Chapitre 3

Sous-groupes $\bigwedge\!\!\bigwedge$-définissables du groupe additif d'un corps séparablement clos

Introduction

Dans ce chapitre nous étudions les sous-groupes $\bigwedge\!\!\bigwedge$-définissables du groupe additif d'un corps L séparablement clos de degré d'imperfection fini strictement positif, et plus particulièrement, la structure induite sur les sous-groupes $\bigwedge\!\!\bigwedge$-définissables additifs minimaux localement modulaires, qui sont des exemples de groupes minimaux d'exposant borné. Les théories de corps séparablement clos sont stables non superstables [Wo 79] et en fait aucun ensemble définissable n'est rangé. Les groupes minimaux ne sont donc pas définissables mais $\bigwedge\!\!\bigwedge$-définissables.

L'étude des ensembles $\bigwedge\!\!\bigwedge$-définissables dans un corps séparablement clos est beaucoup plus complexe que dans un corps algébriquement clos. Contrairement au cas des corps algébriquement clos, il n'y a pas directement l'élimination des quantificateurs et on est obligé d'introduire une topologie, limite de topologie de Zariski, qui n'est alors plus noethérienne. Malgré cette difficulté, les travaux de M. Messmer [Me 94], de E. Hrushovski [Hr 96] et de F. Delon [De 98] ont abouti en particulier (et en utilisant la trichotomie des géométries de Zariski [HZ 96]) à la dichotomie suivante sur les types minimaux : un type minimal dans un corps séparablement clos L de caractéristique p est soit localement modulaire, soit non orthogonal à $L^{p^\infty} := \cap_{n\in\omega} L^{p^n}$ qui est le sous-corps algébriquement clos maximal de L.

Récemment, E. Bouscaren et F. Delon [BD2] ont donné une description complète des groupes minimaux $\bigwedge\!\!\bigwedge$-définissables dans L et grâce à la dichotomie précédente, elles ont ainsi obtenu une description des groupes minimaux $\bigwedge\!\!\bigwedge$-définissables localement modulaires et de ceux non localement modulaires. Leur description souligne de plus une dichotomie transversale à la précédente : un groupe minimal $\bigwedge\!\!\bigwedge$-définissable est ou bien divisible, et dans ce cas de rang de transcendance fini, ou bien d'exposant p, et dans ce cas définissablement isomorphe à un sous-groupe du groupe additif de L et de rang de transcendance arbitraire. La classe des groupes minimaux additifs $\bigwedge\!\!\!\bigwedge$-définissables (les sous-groupes minimaux du groupe additif de L) est donc riche.

Notre étude des sous-groupes minimaux additifs $\bigwedge\!\!\!\bigwedge$-définissables confirmera cette richesse.

Dans la section suivant celle des préliminaires, nous montrons que tout sous-groupe additif $\bigwedge\!\!\!\bigwedge$-définissable est en fait défini par les zéros de polynômes additifs (3.2.8).

Dans la troisième section, nous regardons le groupe additif du corps L muni de sa structure de module sur l'anneau des endomorphismes définissables dans la structure de corps L : nous commençons par donner une description de l'anneau des endomorphismes définissables (3.3.1) et nous en déduisons, d'une part, l'élimination des quantificateurs pour la structure de module sur le groupe additif (3.3.4) et d'autre part, que tout groupe 1-basé peut être étudié dans cette structure de module (3.3.5). L'élimination des quantificateurs avait été démontré auparavant en utilisant un autre point de vue par P. Dellunde, F. Delon et F. Point [DDP].

Nous commençons ensuite l'étude de la structure induite sur un sous-groupe additif minimal localement modulaire $\bigwedge\!\!\!\bigwedge$-définissable dans les quatrième et cinquième sections. Le théorème 1.3.6 dû à E. Hrushovski [Hr 85] montre l'importance du corps des quasi-endomorphismes dans cette étude, mais dans le cas de groupes d'exposant bornés les travaux de E. Hrushovski et J. Loveys [HL] soulignent les difficultés techniques à décrire la structure induite à partir de ce théorème (voir section 1.4).

Nous nous intéressons aux rapports entre le corps de quasi-endomorphismes et l'anneau des endomorphismes définissables. Nous montrons qu'il existe des sous-groupes additifs minimaux $\bigwedge\!\!\!\bigwedge$-définissables localement modulaires (et d'autres non localement modulaires) dont le corps de quasi-endomorphismes est infini et n'est pas un corps de fractions de l'anneau des endomorphismes définissables qui lui, est fini (3.5.16).

Par ailleurs, nous construisons $2^{\aleph_0}$ sous-groupes minimaux additifs définis sur le vide, deux à deux orthogonaux et $\aleph_0$-catégoriques. La structure induite sur ces groupes est exactement celle d'un $\mathbb{F}_p$-espace vectoriel (3.5.20).

Nous remarquons que l'on peut voir la locale modularité sur le corps de quasi-endomorphismes mais pas sur l'anneau des endomorphismes définissables : tout groupe additif minimal $\bigwedge\!\!\!\bigwedge$-définissable non localement modulaire est isogène à $(L^{p^\infty}, +)$ et donc a même corps de quasi-endomorphismes que celui-ci ; par contre, il existe un groupe additif minimal $\bigwedge\!\!\!\bigwedge$-définissable localement modulaire et un autre non localement modulaire ayant même anneau d'endomorphismes définissables (3.4.24 et 3.5.9).

Les exemples connus de types de L rangés et de rang infini sont des types triviaux [CCSSW]. Dans la dernière section, nous donnons une construction de types additifs de L de rang U égal à ω (3.6.5). Nous montrons ainsi qu'il existe une infinité de sous-groupes additifs de rang U égal à ω dont les types génériques sont deux à deux orthogonaux et parmi lesquels certains sont 1-basés et d'autres non (3.6.6, 3.6.7 et 3.6.8).

3.1 Notations et préliminaires

Dans ce chapitre nous nous plaçons dans un corps séparablement clos de degré d'imperfection fini strictement positif. Un corps est dit séparablement clos s'il n'a pas d'extension algébrique séparable propre (remarque : un corps de caractéristique 0 séparablement clos est algébriquement clos).

La théorie $SCF_{p,\nu}$ des corps séparablement clos de degré d'imperfection $\nu > 0$ est complète [Er 67], stable non superstable [Wo 79].

Pour toute la suite on fixe un corps L séparablement clos de caractéristique $p > 0$ et de degré d'imperfection fini $\nu > 0$ (c'est-à-dire $[L : L^p] = p^\nu$).

Tout au long de cette section, nous fixons les notations que nous utiliserons dans la suite de ce chapitre. Nous commençons par rappeler les résultats généraux de théorie des modèles concernant les corps séparablement clos (paragraphes 3.1.1 et 3.1.2). Pour ces résultats nos références sont [De 88], [Me 94], [Me 96] et [De 98].

E. Bouscaren et F. Delon [BD1] ont montré que tout groupe définissable dans L est définissablement isomorphe au groupe des points L-rationnels d'un groupe algébrique définissable sur L. Nous citons dans le paragraphe 3.1.3 les résultats de leur article qui nous seront utiles. Ensuite, nous énonçons un corollaire 3.1.25 immédiat, sur les sous-groupes minimaux du groupe additif de L, de la description par E. Bouscaren et F. Delon [BD2] des groupes minimaux dans L et du fait que tout type minimal dans L a une géométrie de Zariski (E. Hrushovski puis F. Delon). Enfin nous terminons ces préliminaires par une question ouverte sur la connexité par fini.

3.1.1 p-base et composantes itérées

Pour étudier plus précisément la théorie d'un corps séparablement clos L de degré d'imperfection fini $\nu > 0$, il est pratique d'enrichir le langage en lui ajoutant une p-base. On fixe une **p-base** B et pour $i \in p^\nu$ on note m_i le monôme $\prod_{j\in\nu} b_j^{i(j)}$.

Alors $(m_i : i \in p^\nu)$ forme une base du L^p espace vectoriel L. On note $(x_i : i \in p^\nu)$ les **p-composantes** de x tels que $x = \sum x_i^p m_i$.
On se place dans le langage $\mathcal{L}_{p,\nu} = \{0, 1, +, -, .\} \cup \{b_0, .., b_{\nu-1}\} \cup \{f_i : i \in p^\nu\}$ et on considère dans ce langage la théorie $T_{p,\nu}$, théorie de L dans $\mathcal{L}_{p,\nu}$ où l'on a interprété $f_i(x)$ par x_i. En fait cette théorie est axiomatisée par

$$SCF_{p,\nu} \cup \{B \text{ est une } p\text{-base }\} \cup \{\forall x\ x = \sum_{i\in p^\nu} f_i(x)^p m_i\}.$$

Théorème 3.1.1. *$T_{p,\nu}$ est complète, a l'élimination des quantificateurs, est stable non superstable et a l'élimination des imaginaires.*

Ce théorème découle de la description des types par des idéaux.

On introduit pour cela les notions d'idéaux séparables et de λ-topologie mais auparavant on étend les notations précédentes pour introduire les p-composantes itérées : $f_\emptyset$ est l'identité et $m_\emptyset = 1$ et pour tout $n > 0$ et $i \in (p^\nu)^n$,

$$f_i = f_{i(n-1)} \circ .. \circ f_{i(0)} \text{ et } m_i = m_{i(n-1)}^{p^{n-1}} \dots m_{i(0)}.$$

Alors pour tout entier n et $x \in L$:

$$x = \sum_{i \in (p^\nu)^n} f_i(x)^{p^n} m_i$$

les m_i formant une base du L^{p^n}-espace vectoriel L.

On note $p^\infty := (p^\nu)^{<\omega}$ et pour $x \in L$ on note $x_\infty := (x_i : i \in (p^\nu)^{<\omega})$ la suite des composantes itérées de x définie par $x_i = f_i(x)$.
Pour $n \geq 0$, soit λ_n la bijection de L dans $L^{\times p^{\nu n}}$ définie par $\lambda_n(x) = (x_i)_{i \in p^{\nu n}}$ et pour $x \in L$, $x_{=n} := \lambda_n(x)$ et $x_{\leq n} := (x_{=0}, \ldots, x_{=n})$. On étend de manière naturelle ces notations aux uples.

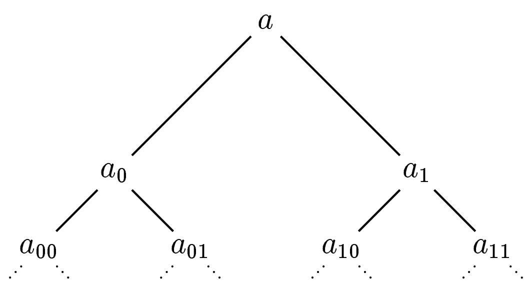
Pour une suite $(a_j)_{j \in J}$ d'éléments de L, on note pour tout $j \in J$ et $i \in p^\infty$, $a_{j,i}$ l'élément $f_i(a_j)$.

Enfin pour $i \in p^\infty$, $j \in p^\infty$ et $a \in L$ on note $a_{i \frown j}$ ou plus simplement a_{ij} l'élément $f_j \circ f_i(a)$.

Remarque 3.1.2. Nous avons considéré ci-dessus p^ν comme ensemble des applications de ν dans p et pour tout n, $p^{\nu n}$ comme ensemble des applications de n dans p^ν. Par la suite dans certaines preuves techniques et certains exemples, il sera pratique de voir ces ensembles comme les entiers correspondants et donc comme ensembles des entiers naturels les précédant. Pour qu'il n'y ait alors pas de confusion il faut choisir l'ordre que l'on met sur p^ν et sur $p^{\nu n}$. Nous choisissons l'ordre lexicographique inverse, c'est à dire pour $i, j \in p^\nu$, $i < j$ s'il existe $l < \nu$ tel que $i(l) < j(l)$ et pour tout $k > l$, $i(k) = j(k)$. Nous faisons de même sur $(p^\nu)^n$ à partir de l'ordre défini sur p^ν. Nous avons choisi cet ordre de telle manière que pour $0 \leq i < p^{\nu n} < p^{\nu m}$, m_i correspond alors au même élément, que l'on considère i comme le $(i+1)$ème élément de $p^{\nu n}$ ou de $p^{\nu m}$. On a par exemple $m_0 = 1$, $m_1 = b_0$ et $m_{p-1} = b_0^{p-1}$ (alors que si l'on avait choisi l'ordre lexicographique classique, m_1 serait égal à $b_{\nu-1}^{p^n}$ pour 1 le second élément de $p^{\nu n}$).

Par contre pour $a \in L$, a_i dépend nécessairement de la hauteur où se trouve i. On utilisera donc quand k est un entier fixé la notation "abusive" a_k et f_k seulement pour $0 \leq k < p^\nu$. Ainsi $a_0 = f_0(a)$ correspond à la composante en $m_0 = 1$ de a, a_1 correspond lui à la composante en $m_1 = b_0$ et a_{p-1} à la composante en $m_{p-1} = b_0^{p-1}$.

Enfin on utilisera simplement a_{10} pour la composante en m_0 de $a_1 = f_1(a)$, (c'est-à-dire $a_{10} = f_0(f_1(a))$), sachant que 10 ne sera jamais employé pour *dix*. (La notation a_{10} étant plus courte que $a_{1 \frown 0}$.)



Composantes itérées pour $p = 2$ et $\nu = 1$

Définition 3.1.3. Pour $x \in L$ et $n \in \omega$, nous définissons $x_{\bar{0}(n)}$ par récurrence de la manière suivante : $x_{\bar{0}(0)} = x$ et $x_{\bar{0}(n+1)} = f_0(x_{\bar{0}(n)}) = x_{\bar{0}(n)0}$. Nous définissons $x_{\bar{1}(n)}$ de façon identique à l'aide de f_1 au lieu de f_0.

Par la suite quand aucune confusion n'est possible, on ne fait pas de différence dans les notations entre les éléments et les uples d'éléments.

Enfin s'il n'y a pas d'autre précision L est toujours considéré comme $\mathcal{L}_{p,\nu}$-structure.

Fait 3.1.4. *Soit $A \subset L$.*
- $\mathbb{F}_p(B, f_i(A); i \in p^\infty)^{sep}$*, la clôture séparable de* $\mathbb{F}_p(B, f_i(A); i \in p^\infty))$*, est un modèle premier au-dessus de A.*
- *La clôture définissable de A est $\mathbb{F}_p(B, f_i(A); i \in p^\infty)$.*
- *Par élimination des imaginaires tout ensemble définissable sur $acl^{eq}(A)$ est définissable sur $\mathbb{F}_p(B, f_i(A); i \in p^\infty)^{sep}$.*

Définition 3.1.5. Soit K un sous-corps définissablement clos de L.

Le **rang de transcendance** noté RT d'un ensemble infiniment définissable Δ sur K est égal au maximum des degrés de transcendance de $K(x_\infty)$ sur K pour $x \in \Delta$. On note $K\!<\!x\!>:= K(x_\infty)^{sep}$ le modèle premier au-dessus de $K \cup \{x\}$ et donc $\mathrm{RT}(\Delta) = \sup_{x\in\Delta} \deg tr(K\!<\!x\!>/K)$.

Le corps $L^{p^\infty} := \cap_{n\in\omega} L^{p^n}$ est l'unique sous-corps algébriquement clos maximal de L. Il est minimal de rang de transcendance 1 et c'est un pur corps algébriquement clos au sens suivant :

Fait 3.1.6. *Soit K un sous-corps définissablement clos de L.*

Soit k un entier et D une partie de $L^{\times k}$ définissable sur K. Alors $D \cap (L^{p^\infty})^{\times k}$ est définissable dans le pur corps L^{p^∞} sur K^{p^∞}.

3.1.2 Idéaux séparables

On rappelle un résultat général sur les corps de définition des idéaux qui sera utile par la suite :

Définition. Soit F un corps et $F[X_i : i \in J]$ un anneau de polynômes sur F. On dit que $C \subseteq F$ est un **corps de définition** d'un idéal I de $F[X_i : i \in J]$, si cet idéal I est engendré par des polynômes sur C.

Fait 3.1.7. *[L 58] Tout idéal $I \in F[X_i : i \in J]$ a un plus petit corps de définition $C(I)$ qui de plus vérifie la propriété suivante : pour tout automorphisme σ du corps F, σ laisse globalement invariant I si et seulement si σ fixe point par point $C(I)$.*

On fixe maintenant un sous-corps K de L, définissablement clos (c'est-à-dire clos par les f_i et contenant $\mathbb{F}_p(B)$).

Notation 3.1.8. Soit $K[X_\infty] := K[X_i; i \in p^\infty]$ l'anneau des polynômes sur K à une infinité d'indéterminées indexées par p^∞. Pour un k-uple d'indéterminées $X = (X_1, \dots, X_k)$, on note de même $K[X_\infty]$ l'anneau $K[X_{1,\infty}, \dots, X_{k,\infty}]$.
Pour $n \in \omega$, soient

$$K[X_{\leq n}] := K[X_i; i \in (p^\nu)^{\leq n}] \text{ et } K[X_{=n}] := K[X_i; i \in (p^\nu)^n]$$

et pour I un idéal de $K[X_\infty]$ soient

$$I_{\leq n} := I \cap K[X_{\leq n}] \text{ et } I_{=n} := I \cap K[X_{=n}].$$

Pour une indéterminée X on note I^0 l'idéal de $K[X_\infty]$ engendré par les polynômes $X_i - \sum_{j \in p^\nu} X^p_{i\frown j} m_j$ pour $i \in p^\infty$. Pour $X = (X_1, .., X_k)$ un uple d'indéterminées, s'il n'y a pas de risque de confusion, on note aussi I^0 l'idéal de $K[X_\infty]$ engendré par les idéaux $I^0(X_i)$ de $K[X_{i,\infty}]$.
Pour décrire le type de $x \in L$ sur K on va simplement considérer l'idéal associé

$$I(x, K) := \{P \in K[X_\infty]; P(x_\infty) = 0\}.$$

Notation 3.1.9. Pour q un type complet sur K on note $I(q)$ l'idéal $I(a, K)$ pour a réalisant q.

