigma)_I := \{g \in A^I \mid g \circ \sigma \in \mathcal{S}\}$.

Lemme 2.2.2. Soient A, I, J des ensembles non vides, $\mathcal{R} \subseteq A^J, \sigma : I \to J, \tau : J \to I$ et $f \in O_A$ tels que $f \lhd \mathcal{R}$. Alors $f \lhd \mathcal{R} * \sigma$ et $f \lhd (\mathcal{R} : \tau)_I$.

Démonstration. i) Montrons que $f \lhd \mathcal{R}*\sigma$. Soient n l'arité de f, $w_1, ..., w_n \in \mathcal{R}*\sigma$ et $k \in \{1, ..., n\}$. Puisque $w_k \in \mathcal{R} * \sigma$, il existe $v_k \in \mathcal{R}$ tel que $w_k = v_k \circ \sigma$. Soit

$$\begin{array}{llll} g: & J & \to & A \\ & j & \mapsto & g(j) = f(v_1(j), ..., v_n(j)) \end{array}$$

Puisque $v_1, ..., v_n \in \mathcal{R}$ et $f \lhd \mathcal{R}$, alors $g \in \mathcal{R}$ car $g = f(v_1, ..., v_n)$. Donc $g \circ \sigma \in \mathcal{R} * \sigma$. Ainsi $g \circ \sigma = \{f(v_1 \circ \sigma(i), ..., v_n \circ \sigma(i)) \mid i \in I\} = \{f(w_1(i), ..., w_n(i)) \mid i \in I\}$. Donc $f(w_1, ..., w_n) = g \circ \sigma \in \mathcal{R} * \sigma$.
ii) Soient n l'arité de f, $g_1, ..., g_n \in (\mathcal{R} : \tau)_I$ et $k \in \{1, ..., n\}$. Puisque $g_k \in (\mathcal{R} : \tau)_I$, alors $g_k \circ \tau \in \mathcal{R}$. $g_1 \circ \tau, ..., g_n \circ \tau \in \mathcal{R}$ et $f \lhd \mathcal{R}$ entrainent $f(g_1, ..., g_n) = \{f(g_1 \circ \tau(j), ..., g_n \circ \tau(j)) \mid j \in J\} \in \mathcal{R}$. Or $\{f(g_1 \circ \tau(j), ..., g_n \circ \tau(j)) \mid j \in J\} = \{f(g_1(i), ..., g_n(i)) \mid i \in I\} \circ \tau$. Donc $\{f(g_1(i), ..., g_n(i)) \mid i \in I\} \circ \tau \in \mathcal{R}$ c'est-à-dire $\{f(g_1(i), ..., g_n(i)) \mid i \in I\} \in (\mathcal{R} : \tau)_I$. On conclut que $f \lhd (\mathcal{R} : \tau)_I$. $\square$

Définition 2.2.3. Soient $m \in \mathbb{N}$, A un ensemble non vide et $F \subseteq O_A$. Nous définissons $Inv^{(m)}(F) = \{\mathcal{R} \subseteq A^m \mid \forall f \in F : f \triangleleft \mathcal{R}\}$ et $Inv(F) = \bigcup_{m=0}^{+\infty} Inv^{(m)}(F)$.

Notation 2.2.3. Soient $m \in \mathbb{N}$, A et I des ensembles non vides et $\mathcal{R} \subseteq A^I$. On note $Pol^{(m)}(\mathcal{R})$ l'ensemble des opérations m-aires qui préservent $\mathcal{R}$.

Proposition 2.2.4. Si $I_J (j \in J$ avec $J \neq \emptyset)$ sont des ensembles, $\mathcal{R}_j \subseteq A^{I_J}$ pour $j \in J$ et $\mathcal{R} = \{\mathcal{R}_j \mid j \in J\}$, alors $Pol^{(m)}(\mathcal{R}) = \bigcap_{\sigma \in \mathcal{R}} Pol^{(m)}(\sigma)$ et $Pol(\mathcal{R}) = \bigcup_{m=0}^{+\infty} Pol^{(m)}(\mathcal{R})$.

Démonstration. i)

$$\begin{aligned} f \in Pol^{(m)}(\mathcal{R}) &\Leftrightarrow f \triangleleft \mathcal{R} \\ &\Leftrightarrow \forall \sigma \in \mathcal{R}, f \in Pol^{(m)}(\sigma) \\ &\Leftrightarrow f \in \bigcap_{\sigma \in \mathcal{R}} Pol^{(m)}(\sigma) \end{aligned}$$

Donc $Pol^{(m)}(\mathcal{R}) = \bigcap_{\sigma \in \mathcal{R}} Pol^{(m)}(\sigma)$

ii) $\subseteq$)

$$\begin{aligned} f \in Pol(\mathcal{R}) &\Rightarrow f \text{ préserve chaque relation de } \mathcal{R} \\ &\Rightarrow \exists m \in \mathbb{N}, \exists \sigma \in \mathcal{R}, \sigma\ m - \text{aire tel que } f \triangleleft \sigma \\ &\Rightarrow \exists m \in \mathbb{N} \mid f \in Pol^{(m)}(\mathcal{R}) \\ &\Rightarrow f \in \bigcup_{m=0}^{+\infty} Pol^{(m)}(\mathcal{R}) \end{aligned}$$

Donc $Pol(\mathcal{R}) \subseteq \bigcup_{m=0}^{+\infty} Pol^{(m)}(\mathcal{R})$.

$\supseteq$) Pour $m \geq 0$,

$$Pol^{(m)}(\mathcal{R}) \subseteq Pol(\mathcal{R}) \Rightarrow \bigcup_{m=0}^{+\infty} Pol^{(m)}(\mathcal{R}) \subseteq Pol(\mathcal{R})$$

On conclut d'après les deux inclusions que $Pol(\mathcal{R}) = \bigcup_{m=0}^{+\infty} Pol^{(m)}(\mathcal{R})$.

□

Théorème 2.2.5. Soient F_1, F_2 des parties de O_A et S_1, S_2 des parties de $\mathcal{R}_A$. Alors :

a) si $F_1 \subseteq F_2$, alors $InvF_2 \subseteq InvF_1$

b) si $S_1 \subseteq S_2$, alors $PolS_2 \subseteq PolS_1$

c) $F_1 \subseteq Pol\ InvF_1$

d) $S_1 \subseteq Inv\ PolS_1$

e) $InvF_1 = Inv\ Pol\ InvF_1$

f) $PolS_1 = Pol\ Inv\ PolS_1$

Démonstration. a) Supposons que $F_1 \subseteq F_2$ et soit $\sigma \in InvF_2$. Alors σ est préservée par toutes les opérations de F_2 et en particulier celles de F_1 par hypothèse. Il en résulte que $\sigma \in InvF_2$. Donc $InvF_2 \subseteq InvF_1$.

b) Supposons que $S_1 \subseteq S_2$ et soit $f \in PolS_2$. Alors f préserve toutes les relations de S_2 et en particulier celles de S_1 par hypothèse. Il en résulte que $f \in polS_1$. Donc $PolS_2 \subseteq PolS_1$.

c) Soit $f \in F_1$. Alors f préserve toutes les relations de $InvF_1$. D'où $f \in Pol\ InvF_1$ et donc $F_1 \subseteq Pol\ InvF_1$.

d) Soit $\sigma \in S_1$. Alors σ est préservée par toutes les opérations de $PolS_1$. D'où $\sigma \in Inv\ PolS_1$ et donc $S_1 \subseteq Inv\ PolS_1$.

e) D'après c), $F_1 \subseteq Pol\ InvF_1$. En appliquant a) à cette inclusion, on obtient $Inv\ Pol\ InvF_1 \subseteq InvF_1$. D'après d) $S_1 \subseteq Inv\ PolS_1$. En posant $S_1 = InvF_1$, on obtient $InvF_1 \subseteq Inv\ Pol\ InvF_1$. D'où $InvF_1 = Inv\ Pol\ InvF_1$.

f) D'après d), $S_1 \subseteq Inv\ PolS_1$. En appliquant b) à cette inclusion, on obtient $Pol\ Inv\ PolS_1 \subseteq PolS_1$. D'après c) $F_1 \subseteq Pol\ InvF_1$. En posant $F_1 = PolS_1$, on obtient $PolS_1 \subseteq Pol\ Inv\ PolS_1$. D'où $PolS_1 = Pol\ Inv\ PolS_1$. $\square$

Lemme 2.2.6. Soient $\mathcal{C}$ un clone sur A, $n \in \mathbb{N}$, $f \in \mathcal{C} \cap O_A^{(n)}$ et $\mathcal{R} = \mathcal{C} \cap O_A^{(n)}$. Alors f $\triangleleft \mathcal{R}$.

