Université de Montréal

Clones sous-maximaux inf-réductibles

par

Andrei-Paul Grecianu

Département de mathématiques et de statistique
Faculté des arts et des sciences

Mémoire présenté à la Faculté des études supérieures
en vue de l'obtention du grade de
Maître ès sciences (M.Sc.)
en Discipline

Orientation mathématiques fondamentales

septembre 2009

Université de Montréal

Faculté des études supérieures

Ce mémoire intitulé

Clones sous-maximaux inf-réductibles

présenté par

Andrei-Paul Grecianu

a été évalué par un jury composé des personnes suivantes :

Abraham Broer

(président-rapporteur)

Ivo G. Rosenberg

(directeur de recherche)

Khallid Benabdallah

(membre du jury)

Mémoire accepté le:

_____

Résumé

Le treillis des clones sur un ensemble fini est assez peu connu sur un ensemble de taille plus grande que 2. En 1970, tous les clones maximaux sur un ensemble fini ont été décrits. Entre temps, pas mal de travail a été fait pour identifier les clones sous-maximaux, soit les clones se trouvant directement en-dessous d'un clone maximal, et ceux-ci ont tous été décrits pour un ensemble de taille 3.

Un clone est dit inf-réductible s'il peut être décrit comme l'intersection de deux clones le contenant de façon propre. Après une courte introduction et un survol de quelques résultats connus importants, je présenterai des résultats non-publiés sur les sous-clones maximaux inf-réductibles de clones préservant une relation d'équivalence, ou de clones de fonctions quasi-linéaires.

Mots-clé

Théorie des clones, Algèbres de fonctions sur un ensemble fini, Théorie des relations, Relations d'équivalence, Algèbre linéaire.

Abstract

The lattice of clones on a finite set is relatively little known for a set whose size is greater than 2. In 1970, all maximal clones on a finite set were described. In the meantime, a lot of work has been done to identify sub-maximal clones, that is clones that lie directly beneath a maximal clone, and they have all been identified for a set of size 3.

A clone is said to be inf-reducible if it can be described as the intersection of two clones in which it is properly contained. After a short introduction and a survey of important known results, I will present unpublished results on the inf-reducible maximal sub-clones of clones preserving equivalence relations, or of clones of quasi-linear functions.

Key-words

Clone theory, Function algebras on finite sets, Relation theory, Equivalence relations, Linear algebra.

Remerciements

J'aimerais remercier mes parents, Mr. Rosenberg pour la supervision (et le soutien) et en général tous ceux qui m'ont aidé durant les six dernières années.

TABLE DES MATIÈRES

Chapitre 1

INTRODUCTION, DÉFINITIONS ET RÉSULTATS CLASSIQUES

1.1. INTRODUCTION

L'étude des clones a commencé avec l'article de Post publié en 1941 [**9**] où Post introduit le terme de classe itérative de fonctions sur l'ensemble $\{0,1\}$, une classe itérative étant un ensemble de fonctions en une ou plusieurs variables fermé sur l'itération finie (substitution d'une variable par l'image d'une autre fonction de la classe).

En décrivant l'ensemble des classes itératives sur $\{0,1\}$, Post pût prouver un nombre de résultats en logique mathématique, plus particulièrement de trouver un ensemble générateurs des tautologies dans le calcul propositionnel, ainsi que l'équivalence de deux ensembles de propositions logiques quant aux propositions qui peuvent en découler. Il arriva à ces résultats en regardant une proposition logique dépendant de n déclarations comme une fonction en n variables sur $\{0,1\}$.

Il était logique d'essayer d'utiliser le même outil pour étudier les logiques ayant k valeurs de vérité possibles. De même le passage des classes itératives aux clones (un clone étant une classe itérative contenant les projections) car la fonction $I(x) = x$ est en général présente dans la plupart des systèmes étudiés...

En particulier, comme on sait que les fonctions $\vee, \wedge$ et $\neg$ engendrent toutes les fonctions possibles sur $\{0,1\}$, on peut se demander quel clone de fonctions engendreraient-elles pour une logique ayant k valeurs de vérité possibles (selon les intérprètations que l'on donne à ces valeurs).

Entre temps, un nombre d'autres applications sont apparues, tout particulièrement en algèbre universelle où, étant donné deux algèbres $(E, \sigma_1, ..., \sigma_i)$ et $(E, \tau_1, ..., \tau_j)$ sur le même ensemble, elles définissent de fait la même algèbre (ayant le même ensemble d'opérations terme) si et seulement si les ensembles $\{\sigma_1, ..., \sigma_i\}$ et $\{\tau_1, ..., \tau_j\}$ engendrent le même clone sur l'ensemble E.

En 1959, Janov et Mučnik ont prouvé [**5**] que, contrairement au treillis de classes itératives sur $\{0,1\}$ qui est dénombrable et facile à énumérer, celui sur $\{0,1,2\}$ a la cardinalité du continuum. Toutefois, des résultats non-triviaux ont

pu être découverts en se concentrant sur des clones placés assez haut ou assez bas dans le treillis, et en particulier, en 1970, Rosenberg a prouvé [**10**] que, sur un ensemble fini, il y aura un nombre fini de clones maximaux faciles à décrire.

Il était logique de se demander si la même chose restait vrai pour les clones sous-maximaux, c'est à dire ceux placés directement en-dessous des clones maximaux. Une réponse générale n'a pas encore été apportée, mais en 1982, Lau a décrit [**6**] l'ensemble de tous les clones sous-maximaux sur l'ensemble $\{0, 1, 2\}$.

De même, certains autres résultats ont été découvert. Rosenberg et Szendrei on décrit en 1985 [**12**] tous les clones sous-maximaux de fonctions qui commutent avec une permutation sans points fixes d'ordre premier. De même, Arto Salomaa décrivit en 1964 [**13**] les clones sous-maximaux de fonctions sur un ensemble de taille p premier qui peuvent s'écrire sous la forme $A(x_1, ..., x_n) = a_0 + \sum a_i x_i$ $(mod\ p)$ pour certaines constantes $a_0, ..., a_n$, résultat qui fut élargi en en 1982 par Bagyinszki et Demetrovics [**2**] qui décrivirent l'ensemble de tous les sous-clones de fonctions qui peuvent s'écrire sous la forme plus haut.

Dans ce travail, après une présentation des notions et résultats de base et un bref survol des résultats décrits plus haut, je présenterai quelques résultats non-publiés. Le premier groupe de résultats (sections 3.1 et 3.2), dues à Lau et Rosenberg et n'ayant été que vérifiés et transcrits au propre par l'auteur, sera centré sur les clones sous-maximaux de fonctions présèrvant une relation d'équivalence. Le deuxième groupe de résultats (sections 3.3 à 3.6) sont dûs à l'auteur et seront centrés sur les clones de fonctions quasi-linéaires, celles-ci étant une généralisation des fonctions étudiées par Salomaa, Bagyinszki et Demetrovics. La section 3.7 ne présente pas un résultat complet, mais a été incluse par l'auteur dans le travail à cause de la présence d'un nombre de propositions non-triviales ainsi que d'une conjecture quant au résultat complet et à une ébauche de preuve de celui-ci.

Selon l'avis de l'auteur, les clones sous-maximaux de fonctions quasi-linéaires pourraient être décrits au complet (dans un travail d'une envergure considérablement plus grande que celui-ci), ceux-ci ayant une structure facile à étudier à l'aide de l'algèbre classique. En particulier l'auteur à pu les partager (proposition 3.4.1) en deux sortes différentes selon qu'ils contiennent toutes les fonctions de la forme $f_a(x) = x + a$ ou non (en quel cas ils auront une structure très particulière), ainsi que donner des exemples de clones sous-maximaux contenant ces fonctions (sections 3.4 et 3.5) et des exemples de clones sous-maximaux ne les contenant pas (section 3.6).

1.2. DÉFINITIONS

Définition 1.2.1 (E_k, Fonction n-aire). *Soit E un ensemble fini quelconque avec $k = |E| > 1$. Puisque E est fini, nous allons sans perdre de généralité supposer que $E = \{0, 1, ..., k-1\} = E_k$. Une fonction n-aire sur E_k est une application quelconque $f : E_k^n \to E_k$ (nous allons supposer $n > 0$).*

Définition 1.2.2 (P_k^n, P_k). *Nous allons définir P_k^n comme étant l'ensemble des fonctions n-aires sur E_k et $P_k = \bigcup_{n\geq 1} P_k^n$, l'ensemble des fonctions d'arité finie sur E_k. Nous n'allons pas faire de différence entre les fonctions selon leurs constructions ou formules, i.e. le terme $f = g$ voudra dire que f et g définissent la même application n-aire sur E_k, même si leurs formules ou constructions sont différentes.*

Définition 1.2.3 (Projections, J_k). *Pour $1 \leq i \leq n$, la i-ème projection sur E_k, e_i^n, est la fonction $e_i^n : E_k^n \to E_k$ définie par $e_i^n(x_1, ..., x_n) = x_i$. Nous allons définir J_k comme étant l'ensemble de toutes les projections sur E_k.*

Définition 1.2.4 (Clone). *Il existe plusieurs façons de définir les clones de P_k. Nous allons donner deux définitions différentes (mais équivalentes) :*

Un sous-ensemble C de P_k est un clone si $J_k \subseteq C$ et que pour toutes fonctions f n-aire et $g_1, ..., g_n$ m-aires, f et g_i dans C, la fonction m-aire h définie par $h(x_1, ..., x_m) = f(g_1(x_1, ..., x_m), ..., g_n(x_1, ..., x_m))$ est dans C.

De façon équivalente, avec f n-aire et g m-aire, soient :
i) $h_1(x_1, ..., x_n) = f(x_2, ..., x_n, x_1)$.
ii) $h_2(x_1, ..., x_n) = f(x_2, x_1, x_3, ..., x_n)$.
iii) $h_3(x_1, ..., x_{n-1}) = f(x_1, x_1, x_2, ..., x_{n-1})$ *avec* $n \geq 2$.
iv) $h_4(x_1, ..., x_{n+1}) = f(x_1, ..., x_n)$
v) $h_5(x_1, ..., x_{m+n-1}) = f(g(x_1, ..., x_m), x_{m+1}, ..., x_{m+n-1})$

Un sous-ensemble C de P_k est un clone si pour tout f n-aire et g m-aire dans C, h_1, h_2, h_3, h_4 et h_5 seront aussi des éléments de C et que $J_k \subseteq C$.

Il est assez facile à voir que les deux définitions ci-haut sont équivalentes. En effet, on peut construire les fonctions h_1, h_2, h_3, h_4 et h_5 à partir de f, g et des projections. De façon similaire, la composition de fonctions qu'on utilise à la première définition peut être construite à partir de f et de g en utilisant la composition de la deuxième fonction, les permutations et les identifications de variables en se rappelant que $(1, 2, ..., n)$ et $(1, 2)$ engendrent S_n, le groupe des permutations d'un ensemble de n éléments.

Nous n'allons en général pas expliquer au long la construction des fonctions à moins que celle-ci ne soit difficile à voir. Par exemple si f est 3-aire et g 2-aire, $h(x_1, ..., x_4) = f(e_3^4(x_1, ..., x_4), g(e_1^4(x_1, ..., x_4), e_2^4(x_1, ..., x_4)), e_4^4(x_1, ..., x_4))$

sera tout simplement écrite sous la forme $h(x_1, ..., x_4) = f(x_3, g(x_1, x_2), x_4)...$

Définition 1.2.5 (Relation n-aire). *Une relation n-aire sur E_k est un sous-ensemble quelconque de E_k^n.*

Définition 1.2.6 (Fonction préservant une relation). *Soit σ une relation n-aire sur E_k et f une fonction m-aire sur E_k. Nous allons dire que f préserve σ si, pour tout $X_1, ..., X_m$ éléments de σ avec $X_i = (x_{i_1}, ..., x_{i_n})$ pour tout $i = 1, ..., m$, $(f(x_{1_1}, ..., x_{m_1}), ..., f(x_{1_n}, ..., x_{m_n}))$ sera dans σ.*

Définition 1.2.7 ($Pol\sigma$). *Nous allons définir $Pol\sigma$ comme étant l'ensemble de toutes les fonctions de P_k préservant la relation σ. Il est assez facile à voir que $Pol\sigma$ est un clone sur E_k pour toute relation σ de E_k.*

Remarque 1.2.1. *Quoique le langage des relations nous offre une façon simple et élégante de définir la plupart des clones qui sont en général étudiés, et en particulier tous les clones dont nous traiterons dans ce mémoire; nous allons préférer, lorsque possible, de décrire les clones en décrivant leurs éléments de façon plus explicite, comme par exemple à la section 1.3 lorsque nous décrirons les fonctions auto-duales et quasi-linéaires.*

Définition 1.2.8 ($\langle A \rangle$, $\langle B \rangle_{\tau_1,...,\tau_i}$). *Soit A un sous-ensemble de P_k. Nous allons définir $\langle A \rangle$ comme étant le clone engendré par l'ensemble de fonctions A, c'est à dire le plus petit clone (par rapport à l'inclusion) contenant A. Pour éviter les confusions, si E est un ensemble quelconque fermé sur les opérations $\tau_1, ..., \tau_i$ et B est un sous-ensemble quelconque de E, $\langle B \rangle_{\tau_1,...,\tau_i}$ sera le plus petit (par rapport à l'inclusion) sous-ensemble de E fermé sur $\tau_1, ..., \tau_i$ et contenant B.*

Remarque 1.2.2. *L'ensemble des clones sur E_k, ordonné par l'inclusion, forme un treillis* [1, p.42]. *Si C_1 et C_2 sont deux clones sur E_k, l'infimum de C_1 et C_2 sera $C_1 \bigcap C_2$ et leur suprémum sera $\langle C_1 \bigcup C_2 \rangle$. Ce treillis possède un unique élément maximal, P_k, et un unique élément minimal, J_k.*

1.3. Treillis de Post

Le treillis des sous-clones de P_2 a été décrit en entier dans [**9**] (en fait, Post a décrit l'ensemble des sous-classes de P_2, une classe ne contenant pas nécessairement les projections). Une version de la preuve peut être trouvée dans le livre de Lau, [1, p.145-158]. La notation utilisée ainsi que l'image ci-contre en sont d'ailleurs tirées. Nous allons prendre $\wedge$, $\vee$ et $\neg$ comme étant les opérations logiques habituelles. Nous définirons :

Définition 1.3.1. $M = Pol\{(0,0),(0,1),(1,1)\}$, *l'ensemble des fonctions monotones par rapport à l'ordre* $0 \leq 1$, *c'est à dire telles que, si* $x_i \leq y_i$ *pour tout* i, $f(x_1,...,x_n) \leq f(y_1,...,y_n)$

$S = Pol\{(0,1),(1,0)\}$, *l'ensemble des fonctions auto-duales, c'est à dire telles que* $f(x_1,...,x_n) = \neg f(\neg x_1,...,\neg x_n)$.

$L = \{f : E_2^n \to E_2$ *telle qu'il existe* $a_0,...,a_n$ *de* E_2 *avec* $f(x_1,...,x_n) = a_0 + a_1x_1 + ... + a_nx_n (mod\ 2)\}$, *l'ensemble des fonctions linéaires.*

$T_{a,n} = Pol(E_2^n \setminus \{(a,...,a)\})$ *pour un* n *naturel et un* a *dans* E_2, $T_{a,\infty} = \bigcap_{n\geq 1} T_{a,n}$ *(à remarquer que* $T_{a,1} \supsetneq T_{a,2} \supsetneq ... \supsetneq T_{a,\infty}$ *pour tout* a *dans* E_2*).*

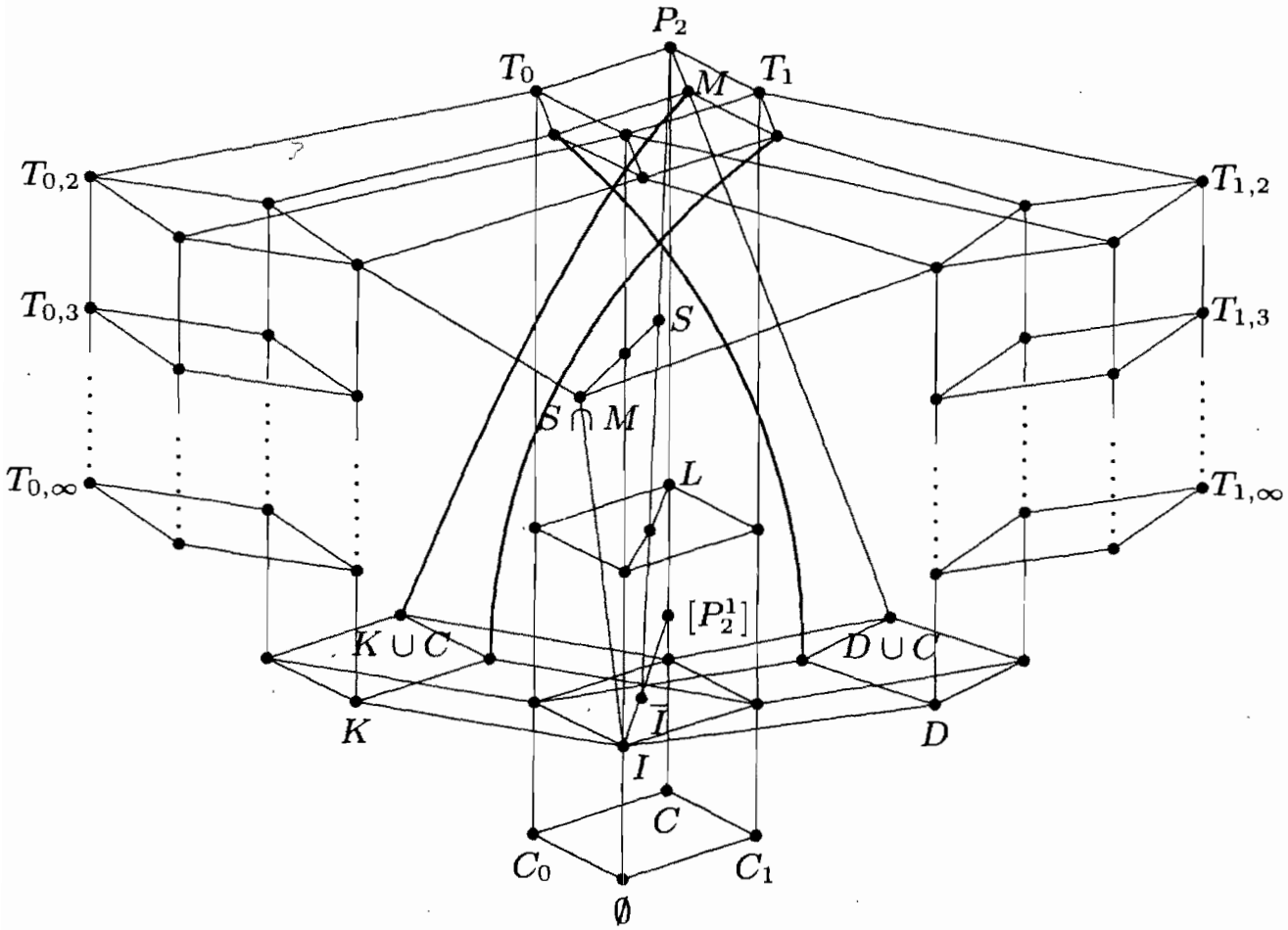
$K = \langle\wedge\rangle, D = \langle\vee\rangle, I = \langle\neg\rangle$.