Pour tout $n \in \omega$ et a réalisant q, on note

$$q_n := \{P(x_{\leq n}) = 0, Q(x_{\leq n}) \neq 0;\ P, Q \in K[X_{\leq n}],\ P(a_{\leq n}) = 0,\ Q(a_{\leq n}) \neq 0\}.$$

Par élimination des quantificateurs q sera égal à la conjonction des q_n.

Définition. Un idéal I d'une K-algèbre C est **séparable** si pour tous $P_i \in C$, $i \in p^\nu$, tels que $\sum_{i \in p^\nu} P_i^p m_i \in I$ alors $P_i \in I$ pour tout $i \in p^\nu$.

La proposition qui suit démontre l'élimination des quantificateurs et la stabilité de $T_{p,\nu}$:

Proposition 3.1.10. *Supposons L $|K|^+$-saturé.*
L'application qui à $x \in L^{\times k}$ associe $I(x, K)$ définit une bijection entre les k-types sur K et les idéaux premiers séparables de $K[X_\infty]$ contenant I^0.

Remarque. La preuve se fait en deux temps. Tout d'abord on suppose que K est séparablement clos (c'est-à-dire $K \models T_{p,\nu}$). Ensuite avec le fait 3.1.7, on peut montrer un lemme (voir [De 88] lemme 32) qui permet de montrer la surjectivité de l'application dans le cas général. En fait pour un idéal I premier séparable de $K[X_\infty]$ il existe P premier séparable (par exemple $P = I \otimes_K K^{sep}$) de $K^{sep}[X_\infty]$ tel que $I = P \cap K[X_\infty]$.

Remarque 3.1.11. i) I^0 est séparable et $I^0 = I(g, K)$ où g réalise l'unique générique du groupe additif L au dessus de K qui est aussi l'unique générique du groupe multiplicatif de L (cf. [Po 87]).

ii) Pour tout polynôme $P \in K[X_\infty]$, il existe des polynômes $P_i \in K[X_\infty]$ uniques modulo I^0 tels que $P \equiv \sum_{i\in p^\nu} P_i^p m_i$ modulo I^0.

iii) Soit I un idéal de $K[X_\infty]$ contenant I^0 alors I est séparable si et seulement si $I \otimes_K L$ est un idéal séparable de $L[X_\infty]$.

$\triangleright$ Nous montrons seulement l'implication du iii). (La réciproque du iii) est immédiate et n'utilise pas le fait que I contient I^0.)

Supposons I séparable. Soit $\sum_{i\in p^\nu} P_i^p m_i \in I \otimes_K L$. Donc

$$\sum_{i\in p^\nu} P_i^p m_i = R_1Q_1 + \ldots + R_nQ_n \text{ avec } R_j \in L[X_\infty] \text{ et } Q_j \in I.$$

Avec le ii) et la séparabilité de I, il existe pour tout j des polynômes $R_{j,i} \in L[X_\infty]$ et $Q_{j,i} \in I$ tels que

$$R_jQ_j \equiv \left(\sum_{i\in p^\nu} R_{j,i}^p m_i\right)\left(\sum_{i\in p^\nu} Q_{j,i}^p m_i\right) \quad (mod\ I^0 \otimes_K L).$$

D'où

$$P_i \equiv \sum_j \sum_{l+k\equiv i(p)} (m_l m_k m_i^{-1})^{1/p} R_{j,l} Q_{j,k} \quad (mod\ I^0 \otimes_K L)$$

et $P_i \in I \otimes_K L$ si $I \supseteq I^0$. $\triangleleft$

λ-topologie

Définition. Pour un ensemble de polynômes $S \subseteq K[X_\infty]$ on définit un **λ-fermé** :

$$V(S) := \{x \in L^{\times k}; S(x_\infty) = 0\}.$$

La **λ-topologie (définie sur K)** de $L^{\times k}$ est définie par l'ensemble des λ-fermés $V(S)$ avec $S \subseteq K[X_\infty]$.

Si $S \subseteq K[X_{=n}]$, $V(S)$ est par définition un **λ_n-fermé**. La λ-topologie est la limite des λ_n-topologies noethériennes.

A une partie A de $L^{\times k}$, on associe l'idéal

$$I(A, K) := \{P \in K[X_\infty]; P(a_\infty) = 0 \text{ pour tout } a \in A\}.$$

(Quand K est fixé on écrit tout simplement $I(A)$.)

L'élimination des quantificateurs de $T_{p,\nu}$ se traduit par le fait que tout ensemble définissable sur K est combinaison booléenne finie de λ-fermés définissables sur K, ce qu'on appelle un **λ-constructible**. En fait c'est un **λ_n-constructible** pour un certain n (une combinaison booléenne finie de λ_n-fermés définissables sur K). On dit plus généralement qu'un ensemble est $\bigwedge$-définissable **au niveau** n si c'est une intersection de λ_n-constructibles.

Comme dans tout espace topologique on définit les λ-fermés irréductibles, les composantes irréductibles d'un λ-fermé et la notion de générique topologique. Tout fermé est l'union de ses sous-ensembles fermés irréductibles et si un fermé est union d'un nombre fini de sous-ensembles irréductibles maximaux alors ces sous-ensembles sont toutes les composantes irréductibles de ce fermé.

On dit qu'un type complet q sur K est un générique topologique d'un fermé sur K si $V(I(q))$ est une composante irréductible de ce fermé.

Proposition 3.1.12 ("Nullstellensatz"). *Supposons $K \preccurlyeq L$ et L $\aleph_1$-saturé. (Éventuellement $K = L$; $I(A)$ désigne $I(A, K)$ pour $A \subseteq L^{\times k}$)*

1. *L'application qui à A, une partie de $L^{\times k}$, associe l'idéal $I(A)$ définit une bijection entre les λ-fermés sur K de $L^{\times k}$ et les idéaux séparables contenant I^0 de $K[X_\infty]$. L'application réciproque est l'application qui à I associe $V(I)$.*
2. *Un λ-fermé A est irréductible si et seulement si $I(A)$ est premier.*
3. *Soient $C \subseteq A$ des λ-fermés de $L^{\times k}$. Alors C est une composante irréductible de A si et seulement si $I(C)$ est un idéal premier minimal au dessus de $I(A)$.*

Remarque 3.1.13. Le "Nullstellensatz" est vrai en supposant seulement K définissablement clos.

$\triangleright$ Il faut vérifier le 1. (le 2. et 3. se déduisent de la même manière que dans le cas K séparablement clos).
L'application $A \mapsto I(A, K)$ est toujours injective car pour A λ-fermé, $A = V(I(A, K))$. Pour montrer la surjectivité on utilise la remarque 3.1.11. Soit I un idéal séparable de $K[X_\infty]$ contenant I^0. Alors $I \otimes_K L$ est séparable et contient $I^0 \otimes_K L$. En appliquant le "Nullstellensatz" au-dessus de L on obtient $I(V(I), L) = I \otimes_K L$, d'où $I(V(I), K) = I$. $\triangleleft$

Fait 3.1.14. *Si A est un λ-fermé définissable alors A a un nombre fini de composantes irréductibles.*

En utilisant le "Nullstellensatz" et la notion de corps de définition 3.1.7, on montre l'élimination des imaginaires pour $T_{p,\nu}$ (cf. [De 88], [Me 96] ou [De 98]).

En particulier, avec le "Nullstellensatz" on peut définir la notion de corps de définition d'un λ-fermé A : K est un **corps de définition** de A si K est un corps de définition de $I(A, L)$ (c'est-à-dire $I(A, L) = I(A, K) \otimes_K L$).

On en déduit le résultat suivant :

Corollaire 3.1.15. *Soit A un λ-fermé sur L. (K est toujours supposé définissablement clos.) Les propriétés suivantes sont équivalentes :*

– *A est $\bigwedge$-définissable sur K (au sens de la théorie des modèles).*

– *K est un corps de définition de A.*
– *A est λ-fermé sur K.*

$\triangleright$ Supposons A $\bigwedge\!\!\!\bigwedge$-définissable sur K. On peut supposer L $|K|^+$-saturé. (Il suffit pour cela de se plonger dans une extension élémentaire de L.) Tout automorphisme de la structure L fixant point par point K, fixe globalement A, donc $I(A, L)$ et donc point par point $C(I(A, L))$. Comme K est définissablement clos et L $|K|^+$-saturé, $C(I(A, L)) \subseteq K$ et par conséquent K est un corps de définition de A. Les autres implications sont évidentes. $\triangleleft$

Idéaux séparables et clôture de Zariski dans L

On note $\bar{K}$ et $\bar{L}$ les clôture algébriques de K et L. De même pour $S \subseteq \bar{L}[X]$ on note $\bar{V}(S)$ le fermé de Zariski défini par S dans $\bar{L}^{\times k}$ et pour $A \subseteq \bar{L}^{\times k}$, on note $\bar{I}(A) := \{P \in \bar{L}[X]; P(a) = 0 \text{ pour tout } a \in A\}$. On note $\bar{A}$ la clôture de Zariski de $A \subseteq L^{\times k}$ dans $\bar{L}^{\times k}$.

Si A est un λ_0-fermé on a évidemment $\bar{A} = \bar{V}(I(A)_{=0})$.

Remarque. Les corps K et L n'étant pas algébriquement clos, les notions de définissable au sens de la théorie des modèle et de définissables au sens de la géométrie algébrique sont distinctes. Quand nous parlerons de fermés de Zariski ou de variétés définies sur K (ou sur L), ce sera toujours au sens de la géométrie algébrique.

Fait 3.1.16. – *Un idéal I premier séparable de $L[X]$ est absolument premier (c'est-à-dire $I \otimes_L \bar{L}$ est un idéal premier de $\bar{L}[X]$).*
– *Si V est une variété irréductible de $\bar{L}$ définie sur L alors $V(L)$ est Zariski dense dans V.*
– *Un idéal I séparable de $L[X]$ est absolument réduit c'est-à-dire si $I_1, \ldots, I_n$ sont les idéaux premiers minimaux de $L[X]$ contenant I, alors dans $\bar{L}[X]$, les idéaux premiers minimaux contenant $I \otimes_L \bar{L}$ sont exactement les $I_1 \otimes_L \bar{L}, \ldots, I_n \otimes_L \bar{L}$.*

3.1.3 Groupes définissables

Nous citons maintenant quatre résultats utiles pour la suite que l'on trouve dans [BD1]. Nous supposons ici que K est une sous-structure élémentaire de L (c'est à dire K est séparablement clos).

Proposition 3.1.17. *[BD1] Soit G un groupe $\bigwedge\!\!\!\bigwedge$-définissable sur K dans L avec une multiplication rationnelle (c'est-à-dire pour tout a, b de G, $a \cdot b \in K(a, b)$). Alors si q est un type générique de G (au sens du groupe) alors $I(q, K)$ est minimal parmi les $I(r, K)$ pour r parcourant les types complets sur K dans G.*

Proposition 3.1.18. *[BD1] Soit H un sous-groupe définissable sur K d'un groupe G λ_0-fermé sur K à multiplication rationnelle. Si H est λ_n-constructible alors H est λ_n-fermé.*

Proposition 3.1.19. *[Hr 96] ou [BD1] Soit G un groupe algébrique connexe défini sur K. Alors $G(L)$, comme groupe définissable dans L, est connexe.*

Proposition 3.1.20. *[BD1] Tout groupe G définissable sur K dans L est connexe par fini. La composante connexe de G est donc d'indice fini dans G et définissable sur K.*

Remarque 3.1.21. En particulier tout sous-groupe définissable de $(L, +)$ sur K est λ-fermé et connexe par fini. De plus, dans ces groupes, la notion de générique topologique coïncide avec celle de générique de groupes.

Enfin E. Bouscaren et F. Delon ont montré que l'étude des sous-groupes commutatifs définissables d'exposant p se ramène à l'étude des sous-groupes définissables du groupe additif :

Proposition 3.1.22. *[BD2] Soit G un groupe commutatif d'exposant p et $\bigwedge$-définissable sur K. Alors G est définissablement isomorphe à un sous-groupe λ-fermé de $(L, +)$.*

Par la suite nous appellerons un sous-groupe de $(L, +)$, **sous-groupe additif**.

3.1.4 Groupes minimaux

E. Bouscaren et F. Delon donnent la description suivante des groupes minimaux dans un corps séparablement clos.

Proposition 3.1.23. *[BD2] Soit G un groupe $\bigwedge$-définissable minimal dans L.*

1. Si G est non-orthogonal à L^{p^∞}, alors G est définissablement isogène à un groupe algébrique de dimension 1 défini sur L^{p^∞}. Plus précisément :
- *soit G est définissablement isomorphe à $((L^{p^\infty})^*, \cdot)$,*
- *soit G est définissablement isomorphe à $A(L^{p^\infty})$ pour A une courbe elliptique définie sur L^{p^∞},*
- *soit G est définissablement isogène à $(L^{p^\infty}, +)$.*

2. Si G est orthogonal à L^{p^∞}, alors
- *soit G est divisible et G est définissablement isomorphe à $p^\infty A(L) := \cap_{n\in\omega} p^n A(L)$ pour A une variété abélienne simple définie sur L,*
- *soit G est d'exposant p et est définissablement isomorphe à un sous-groupe λ-fermé de $(L, +)$.*

Cette description des groupes minimaux sépare les groupes localement modulaires de ceux non localement modulaires car tout type minimal de L est soit non orthogonal à L^{p^∞} et donc non localement modulaire, soit localement modulaire. Ceci vient des résultats suivants : d'une part E. Hrushovski [Hr 96] a montré que les types minimaux dans L qui sont minces (c'est-à-dire de rang de transcendance fini) ont une géométrie de Zariski et ensuite F. Delon [De 98] a montré ce résultat pour tous les types minimaux de L. D'autre part tout type minimal ayant une géométrie de Zariski est soit localement modulaire, soit non-orthogonal à un corps minimal $\bigwedge$-définissable [HZ 96] ou [Ma 98]. Enfin à isomorphisme définissable près L^{p^∞} est l'unique corps minimal $\bigwedge$-définissable de L [Me 94, Hr 96].

Donc :

Fait 3.1.24. *[BD2] Un type minimal de L est soit localement modulaire, soit non orthogonal à L^{p^∞}.*

Nous utiliserons par la suite le corollaire de (3.1.24) et (3.1.23) pour les sous-groupes minimaux additifs :

Corollaire 3.1.25. *[BD2] Soit G un sous-groupe de $(L, +)$ $\bigwedge$-définissable minimal dans L. Les propriétés suivantes sont équivalentes :*
- G est non localement modulaire
- G est non orthogonal à L^{p^∞}
- G est définissablement isogène à $(L^{p^\infty}, +)$.

Remarque. [BD2] Il existe des sous-groupes minimaux de $(L, +)$ définissablement isogènes mais non définissablement isomorphes à $(L^{p^\infty}, +)$.

3.1.5 Composante connexe

E. Bouscaren et F. Delon ont montré que tout groupe définissable dans L est connexe par fini [BD1]. Ce n'est pas le cas des groupes $\bigwedge$-définissables. Voici un contre exemple dans le groupe multiplicatif de L qui est même de rang U égal à 1 :

Exemple 3.1.26. Soit $b := b_0$ le premier élément de la p-base. Soit pour tout entier n, $G_n := \cup_{i<p^n}(b^i(L^{p^n})^*, \cdot)$. Soit $G := \cap_n G_n$. Alors pour tout n, $G_n^0 = ((L^{p^n})^*, \cdot)$ et donc $G^0 = ((L^{p^\infty})^*, \cdot)$.

Voici une construction de contre-exemples dans le groupe additif de L :

Construction 3.1.27. Soit $(G_n)_{n\in\omega}$ une suite strictement décroissante de sous-groupes additifs de $(L, +)$ définissables et connexes. Pour tout $n \in \omega$, soit $a_n \in G_n \setminus G_{n+1}$. Soit pour tout $n \in \omega$, H_n le sous-groupe de $(L, +)$ engendré par G_{n+1} et $a_0, \dots, a_n$. Alors H_n est une suite strictement décroissante. Soit H l'intersection de cette suite. La composante connexe de H est l'intersection des G_n et est donc d'indice infini dans H.

Se pose alors la question suivante : dans un groupe connexe $\bigwedge$-définissable de L, les groupes relativement définissables sont-ils tous connexes par fini ? E. Hrushovski a répondu positivement à cette question pour les groupes $\cap_n p^n A(L)$ où A est une variété abélienne définie sur L. Les groupes utilisés dans la preuve de Mordell-Lang due à E. Hrushovski [Hr 96] sont les groupes $\cap_n p^n A(L)$ où A est une variété semi-abélienne définie sur L et E. Bouscaren et F. Delon [BD2] ont montré qu'un groupe $\bigwedge$-définissable de L commutatif et divisible est définissablement isomorphe à un tel groupe.