Démonstration. Soient $g_1, ..., g_m \in \mathcal{R}$ et $f \in \mathcal{C} \cap O_A^{(m)}$. Alors $f(g_1, ..., g_m) \in \mathcal{C} \cap O_A^{(n)} = \mathcal{R}$ car $\mathcal{C}$ est un clone. D'où $f \triangleleft \mathcal{R}$. $\square$

Théorème 2.2.7. Soient $\mathcal{C}$ un clone sur A, $n \in \mathbb{N}, f : A^n \to A$ et $\mathcal{R} = \mathcal{C} \cap O_A^{(n)}$. Alors les propriétés suivantes sont équivalentes :

a) $f \in \mathcal{C}$

b) $f \triangleleft \mathcal{R}$

Si A est fini et $m = \mid A \mid^n$, alors chacune des propriétés précédentes est équivalente à :

c) $f \in Pol\ Inv^{(m)}(\mathcal{C})$

Démonstration. a) $\Rightarrow$ b) a été démontré au Lemme 2.2.6.

b) $\Rightarrow$ a) Supposons que $f \triangleleft \mathcal{R}$. Nous savons que $p_1^{(n)}, ..., p_n^{(n)} \in \mathcal{R}$ où

$$\begin{array}{rccl} p_i^{(n)}: & A^n & \to & A \\ & (x_1,...,x_n) & \mapsto & p^{(n)}(x_1,...,x_n) \ = x_i \end{array}$$

Puisque $f \lhd \mathcal{R}$, nous avons $\{f(p_1^{(n)}(i),...,p_n^{(n)}(i)) \mid i \in A^n\} \in \mathcal{R}$. D'où $f(p_1^{(n)},...,p_n^{(n)}) \in \mathcal{R}$. Ainsi $f \in \mathcal{R}$ et par suite $f \in \mathcal{C}$.

a) $\Rightarrow$ c) Supposons que $f \in \mathcal{C}$. Par le Théorème 2.2.5, nous avons $\mathcal{C} \subseteq Pol\ Inv(\mathcal{C})$. Puisque $Inv^{(m)}(\mathcal{C}) \subseteq Inv(\mathcal{C})$, alors a) du Théorème 2.2.5 permet d'écrire $Pol\ Inv(\mathcal{C}) \subseteq Pol\ Inv^{(m)}(\mathcal{C})$. D'où $f \in \mathcal{C} \subseteq Pol\ Inv(\mathcal{C}) \subseteq Pol\ Inv^{(m)}(\mathcal{C})$.

c) $\Rightarrow$ b) Supposons que $f \in Pol\ Inv^{(m)}(\mathcal{C})$. Du Lemme 2.2.6, pour toute opération $g \in \mathcal{C}, g \lhd \mathcal{R}$. Soient $\pi : \{1,...,m\} \to A^m$ une bijection et $\mathcal{R}_1 = \mathcal{R} * \pi = \{r \circ \pi \mid r \in \mathcal{R}\}$. $\mathcal{R}_1$ est un sous-ensemble de A^m. Par le Lemme 2.2.2, on aura $g \lhd \mathcal{R}_1$ pour tout $g \in \mathcal{C}$. Ainsi $\mathcal{R}_1 \in Inv^{(m)}(\mathcal{C})$. Puisque $f \in Pol\ Inv^{(m)}(\mathcal{C})$, on aura $f \lhd \mathcal{R}_1$. Maintenant $\mathcal{R} = \{f \circ \pi^{-1} \mid f \in \mathcal{R}_1\}$ et par le Lemme 2.2.2, $f \lhd (\mathcal{R}_1 * \pi^{-1}) = \mathcal{R}$. □

Théorème 2.2.8. Soient A un ensemble fini, $\mathcal{C}$ un clone sur A. Alors $\mathcal{C} = Pol\ Inv(\mathcal{C})$.

Démonstration. Le c) du Théorème 2.2.5 nous permet de conclure que $\mathcal{C} \subseteq Pol\ Inv(\mathcal{C})$.
Réciproquement soient $f \in Pol\ Inv(\mathcal{C})$, n l'arité de f, $m = |\ A\ |^n$. Alors $Inv^{(m)}(\mathcal{C}) \subseteq Inv(\mathcal{C})$. Par le b) du Théorème 2.2.5, on a $Pol\ Inv(\mathcal{C}) \subseteq Pol\ Inv^{(m)}(\mathcal{C})$. D'où $f \in Pol\ Inv^{(m)}(\mathcal{C})$. En appliquant le Théorème 2.2.7, on a $f \in \mathcal{C}$. □

Corollaire 2.2.9. Soient A un ensemble fini, F un sous-ensemble de O_A. Alors $Pol\ Inv(F)$ est un clone et pour tout clone $\mathcal{D}$ avec $F \subseteq \mathcal{D}$, nous avons $Pol\ Inv(F) \subseteq \mathcal{D}$.

Démonstration. Du Lemme 2.1.3 on conclut que $Pol\ Inv(F)$ est un clone.
Soit $\mathcal{D}$ un clone avec $F \subseteq \mathcal{D}$. En appliquant a) du Théorème 2.2.5, on obtient $Inv(\mathcal{D}) \subseteq Inv(F)$. En appliquant b) du Théorème 2.2.5, on obtient $Pol\ Inv(F) \subseteq Pol\ Inv(\mathcal{D})$. D'après le Théorème 2.2.8, $Pol\ Inv(\mathcal{D}) = \mathcal{D}$. D'où $Pol\ Inv(F) \subseteq \mathcal{D}$. □

Lemme 2.2.10. Soit ρ une relation binaire. $Pol(\rho) = O_{E_k}$ si et seulement si $\rho \in \{\emptyset, \Delta_{E_k}, E_k^2\}$.

Démonstration. Supposons que $Pol(\rho) = O_{E_k}$ et $\rho \notin \{\emptyset, \Delta_{E_k}, E_k^2\}$.
S'il existe $a \in E_k$ tel que $(a,a) \notin \rho$, alors on considère l'opération unaire f définie sur E_k par $f(x) = a$. Puisque $\rho \neq \emptyset$, il existe $(x,y) \in \rho$ et $(f(x), f(y)) = (a,a) \notin \rho$. Donc $f \notin Pol\rho = O_{E_k}$. Ce qui est absurde.
Sinon $\Delta_{E_k} \subsetneq \rho \subsetneq E_k^2$. Alors il existe $(a,b) \in E_k^2$ tel que $(a,b) \notin \rho$ et $(x,y) \in \rho$ tel que $x \neq y$. on

considère l'opération unaire g définie sur E_k par :

$$g(t) = \begin{cases} a & \text{si } t = x \\ b & sinon \end{cases}$$

$(x, y) \in \rho$ et $(g(x), g(y)) = (a, b) \notin \rho$. Donc $g \notin Pol\rho = O_{E_k}$. Ce qui est absurde.
Donc $\rho \in \{\emptyset, \Delta_{E_k}, E_k^2\}$.
Réciproquement supposons que $\rho \in \{\emptyset, \Delta_{E_k}, E_k^2\}$. Alors $Pol(\emptyset) = O_{E_k}, Pol(\Delta_{E_k}) = O_{E_k}$ et $Pol(E_k^2) = O_{E_k}$. □

Lemme 2.2.11. Soit θ une relation binaire telle que $\theta \notin \{\emptyset, \Delta_{E_k}, E_k^2\}$ et ρ une relation d'équivalence non triviale sur E_k. Si $Pol(\theta) = Pol(\rho)$, alors $\theta = \rho$.

Démonstration. Supposons que $Pol(\theta) = Pol(\rho)$
Montrons que $\rho \subseteq \theta$.
Soit $(x, y) \in \rho$.
Si $x = y$ alors $(x, x) \in \Delta_{E_k}$. Considérons l'opération unaire f définie sur E_k par $f(t) = x$. $(x, y) \in \rho$ entraine $(f(x), f(y)) = (x, x) \in \rho$. Donc $f \in Pol(\rho) = Pol(\theta)$ par hypothèse. Puisque $\theta \neq \emptyset$ alors il existe $(a, b) \in \theta$. $(a, b) \in \theta$ et $f \in Pol(\theta)$ entrainent $(f(a), f(b)) = (x, x) \in \theta$. Donc $(x, x) \in \theta$. Ainsi $\Delta_{E_k} \subseteq \theta$ et par suite $(x, y) \in \theta$. Ceci montre aussi que θ est réflexive.
Si $x \neq y$, alors soit $(a, b) \in \theta$ avec $a \neq b$.
Si $(a, b) \in \rho$, alors on considère l'opération unaire g définie par :

$$g(t) = \begin{cases} x & \text{si } t = a \\ y & sinon \end{cases}$$

On a : $g(\rho) \subseteq \{(x, x); (x, y); (y, y); (y, y)\} \subseteq \rho$ (car ρ est réflexive et symétrique). Donc $g \in Pol(\rho) = Pol(\theta)$ par hypothèse. $(a, b) \in \theta$ et $g \in Pol(\theta)$ entrainent $(g(a), g(b)) = (x, y) \in \theta$.
Si $(a, b) \notin \rho$, alors on considère l'opération unaire h définie par :

$$h(t) = \begin{cases} x & \text{si } (t, a) \in \rho \\ y & \text{si } (t, a) \notin \rho \end{cases}$$

On a : $h(\rho) \subseteq \{(x, x); (y, y)\} \subseteq \rho$ (car ρ est réflexive). Donc $h \in Pol(\rho) = Pol(\theta)$ d'après l'hypothèse. $(a, b) \in \theta$ et $h \in Pol(\theta)$ entrainent $(h(a), h(b)) = (x, y) \in \theta$. Donc $\rho \subseteq \theta$
Montrons que θ est symétrique.
Soit $(x, y) \in \theta$.
Si $(x, y) \in \rho$, alors $(y, x) \in \rho \subseteq \theta$ (car ρ est symétrique). Donc $(y, x) \in \theta$. Si $(x, y) \notin \rho$, alors on considère l'opération unaire j définie par :

$$j(t) = \begin{cases} y & \text{si } (t,x) \in \rho \\ x & sinon \end{cases}$$

On a : $j(\rho) \subseteq \{(x,x);(y,y)\} \subseteq \rho$ (car ρ est réflexive). Donc $j \in Pol(\rho) = Pol(\theta)$ par hypothèse. $(x,y) \in \theta$ et $j \in Pol(\theta)$ entrainent $(j(x), j(y)) = (y,x) \in \theta$. D'où θ est symétrique.
Montrons que $\theta \subseteq \rho$.
Supposons le contraire c'est-à-dire qu'il existe (x,y) dans ρ et $(x,y) \notin \rho$.
Soit $(a,b) \in \rho$ tel que $a \neq b$. On considère l'opération unaire k définie par :

$$k(t) = \begin{cases} x & \text{si } t = a \\ y & sinon \end{cases}$$

$k(\theta) \subseteq \{(x,x);(y,y);(x,y);(y,x)\} \subseteq \theta$ (car θ est réflexive et symétrique). Donc $k \in Pol(\theta)$. Mais $k \notin Pol(\rho)$. En effet, $(a,b) \in \rho$ et $(k(a), k(b)) = (x,y) \notin \rho$. Ce qui est absurde car $Pol(\rho) = Pol(\theta)$. D'où $\theta \subseteq \rho$ et on a donc l'égalité. □

Corollaire 2.2.12. Si θ est une relation binaire réflexive et symétrique, ρ une relation d'équivalence non triviale telle que $\rho \subsetneq \theta$ et $\theta \notin \{\emptyset, \Delta_{E_k}, E_k^2\}$, alors $Pol(\theta) \nsubseteq Pol(\rho)$.