Nous aurons aussi besoin des classes suivantes (qui ne sont pas des clones) : C_a, l'ensemble des fonctions constantes, d'arité finie, prenant la valeur a (a élément de E_2), C l'ensemble des fonctions constantes ($C_0 \bigcup C_1$)

Théorème 1.3.1 (Post, 1941). [**9**, p.43-101] *Le treillis des sous-clones de* P_2 *est dénombrablement infini. Les sous clones de* P_2 *sont, pour* u *élément de* $\mathbb{N}\bigcup\{\infty\}$ *et* a *élément de* E_2 *:*

$P_2, S, M, L, K, D, I, J_2, T_{a,u}, T_{0,u} \bigcap T_{1,1}, T_{1,u} \bigcap T_{0,1}, T_{a,u} \bigcap M, T_{0,u} \bigcap M \bigcap T_{1,1}$, $T_{1,u} \bigcap M \bigcap T_{0,1}, K \bigcup C, K \bigcup C_a, D \bigcup C, D \bigcup C_a, I \bigcup C, I \bigcup C_a, J_2 \bigcup C, J_2 \bigcup C_a$, $S \bigcap T_{0,1}, S \bigcap M, S \bigcap L, S \bigcap L \bigcap T_{0,1}, L \bigcap T_{a,1}$.

Les inclusions seront claires dans l'image du treillis, image tirée du livre de Lau [1, p.149].


P_2
T_0
M
T_1
$T_{0,2}$
$T_{1,2}$
$T_{0,3}$
$T_{1,3}$
S
$S \cap M$
$T_{0,\infty}$
L
$T_{1,\infty}$
$[P_2^1]$
$K \cup C$
$D \cup C$
K
$\bar{I}$
D
I
C
C_0
C_1
$\emptyset$

1.4. Critère de complétude de Rosenberg

Contrairement au cas de P_2, le treillis des sous-clones de P_k pour k plus grand que 2 est très peu connu. Janov et Mučnik ont montré [**5**] que, alors que le treillis des sous clones de P_2 est dénombrable, celui de P_k est de la cardinalité du continuum pour tout k plus grand que 2.

Le critère de complétude de Rosenberg [**10**], qui est à la base de ce travail, dit que, pour un k fini, l'ensemble des clones maximaux est fini et ces clones peuvent tous être décrits comme les clones de fonctions préservant certaines relations. Nous allons rapidement définir les sous-clones maximaux de P_k pour tout k fini.

Les résultats qui suivent proviennent de [**10**]. Une version des preuves est présentée dans [**1**, p.163-210].

Définition 1.4.1 (Fonctions monotones). *Soit $\leq$ une relation d'ordre sur E_k, c'est à dire une relation binaire réflexive, transitive et anti-symmétrique, possédant un plus grand élément M et un plus petit élément m, c'est à dire telle que $m \leq x \leq M$ pour tout x.*

Comme dans le cas $k = 2$, nous allons dire que f, une fonction n-aire sur E_k est monotone par rapport à $\leq$ si, pour tous n-tuples $(x_1, ..., x_n)$ et $(y_1, ..., y_n)$ pour lesquels $x_i \leq y_i$ pour tout i on a que $f(x_1, ..., x_n) \leq f(y_1, ..., y_n)$.

Pour certaines relations, telles les ordres et les équivalences, on va écrire $a \leq b$ ou $a \sim b$ au lieu de $(a, b) \in \leq$ ou $(a, b) \in \sim$.

Comme dans le cas $k = 2$, on remarque que cette définition est équivalente (de façon évidente) à celle de l'ensemble $Pol \leq$.

Proposition 1.4.1. *Soit $\leq$ et $\preceq$ deux relations d'ordre sur E_k. $Pol \leq = Pol \preceq$ si et seulement si $a \leq b \Leftrightarrow a \preceq b$ ou $a \leq b \Leftrightarrow b \preceq a$.*

Démonstration. Prouvons d'abord le 'si'. Il est évident que, si $x \leq y \Leftrightarrow x \preceq y, Pol \leq = Pol \preceq$. Nous allons donc regarder ce qui se passe si $x \leq y \Leftrightarrow y \preceq x$. Il est évident que, si f est dans $Pol \leq$ et que $(x_1, ..., x_n)$ et $(y_1, ..., y_n)$ sont tels que $x_i \preceq y_i$ pour tout i, alors $y_i \leq x_i$ pour tout i, donc $f(y_1, ..., y_n) \leq f(x_1, ..., x_n)$, et donc $f(x_1, ..., x_n) \preceq f(y_1, ..., y_n)$. $Pol \leq$ est donc contenu dans $Pol \preceq$, et vice-versa par symmétrie, donc $Pol \leq = Pol \preceq$.

Maintenant pour le 'seulement si', soit $\leq$ et $\preceq$ deux relations d'ordre possédant un unique élément maximal et un unique élément minimal telles que $\leq$ et $\preceq$ ne sont ni équivalentes ni inverses. Soit $M_\leq$ et $m_\leq$ les uniques éléments maximaux et minimaux par rapport à $\leq$, et $M_\preceq$ et $m_\preceq$ les éléments correspondants pour $\preceq$. Si $m_\preceq \neq M_\leq \neq M_\preceq$, soit f défini par $f(x) = M_\leq$ si $x = M_\leq$, $M_\preceq$ sinon, f préserve $\leq$ mais pas $\preceq$.

Si $M_{\leq} = M_{\preceq}$ et que $a \leq b$, alors f_{ab} défini par $f_{ab}(x) = b$ si $x = M_{\leq}$, a sinon préserve $\leq$, donc pour que $Pol \leq = Pol \preceq$, il faut que $a \preceq b$. Par symmétrie, on a que $a \leq b \Leftrightarrow a \preceq b$.

Si $M_{\leq} = m_{\preceq}$ et que $a \leq b$, alors f_{ab} défini par $f_{ab}(x) = b$ si $x = M_{\leq}$, a sinon préserve $\leq$, donc pour que $Pol \leq = Pol \preceq$, il faut que $b \preceq a$. Par symmétrie, on a que $a \leq b \Leftrightarrow a \preceq b$.

□

Définition 1.4.2 (Fonctions auto-duales). *Soit t une fonction 1-aire sur E_k et f une fonction n-aire quelconque sur E_k. Nous allons dire que f commute avec t si pour tout n-tuple $(x_1, ..., x_n)$ de E_k, $t(f(x_1, ..., x_n)) = f(t(x_1), ..., t(x_n))$.*

Soit s une permutation de E_k d'ordre premier ne possédant aucun point fixe. Une fonction n-aire f est dite auto-duale par rapport à s si f commute avec s.

Proposition 1.4.2. *Nous allons définir la relation binaire s^o comme étant le graphe de s, $s^o = \{(x, s(x)) | x$ dans E_k quelconque$\}$. $Pols^o$ est l'ensemble des fonctions auto-duales par rapport à s.*

Démonstration. Soit f une fonction n-aire de $Pols^o$ et soit $(x_1, ..., x_n)$ un n-tuple quelconque de E_k. On sait que $(x_i, s(x_i))$ est dans s^o pour tout i, et donc que $(f(x_1, ..., x_n), f(s(x_1), ..., s(x_n)))$ est aussi dans s^o. En d'autres mots que $f(s(x_1), ..., s(x_n)) = s(f(x_1, ..., x_n)$.

De même, si f une fonction n-aire de P_k commute avec s et que l'on a deux n-tuples $(x_1, ..., x_n)$ et $(y_1, ..., y_n)$ avec (x_i, y_i) dans s^o pour tout i, cela veut dire que $y_i = s(x_i)$ pour tout i et que $f(y_1, ..., y_n) = s(f(x_1, ..., x_n))$... en d'autres mots que f préserve s^o.

□

Remarque 1.4.1. *On voit clairement du fait plus haut que cette définition des fonctions auto-duales sur E_k est une généralisation de la définition des fonctions auto-duales dans le cas $k = 2$.*

Proposition 1.4.3. *Soient s et t des permutations d'ordre premier p et q sans points fixes sur E_k. Alors $Pols^o = Polt^o$ si et seulement si il existe $i > 0$ tel que $s^i = t$.*

Démonstration. Supposons tout d'abord que $s^i = t$ et que f est une fonction n-aire de $Pols^o$. $f(s^i(x_1), ..., s^i(x_n)) = s(f(s^{i-1}(x_1), ..., s^{i-1}(x_n))) = ... = s^i(f(x_1, ..., x_n))$, donc par le fait plus haut, $Pols^o \subseteq Polt^o$, et puisque $s^i = t$ si et seulement si $t^j = s$ puisque s et t sont d'ordre premier, on a que $Pols^o = Polt^o$

Supposons maintenant $Pols^o = Polt^o$. s préserve s^o et donc préserve t^o. Soit $T_1, ..., T_m$ les orbites de t et $t_1, ..., t_m$ une ensemble de représentatifs de ces orbites. Puisque s est unaire, s est défini par ses images sur le t_i car tout élément de E_k

peut être écrit comme $t^i(t_j)$ pour un i et j quelconques. Soit a_i la fonction unaire définie par $a_i(t_j) = t_i$ pour tout j et a commute avec t.

$s(t_i)$ doit être encore dans T_i, car sinon $a_i(s(t_i)) \neq s(a_i(t_i))$, ce qui serait une contradiction avec le fait que a_i est élément de $Polt^o$, et donc de $Pols^o$. De plus, si $s(t_i) = t^{i'}(t_i)$ et $s(t_j) = t^{j'}(t_j)$, alors $i' = j'$ puisque $s(a_i(t_j)) = t^{i'}(t_i)$ et $a_i(s(t_j)) = t^{j'}(t_i)$.

□

Remarque 1.4.2. *La preuve de la proposition plus haut explique pourquoi il est important que s soit d'ordre premier. Si elle ne l'était pas, il existerait t non-triviale telle que $s^i = t$ mais $t^j \neq s$ pour tout j, ce qui nous donnerait que $Pols^o \subsetneq Polt^o$.*

On a aussi demandé dans la définition que s soit sans points fixes. La raison est simple. Soit S l'ensemble des points fixes de s, et supposons S non-vide. Soit f une fonction n-aire qui commute avec s et soit $(s_1, ..., s_n)$ un n-tuple d'éléments de S. $f(s_1, ..., s_n) = f(s(s_1), ..., s(s_n)) = s(f(s_1, ..., s_n))$ et il s'ensuit que $f(s_1, ..., s_n)$ est lui-même un élément de S, donc que $Pols^o \subsetneq PolS$, les deux ensembles étant non égaux car, si a est dans S et b n'y est pas, f_{ab} 1-aire définie par $f_{ab}(x) = a$ si x dans S, $f_{ab}(x) = b$ sinon, f_{ab} préserve S mais ne commute pas avec s puisque $s(b) \neq b$.

Définition 1.4.3 (Fonctions quasi-linéaires). *Soit $k = p^m$ (p premier, $m \geq 1$) et + une opération binaire telle que $(E_k, +) \cong \mathbb{Z}_p^m$. Supposons sans perdre de généralité que $0 \in E_k$ est l'élément neutre de l'addition.*

Une fonction n-aire A est quasi-linéaire par rapport à + si pour tous n-tuples $(x_1, ..., x_n)$ et $(y_1, ..., y_n)$, $A(x_1, ..., x_n) + A(y_1, ..., y_n) = A(x_1 + y_1, ..., x_n + y_n) + A(0, ..., 0)$.

Proposition 1.4.4. *Nous allons définir $\lambda_+ = \{(x_1, x_2, x_3, x_4) | x_1 + x_2 = x_3 + x_4\}$. $Pol\lambda_+$ est l'ensemble des fonctions quasi-linéaires par rappor à +.*

Démonstration. La proposition est triviale. Si une fonction n-aire A est quasi-linéaire par rapport à + et que $X_i = (x_{i_1}, ..., x_{i_n})$ pour $X_1, ..., X_4$ et $x_{1_i} + x_{2_i} = x_{3_i} + x_{4_i}$ pour tout i, $A(X_1) + A(X_2) = A(X_1 + X_2) + A(0, ..., 0) = A(X_3 + X_4) + A(0, ..., 0) = A(X_3) + A(X_4)$.

De la même façon, si la fonction n-aire A est dans $Pol\lambda_+$ et que l'on a deux n-tuples $X = (x_1, ..., x_n)$ et $Y = (y_1, ..., y_n)$, $(x_i, y_i, x_i + y_i, 0)$ sera dans λ_+ pour tout i, et il s'ensuit que $(A(X), A(Y), A(X + Y), A(0, ..., 0))$ sera dans λ_+, en d'autres mots que $A(x_1, ..., x_n) + A(y_1, ..., y_n) = A(x_1 + y_1, ..., x_n + y_n) + A(0, ..., 0)$.

□

Proposition 1.4.5. *A une fonction n-aire de P_k est dans $Pol\lambda_+$ si et seulement si il existe un élément a de E_k et $A_1, ..., A_n$ des endomorphismes de $(E_k, +)$ tels*

que pour tout n-tuple $(x_1, ..., x_n)$, $A(x_1, ..., x_n) = a + \sum_{i=1}^{n} A_i x_i$.

Démonstration. Soit C l'ensemble des fonctions possédant une telle formule relativements aux éléments de E_k et aux endomorphismes de $(E_k, +)$. Il est assez évident que si f a une telle formule, f préservera la relation λ_+, donc $C \subseteq Pol\lambda_+$.

Pour prouver l'autre direction, nous allons passer par une autre représentation des fonctions quasi-linéaires. Définissons une opération binaire $\cdot$ telle que $(E_k, +, \cdot) \cong \mathbb{F}_{p^m}$.

Toute fonction sur E_k peut être écrite sous la forme d'un polynôme par rapport aux opérations $+$ et $\cdot$. Pour voir cela, remarquons qu'il y a $k^{(k^n)}$ fonctions n-aires possibles sur E_k et que, puisque l'idéal des polynômes qui sont toujour zéro sur $\mathbb{F}_{p^m}$ est engendré par $x^k - x$, tout polynôme en n variables sur $\mathbb{F}_{p^m}$ prendra les mêmes valeurs (sur $\mathbb{F}_{p^m}$) que l'un des polynômes de la forme $\sum_{(i_1,...,i_n)\in\{0,...,k-1\}^n} a_{i_1,...,i_n} x_1^{i_1} ... x_n^{i_n}$, et le nombre de polynômes de cette forme est exactement $k^{(k^n)}$.

Je prétends que toute fonction quasi-linéaire n-aire posséde une forme polynômiale $a_0 + \sum_{(i,k)\in\{1,...,n\}\times\{0,...,m-1\}} a_{i,k} x_i^{p^k}$. Pour voir cela, il suffit de se rappeler que $(x + y)^{p^k} = x^{p^k} + y^{p^k}$ dans $\mathbb{F}_{p^m}$, et donc que toutes les fonctions ayant une telle forme polynômiale sont quasi-linéaires.

D'un autre côte, quoique $(x, y, x + y, 0)$ est dans λ_+ pour tous x et y (nous supposons ici que 0 est l'élément neutre de $+$), $x^j + y^j \neq (x + y)^j + 0^j$, sauf dans des cas spéciaux, donc toutes les fonctions quasi-linéaires ont une telle forme polynômiale.

Il y a donc k^{mn+1} fonctions quasi-linéaires n-aires possibles. Nous savons que toutes les fonctions ayant des formules utilisant les endomorphismes sont quasi-linéaires, et il y a $k(p^{m^2n}) = k^{mn+1}$ telles fonctions. Il d'ensuit que $C = Pol\lambda_+$. □

Remarque 1.4.3. *On voit clairement du fait plus haut que cette définition des fonctions quasi-linéaires sur E_k est une généralisation de la définition des fonctions linéaires dans le cas $k = 2$.*

Les endomorphismes A_i peuvent bien entendu être représentées comme des matrices $m \times m$ sur $\mathbb{Z}_p$ par rapport à une base de $(E_k, +)$. Nous allons en général préferer parler d'endomorphismes pour ne pas avoir à choisir une représentation, ce qui nous permettra d'en choisir une qui simplifie les preuves lorsqu'on en aura besoin (par exemple à la section 3.5).

Proposition 1.4.6. *Soit $+$ et $\oplus$ deux opérations binaires sur E_k telles que $(E_k, +) \cong (E_k, \oplus) \cong \mathbb{Z}_p^m$. Alors $Pol\lambda_+ = Pol\lambda_\oplus$ si et seulement si il existe*

un élément c de E_k tel que $f : E_k \to E_k$, $f(x) = x + c$ est un isomorphisme entre $(E_k, \oplus)$ et $(E_k, +)$.

Démonstration. Supposons $Pol\lambda_+ = Pol\lambda_\oplus$ et soit d l'élément neutre de $\oplus$. Soit $g(x, y) = x \oplus y$, g est quasi-linéaire par rapport à $\oplus$, et doit donc l'être par rapport à $+$. Or, (x, d, d, x) et (d, y, d, y) sont dans λ_+ pour tous x et y, et donc $g(x, d) + g(y, d) = g(d, d) + g(x, y)$, en d'autres mots que $x + y = d + x \oplus y$, et donc $x \oplus y = x + y - d$. Soit $f : E_k \to E_k$, $f(x) = x - d$.

$f(x \oplus y) = f(x + y - d) = x + y - d - d = (x - d) + (y - d) = f(x) + f(y)$
Il s'ensuit que f est un homomorphisme, et étant injectif sur un ensemble fini, il est un isomorphisme.

Supposons maintenant qu'il existe un c tel que $f(x) = x + c$ est un isomorphisme entre $(E_k, \oplus)$ et $(E_k, +)$. Ceci revient à dire que $x \oplus y = x + y - c$. Si $x + y = x' + y'$, alors $x + y - c = x' + y' - c$, et donc que $x \oplus y = x' \oplus y'$. Donc $\lambda_+ \subseteq \lambda_\oplus$. De la même façon, si $x \oplus y = x' \oplus y'$, alors $x + y - c = x' + y' - c$ et donc $x + y = x' + y'$. Donc, $\lambda_+ = \lambda_\oplus$, et par là-même $Pol\lambda_+ = Pol\lambda_\oplus$.