Par contre parmi les sous-groupes additifs la réponse est négative. Voici un contre-exemple dû à F. Delon :

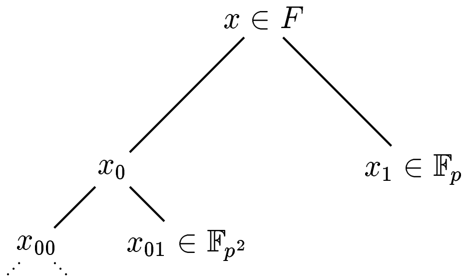
Exemple 3.1.28. Nous utilisons la remarque sur les notations 3.1.2 et la définition 3.1.3. Soit b le premier élément de la p-base. Soit le sous-groupe de $(L, +)$

$$F := \{x \in L;\ x_{\bar{0}(n)} = x^p_{\bar{0}(n+1)} + b x^p_{\bar{0}(n)1} \text{ et } x_{\bar{0}(n)1} \in L^{p^\infty}, \text{ pour tout } n\}.$$

Soit

$$G := \{(x, y) \in F \times F;\ y_{\bar{0}(n)1} = x^{p^{n+1}}_{\bar{0}(n)1} - x_{\bar{0}(n)1}, \text{ pour tout } n\}.$$

Alors G est un groupe connexe non rangé par le rang U car il contient une suite strictement décroissante de groupes connexes. Soit le sous-groupe relativement définissable de G, $H := G \cap (L \times \{0\})$. La composante connexe de H est $L^{p^\infty} \times \{0\}$ et est donc d'indice infini dans H. Le groupe H est de rang U un.



Groupe H

On peut aussi dans la construction précédente ne pas utiliser le groupe F et remplacer G par

$$G' := \{(x, y) \in L \times L;\ y_{\bar{0}(n)1} = x^p_{\bar{0}(n)1} - x_{\bar{0}(n)1},\ \text{pour tout } n\}.$$

Remarque. Les groupes commutatifs divisibles sont minces donc de rang U fini. Par contre le contre-exemple (3.1.28) dans le cas additif n'est pas rangé. Il reste donc la question ouverte suivante : dans un groupe connexe $\bigwedge$-définissable et mince (ou seulement de rang U fini, ou rangé par le rang U) de L, les groupes relativement définissables sont-ils tous connexes par fini ?

3.2 Sous-groupes additifs et p-polynômes

Dans toute cette partie L est un modèle fixé de $T_{p,\nu}$ et K est un sous-corps de L définissablement clos.

Nous montrons que tout sous-groupe de $(L^{\times k}, +)$ définissable sur K est défini pour un entier n par des p-polynômes de $K[X_{=n}]$ (3.2.3).

Nous en déduisons que pour tout sous-groupe G de $(L^{\times k}, +)$ $\bigwedge$-définissable sur K, $I(G)$ est engendré par des p-polynômes de $K[X_\infty]$ (3.2.8).

Commençons par remarquer qu'un sous-groupe additif λ_n-fermé λ_n-irréductible est connexe :

Lemme 3.2.1. *Supposons K séparablement clos.*

Soit G un sous-groupe de $(L^{\times k}, +)$ et I un idéal premier séparable de $K[X_{\leq n}]$ ou de $K[X_\infty]$ tel que $G = V(I)$. Alors G est connexe.

$\triangleright$ Si I est un idéal de $K[X_\infty]$ alors G est l'intersection des groupes $G_m := V(I_{\leq m})$ et les $I_{\leq m}$ sont alors premier séparable. De plus par stabilité si chacun des groupes G_m est connexe alors G aussi. (Ce résultat est aussi une conséquence directe du fait que dans G, un générique topologique est un générique de groupes et réciproquement (3.1.21).)

Il suffit donc de montrer le résultat pour I idéal de $K[X_{\leq n}]$. On peut supposer $n=0$ en remplaçant G par $\lambda_n(G)$.

Soit $H=\bar{V}(I)$. Comme I est absolument premier (3.1.16), H est un fermé irréductible dans le corps algébriquement clos $\bar{L}$. Donc H est connexe. De plus $G=H(L)$ et H est un groupe algébrique, donc G est connexe par (3.1.19). ◁

Remarque. L'argument H est un groupe algébrique est essentiel dans la preuve précédente. En effet E. Bouscaren et F. Delon [BD1] ont donné un exemple de groupe dans L, λ_0-fermé irréductible mais non connexe.

Définition. Soit F un corps de caractéristique p.

Soit P un polynôme de $F[X_i;\ i\in I]$. On dit que P est un **p-polynôme** s'il est somme de monômes de la forme $a_{i,j}X_i^{p^j}$. Dans ce cas P est un **polynôme additif** c'est-à-dire $P((a_1+b_1),\dots,(a_k+b_k))=P(a_1,\dots,a_k)+P(b_1,\dots,b_k)$ pour tout $a_i,b_i\in F$.

On trouve dans [Hu 87] (chapitre VII 20) les résultats classiques suivants :

Fait 3.2.2. *Soit F algébriquement clos.*

i) Si $P\in F[(X_1,\dots,X_k]$ est un polynôme additif sur $F^{\times k}$ alors P est un p-polynôme.

ii) Si $P\in F[(X_1,\dots,X_k]$ est sans facteur carré et si l'ensemble des zéros de P est un sous-groupe de $(F^{\times k},+)$ alors P est un p-polynôme.

iii) Si G est un sous-groupe fermé connexe de $(F^{\times k},+)$ alors il existe un automorphisme ϕ de $(F^{\times k},+)$ défini par des p-polynômes tel que $\phi(G)$ est un sous-groupe vectoriel de $(F^{\times k},+)$. Ainsi G est une intersection des noyaux de p-polynômes.

iv) Si G est un sous-groupe fermé de $(F^{\times k},+)$ alors G est une intersection des noyaux de p-polynômes (exercice 7).

Nous allons en déduire la proposition suivante dans le cadre séparablement clos :

Proposition 3.2.3. *Si G est un sous-groupe définissable sur K de $(L^{\times k},+)$ alors il existe des p-polynômes $P_0,\dots,P_l$ de $K[X_\infty]$ tel que $G=V(\{P_0,\dots,P_l\})$.*

Remarque. Quand on a $G=V(\{P_0,\dots,P_l\})$ alors $G=V(\{Q\})$ pour $Q=\sum_i P_i^{p^n}m_i$ tel que $p^{\nu n}\geq l+1$.

Pour la preuve de 3.2.3 on peut supposer que L est $|K|^+$-saturé (il suffit pour cela de se placer dans une extension élémentaire suffisamment saturée de L).

On décompose la preuve de cette proposition en trois lemmes :

Lemme 3.2.4. *La proposition est vraie pour G fini.*

▷ Soient G un sous-groupe fini de $(L^{\times k},+)$ et n un entier tel que $p^{\nu n}\geq k$.

Soit $H=\lambda_n^{-1}(G\times\{0\}^{p^{\nu n}-k})$. Alors H est un sous-groupe fini de $(L,+)$ définissable sur K.

Soit $P(X)=\prod_{h\in H}(X-h)$. Comme H est définissable sur K et K est définissablement clos, les racines de P sont globalement fixé par tout automorphisme de L fixant K. Donc P est un polynôme de $K[X]$. En appliquant le deuxième point du fait 3.2.2 on en déduit que P est un p-polynôme. Soit $Q(X_0,\dots,X_{k-1}):=P(X_0^{p^n}m_0+\dots+X_{k-1}^{p^n}m_{k-1})$. Alors Q est un p-polynôme de $K[X_0,\dots,X_{k-1}]$ et $G=V(Q)$. (Ici on utilise la notation décrite dans (3.1.2).) ◁

Lemme 3.2.5. *Supposons $K \preccurlyeq L$.*

Soit G un sous-groupe λ_0-fermé sur K de $(L^{\times k}, +)$. Alors il existe des p-polynômes $P_1, \ldots, P_l$ de $K[X]$ tels que $G = V(\{P_1, \ldots, P_l\})$.

▷ Soit $\bar{G}$ la clôture de Zariski de G dans $\bar{L}^{\times k}$. Par (3.2.2 iv) il existe des p-polynômes $P_1, \ldots, P_l$ de $\bar{K}[X]$ tels que $\bar{G} = \bar{V}(\{P_1, \ldots, P_l\})$ (X est un k-uple). En élevant les P_i à une puissance p^m suffisante, on peut les supposer à coefficient dans K. D'où $G = \bar{G}(L) = V(\{P_1, \ldots, P_l\})$ (3.1.16). ◁

Lemme 3.2.6. *Supposons K seulement définissablement clos.*

Soit G un sous-groupe connexe λ_0-fermé sur K de $(L^{\times k}, +)$. Alors il existe des p-polynômes $P_1, \ldots, P_n$ de $K[\bar{X}]$ tels que $G = V(\{P_1, \ldots, P_n\})$.

De plus si g est un générique de G au-dessus de K tel que $g := (\bar{x}, y_1, \ldots, y_n)$ où $\bar{x}$ est une base de transcendance séparante de $K(g)$ au dessus de K, alors nous pouvons choisir les polynômes $P_1, \ldots, P_n$ tels que pour tout $i \in \{1, \ldots, n\}$, $P_i \in K[\bar{X}, Y_1, \ldots, Y_i]$, P_i est unitaire et de degré minimal en Y_i, parmi les p-polynômes de $K^{sep}[\bar{X}, Y_1, \ldots, Y_i]$ de degré > 0 en Y_i et s'annulant en g, et pour tout $j < i$ $\deg_{Y_j}(P_i) < \deg_{Y_j}(P_j)$. Les polynômes P_i sont les uniques polynômes vérifiant les propriétés ci-dessus.

▷ Soit g réalisant le générique de G au-dessus de K (qui est stationnaire).

On peut supposer que $g := (\bar{x}, \bar{y})$ tel que $\bar{x}$ est une base de transcendance séparante de $K(g)$ au dessus de K. Soit $m = l(\bar{x})$ et $n = l(\bar{y})$. ($k = m + n$).

Soit $\bar{G}$ la clôture de Zariski de G dans $\bar{L}^{\times k}$.

Par (3.1.16) g réalise le générique de $\bar{G}$ au-dessus de $\bar{K}$. Soit pour tout $i \in \{1, \ldots, n\}$, $g_i = (\bar{x}, y_1, \ldots, y_i)$ et $\bar{G}_i$ la projection de $\bar{G}$ sur $\bar{L}^{\times(m+i)}$.

Chaque g_i réalise donc le générique de $\bar{G}_i$. Par (3.2.2 iii), pour tout i, il existe un p-polynôme dans $\bar{K}[\bar{X}, Y_1, \ldots, Y_i]$ de degré ≥ 1 en Y_i s'annulant en g_i. On peut supposer ces p-polynômes à coefficient dans K^{sep} en les élevant à une puissance p^m suffisante.

On construit par récurrence sur i des p-polynômes $P_i \in K^{sep}[\bar{X}, Y_1, \ldots, Y_i]$ tels que $P_i(g_i) = 0$, P_i est unitaire et de degré minimal p^{n_i} en Y_i et tels que $\deg_{Y_j}(P_i) < \deg_{Y_j}(P_j)$ pour tout $j < i$.

Supposons que pour $i \leq n$, $P_1, \ldots, P_i$ sont définis. D'après ce qui précède, on peut choisir un p-polynôme $P'_{i+1} \in K^{sep}[\bar{X}, Y_1, \ldots, Y_{i+1}]$ unitaire, de degré minimal $p^{n_{i+1}}$ en Y_{i+1} tel que $P'_{i+1}(g_{i+1}) = 0$. Si $i = 0$ on prend $P_1 = P'_1$. Sinon, on abaisse successivement le degré en Y_i, puis en $Y_{i-1}, \ldots$, jusqu'en Y_1 tels que $\deg_{Y_j}(P_i) < \deg_{Y_j}(P_j)$ pour tout $j < i$. On utilise pour cela la technique suivante : si on a $P(X)$ un p-polynôme unitaire de degré p^m et $Q(X)$ un p-polynôme de degré $p^{m'}$ tel que $m' > m$ alors il existe un p-polynôme $Q'(X)$ tel que $\deg(Q') < \deg(Q)$ et tel que Q' et Q sont congrus modulo P. On remplace simplement dans Q, $X^{p^{m'}}$ par $(X^{p^m} - P(X))^{p^{m'-m}}$.

Après ces opérations on obtient un p-polynôme P_{i+1} vérifiant toutes les bonnes propriétés.

On a en fait construit ces polynômes P_i de telle manière qu'ils soient à coefficients dans K. En effet comme $\mathrm{tp}(g/K)$ est stationnaire, tout automorphisme σ de L fixant K point par point laisse fixe les P_i : soit $i \in \{1, \ldots, n\}$, comme P_i est unitaire en Y_i, on a $\sigma(P_i) - P_i$ de degré strictement plus petit en Y_i que P_i, il est donc nul en Y_i ; puis en utilisant les hypothèses $\deg_{Y_j}(P_i) < \deg_{Y_j}(P_j)$ pour tout $j < i$, on en déduit qu'il est nul en $Y_{i-1}, \ldots$, en Y_1 ; enfin comme $\bar{x}$ est transcendant, il est nul. Pour la même raison les polynômes P_i sont uniques.

Montrons maintenant que $G = V(\{P_1, \ldots, P_n\})$.

Par (3.2.5) il suffit de vérifier que pour tout Q p-polynôme de $K^{sep}[\bar{X}, \bar{Y}]$ tel que $Q(g) = 0$ alors $Q \in < P_1, \ldots, P_n >$.

Soit Q un p-polynôme. En utilisant la même méthode que pour la construction successive des P_i, on a $Q(\bar{X}, \bar{Y}) \equiv Q_0(\bar{X}) + Q_1(Y_1) + \ldots + Q_n(Y_n) \pmod{P_1, \ldots, P_n}$ avec $\deg(Q_i) < \deg_{Y_i}(P_i)$.

On en déduit que si $Q(g) = 0$ alors $Q_n = 0, \ldots, Q_1 = 0$, et $Q_0 = 0$. D'où $Q \in < P_1, \ldots, P_n >$. $\triangleleft$

$\triangleright$ **Preuve de la proposition 3.2.3**

Soit G un sous-groupe définissable sur K de $(L^{\times k}, +)$. Soit G^0 sa composante connexe. Alors G^0 est un sous-groupe définissable sur K et d'indice fini dans G (3.1.20). Par (3.1.18) et (3.1.15) les groupes G et G^0 sont des λ-fermés sur K. Pour un certain n, $H := \lambda_n(G)$ et $H^0 = \lambda_n(G^0)$ sont λ_0-fermés sur K.

Par (3.2.6) il existe $P_1, \ldots, P_l$ des p-polynômes de $K[X]$ (où X est un $k \cdot p^{\nu n}$-uple de variables) tels que $H^0 = V(\{P_1, \ldots, P_l\})$.

Soit ϕ le morphisme de $L^{\times k \cdot p^{\nu n}}$ dans $L^{\times l}$ qui à x associe $(P_1(x), \ldots, P_l(x))$. Alors $H^0 = \ker \phi$ et donc $\phi(H)$ est un sous-groupe fini de $(L^{\times l}, +)$ définissable sur K car H^0 est d'indice fini dans H. Il existe donc un polynôme Q dans $K[Y]$ tel que $\phi(H) = V(\{Q\})$ (3.2.4).

De plus $H = \phi^{-1}(\phi(H))$ car $\ker \phi \subseteq H$.

D'où $H = V(\{R\})$ avec $R(X) = Q(P_1(X), \ldots, P_l(X))$.

Soit Z un k-uple de variables. Alors $G = V(\{R(Z_{=n})\}$ car $G = \lambda_n^{-1}(H)$. $\triangleleft$

Avec le lemme suivant on montre que l'idéal séparable correspondant au groupe G est en fait engendré par des p-polynômes.

Lemme 3.2.7. *Soit $S \subseteq K[X_\infty]$. Si S est un ensemble de p-polynômes alors $I(V(S), K)$ est engendré par des p-polynômes.*

$\triangleright$ Soit P un polynôme de $K[X_{=n}]$. Il existe des $P_i \in K[X_{=n+1}]$ uniques tels que

$$P \equiv \sum_{i \in p^\nu} P_i^p m_i \ (\bmod\ I^0).$$

Il est simple de voir que si P est un p-polynôme les P_i aussi.

On peut donc supposer S clos par ce procédé. C'est à dire si $P \in S$ il existe $P_i \in S$ tel que $P \equiv \sum_{i \in p^\nu} P_i^p m_i$ (mod I^0).

L'idéal $I =< S \cup I^0 >$ est alors séparable.

En effet si $\sum_{i \in p^\nu} Q_i^p m_i \in I$ alors modulo I^0 cette somme est égale à une somme de termes $a \cdot P$ où $P \in S$ et $a \in K[X_\infty]$. On a

$$a \cdot P \equiv (\sum_{i \in p^\nu} a_i^p m_i) \cdot (\sum_{i \in p^\nu} P_i^p m_i)$$

avec les $P_i \in S$.

On en déduit qu'il existe des $b_{i,j} \in K[X_\infty]$ tels que

$$a \cdot P \equiv \sum_{i \in p^\nu} \left(\sum_{j \in p^\nu} b_{i,j} \cdot P_j \right)^p m_i.$$

Et donc chaque Q_i est dans $< S \cup I^0 >$.

Alors $I(V(S)) = I$ ("Nullstellensatz" 3.1.12 et 3.1.13). $\lhd$

Remarque. Cette preuve ne montre pas que pour tout ensemble S de p-polynômes dans $K[X_{=n}]$, l'idéal $I(V(S), K)_{\leq n}$ est engendré par des p-polynômes.

Proposition 3.2.8. *Si G est un sous-groupe $\bigwedge\!\!\!\bigwedge$-définissable sur K de $(L^{\times k}, +)$ alors $I(G)$ est engendré par des p-polynômes de $K[X_\infty]$.*

$\rhd$ Par stabilité le groupe G est l'intersection de sous-groupes définissables sur K de $(L^{\times k}, +)$. On applique la proposition 3.2.3 à ces groupes et on en déduit qu'il existe $S \subseteq K[X_\infty]$ ensemble de p-polynômes tel que $G = V(S)$. On termine en appliquant le lemme 3.2.7. $\lhd$

3.3 Structure de module d'un corps séparablement clos

Nous fixons toujours L un modèle de $T_{p,\nu}$ et K un sous-corps définissablement clos de L. De plus nous supposons L $|K|^+$-saturé.