Démonstration. $\rho \subsetneq \theta$ entraine qu'il existe $(x,y) \in \theta$ tel que $(x,y) \notin \rho$.
Soit $(a,b) \in \rho$ tel que $a \neq b$. On considère l'opération unaire m définie par :

$$m(t) = \begin{cases} x & \text{si } t = a \\ y & sinon \end{cases}$$

$m(\theta) \subseteq \{(x,x);(y,y);(x,y);(y,x)\} \subseteq \theta$ (car θ est réflexive et symétrique). Donc $m \in Pol(\theta)$. Mais $m \notin Pol(\rho)$. En effet $(a,b) \in \rho$ et $(m(a), m(b)) = (x,y) \notin \rho$. D'où $Pol(\theta) \nsubseteq Pol(\rho)$. □

2.2.2 Connexion de Galois

Définition 2.2.4. Soient A et B deux ensembles ; $\sigma : \mathcal{P}(A) \to \mathcal{P}(B)$ et $\tau : \mathcal{P}(B) \to \mathcal{P}(A)$ deux applications. On dit que (σ, τ) est une connexion de Galois de A et B si pour tous $X, X_1 \subseteq A$, $Y, Y_1 \subseteq B$, les conditions suivantes sont vérifiées :
a) $X \subseteq X_1 \Rightarrow \sigma(X_1) \subseteq \sigma(X)$
b) $Y \subseteq Y_1 \Rightarrow \tau(Y_1) \subseteq \tau(Y)$
c) $X \subseteq \tau\sigma(X)$
d) $Y \subseteq \sigma\tau(Y)$

Exemple 2.2.1. Soient A, B deux ensembles non vides, $\mathcal{R} \subseteq A \times B$ avec $\mathcal{R} \neq \emptyset$, $\sigma : \mathcal{P}(A) \to \mathcal{P}(B)$ et $\tau : \mathcal{P}(B) \to \mathcal{P}(A)$ des applications définies par :
$\sigma(X) = \{y \in B \mid \forall x \in X : (x, y) \in \mathcal{R}\}$
$\tau(Y) = \{x \in A \mid \forall y \in Y : (x, y) \in \mathcal{R}\}$
Montrons que (σ, τ) est une connexion de Galois entre A et B.
a) Soient $X, X_1 \subseteq A$ tels que $X \subseteq X_1$. Soit $y \in \sigma(X_1)$. Alors $\forall x \in X_1, (x, y) \in \mathcal{R}$. En particulier pour $x \in X, (x, y) \in \mathcal{R}$. Donc $y \in \sigma(X)$. On conclut que $\sigma(X_1) \subseteq \sigma(X)$.
b) Soient $Y, Y_1 \subseteq B$ tels que $Y \subseteq Y_1$. Soit $x \in \tau(Y_1)$. Alors $\forall y \in Y_1, (x, y) \in \mathcal{R}$. En particulier pour $y \in Y, (x, y) \in \mathcal{R}$. Donc $x \in \tau(Y)$. On conclut que $\tau(Y_1) \subseteq \tau(Y)$.
c) Soit $x \in X$. Alors x est en relation avec tous les éléments de $\sigma(X)$. D'où $x \in \tau(\sigma(X))$. Donc $X \subseteq \tau(\sigma(X))$.
d) Soit $y \in Y$. Alors y est en relation avec tous les éléments de $\tau(Y)$. D'où $y \in \sigma(\tau(Y))$. Donc $Y \subseteq \sigma(\tau(Y))$.
Donc (σ, τ) est une connexion de Galois entre A et B.

Théorème 2.2.13. Le couple (Pol, Inv) est une connexion de Galois entre O_A et $\mathcal{R}_A$.

Démonstration. Provient du Théorème 2.2.5. □

2.3 Clones maximaux et clones minimaux

2.3.1 Clones maximaux

Définition 2.3.1. Un clone $\mathcal{C}$ sur E_k est dit maximal si O_{E_k} est le seul clone contenant $\mathcal{C}$ de façon stricte.

Proposition 2.3.1. $\mathcal{C}$ est maximal sur E_k si et seulement si pour tout $f \in O_{E_k} \backslash \mathcal{C}$, on a $< \mathcal{C} \cup \{f\} > = O_{E_k}$.

Démonstration. $\Rightarrow$) Supposons que $\mathcal{C}$ soit maximal sur E_k et soit $f \in O_{E_k} \setminus \mathcal{C}$ une opération.
$\mathcal{C} \subset < \mathcal{C} \cup \{f\} > \subseteq O_{E_k}$. Par hypothèse, $< \mathcal{C} \cup \{f\} > = O_{E_k}$.
$\Leftarrow$) Réciproquement supposons que pour tout $f \in O_{E_k} \setminus \mathcal{C}$, on a $< \mathcal{C} \cup \{f\} > = O_{E_k}$. Supposons en outre que $\mathcal{C}$ n'est pas maximal sur E_k. Alors il existe un autre clone $\mathcal{D}$ tel que $\mathcal{C} \subset \mathcal{D} \subset O_{E_k}$. Soit $f_1 \in \mathcal{D} \setminus \mathcal{C}$. Alors $< \mathcal{C} \cup \{f_1\} > \subseteq < \mathcal{D} > = \mathcal{D}$ c'est-à-dire $O_{E_k} \subseteq \mathcal{D}$ par hypothèse. Ce qui est absurde car $\mathcal{D} \subset O_{E_k}$.
Il en résulte que $\mathcal{C}$ est maximal sur E_k. □

Théorème 2.3.2. (de classification de Rosenberg) [3]
Soit E_k un ensemble fini à k éléments avec $k \geq 2$. Un clone $\mathcal{C}$ sur E_k est maximal si et seulement s'il est de la forme $Pol\rho$ où ρ est une relation de l'un des six types suivants :
a) une relation d'ordre bornée,
b) une relation centrale,
c) une relation régulière,
d) une relation d'équivalence non triviale,
e) le graphe d'une permutation de E_k sans point fixe et d'ordre premier,
f) une relation affine.

Exemple 2.3.1. a)

$$\rho = \begin{pmatrix} 0 & 1 & 2 & 3 & 0 & 0 & 0 & 1 & 3 \\ 0 & 1 & 2 & 3 & 1 & 2 & 3 & 2 & 2 \end{pmatrix}$$

est une relation d'ordre bornée par 0 et 2 sur E_4. Donc $\mathcal{C} = Pol\rho$ est un clone maximal de E_4.
b)

$$\rho = \begin{pmatrix} 0 & 1 & 2 & 3 & 0 & 0 & 0 & 1 & 2 & 3 \\ 0 & 1 & 2 & 3 & 1 & 2 & 3 & 0 & 0 & 0 \end{pmatrix}$$

est une relation binaire centrale sur E_4. Donc $\mathcal{C} = Pol\rho$ est un clone maximal de E_4.
c)

$$\rho = \begin{pmatrix} 0 & 1 & 2 & 3 & 0 & 1 \\ 0 & 1 & 2 & 3 & 1 & 0 \end{pmatrix}$$

$$\rho_1 = \{\ (x_1, x_2, x_3\ ) \in E_4^3 \mid (x_1, x_2) \in \rho \text{ ou } (x_1, x_3) \in \rho \text{ ou } (x_2, x_3) \in \rho\ \}$$

est une relation régulière sur E_4. Donc $\mathcal{C} = Pol\rho_1$ est un clone maximal de E_4.
d)

$$\rho = \begin{pmatrix} 0 & 1 & 2 & 3 & 0 & 1 & 1 & 2 & 0 & 2 \\ 0 & 1 & 2 & 3 & 1 & 0 & 2 & 1 & 2 & 0 \end{pmatrix}$$

est une relation d'équivalence non triviale sur E_4. Donc $\mathcal{C} = Pol\rho$ est un clone maximal de E_4.
e)

$$\rho = gr(\sigma) = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 1 & 0 & 3 & 2 \end{pmatrix}$$

est le graphe d'une permutation de E_4 sans point fixe d'ordre 2. Donc $\mathcal{C} = Pol\rho$ est un clone maximal de E_4.

f)

$$\rho = \begin{pmatrix} 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix}$$

est une relation affine sur E_2. Donc $\mathcal{C} = Pol\rho$ est un clone maximal de E_2.

2.3.2 Clones minimaux

Définition 2.3.2. Un clone $\mathcal{C}$ sur E_k est dit minimal si le seul clone qu'il contient de façon stricte est P_{E_k}.

Proposition 2.3.3. $\mathcal{C}$ est minimal sur E_k si et seulement si pour tout $P \in \mathcal{C} \setminus P_{E_k}$, on a $< P_{E_k} \cup \{P\} > = \mathcal{C}$.