□

Définition 1.4.4 (Relation d'équivalence). *Une relation binaire, $\sim$ sur E_k est dite une relation d'équivalence si :*
i)$x \sim x$ pour tout x dans E_k (refléxivité)
ii)$x \sim y \Leftrightarrow y \sim x$ (symmétrie)
iii)$x \sim y$ et $y \sim z$ implique que $x \sim z$ (transitivité)

Définition 1.4.5 (Relation centrales). *Une relation n-aire δ sur E_k, avec $n < k$, est dite centrale si elle possède les propriétés suivantes :*
i) Tout n-tuple $(x_1, ..., x_n)$ où $x_i = x_j$ pour quelque $i \neq j$ est élément de δ.
ii) Pour tout s dans S_n, $(x_1, ..., x_n)$ dans δ, $(x_{s(1)}, ..., x_{s(n)})$ dans δ aussi.
iii) Il existe au moins un élément dit central, c, c'est à dire un élément tel que tout n-tuple de la forme $(c, x_1, ..., x_{n-1})$ est dans δ.

Il est facile à voir qu'une relation centrale unaire est un sous-ensemble de E_k, et que les clones de fonctions préservant les relations centrales sont une généralisation des clones $T_{0,1}$ et $T_{1,1}$ du treillis de Post.

Définition 1.4.6 (Relation h-régulière). *Finalement, soit $3 \leq h \leq k$ et m naturel tel que $h^m \leq k$ et soient $\vartheta_1, ..., \vartheta_m$ des relations d'équivalence sur E_k telles que chaque ϑ_i a exactement h classes d'équivalence et que si on choisit $\varepsilon_1, ..., \varepsilon_m$ des classes d'équivalence quelconques ε_i de ϑ_i, leur intersection sera non-vide. On dira que l'ensemble $\{\vartheta_1, ..., \vartheta_m\}$ est un ensemble h-régulier de classes d'équivalence.*

Soit donc ϑ une relation h-aire, avec $3 \leq h \leq k$, on dira que ϑ est une relation h-régulière si il existe un ensemble de relations d'équivalence h-régulières $\{\vartheta_1, ..., \vartheta_m\}$ tel que $(a_1, ...a_h)$ est dans ϑ si et seulement si pour tout i plus petit

ou égal à m, il existe r et s différents tels que (a_r, a_s) *est dans* ϑ_i.

Théorème 1.4.1 (Critère de Complétude de Rosenberg). **[10]** *Soit C un sous-clone de* P_k *avec k fini. C est maximal si et seulement si C est soit un clone de fonctions monotones par rapport à un ordre possédant un maximum et minimum, soit un clone de fonctions auto-duales par rapport à une permutation sans point fixe d'ordre premier, soit un clone de fonctions quasi-linéaires par rapport à une fonction opération* $+$ *avec* $(E_k, +) \cong \mathbb{Z}_p^m$ *soit C est un clone de fonctions préservant une relation centrale, d'équivalence ou h-régulière non-triviale.*

Chapitre 2

RÉSULTATS CONNUS

Un clone est dit sous-maximal s'il s'agit d'un sous-clone maximal d'un clone maximal. Quoiqu'ils ne sont pas aussi connus que les maximaux, quelques résultats existent déjà. Je présenterai un bref survol des clones sous-maximaux de P_2 (corollaire au treillis de Post) et de ceux de P_3 (qui sont tous connus), puis présenterai quelques résultats généraux sur les clones sous-maximaux de fonctions auto-duales ou linéaires.

Je finirai par présenter un résultat théorique sur la forme que prend un clone majorant un clone préservant une relation donnée qui sera un lemme fondamental pour les sections 3.1 et 3.2.

2.1. CLONES SOUS-MAXIMAUX DE P_2

En regardant le treillis de Post, on arrive facilement au résultat suivant :

Théorème 2.1.1 (Clones sous-maximaux de P_2). [9] *P_2 a exactement les 11 clones sous-maximaux suivants (en ré-utilisant la notation du 1.2) :*

$$T_{0,2}, T_{1,2}, T_{0,1} \bigcap M, T_{0,1} \bigcap T_{1,1}, M \bigcap T_{1,1}, T_{0,1} \bigcap L, L \bigcap T_{1,1},$$
$$K \bigcup C, D \bigcup C, S \bigcap L, S \bigcap T_{1,1}.$$

2.2. CLONES SOUS-MAXIMAUX DE P_3

Les clones sous-maximaux ont aussi été décrits en entier, quoique en plusieurs étapes. Nous allons supposer que $E_3 = \{a, b, c\}$, pour pouvoir traiter les cas dans l'abstrait.

Les résultats ont été publiés progressivement dans divers article (réfèrences ci-dessus), mais une version de la preuve complète peut être trouvée dans [1, p.399-432], tirée en grande partie de [6].

Théorème 2.2.1 (Machida, 1979). [7] *Soit $a \leq b \leq c, \wedge$ et $\vee$ le max et min par rapport à l'ordre plus haut et Pol $\leq^1$ les fonctions monotones unaires. Pol $\leq a$ exactement les 13 sous-clones maximaux suivants :*

$Pol \leq \bigcap Pol\{a\}, Pol \leq \bigcap Pol\{c\}, Pol \leq \bigcap Pol\{a,b\}, Pol \leq \bigcap Pol\{a,c\},$
$Pol \leq \bigcap Pol(E_3^3 \setminus \{(x,y,z)|x \neq y \neq z \neq x\}), Pol \leq \bigcap Pol\{b,c\},$
$Pol \leq \bigcap Pol\{\delta\}(\delta$ *centrale),* $\langle Pol \leq^1 \bigcup\{\vee\}\rangle, \langle Pol \leq^1 \bigcup\{\wedge\}\rangle,$
$Pol \leq \bigcap Pol(a \sim b), Pol \leq \bigcap Pol(b \sim c).$

Théorème 2.2.2 (Marchenkov, Demetrovics et Hannak, 1980). **[8]** $Pol\{(0,1),(1,2),(2,0)\}$ *a exactement deux sous-clones maximaux :*

$Pol\{(0,1),(1,2),(2,0)\} \bigcap Pol\{0\}, Pol\{(0,1),(1,2),(2,0)\} \bigcap Pol\lambda_+$ *pour un* $+$ *quelconque (ce sera le même clone).*

Théorème 2.2.3 (Bagyinszki et Demetrovics, 1982). **[2]** $Pol\lambda_+$ *sera le même clone pour toute addition* $+$*, et aura cinq sous-clones maximaux :*

$Pol\lambda_+ \bigcap Pol\{x\}$ *pour un* x *quelconque de* $E_3, Pol\lambda_+ \bigcap Pol\{(0,1),(1,2),(2,0)\},$
$\langle Pol\lambda_+^1\rangle.$

Théorème 2.2.4 (Lau, 1982). **[6]** $Pol\{a\}$ *a exactement les 12 sous-clones maximaux :*

$Pol\{a\} \bigcap Pol\{b\}, Pol\{a\} \bigcap Pol\{c\}, Pol\{a\} \bigcap Pol\{a,b\}, Pol\{a\} \bigcap Pol\{a,c\},$
$Pol\{(a,a),(a,b),(b,a),(a,c),(c,a)\}, Pol\{a\} \bigcap Pol(a \geq b \geq c),$
$Pol\{a\} \bigcap Pol\delta_a$ *où* δ_a *est l'unique relation centrale 3-aire avec a central,*
$Pol\{a\} \bigcap Pol(b \sim c), Pol\{(a,a),(b,c),(c,b)\}, Pol\{a\} \bigcap Pol(a \geq c \geq b),$
$Pol\{a\} \bigcap Pol\{b,c\}, Pol\{(a,a),(a,b),(b,a),(a,c),(c,a),(b,c),(c,b)\}.$

$Pol\{a,b\}$ *a exactement les 15 sous-clones maximaux :*

$Pol\{a,b\} \bigcap Pol\{a\}, Pol\{a,b\} \bigcap Pol\{b\}, Pol\{a,b\} \bigcap Pol\{c\},$
$Pol\{a,b\} \bigcap Pol\{(a,a),(a,b),(b,b)\}, Pol\{a,b\} \bigcap Pol\{(a,b),(b,a)\},$
$Pol\{a,b\} \bigcap Pol(b \sim a), Pol\{(a,a,c),(b,b,c)\} \bigcup \{a,b\}^3$
$Pol\{a,b\} \bigcap Pol\{v \in \{a,b\}^4$ *tel que* a *et* b *apparaissent un nombre pair de fois*$\},$
$Pol\{a,b\} \bigcap Pol\{\delta_c\}$ *où* δ_c *est l'unique relation centrale avec* c *central,*
$Pol\{(a,a),(b,b),(a,c)\}, Pol\{(a,a),(b,b),(b,c)\}, Pol\{(a,a),(a,b),(b,a),(b,b),(a,c)\},$
$Pol\{(a,a),(a,b),(b,a),(b,b),(b,c)\}, Pol(E_k^2 \setminus \{(c,c)\}),$
$Pol\{(a,a,a),(b,b,b),(a,a,b),(b,b,a),(a,b,c),(b,a,c),(a,a,c),(b,b,c)\}.$

Soit δ_a *l'unique relation centrale ternaire avec a central.* $Pol\delta_a$ *a exactement sept clones sous-maximaux :*

$Pol\delta_a \bigcap Pol\{a\}, Pol\delta_a \bigcap Pol\{a,b\}, Pol\delta_a \bigcap Pol\{a,c\}, Pol\delta_a \bigcap Pol\{b,c\},$
$Pol\delta_a \bigcap Pol\sigma_a, \sigma_a$ *l'unique relation centrale binaire avec a central,*
$Pol\delta_a \bigcap Pol(E_3^2 \setminus \{(c,b)\}), Pol\delta_a \bigcup \{a,c\}^3$
$Pol\delta_a \bigcap Pol\{(a,a,a),(b,b,b),(c,c,c),(a,b,c),(b,a,c),(a,c,b),(c,a,b)\} \bigcup \{a,b\}^3\}$

$Pol(a \sim b)$ *a exactement les 13 sous-clones maximaux suivants :*

$Pol(a \sim b) \bigcap Pol\{c\}, Pol(a \sim b) \bigcap Pol\{a,b\}, Pol(a \sim b) \bigcap Pol\{a,c\},$
$Pol(a \sim b) \bigcap Pol\{b,c\}, Pol\{a,b\}^3 \bigcup \{(a,a,c),(b,b,c),(c,c,a),(c,c,b),(c,c,c)\},$
$Pol((a \sim b) \setminus \{(b,a)\}), Pol(a \sim b) \bigcap Pol\sigma_a,$
$Pol(a \sim b) \bigcap Pol\sigma_b$ *où les* σ_x *sont les relations centrales binaires avec* x *central,*
$Pol(E_3^2 \setminus \{(c,a),(c,b)\}), Pol\{(x,y,z)$ *tels que* $x = y\} \bigcup \{(a,b,c),(b,a,c)\},$
$Pol\{(x,y,z,w) | \{x,y,z,w\} = \{a,b\},$ *chaque lettre apparaît deux fois*$\} \bigcup \{(x,x,x,x)\},$
$Pol(\{(x_1,...,x_4) \in E_3^4, c$ *apparaît deux fois dans le 4-uple*$\} \bigcup \{(c,c,c,c)\})$.

Soit $P_3(2)$ *l'ensemble des fonctions de* P_3 *dont l'image n'est pas* E_3 *au complet. Soit* P_3^1 *l'ensemble des fonctions unaires sur* E_3. $P_3(2) \bigcup \langle P_3^1 \rangle$ *est un clone maximal et il a les 5 sous-clones maximaux suivants :*

$P_3(2) \bigcup \langle Id, f(x) = 2x (mod\ 3) \rangle, P_3(2) \bigcup \langle Id, f(x) = 2x + 1 (mod\ 3) \rangle,$
$P_3(2) \bigcup \langle Id, f(x) = 2x + 2 (mod\ 3) \rangle,$
$P_3(2) \bigcup \langle Id, f(x) = x + 1, f(x) = 2x + 2 (mod\ 3) \rangle,$
$\{f \in P_3^n, n$ *quelconque, tel qu'il existe des fonctions unaires* $f_0, ..., f_n$ *telles que* $f(x_1, ..., x_n) = f_0(\sum f_i(x_i) (mod\ 3))\} \bigcup \langle P_3^1 \rangle$.

Théorème 2.2.5 (Lau 1982). **[6]** *Les seuls clones sous-maximaux de* P_3 *sont ceux décrits plus haut.*

2.3. Clones sous-maximaux de fonctions auto-duales

Les sous-clones maximaux de fonctions auto-duales ont été décrits en entier. Soit s une permutation d'ordre p (p premier) sans points fixes.

Définition 2.3.1 (Relation fermée sur s). *Une relation h-aire quelconque* γ *est dite fermée sur s si, pour tout* $(x_1, ..., x_h)$ *élément de* γ *et pour tout* $(i_1, ..., i_h)$ *un h-tuple d'entiers,* $(s^{i_1}(x_1), ..., s^{i_h}(x_h))$ *sera aussi dans* γ.

Définition 2.3.2 (Relation transversale à s). *De plus, une relation d'équivalence* $\sim$ *est dite transversale à s si s envoie chaque classe d'équivalence de* $\sim$ *sur une autre classe de* $\sim$ *(s induit une permutation des classes d'équivalence de* $\sim$*). En d'autre mots, s préserve* $\sim$ *et chaque orbite de s rencontre chaque classe d'équivalence de* $\sim$ *en un et un seul élément.*

Un sous-ensemble de E_k *est dit transversal à s si le sous-ensemble contient au plus un élément de chaque orbite de s.*

Si q et r sont des premiers tels que $q^n \equiv 1 \bmod r$, on va dénoter par $G(q,r)$ le groupe des polynômes de la forme $ax + b$ dans $F_{q^n}[x]$ tels que $a^r = 1$ (avec la composition comme opération interne).

Si G est un groupe dont l'ordre divise k, nous allons définir une représentation semi-régulière de G sur E_k de la façon suivante :

Nous allons diviser E_k en $F_1, ..., F_{k/|G|}$, tous d'ordre $|G|$, et nous allons choisir des bijections arbitraires $\varphi_i : F_i \to G$. Nous définissons la représentation $\varphi : G \to S_k$ de la façon suivante : si $x \in F_i$, $g\varphi_i(x) \in F_j$, $g^\varphi(x) = \varphi_j^{-1}(g\varphi_i(x))$.

Proposition 2.3.1 (Pálfy, 1985). [**12**, proposition 2.2] *Un groupe fini a un sous-groupe maximal d'ordre p si et seulement si il est isomorphe à l'un des groupes suivants :*
i) Un groupe abélien d'ordre pq pour un q premier, pas nécessairement différent de p
ii) $G(p,q)$ pour un premier q tel que $p \equiv 1$ mod q
iii) $G(q,p)$ pour un premier q différent de p

Théorème 2.3.1 (Rosenberg et Szendrei, 1985). [**12**, théorème 2.3] *$Pols^o$ possède exactement les sous-clones maximaux suivants :*
$Pols^o \bigcap Pol\lambda_+$ où $+$ est telle que $s(x) = x + c$ pour un c fixe,
$Pols^o \bigcap Pol \sim$, $\sim$ est une équivalence soit fermée soit transversale sur s,
$Pols^o \bigcap Pol\delta$, δ est centrale fermée sur s, ou unaire transversale à s,
$Pols^o \bigcap Pol\gamma$, γ est une relation h-régulière fermée sur s,
$Pols^o \bigcap Polt^o$, t est une permutation de E_k telle que $\langle s,t\rangle_o$ est une représentation semi-régulière d'un groupe ayant un sous-groupe maximal d'ordre p (décrit plus haut).

2.4. Clones sous-maximaux de fonctions linéaires

Une fonctions n-aire f sur E_k est dite linéaire s'il existe des éléments $a_0, ..., a_n$ tels que $f(x_1, ..., x_n) = a_0 \sum a_i x_i$ mod k. Il est assez facile à voir que l'ensemble des fonctions linéaires est un clone et que, si k est premier, il s'agit d'un clone de fonctions quasi-linéaires sur E_k.

Les sous-clones maximaux de fonctions linéaires ont été entièrement décrits 1998 par Bulatov dans [**4**]. Les sous-clones maximaux de fonctions linéaires lorsque k est premier étaient connus depuis plus longtemps.

Théorème 2.4.1 (Salomaa 1964, Szendrei 1980, Bagyinszki et Demetrovics 1982). [**13**], [**2**, théorèmes 3 et 6], [**14**, théorème 4.1] *Soit L_p le clone de fonctions linéaires sur E_p (p premier), et soit L_p^1 l'ensemble des fonctions linéaires unaires. Il y a exactement $p+3$ clones de fontions linéaires qui ne soit pas contenus dans $\langle L_p^1\rangle$:*
$L_p, L_p \bigcap Pol\{(0,1)\}$,
$L_p \bigcap Pol\{(x, x+1) | x \in E_p\}$,
$L_p \bigcap Pol\{x\}$ avec x élément de E_p quelconque.

Corollaire 2.4.1. *Les sous-clones maximaux de L_p sont les suivants :*
$\langle L_p^1\rangle$,
$L_p \bigcap Pol\{(0,1)\}$,
$L_p \bigcap Pol\{(x, x+1) | x$ dans $E_p\}$,

$L_p \bigcap Pol\{x\}$ *avec* x *élément de* E_p *quelconque.*

2.5. CLONES MAJORANT UN CLONE PRÉSERVANT UNE RELATION DONNÉE

Dans [**3**], Bodnarchuk, Kaluzhnin, Kotov et Romov ont développé une théorie de Galois pour les clones, établissant une connection de Galois entre le treillis des sous-clones de P_k et le treillis des co-clones sur E_k, un co-clone étant un ensemble de relations fermé sur certaines opérations internes.

Comme cette théorie est assez complexe et que nous ne l'utiliserons pas directement, nous ne présenterons pas cette théorie ici. Nous aurons quand même besoin d'un résultat qui en découle, présenté comme le corollaire 2 dans [**11**]. Ce résultat sera utilisé aux sections 3.1 et 3.2 sous le nom de lemme fondamental. Avant de le présenter, nous avons besoin de quelques notions préliminaires.