P. Dellunde, F. Delon et F. Point [DDP] ont étudié la théorie de module des corps séparablement clos sur l'anneau des endomorphismes $\mathbb{F}_p(B)\{\alpha\}$ engendré par $\mathbb{F}_p(B)$ et le Frobénius α. Les auteurs ont axiomatisé cette théorie, montré qu'elle est complète et qu'elle admet l'élimination des quantificateurs dans le langage enrichi par des fonctions additives qui sont l'analogue des fonctions f_i du langage du corps.

Ici nous adoptons un point de vue différent. Nous étudions uniquement la structure de module de $(L, +)$ sur l'anneau $\mathrm{End}_K(L, +)$ de tous les endomorphismes définissables sur K. Même si $K = \mathbb{F}_p(B)$, cet anneau contient strictement $\mathbb{F}_p(B)\{\alpha\}$, par contre le langage enrichi par les fonctions additives [DDP] est alors $\emptyset$-interdéfinissable avec celui que nous considérons.

Nous montrons que l'anneau $\mathrm{End}_K(L, +)$ correspond à l'ensemble des p-polynômes de $K[X_\infty]$ quotienté par I^0 (3.3.1). Ceci nous permet de déduire directement l'élimination des quantificateurs dans ce langage (3.3.4) et de plus de montrer que si K est séparablement clos (c'est-à-dire si K est une sous-structure élémentaire de L), la structure induite d'un sous-groupe additif 1-basé dans la structure de corps L au-dessus de K, est la même que la structure induite dans la structure réduite de module (3.3.5).

3.3.1 Endomorphismes du groupe additif

Nous allons décrire l'anneau $\mathrm{End}_K((L,+))$ des endomorphismes de $(L,+)$ définissables au-dessus de K. Pour cela nous considérons ces endomorphismes comme agissant à gauche sur L.

Cet anneau contient naturellement le Frobenius que l'on note α, les f_i et toutes les homothéties de rapport dans K que nous appellerons ensuite les endomorphismes scalaires. Nous allons montrer qu'il est engendré en fait par ces endomorphismes.

Notons pour l'instant $K\{\alpha,(f_i)_{i\in p^\nu}\}$ le sous-anneau de $\mathrm{End}_K((L,+))$ engendré par les endomorphismes ci-dessus (Frobenius, f_i et homothéties) et $K\{\alpha\}$ le sous-anneau de $K\{\alpha,(f_i)_{i\in p^\nu}\}$ engendré par le Frobenius et les homothéties de rapport dans K. On a évidemment les relations suivantes dans $K\{\alpha,(f_i)_{i\in p^\nu}\}$:

1. $\alpha\cdot a=a^p\cdot\alpha$ pour $a\in K$.
2. $f_i\cdot m_i\cdot\alpha=1$ et $f_i\cdot m_j\cdot\alpha=0$ pour $i,j\in p^\nu, i\neq j$.
3. $f_i\cdot a=\displaystyle\sum_{j,l\in p^\nu;\ l+j\equiv i\ (p)} a_l\cdot\left(m_lm_jm_i^{-1}\right)^{1/p}\cdot f_j$ pour $i\in p^\nu$ et $a\in K$.
4. $\displaystyle\sum_{i\in p^\nu} m_i\cdot\alpha\cdot f_i=1$.

Avec ces relations on peut montrer simplement par induction que tout élément de $K\{\alpha,(f_i)_{i\in p^\nu}\}$ s'écrit pour tout n assez grand sous la forme

$$\sum_{i\in(p^\nu)^n}\left(\sum_j a_{i,j}\cdot\alpha^j\right)\cdot f_i.$$

Nous avons donc les relations suivantes :

5. pour tout $r\in K\{\alpha,(f_i)_{i\in p^\nu}\}$ il existe N tel que pour tout $n\geq N$ et $i\in p^{\nu n}$, $r_i=r\cdot m_i\cdot\alpha^n\in K\{\alpha\}$ et $r=\sum_{i\in(p^\nu)^n} r_i\cdot f_i$.

Définition. En utilisant la relation 1, on montre que tout élément $r\in K\{\alpha\}$ s'écrit de manière unique sous la forme $\sum_{j\in\omega}a_j\alpha^j$ où tous les a_j sauf un nombre fini sont nuls. On peut donc lui associer le p-polynôme de $K[X]$,

$$P_r=\sum_{j\in\omega}a_jx^{p^j},$$

ainsi on a $r\cdot x=P_r(x)$ pour tout $x\in L$. Inversement, à un p-polynôme P de $K[X]$ on peut associer l'unique endomorphisme r_P dans $K\{\alpha\}$ tel que $P_{r_P}=P$.

De même à tout p-polynôme $P=\sum_{i\in p^\infty}P_i(X_i)$ de $K[X_\infty]$, on peut associer un endomorphisme r_P de $K\{\alpha,(f_i)_{i\in p^\nu}\}$ défini par

$$r_P=\sum_{i\in p^\infty} r_{P_i}\cdot f_i.$$

Alors évidemment pour tout $x\in L$, $r_P\cdot x=P(x)$.

Le théorème suivant montre que tout élément de $\mathrm{End}_K((L,+))$ s'écrit de manière unique sous la forme r_P pour un P p-polynôme appartenant à $K[X_{=n}]$.

Théorème 3.3.1. *L'anneau des endomorphismes de $(L,+)$ définissables sur K est engendré par les endomorphismes scalaires dans K, les endomorphismes f_i et le Frobénius :*

$$\mathrm{End}_K((L,+)) = K\{\alpha, (f_i)_{i\in p^\nu}\}.$$

Plus précisément

$$\begin{aligned}\mathrm{End}_K((L,+)) &= \cup_{n\in\omega}\{r_P; P \text{ } p\text{-polynôme de } K[X_{=n}]\}\\ &= \{r_P; P \text{ } p\text{-polynôme de } K[X_\infty]\}.\end{aligned}$$

On a l'unicité suivante : si $r_P = r_Q$ pour P et Q des p-polynômes de $K[X_{=n}]$ alors $P = Q$. Plus généralement si $r_P = r_Q$ pour P et Q des p-polynômes de $K[X_\infty]$ alors $P - Q \in I^0$.

Ainsi par la relation 4 pour tout $r \in \mathrm{End}_K((L,+))$, il existe un entier N tel que pour tout $n \geq N$, il existe un unique p-polynôme de $K[X_{=n}]$, que l'on note $P_{r,n}$, qui vérifie $r = r_{P_{r,n}}$.

Enfin l'anneau des endomorphismes du groupe $(L^{\times m},+)$ définissables sur K est l'anneau $\mathcal{M}_{m,m}(\mathrm{End}_K((L,+)))$ des matrices sur $\mathrm{End}_K((L,+))$.

▷ Soit g un endomorphisme de $(L,+)$ définissable sur K. En tant qu'application définissable on sait par compacité qu'il existe un entier n, des ensembles définissables sur K, $D_1,\dots,D_n$, recouvrant L tels que $g_{|D_i} = P_i/Q_i$ où $P_i, Q_i \in K[X_\infty]$ et $Q_i \neq 0$ sur D_i (car pour tout $a \in L$, $\mathrm{dcl}(K \cup \{a\}) = K(a_\infty)$ (3.1.4)). Il existe donc m tel que l'on peut supposer $P_i, Q_i \in K[X_{=m}]$ et D_i défini par $(R_i \neq 0) \wedge (S_i = 0)$ avec R_i et S_i dans $K[X_{=m}]$.

Pour tout $j \in (p^\nu)^m$ on définit $g_j = g \circ m_j \circ \alpha^m$ (c'est-à-dire $g_j(x) = g(m_j.x^{p^m})$).

Comme g est un endomorphisme,

$$g = \sum_{j\in(p^\nu)^m} g_j \circ f_j.$$

Les g_j sont aussi des endomorphismes de $(L,+)$.

Pour tout polynôme T de $K[X_{=m}]$ et tout $j \in (p^\nu)^m$ on définit

$$T^j(X_j) := T(0,.,0,X_j,0,..,0)$$

tel que dans la deuxième expression X_j se trouve à la j-ième place.

Soit D_i^j défini par $(R_i^j \neq 0) \wedge (S_i^j = 0)$, $D_i^j := D_i \cap (0 \times \dots \times 0 \times L \times 0 \times \dots \times 0)$.

Alors $g_{j|D_i^j} = P_i^j/Q_i^j$ et chaque g_j est donné par une fraction rationnelle de $K(X_j)$ sur un ensemble cofini de L.

Par conséquent chaque g_j est égal à un polynôme P_j de $K[X_j]$ additif sur L. Chaque g_j est donc un p-polynôme.

Donc g est égal à un p-polynôme P de $K[X_{=m}]$, c'est à dire $g = r_P$.

Montrons l'unicité : soit P un p-polynôme de $K[X_{=n}]$ tel que $r_P = 0$. Par les relations 5, pour tout $i \in p^{\nu n}$, $r_{P_i} = r_P \cdot m_i \cdot \alpha^n = 0$. D'où $P_i = 0$ et donc $P = 0$.

Si P est un p-polynôme de $K[X_\infty]$, en faisant des changements de variables du type X_j remplacé par $\sum_{i \in p^\nu} m_i X^p_{j\frown i}$, on obtient un p-polynôme P' de $K[X_{=n}]$ congru à P modulo I^0. Ces changements de variables reviennent à remplacer dans $\mathrm{End}_K((L,+))$, $r_{P_j} \cdot f_j$ par $r_{P_j} \cdot (\sum_{i \in p^\nu} m_i \cdot \alpha \cdot f_{j\frown i})$. On a donc $r_P = r_{P'}$. On en déduit avec le résultat précédent que si $r_P = 0$, $P \in I_0$. $\triangleleft$

Le corollaire suivant permet de montrer que L n'a pas de sous-module définissable (3.3.9).

Corollaire 3.3.2. $\mathrm{End}_K((L,+))$ *n'a pas d'idéal bilatère non trivial.*

$\triangleright$ Soit r un endomorphisme dans $\mathrm{End}_K((L,+))$ différent de 0. On montre que l'idéal bilatère $< r >$ engendré par r est tout $\mathrm{End}_K((L,+))$.

Par (3.3.1) et les relations 5, il existe n tel que pour tout $i \in p^{\nu n}$, $r \cdot m_i \cdot \alpha^n \in K\{\alpha\}$. Comme $r = \sum_{i \in p^{\nu n}} r \cdot m_i \cdot \alpha^n \cdot f_i$, il existe dans $< r >$ un élément non nul de $K\{\alpha\}$ qui s'écrit $\sum_j a_j \alpha^j = P(\alpha)$ où $P \in K[X]$.

On fait maintenant une induction sur le degré de P. Si P est de degré 0, il est évident que $1 \in < P(\alpha) >$.

Si $\deg(P) = m + 1$ alors il y a deux possibilités :

Ou bien $P(X) = Q(X) \cdot X$. Il existe $l \in p^\nu$ tel $f_l \cdot P(\alpha) \neq 0$ d'après la relation 4. Alors :

$$f_l \cdot P(\alpha) = \sum_{j>0} \left(\sum_{i \in p^\nu} b_{j,i} f_i \alpha^j \right) = \sum_{j>0} b_{j,0} \alpha^{j-1} = R(\alpha).$$

Le p-polynôme R de $K[X]$ est non nul et de degré strictement inférieur à celui de P.

Ou bien en multipliant par un élément de K on peut supposer $P = 1 + Q(X)$ avec $Q \neq 0$. On multiplie encore par f_i à gauche tel que $f_i \cdot Q(\alpha) \neq 0$. On obtient alors un élément qui s'écrit $f_i + S(\alpha)$ avec $0 \leq \deg(S) < \deg(P)$. On choisit $l \neq i$ et on multiplie à droite par $m_l \cdot \alpha$ pour supprimer f_i. On obtient alors un polynôme de degré au plus celui de P mais qui se factorise par X. On applique le premier cas pour terminer. $\triangleleft$

3.3.2 Structure de $\mathrm{End}_K((L,+))$-module sur $(L,+)$

Nous nous intéressons aux rapports entre la structure de corps L au-dessus de K et la structure réduite de module sur l'anneau $\mathrm{End}_K((L,+))$. Notons $L_{K\text{-mod}}$ la structure de $\mathrm{End}_K((L,+))$-module sur $(L,+)$.

En utilisant la proposition 3.2.3 nous montrons :

Proposition 3.3.3. *Tout sous-groupe de $(L^{\times k},+)$ définissable sur K dans la structure de corps L est définissable sur $\emptyset$ dans la structure de module $L_{K\text{-mod}}$ par une formule atomique (et par stabilité tout sous-groupe de $(L^{\times k},+)$ $\bigwedge\!\!\bigwedge$-définissable sur K dans la structure de corps L est $\bigwedge\!\!\bigwedge$-définissable sur $\emptyset$ dans la structure de module $L_{K\text{-mod}}$).*

▷ Soit G un sous-groupe de $(L^{\times k}, +)$ définissable sur K dans L.
Par (3.2.3), il existe un p-polynôme P dans $K[X_{1,\infty}, \dots, X_{k,\infty}]$ tel que $G = V(\{P\})$.
Alors $P = \sum_{j=1}^{k} P_j[X_{j,\infty}]$.
Le groupe G est donc défini dans la structure de module $L_{K\text{-mod}}$ par

$$\sum_{j=1}^{k} r_{P_j}(x_j) = 0.$$

◁

Corollaire 3.3.4. *La structure de module $L_{K\text{-mod}}$ a l'élimination des quantificateurs.*

▷ Dans un module, tout ensemble définissable (sur vide) est combinaison booléenne d'ensembles définissables (sur vide) par une *pp*-formule [Zi 84]. Dans la structure $L_{K\text{-mod}}$, un ensemble $\emptyset$-définissable par une *pp*- formule est de la forme $\bar{a} + G$ où $\bar{a} \in K$ et G est un groupe K- définissable dans la structure de corps L. Par (3.3.3), G est défini par une formule atomique dans la structure de module $L_{K\text{-mod}}$ et donc $\bar{a} + G$ aussi. ◁

Corollaire 3.3.5. *Supposons K séparablement clos (c'est-à-dire $K \preccurlyeq L$).*

Soit G un sous-groupe 1-basé de $(L^{\times k}, +)$ $\bigwedge\!\!\!\bigwedge$-définissable sur K dans L. Alors la structure induite sur G par la structure de corps L au-dessus de K est identique à celle induite par la structure de module $L_{K\text{-mod}}$ au-dessus du vide. De plus tout relativement définissable (à paramètres quelconques) de G dans la structure de corps L est relativement définissable dans la structure de module $L_{K\text{-mod}}$.

▷ Tout partie de $L^{\times k}$ définissable sur $\mathrm{acl}^{eq}(K)$ dans la structure de corps L est en fait définissable sur K car K est une sous-structure élémentaire de L.

Un ensemble relativement définissable D de G^n dans la structure de corps L est combinaison booléenne de translatés T de sous-groupes de G^n relativement définissables sur K (1.3.2). Par (3.3.3), D est relativement définissable dans la structure de module $L_{K\text{-mod}}$.

De plus, si D est relativement définissable sur K dans la structure de corps L, alors par (1.3.2), chaque translaté T est relativement définissables sur K dans L. Or un tel translaté T est nécessairement de la forme $\bar{a} + H$ où $\bar{a} \in K$, car K est un modèle. Ces translatés sont alors $\emptyset$-définissable dans la structure de module $L_{K\text{-mod}}$ (3.3.3). ◁

Pour $K = \mathbb{F}_p(B)$, nous avons retrouvé le résultat d'élimination des quantificateurs (3.3.4) démontré par P. Dellunde, F. Delon et F. Point pour leur théorie de $\mathbb{F}_p(B)\{\alpha\}$-module enrichie par les f_i. Voici leur résultat principal :

Théorème 3.3.6. *[DDP] Soit $\mathcal{L}_K = \mathcal{L}_{K\{\alpha\}} \cup \{f_i, i \in p^\nu\}$*

Soit T_K la $\mathcal{L}_K$ théorie suivante :

1. *axiomes de $K\{\alpha\}$-modules à gauche.*
2. *$\forall x \exists^{=\deg(P_r)} y,\ r \cdot y = x$, pour tout r dans $K\{\alpha\}$ tel que P_r est séparable.*
3. *$\forall x\ x = \sum_{i \in p^\nu} m_i \cdot \alpha \cdot f_i(x)$.*
4. *$\forall x \forall (x_i)_{i \in p^\nu} \Big(x = \sum_{i \in p^\nu} m_i \cdot \alpha \cdot x_i \to \wedge_i x_i = f_i(x)\Big)$.*

Alors T_K est complète, élimine les quantificateurs et a pour modèle premier K^{sep}.

Remarque. Dans [DDP] cette preuve est faite pour $K = \mathbb{F}_p(B)$ mais les auteurs utilisent seulement le fait que K contient B et est clos par les f_i.

On peut traduire ce théorème dans le langage de $\mathrm{End}_K((L,+))$-module. Les axiomes 3 et 4 sont inclus dans les axiomes de $\mathrm{End}_K((L,+))$-module à gauche :

Corollaire 3.3.7. *La théorie de $L_{K\text{-}mod}$ a l'élimination des quantificateurs, a pour modèle premier K^{sep} et est axiomatisé par :*

1. *axiomes de* $\mathrm{End}_K((L,+))$*-modules à gauche.*
2. $\forall x \exists^{=\deg(P_r)} y,\ r \cdot y = x$*, pour tout r dans $K\{\alpha\}$ tel que P_r est séparable.*

Définition. Pour toute partie A de L, on définit l'idéal à gauche de $\mathrm{End}_K((L,+))$,

$$\mathrm{Ann}(A) := \{r \in \mathrm{End}_K((L,+)); r \cdot a = 0 \text{ pour tout } a \in A\}.$$

Pour J un idéal à gauche de $\mathrm{End}_K((L,+))$, on désigne par $< S(J) >$ l'idéal de $K[X_\infty]$ engendré par $S(J) := \{P \in K[X_\infty]; P\ \ p\text{-polynôme et } r_P \in J\}$.