Démonstration. $\Rightarrow$) Supposons que $\mathcal{C}$ soit minimal sur E_k et soit $P \in \mathcal{C} \setminus P_{E_k}$. Alors, $\{P\} \subseteq \mathcal{C}$ et $P_{E_k} \subseteq \mathcal{C}$. Donc $P_{E_k} \cup \{P\} \subseteq \mathcal{C}$ et par suite $< P_{E_k} \cup \{P\} > \subseteq \mathcal{C}$. De plus, $P_{E_k} \subsetneq \; < P_{E_k} \cup \{P\} > \subseteq \mathcal{C}$. Par minimalité de $\mathcal{C}$, $< P_{E_k} \cup \{P\} > = \mathcal{C}$.

$\Leftarrow$) Réciproquement, supposons que pour tout $P \in \mathcal{C} \setminus P_{E_k}$, on a $< P_{E_k} \cup \{P\} > = \mathcal{C}$. Supposons de plus que $\mathcal{C}$ ne soit pas minimal sur E_k. Alors il existe un autre clone $\mathcal{E}$ tel que $P_{E_k} \subset \mathcal{E} \subset \mathcal{C}$. Soit $f_2 \in \mathcal{E} \setminus P_{E_k}$. Alors $< P_{E_k} \cup \{f_2\} > \subseteq < \mathcal{E} > = \mathcal{E}$ c'est-à-dire $\mathcal{C} \subseteq \mathcal{E}$ par hypothèse. Ce qui est absurde car $\mathcal{E} \subset \mathcal{C}$.

Il en résulte que $\mathcal{C}$ est minimal sur E_k. □

Théorème 2.3.4. (de classification de Rosenberg) [3]

Un clone $\mathcal{C}$ est minimal s'il est généré par une opération $f \in O_{E_k} \setminus P_{E_k}$ de l'un des cinq types suivants :

a) une opération 1-aire qui est une rétraction (c'est-à-dire $f^2 = f$) ou une permutation d'ordre premier,

b) une opération binaire idempotente (c'est-à-dire $f(x, x) = x$),

c) une opération majoritaire (c'est-à-dire $f(x, x, y) = f(x, y, x) = f(y, x, x) = x$),

d) une opération minoritaire (c'est-à-dire $f(x, y, z) = x + y + z$ où $(E_k, +)$ est un 2-groupe élémentaire),

e) une semi-projection non triviale k-aire $(k \geq 3)$ [c'est-à-dire $\exists\, i \in \{1, ..., k\}$ tel que $f(x_1, ..., x_k)$ $= x_i$ chaque fois que $\mid \{x_1, ..., x_k\} \mid < k$].

Exemple 2.3.2. a) $f : \mathbb{Z}_3 \to \mathbb{Z}_3$ est une opération définie par : $f(0) = 1$, $f(1) = 1$, $f(2) = 2$.
f est une opération 1-aire qui est une rétraction. Donc $\mathcal{C} = < f >$ est un clone minimal de $\mathbb{Z}_3$.
b)

$$\begin{array}{rccl} f : & \mathbb{Z}_3^2 & \to & \mathbb{Z}_3 \\ & (x, y) & \mapsto & f(x, y) \quad = 2x + 2y \end{array}$$

est une opération binaire idempotente. Donc $\mathcal{C} = < f >$ est un clone minimal de $\mathbb{Z}_3^2$.
c) $f : \mathbb{Z}_3^3 \to \mathbb{Z}_3$ est une opération définie par :

$$f(x, y, z) = \begin{cases} x & \text{si } (x = y \text{ ou } x = z) \\ y & \text{si } y = z \\ 0 & \text{ailleurs} \end{cases}$$

f est une opération majoritaire. Donc $\mathcal{C} = < f >$ est un clone minimal de $\mathbb{Z}_3^3$.
d)

$$\begin{array}{rccl} f : & \mathbb{Z}_2^3 & \to & \mathbb{Z}_2 \\ & (x, y, z) & \mapsto & f(x, y, z) \quad = x + y + z \end{array}$$

est une opération minoritaire. Donc $\mathcal{C} = < f >$ est un clone minimal de $\mathbb{Z}_2^3$.
e) $f : \mathbb{Z}_3^3 \to \mathbb{Z}_3$ est une opération définie par :

$$f(x, y, z) = \begin{cases} x & \text{si } \mid \{x, y, z\} \mid < 3 \\ 1 & \text{sinon} \end{cases}$$

f est une semi-projection non triviale 3-aire. Donc $\mathcal{C} = < f >$ est un clone minimal de $\mathbb{Z}_3^3$.

CHAPITRE TROIS

APPROCHE CATÉGORIELLE DES CLONES

Dans ce chapitre, nous introduirons la théorie de Lawvere et nous étudierons le lien entre cette théorie et celle des clones.

3.1 Catégories, foncteurs et transformations naturelles

3.1.1 Catégories

Définition 3.1.1. Une catégorie $\mathfrak{C}$ consiste en les données suivantes :
1) Une classe $ob(\mathfrak{C})$ dont les éléments notés A, B, C,... sont appelés les objets de $\mathfrak{C}$.
2) Une classe $Mor(\mathfrak{C})$ dont les éléments notés f, g, h,... sont appelés les morphismes ou les flèches de $\mathfrak{C}$. Chaque objet f de $Mor(\mathfrak{C})$ possède un domaine dom(f) et un codomaine cod(f) qui sont les objets de $\mathfrak{C}$. On notera f : dom$(f) \to$ cod(f) pour signifier que f a pour domaine dom(f) et pour codomaine cod(f).
3) Une composition des flèches de $\mathfrak{C}$ qui, à tout couple (f, g) de flèches de $\mathfrak{C}$ tel que cod(f) = dom(g) associe une unique flèche $g \circ f$ dont le domaine est celui de f et le codomaine celui de g.
4) Une correspondance qui, à tout objet A de $\mathfrak{C}$ associe une flèche 1_A qui a pour domaine A et pour codomaine A.
Ces quatre données doivent satisfaire les deux axiomes suivants :
axiome 1 : pour toutes flèches $f : A \to B$, $g : B \to C$ et $h : C \to D$ de $\mathfrak{C}$, on a : $(h \circ g) \circ f = h \circ (g \circ f)$.
axiome 2 : Si f est une flèche de A vers B, alors $f \circ 1_A = f$ et $1_B \circ f = f$.

Notation 3.1.1. La classe des flèches pour une catégorie $\mathfrak{C}$ est encore notée $hom_{\mathfrak{C}}(A, B)$ ou $Hom_{\mathfrak{C}}(A, B)$ ou $\mathfrak{C}(A, B)$.

Exemple 3.1.1. 1) La catégorie (ens) des ensembles. Les objets sont les ensembles ; une flèche est une application d'un ensemble vers un autre ; la composition est celle usuelle des applications ; si A est un ensemble, 1_A sera pris à être l'application identique.
2) La catégorie (top) des espaces topologiques. Les objets sont les espaces topologiques ; les flèches sont les applications continues ; la composition est prise à être la composition usuelle des applications ; le morphisme unité est pris à être l'application identique.
3) La catégorie des espaces de Banach. Les objets sont les espaces de Banach ; les flèches sont les applications linéaires continues ; la composition est celle usuelle des applications ; les flèches unités sont les applications identiques.
4) La catégorie des groupes. Les objets sont les groupes ; les flèches sont les homomorphismes de groupes ; la composition est celle des homomorphismes de groupes ; le morphisme unité est pris à être l'application identique.
5) La catégorie des groupes abéliens. Les objets sont les groupes abéliens ; les flèches sont les homomorphismes de groupes abéliens ; la composition est celle des homomorphismes de groupes abéliens ; le morphisme unité est pris à être l'application identique.
6) La catégorie des espaces vectoriels. Les objets sont les espaces vectoriels ; les flèches sont les homomorphismes d'espaces vectoriels ; La composition est celle des homomorphismes d'espaces vectoriels ; le morphisme unité est pris à être l'application identique.

Définition 3.1.2. Soit $\mathfrak{C}$ une catégorie donnée. L'on dit d'une catégorie $\mathfrak{C}'$ qu'elle est sous catégorie de la catégorie $\mathfrak{C}$ si les conditions suivantes sont réunies :
1) $ob(\mathfrak{C}') \subset ob(\mathfrak{C})$.
2) Si on désigne par $Hom_{\mathfrak{C}}(A, B)$ la classe des flèches de A vers B dans $\mathfrak{C}$, la deuxième condition est : pour tous objets C, D de $\mathfrak{C}'$, $Hom_{\mathfrak{C}'}(C, D) \subset Hom_{\mathfrak{C}}(C, D)$.
3) Pour toutes flèches f et g, la composée de f suivie de g $(g \circ f)$ dans $\mathfrak{C}'$ est égale à la composée de f suivie de g dans $\mathfrak{C}$.
4) Pour tout C objet de $\mathfrak{C}'$, le morphisme unité en C calculé dans $\mathfrak{C}'$ est le même que le morphisme unité en C calculé dans $\mathfrak{C}$.

Remarque 3.1.1. Si dans la deuxième condition de la Définition 3.1.2 l'inclusion est remplacée par l'égalité, alors on dit que $\mathfrak{C}'$ est une sous catégorie pleine de $\mathfrak{C}$.

Exemple 3.1.2. 1) La catégorie des ensembles finis est une sous catégorie de la catégorie des ensembles.
2) La catégorie des espaces topologiques séparés au sens de Hausdoff est une sous catégorie de la

catégorie des espaces topologiques.
3) Soient (Group) la catégorie des groupes et (Ab) la catégorie des groupes abéliens. (Ab) est une sous catégorie pleine de (Group).