Soit ϱ_l une relation h-aire sur E_l et ϱ_k une relation h-aire sur E_k. $\varphi : E_l \to E_k$ est dite un homomorphisme de ϱ_l vers ϱ_k si, pour tout $(x_1, ..., x_h) \in \varrho_l$, $(\varphi(x_1), ..., \varphi(x_h)) \in \varrho_k$. On dénotera par $Hom(\varrho_l, \varrho_k)$ l'ensemble des homomorphismes de ϱ_l vers ϱ_k.

Soit $p \leq l$, ϱ_l et ϱ_k comme au paragraphe plus haut.
$\varrho_l \curvearrowright_p \varrho_k = \{(\varphi(0), ..., \varphi(p-1)) | \varphi \in Hom(\varrho_l, \varrho_k)\}$, la relation définie par la projection sur E_p des homomorphismes de ϱ_l vers ϱ_k.

Lemme 2.5.1. *Soit* α *une relation sur* E_k *et* C *un clone de* P_k *tel que* $Pol\alpha \subseteq C$. *Alors il existe* $2 \leq p \leq l \leq k$ *et une certaine relation* A *sur* E_l *telle que* $C = Pol(\alpha \curvearrowright_p A)$.

De plus, on peut supposer que A *"hérite" certaines des propriétés de* α. *En particulier, si* α *est une relation d'équivalence sur* E_k, *on peut supposer que* A *est une relation d'équivalence sur* E_l.

Si $\alpha = s^o$ *ou* s *est une permutation sans points fixes n'ayant que des cycles de longueur* p *(premier), nous pouvons supposer que* $A = t^o$ *où* t *est une fonction partielle sans points fixes sur* E_l *dont tous les cycles sont de longueur* p *et dont tous les chemins sont de longueur strictement plus petite que* p.

Chapitre 3

RÉSULTATS NOUVEAUX

On dit qu'un clone est inf-réductible s'il peut être décrit comme l'intersection de deux autres clones le contenant strictement. Dans cette section, je présenterai quelques résultats que l'auteur pense encore non-publiés sur les clones sous-maximaux inf-réductibles. À noter que, quoique ces résultats sont nouveaux en autant que l'auteur le sache, il n'est pas impossible qu'ils aient déjà été publiés sans que l'auteur s'en soit rendu compte...

La première partie de ces résultats, centrée sur les clones sous-maximaux inf-réductibles des clones préservant une relation d'équivalence, est due aux professeurs Lau et Rosenberg et n'a été que retranscrite et vérifiée par l'auteur. La deuxième partie, centrée sur les clones sous-maximaux inf-réductibles de fonctions quasi-linéaires, est due à l'auteur.

La provenence des preuves est clairement indiquée au début des sections.

3.1. CLONES DE FONCTIONS PRÉSERVANT DEUX RELATIONS D'ÉQUIVALENCE

Soient α et β deux relations d'équivalence sur E_k. On va dire que α et β sont comparables si $\alpha \subseteq \beta$ ou $\beta \subseteq \alpha$. On va dire que α et β sont orthogonales si $k = uv$, α a $A_1, ..., A_u$ comme classes d'équivalence, $|A_i| = v$ pour tout i, et β a $B_1, ..., B_v$ comme classes d'équivalence avec $|B_j| = u$ pour tout j et $|A_i \bigcap B_j| = 1$ pour tout i, j.

Pour alléger la notation, on écrira $x\alpha y$ pour dire que $(x, y) \in \alpha$. Nous noterons par ω_2 la relation $\{(a, a)$, a un élément de $E_k\}$.
Les résultats de cette section sont dues à Lau et Rosenberg (encore non-publiés).

Lemme 3.1.1. *Soit $2 \leq p \leq l \leq k$, A et B deux relations d'équivalence sur E_l et $\sigma = A \times B \curvearrowright_p \alpha \times \beta$. Soit $C = A \bigcap E_p^2 \setminus \omega_2$. Si C est non-vide et $\alpha \subseteq \beta$, alors $Pol\sigma \subseteq Pol\alpha$.*

Démonstration. Soit (i,j) dans C et $\pi = pr_{ij}\sigma$. De toute évidence, $Pol\sigma \subseteq Pol\pi$.

Soit $a\alpha b$ et définissons $\varphi_{ab} : E_l \to E_k$ par $\varphi_{ab}(i) = a$, $\varphi_{ab}(x) = b$ pour tout x différent de i. Par $(a,b) \in \alpha \subseteq \beta$, on voit facilement que φ_{ab} est un homomorphisme de A et α ainsi que de B et β. Donc (a,b) est dans π.

Puisque φ_{xy} est dans $Hom(A \times B, \alpha \times \beta)$ pour tout $x\alpha y$, on voit que $\alpha \subseteq \pi$. De plus, tout (x,y) de π est l'image de (i,j) par un certain φ avec φ un homomorphisme de A et de α et iAj, donc $\pi \subseteq \alpha$
$\Rightarrow \alpha = \pi$.
$\Rightarrow Pol\sigma \subseteq Pol\pi = Pol\alpha$.

□

Lemme 3.1.2. *Soit $D = (B \setminus A) \bigcap E_p^2$. Si D est non-vide et $\alpha \subseteq \beta$, alors $Pol\sigma \subseteq Pol\beta$ (σ tel que défini à la proposition 3.1.1).*

Démonstration. Soit (i,j) dans D et $\pi = pr_{ij}\sigma$. De toute évidence, $Pol\sigma \subseteq Pol\pi$.

Soit $a\beta b$ et définissons $\varphi_{ab} : E_l \to E_k$ par $\varphi_{ab}(x) = a$ si xAi, $\varphi_{ab}(x) = b$ sinon. Par $(a,b) \in \beta$, on voit facilement que φ_{ab} est un homomorphisme de B et β. De plus, (i,j) n'est pas dans A, donc si xAy, soit $\varphi_{ab}(x) = \varphi_{ab}(y) = a$, soit $\varphi_{ab}(x) = \varphi_{ab}(y) = b$ selon que x et y soient dans la même classe d'équivalence que i ou pas, donc φ_{ab} est aussi un homomorphisme de A et α. Donc (a,b) est dans π.

Puisque φ_{xy} est dans $Hom(A \times B, \alpha \times \beta)$ pour tout $x\beta y$, on voit que $\beta \subseteq \pi$. De plus, tout (x,y) de π est l'image de (i,j) par un certain φ avec φ un homomorphisme de B et de β et iBj, donc $\pi \subseteq \beta$
$\Rightarrow \beta = \pi$.
$\Rightarrow Pol\sigma \subseteq Pol\pi = Pol\beta$.

□

Corollaire 3.1.1. *Si C et D sont non-vides, $Pol\sigma \subseteq Pol\alpha \bigcap Pol\beta$, donc $Pol\sigma = Pol\alpha \bigcap Pol\beta$ par le lemme fondamental.*

Lemme 3.1.3. *Si $\alpha \subseteq \beta$, que C est vide mais D ne l'est pas, alors $Pol\sigma = Pol\beta$.*

Démonstration. On sait que $Pol\sigma \subseteq Pol\beta$. Définissons $\tau = B \curvearrowright_p \beta$, $\sigma \subseteq \tau$, et φ un homomorphisme de B et de β.
Définissons φ' comme suit :
$\varphi'(x) = \varphi(a)$ si xAa pour un certain a dans E_p, $\varphi'(x) = \varphi(b)$ si xBb pour un certain b minimal dans E_p mais que la condition plus haut n'est pas respectée,

$\varphi'(x) = 1$ autrement.

φ est bien défini car chaque classe d'équivalence de A a au plus un élément de E_p.

Si xBy, soit $\varphi'(x) = \varphi'(y) = 1$, soit $\varphi'(x) = \varphi(x')$, $\varphi'(y) = \varphi(y')$ avec $x'By'$, et donc $\varphi'(x)\beta\varphi'(y)$ puisque φ est un homomorphisme de B et de β.
$\Rightarrow \varphi' \in Hom(B, \beta)$.

De plus, si xAy, $\varphi'(x) = \varphi'(y)$ par $A \subseteq B$, et donc $\varphi' \in Hom(A \times B, \alpha \times \beta)$. Puisque $\varphi'(x) = \varphi(x)$ pour x dans E_p, $\tau \subseteq \sigma$, et donc $\tau = \sigma$.
$\Rightarrow Pol\beta \subseteq Pol\tau = Pol\sigma \subseteq Pol\beta$.

□

Lemme 3.1.4. *Si $\alpha \subseteq \beta$, que C est non-vide mais que D l'est, alors $Pol\sigma = Pol\alpha$.*

Démonstration. Définissons $\tau = A \curvearrowright_p \alpha$, $\sigma \subseteq \tau$.

Soit φ un homomorphisme de A et de α, et définissons $\varphi' : E_l \to E_k$ comme suit :
$\varphi'(x) = \varphi(x)$ si xAa pour un certain a dans E_p, $\varphi'(x) = \varphi(b)$ si xBb pour un certain b minimal dans E_p mais que la condition du haut n'est pas respectée, $\varphi'(x) = 1$ autrement

Soit xBy. Si xAa et yAa' pour a et a' dans E_p, alors aAa' car sinon D ne serait pas vide. Donc xAy, et $\varphi'(x)A\varphi'(y)$ car $\varphi'(x) = \varphi(x)$ dans ce cas-là.

Si xAa pour un a dans E_p et que yBa' pour un a' dans E_p mais que $(x, a) \notin A$ pour tout a dans E_p, alors aBa', et donc aAa', et donc $\varphi'(y) = \varphi(a')$, et puisque φ est un homomorphisme de A dans α et que $xAaAa'$, alors $\varphi'(x)\alpha\varphi'(y)$, et donc $\varphi'(x)\beta\varphi'(y)$.

Dans tous les autres cas, $\varphi'(x) = \varphi'(y)$, donc $\varphi' \in Hom(A \times B, \alpha \times \beta)$.

Puisque φ' se restreint à φ sur E_p, on voit que $\tau \subseteq \sigma$, et donc $\tau = \sigma$.
$\Rightarrow Pol\alpha \subseteq Pol\tau = Pol\sigma \subseteq Pol\alpha$.

□

Lemme 3.1.5. *Si $\alpha \subseteq \beta$, que C et D sont vides, alors $\sigma = E_k^p$.*

Démonstration. Toute classe d'équivalence de B (et de A) rencontre E_p en au plus un élément, donc pour une fonction arbitraire $\varphi : E_p \to E_k$, on peut étendre φ à un homomorphisme de A dans α et de B dans β en définissant $\varphi'(x) = \varphi(a)$

si a est dans E_p et xBa, 1 sinon.

□

Proposition 3.1.1. *Si α et β sont des relations d'équivalence sur E_k avec $\omega_2 \subsetneq \alpha \subsetneq \beta \subsetneq E_k^2$, alors $Pol\alpha$ et $Pol\beta$ couvrent $Pol\alpha \bigcap Pol\beta$.*

Démonstration. Par le lemme fondamental, si $Pol\alpha \bigcap Pol\beta \subseteq P$, il existe des relations d'équivalence A et B sur E_l avec $P = Pol(A \times B \curvearrowright_p \alpha \times \beta)$.

De toute évidence, pour reprendre la notation plus haut, soit C et D sont vides, soit C et D sont non-vides, soit l'un de C et de D est non-vide. Les lemmes 3.1.(2-5) terminent la preuve.

□

Proposition 3.1.2. *Si α n'est pas contenue dans β, ni vice-versa, et que γ est une relation d'équivalence telle que $\alpha \setminus \beta \subsetneq \gamma$ et $Pol\alpha \bigcap Pol\beta \subseteq Pol\gamma$, alors $Pol\alpha \bigcap Pol\beta \subsetneq Pol\gamma$.*

Démonstration. Soit $(a_1, a_2) \in \alpha \setminus \beta$ et $(b_1, b_2) \in \beta \setminus \alpha$, et définissons f sur E_k comme suit :
$f(x) = a_1$ si $x\alpha b_1$, a_2 sinon

$Im(f) = \{a_1, a_2\}$, avec $(a_1, a_2) \in \alpha \setminus \beta \subseteq \gamma$, donc f préserve γ, mais $f(b_1) = a_1$, $f(b_2) = a_2$ avec $(a_1, a_2) \notin \beta$.

□

Proposition 3.1.3. *Si α n'est pas contenue dans β, ni vice-versa, et que $Pol\alpha \bigcap Pol\beta$ est sous-maximal dans $Pol\alpha$, alors $\alpha \bigcap \beta = \omega_2$.*

Démonstration. Définissons $\gamma = \alpha \bigcap \beta$, et supposons que $\gamma \neq \omega_2$. Par $\alpha \neq \gamma$ et maximalité des deux, $Pol\alpha \bigcap Pol\gamma \subsetneq Pol\alpha$. De plus, $Pol\alpha \bigcap Pol\beta \subseteq Pol\gamma$ de toute évidence.

Mais, avec $(a_1, a_2) \in \alpha \setminus \beta$ et $(b_1, b_2) \in \beta \setminus \alpha$, en réutilisant la fonction de la proposition 3.1.2, on voit que $Pol\alpha \bigcap Pol\beta \subsetneq Pol\gamma \bigcap Pol\alpha \subsetneq Pol\alpha$. Contradiction.

□

Soit γ et δ deux relations binaires sur E_k. Nous allons définir par $\gamma \circ \delta$ la composition de relations comme la relation $\{(x, y) \in E_k^2$ tels que il existe z avec $x\delta z$ et $z\gamma y$.

Lemme 3.1.6. *Soit $\sigma = (\alpha \circ \beta) \bigcap (\beta \circ \alpha)$, R la relation d'équivalence définie sur E_4 par $1R3$ et $2R4$ et S la relation d'équivalence définie par $1S4$ et $2S3$. Alors*

$\sigma = R \times S \curvearrowright_2 \alpha \times \beta$.

Démonstration. Soit (a, b) dans σ, cela veut dire qu'il existe u et v tels que $a\alpha u$, $b\beta u$, $a\beta v$ et $b\alpha v$.
Soit $\varphi : E_4 \to E_k$, $\varphi(1) = a$, $\varphi(2) = b$, $\varphi(3) = u$, $\varphi(4) = v$. Il est facile à voir que φ est un homomorphisme de R et α et de S et β.

Puisque l'on peut définir un tel φ pour tout (a, b) dans σ, alors $\sigma \subseteq R \times S \curvearrowright_2 \alpha \times \beta$.

De plus, si (a, b) est dans $R \times S \curvearrowright_2 \alpha \times \beta$, cela veut dire qu'il existe un certain φ tel que $\varphi(1) = a$, $\varphi(2) = b$. Dans ce cas, $a\alpha\varphi(3)$, $b\beta\varphi(3)$, $a\beta\varphi(4)$ et $b\alpha\varphi(4)$, donc $R \times S \curvearrowright_2 \alpha \times \beta \subseteq \sigma$.

□

Lemme 3.1.7. *Soit $tr\sigma$ la fermeture transitive de σ. Si $Pol\alpha \bigcap Pol\beta$ est sous-maximal dans $Pol\alpha$, alors $tr\sigma = E_k^2$.*

Démonstration. Soit $a\alpha b$, $a \neq b$. Puisque $a\beta a$ et $b\beta b$, (a, b) est dans σ, donc $\sigma \neq \omega_2$.

Puisque σ est réflexive et symétrique (car α et β le sont), alors $tr\sigma$ est une relation d'équivalence. De plus $\beta \subseteq tr\sigma$ car si $a\beta b$, on a juste à utiliser que $a\alpha a$ et $b\alpha b$
$\Rightarrow tr\sigma \neq \alpha$.

$\alpha \prec \beta \subsetneq tr\sigma$ puisque $\alpha \subsetneq \sigma$, et par le lemme 3.1.6 on sait que $Pol\alpha \bigcap Pol\beta \subseteq Poltr\sigma$, donc on sait que $Pol\alpha \bigcap Pol\beta \subsetneq Pol\alpha \bigcap Poltr\sigma$ par la proposition 3.1.2. Si $tr\sigma \neq E_k^2$, $tr\sigma$ ne sera pas une relation triviale et $Pol\alpha \bigcap Poltr\sigma \subsetneq Pol\alpha$.

□

Nous savons **[10]** que, puisque σ est réflexive et symmétrique et que $\sigma \neq \omega_2$, alors soit $\sigma = E_k^2$, soit il existe une relation δ centrale ou régulière telle que $Pol\sigma \subseteq Pol\delta$.

Proposition 3.1.4. *Si α et β ne sont pas comparables et que $Pol\alpha \bigcap Pol\beta$ est sous-maximal dans $Pol\alpha$, alors $\alpha \circ \beta = E_k^2 = \beta \circ \alpha$.*

Démonstration. Si σ n'est pas triviale, alors $Pol\alpha \bigcap Pol\beta \subseteq Pol\sigma \subseteq Pol\delta$, donc $Pol\alpha \bigcap Pol\beta \subseteq Pol\alpha \bigcap Pol\delta \subsetneq Pol\alpha$. Il nous suffit donc de montrer que $Pol\alpha \bigcap Pol\beta \subsetneq Pol\alpha \bigcap Pol\delta$.

1) Supposons δ est centrale d'arité plus grande que 1 et que z est un élément central. Soit Z la classe d'équivalence de z dans α.

Si Z contient plus que seulement z, soit a dans Z avec $a \neq z$, et soit b quelconque, $b \neq z$, avec $b\beta c$ pour un certain $c \neq b$. Définissons une fonction 1-aire f comme suit : $f(b) = a$, $f(x) = z$ si $x \neq b$. $Imf = \{a, z\}$, donc f préserve autant α que δ, mais $f(b) = a$, $f(c) = z$ pour (a, z) pas dans β, donc f ne préserve pas β.

Si z est isolé dans α, soit Z' sa classe d'équivalence dans β, $|Z'| \neq 1$ par le lemme 3.1.7. Soit donc b dans Z', $b \neq z$, et c pas dans Z', et définissons une fonction 1-aire f comme suit : $f(z) = z$, $f(x) = c$ si $x \neq z$. Puisque $f(z) = z$ et que z est isolé dans α, alors f préserve autant α que δ, mais $f(b) = c$, $f(z) = z$ pour $b\beta z$ mais c pas dans Z', donc f ne préserve pas β.

2) Supposons que δ est régulière, $a\beta b$ avec $a \neq b$ et $c\alpha d$ avec (c, d) pas dans β. Définissons une fonction 1-aire f comme suit : $f(a) = c$, $f(x) = d$ si $x \neq a$. f préserve α car $c\alpha d$ et préserve δ car δ est complétement réflèxive et est de arité plus grande que 2 avec $|Im(f)| = 2$. toutefois f ne préserve pas β car $(f(a), f(b)) = (c, d)$ n'est pas dans β.

3) Supposons enfin δ 1-aire, z un élément quelconque de δ et Z la classe d'équivalence de z dans α.