Remarque 3.3.8. $< S(J) >$ est un idéal séparable contenant I^0.

Il suffit d'utiliser la preuve de (3.2.7) avec $S(J)$. Alors $S(J)$ contient I^0. D'autre part pour tout $P \in S$ et P_i p-polynômes, tels que $P \equiv \sum_{i \in p^\nu} P_i^p m_i \pmod{I^0}$, les P_i sont dans $S(J)$ car alors $r_P = \sum_{i \in p^\nu} m_i \cdot \alpha \cdot r_{P_i}$ et $r_{P_i} = f_i \circ r_P$.

Proposition 3.3.9. *Pour tout sous-groupe G de $(L,+)$ $\bigwedge\!\!\bigwedge$-définissable sur K dans L,*

$$G = \{x \in L; r \cdot x = 0, \ \textit{pour tout } r \in \mathrm{Ann}(G)\} \ \textit{ et } \ I(G,K) =< S(\mathrm{Ann}(G)) > .$$

Donc $L_{K\text{-}mod}$ n'a pas de sous-module $\emptyset$-définissable non trivial.

$\triangleright$ Par (3.2.8), $I(G,K) =< S(\mathrm{Ann}(G)) >$ et donc $G = V(S(\mathrm{Ann}(G)))\}$.

Soit M un sous-module $\emptyset$-définissable de $L_{K\text{-mod}}$. Alors $\mathrm{Ann}(M)$ est un idéal bilatère de $\mathrm{End}_K((L,+))$. D'après (3.3.2) cet idéal est trivial ; M est donc trivial. $\triangleleft$

3.4 Endomorphismes de sous-groupes minimaux du groupe additif

Nous rappelons que L est un modèle fixé de $T_{p,\nu}$ et K un sous-corps définissablement clos de L. De plus nous supposons L $|K|^+$-saturé. Nous étudions dans ce qui suit les endomorphismes définissables sur K de sous-groupes additifs définissables sur K. En fait, les classes d'exemples de sous-groupes minimaux que nous considérons sont définissables sur $\emptyset$ (c'est-à-dire sur $\mathbb{F}_p(B)$). Donc pour les exemples localement modulaires, les endomorphismes sont définissables sur $\mathbb{F}_p(B)^{sep}$ (1.3.2 iv). Nous notons toujours α le Frobénius.

Nous montrons dans cette section que tout endomorphisme définissable d'un sous-groupe du groupe additif est la restriction d'un endomorphisme du groupe additif lui-même (3.4.7). Nous montrons aussi que pour tout sous-groupe minimal additif G non isomorphe à $(L^{p^\infty}, +)$ (en particulier pour tout sous-groupe localement modulaire), il existe un entier $n > 0$ tel que le corps $K \cap \mathrm{End}_K(G)$ des endomorphismes-homothéties scalaires de G est égal à $\mathbb{F}_{p^n}$ (3.4.8).

Nous remarquons dans le paragraphe 3.4.4 suivant qu'il existe un nombre arbitraire des sous-groupes additifs minimaux deux à deux orthogonaux et que les sous-groupes additfs minimaux témoignent de la DOP.

Nous étudions ensuite les anneaux d'endomorphismes de certains sous-groupes minimaux additifs localement modulaires : nous montrons que la locale modularité d'un sous-groupe minimal ne se voit pas sur l'anneau des endomorphismes (3.4.24) (alors que nous verrons dans la section suivante qu'elle se voit sur le corps des quasi-endomorphismes). En effet il existe des sous-groupes minimaux localement modulaires dont l'anneau des endomorphismes est réduit à $\mathbb{F}_p$ (3.4.23) et nous donnons un exemple de sous-groupe minimal non localement modulaire ayant aussi comme anneau des endomorphismes $\mathbb{F}_p$ (3.4.3).

3.4.1 Deux exemples de sous-groupes additifs minimaux non localement modulaires

Nous savons que tout sous-groupe minimal du groupe additif non localement modulaire est définissablement isogène à $(L^{p^\infty}, +)$ (3.1.25). E. Bouscaren et F. Delon [BD2] ont donné un exemple de groupe minimal définissablement isogène mais non définissablement isomorphe à $(L^{p^\infty}, +)$.

Nous montrons que l'anneau des endomorphismes définissables sur K de cet exemple est réduit à $\mathbb{F}_p$ alors que celui de $(L^{p^\infty}, +)$ est égal à l'anneau des endomorphismes définissables sur K^{p^∞} de $(L^{p^\infty}, +)$ dans sa structure de pur corps algébriquement clos.

Commençons par L^{p^∞} :

Proposition 3.4.1. *Les endomorphismes de $(L^{p^\infty}, +)$ définissables sur K sont de la forme $r_P \cdot \alpha^{-n}$ où P est un p-polynôme de $K^{p^\infty}[X]$. L'anneau de ces endomorphismes est donc égal à $K^{p^\infty}\{\alpha, \alpha^{-1}\}$.*

$\triangleright$ Soit $f : (L^{p^\infty}, +) \to (L^{p^\infty}, +)$ un endomorphisme K-définissable. Par compacité il existe un entier m et un homomorphisme $\tilde{f} : (L^{p^m}, +) \to (L, +)$ définissable sur K tels que $f = \tilde{f}$ sur L^{p^∞}.

A nouveau par compacité et (3.1.4), il existe un recouvrement fini de L^{p^m} par des parties $D_1, \ldots, D_l$ définissables sur K et des fractions rationnelles $R_1, \ldots, R_l \in K(X_{=n})$ tels que $\tilde{f}(x) = R_i(x_{=n})$ pour tout $x \in D_i$.

Soient $C_i = D_i \cap L^{p^\infty}$. Les C_i sont alors définissables sur $K \cap L^{p^\infty} = K^{p^\infty}$ dans la structure L^{p^∞} (3.1.6).

Maintenant sur L^{p^∞}, $x_{=n} = (\alpha^{-n}(x), 0, \ldots, 0)$. En posant donc $g = f \cdot \alpha^n$, on obtient pour tout i, $g(x) = R'_i(x) = R_i(x, 0, \ldots, 0)$ sur $C'_i = \alpha^{-n}(C_i)$.

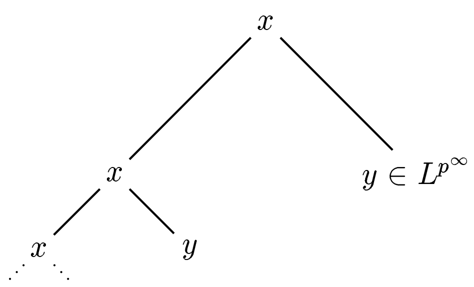
Donc g est égal à l'une des fractions rationnelles R'_i qui est alors un p-polynôme à paramètres dans K. Il est évidemment à paramètres dans L^{p^∞} et donc dans K^{p^∞}. $\triangleleft$

En fait cette preuve est l'analogue de celle qui montre le même résultat pour un pur corps algébriquement clos. On pourrait aussi d'ailleurs l'en déduire en utilisant (3.1.6) :

Fait 3.4.2. *Soient F un corps algébriquement clos et F_0 un sous-corps parfait de F. Alors l'anneau des endomorphismes définissables sur F_0 de $(F,+)$ est $F_0\{\alpha,\alpha^{-1}\}$.*

Remarque. Sur L^{p^∞}, $\alpha^{-1} = f_0$ (où $0 = (0,\dots,0) \in p^\nu$) et donc tout endomorphisme de $(L^{p^\infty},+)$ définissable est restriction d'un endomorphisme de $(L,+)$ définissable. Nous allons montrer dans la partie suivante que ce résultat est vrai pour tout sous-groupe connexe définissable de $(L,+)$.

Étudions maintenant l'anneau des endomorphismes de l'exemple donné dans [BD2]. Ce groupe est $G := \{x;\ \exists y \in L^{p^\infty},\ x = x^p + by^p\}$ avec $b \in K - K^p$. On peut supposer $b = b_0$ le premier élément de la p-base.



Groupe G

Pour démontrer que le groupe G n'est pas isomorphe à L^{p^∞}, E. Bouscaren et F. Delon montrent en particulier que pour tout homomorphisme ϕ du groupe $(G,+)$ dans $(L,+)$ définissable sur K, il existe m tel que $\alpha^m \circ \phi$ est égal à un p-polynôme de $K[X]$. Nous allons en déduire que G a très peu d'endomorphismes définissables.

Proposition 3.4.3. *L'anneau des endomorphismes de G définissables sur K est réduit à $\mathbb{F}_p$.*

$\triangleright$ On note $0 = (0,\dots,0)$, $1 = (1,0,\dots,0)$ et $p-1 = (p-1,0,\dots,0)$, ces trois éléments de p^ν (voir notations 3.1.2) et on note $b = b_0$ le premier élément de la p-base.

Ainsi pour tout $x \in L$,

$$x = x_0^p + x_1^p b + \ldots + x_{p-1}^p b^{p-1} + \sum_{p \le i < p^\nu} x_i m_i$$

et donc

$$G = \{x;\ x_0 = x,\ x_1 \in L^{p^\infty},\ x_i = 0 \text{ pour tous les autres } i \in p^\nu\}$$

Pour $x \in G$ on note $y := x_1$.

Soit ϕ un endomorphisme de G définissable sur K. Par [BD2], il existe un entier m et un p-polynôme P_0 de $K[X]$ tel que $\alpha^m \circ \phi = P_0$.

Nous allons montrer par récurrence sur $l \leq m$ que pour tout $x \in G$,

$$\alpha^{m-l} \circ \phi(x) = P_l(x) + \sum_{j=1}^{l} c_j y^{p^{1-j}}$$

où P_l est un p-polynôme de $K[X]$ et les $c_j \in K$.

Ce résultat est vrai pour $l = 0$ et s'il est vrai pour un $l < m$, alors pour tout $x \in G$,

$$\begin{aligned}\alpha^{m-l-1} \circ \phi(x) &= f_0(\alpha^{m-l} \circ \phi(x)) \\ &= f_0(P_l(x) + \sum_{j=1}^{l} c_j y^{p^{1-j}}) \\ &= f_0(\sum_{j \geq 0} a_j x^{p^j} + \sum_{j=1}^{l} c_j y^{p^{1-j}})\end{aligned}$$

Or

$$a_0 x = (a_{0,0}^p + \ldots + a_{0,p-1}^p b^{p-1} + \ldots)(x^p + by^p) = (a_{0,0}x + a_{0,p-1}by)^p + \ldots$$

(Ici, $a_{0,0} = f_0(a_0)$ et $a_{0,p-1} = f_{p-1}(a_0)$.)

Donc $f_0(a_0 x) = a_{0,0}x + a_{0,p-1}by$.
Pour tout $j > 0$,

$$f_0(a_j x^{p^j}) = f_0((a_{j,0} x^{p^{j-1}})^p + \ldots) = a_{j,0} x^{p^{j-1}}.$$

De plus comme $y \in L^{p^\infty}$, pour tout $j \in \{1, \ldots, l\}$,

$$f_0(c_j y^{p^{1-j}}) = f_0((c_{j,0} y^{p^{-j}})^p + \ldots) = c_{j,0} y^{p^{-j}}.$$

Donc

$$\alpha^{m-l-1} \circ \phi(x) = a_{0,0}x + a_{0,p-1}by + \sum_{j>0} a_{j,0} x^{p^{j-1}} + \sum_{j=1}^{l} c_{j,0} y^{p^{-j}}.$$

Pour $l = m$, il existe donc a_j et c_j dans K tel que tout $x \in G$,

$$\phi(x) = \sum_{j=0}^{n} a_j x^{p^j} + \sum_{j=1}^{m} c_j y^{p^{1-j}}.$$

Alors, pour les mêmes raisons que précédemment, pour tout $x \in G$,

$$f_0 \circ \phi(x) = a_{0,0}x + a_{0,p-1}by + \sum_{j=1}^{n} a_{j,0} x^{p^{j-1}} + \sum_{j=1}^{m} c_{j,0} y^{p^{-j}}.$$

Par ailleurs pour tout $x \in G$ $f_0 \circ \phi(x) = \phi(x)$ puisque ϕ est un endomorphisme de G. On a donc l'égalité suivante sur G :

$$(1) \quad \sum_{j=0}^{n} a_j x^{p^j} + \sum_{j=1}^{m} c_j y^{p^{1-j}} = a_{0,0}x + \sum_{j=1}^{n} a_{j,0} x^{p^{j-1}} + a_{0,p-1} by + \sum_{j=1}^{m} c_{j,0} y^{p^{-j}}.$$

On peut remarquer que si une équation sur G du type suivant,

$$\sum_{j=0}^{l} d_j x^{p^j} + \sum_{j=0}^{r} e_j y^{p^{-j}} = 0,$$

a une infinité de solutions alors les coefficients d_j et e_j sont tous nuls. (Pour cela il suffit d'élever à la puissance p^{r+1} et de remplacer y^p par $(x - x^p)/b$.)

Par (1) les a_j sont nuls pour $j \geq 1$. Nous pouvons donc supposer $n = 0$. On obtient de plus les égalités suivantes : $a_0 = a_{0,0}$, $c_1 = a_{0,p-1} \cdot b$, $c_j = c_{j-1,0}$ pour $1 < j \leq m$ et $c_{m,0} = 0$.

Par ailleurs pour tout $i \neq 0,\ 1$, et $x \in G$,

$$f_i \circ \phi(x) = 0 = a_{0,i}x + \text{termes en } y,\ y^{p^{-1}},\ y^{p^{-m}}.$$

D'où $a_{0,i} = 0$ pour tout $i \neq 0,\ 1$.

En supposant maintenant $p \neq 2$, on peut conclure rapidement : en effet $p - 1 \neq 1$ d'où $a_{0,p-1} = 0$ et donc tous les c_j sont nuls.

Par conséquent, on a montré dans ce cas que pour tout $x \in G$, $\phi(x) = a_0 x$ avec $a = a_{0,0}$ et $a_{0,i} = 0$ pour tout $i \neq 0,\ 1$. Un tel homomorphisme correspond à la multiplication par un élément de $\mathbb{F}_p$. En effet pour tout $x \in G$,

$$\phi(x) = a_0 x = (a_{0,0}^p + b a_{0,1}^p)(x^p + by^p) = (a_{0,0}x)^p + b(a_{0,0}y + a_{0,1}x)^p + b^2(a_{0,1}y)^p.$$

Comme $p \neq 2$, $a_{0,1} = 0$ et donc $a_0 = a_0^p$.

En général, sans supposer $p \neq 2$, on a $f_1(\phi(x)) \in L^{p^\infty}$. C'est à dire pour tout $x \in G$,

$$a_{0,1}x + a_{0,0}y + \sum_{j=1}^{m} c_{j,1} y^{p^{-j}} \in L^{p^\infty}.$$

D'où $a_{0,1} \in L^{p^\infty}$ car $1 \in G$. Ainsi pour tout $i \in p^{\nu n}$ non nul, en composant par f_i, alors $a_{0,0\frown i} = 0$ et pour tout j, $c_{j,1\frown i} = 0$. D'où $a_{0,1}$, $a_{0,0}$ et les $c_{j,1}$ sont dans L^{p^∞}. Par conséquent, $a_{0,1}$ est nul sinon on aurait $G \subseteq L^{p^\infty}$. On a donc $a_{0,i}$ nul pour tout $i \neq 0$, donc d'après les résultats venant de (1), les c_i sont nuls et $a_0 = a_0^p$. D'où $\phi(x) = a_0 x$ avec $a_0 \in \mathbb{F}_p$. $\lhd$

3.4.2 Endomorphismes de sous-groupes additifs

Après ces deux exemples nous allons montrer que tout endomorphisme d'un sous-groupe connexe définissable de $(L,+)$ est restriction d'un endomorphisme de $(L,+)$.

Proposition 3.4.4. *Soient G un sous-groupe de $(L,+)$, définissable sur K et connexe, et ϕ un homomorphisme de G dans $(L,+)$ définissable sur K. Alors il existe ψ un endomorphisme de $(L,+)$ définissable sur K (et donc défini par un p-polynôme de $K[X_\infty]$) qui prolonge ϕ.*

Remarque. Par (3.3.3) la proposition (3.4.4) est équivalente à la proposition suivante : soit G un sous-groupe de $(L,+)$ définissable sur $\emptyset$ dans la structure de module $L_{K\text{-mod}}$. Alors tout homomorphisme de G dans $(L,+)$ définissable sur $\emptyset$ dans la structure de module $L_{K\text{-mod}}$ est restriction d'un endomorphisme de $(L,+)$ définissable sur $\emptyset$ dans la structure de module $L_{K\text{-mod}}$.

Pour démontrer la proposition 3.4.4, nous allons plonger G dans $\bar{L}$ et nous utiliserons alors les deux lemmes suivants, le premier étant l'analogue de cette proposition dans le cas des corps algébriquement clos et le second portant sur le prolongement des homomorphismes définis génériquement dans une structure stable.

Lemme 3.4.5. *Soient F un corps algébriquement clos et F_0 un sous-corps algébriquement clos de F.*

Soient G un sous-groupe connexe de $(F^{\times k},+)$ définissable sur F_0 et ϕ un homomorphisme définissable sur F_0 de G sur un sous-groupe H de $(F^{\times k'},+)$. Alors il existe un homomorphisme ψ de $F^{\times k}$ dans H prolongeant ϕ et encore définissable sur F_0.