Définition 3.1.3. Une catégorie $\mathfrak{C}$ est dite petite si la classe des objets est un ensemble.

Exemple 3.1.3. Soient $(X, \leq)$ un ensemble pré-ordonné et $cat((X, \leq))$ la catégorie associée à cet ensemble pré-ordonné. $ob(cat((X, \leq))) = X$. Donc $cat((X, \leq))$ est une petite catégorie.

Définition 3.1.4. Une catégorie $\mathfrak{C}$ est dite localement petite si la classe des morphismes est un ensemble.

Exemple 3.1.4. Soient $(M, *, e)$ un monoïde et $cat((M, *, e))$ la catégorie associée à ce monoïde. $Mor(cat((M, *, e))) = M$. Donc $cat((M, *, e))$ est une catégorie localement petite.

3.1.2 Foncteurs

Définition 3.1.5. Soient $\mathfrak{C}$ et $\mathfrak{D}$ deux catégories. Un foncteur F de $\mathfrak{C}$ à $\mathfrak{D}$ consiste en la donnée de deux correspondances $F_0 : ob(\mathfrak{C}) \to ob(\mathfrak{D})$ et $F_m : Mor(\mathfrak{C}) \to Mor(\mathfrak{D})$ telles que si $f : A \to B$ est une flèche de $\mathfrak{C}$, alors $F_m(f)$ est une flèche de $\mathfrak{D}$ allant de $F_0(A)$ vers $F_0(B)$ (foncteur covariant) ou $F_m(f)$ est une flèche de $\mathfrak{D}$ allant de $F_0(B)$ vers $F_0(A)$ (foncteur contravariant). Ces données sont assujetties aux axiomes suivants :
axiome 1 : Pour toutes flèches f et g de $\mathfrak{C}$, si $g \circ f$ existe alors $F_m(g \circ f) = F_m(g) \circ F_m(f)$ (foncteur covariant), et $F_m(g \circ f) = F_m(f) \circ F_m(g)$ (foncteur contravariant).
axiome 2 : Pour tout objet A de $\mathfrak{C}$, $F_m(1_A) = 1_{F_0(A)}$.

Notation 3.1.2. La fonction objet F_0 et la fonction morphisme F_m seront toutes notées F du nom du foncteur.

Exemple 3.1.5. 1) Soient $(X, \leq)$ et $(Y, \leq)$ deux ensembles pré-ordonnés vus comme des catégories et $F : (X, \leq) \to (Y, \leq)$ une application croissante. Alors, F est un foncteur covariant.
En effet soit $f : x \to y$ une flèche dans X. Elle n'existe que si $x \leq y$. F étant croissante, $F(x) \leq F(y)$ dans Y. Donc F est une flèche dans Y.
Soient $f : x \to y$ et $g : y \to z$ deux flèches dans X. Elles n'existent que si $x \leq y$ et $y \leq z$. Ainsi $x \leq z$ et donc $g \circ f : x \to z$. De plus $F(x) \leq F(z)$ et donc $F(g \circ f) : F(x) \to F(z)$. $f : x \to y$ n'existe que si $x \leq y$. F étant croissante, $F(x) \leq F(y)$. Donc $F(f) : F(x) \to F(y)$. $g : y \to z$ n'existe que si $y \leq z$. F étant croissante, $F(y) \leq F(z)$. Donc $F(g) : F(y) \to F(z)$.

$(Y, \leq)$ étant un ensemble pré-ordonné, $F(x) \leq F(z)$ et donc $F(g) \circ F(f) : F(x) \to F(z)$. Donc $F(g \circ f) = F(g) \circ F(f)$.
$1_x : x \to x$ existe puisque $x \leq x$. F étant croissante, $F(x) \leq F(x)$. Donc $F(1_x) : F(x) \to F(x)$. D'où $F(1_x) = 1_{F(x)}$.
2) Soient $(A, \perp, e_A)$ et $(B, \top, e_B)$ deux monoïdes vus comme des catégories et $F : (A, \perp, e_A) \to (B, \top, e_B)$ un homomorphisme de monoïde. Alors, F est un foncteur covariant.
En effet si l'on note $\triangle$ l'unique objet du premier monoïde et $\sqcap$ l'unique objet du deuxième monoïde, alors $F(\triangle) = \sqcap$ forcement.
$F(a \perp a') = F(a) \top F(a')$ et $F(e_A) = e_B$ car F est un homomorphisme de monoïde.
3)

$$\begin{array}{cccc} F: & (anneau) & \to & (ens) \\ & A & \mapsto & F(A) & = \{a^2, a \in A\} \end{array}$$

où $(anneau)$ est la catégorie des anneaux est un foncteur covariant. En effet soient $A,\ B$ et C trois anneaux et $f : A \to B$, $g : B \to C$ deux homomorphismes d'anneaux tels que

$$\begin{array}{cccc} F(f): & F(A) & \to & F(B) \\ & a^2 & \mapsto & F(f)(a^2) & = (f(a))^2 \end{array}.$$

On a pour tout $a \in A$, $F(g \circ f)(a^2) = (g(f(a)))^2 = F(g)((f(a))^2) = F(g) \circ F(f)(a^2)$. Ainsi, $F(g \circ f) = F(g) \circ F(f)$.
Soit A un anneau et $1_A : A \to A$ l'homomorphisme identique de A. Montrons que $F(1_A) = 1_{F(A)}$.

$$\begin{array}{cccc} F(1_A): & F(A) & \to & F(A) \\ & a^2 & \mapsto & F(1_A)(a^2) & = (1_A(a))^2 = a^2 \end{array}.$$

Ainsi, $F(1_A)(a^2) = (1_A(a))^2 = a^2 = 1_{F(A)}(a^2)$ pour tout a élément de A. Donc $F(1_A) = 1_{F(A)}$.
4)

$$\begin{array}{cccc} \mathcal{P}: & (ens) & \to & (ens) \\ & A & \mapsto & \mathcal{P}(A) & = \{B \mid B \subseteq A\} \end{array}$$

est un foncteur contravariant. En effet soient $A,\ B$ et D trois ensembles et $f : A \to B$, $g : B \to D$ deux applications telles que

$$\begin{array}{cccc} \mathcal{P}(f): & \mathcal{P}(B) & \to & \mathcal{P}(A) \\ & C & \mapsto & \mathcal{P}(f)(C) & = f^{-1}(C) \end{array}$$

Montrons que $\mathcal{P}(g \circ f) = \mathcal{P}(f) \circ \mathcal{P}(g)$. Soit $E \in \mathcal{P}(D)$. Alors $\mathcal{P}(g \circ f)(E) = (g \circ f)^{-1}(E) = f^{-1} \circ g^{-1}(E) = f^{-1}(g^{-1}(E)) = f^{-1}(\mathcal{P}(g)(E)) = \mathcal{P}(f)(\mathcal{P}(g)(E)) = \mathcal{P}(f) \circ \mathcal{P}(g)(E)$ et ce

$\forall E \in \mathcal{P}(D)$. Donc $\mathcal{P}(g \circ f) = \mathcal{P}(f) \circ \mathcal{P}(g)$.
Soit A un ensemble et $1_A : A \to A$ l'application identique. Montrons que $\mathcal{P}(1_A) = 1_{\mathcal{P}(A)}$.

$$\begin{array}{rccl} \mathcal{P}(1_A): & \mathcal{P}(A) & \to & \mathcal{P}(A) \\ & C & \mapsto & \mathcal{P}(1_A)(C) \quad = 1_A(C) = C \end{array}.$$

Ainsi, $\mathcal{P}(1_A)(C) = 1_A(C) = C = 1_{\mathcal{P}(A)}(C)$. D'où $\mathcal{P}(1_A) = 1_{\mathcal{P}(A)}$.

Définition 3.1.6. Soient $\mathfrak{C}$ une catégorie localement petite, A, B et C trois objets de $\mathfrak{C}$. Un foncteur hom-covariant est un foncteur

$$\begin{array}{rccl} hom_{\mathfrak{C}}(A,-): & \mathfrak{C} & \to & (ens) \\ & B & \mapsto & hom_{\mathfrak{C}}(A,-)(B) \quad = hom_{\mathfrak{C}}(A,B) \end{array}$$

obtenu en fixant A et en laissant varier B et tel que si $f : B \to C$ est une flèche de $\mathfrak{C}$, alors

$$\begin{array}{rccl} hom_{\mathfrak{C}}(A,f): & hom_{\mathfrak{C}}(A,B) & \to & hom_{\mathfrak{C}}(A,C) \\ & \alpha & \mapsto & hom_{\mathfrak{C}}(A,f)(\alpha) \quad = f \circ \alpha \end{array}.$$

Théorème 3.1.3. Le foncteur hom-covariant conserve la composition et l'identité.