Si $|Z| > 1$, soit a tel que $a\alpha z$ $(a \neq z)$ et $b\beta c$ avec $b \neq c$ quelconques. Si b est dans δ et c ne l'est pas, définissons $f(x) = z$ si $x \in \delta$, $f(x) = a$ sinon. Il est évident que f préserve α car $a\alpha z$, et f préserve δ car $z \in \delta$, mais $b\beta c$ et $(z, a) \notin \beta$ par la proposition 3.1.3. Si ni b ni c ne sont dans δ, définissons $f'(x) = z$ si $x \in \delta$ ou si $x = b$, $f'(x) = a$ sinon. De tout évidence, f' préserve α et δ mais pas β car $(f'(b), f'(c)) \notin \beta$. Enfin, supposons b et c sont dans δ et définissons $g(x, y) = z$ si $(x, y) \in \delta^2$ ou $x = b$, $g(x, y) = a$ sinon ; g préserve α et δ, mais si x n'est pas dans δ (doit exister si δ est non-triviale), $b\beta c$ et $x\beta x$ mais $z = g(b, x)$ et $a = g(c, x)$.

Si $|Z| = 1$, il s'ensuit qu'il doit exister un certain b avec $b\beta z$ et $b \neq z$. Soit c tel que $(c, z) \notin \beta$. Si c est élément de δ, définissons $f(x) = z$ si $x = z$, $f(x) = c$ sinon. De toute évidence, f préserve δ et puisque z est isolé dans α, f préserve aussi α, mais $z\beta b$, $(f(z) = z, f(b) = c) \notin \beta$.

Si $c \notin \delta$, en prenant Z' comme étant la classe d'équivalence de z dans β, nous pouvons supposer que $\delta \subseteq Z'$ (car sinon on aurait pu choisir un c qui soit dans δ sans être dans Z'). Si $\delta = Z'$, nous savons qu'il doit exister un certain $a \in \delta$ et un certain $a' \notin \delta$ tel que $a\alpha a'$ par le lemme 3.1.7. Nous définirons donc $g \in P_k^2$ par $g(z, y) = g(x, z) = z$ pour x et y arbitraires, $g(x, y) = a$ si x et y dans δ, $g(x, y) = a'$ sinon. g préserve α car $a\alpha a'$ et z est isolé dans α, et g préserve δ car a et z sont dans δ, mais $(z, c)\beta(b, c)$, alors que $(z, a') \notin \beta$. Finalement, si $\delta \neq Z'$ et que l'on ne peut trouver de a et a' comme définis plus haut, cela revient à dire que tous les éléments de δ sont isolés dans α (si on peut trouver des a et a' comme plus haut, on ré-utilise la même construction). Soit donc $f(x) = x$ si x est dans

δ, $f(x) = c$ sinon. f préserve δ de façon triviale, et f préserve α car les éléments de δ y sont isolés, mais il existe forcément un $b \in Z' \setminus \delta$, et $(f(z), f(b))$ ne sera pas dans β.

$\Rightarrow$ si $\sigma \neq E_k^2$, $Pol\alpha \bigcap Pol\beta \subsetneq Pol\alpha \bigcap Pol\delta \subsetneq Pol\alpha$.

□

Lemme 3.1.8. *Soit α et β des relations d'équivalence orthogonales et $Pol\alpha \bigcap Pol\beta \subseteq C$.*
Si $C = Pol(R \times S \curvearrowright_p \alpha \times \beta)$ avec R et S des fonctions sur E_l, on peut supposer que $l = p$.

Démonstration. Définissons $R_h = R \bigcap E_{l-h}^2$ et $S_h = S \bigcap E_{l-h}^2$, $\sigma_h = R_h \times S_h \curvearrowright_p \alpha \times \beta$.
Si φ est élément de $Hom(R_{h-1} \times S_{h-1}, \alpha \times \beta)$, la restriction de φ à E_{l-h}^4 est un homomorphisme entre $R_h \times S_h$ et $\alpha \times \beta$, et donc $\sigma_{h-1} \subseteq \sigma_h$.

De plus, si $h \leq l - p$ et φ élément de $Hom(R_h \times S_h, \alpha \times \beta)$, définissons $z = l - h + 1$ et $R^{(z)}$ et $S^{(z)}$ comme étant les classes d'équivalence de R et S contenant z.

1) Si $|R_{h-1}^{(z)}| \neq 1 \neq |S_{h-1}^{(z)}|$, que φ envoie $R_{h-1}^{(z)}$ dans la classe d'équivalence A de α et $S_{h-1}^{(z)}$ dans B de β. Par définition, $A \bigcap B = \{t\}$, alors on peut étendre φ à un homomorphisme de $R_{h-1} \times S_{h-1}$ dans $\alpha \times \beta$ en fixant $\varphi(z) = t$.

2) Si $|R_{h-1}^{(z)}| = 1 \neq |S_{h-1}^{(z)}|$ et que φ envoie $S_{h-1}^{(z)}$ dans la classe d'équivalence B de β. On peut à nouveau étendre φ en fixant $\varphi(z)$ dans B (R ne compte pas ici).

3) $|R_{h-1}^{(z)}| \neq 1 = |S_{h-1}^{(z)}|$ suit de 2) par symmétrie.

4) $|R_{h-1}^{(z)}| = 1 = |S_{h-1}^{(z)}|$ est trivial.

Donc, dans tous les cas, on peut étendre un homomorphisme si $h \leq l - p$, et donc $\sigma_h \subseteq \sigma_{h-1}$
$\Rightarrow \sigma_h = \sigma_{h-1}$ si $h \leq l - p$, donc $\sigma = \sigma_{l-p}$ et nous pouvons supposer que R et S sont sur E_p.

□

Lemme 3.1.9. *Supposons R et S sont sur E_p et $\sigma = R \times S \curvearrowright_p \alpha \times \beta$.*
Si $R \neq \omega_2$, alors $Pol\sigma \subseteq Pol\alpha$.
Si $S \neq \omega_2$, alors $Pol\sigma \subseteq Pol\beta$.

Démonstration. Soit iRj avec $i \neq j$, et $\pi = pr_{ij}\sigma$. On va prouver que $\pi = \alpha$ ($\pi \subseteq \alpha$ par le fait que iRj). Soit $a\alpha b$, $a \neq b$, et $f_{ab}(x) = a$ si xSa, b sinon.

On a que f est un homomorphisme de R et α puisque $a\alpha b$, et on a aussi que f est un homomorphisme de S et β car f est constant sur les classes d'équivalence de S, f est donc dans $Hom(R \times S, \alpha \times \beta)$, et $a\pi b$. Puisque f_{ab} peut être construit pour tous $a\alpha b$, $\alpha \subseteq \pi \Rightarrow \alpha = \pi$.
$\Rightarrow Pol\sigma \subseteq Pol\pi = Pol\alpha$.

□

Théorème 3.1.1. *Soit α et β deux relations d'équivalence sur E_k. Les affirmations suivantes sont équivalentes :*
i) $Pol\alpha \bigcap Pol\beta$ est maximal dans $Pol\alpha$.
ii) α et β sont soit comparables soit orthogonales.
iii) $Pol\alpha \bigcap Pol\beta$ est maximal dans $Pol\alpha$ et dans $Pol\beta$.

Démonstration. *i)* $\Rightarrow$ *ii)*

Par les propositions 3.1.3 et 3.1.4, si $Pol\alpha \bigcap Pol\beta$ est maximal dans $Pol\alpha$ et que α et β ne sont pas comparables, alors $\alpha \bigcap \beta = \omega_2$ et $\alpha \circ \beta = E_k^2 = \beta \circ \alpha$.

Puisque $\alpha \circ \beta = E_k^2 = \beta \circ \alpha$, chaque classe d'équivalence de α doit intersecter chaque classe d'équivalence de β en au moins un point, mais puisque $\alpha \bigcap \beta = \omega_2$, chaque classe d'équivalence de α doit intersecter chaque classe d'équivalence de β en au plus un point
$\Rightarrow \alpha$ et β sont orthogonales.

ii) $\Rightarrow$ *iii)*

Par la proposition 3.1.1, si α et β sont comparables, $Pol\alpha \bigcap Pol\beta$ est maximal autant dans $Pol\alpha$ que dans $Pol\beta$. Par le lemme 3.1.8, avec $C = Pol(R \times S \curvearrowright_p \alpha \times \beta)$, on peut supposer que R et S sont dans E_p.

Si $R \neq \omega_2 \neq S$, $Pol\alpha \bigcap Pol\beta \subseteq Pol\sigma \subseteq Pol\alpha \bigcap Pol\beta$.
Si $R = \omega_2 = S$, σ est de toute évidence E_k^p et $Pol\sigma = P_k$.

Si $R \neq \omega_2 = S$, alors $Pol\sigma \subseteq Pol\alpha$ par le lemme 3.1.9. Puisque $S = \omega_2$, tout homomorphisme de R et α est aussi un homomorphisme de S et β, donc $\sigma = R \curvearrowright_p \alpha$ et $Pol\alpha \subseteq Pol\sigma \Rightarrow Pol\alpha = Pol\sigma$.

Par symmétrie, si $R = \omega_2 \neq S$, $Pol\beta = Pol\sigma$, et donc si α et β sont orthogonales, les seuls clones majorant $Pol\alpha \bigcap Pol\beta$ sont $Pol\alpha$, $Pol\beta$ et P_k.
iii) $\Rightarrow$ *i)* est trivial...

□

3.2. CLONES DE FONCTIONS AUTO-DUALES PRÉSERVANT UNE ÉQUIVALENCE

Soit s une permutation d'ordre p, p premier, sans points fixes et θ une relation d'équivalence sur E_k, et définissons $s^o = \{(x, s(x))|x \in E_k\}$.

Il est connu ([**12**]) que $Pols^o \bigcap Pol\theta$ est sous-maximal dans $Pols^o$ si et seulement si les orbites de s sont soit perpendiculaires soit comparables aux classes d'équivalence de θ. Nous allons chercher une condition nécessaire et suffisante pour que $Pols^o \bigcap Pol\theta$ soit sous-maximal dans $Pol\theta$.

Pour le reste de la section, si X est défini comme un n-tuple, on supposera $X = (x_1, ..., x_n)$.

Les résultats de cette section sont dues à Lau et Rosenberg (encore non-publiés)..

Lemme 3.2.1. *Si $Pols^o \bigcap Pol\theta$ est sous-maximal dans $Pol\theta$, alors soit $s^o \subseteq \theta$, soit $s^o \bigcap \theta$ est vide.*

Démonstration. Soit $\tau = \{x \in E_k|(x, s(x)) \in \theta\}$, et soit f dans $(Pols^o \bigcap Pol\theta)^n$. Soit X dans τ^n, $s(f(X)) = f(s(X))\theta f(X)$ puisque $s(f(X)) = f(s(X))$, $X\theta Y \Rightarrow f(X)\theta f(Y)$ et $s(X)\theta X$.

Donc $Pols^o \bigcap Pol\theta \subsetneq Pol\tau$, l'inclusion étant propre car $Pol\tau$ contient au moins une fonction constante si τ est non-vide.

Donc $Pols^o \bigcap Pol\theta \subsetneq Pol\tau \bigcap Pol\theta \subseteq Pol\theta$, et pour que on ait la sous-maximalité désirée il faur que $Pol\tau \bigcap Pol\theta = Pol\theta$.

Par la maximalité de $Pol\theta$ et $Pol\tau$, cela n'est possible que si $Pol\tau = P_k$, donc si $\tau \in \{\phi, E_k\}$

□

Proposition 3.2.1. *Si $Pols^o \bigcap Pol\theta$ est sous-maximal dans $Pol\theta$, alors soit $s^o \subseteq \theta$, soit s applique chaque classe d'équivalence de θ sur une seule autre de façon surjective.*

Démonstration. Définissons $x \sim y$ si et seulement si $s(x)\theta s(y)$. De toute évidence, $\sim$ est une relation d'équivalence non-triviale car c'est la pré-image de θ (une relation d'équivalence non-triviale) par s (une symmétrie).

Soit f dans $(Pols^o \bigcap Pol\theta)^n$ et X et Y des n-tuples avec $X \sim Y$ terme à terme. Alors $s(X)\theta s(Y)$, donc $f(s(X))\theta f(s(Y))$, donc $s(f(X))\theta s(f(Y))$, donc $f(X) \sim f(Y)$

$\Rightarrow Pol\theta \bigcap Pols^o \subsetneq Pol\theta \bigcap Pol \sim\subseteq Pol\theta$, la première inclusion étant stricte car $Pol\theta \bigcap Pol \sim$ contient toutes les fonctions constantes et $Pols^o$ n'en contient aucune.

Donc si $Pols^o \bigcap Pol\theta$ est sous-maximal dans $Pol\theta$, il faut que $\sim = \theta$ car ce sont toutes deux des relations d'équivalence non-triviales.

Si $\tau = E_k$, $x\theta y \Rightarrow s(x)\theta s(y)$, donc $x \sim y$, car $x\theta s(x)$ et $y\theta s(y)$, $x \sim y \Rightarrow x\theta y$ par le même argument.

Si $\tau = \phi$, on sait $s(x)$ est toujours dans une autre classe d'équivalence que x. $x\theta y \Rightarrow s(x)\theta s(y)$, donc s envoie chaque classe d'équivalence de θ sur une autre. $s(x)\theta s(y) \Rightarrow s^2(x)\theta s^2(y) \Rightarrow ... \Rightarrow x = s^p(x)\theta s^p(y) = y$, donc s applique chaque classe d'équivalence de θ sur une autre classe d'équivalence de façon surjective. □

Lemme 3.2.2. *Soit χ une relation d'équivalence sur E_l, $q \leq l \leq k$, et t^o le graphe d'une fonction injective partielle sur E_l avec $t^o \subsetneq \chi$ et t^o étant composé de cycles de longueur p et de chemins orientés de longueur plus petite que p.*

Soit T l'ensemble des cycles et chemins orientés de t et $\sigma = (t^o \times \chi) \curvearrowright_q (s^o \times \theta)$.
a) Si $|E_q \bigcap C| \geq 2$ pour un certain C dans T, alors $Pol\sigma \subseteq Pols^o$.
b) Si $|E_q \bigcap B| \leq 1$ pour toute classe d'équivalence B de χ, alors $\sigma = E_k^q$.
c) Soit B une classe d'équivalence de χ avec $i, j \in E_q \bigcap C$, $i \neq j$. Si i et j sont dans C_i et C_j dans T avec $C_i \neq C_j$, alors $Pol\sigma \subseteq Pol\theta$.

Démonstration. a) Soit $i, j \in E_q \bigcap C$ avec $j = t^n(i)$. Pour un a quelconque dans E_k, définissons $\varphi_a : E_l \rightarrow E_k$ comme suit :
Pour tout C' de T, choisissons un certain $x_{C'} \in C'$ avec $x_C = i$
Pour tout $y = t^n(x_{C'})$, $\varphi_a(y) = s^n(a)$. Finalement, si $y \notin C$ pour tout C de T, fixons $\varphi_a(y) = a$.

De toute évidence, $\varphi_a \in Hom(t^o, s^o)$, et puisque $Im(\varphi_a) = \langle s \rangle(a)$ et que $\tau = E_k$, $\varphi_a(x)\theta\varphi_a(y)$ pour tout x, y dans E_l.

Soit $\xi = pr_{ij}\sigma$, $(a, s^n(a))$ est dans ξ pour tout a car φ_a est dans $Hom(t^o \times \chi, s^o \times \theta)$. De plus, pour tout (x, y) dans ξ, $(x, y) = (\varphi(i), \varphi(s^n(i))$ avec φ un homomorphisme de t^o et s^o
$\Rightarrow \xi = (s^n)^o$, et $Pol\xi = Pol(s^n)^o = Pols^o$.

b) Si $|E_q \bigcap B| \leq 1$ pour toute classe d'équivalence de χ, et avec $t^o \subsetneq \chi$, on peut de toute évidence étendre toute fonction arbitraire $\varphi : E_q \rightarrow E_k$ à un homomorphisme entre $\chi \times t^o$ et $\theta \times s^o$ puisque les projections de χ et de t^o sur E_q sont triviales, donc $\sigma = E_k^q$.

c) Pour tout (a,b) dans θ, définissons $\varphi_{ab} : E_l \to E_k$ comme suit : $\varphi_{ab}(i) = a$, $\varphi_{ab}(j) = b$, $\varphi_{ab} \in Hom(t^o, s^o)$. Par (a,b) dans θ et $s^o \subsetneq \theta$, on sait que $\varphi_{ab} \in Hom(\chi, \theta)$

En définissant à nouveau $\xi = pr_{ij}\sigma$, on aura que $\theta \subseteq \xi$ car $\varphi_{ab} \in Hom(\chi \times t^o, \theta \times s^o)$, et que $\xi \subseteq \theta$ car $i\chi j$, et donc pour tout (x,y) dans ξ, $(x,y) = (\varphi(x), \varphi(y))$ avec $\varphi \in Hom(\chi, \theta)$.

□

Proposition 3.2.2. *Si $s^o \subsetneq \theta$, alors $Pols^o \bigcap Pol\theta$ est sous-maximal dans $Pol\theta$.*

Démonstration. Par le lemme fondamental, nous savons que pour tout sous-clone D de P_k avec $Pols^o \bigcap Pol\theta \subseteq D$, D est de la forme $Pol\sigma$ pour un certain σ défini comme au lemme 3.2.2. Nous ré-utiliserons donc la notation définie au lemme 3.2.2.

Si $|E_q \bigcap B| \leq 1$ pour toute classe d'équivalence B de χ, nous savons par le lemme 3.2.2 que $D = P_k$

Si $|E_q \bigcap C| \geq 2$ pour un certain C dans T et qu'il y a deux éléments i et j avec $C_i \neq C_j$, $(i,j) \in \chi$ et i,j dans E_q, alors par la proposition 3.2.1, $D \subseteq Pols^o \bigcap Pol\theta$, donc $D = Pols^o \bigcap Pol\theta$.

Supposons que $|E_q \bigcap C| \geq 2$ pour un certain C dans T mais que si $(i,j) \in \chi$ avec i,j dans E_q, alors $C_i = C_j$. Soit $\varphi : E_q \to E_k$ arbitraire telle que $\varphi(t(x)) = s(\varphi(x))$ pour tout x, on peut la prolonger à E_l pour obtenir φ' qui soit dans $Hom(t^o \times \chi, s^o \times \theta) \Rightarrow (t^o \times \chi) \curvearrowright_q (s^o \times \theta) = t^o \curvearrowright_q s^o \Rightarrow D = Pols^o$.