$\triangleright$ Par (3.2.2) il existe un entier l et un automorphisme β de $(F^{\times k},+)$ qui envoie G sur $F^{\times l}\times\{0\}^{k-l}$ et qui est définissable sur F_0 (en fait cet automorphisme et son inverse sont définis par des p-polynômes sur $F_0[X_1,\dots,X_k]$, c'est-à-dire $\beta(\bar{x})=(P_1(\bar{x}),\dots,P_k(\bar{x}))$ et $\beta^{-1}(\bar{x})=(Q_1(\bar{x}),\dots,Q_k(\bar{x}))$).

Soit $\gamma:=\beta^{-1}$. Alors $\beta=(\beta_1,\dots,\beta_k)$ et $\gamma=(\gamma_1,\dots,\gamma_k)$ tels que les β_i et les γ_i sont des homomorphismes de $(F^{\times k},+)$ dans $(F,+)$ définissables sur F_0. Soit

$$\psi(\bar{x}):=\phi\left(\gamma_1\left(\beta_1(\bar{x}),\dots,\beta_k(\bar{x}),0,\dots,0\right),\dots,\gamma_k\left(\beta_1(\bar{x}),\dots,\beta_k(\bar{x}),0,\dots,0\right)\right).$$

Alors ψ est un homomorphisme de $F^{\times k}$ dans $\phi(G)$ qui prolonge ϕ et est définissable sur F_0. $\triangleleft$

Lemme 3.4.6. *Soient N une structure stable saturée et $M\preccurlyeq N$, $|M|<|N|$.*

Soient G et H deux groupes définissables sur M dans N. Supposons G connexe et p son type générique.

Soit $\Gamma\subseteq G\times H$ le graphe d'une fonction de G dans H définissable sur M (non nécessairement définie sur tout G). Supposons que Γ définit génériquement un homomorphisme de G dans H. C'est à dire $\Gamma\cap(p(N)\times H)$ est le graphe d'une application ϕ de $p(N)$ dans H telle que pour tous g,g' indépendants réalisant p , $\phi(g^{-1})=\phi(g)^{-1}$ et $\phi(gg')=\phi(g)\phi(g')$.

Alors il existe ψ un homomorphisme définissable sur M de G dans H qui prolonge ϕ.

▷ Soient $a \in G$ et g, g' deux génériques de G tels que a, g, et g' sont indépendants. On a alors

$$\phi(g')^{-1}\phi(g) = \phi({g'}^{-1}g) = \phi({g'}^{-1}a(g^{-1}a)^{-1}) = \phi({g'}^{-1}a)\phi(g^{-1}a)^{-1}$$

D'où $\phi(g)\phi(g^{-1}a) = \phi(g')\phi({g'}^{-1}a)$.

On peut donc définir $\psi(a)$ par $\phi(g)\phi(g^{-1}a)$ pour g générique de G indépendant de a.

Alors ψ est $\mathcal{M}$-définissable sur M (par définissabilité du type p sur M).

On montre que ψ est un homomorphisme. Soient a, b dans G. Soit g un générique indépendant de a, b. Alors

$$\psi(a)\psi(b) = (\phi(g)\phi(g^{-1}a)) \cdot (\phi(a^{-1}g)\phi((a^{-1}g)^{-1}b)) = \phi(g)\phi(g^{-1}ab) = \psi(ab).$$

Pour montrer la définissabilité de ψ, on utilise un argument de compacité : il existe par compacité une formule F dans p telle que ψ restreint à F est définissable par Γ, car $p(x) \wedge (y = \psi(x))$ implique $\Gamma(x, y)$. Maintenant F est une formule générique, donc G est recouvert par un nombre fini de translatés de F, ce qui donne la définissabilité de ψ. ◁

▷ **Preuve de la proposition 3.4.4**

Soit G un sous-groupe de $(L, +)$, définissable sur K et connexe, et ϕ un morphisme de G dans $(L, +)$ définissable sur K.

Comme ϕ est une application définissable sur K, il existe un entier n, des ensembles définissables sur K, $D_1, \ldots, D_n$ recouvrant G tels que $\phi_{|D_i} = P_i/Q_i$ où $P_i, Q_i \in K[X_\infty]$ et $Q_i \neq 0$ sur D_i (car pour tout $a \in L$, $\mathrm{dcl}(K \cup \{a\}) = K(a_\infty)$ (3.1.4)).

Il existe donc un entier m tel que G est λ_m-fermé, les D_i sont λ_m-constructibles et P_i et Q_i sont des polynômes de $K[X_{=m}]$.

Soient $G' := \lambda_m(G)$ et ϕ' l'homomorphisme de G' dans $(L, +)$ associé à ϕ défini par $\phi'(\bar{x}) := \phi(\lambda_m^{-1}(\bar{x}))$. Alors G' est un sous-groupe λ_0-fermé de $L^{\times p^{\nu m}}$. Soient $D'_i := \lambda_m(D_i)$. Alors pour tout i, $\phi'_{|D'_i}(\bar{x}) = P_i(\bar{x})/Q_i(\bar{x})$ où l'on considère les polynômes P_i et Q_i dans $K[\bar{X}]$ avec $\bar{X}$ un $p^{\nu m}$-uple de variables.

Le groupe G' est connexe et a donc un seul type générique qui correspond à son générique topologique. On peut supposer qu'il appartient à D'_1.

Soit $\bar{G}'$ la clôture de Zariski de G dans $\bar{L}^{\times p^{\nu m}}$. Soit Γ la partie de $(\bar{G}', \bar{L})$ définissable sur K par

$$\Gamma := \{(\bar{x}, y); \bar{x} \in \bar{G}',\ Q_1(\bar{x}) \neq 0 \text{ et } P_1(\bar{x}) = Q_1(\bar{x})y\}.$$

Comme G' est λ_0-fermé, $G' = \bar{G}'(L)$ et les génériques de G' dans L sont génériques dans $\bar{G}'$ (3.1.16 et 3.1.21).

On en déduit que Γ définit génériquement un homomorphisme de $\bar{G}'$ dans $(\bar{L}, +)$. Donc par (3.4.6) il existe ψ un homomorphisme définissable sur $\bar{K}$ de $\bar{G}'$ dans $(\bar{L}, +)$ qui prolonge l'homomorphisme générique défini par Γ. Il est donc égal à ϕ' sur les génériques de G' et comme tout élément de G' est somme de deux génériques, ψ prolonge ϕ'.

Par (3.4.5), ψ se prolonge en un homomorphisme de $(\bar{L}^{\times p^{\nu m}}, +)$ dans $(\bar{L}, +)$ définissable sur $\bar{K}$. Donc par (3.4.2) il existe $(a_{i,j})_{i\in\{1,\dots,p^{\nu m}\},j\in\mathbb{Z}}$ une famille d'éléments de $\bar{K}$ presque tous nuls tels que :

$$\psi(\bar{x}) = \sum_{i=1}^{p^{\nu m}} \sum_{j\in\mathbb{Z}} a_{i,j}\alpha^j(x_i).$$

En composant par une puissance suffisante de α, on obtient pour tout $\bar{x} \in G'$, $\alpha^r \circ \phi'(\bar{x}) = S(\bar{x})$ où S est un p-polynôme de $K^{sep}[\bar{X}]$. Comme $\alpha^r \circ \phi'$ est définissable sur K, nous pouvons supposer que S est un p-polynôme de $K[\bar{X}]$: en effet il suffit de considérer le sous-groupe H connexe λ_0-fermé de $(L^{\times p^{\nu m}} \times L, +)$ défini par le graphe de $\alpha^r \circ \phi'$. Alors par (3.2.6) et du fait que pour tout $(\bar{x}, y) \in H$, $y = S(\bar{x})$, il existe un p-polynôme P de $K[\bar{X}, Y]$ unitaire et de degré 1 en Y tel que pour tout $(\bar{x}, y) \in H$, $P(\bar{x}, y) = 0$.

Enfin $\phi' = f_0^r \circ \alpha^r \circ \phi'$, d'où pour tout $\bar{x} \in G'$, $\phi'(\bar{x}) = S'(\bar{x}_{=r})$ où S' est un p-polynôme de $K[\bar{X}_{=r}]$ et donc pour tout $x \in G$, $\phi(x) = T(x_{=m+r})$ où T est un p-polynôme de $K[X_{=m+r}]$. $\triangleleft$

On peut donc montrer de même que tout endomorphisme de sous-groupe additif $\bigwedge\!\!\!\bigwedge$-définissable est restriction d'un endomorphisme de $(L, +)$:

Corollaire 3.4.7. *Soit G un sous-groupe de $(L, +)$ $\bigwedge\!\!\!\bigwedge$-définissable sur K et connexe. Les homomorphismes de G dans $(L, +)$ définissables sur K sont restrictions d'endomorphismes de $(L, +)$ définissables sur K. Soient* $\mathrm{End}_K(G)$ *l'ensemble de ces endomorphismes,* $\mathrm{End}_K((L, +), G)$ *l'ensemble des endomorphismes de $(L, +)$ laissant globalement invariant G et* $\mathrm{Ann}_K(G)$ *l'ensemble des endomorphismes de $(L, +)$ s'annulant sur G. Alors :*

$$\mathrm{End}_K(G) = \mathrm{End}_K((L, +), G)/\mathrm{Ann}_K(G).$$

Pour H un sous-groupe de $(L^{\times k}, +)$ $\bigwedge\!\!\!\bigwedge$-définissable sur K et connexe, les homomorphismes de H dans $(L, +)$ définissables sur K sont restrictions d'homomorphismes de $(L^{\times k}, +)$ dans $(L, +)$ définissables sur K. On a ici

$$\mathrm{End}_K(H) = \mathcal{M}_{k,k}(\mathrm{End}_K((L, +), H))/(\mathrm{Ann}_K(H))^{\times k}$$

où

$$\mathrm{Ann}_K(H) := \{(r_1, \dots, r_k) \in (\mathrm{End}_K(L, +))^{\times k};\ \forall h \in H,\ \sum r_i \cdot h_i = 0\}.$$

$\triangleright$ Par stabilité G est une intersection de sous-groupes de $(L, +)$ définissables sur K. Avec (3.1.20) G est en fait une intersection de sous-groupes G_i de $(L, +)$ définissables sur K et connexes. Si ϕ est un homomorphisme définissable sur K alors par compacité ϕ est restriction d'un homomorphisme de G_i dans $(L, +)$. En utilisant la proposition précédente, on en déduit que ϕ est restriction d'un endomorphisme de $(L, +)$.

Pour H il suffit d'utiliser λ_m^{-1} avec $p^{\nu m} \geq k$. Ainsi on obtient un homomorphisme d'un groupe G comme ci-dessus dans $(L, +)$. Cet homomorphisme est restriction d'un endomorphisme de $(L,+)$. On applique maintenant λ_m, on obtient ainsi un homomorphisme de $(L^{\times p^{\nu m}},+)$ dans $(L,+)$. En gardant les k premières coordonnées on conclut.

On peut en fait remarquer que dans la proposition précédente 3.4.4 on a utilisé le fait que G est un sous-groupe de $(L,+)$ seulement pour ne pas alourdir les notations avec un entier k supplémentaire. La preuve est donc la même pour G sous-groupe de $(L^{\times k},+)$ et ceci permet de conclure directement pour le deuxième point de notre corollaire. ◁

3.4.3 Corps des endomorphismes-homothéties d'un sous-groupe additif minimal

Pour G un sous-groupe additif minimal définissable sur K, nous appelons corps des endomorphismes-homothéties de G définissables sur K, le corps $K \cap \mathrm{End}_K(G)$.

Proposition 3.4.8. *Soit G un sous-groupe de $(L,+)$ minimal $\bigwedge\!\!\bigwedge$-définissable sur K. Si G n'est pas définissablement isomorphe à $(L^{p^\infty},+)$ (en particulier si G est localement modulaire) alors il existe un entier $n>0$ tel que $K \cap \mathrm{End}_K(G) = \mathbb{F}_{p^n}$.*

▷ Pour tout entier l soit $G_l := V(I(G)_{\leq l})$. Les groupes G_l sont connexes puisque G est connexe : en effet pour tout entier l, $I_{K^{sep}}(G)_{\leq l}$ est premier séparable donc $G_l = V(I_{K^{sep}}(G)_{\leq l})$ est connexe (3.2.1).

Montrons que si $k \in K \cap \mathrm{End}_K(G)$ et k non nul alors pour tout l, $kG_l = G_l$. Pour tout l,

$$I(kG)_{\leq l} = \{Q(X_{\leq l});\ Q(X_{\leq l}) := P(k^{-1}X_{\leq l}) \text{ et } P(X_{\leq l}) \in I(G)_{\leq l}\}.$$

Donc $V(I(kG)_{\leq l}) = kV(I(G)_{\leq l}) = kG_l$. D'autre part par minimalité de G, $kG = G$, donc $G_l = V(I(kG)_{\leq l}) = kG_l$.

On en déduit que

$$K \cap \mathrm{End}_K(G) = K \cap \bigcap_{l\in\omega} \mathrm{End}_K(G_l).$$

Étudions maintenant $K \cap \mathrm{End}_K(G_l)$ pour l fixé. Fixons un élément g non nul de G.

Soit $H := \lambda_l(G_l)$ sous-groupe connexe de $(L^{\times p^{\nu l}},+)$ λ_0-fermé sur K. Soit h un générique de H au-dessus de K. On peut supposer que $h = \bar{x}y_1 \dots y_{n_l}$ avec $\bar{x}$ base de transcendance séparante de $K(h)$ au-dessus de K. Par (3.2.6), il existe des p-polynômes $P_1, \dots, P_n$ de $K[\bar{X}, Y_1, \dots, Y_n]$ tels que $H = V(\{P_1, \dots, P_n\})$ et tels que pour tout $i \in \{1, \dots, n\}$, $P_i \in K[\bar{X}, Y_1, \dots, Y_i]$, P_i est unitaire et de degré minimal n_i en Y_i parmi les p-polynômes de $K^{sep}[\bar{X}, Y_1, \dots, Y_i]$ de degré >0 en Y_i et s'annulant en h, et pour tout $j<i$ $\deg_{Y_j}(P_i) < \deg_{Y_j}(P_j)$. Par ailleurs en renommant les variables à l'aide de la bijection λ_l, ces polynômes se voient aussi comme p-polynômes dans $K[Z_{=l}]$, tels que

$$G_l = \{z \in L;\ P_1(z_{=l}) = \ldots = P_n(z_{=l}) = 0\}.$$

Soit $k \in K \cap \mathrm{End}_K(G_l)$. Alors $k^{p^l} \in \mathrm{End}_K(G_l)$, donc $k \in \mathrm{End}_K(H)$. Par la propriété de minimalité sur les polynômes $P_1, \ldots, P_n$, on a alors pour tout $i \in \{1, \ldots, n\}$,

$$P_i(k\bar{X}, kY_1, \ldots, kY_i) = k^{p^{n_i}} P_i(\bar{X}, Y_1, \ldots, Y_i).$$

Si pour un i, il existe un entier $m \neq n_i$ tel qu'une variable à la puissance p^m est présente dans P_i, alors $k^{p^m} = k^{p^{n_i}}$, donc $k \in \mathbb{F}_{p^{|n_i - m|}}$. Dans ce cas, $K \cap \mathrm{End}_K(G_l)$ est fini.
Sinon, pour tout i,

$$P_i(Z_{=l}) = \sum_{j \in p^{\nu l}} a_j Z_j^{p^{n_i}}.$$

Montrons alors que $gL^{p^\infty} \subseteq G_l$. Rappelons que g est un élément fixé de G. Soit $c \in L^{p^\infty}$ alors pour tout $i \in \{1, \ldots, n\}$,

$$P_i((cg)_{=l}) = \sum_{j \in p^{\nu l}} a_j((cg)_j)^{p^{n_i}} = \sum_{j \in p^{\nu l}} a_j(c^{p^{-l}} g_j)^{p^{n_i}} = c^{p^{n_i - l}} P_i(g) = 0.$$

Donc $cg \in G_l$.

On a donc montré que ou bien il existe l, tel que $K \cap \mathrm{End}_K(G_l)$ est fini et donc $K \cap \mathrm{End}_K(G)$ est un corps fini, ou bien pour tout l, $gL^{p^\infty} \subseteq G_l$ et donc $gL^{p^\infty} \subseteq G$. Dans ce second cas par minimalité de G, $G = gL^{p^\infty}$. $\triangleleft$

3.4.4 Sous-groupes minimaux additifs orthogonaux

Nous montrons que si $|K|^{\aleph_0} > |K|$, il existe $|K|^{\aleph_0}$ sous-groupes additifs minimaux de rang de transcendance 1 définis sur K et deux à deux orthogonaux. Nous en déduisons qu'il existe des sous-groupes minimaux additifs orthogonaux à tout sous-groupe additif minimal défini sur $\mathbb{F}_p(B)^{sep}$. En fait la construction par F. Delon [De 88] de types orthogonaux à un corps donné K, montre aussi l'existence de sous-groupes minimaux orthogonaux à K et montre ainsi que les sous-groupes additifs témoignent de la multidimensionalité de $T_{p,\nu}$ et de la DOP. Ceci n'est pas en contradiction avec la non-multidimensionalité des théories de module et du résultat (3.3.3), car les sous-groupes additifs définis sur un sur-corps de K dans L ne sont pas nécessairement définissable dans la structure de module L_{K-mod}.