Démonstration. Soient A, B, C et D quatre objets de $\mathfrak{C}$, $f : B \to C$ et $g : C \to D$ deux flèches de $\mathfrak{C}$. Montrons que $hom_{\mathfrak{C}}(A, g \circ f) = hom_{\mathfrak{C}}(A, g) \circ hom_{\mathfrak{C}}(A, f)$.
Soit $x : A \to B$. On a : $hom_{\mathfrak{C}}(A, g \circ f)(x) = (g \circ f) \circ x = g \circ (f \circ x) = hom_{\mathfrak{C}}(A, g)(f \circ x) = hom_{\mathfrak{C}}(A, g)(hom_{\mathfrak{C}}(A, f))(x) = hom_{\mathfrak{C}}(A, g) \circ hom_{\mathfrak{C}}(A, f)(x)$ pour toute flèche $x : A \to B$. Donc $hom_{\mathfrak{C}}(A, g \circ f) = hom_{\mathfrak{C}}(A, g) \circ hom_{\mathfrak{C}}(A, f)$ et par suite le foncteur hom-covariant conserve la composition.
Montrons que $hom_{\mathfrak{C}}(A, 1_B) = 1_{hom_{\mathfrak{C}}(A,B)}$. On a :

$$\begin{array}{rccl} hom_{\mathfrak{C}}(A,1_B): & hom_{\mathfrak{C}}(A,B) & \to & hom_{\mathfrak{C}}(A,B) \\ & \alpha & \mapsto & hom_{\mathfrak{C}}(A,1_B)(\alpha) \quad = 1_B \circ \alpha = \alpha \end{array}.$$

Donc $hom_{\mathfrak{C}}(A, 1_B)(\alpha) = 1_B \circ \alpha = \alpha = 1_{hom_{\mathfrak{C}}(A,B)}(\alpha)$ pour toute flèche $\alpha : A \to B$. Donc $hom_{\mathfrak{C}}(A, 1_B) = 1_{hom_{\mathfrak{C}}(A,B)}$ et par suite le foncteur hom-covariant conserve l'identité. □

Définition 3.1.7. Soient $\mathfrak{C}$ une catégorie localement petite, A, B et C trois objets de $\mathfrak{C}$. Un foncteur hom-contravariant est un foncteur

$$\begin{array}{rccl} hom_{\mathfrak{C}}(-,B): & \mathfrak{C} & \to & (ens) \\ & A & \mapsto & hom_{\mathfrak{C}}(-,B)(A) \quad = hom_{\mathfrak{C}}(A,B) \end{array}$$

obtenu en fixant B et en laissant varier A et tel que si $f : A \to C$ est une flèche de $\mathfrak{C}$, alors

$$\begin{array}{rccl} hom_{\mathfrak{C}}(f,B): & hom_{\mathfrak{C}}(C,B) & \to & hom_{\mathfrak{C}}(A,B) \\ & \alpha & \mapsto & hom_{\mathfrak{C}}(f,B)(\alpha) \ = \alpha \circ f \end{array}.$$

Théorème 3.1.4. Le foncteur hom-contravariant conserve la composition et l'identité.

Démonstration. Soient A, B, C et D quatre objets de $\mathfrak{C}$, $f : A \to C$ et $g : C \to D$ deux flèches de $\mathfrak{C}$. Montrons que $hom_{\mathfrak{C}}(g \circ f, B) = hom_{\mathfrak{C}}(f, B) \circ hom_{\mathfrak{C}}(g, B)$.
Soit $x : D \to B$. On a : $hom_{\mathfrak{C}}(g \circ f, B)(x) = x \circ (g \circ f) = (x \circ g) \circ f = hom_{\mathfrak{C}}(f, B)(x \circ g) = hom_{\mathfrak{C}}(f, B)(hom_{\mathfrak{C}}(g, B)(x)) = hom_{\mathfrak{C}}(f, B) \circ hom_{\mathfrak{C}}(g, B)(x)$ pour toute flèche $x : D \to B$. Donc $hom_{\mathfrak{C}}(g \circ f, B) = hom_{\mathfrak{C}}(f, B) \circ hom_{\mathfrak{C}}(g, B)$ et par suite le foncteur hom-contravariant conserve la composition.
Montrons que $hom_{\mathfrak{C}}(1_A, B) = 1_{hom_{\mathfrak{C}}(A,B)}$. On a :

$$\begin{array}{rccl} hom_{\mathfrak{C}}(1_A,B): & hom_{\mathfrak{C}}(A,B) & \to & hom_{\mathfrak{C}}(A,B) \\ & \alpha & \mapsto & hom_{\mathfrak{C}}(1_A,B)(\alpha) \ = \alpha \circ 1_A = \alpha \end{array}.$$

Donc $hom_{\mathfrak{C}}(1_A, B)(\alpha) = \alpha \circ 1_A = \alpha = 1_{hom_{\mathfrak{C}}(A,B)}(\alpha)$ pour toute flèche $\alpha : A \to B$. Donc $hom_{\mathfrak{C}}(1_A, B) = 1_{hom_{\mathfrak{C}}(A,B)}$ et par suite le foncteur hom-contravariant conserve l'identité. □

Dans la suite, nous dirons simplement foncteur pour foncteur covariant.

Définition 3.1.8. Soient $F : \mathfrak{C} \to \mathfrak{D}$ et $G : \mathfrak{D} \to \mathfrak{F}$ deux foncteurs. On définit la composition de F et G dans cet ordre par $(G \circ F)(A) = G(F(A))$ où A est un objet de $\mathfrak{C}$ et $(G \circ F)(f) = G(F(f))$ où f est un morphisme de $\mathfrak{C}$.

Théorème 3.1.5. Soient $F : \mathfrak{C} \to \mathfrak{D}$ et $G : \mathfrak{D} \to \mathfrak{F}$ deux foncteurs tels que $(G \circ F)(A) = G(F(A))$ où A est un objet de $\mathfrak{C}$ et $(G \circ F)(f) = G(F(f))$ où f est un morphisme de $\mathfrak{C}$. Alors $G \circ F$ est un foncteur de $\mathfrak{C}$ vers $\mathfrak{F}$.

Démonstration. Soit $f : A \to B$ une flèche de $\mathfrak{C}$. Alors, $F(f) : F(A) \to F(B)$ est une flèche de $\mathfrak{D}$ car F est un foncteur. Par suite, $G(F(f)) : G(F(A)) \to G(F(B))$ est une flèche de $\mathfrak{F}$ car G est un foncteur.
Soient f et g deux flèches de $\mathfrak{C}$ telles que $g \circ f$ existe. Alors, on a :

$$\begin{aligned} (G \circ F)(g \circ f) &= G(F(g \circ f)) \quad \text{par définition} \\ &= G(F(g) \circ F(f)) \quad \text{car F est un foncteur} \\ &= G(F(g)) \circ G(F(f)) \quad \text{car G est un foncteur} \\ &= (G \circ F)(g) \circ (G \circ F)(f) \quad \text{par définition} \end{aligned}$$

Soit A un objet de $\mathfrak{C}$. Alors, on a :

$$\begin{aligned}(G \circ F)(1_A) &= G(F(1_A)) \quad \text{par définition}\\ &= G(1_{F(A)}) \quad \text{car F est un foncteur}\\ &= 1_{G(F(A))} \quad \text{car G est un foncteur}\\ &= 1_{(G\circ F)(A)} \quad \text{par définition}\end{aligned}$$

D'où le résultat. $\square$

Définition 3.1.9. Soit $\mathfrak{C}$ une catégorie donnée. On définit le foncteur identique de $\mathfrak{C}$ dans $\mathfrak{C}$ par $1_{\mathfrak{C}}(A) = A$ où A est un objet de $\mathfrak{C}$ et $1_{\mathfrak{C}}(f) = f$ où f est un morphisme de $\mathfrak{C}$.

Théorème 3.1.6. Soit $\mathfrak{C}$ une catégorie donnée telle que $1_{\mathfrak{C}}(A) = A$ où A est un objet de $\mathfrak{C}$ et $1_{\mathfrak{C}}(f) = f$ où f est un morphisme de $\mathfrak{C}$. Alors $1_{\mathfrak{C}}$ est un foncteur.

Démonstration. Soit $f : A \to B$ une flèche de $\mathfrak{C}$. Alors, $1_{\mathfrak{C}}(f)$ est une flèche de $\mathfrak{C}$ car $1_{\mathfrak{C}}(f) = f$, $1_{\mathfrak{C}}(A) = A$ et $1_{\mathfrak{C}}(B) = B$.
Soient f et g des morphismes de $\mathfrak{C}$ tels que $g \circ f$ existe. Alors, on a :

$$\begin{aligned}1_{\mathfrak{C}}(g \circ f) &= g \circ f \quad \text{par définition}\\ &= 1_{\mathfrak{C}}(g) \circ 1_{\mathfrak{C}}(f) \quad \text{par définition}\end{aligned}$$

Soit A un objet de $\mathfrak{C}$. Alors, on a :

$$\begin{aligned}1_{\mathfrak{C}}(1_A) &= 1_A \quad \text{par définition}\\ &= 1_{1_{\mathfrak{C}}(A)} \quad \text{par définition}\end{aligned}$$

$\square$

Théorème 3.1.7. Si $F : \mathfrak{C} \to \mathfrak{D}$ est un foncteur, alors $1_{\mathfrak{D}} \circ F = F$ et $F \circ 1_{\mathfrak{C}} = F$.