Par le même argument, si $|E_q \bigcap C| \leq 1$ pour tout C de T, mais $|E_q \bigcap B| \geq 2$ pour une classe d'équivalence B de χ, alors $(t^o \times \chi) \curvearrowright_q (s^o \times \theta) = \chi \curvearrowright_q \theta \Rightarrow D = Pol\theta$.

□

Proposition 3.2.3. *Si s applique chaque classe d'équivalence de θ sur une autre de façon surjective, alors $Pols^o \bigcap Pol\theta \subsetneq Pol\varepsilon \subsetneq Pol\theta$ avec $\varepsilon = s^o \circ \theta$.*

Démonstration. 1) $Pols^o \bigcap Pol\theta \subsetneq Pol\varepsilon$

Soit X et Y deux n-tuples tels que (x_i, y_i) est dans ε pour tout i, et soit f dans $(Pols^o \bigcap Pol\theta)^n$

Il doit exister un Z tel que (x_i, z_i) est dans θ pour tout i et $s(Z) = Y$. $(f(X), f(Z)) \in \theta$, $f(Y) = f(s(Z)) = s(f(Z)) \Rightarrow (f(X), f(Y))$ est dans ε.

De plus, définissons $\{a_i\}$ un ensemble de représentatifs pour les classes d'équivalences de θ tels qu'il existe j tel que $(s(a_j), a_i) \in \theta$, $s(a_j) \neq a_i$. Définissons $f(x) = a_i$ tel que $(a_i, x) \in \theta$. f est dans $Pol\varepsilon$, mais ne commute pas avec s, donc $Pols^o \bigcap Pol\theta \neq Pol\varepsilon$.

2) $Pol\varepsilon \subsetneq Pol\theta$

Soit X et Y deux n-tuples tels que $(x_i, y_i) \in \theta$ pour tout i, et soit f dans $(Pol\varepsilon)^n$.

$(x_i, s(y_i))$ est dans ε pour tout i, donc $(f(X), f(s(Y)))$ est dans ε, donc $(f(X), s^{-1}(f(s(Y)))) \in \theta$. De plus, $(y_i, s(y_i))$ est dans ε pour tout i,
donc $(f(Y), s^{-1}(f(s(Y)))) \in \theta \Rightarrow (f(X), f(Y)) \in \theta$.

Mais $Pol\theta$ contient toutes les fonctions constantes, alors que $Pol\varepsilon$ ne les contient de toute évidence pas car x et $s(x)$ ne sont jamais dans la même classe d'équivalence de $\theta \Rightarrow Pol\varepsilon \subsetneq Pol\theta$.

□

Théorème 3.2.1. *$Pols^o \bigcap Pol\theta$ est sous-maximal dans $Pol\theta$ si et seulement si $x\theta s(x)$ pour tout x.*

Démonstration. La preuve est triviale. Par la proposition 3.2.1, soit $s^o \subsetneq \theta$ soit s envoie chaque classe d'équivalence de θ sur une autre de façon surjective, faisant de fait une permutation des classes d'équivalence de θ.

Par les propositions 3.2.2 et 3.2.3, $Pols^o \bigcap Pol\theta$ sera sous-maximal dans $Pol\theta$ si et seulement si $s^o \subsetneq \theta$, c'est à dire que $(x, s(x)) \in \theta$ pour tout x.

□

Remarque 3.2.1. *Comme vu à la section 2.3, $Pol\theta \bigcap Pols^o$ est maximal dans $Pols^o$ si et seulement si θ est soit fermée sur s, soit transversale à la relation d'équivalence définie par les orbites de s. On vient de voir que $Pol\theta \bigcap Pols^o$ est maximal dans $Pol\theta$ si et seulement si θ est fermée sur s. Il s'ensuit que tout clone de la forme $Pol\theta \bigcap Pols^o$ qui est maximal dans $Pol\theta$ l'est aussi dans $Pols^o$, mais pas vice-versa.*

3.3. CLONES DE FONCTIONS QUASI-LINÉAIRES AUTO-DUALES

Soit s une permutation d'ordre premier p sans points fixes sur E_k, et $k = p^m$. Soit $+$ une opération binaire sur E_k telle que $(E_k, +) \cong \mathbb{Z}_p^m$ et supposons sans perdre de généralité que 0 en est le neutre.

Définissons $Pol\lambda_+$ comme le clone des fonctions quasi-linéaires par rapport à $+$ et $Pols^o$ comme étant le clone des fonctions auto-duales par rapport à s.

Il est connu (voir section 2.3) que $Pols^o \bigcap Pol\lambda_+$ est maximal dans $Pols^o$ si et seulement si il existe un c fixe tel que $s(x) = x + c$ pour tout x dans E_k. Nous allons chercher une condition nécessaire et suffisante pour que $Pols^o \bigcap Pol\lambda_+$ soit maximal dans $Pol\lambda_+$.

Les résultats de cette section sont dues à l'auteur.

Proposition 3.3.1. *Si $Pols^o \bigcap Pol\lambda_+$ est maximal dans $Pol\lambda_+$, alors il existe un c fixe tel que $s(x) = x + c$ pour tout x dans E_k*

Démonstration. Définissons $c(x) = s(x) - x$ pour tout x dans E_k.
Définissons $x \sim y$ si et seulement si $c(x) = c(y)$. Il est évident que $\sim$ est une relation d'équivalence sur E_k.

Soit A une fonction n-aire de $Pols^o \bigcap Pol\lambda_+$, $X = (x_1, ..., x_n)$ et $Y = (y_1, ..., y_n)$ deux n-tuples tels que $x_i \sim y_i$ pour tout i.

$c(A(X)) = s(A(X)) - A(X) = A(s(X)) - A(X)$
$= A(x_1 + c(x_1), ...) - A(X) = A(X) + A(c(x_1), ..., c(x_n)) - A(0, ..., 0) - A(X)$
$= A(c(x_1), ..., c(x_n)) - A(0, ..., 0) = A(c(y_1), ..., c(y_n)) - A(0, ..., 0)$
$= s(A(Y)) - A(Y) = c(A(Y))$

Donc, si deux n-tuples sont terme-à-terme équivalents, les valeurs de A sur les n-tuples seront équivalentes pour tout A n-aire dans $Pols^o \bigcap Pol\lambda_+$. Donc $Pols^o \bigcap Pol\lambda_+ \subseteq Pol \sim \bigcap Pol\lambda_+ \subseteq Pol\lambda_+$.

Mais puisque $\sim$ est un relation d'équivalence, Pol$\sim$ contient toutes les fonctions constantes. Donc $Pols^o \bigcap Pol\lambda_+ \subsetneq Pol \sim \bigcap Pol\lambda_+ \subseteq Pol\lambda_+$.

Pour que $Pols^o \bigcap Pol\lambda_+$ soit maximal dans $Pol\lambda_+$, il faut que $Pol \sim \bigcap Pol\lambda_+ = Pol\lambda_+$. Par maximalité de $Pol \sim$, il faut que $Pol \sim = P_k$, donc que $\sim$ soit ou triviale, n'ayant que des classes d'équivalence de un élément, ou totale, ayant une seule classe d'équivalence qui soit E_k.

Puisque $c(x) \neq 0$ pour tout x car s est sans point fixe, il y a au moins x et y dans E_k, $x \neq y$, avec $c(x) = c(y)$. Donc, pour que $\sim$ soit triviale, il faut que

$\sim= E_k^2$, donc que $c = c(a) = c(b)$ pour tout a et b.

□

Lemme 3.3.1. *Si $s(x) = x + c$ pour tout x dans E_k,*
$Pols^o \bigcap Pol\lambda_+ = \{A(x_1, ..., x_n) = a + \sum A_i x_i | (\sum A_i)c = c\}$.
Pour alléger la notation, définissons $D = \{A(x_1, ..., x_n) = a + \sum A_i x_i | (\sum A_i)c = c\}$.

Démonstration. 1)$D \subseteq Pols^o \bigcap Pol\lambda_+$

$A(x_1, ..., x_n) = a + \sum A_i x_i \in D$
$A(s(x_1), ..., s(x_n)) = a + \sum A_i(x_i + c) = a + \sum A_i x_i + \sum A_i c$
$= a + \sum A_i x_i + (\sum A_i)c = a + \sum A_i x_i + c$
$= s(a + \sum A_i x_i) = s(A(x_1, ..., x_n))$

Donc pour A dans D arbitraire, A est contenu dans $Pols^o \bigcap Pol\lambda_+$.

2)$Pols^o \bigcap Pol\lambda_+ \subseteq D$

$A(x_1, ..., x_n) = a + \sum A_i x_i \in Pols^o \bigcap Pol\lambda_+$
$A(s(x_1), ..., s(x_n)) = a + \sum A_i(x_i + c) = a + (\sum A_i x_i) + (\sum A_i)c$
$= s(A(x_1, ..., x_n)) = a + (\sum A_i x_i) + c \Rightarrow (\sum A_i)c = c$

Donc pour A dans $Pols^o \bigcap Pol\lambda_+$ arbitraire, A est dans D

□

Lemme 3.3.2. *Soit $B_1(x) = b + Bx \in Pol\lambda_+ \setminus Pols^o$, $C_0(x) = 0$ pour tout x.*
Si pour un certain c fixe, $s(x) = x + c$ pour tout x, alors $C_0 \in \langle D \bigcup \{B_1\} \rangle$

Démonstration. Par le lemme 3.3.1, on voit que $f_{-a}(x) = x - a$ est dans D pour tout a, ce qui veut dire que, par abus de notation, $B(x) = f_{-b}(B_1(x)) = Bx$ est dans $\langle D \bigcup \{B_1\} \rangle$.

1) Supposons $Bc = ac$ pour un a dans $\mathbb{Z}_p$, $a \neq 1$, alors $(B + (1 - a)I)c = c$
Donc, par le lemme 3.3.1, $B_2(x_1, x_2) = Bx_1 + (1 - a)x_2$ est dans D
Donc, $B_2(x_1, B(x_1)) = (2 - a)Bx_1$ est dans $\langle D \bigcup \{B_1\} \rangle$
Donc, $B_2((2 - a)Bx_1, B^2(x_1)) = (3 - 2a)B^2 x_1$ est dans $\langle D \bigcup \{B_1\} \rangle$
etc...

Par récurrence, $(1 + i(1 - a))B^i x_1$ est dans $\langle D \bigcup \{B_1\} \rangle$ pour tout i

Nous identifierons $(E_k, +)$ avec l'espace vectoriel $\mathbb{Z}_p^m$.
Puisque $a \neq 1$, $\langle 1 - a \rangle_+ = \mathbb{Z}_p$ et il existe $j \in \mathbb{Z}_p$ tel que $j(1 - a) = -1$, où $+$ est l'addition mod p. Donc $(1 + j(1 - a))B^j x_1 = 0B^j x_1 = C_0$ est dans $\langle D \bigcup \{B_1\} \rangle$.

2) Supposons Bc et c sont linéairement independants, alors il existe $y_1, ..., y_{m-2}$ tels que $\{c, Bc, y_1, ..., y_{m-2}\}$ est une base de E_k sur $\mathbb{Z}_p$.

Soit f l'extension linéaire de $f(c) = c$, $f(Bc) = f(y_i) = 0$ pour tour i.
Soit g l'extension linéaire de $g(c) = g(Bc) = g(y_i) = c$ pour tout i.

Puisque f et g sont linéaires et que $f(c) = g(c) = c$, f et g sont dans D, (en effet, $f(s(x)) = f(x + c) = f(x) + f(c) = f(x) + c = s(f(x))$).

Alors $A(x) = f(B(g(x)))$ est dans $\langle D \bigcup \{B_1\}\rangle$, mais pour tout x, $g(x) = ac$ pour un certain a dans $\mathbb{Z}_p$, donc $A(x) = f(B(ac)) = f(aBc) = af(Bc) = a0 = 0$ pour tout x
$\Rightarrow A = C_0 \in \langle D \bigcup \{B_1\}\rangle$

□

Théorème 3.3.1. *$Pols^o \bigcap Pol\lambda_+$ est maximal dans $Pol\lambda_+$ si et seulement si il y a un c fixe tel que $s(x) = x + c$ pour tout x.*

Démonstration. $\Rightarrow$: Proposition 3.3.1
$\Leftarrow$: Soit $B'(x_1, ..., x_n) = b + \sum B_i x_i \in Pol\lambda_+ \setminus Pols^o$.
$B(x_1, ..., x_n) = f_{-b}(B'(x_1, ..., x_n) = \sum B_i x_i$ est dans $\langle D \bigcup \{B_1\}\rangle$ par argument plus haut.

Si B est constante, on voit tout de suite que $B = C_0$.
Si B est 1-aire, on a prouvé au lemme 3.3.2 que C_0 est dans $\langle D \bigcup \{B\}\rangle$.
Si B est n-aire avec $n \geq 2$, $B_1(x_1) = B(x_1, ..., x_1) = (\sum B_i)x_1$ est dans $\langle D \bigcup \{B\}\rangle$.

Par lemme 3.3.1, on sait que $(\sum B_i)c \neq c$, donc B_1 n'est pas dans D, donc C_0 est dans $\langle D \bigcup \{B\}\rangle$ par lemme 3.3.2.
Il suffit donc de montrer que $\langle D \bigcup \{C_0\}\rangle = Pol\lambda_+$.

Soit $A((x_1, ..., x_n) = a + \sum A_i x_i$ une fonction quasi-linéaire quelconque, et soit $A_{n+1} = I - \sum A_i$ (où I reprèsente l'identité), $(\sum A_i + A_{n+1})c = c$, donc par le lemme 3.3.1, $A'(x_1, ..., x_{n+1}) = a + \sum A_i x_i \in D$.
$\Rightarrow A(x_1, ..., x_n) = A'(x_1, ..., x_n, C_0(x_{n+1})) \in \langle D \bigcup \{C_0\}\rangle$ pour $A \in Pol\lambda_+$ quelconque
$\Rightarrow Pol\lambda_+ = \langle D \bigcup \{C_0\}\rangle$ contenu dans $\langle D \bigcup \{B\}\rangle$ contenu dans $Pol\lambda_+$ pour tout $B \in Pol\lambda_+ \setminus Pols^o$

□

Remarque 3.3.1. *On peut voir que ce résultat est une généralisation du résultat pour $m = 1$ présenté à la section 2.4. Il est aussi intéressant de remarquer que $Pol\lambda_+ \bigcap Pols^o$ est sous-maximal dans $Pol\lambda_+$ si et seulement si il est aussi maximal dans $Pols^o$, comme à la section 2.3*

3.4. CLONES DE FONCTIONS QUASI-LINÉAIRES MONOTONES

Soit $\leq$ une relation d'ordre sur E_k possédant un plus grand et un plus petit élément. Supposons que $k = p^m$. Soit $+$ une opération binaire sur E_k telle que $(E_k, +) \cong \mathbb{Z}_p^m$ et supposons sans perdre de généralité que 0 en est le neutre.

Définissons $Pol\lambda_+$ comme le clone des fonctions quasi-linéaires par rapport à $+$ et $Pol \leq$ comme étant le clone des fonctions monotones par rapport à $\leq$. Nous allons chercher une condition nécessaire et suffisante pour que $Pol \leq \bigcap Pol\lambda_+$ soit maximal dans $Pol\lambda_+$.

Les propositions 1 et 2 seront ré-utilisées aux sections 3.5, 3.6 et 3.7, et seront donc formulées en des termes aussi généraux que possible.

Les résultats de cette section sont dues à l'auteur.

Proposition 3.4.1. *Soit $C \subsetneq Pol\lambda_+$. Si C est maximal dans $Pol\lambda_+$, C doit satisfaire à l'une de ces deux propriétés :*
i) Soit $f_a(x) = x + a$ et $\Delta = \{f_a | a \in E_k\}$. $\Delta \subsetneq C$.
ii) Pour tous $A_1, ..., A_n$ de $End(E_k, +)$, il existe au moins un $a_{A_1,...,A_n}$ tel que $A(x_1, ..., x_n) = a_{A_1,...,A_n} + \sum A_i x_i$ est dans C (condition(*)).

Démonstration. Supposons par la contraposée que C ne satisfait à aucune des deux conditions. Nous allons montrer que $C \subsetneq \langle C \bigcup \Delta \rangle \subsetneq Pol\lambda_+$.

$C \subsetneq \langle C \bigcup \Delta \rangle$ par hypothèse. Définissons un C" de la façon suivante :
$C' = \{f \in Pol\lambda_+^n$ tel que $f(0, ..., 0) = 0$ et il existe un certain a tel que $f_a(f(x_1, ..., x_n)) \in C\}$, C" $= \{f_a(f)$ tels que $f \in C'$ et $a \in E_k$ quelconque$\}$.

Si $A(x_1, ..., x_n) = \sum A_i x_i$ est dans C', il y a $a_{A_1,...,A_n}$ tel que $A'(x_1, ..., x_n) = f_a(A(x_1, ..., x_n)$ est dans C, donc $A = f_{-a}(A')$ donc $C' \subseteq \langle C \bigcup \Delta \rangle$

De plus, soit A un élément de $\langle C \bigcup \Delta \rangle$. A doit donc être une itération finie de fonctions de C et de fonctions f_a, avec a dans E_k.

$B(x_1, ..., x_n) = b + \sum B_i x_i$, $B(x_1, ..., f_a(x_i), ..., x_n) = b + B_i a + \sum B_i x_i$
$= f_{b+B_i a}(B(x_1, ..., x_n))$. Ainsi donc, toute itération finie, disons A, de fonctions de C et de fonctions de la forme f_a peut être écrite sous la forme $A(x_1, ..., x_n) = f_{a'}(A'(x_1, ..., x_n))$, où A' est une itération finie de fonctions de C (et donc A' une fonction de C).

Mais alors tout A de $\langle C \bigcup \Delta \rangle$ est de la forme $A(x_1, ..., x_n) = a + \sum A_i x_i$ et il existe $a_{A_1,...,A_n}$ tel que $A'(x_1, ..., x_n) = a_{A_1,...,A_n} + \sum A_i x_i$ est dans C.
$\Rightarrow \langle C \bigcup \Delta \rangle \subseteq C$", et C" $\subsetneq Pol\lambda_+$ par hypothèse.

□

Remarque 3.4.1. *Si C satisfait les deux conditions plus haut, cela veut dire que pour tout $A_1, ..., A_n$ il y a un a tel que $a + \sum A_i x_i$ est dans C, et f_{-a} est dans C, donc $\sum A_i x_i$ en fait aussi partie. Soit donc $B(x_1, ..., x_n) = b + \sum B_i x_i$ une fonction quasi-linéaire quelconque, $B = f_b(\sum B_i x_i)$, et donc $B \in C$.*

Donc, si $\Delta \subsetneq C$ et C satisfait la condition(*), il s'ensuit que $C = Pol\lambda_+$.