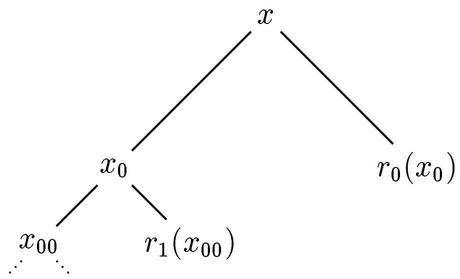
Nous terminons ce paragraphe par une construction ("effective") de $2^{\aleph_0}$ sous-groupes additifs minimaux de rang transcendance 1 définis sur le vide et deux à deux orthogonaux.

Nous allons utiliser une construction introduite dans [BD2] qui a permis aux auteurs de montrer l'existence de sous-groupes minimaux additifs de rang de transcendance infini.

Définition. Nous rappelons que pour $x \in L$ et $n \in \omega$, $x_{\bar{0}(n)}$ est défini par récurrence de la manière suivante : $x_{\bar{0}(0)} = x$ et $x_{\bar{0}(n+1)} = f_0(x_{\bar{0}(n)}) = x_{\bar{0}(n)0}$ (3.1.3).

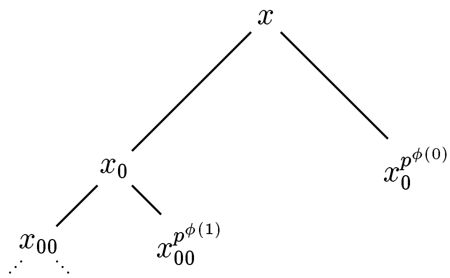
Soit $b = b_0$ le premier élément de la p-base.

Pour $r = (r_n)_{n\in\omega}$ une suite d'éléments de $K\{\alpha\}$ soit le sous-groupe de $(L,+)$ $G_r := \{x \in L;\ x_{\bar{0}(n)} = x^p_{\bar{0}(n+1)} + (r_n(x_{\bar{0}(n+1)}))^p b$ pour tout $n \in \omega\}$.



Groupes G_r

Pour ϕ une application de ω dans ω soit $G_\phi := G_r$ pour $r_n = \alpha^{\phi(n)}$.

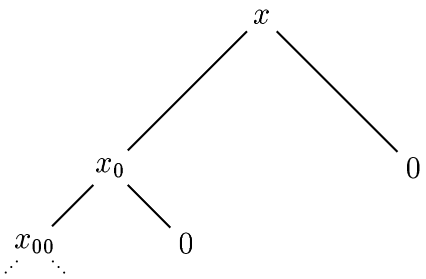


Groupes G_ϕ

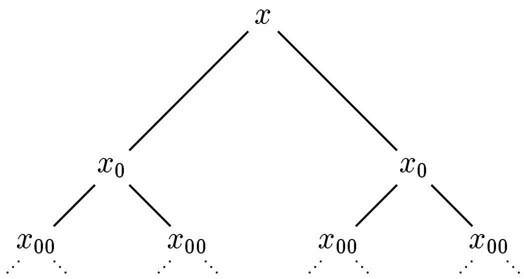
On définit $\deg(G_r)(n) := \prod_{0\le j<n} \deg(X^p + (P_{r_j}(X))^p b)$.

On a donc $\deg(G_\phi)(n) = \prod_{0\le j<n} p^{\phi(j)+1}$.

Remarque. Si $r = (0)$ alors G_r que l'on note $G_{(0)} = L^{p^\infty}$. Si ϕ est l'application nulle, G_ϕ que l'on note G_0 est isomorphe à L^{p^∞}. En fait G_0 est l'ensemble des points tels que $f_0(x_{\bar{0}(n)}) = f_1(x_{\bar{0}(n)})$ et $f_i(x_{\bar{0}(n)}) = 0$ pour $1 < i < p^\nu$. En prenant $a \in G_0$ non nul, on a $aL^{p^\infty} \subseteq G_0$ et par minimalité l'égalité.



Groupe $(L^{p^\infty}, +)$



Groupe G_0

Fait 3.4.9. *[BD2] Tous les groupes G_r sont minimaux de rang de transcendance un.*

Si x réalise le type générique de G_r, pour tout entier i, $[K(x_{\leq i}) : K(x)] = \deg(G_r)(i)$.

Si G_s est non orthogonal à G_r il existe des entiers n et k tels que pour tout entier i, $\deg(G_s)(i) \leq k \cdot \deg(G_r)(i+n)$.

Remarque. Le groupe G_n correspondant à l'application ϕ constante égale à n, est orthogonal à L^{p^∞} pour $n \geq 1$.

Corollaire 3.4.10. *Il existe $|K|^{\aleph_0}$ sous-groupes minimaux additifs définis sur K, localement modulaires et de rang de transcendance un.*

$\triangleright$ Par 3.4.9 il existe $|K|^{\aleph_0}$ sous-groupes minimaux additifs définis sur K de rang de transcendance un et orthogonaux au groupe $(L^{p^\infty}, +)$. Par 3.1.25 ces groupes sont localement modulaires. $\triangleleft$

Corollaire 3.4.11. *Si $|K|^{\aleph_0} > |K|$, il existe $|K|^{\aleph_0}$ sous-groupes additifs minimaux définis sur K, localement modulaires, de rang de transcendance un, et deux à deux orthogonaux.*

$\triangleright$ Soit G un sous-groupe additif minimal localement modulaire défini sur K. Par 1.3.7 il y a au plus $|K|$ groupes minimaux $\bigwedge\!\!\!\bigwedge$-définissables sur K non orthogonaux à G. On conclut par 3.4.10. $\triangleleft$

Corollaire 3.4.12. *Soit k_0 un sous-corps infini de K. Si $|K|^{\aleph_0} > |K|$ et si $|K|^{\aleph_0} > |k_0|^{\aleph_0}$, il existe un sous-groupe additif minimal localement modulaire défini sur K, de rang de transcendance un et orthogonal à tout groupe minimal $\bigwedge\!\!\!\bigwedge$-définissable sur k_0.*

$\triangleright$ Il y a au plus $|k_0|^{\aleph_0}$ groupes minimaux $\bigwedge\!\!\!\bigwedge$-définissables sur k_0. Par 1.3.7 il y a donc au plus $|K| \cdot |k_0|^{\aleph_0}$ groupes minimaux localement modulaires, $\bigwedge\!\!\!\bigwedge$-définissables sur K, et non orthogonaux à un de ces groupes $\bigwedge\!\!\!\bigwedge$-définissables sur k_0. On conclut par 3.4.10. $\triangleleft$

En fait en utilisant la construction de types orthogonaux de F. Delon [De 88], qui lui permet de montrer que la théorie $T_{p,\nu}$ a la DOP, on obtient immédiatement des sous-groupes minimaux additifs orthogonaux à $\mathbb{F}_p(B)^{sep}$. On peut alors remarquer que la DOP se voit avec les types additifs.

Proposition 3.4.13. *(voir [De 88]) Soit $k_0 \preccurlyeq K \preccurlyeq L$, tels que K est de degré de transcendance infini sur k_0, alors il existe un type q sur K orthogonal à k_0 que l'on peut de plus choisir minimal additif (c'est-à-dire générique d'un sous-groupe additif minimal).*

Cette proposition est un corollaire immédiat du résultat suivant :

Proposition 3.4.14. *[De 88] On dit qu'un idéal I de $K[X_\infty]$ a une* **croissance faible** *sur un sous-corps k_0 de K, s'il existe un entier m tel que pour tout n, $I_{\leq n}$ admet un corps de définition de degré de transcendance sur k_0 plus petit que $mp^{\nu n}$.*

Un type minimal p sur K tel que $I(p)$ n'est pas à croissance faible sur k_0 est orthogonal à k_0.

Nous allons maintenant donner une construction de sous-groupes additifs minimaux deux à deux orthogonaux :

Construction 3.4.15. Il existe $2^{\aleph_0}$ sous-groupes additifs minimaux de rang de transcendance un, définis sur $\emptyset$ et deux à deux orthogonaux.

Pour cette construction nous utilisons le petit lemme suivant :

Lemme 3.4.16. *Il existe une famille de parties de ω, $(O_\alpha)_{\alpha\in 2^\omega}$ telle que si $\alpha < \beta < 2^\omega$, $O_\alpha \subset O_\beta$ et $O_\beta \setminus O_\alpha$ est infini et contient des segments d'entiers arbitrairement longs.*

▷ Pour le corollaire 3.4.15 nous n'aurons besoin seulement que de la condition suivante : si $\alpha < \beta < 2^\omega$, $O_\alpha \subset O_\beta$ et $O_\beta \setminus O_\alpha$ est infini. Il suffit d'utiliser pour cela une bijection de ω avec $\mathbb{Q}$ et pour tout $\alpha \in \mathbb{R}$, prendre l'ensemble $O_\alpha :=]-\infty, r] \cap \mathbb{Q}$.

Par contre pour la preuve de (3.4.23) nous aurons besoin de la condition supplémentaire : si $\alpha < \beta$ alors $O_\beta \setminus O_\alpha$ contient des segments d'entiers arbitrairement longs. Pour obtenir une telle famille de parties de ω, on construit par induction sur la longueur de ε une famille de partitions de ω en parties contenant des segments d'entiers arbitrairement longs $(A_\varepsilon, B_\varepsilon, C_\varepsilon, D_\varepsilon, E_\varepsilon)_{\varepsilon\in 2^{<\omega}}$ ayant les propriétés suivantes :

Pour tout $\varepsilon \in 2^{<\omega}$,

$$\begin{array}{rcl} A_{\varepsilon\frown 0} & = & A_\varepsilon \cup C_\varepsilon \cup E_\varepsilon, \\ B_{\varepsilon\frown 0} & \supseteq & B_\varepsilon, \\ A_{\varepsilon\frown 1} & \supseteq & A_\varepsilon, \\ B_{\varepsilon\frown 1} & = & B_\varepsilon \cup D_\varepsilon \cup E_\varepsilon \text{ et} \\ \{0,\dots,l(\varepsilon)-1\} & \subset & A_\varepsilon \cup B_\varepsilon. \end{array}$$

Soit $(A_\emptyset, B_\emptyset, C_\emptyset, D_\emptyset, E_\emptyset)$ une partition quelconque de ω en parties contenant des segments d'entiers arbitrairement longs.

Supposons $(A_\varepsilon, B_\varepsilon, C_\varepsilon, D_\varepsilon, E_\varepsilon)$ construit.
On construit $(A_{\varepsilon\frown 0}, B_{\varepsilon\frown 0}, C_{\varepsilon\frown 0}, D_{\varepsilon\frown 0}, E_{\varepsilon\frown 0})$ de la manière suivante : on pose $A_{\varepsilon\frown 0} = A_\varepsilon \cup C_\varepsilon \cup E_\varepsilon$. On fait une partition de D_ε en quatre parties $D_\varepsilon \cap \{0,\dots,l(\varepsilon)\}$, C, D, E telles que C, D, E contiennent des segments d'entiers arbitrairement longs.

On pose $B_{\varepsilon\frown 0} = B_\varepsilon \cup (D_\varepsilon \cap \{0,\dots,l(\varepsilon)\})$, $C_{\varepsilon\frown 0} = C$, $D_{\varepsilon\frown 0} = D$ et $E_{\varepsilon\frown 0} = E$.
On construit de manière équivalente $(A_{\varepsilon\frown 1}, B_{\varepsilon\frown 1}, C_{\varepsilon\frown 1}, D_{\varepsilon\frown 1}, E_{\varepsilon\frown 1})$.

Pour tout $\alpha \in 2^\omega$ on définit

$$O_\alpha = \bigcup_{n \in \omega} B_{\alpha_{|n}} = \omega \setminus (\bigcup_{n \in \omega} A_{\alpha_{|n}}).$$

Si $\alpha < \beta$ alors il existe $\varepsilon \in 2^{<\omega}$, α' et β' tels que $\alpha = \varepsilon \frown 0 \frown \alpha'$ et $\beta = \varepsilon \frown 1 \frown \beta'$. Alors

$$O_\alpha \subseteq \omega \setminus A_{\varepsilon \frown 0} = B_\varepsilon \cup D_\varepsilon \subset B_\varepsilon \cup D_\varepsilon \cup E_\varepsilon = B_{\varepsilon \frown 1} \subseteq O_\beta.$$

Donc $O_\beta \setminus O_\alpha$ contient E_ε qui, lui, contient des segments d'entiers arbitrairement longs. $\lhd$

$\rhd$ **Construction 3.4.15**

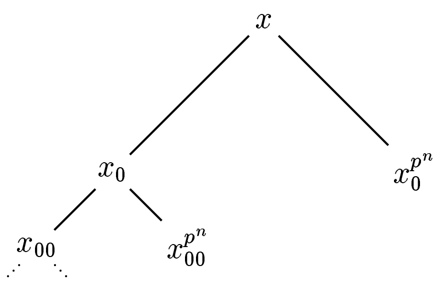
Soit pour tout $\alpha \in 2^\omega$, ϕ_α la fonction qui à n associe 1 si $n \in O_\alpha$ et 0 sinon.

Montrons que les groupes G_{ϕ_α} sont deux à deux orthogonaux. Supposons pour $\alpha < \beta$ que G_{ϕ_β} est non orthogonal à G_{ϕ_α}. Alors il existe n et k tels que pour tout i, $\deg(G_{\phi_\beta})(i) \leq k \cdot \deg(G_{\phi_\alpha})(i+n)$ (3.4.9). Soit m un entier tel que $p^m > kp^{2n}$. Il existe un entier j tel que $O_\beta \setminus O_\alpha$ contient plus de m entiers strictement inférieurs à j. Alors $\deg(G_{\phi_\beta})(j) \geq p^m \cdot \deg(G_{\phi_\alpha})(j)$ car si $x = x_0^p + x_0^p b$, alors $[K(x_0) : K(x)] = p$ et si $x = x_0^p + x_0^{p^2} b$, alors $[K(x_0) : K(x)] = p^2$. De même $\deg(G_{\phi_\alpha})(j+n) \leq p^{2n} \deg(G_{\phi_\alpha})(j)$. Donc $\deg(G_{\phi_\beta})(j) > k \cdot \deg(G_{\phi_\alpha})(j+n)$ car $p^m > kp^{2n}$. $\lhd$

3.4.5 Anneaux d'endomorphismes de sous-groupes minimaux additifs localement modulaires

Étudions maintenant les anneaux d'endomorphismes de certaines classes de sous-groupes minimaux additifs définis sur le vide et leurs endomorphismes définissables. Nous utilisons pour cela le fait que tout endomorphisme définissable se prolonge à $(L, +)$ (3.4.4).

Soient n un entier et ϕ l'application constante à n. Nous rappelons que G_n est le groupe G_ϕ.



Groupe G_n

Nous étudions l'anneau des endomorphismes des groupes G_n pour $n > 0$.

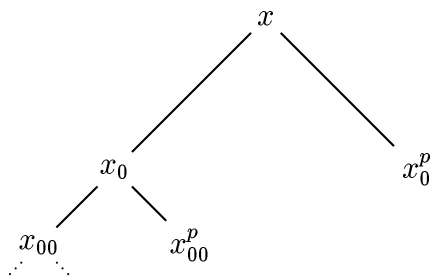
Proposition 3.4.17. *L'anneau des endomorphismes de G_1 définissables sur K est égal à*

$$\mathbb{F}_p\{f_{0|G_1}, f_{0|G_1}^{-1}\} \simeq \mathbb{F}_p[X, X^{-1}].$$

Plus généralement pour tout entier $n \geq 1$,

$$\mathrm{End}_K(G_n) = \mathbb{F}_{p^n}\{f_{0|G_n}, f_{0|G_n}^{-1}\}$$

▷ La preuve est identique quelque soit n. Pour simplifier les notations nous nous contentons d'écrire celle pour G_1. Rappelons que G_1 est défini par les relations suivantes : pour tout $n \in \omega$, $x_{\bar{0}(n)} = x^p_{\bar{0}(n+1)} + bx^{p^2}_{\bar{0}(n+1)}$ (où $b = b_0$ est le premier élément de la p-base et pour tout n, $x_{\bar{0}(n)} = f_0^n(x)$).



Groupe G_1

L'application f_0 restreint à G_1 définit un isomorphisme. Son inverse est l'application qui à x associe $x^p + bx^{p^2}$. En effet $x = x_0^p + bx_0^{p^2} \in G_1$ si et seulement si $x_0 \in G_1$.

Soit g un endomorphisme définissable sur K de G_1. Par (3.4.7 et 3.3.1) il existe P un p-polynôme de $K[X_\infty]$ tel que pour tout $x \in G_1$, $g(x) = P(x_\infty)$. Par la définition de G_1 on peut supposer que P est un p-polynôme de $K[X_{\bar{0}(n)}]$ pour un certain n. D'où $g(x) = P(f_0^n(x))$. Ainsi l'application qui à x associe $P(x)$ est un endomorphisme de G_1.

On s'est donc ramené à un endomorphisme h défini par $h(x) = \sum_{j=0}^m a_j x^{p^j}$. avec $a_j \in K$.

On reprend les notations (3.1.2). Dans ce qui suit on a donc, $a_{0,0} = f_0(a_0)$, $a_{0,1} = f_1(a_0)$, $a_{0,p-1} = f_{p-1}(a_0)$ et plus généralement pour tout $j \in \{0, \ldots, m\}$ et $i < p^\nu$, $a_{j,i} = f_i(a_j)$.