Démonstration. Pour tout objet A de $\mathfrak{C}$, $1_{\mathfrak{D}} \circ F(A) = 1_{\mathfrak{D}}(F(A)) = F(A)$. Pour tout morphisme f de $\mathfrak{C}$, $1_{\mathfrak{D}} \circ F(f) = 1_{\mathfrak{D}}(F(f)) = F(f)$. Donc $1_{\mathfrak{D}} \circ F = F$.
Pour tout A de $\mathfrak{C}$, $F \circ 1_{\mathfrak{C}}(A) = F(1_{\mathfrak{C}}(A)) = F(A)$. Pour tout morphisme f de $\mathfrak{C}$, $F \circ 1_{\mathfrak{C}}(f) = F(1_{\mathfrak{C}}(f)) = F(f)$. Donc $F \circ 1_{\mathfrak{C}} = F$. $\square$

3.1.3 Transformations naturelles

Définition 3.1.10. Soient F et G deux foncteurs de $\mathfrak{C}$ vers $\mathfrak{D}$. Une transformation naturelle α : $F \Longrightarrow G$ de F à G consiste à se donner pour tout objet A de $\mathfrak{C}$ une $\mathfrak{D}$ - flèche $\alpha_A : F(A) \to G(A)$ appelé composante de α en A ; cette classe de flèches (α_A) est assujettie au seul axiome suivant : Pour toute $\mathfrak{C}$ - flèche $f : A \to B$, l'on a le diagramme commutatif suivant :

$$\begin{tikzcd}
FA \arrow[r, "Ff"] \arrow[d, "\alpha_A"'] & FB \arrow[d, "\alpha_B"] \\
GA \arrow[r, "Gf"'] & GB
\end{tikzcd}$$

FIGURE 3.1 – Diagramme commutatif caractérisant une transformation naturelle

Exemple 3.1.6. 1) Le déterminant est une transformation naturelle.
Soient R un anneau unitaire et $\mathrm{M}_n(R)$ l'ensemble des matrices carrées d'ordre n à coefficient dans R et det_R le déterminant suivant R c'est-à-dire l'application définie par :

$$\begin{array}{rcccl} det_R : & \mathrm{M}_n(R) & \to & R & \\ & (a_{ij}) & \mapsto & det_R(a_{ij}) & = \displaystyle\sum_{\sigma \in S_n} sign(\sigma) a_{1\sigma(1)} ... a_{n\sigma(n)} \end{array}.$$

R et $\mathrm{M}_n(R)$ sont des anneaux unitaires et det_R est un homomorphisme de monoïdes multiplicatifs. On va donc considérer les deux correspondances suivantes : $\mathrm{M}_n(-)$: (anneau) $\to$ (monoïde) et U : (anneau) $\to$ (monoïde) définies sur les objets par $\mathrm{M}_n(R, +, \cdot) = (\mathrm{M}_n(R), \cdot)$ et $U(R, +, \cdot) = (U(R), \cdot)$. M_n et U sont des foncteurs c'est-à-dire qu'ils sont aussi définis sur les flèches et conservent la composition et les identités. Si $f : R \to S$ est un homomorphisme d'anneaux unitaires, alors

$$\begin{array}{rcccl} \mathrm{M}_n(f) : & \mathrm{M}_n(R) & \to & \mathrm{M}_n(S) & \\ & (a_{ij}) & \mapsto & \mathrm{M}_n(f)((a_{ij})) & = (f((a_{ij}))) \end{array}$$

et

$$\begin{array}{rcccl} U(f) : & U(R) & \to & U(S) & \\ & a & \mapsto & U(f)(a) & = f(a) \end{array}.$$

De plus, $U(f) \circ det_R = det_S \circ \mathrm{M}_n(f)$. Donc $det : \mathrm{M}_n \Longrightarrow U$ est une transformation naturelle.
2)

$$\begin{array}{rccl} U_1 : & (top) & \to & (ens) \\ & (X,\tau) & \mapsto & U_1((X,\tau)) \quad = X \end{array}$$

est un foncteur. Considérons $\alpha : U_1 \to hom_{(top)}(1,-)$ définie par : pour tout (X,τ) objet de (top),

$$\begin{array}{rccl} \alpha_{(X,\tau)} : & X & \to & hom_{(top)}(1,X) \\ & x & \mapsto & \alpha_{(X,\tau)}(x) \quad = i_x \end{array}$$

où

$$\begin{array}{rccl} i_x : & 1 & \to & X \\ & 0 & \mapsto & i_x(0) \quad = x \end{array}$$

α est une transformation naturelle. En effet, soit $f : (X,\tau) \to (Y,\sigma)$ un morphisme de (top). Montrons que $\alpha_{(Y,\sigma)} \circ U_1(f) = hom_{(top)}(1,f) \circ \alpha_{(X,\tau)}$. Soit $x \in X$. On a :
$\alpha_{(Y,\sigma)} \circ U_1(f)(x)(0) = \alpha_{(Y,\sigma)}(f(x))(0) = i_{f(x)}(0) = f(x)$ et $hom_{(top)}(1,f) \circ \alpha_{(X,\tau)}(x)(0) = f \circ \alpha_{(X,\tau)}(x)(0) = f \circ i_x(0) = f(i_x(0)) = f(x)$. Donc $\alpha_{(Y,\sigma)} \circ U_1(f) = hom_{(top)}(1,f) \circ \alpha_{(X,\tau)}$.

Définition 3.1.11. Soient F, G et H trois foncteurs de $\mathfrak{C}$ vers $\mathfrak{D}$, $\alpha : F \Longrightarrow G$, $\beta : G \Longrightarrow H$ et C un objet de $\mathfrak{C}$. On définit la composition de α et β dans cet ordre par $(\beta \circ \alpha)_C := \beta_C \circ \alpha_C$.

Théorème 3.1.8. Soient F, G et H trois foncteurs de $\mathfrak{C}$ vers $\mathfrak{D}$, $\alpha : F \Longrightarrow G$, $\beta : G \Longrightarrow H$ et C un objet de $\mathfrak{C}$. La seule règle $(\beta \circ \alpha)_C := \beta_C \circ \alpha_C$ détermine une transformation naturelle $\beta \circ \alpha : F \Longrightarrow H$ de F à H.

Démonstration. Considérons la situation suivante :

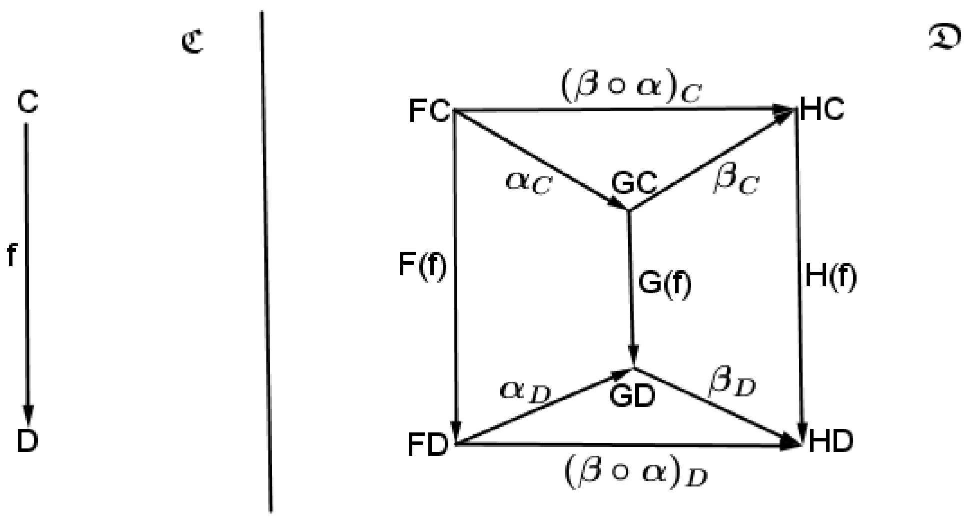


FIGURE 3.2 – Diagramme commutatif issu des transformations naturelles α et β

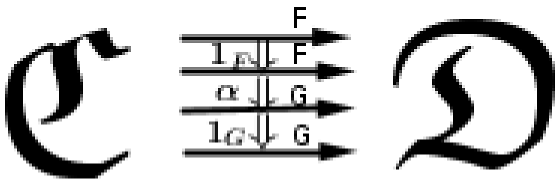
On a :

$$\begin{aligned} H(f) \circ (\beta \circ \alpha)_C &= H(f) \circ \beta_C \circ \alpha_C \\ &= \beta_D \circ G(f) \circ \alpha_C \\ &= \beta_D \circ \alpha_D \circ F(f) \\ &= (\beta \circ \alpha)_D \circ F(f) \end{aligned}$$

D'où le résultat. □

Définition 3.1.12. Soit F un foncteur de $\mathfrak{C}$ dans $\mathfrak{D}$. La seule règle $(1_F)_C = 1_{FC} : FC \to FC$ détermine une transformation naturelle de F vers F. Cette transformation naturelle est appelée la transformation naturelle identique de F vers F.

Théorème 3.1.9. Considérons la situation suivante :



Alors, $1_G \circ \alpha = \alpha$ et $\alpha \circ 1_F = \alpha$.

Démonstration. Soit C un objet de $\mathfrak{C}$. Alors, on a : $(1_G \circ \alpha)_C = (1_G)_C \circ \alpha_C = 1_{GC} \circ \alpha_C = \alpha_C$. Donc $1_G \circ \alpha = \alpha$.
$(\alpha \circ 1_F)_C = \alpha_C \circ (1_F)_C = \alpha_C \circ 1_{FC} = \alpha_C$. Donc $\alpha \circ 1_F = \alpha$. □

3.2 Théories de Lawvere

Définition 3.2.1. Soient A et B deux objets d'une catégorie. Le produit de A et de B est le couple $(p_A : A \times B \to A,\ p_B : A \times B \to B)$ ayant la propriété universelle que pour tout couple $(q_A : X \to A,\ q_B : X \to B)$, il existe un et un seul morphisme $\phi : X \to A \times B$ tel que $q_A = p_A \circ \phi$ et $q_B = p_B \circ \phi$.

Exemple 3.2.1. Dans la catégorie (ens) des ensembles, le produit de deux objets est leur produit muni des projections canoniques.

Définition 3.2.2. Soit $(A_i)_{1 \leq i \leq n}$ une famille de n objets d'une catégorie. Le produit de ces objets est la famille $(p_{A_i} : A_1 \times A_2 \times ... \times A_n \to A_i)_{1 \leq i \leq n}$ ayant la propriété universelle que pour toute famille $(q_{A_i} : X \to A_i)_{1 \leq i \leq n}$, il existe un unique morphisme $\phi : X \to A_1 \times A_2 \times ... \times A_n$ tel que l'on ait $\forall i = 1, ..., n\ \ q_{A_i} = p_{A_i} \circ \phi$.