Proposition 3.4.2. *Soit $C \subsetneq Pol\lambda_+$. Si C satisfait la condition(*), il existe $g \in C \bigcap S_k$ tel que g possède un point fixe et un $(k-1)$-cycle.*

Démonstration. Définissons une opération $\cdot$ sur E_k telle que $(E_k, +, \cdot) \cong \mathbb{F}_{p^m}$. Il est bien connu que le groupe multiplicatif du corps est cyclique. Choisissons donc a qui engendre le groupe multiplicatif au complet. $g'(x) = a \cdot x$ est de toute évidence linéaire, donc si C satisfait la condition(*), il existe un b tel que $g(x) = a \cdot x + b$ est dans C.

La fonction $g^n(x) = g(g(...(g(x))...)) = a^n \cdot x + c$ (pour un c calculable). Pour tout d différent de 0 ou 1 et e quelconque, le polynôme $(d-1) \cdot x + e$ a une unique racine, et donc g^n a un unique point fixe (le même que g) pour tout n plus petit que $k-1$.

Or, si g aurait un cycle d'une longueur plus petite que $k-1$, il y aurait un n plus petit que $k-1$ tel que g^n aurait plus qu'un point fixe. Donc, puisque g possède un point fixe $((a-1)^{-1} \cdot (-b))$ et n'a aucun cycle de longueur plus petite que $k-1$, g est un $(k-1)$-cycle.

□

Théorème 3.4.1. *$Pol\lambda_+ \bigcap Pol \leq$ n'est jamais maximal dans $Pol\lambda_+$.*

Démonstration. Soit f un élément de S_k et m et M les plus petit et plus grand éléments par rapport à $\leq$. Si f préserve $\leq$, alors il faut que m et M soit des points fixes de f. Pour voir cela, il suffit de remarquer que $f^{-1}(m) \geq m \Rightarrow m \geq f(m)$ et $f^{-1}(M) \leq M \Rightarrow M \leq f(M)$.

Pour tout a différent de 0, f_a est une permutation sans points fixes, donc Δ n'est pas contenu dans $Pol\lambda_+ \bigcap Pol \leq$. De plus, par la proposition 3.4.2, si $Pol\lambda_+ \bigcap Pol \leq$ satisfairait la condition(*), il y aurait une permutation ayant un seul point fixe dans $Pol \leq$...

Donc, puisque Δ n'est pas contenu dans $Pol\lambda_+ \bigcap Pol \leq$ et que $Pol\lambda_+ \bigcap Pol \leq$ ne peut satisfaire la condition(*), $Pol\lambda_+ \bigcap Pol \leq$ n'est pas maximal dans $Pol\lambda_+$ par la proposition 3.4.1.

□

3.5. Clones de fonctions quasi-linéaires préservant une équivalence

Soit $\sim$ une relation d'équivalence sur E_k. Supposons que $k = p^m$. Soit $+$ une opération binaire sur E_k telle que $(E_k, +) \cong \mathbb{Z}_p^m$ et supposons sans perdre de généralité que 0 en est le neutre.

Définissons $Pol\lambda_+$ comme le clone des fonctions quasi-linéaires par rapport à $+$ et $Pol \sim$ comme étant le clone des fonctions préservant la relation $\sim$. Nous allons chercher une condition nécessaire et suffisante pour que $Pol \sim \bigcap Pol\lambda_+$ soit maximal dans $Pol\lambda_+$.

La proposition 1 sera ré-utilisé aux sections 3.6 et 3.7, et sera donc formulée en des termes aussi généraux que possible.

Les résultats de cette section sont dues à l'auteur.

Lemme 3.5.1. *Soit H un sous-groupe de $\mathbb{Z}_p^m \rtimes GL_m(\mathbb{Z}_p)$ (avec l'action évidente) tel que, pour tout A dans $GL_m(\mathbb{Z}_p)$, il existe au moins un a tel que aA soit dans H.*

Alors ou $|H| = |GL_m(\mathbb{Z}_p)|$, ou $H = \mathbb{Z}_p^m \rtimes GL_m(\mathbb{Z}_p)$.

Démonstration. Pour tout A dans $GL_m(\mathbb{Z}_p)$, choisissons un a tel que $aA \in H$ (nous savons qu'un tel a doit exister par hypothèse).Soit $E = \mathbb{Z}_p^m \bigcap H$. Pour tout $e \in E$, $eIaA = (e + a)A$ est dans H, donc pour tout A pour lequel on a choisi l'élément a, $(a + E)A \subsetneq H$ et $|H| \geq |E||GL_m(\mathbb{Z}^p)|$.

D'un autre côté, $E \lhd H$ et H contient au moins un représentant de chaque translaté de $\mathbb{Z}_p^m$, donc $\mathbb{Z}_p^m H = \mathbb{Z}_p^m \rtimes GL_m(\mathbb{Z}_p)$. Donc, par le deuxième théorème d'isomorphismes, $H/E \cong \mathbb{Z}_p^m \rtimes GL_m(\mathbb{Z}_p)/\mathbb{Z}_p^m = GL_m(\mathbb{Z}_p)$, $|H| = |E||GL_m(\mathbb{Z}_p)|$ et pour tout A de $Aut(E_k, +)$ pour lequel on a choisi l'élément a, si hA est dans H, alors h est dans $a + E$.

Mais, pour tout A pour lequel on a choisi l'élément a et pour tout $e \in E$, $aAeI = (a + Ae)A$ est dans H, donc $a + Ae$ est dans $a + E$, donc Ae est dans E pour tout e dans E, A dans $GL_m(\mathbb{Z}_p)$,
$\Rightarrow E$ est un sous-groupe charactéristique de $\mathbb{Z}_p^m$
$\Rightarrow E = \{0\}$ ou $E = \mathbb{Z}_p^m$.

□

Proposition 3.5.1. *Soit C un sous-clone propre de $Pol\lambda_+$ tel que C respecte la condition(*). Alors pour tout A de $Aut(E_k, +)$, il existe un unique a tel que $f(x) = Ax + a$ soit dans C.*

Si C respecte la condition(*) et que $|C \bigcap \Delta| > 1$, alors $C = Pol\lambda_+$

Démonstration. Tout d'abord, remarquons que $Pol\lambda_+ \bigcap S_k \cong \mathbb{Z}_p^m \rtimes GL_m(\mathbb{Z}_p)$. En effet, $(E_k, +) \cong \mathbb{Z}_p^m$ par définition (et donc $Aut(E_k, +) \cong GL_m(\mathbb{Z}_p)$). De plus, si f est une fonction 1-aire, quasi-linéaire et inversible (en d'autres mots, f est dans $Pol\lambda_+ \bigcap S_k$), il doit y avoir un automorphisme A de $(E_k, +)$ et un élément a de E_k tel que $f(x) = a + Ax$. La remarque devient évidente lorsque l'on pense que $(a + Ax) \circ (b + Bx) = a + A(b + Bx) = a + Ab + ABx$ tout comme $aAbB = (a + Ab)AB$ dans $\mathbb{Z}_p^m \rtimes GL_m(\mathbb{Z}_p)$.

Ensuite, si C est un sous-clone propre de $Pol\lambda_+$ respectant la condition(*), il faut que $C \bigcap S_k$ soit un sous-groupe de $Pol\lambda_+ \bigcap S_k$ tel que pour tout automorphisme A de $(E_k, +)$, il existe au moins un élément a de E_k tel que $f(x) = a + Ax$ soit dans C. De plus, si C est propre dans $Pol\lambda_+$, il s'ensuit que $\Delta \nsubseteq C$, et donc que $C \bigcap S_k$ est un sous-groupe propre de $Pol\lambda_+ \bigcap S_k$, et donc que $|C \bigcap S_k| = |Aut(E_k, +)|$ par le lemme 3.5.1.

Si C respecte (*) et $|C \bigcap \Delta| > 1$, alors $\Delta \subsetneq C$ par le lemme 3.5.1, et donc $C = Pol\lambda_+$.

□

Proposition 3.5.2. *Soit $C = Pol \sim \bigcap Pol\lambda_+$, et $\Delta \subsetneq C$. Alors il existe E un sous-espace de E_k sur $\mathbb{Z}_p$ tel que $a \sim b$ si et seulement si $a - b \in E$.*

Dans ce cas-là, $C = \{A(x_1, ..., x_n) = a + \sum A_i x_i | E$ est A_i-invariant $\forall i\}$.

Démonstration. Soit $E = \{x | x \sim 0\}$. Si x et y sont dans E et que $\Delta \subseteq C$, alors $0 \sim y$ implique que $y + x \sim 0 + x = x \sim 0$, donc E est un sous-espace de E_k. De plus, si $a \sim b$ alors $a - b \sim b - b = 0$, et si $a - b \sim 0$ alors $a = a - b + b \sim 0 + b = b$.

Soit $C' = \{A(x_1, ..., x_n) = a + \sum A_i x_i | E$ est A_i-invariant pour tout $i\}$. Il nous reste à montrer que $C = C'$.

Soit $A(x_1, ..., x_n) = a + \sum A_i x_i$ un élément quelconque de C', $X = (x_1, ..., x_n)$ et $Y = (y_1, ..., y_n)$ tels que x_i est congru modulo E à y_i pour tout i.

$A(X) - A(Y) = a + \sum A_i x_i - a - \sum A_i y_i = \sum A_i(x_i - y_i)$. Puisque A est élément de C' et que x_i est congru modulo E à y_i pour tout i, $A_i(x_i - y_i)$ sera dans E pour tout i, et donc $A(X) - A(Y)$ sera dans E.
$\Rightarrow C' \subseteq C$.

Soit $A(x_1, ..., x_n) = a + \sum A_i x_i$ un élément quelconque de C et e un élément quelconque de E. Les n-tuples $0^n = (0, ..., 0)$ et $e_i^n = (0, ..., 0, e, 0, ..., 0)$ où le e est à la i-ème place seront terme à terme équivalents pour tout i, donc $A(0^n) - A(e_i^n)$ sera dans E. Or, $A(0^n) - A(e_i^n) = A_i e$, donc pour tout i et pour tout e élément de E, il faut que $A_i e$ soit dans E.

$\Rightarrow C \subseteq C'$.

□

Lemme 3.5.2. *Si C satisfait la condition(*), alors $\sim$ possède un point isolé.*

Démonstration. Par la proposition 3.4.2, si C satisfait la condition(*), il faut qu'il existe $g \in C \bigcap S_k$ tel que g soit un $(k-1)$-cycle. Soit x l'élément fixe de g. Si $x \sim y$ avec $x \neq y$, il faudrait que $x \sim g^n(y)$ pour tout n, donc que $x \sim z$ pour tout z se trouvant sur le $(k-1)$-cycle, et donc que $\sim = E_k^2$. x doit donc être un élément isolé de $\sim$.

□

Proposition 3.5.3. *Si C est maximal dans $Pol\lambda_+$, alors il existe E un sous-espace de E_k tel que $a \sim b$ si et seulement si $a - b \in E$.*

Démonstration. Par les propositions 3.4.1 et 3.5.2, il suffit de montrer que C ne peut satisfaire la condition(*) et être maximal.

Par le lemme 3.5.2, si C satisfait la condition(*), $\sim$ doit avoir un point isolé qui soit le point fixe de g, un $(k-1)$-cycle de C. Supposons $g(x) = Ax + a$. À remarquer que A est dans $Aut(E_k, +)$ car g est inversible.

Si C satisfait la condition(*), il y aurait a' tel que $g'(x_1, x_2) = Ax_1 + Ix_2 + a'$ soit dans C. C_0, la fonction constante à valeur 0, est dans C, et donc $g'(C_0(x_1), x_2) = Ix_2 + a'$ et $g'(x_1, C_0(x_2)) = Ax_1 + a'$ sont aussi des éléments de C. Donc, par la proposition 3.5.1, pour que C soit maximal, il faudrait que $a = a' = 0$ et 0 est un point isolé de $\sim$.

Par la condition(*), $f(x_1, ..., x_p) = \sum x_i$ est dans C (il aurait fallu qu'il y ait une certaine constante compatible, et ce doit être 0 car C_0 est dans C). Supposons que $x \sim y$ avec $x \neq y$. Alors les p-tuples $(x, ..., x)$ et $(y, x, ..., x)$ sont terme à terme équivalents, mais $f(x, ..., x) = 0$ et $f(y, x, ..., x) = y - x \neq 0$. Donc, pour que C satisfasse la condition(*) et soit maximale, $\sim$ devrait être la relation triviale $x \sim x$...

□

Lemme 3.5.3. *Soit $E = \{(x_1, ..., x_u, 0, ..., 0) | x_i$ un élément de $\mathbb{Z}_p\}$ un sous-espace de $\mathbb{Z}_p^m$. $R = \{M$ un élément de $\mathbb{Z}_p^{m \times m} | E$ est M-invariant$\}$ est un sous-anneau maximal de $\mathbb{Z}_p^{m \times m}$.*

Démonstration. De tout évidence, $R = \{M \in \mathbb{Z}_p^{m \times m} | M_{ij} = 0$ si $i \leq u$ et $j > u\}$ (nous supposons que les matrices agissent par multiplication à gauche sur des vecteurs mis sous forme de colonne). Soit M une matrice de $\mathbb{Z}_p^{m \times m} \setminus R$. De toute évidence, il existe $M' \in R$ telle que $M'_{ij} = M_{ij}$ si $i > u$ ou $j \leq u$, et $M - M'$ est

dans $\langle R \bigcup \{M\} \rangle_{+,\cdot}$.

Soit M^{ij} la matrice $m \times m$ sur $\mathbb{Z}_p$ telle que $M^{ij}_{i'j'} = 1$ si $i' = i$ et $j' = j$, 0 sinon. Les matrices n'ayant des entrées non-nulles que sur la diagonale étant dans R, nous pouvons multiplier les lignes et les colonnes de M' (multiplication à gauche et à droite) pour obtenir M^{ij} pour un certain $i > u$ ou $j \leq u$ à partir de $M - M'$.

De toute évidence, M^{ij} est déjà dans R si $i > u$ ou $j \leq u$, et nous venons de voir que au moins un M^{ij} avec $i > u$ et $j \leq u$ est dans $\langle R \bigcup \{M\} \rangle_{+,\cdot}$. De plus, les matrices permutant les lignes i' et j' sont dans R si $i' > u < j'$, ainsi que les matrices permutant (par multiplication à gauche) les colonnes i'' et j'' sont aussi dans R si $i'' \leq u \geq j''$.

Par là même, ayant M^{ij} avec $i \leq u$ et $j > u$ dans $\langle R \bigcup \{M\} \rangle_{+,\cdot}$, ainsi que toute les M^{ij} avec $i > u$ ou $j \leq u$ ainsi que les matrices permutant les lignes et les colonnes définies plus haut, nous aurons que $M^{ij} \in \langle R \bigcup \{M\} \rangle_{+,\cdot}$ pour tout i et j. Il en résulte évidemment que $\langle R \bigcap \{M\} \rangle_{+,\cdot} = \mathbb{Z}_p^{m \times m}$.

□

Remarque 3.5.1. *Le fait reste vrai pour tout sous-espace de $\mathbb{Z}_p^m$, puisque pour tout $E < \mathbb{Z}_p^m$, l'anneau des matrices préservant E est le conjugué par des matrices de changement de base de l'anneau préservant un sous-espace E' de la forme plus haut.*

Théorème 3.5.1. *$Pol \sim \bigcap Pol\lambda_+$ est maximal dans $Pol\lambda_+$ si et seulement si il existe E un sous-espace de E_k tel que $a \sim b$ si et seulement si $a - b \in E$.*

Démonstration. Par les propositions 3.5.2 et 3.5.3, il suffit de montrer que $\{A(x_1, ..., x_n) = a + \sum A_i x_i | E$ est A_i-invariant pour tout $i\}$ est maximal dans $Pol\lambda_+$ pour tout E sous-espace de E_k.

Soit $\{e_1, ..., e_u\}$ une base de E. Il existe $h_1, ..., h_{m-u}$ tels que $\{e_1, ..., e_u, h_1, ..., h_{m-u}\}$ est une base de E_k. Par rapport à cette base, nous pouvons écrire les éléments de E_k comme des vecteurs m-aires sur $\mathbb{Z}_p$, et E sera le sous-espace décrit au lemme 3.5.3.

De nouveau par rapport à cette base, nous pouvons représenter les endomorphismes de $(E_k, +)$ comme des matrices $m \times m$ sur $\mathbb{Z}_p$. Soit $R' = \{M \in End(E_k, +) | M'(x) = Mx$ est dans $C\}$. Par la proposition 3.5.2, R' sera représenté comme l'anneau R décrit au lemme 3.5.3, et $R' \subseteq C$.

Soit donc $B(x_1, ..., x_n) = b + \sum B_i x_i$, B n'est pas dans C. Cela veut dire qu'il y a B_j qui n'est pas dans R'. $B'(x_1, ..., x_n) = f_{-b}(C_0(x_1), ..., x_j, ..., C_0(x_n))$
$= B_j(x_j)$ sera dans $\langle C \bigcup \{B\} \rangle$.

Puisque $f(x_1, x_2) = x_1 + x_2$ est dans C (I est dans R'), $\langle R' \bigcup \{B_j\}\rangle_{+,\circ}$ sera dans $\langle C \bigcup \{B\}\rangle$ (où $+$ et $\circ$ se réfèrent à l'addition et la composition d'endomorphismes). Mais puisque R' est représentée comme le R décrit au lemme 3.5.3 par rapport à la base plus haut et que B_j n'est pas dans R' (et donc sa représentation pas dans R), $\langle R' \bigcup \{B_j\}\rangle_{+,\circ} = End(E_k, +)$.

Soit donc $A(x_1, ..., x_n) = a + \sum A_i x_i$ une fonction quasi-linéaire quelleconque, et définissons $f(x_1, x_2) = x_1 + x_2$ et, pour M dans $End(E_k, +)$, $M(x) = Mx$.

$A(x_1, ..., x_n) = f_a(f(A_1(x_1), f(A_2(x_2), ..., f(A_{n-1}(x_{n-1}), A_n(x_n))...)))$, toutes des fonctions de $\langle C \bigcup \{B\}\rangle$
$\Rightarrow Pol\lambda_+ = \langle C \bigcup \{B\}\rangle$ pour tout B dans $Pol\lambda_+ \setminus C$.