Exemple 3.2.2. Dans la catégorie des groupes, le produit de n objets est leur produit cartésien et les lois de composition sont définies composante par composante par les lois initiales c'est-à-dire si $(G_1, *_1), ..., (G_n, *_n)$ sont des groupes, la loi $*$ du produit sera définie de la manière suivante : $(a_1, ..., a_n) * (b_1, ..., b_n) = (a_1 *_1 b_1, ..., a_n *_n b_n)\ \forall a_i, b_i \in G_i$.

Définition 3.2.3. Une théorie au sens de Lawvere est une petite catégorie T satisfaisant les propriétés suivantes :
- La classe ob(T) des objets de T est un ensemble dénombrable $\{C_0, ..., C_n, ...\}$.
- Pour tout $n \in \mathbb{N}$, C_n est le produit fini de n copies de C_1 via les projections $(P_i^{(n)} : C_n \to C_1)_{1\leq i\leq n}$ avec pour $n = 1$, $P_1^{(1)} : C_1 \to C_1$ est l'identité sur l'objet C_1.

Définition 3.2.4. Soit X un ensemble, $L(X)$ un groupe abélien et $\eta_X : X \to L(X)$ une application. On appelle groupe abélien libre sur X la donnée d'un couple $(L(X), \eta_X)$ ayant la propriété universelle que pour tout groupe abélien A et toute application $f : X \to A$, il existe un unique morphisme $g : L(X) \to A$ tel que $f = g \circ \eta_X$.

Exemple 3.2.3. Posons pour tout entier naturel n, $C_n = \{0\}^n$. ob$(T) = \{C_0, ..., C_n, ...\}$ et

$$\begin{array}{rccc} p_i^{(n)} : & C_n & \to & C_1 \\ & (0, ..., 0) & \mapsto & p_i^{(n)}(0, ..., 0) = 0 \end{array}.$$

Posons $C_0 = \{0\}^0 = \{*\}$. Une flèche de T est

$$\begin{array}{rccc} f : & C_m & \to & C_n \\ & \underbrace{(0, ..., 0)}_{m \text{ fois}} & \mapsto & f(0, ..., 0) = \underbrace{(0, ..., 0)}_{n \text{ fois}} \end{array}.$$

Si $m = 0$ ou $n = 0$, alors f n'existe pas. Si $m = 0$ et $n = 0$, alors f est l'application vide. Dans la suite, m et n seront différents de 0 et 1_{C_n} sera l'application identique.
Soient $f : C_m \to C_n$ et $g : C_n \to C_p$ deux flèches de T. Alors, la flèche $g \circ f : C_m \to C_p$ existe et est unique.
Montrons que ces quatre données vérifient axiome 1 et axiome 2 de la Définition 3.1.1.
Soient $f : C_m \to C_n,\ g : C_n \to C_p,\ h : C_p \to C_q$ trois flèches avec $m \neq 0,\ n \neq 0,\ p \neq 0,\ q \neq 0$.
Montrons que $(h \circ g) \circ f = h \circ (g \circ f)$.
$(h \circ g) \circ f(\underbrace{0, ..., 0}_{m \text{ fois}}) = (h \circ g)(f(\underbrace{0, ..., 0}_{m \text{ fois}})) = (h \circ g)(\underbrace{0, ..., 0}_{n \text{ fois}}) = h(g(\underbrace{0, ..., 0}_{n \text{ fois}})) = h(\underbrace{0, ..., 0}_{p \text{ fois}}) = (\underbrace{0, ..., 0}_{q \text{ fois}})$.

$h \circ (g \circ f)(\underbrace{0, ..., 0}_{m \text{ fois}}) = h(g \circ f(\underbrace{0, ..., 0}_{m \text{ fois}})) = h(g(f(\underbrace{0, ..., 0}_{m \text{ fois}}))) = h(g(\underbrace{0, ..., 0}_{n \text{ fois}})) = h(\underbrace{0, ..., 0}_{p \text{ fois}}) = (\underbrace{0, ..., 0}_{q \text{ fois}})$.

D'où $(h \circ g) \circ f = h \circ (g \circ f)$.

Supposons que $f : C_m \to C_n$ est une flèche avec $m \neq 0,\ n \neq 0$ et montrons que $1_{C_n} \circ f = f$ et $f \circ 1_{C_m} = f$.

$1_{C_n} \circ f(\underbrace{0, ..., 0}_{m \text{ fois}}) = 1_{C_n}(f(\underbrace{0, ..., 0}_{m \text{ fois}})) = 1_{C_n}(\underbrace{0, ..., 0}_{n \text{ fois}}) = (\underbrace{0, ..., 0}_{n \text{ fois}}) = f(\underbrace{0, ..., 0}_{m \text{ fois}})$. Donc $1_{C_n} \circ f = f$.

$f \circ 1_{C_m}(\underbrace{0, ..., 0}_{m \text{ fois}}) = f(1_{C_m}(\underbrace{0, ..., 0}_{m \text{ fois}})) = f(\underbrace{0, ..., 0}_{m \text{ fois}}) = (\underbrace{0, ..., 0}_{n \text{ fois}}) = f(\underbrace{0, ..., 0}_{m \text{ fois}})$. Donc $f \circ 1_{C_m} = f$.

T ainsi définit est une théorie de Lawvere.

Exemple 3.2.4. La théorie L_G de Lawvere des groupes. Les objets de L_G sont des groupes libres abéliens de n générateurs notés $F_G(n)$. De plus, $F_G(n) = \mathbb{Z}^n$.

Définition 3.2.5. Soient T et T' deux théories de Lawvere telles que $ob(T) = \{C_0, C_1, ..., C_n, ...\}$ et $ob(T') = \{C'_0, C'_1, ..., C'_n, ...\}$. Un morphisme de théories de Lawvere $m : T \to T'$ est un foncteur qui préserve les produits finis et $m(C_1) = C'_1$.

Définition 3.2.6. Un modèle d'une théorie T de Lawvere est un foncteur $G : T \to (ens)$ qui préserve les produits finis.

Exemple 3.2.5. Soit G un groupe et

$$\begin{array}{rccl} hom(-, G) : & L_G & \to & (ens) \\ & \mathbb{Z} & \mapsto & hom(-, G)(\mathbb{Z}) = hom(\mathbb{Z}, G) \end{array}.$$

$hom(-, G)$ est un foncteur contravariant qui préserve les produits finis. Donc $hom(-, G)$ est un modèle de L_G.

Définition 3.2.7. Soient G et H des modèles d'une théorie de Lawvere. Un morphisme $\alpha : G \to H$ de modèle d'une théorie de Lawvere est une transformation naturelle.

Définition 3.2.8. La catégorie des T-modèles notée Mod T est la sous-catégorie pleine de ens^T formée des modèles de T où ens^T est la catégorie des foncteurs de T dans (ens).

Proposition 3.2.1. [2] Un sous-ensemble $\mathcal{C} \subseteq O_{E_k}$ est un clone de E_k si et seulement s'il existe un modèle $m : T \to (ens)$ tel que $\mathcal{C} = \bigcup_{n \in \mathbb{N}^*} \{m(f) \mid f \in T(n, 1)\}$.

Définition 3.2.9. Un clone abstrait consiste :
- pour chaque $n \in \mathbb{N}^*$ un ensemble C_n ; les éléments de C_n étant appelés les symboles d'opérations n-aires,
- pour chaque $n \in \mathbb{N}^*$ et $i \in \{1, ..., n\}$ un symbole d'opération $P_i^{(n)}$,
- pour chaque symbole d'opération n-aire g et les symboles d'opérations m-aires $f_1, ..., f_n$, on a un symbole d'opération m-aire $g(f_1, ..., f_n)$ tel que :
- $(h(g_1, ..., g_n))(f_1, ..., f_m) = h(g_1(f_1, ..., f_m), ..., g_n(f_1, ..., f_m))$,
- $P_i^{(n)}(f_1, ..., f_n) = f_i \quad \forall i \in \{1, ..., n\}$,
- $f(P_1^{(n)}, ..., P_n^{(n)}) = f$.

Conclusion et perspective

Dans ce mémoire, il était question d'exhiber les outils utilisés pour introduire la notion de clone. Pour mener à bien cette étude, nous avons fait recours à des notions telles que la théorie des ensembles, les polymorphismes, les relations invariantes, la connexion de Galois Pol-Inv, les catégories, et la théorie de Lawvere. Et cela nous a permis d'aboutir à des théorèmes caractérisant les clones maximaux et minimaux. Cette étude sur les clones nous permettra d'approfondir nos futures recherches sur "Le treillis des clones sur un ensemble à trois éléments".

Bibliographie

[1] AICHINGER E. (2011) *Basics of clone theory draft.* Course Material for the Come Universal Algebra, JKU Linz, Summer : 2-13.

[2] KERKHOF S., POSCHEL R., SCHNEIDER F.M. (2014) *A short introduction to clones.* Electronic Notes in Theoretical Computer Science 303 : 107-120.

[3] LAU D. (2006) *Function algebras on finite sets.* A Basic Course on Many-Valued Logic and Clone Theory Springer-Verlag, New York, Heidelberg, Berlin,.

[4] MAC LANE S. (1971) *Categories for the working mathematician.* Springer Verlag : 10-55.

[5] POST E.L. (1941) *The two-valued iterative systems of mathematical logic.* Ann. Math. Studies 5, Princeton Univ. Press.

[6] POWER A.J. (1999) *Enriched Lawvere theories.* Theory and Applications of Categories 6 : 83-93.

[7] ROSENBERG I.G. (1983) *Minimal clones I : the five types in : Lectures in universal algebra.* Colloq. Math.Soc. Janos Bolyai 43, North-Holland, Amsterdam : 405-427.