□

Remarque 3.5.2. *Dans le cas $m = 1$, toute relation d'équivalence modulo un sous-espace sera triviale. C'est pourquoi il n'y avait aucun clone sous-maximal de la forme $Pol\lambda_+ \bigcap Pol \sim$ à la section 2.4.*

3.6. Clones de fonctions quasi-linéaires préservant une relation centrale

Soit δ une relation centrale u-aire sur E_k dont d est un élément central. Supposons que $k = p^m$. Soit $+$ une opération binaire sur E_k telle que $(E_k, +) \cong \mathbb{Z}_p^m$ et supposons sans perdre de généralité que 0 en est le neutre.

Définissons $Pol\lambda_+$ comme le clone des fonctions quasi-linéaires par rapport à $+$ et $Pol\delta$ comme étant le clone des fonctions préservant la relation δ. Nous allons chercher une condition nécessaire et suffisante pour que $Pol\delta \bigcap Pol\lambda_+$ soit maximal dans $Pol\lambda_+$.

Les résultats de cette section sont dues à l'auteur.

Lemme 3.6.1. *Si $D = Pol\delta \bigcap Pol\lambda_+$ est maximal dans $Pol\lambda_+$, alors δ est 1-aire.*

Démonstration. Supposons faux. Pour que δ soit non-triviale, il faut qu'il existe $(x_1, ..., x_u) \notin \delta$. $(d, x_2 - x_1 + d, ..., x_u - x_1 + d) \in \delta$, donc $f_{x_1 - d} \notin D$, et donc Δ n'est pas contenu dans D. Par la proposition 3.4.1, cela veut dire que D doit satisfaire la condition(*) pour être maximale.

Il doit donc exister un certain b tel que $f((x_1, x_2) = x_1 + x_2 + b$ est dans D. Mais les n-tuples $(d, x_2 - d - b, x_3, ..., x_u)$ et $(x_1 - d - b, d, -b, ..., -b)$ sont tous deux dans δ, tandis que $f(d, x_1 - d - b) = x_1$, $f(x_2 - d - b, d) = x_2$ et $f(x_i, -b) = x_i$ pour tout i, tandis que $(x_1, ..., x_u) \notin \delta$.

Donc, si $u > 1$, D ne peut satisfaire la condition(*) et ne contient pas Δ.

□

Lemme 3.6.2. *Soit E un sous-ensemble propre de E_k. Si $D = Pol E \bigcap Pol\lambda_+$ est maximal dans $Pol\lambda_+$, alors $|E| = 1$.*

Démonstration. Supposons faux. Si x élément de E et y non, $f_{y-x} \notin D$, et donc Δ n'est pas contenu dans D. Il faudrait donc que D satisfait la condition(*), et donc qu'il existe b tel que $f(x_1, x_2) = x_1 + x_2 + b$ soit dans D. Puisque $|E| > 1$, il existe un $c \in E$, et donc que C_c (la fonction constante à valeur c) soit dans D, tel que $c \neq -b$. $f(x_1, C_c(x_2)) = x_1 + (c - b)$, avec $c - b \neq 0$, serait donc dans D.

Par la proposition 3.5.1, si D satisfait la condition(*) et que $|D \bigcap \Delta| > 1$, alord $D = Pol\lambda_+$ Contradiction.

□

Théorème 3.6.1. *$Pol\delta \bigcap Pol\lambda_+$ est maximal dans $Pol\lambda_+$ si et seulement si δ est 1-aire et $|\delta| = 1$.*

Démonstration. Par les lemmes 3.6.1 et 3.6.2, il suffit de montrer que $Pol\lambda_+ \bigcap Pol\{d\}$ est maximal dans $Pol\lambda_+$ (avec d l'élément central quelconque posé plus haut) pour tout d dans E_k. Soit $D = Pol\lambda_+ \bigcap Pol\{d\}$.

Il est facile à voir que $D = \{A(x_1, ..., x_n) = a + \sum A_i x_i | a = d - \sum A_i d\}$. En effet, pour un A construit comme ci-contre, il est facile à voir que $A(d, ..., d) = d$ et que si $A(d, ..., d) = d$, A doit avoir la forme plus haut. Il est aussi facile à voir que D satisfait la condition(*).

Soit donc $B(x_1, ..., x_n) = b + \sum B_i x_i$ quelconque avec $b \neq d - \sum B_i d$. $f(x_1, x_2) = x_1 - x_2 + d$ est dans D, ainsi que $B'(x_1, ..., x_n) = d - \sum B_i d + \sum B_i x_i$, alors en particulier $f(B(x_1, ..., x_n), B'(x_1, ..., x_n)) = C_{b + \sum B_i d}$ sera dans $\langle D \bigcup \{B\} \rangle$.

Par là-même $f(x_1, C_{b+\sum B_i d}(x_1)) = x_1 + (b + \sum B_i d - d)$ sera dans $\langle D \bigcup \{B\} \rangle$, avec $b - d + \sum B_i d = b - (d - \sum B_i d) \neq 0$ par hypothèse. Mais puisque D satisfait la condition(*), $\langle D \bigcup \{B\} \rangle$ sera un clone satisfaisant (*) et dont l'intersection avec Δ possède plus d'un élément...

$\Rightarrow \langle D \bigcup \{B\} \rangle = Pol\lambda_+$ pour un B quelconque dans $Pol\lambda_+ \setminus D$ par la proposition 3.5.1.

□

Remarque 3.6.1. *On peut voir que ce résultat est une généralisation du résultat pour $m = 1$ présenté à la section 2.4.*

3.7. CLONES DE FONCTIONS POSSÉDANT DEUX REPRÈSENTATIONS QUASI-LINÉAIRES

Supposons que $k = p^m$. Soit $+$ et $\oplus$ deux opérations binaires sur E_k telles que $(E_k, +) \cong (E_k, \oplus) \cong \mathbb{Z}_p^m$ et notons par 0_+ le neutre de $+$ et $0_\oplus$ le neutre de $\oplus$.

Définissons $Pol\lambda_+$ comme le clone des fonctions quasi-linéaires par rapport à $+$ et $Pol\lambda_\oplus$ le clone des fonctions quasi-linéaires par rapport à $\oplus$. Nous allons noter par Δ_+ l'ensemble des fonctions de la forme $f_{a,+}(x) = x + a$ et par $\Delta_\oplus$ l'ensemble des fonctions de la forme $f_{a,\oplus}(x) = x \oplus a$.

Les résultats de cette section sont dues à l'auteur.

Lemme 3.7.1. *Si $g(x, y) = x + y$ est dans $Pol\lambda_\oplus$, alors $Pol\lambda_+ = Pol\lambda_\oplus$.*

Démonstration. La preuve a, en fait, déjà été donnée à la section 1.3, nous la répeterons ici pour plus de clarté.

$(x, 0_+, 0_+, x)$ et $(0_+, y, 0_+, y)$ sont dans $\lambda_\oplus$, et donc $g(x, 0_+) \oplus g(0_+, y) = g(0_+, 0_+) \oplus g(x, y)$, en d'autres mots que $x \oplus y = 0_+ \oplus (x + y)$ et donc que $x + y = x \oplus y \ominus 0_+$.

Soit $f : E_k \to E_k$, $f(x) = x \ominus 0_+$, $f(x+y) = f(x \oplus y \ominus 0_+) = x \oplus y \ominus 0_+ \ominus 0_+ = (x \ominus 0_+) \oplus (y \ominus 0_+) = f(x) \oplus f(y)$. Il s'ensuit que f est un isomorphisme comme celui décrit à la section 1.3.

□

Proposition 3.7.1. *Si $Pol\lambda_+ \bigcap Pol\lambda_\oplus$ est propre et maximal dans $Pol\lambda_+$, alors $\Delta_+ \subsetneq Pol\lambda_\oplus$.*

Démonstration. Par la proposition 3.4.1, il suffit de montrer que $Pol\lambda_+ \bigcap Pol\lambda_\oplus$ ne peut respecter la condition(*) et être propre et maximal dans $Pol\lambda_+$.

Pour respecter la condition(*), il faut qu'il y ait un certain a tel que $g'(x, y) = x + y + a$ soit dans $Pol\lambda_\oplus$. Or, C_{0_+}, la fonction constante à valeur 0_+ est de tout évidence dans $Pol\lambda_+ \bigcap Pol\lambda_\oplus$, et $g'(x, C_{0_+}(y)) = x + a$ est dans $\Delta_+ \bigcap Pol\lambda_\oplus$.

Mais, par la proposition 3.5.1, si $Pol\lambda_+ \bigcap Pol\lambda_\oplus$ respecte la condition(*) et soit propre, il faut que $a = 0$, et donc que $g'(x, y) = g(x, y)$ du lemme 3.7.1, et donc que $Pol\lambda_+ = Pol\lambda_\oplus$.

□

Remarque 3.7.1. *Par symmétrie, la proposition 3.7.2 nous dit aussi que $\Delta_\oplus \subsetneq Pol\lambda_+$. D'ailleurs, pour tous les énoncés de cette section, $+$ et $\oplus$ peuvent être*

interverti par symmétrie.

Proposition 3.7.2. *Si $Pol\lambda_+ \bigcap Pol\lambda_\oplus$ est propre et maximal dans $Pol\lambda_+$, alors dénotant par I la fonction identité, $\{I\} \subsetneq \Delta_+ \bigcap \Delta_\oplus \subsetneq \Delta_+$.*

Démonstration. *i)* $\Delta_+ \neq \Delta_\oplus$

Supposons par l'absurde que $\Delta_+ = \Delta_\oplus$. Alors, pour tout i dans E_k, il y a un certain j tel que $f_{i,+} = f_{j,\oplus}$. Soit $\varphi : E_k \to E_k$, $\varphi(i) = j$ (i et j comme définis plus haut), $f_{\varphi(a+b),\oplus} = f_{a+b,+} = f_{a,+}(f_{b,+}) = f_{\varphi(a),\oplus}(f_{\varphi(b),\oplus}) = f_{\varphi(a)\oplus\varphi(b),\oplus}$, et donc $\varphi(a+b) = \varphi(a) \oplus \varphi(b)$.

Il s'ensuit que φ est un isomorphisme entre $(E_k, +)$ et $(E_k, \oplus)$.

$y \oplus \varphi(x) = f_{\varphi(x),\oplus}(y) = f_{x,+}(y) = x + y = f_{y,+}(x) = f_{\varphi(y),\oplus}(x) = x \oplus \varphi(y)$ pour tous x et y, donc $\varphi(x) \ominus x = \varphi(y) \ominus y$ pour tous x et y, et donc en particulier $\varphi(x) \ominus x = \varphi(0_\oplus)$ pour tout x.

Puisque $\varphi(x) = x \oplus \varphi(0_\oplus)$ et que φ est un isomorphisme entre $(E_k, +)$ et $(E_k, \oplus)$, $Pol\lambda_+ = Pol\lambda_\oplus$.

ii) $\Delta_+ \bigcap \Delta_\oplus \neq \{I\}$

Supposons par l'absurde que $\Delta_+ \bigcap \Delta_\oplus = \{I\}$ et que $Pol\lambda_+ \bigcap Pol\lambda_\oplus$ est propre et maximal dans $Pol\lambda_+$. Soit $G = Pol\lambda_+ \bigcap Pol\lambda_\oplus \bigcap S_k$. De toute évidence, G est un groupe et, par maximalité, $\Delta_+, \Delta_\oplus < G$.

Puisque $Pol\lambda_+ \bigcap S_k \cong \mathbb{Z}_p^m \rtimes GL_m((Z)_p)$ et que $\mathbb{Z}_p^m \lhd \mathbb{Z}_p^m \rtimes GL_m((Z)_p)$, $\Delta_+ \lhd Pol\lambda_+ \bigcap S_k$ et donc $\Delta_+ \lhd G$ car $G \subsetneq Pol\lambda_+$. Puisque par hypothèse, $\Delta_+ \bigcap \Delta_\oplus = \{I\}$ et que $\Delta_+ \lhd \Delta_+\Delta_\oplus$, il s'ensuit que $\Delta_+\Delta_\oplus \cong \Delta_+ \rtimes_\varphi \Delta_\oplus$ pour une certaine action de $\Delta_\oplus$ sur Δ_+.

Mais, puisque $G \subsetneq Pol\lambda_\oplus$, il s'ensuit que $\Delta_\oplus \lhd G$, et donc que $\Delta_+\Delta_\oplus \cong \Delta_+ \times \Delta_\oplus$. Puisque $\Delta_+ \cong \Delta_\oplus \cong \mathbb{Z}_p^m$, $\Delta_+\Delta_\oplus$ sera abélien et donc $f_{a,+}$ commutera avec $f_{b,\oplus}$ pour tous a et b dans E_k.

Supposons que, dans $Pol\lambda_+$, $f_{b.\oplus}(x) = Cx + c$, $f_{a,+} \circ f_{b,\oplus} = Cx + c + a = Cx + c + Ca = f_{b,\oplus} \circ f_{a,+}$. Il s'ensuit que $Ca = a$ pour tout a dans E_k, et donc que $C = I$ et que $f_{b,\oplus} \in \Delta_+$. Puisque ceci serait vrai pour tout b dans E_k, on arrive à une contradiction.

□

Remarque 3.7.2. *De par la proposition 3.7.2, pour que $Pol\lambda_+ \bigcap Pol\lambda_\oplus$ soit propre et maximal dans $Pol\lambda_+$, il faut qu'il existe une image isomorphe de $\mathbb{Z}_p^m$*

dans $\mathbb{Z}_p^m \rtimes GL_m((Z)_p)$ qui ne soit pas égale à $\mathbb{Z}_p^m$ et qui ait une intersection triviale avec $GL_m(\mathbb{Z}_p)$ (l'image de $\Delta_\oplus$ dans $Pol\lambda_+$.

Par calcul direct, on peut voir qu'un exemple d'un tel sous-groupe serait le suivant (avec e_1 et e_2 la base canonique de $\mathbb{Z}_p^2$) :
$\{vA \in \mathbb{Z}_p^2 \rtimes GL_2((Z)_p) | v = (a,b),\ A(e_1) = e_1 + be_2,\ a(e_2) = e_2\}$.

Remarque 3.7.3. *L'auteur ne peut, hélas, amener la preuve jusqu'au bout, mais il peut émettre l'hypothèse que $Pol\lambda_+ \bigcap Pol\lambda_\oplus$ ne sera jamais propre et maximal dans $Pol\lambda_+$.*

Par la proposition 3.7.2, il faut que $\Delta_+ \bigcap \Delta_\oplus$ soit non-trivial mais non-complet. Soit $\Delta = \{a \in E_k | f_{a,+} \in \Delta_\oplus\}$. Puisque $\Delta_+ \bigcap \Delta_\oplus$ est un sous-groupe de Δ_+, il s'ensuit que Δ est un sous-espace non-trivial de $(E_k, +)$, et soit $\sim_\Delta$ la relation d'équivalence moduloΔ.

Je vais émettre l'hypothèse que $Pol\lambda_+ \bigcap Pol\lambda_\oplus \subsetneq Pol\lambda_+ \bigcap Pol \sim_\Delta$. Si l'inclusion serait prouvée, elle serait propre car $g(x,y) = x + y$ serait dans $Pol \sim_\Delta$ mais ne pourrait être dans $Pol\lambda_\oplus$ par le lemme 3.7.1.

De plus, par la proposition 3.5.2, $A(x_1, ..., x_n) = a + \sum A_i x_i$ est dans $Pol \sim_\Delta$ si et seulement si Δ est A_i-invariant pour tout i. On peut déjà prouver que, si A est un automorphisme de $(E_k, +)$ qui est utilisé dans une certaine fonction de $Pol\lambda_+ \bigcap Pol\lambda_\oplus$, puisque C_{0_+} sera dans $Pol\lambda_+ \bigcap Pol\lambda_\oplus$, il s'ensuit que $A(x) = Ax$ sera aussi dans $Pol\lambda_+ \bigcap Pol\lambda_\oplus$.

$A \circ f_{a,+} \circ A^{-1} = f_{Aa,+}$ sera aussi dans $Pol\lambda_+ \bigcap Pol\lambda_\oplus$ pour tout a, et si $Ax = Bx \oplus b$ et que $a \in \Delta$ avec $f_{a,+} = f_{a',\oplus}$, alors $f_{Aa,+} = B((B^{-1}x \ominus B^{-1}b) \oplus a') \oplus b = x \oplus Ba'$, et donc Δ est A-invariant.

Il resterait, pour finir la preuve, à prouver que si B est utilisé dans une certaine fonction de $Pol\lambda_+ \bigcap Pol\lambda_\oplus$ avec B non-inversible, alors Δ serait B-invariant.

BIBLIOGRAPHIE

[1] LAU, D., *Function Algebras on Finite Sets*, Springer Monographs in Mathematics, Springer-Verlag, Berlin-Heidelberg, 2006.

[2] BAGYINSZKI, J. ; DEMETROVICS, J., *The lattice of linear classes in prime-valued logics*, Banach Center Publications 7, Warszawa, 1982.

[3] BODNARCHUK V.G. ; KALUZHNIN L.A. ; KOTOV V.N. ; ROMOV B.A., *Galois theory for Post algebras I-II*, Traduit de Kibernetika Vol. 5, Kiev, 1969.

[4] BULATOV, A.A., *Polynomial Reducts of Modules I. Rough Classification*, Mult.-Valued Log. 3, 1998.

[5] JANOV, JU. I. ; MUČNIK, A.A., *Existence of k-valued closed classes without a finite basis (Russian)*, Dokl. Akad. Nauk. SSSR 127, 1959.

[6] LAU, D., *Submaximalen Klassen von P_3*, J. Inf. Process. Cybern. EIK 18, 1982.

[7] MACHIDA, H., *On closed sets of three-valued monotone logical functions*, Colloquia Mathematica Societatis Janos Bolyài, Finite Algebra and multiple-valued logic, Szeged, 1979.

[8] MARCHENKOV, S.S. ; DEMETROVICS, J. ; HANNAK, L., *On closed classes of self-dual functions in P_3 (Russian)*, Metody Diskretn. Anal. 34, 1980.

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

[10] ROSENBERG, I.G., *Über die funktionale Vollstaändigkeit in den mehrwertigen Logiken*, Rozpravy Československe Akad. Ved. Řada Mat. Přirod. Věd 80, 1970.

[11] ROSENBERG, I.G., *Algebraic structures and relations, a short survey*, Contributions to General Algebra 15, Proceedings of the Klagenfurt Conference, Verlag Johannes Heyn, Klagenfurt, 2004.

[12] ROSENBERG, I.G. ; SZENDREI À., *Submaximal clones with a prime order automorphism*, Acta (Szeged) 49, 1985.

[13] SALOMAA, A.A, *On the composition of functions of several variables ranging over a finite set*, Ann. Univ. Turku. Ser. 53, 1960.

[14] SZENDREI, À., *On closed classes of quasi-linear functions*, Czechoslovak Math. J. 80, 1980.