Pour tout $x \in G_1$ on a :

$$\begin{aligned} h(x) &= (a^p_{0,0} + a^p_{0,1}b + \ldots + a^p_{0,p-1}b^{p-1} + \ldots)(x_0^p + x_0^{p^2}b) + \sum_{j=1}^{m}(\sum_{i\in p^\nu} a^p_{j,i}m_i)(x^{p^{j-1}})^p \\ &= (a_{0,0}x_0 + a_{0,p-1}bx_0^p)^p + (a_{0,1}x_0 + a_{0,0}x_0^p)^p b + \ldots + \sum_{i\in p^\nu}\left(\sum_{j=1}^{m}(a_{j,i}x^{p^{j-1}})\right)^p m_i. \end{aligned}$$

Donc pour tout $x \in G_1$,

$$\begin{aligned}(h(x))_0 &= a_{0,0}x_0 + a_{0,p-1}bx_0^p + \sum_{j=1}^{m} a_{j,0}x^{p^{j-1}},\\ (h(x))_1 &= a_{0,1}x_0 + a_{0,0}x_0^p + \sum_{j=1}^{m} a_{j,1}x^{p^{j-1}}.\end{aligned}$$

Par ailleurs comme h est un endomorphisme de G_1, pour tout $x \in G_1$,

$$\begin{aligned}(h(x))_1 &= (h(x))_0^p, \text{ et}\\ (h(x))_i &= 0 = a_{0,i}x_0 + \text{ termes en } x_0^p \text{ et en } x^{p^j}, \text{ pour } 1 < i < p^\nu.\end{aligned}$$

Pour $i > 1$, en remplaçant x par $x_0^p + bx_0^{p^2}$ dans l'équation $(h(x))_i = 0$, on obtient $a_{0,i} = 0$. De même $a_{0,1} = 0$ car $a_{0,1}x_0$ est le seul terme en x_0 dans l'égalité $(h(x))_1 = (h(x))_0^p$. (On a des équations polynomiales en x_0 ayant une infinité de solutions.)

En considérant à nouveau cette égalité on obtient

$$0 = (a_{0,0} - a_{0,0}^p)x_0^p + \text{ termes en } x^{p^j} \text{ pour } 0 \le j \le m.$$

On en déduit que les termes en x sont nuls (car $x = x_0^p + bx_0^{p^2}$) et donc que $a_{0,0} = a_{0,0}^p$. D'où $a_0 \in \mathbb{F}_p$.

On peut donc se ramener à un degré inférieur en considérant l'application qui à x associe $f_0(h(x) - a_0x)$. $\lhd$

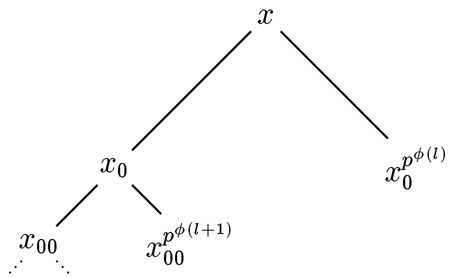
Remarque. Il existe un groupe G localement modulaire minimal tel que son anneau d'endomorphismes est égal à $\mathbb{F}_p\{f_{1|G}, f_{1|G}^{-1}\}$. Pour cela il suffit de prendre le "symétrique" de G_1 : $\{x;\ x_{\bar{1}(n)} = x_{\bar{1}(n+1)}^{p^2} + bx_{\bar{1}(n+1)}^p\}$.

Nous donnons maintenant une classe d'exemples dont l'anneau des endomorphismes est réduit à $\mathbb{F}_p$.

Proposition 3.4.18. *Soit ϕ une application injective de ω dans $\omega \setminus \{0\}$ tel que pour tout entier n il existe un entier $m > n$ tel que $\phi(n)$ et $\phi(m)$ sont premiers entre eux. (Les applications strictement croissantes de ω dans l'ensemble des nombres premiers vérifient ces propriétés.) Alors l'anneau $\mathrm{End}_K(G_\phi)$ des endomorphismes de G_ϕ définissables sur K est réduit à $\mathbb{F}_p$.*

De même pour tout $n > 0$, $\mathrm{End}_K(G_{n\phi}) = \mathbb{F}_{p^n}$.

Nous décomposons la preuve en petits lemmes. Pour tout $l \in \omega$, nous notons $\phi + l$ l'application qui à n associe $\phi(n + l)$ (ces applications vérifient aussi les hypothèses de la proposition). Pour tout $l \in \omega$, le groupe $G_{\phi+l}$ est égal à $f_{\bar{0}(l)}(G_\phi)$



Groupes $G_{\phi+l}$

Lemme 3.4.19. *Soit g un endomorphisme de G_ϕ défini par $g(x) = \sum_{j=0}^m a_j x^{p^j}$. Alors $a_0 \in \mathbb{F}_p$.*

$\triangleright$ On fait le même type de raisonnement que dans la preuve précédente (3.4.17) et on utilise les mêmes notations (3.1.2) : pour tout $x \in G_\phi$ on a :

$$\begin{array}{rcl}
(g(x))_0 & = & a_{0,0}x_0 + a_{0,p-1}bx_0^{p^{\phi(0)}} + \sum_{j=1}^m a_{j,0}x^{p^{j-1}}, \\
(g(x))_1 & = & a_{0,1}x_0 + a_{0,0}x_0^{p^{\phi(0)}} + \sum_{j=1}^m a_{j,1}x^{p^{j-1}}, \\
(g(x))_i & = & 0 = a_{0,i}x_0 + \text{ termes en } x_0^{p^{\phi(0)}} \text{ et en } x^{p^j}, \text{ pour } 1 < i < p^\nu, \text{ et} \\
(g(x))_1 & = & (g(x))_0^{p^{\phi(0)}}.
\end{array}$$

En remplaçant x par $x_0^p + bx_0^{p^{\phi(0)+1}}$, on en déduit de la même manière que dans la proposition 3.4.17 que $a_{0,1} = 0$ et $a_{0,i} = 0$ pour $i > 1$ et que $a_{0,0} = a_{0,0}^{p^{\phi(0)}}$. D'où $a_0 \in \mathbb{F}_{p^{\phi(0)}}$.

En composant g par f_0 on peut considérer un endomorphisme de $G_{\phi+1}$ défini par un p-polynôme de $K[x_0]$ dont le coefficient en x_0 est $a_{0,0}$. Alors $a_{0,0} \in \mathbb{F}_{p^{\phi(1)}}$, d'où $a_0 \in \mathbb{F}_{p^{\phi(1)}}$. En itérant nous montrons que pour tout entier n, $a_0 \in \mathbb{F}_{p^{\phi(n)}}$. Comme il existe un entier n tel que $\phi(0)$ et $\phi(n)$ sont premiers entre eux, on a $a_0 \in \mathbb{F}_p$. $\triangleleft$

Lemme 3.4.20. *Soit $l > 0$ et g un homomorphisme de $G_{\phi+l}$ dans G_ϕ défini par $g(x) = \sum_{j=0}^m a_j x^{p^j}$. Alors $a_0 = 0$.*

▷ Pour tout $x \in G_{\phi+l}$ on a :

$$\begin{aligned}
(g(x))_0 &= a_{0,0}x_0 + a_{0,p-1}bx_0^{p^{\phi(l)}} + \sum_{j=1}^{m} a_{j,0}x^{p^{j-1}}, \\
(g(x))_1 &= a_{0,1}x_0 + a_{0,0}x_0^{p^{\phi(l)}} + \sum_{j=1}^{m} a_{j,1}x^{p^{j-1}}, \\
(g(x))_i &= 0 = a_{0,i}x_0 + \text{ termes en } x_0^{p^{\phi(l)}} \text{ et en } x^{p^j}, \text{ pour } 1 < i < p^\nu, \text{ et} \\
(g(x))_1 &= (g(x))_0^{p^{\phi(0)}}.
\end{aligned}$$

En remplaçant x par $x_0^p + bx_0^{p^{\phi(l)+1}}$, on en déduit toujours de la même façon que $a_{0,1} = 0$ et $a_{0,i} = 0$ pour $i > 1$.

On considère à nouveau l'égalité $(g(x))_1 = (g(x))_0^{p^{\phi(0)}}$. Cela donne :

$$a_{0,0}x_0^{p^{\phi(l)}} + \sum_{j=1}^{m} a_{j,1}x^{p^{j-1}} = a_{0,0}^{p^{\phi(0)}} x_0^{p^{\phi(0)}} + \sum_{j=1}^{m} a_{j,0}^{p^{\phi(0)}} x^{p^{j-1+\phi(0)}}.$$

On remplace x par $x_0^p + bx_0^{p^{\phi(l)+1}}$ et on ne garde que les termes en $x_0^{p^{\phi(0)+t\phi(l)}}$:

$$\begin{aligned}
&\sum_{t\geq 0} a_{\phi(0)+t\phi(l),1}(x_0^{p^{\phi(0)+t\phi(l)}} + b^{p^{\phi(0)+t\phi(l)-1}} x_0^{p^{\phi(0)+(t+1)\phi(l)}}) \\
&= a_{0,0}^{p^{\phi(0)}} x_0^{p^{\phi(0)}} + \sum_{t\geq 1} a_{t\phi(l),0}^{p^{\phi(0)}}(x_0^{p^{\phi(0)+t\phi(l)}} + b^{p^{\phi(0)+t\phi(l)-1}} x_0^{p^{\phi(0)+(t+1)\phi(l)}}).
\end{aligned}$$

(Comme $\phi(l) \neq \phi(0) \neq 0$ le terme $a_{0,0}x_0^{p^{\phi(l)}}$ n'apparaît pas.) On a donc une équation polynomiale du type suivant :

$$a_{0,0}^{p^{\phi(0)}} x_0^{p^{\phi(0)}} + \sum_{t\geq 0} c_t(x_0^{p^{\phi(0)+t\phi(l)}} + b^{p^{\phi(0)+t\phi(l)-1}} x_0^{p^{\phi(0)+(t+1)\phi(l)}}) = 0.$$

Ainsi tous les c_t sont nuls et donc $a_{0,0}$ est nul.

D'où $a_0 = 0$. ◁

Lemme 3.4.21. *Soit $l > 0$ et g un homomorphisme de G_ϕ dans $G_{\phi+l}$ défini par $g(x) = \sum_{j=0}^{m} a_j x^{p^j}$. Alors $a_0 = 0$.*

▷ La preuve est analogue au lemme précédent. Pour tout $x \in G_\phi$ on a :

$$\begin{aligned}
(g(x))_0 &= a_{0,0}x_0 + a_{0,p-1}bx_0^{p^{\phi(0)}} + \sum_{j=1}^{m} a_{j,0}x^{p^{j-1}}, \\
(g(x))_1 &= a_{0,1}x_0 + a_{0,0}x_0^{p^{\phi(0)}} + \sum_{j=1}^{m} a_{j,1}x^{p^{j-1}}, \\
(g(x))_i &= 0 = a_{0,i}x_0 + \text{ termes en } x_0^{p^{\phi(0)}} \text{ et en } x^{p^j} \text{ pour } 1 < i < p^\nu \text{ et} \\
(g(x))_1 &= (g(x))_0^{p^{\phi(l)}}.
\end{aligned}$$

En remplaçant x par $x_0^p + bx_0^{p^{\phi(0)+1}}$, on en déduit que $a_{0,1} = 0$ et $a_{0,i} = 0$ pour $i > 1$.

On considère à nouveau l'égalité $(g(x))_1 = (g(x))_0^{p^{\phi(l)}}$. Cela donne

$$a_{0,0}x_0^{p^{\phi(0)}} + \sum_{j=1}^{m} a_{j,1}x^{p^{j-1}} = a_{0,0}^{p^{\phi(l)}} x_0^{p^{\phi(l)}} + \sum_{j=1}^{m} a_{j,0}^{p^{\phi(l)}} x^{p^{j-1+\phi(l)}}.$$

On remplace x par $x_0^p + bx_0^{p^{\phi(0)+1}}$ et on ne garde que les termes en $x_0^{p^{\phi(l)+t\phi(0)}}$. On obtient alors le même type d'égalité que dans le lemme précédent. On en déduit de même que $a_{0,0} = 0$ donc que $a_0 = 0$. ◁

Corollaire 3.4.22. *Soit $l \geq 0$ et g un homomorphisme de G_ϕ dans $G_{\phi+l}$ défini par $g(x) = \sum_{j=1}^{m} a_j x^{p^j}$. Alors $g = 0$.*

▷ Supposons g non nul. Soit $k > 0$ minimal tel que $a_k \neq 0$. On montre par récurrence sur k que $a_k = 0$ (contradiction).

Toujours par le même type d'équation on a $a_{k,i} = 0$ pour $i > 0$. En considérant $f_0 \circ g$ on obtient un homomorphisme de G_ϕ dans $G_{\phi+l+1}$. On a $(g(x))_0 = \sum_{j=k}^{m} a_{j,0}x^{p^{j-1}}$ qui est un p-polynôme en x. Si $k > 1$ on utilise l'hypothèse de récurrence et on a donc $a_{k,0} = 0$ d'où $a_k = 0$. Si $k = 1$ on conclut de même avec le lemme précédent. ◁

▷ **Preuve de la proposition 3.4.18**

Soit g un endomorphisme définissable sur K de G_ϕ. De même que pour G_1, par (3.4.7 et 3.3.1) il existe un entier n et un p-polynôme P de $K[X_{\bar{0}(n)}]$ tel que $g(x) = P(x_{\bar{0}(n)})$. On montre tout d'abord avec le lemme 3.4.20 que l'application qui à $x_{\bar{0}(n)}$ associe $f_0^n \circ P(x_{\bar{0}(n)})$, endomorphisme de $G_{\phi+n}$, est défini par un p-polynôme de $K[X_{\bar{0}(n)}]$.

En effet si $n > 0$, en considérant l'homomorphisme de $G_{\phi+n}$ dans G_ϕ défini par P, on a $P \in K[X_{\bar{0}(n)}^p]$ (3.4.20). D'où l'application qui à $x_{\bar{0}(n)}$ associe $f_0 \circ P(x_{\bar{0}(n)})$ est définie par un p-polynôme de $K[X_{\bar{0}(n)}]$. En itérant n fois on obtient le résultat ci-dessus.

On obtient donc un endomorphisme de $G_{\phi+n}$ défini par un p-polynôme de $K[X_{\bar{0}(n)}]$. Maintenant en utilisant le lemme 3.4.19 ce dernier p-polynôme est de la forme $aX_{\bar{0}(n)} + R[X_{\bar{0}(n)}]$ avec $a \in \mathbb{F}_p$ et $R \in K[X_{\bar{0}(n)}^p]$. L'application qui à $x_{\bar{0}(n)}$ associe $R(x_{\bar{0}(n)})$ est alors un endomorphisme de $G_{\phi+n}$ et par (3.4.22) $R = 0$. Donc que pour tout $x \in G_\phi$, $f_0^n \circ P(x_{\bar{0}(n)}) = ax_{\bar{0}(n)}$.

Maintenant pour tout $x \in G_\phi$, $x = Q(x_{\bar{0}(n)})$ pour un certain p-polynôme Q de $K[X]$. D'où $g(x) = Q(ax_{\bar{0}(n)}) = aQ(x_{\bar{0}(n)}) = ax$.

La preuve est identique pour les groupes $G_{n\phi}$. ◁

Par (3.4.8), tout sous-groupe minimal localement modulaire a nécessairement un corps d'endomorphismes scalaires fini. Réciproquement :

Corollaire 3.4.23. *Pour tout $n > 0$, il existe $2^{\aleph_0}$ sous- groupes additifs minimaux définis sur $\emptyset$, de rang de transcendance 1 et localement modulaires, deux à deux orthogonaux tels que leur anneau d'endomorphismes définissables sur K est égal à $\mathbb{F}_{p^n}$.*

▷ Il suffit de choisir deux suites de nombres premiers tous distincts (p_n) et (q_n) telles que $q_n \geq 2n + \sum_{i \leq 2n} p_i$.

Soit pour tout $\alpha \in 2^\omega$, ψ_α l'application qui à n associe q_n si $n \in O_\alpha$ et p_n sinon. (O_α est la famille de parties de ω définie dans le lemme 3.4.16.)

Montrons que les groupes G_{ψ_α} sont deux à deux orthogonaux.

Supposons pour $\alpha < \beta$ que G_{ψ_β} est non orthogonal à G_{ψ_α}. Alors il existe n et k tels que pour tout i, $\deg(G_{\psi_\beta})(i) \leq k \cdot \deg(G_{\psi_\alpha})(i+n)$ (3.4.9). Soit $m > n$ un entier tel que $p^m > k$. Il existe un entier $j \geq m$ tel que $\{j, \ldots, j+n\} \subset O_\beta \setminus O_\alpha$. Alors

$$\begin{aligned}
\deg(G_{\psi_\beta})(j+1) &= \deg(G_{\psi_\beta})(j) \cdot p^{1+q_j} \\
&\geq \deg(G_{\psi_\alpha})(j) \cdot p^m \cdot p^{n+1} \cdot \prod_{j \leq l \leq j+n} p^{p_l} \\
&= p^m \cdot \deg(G_{\psi_\alpha})(j) \cdot \prod_{j \leq l \leq j+n} p^{\psi_\alpha(l)+1} \\
&= p^m \cdot \deg(G_{\psi_\alpha})(j+n+1) > k \cdot \deg(G_{\psi_\alpha})(j+n+1).
\end{aligned}$$

De même pour tout $n > 0$, les groupes $G_{n\psi_\alpha}$ sont deux à deux orthogonaux.

Par (3.4.18), pour tout α et $n > 0$, l'anneau des endomorphismes définissables de $G_{n\psi_\alpha}$ est égal à F_{p^n}. ◁

Remarque. Dans ces exemples K n'a pas d'influence sur les endomorphismes définissables. Ceci vient du fait que tout sous-groupe connexe et en particulier tout endomorphisme définissable d'un groupe minimal localement modulaire définissable sur $\emptyset$ est $\mathrm{acl}^{eq}(\emptyset)$-définissable (1.3.2 iv).

Proposition 3.4.24. *Il existe un sous-groupe additif minimal localement modulaire et un sous-groupe additif minimal non localement modulaire qui ont même anneau d'endomorphismes définissables sur K.*

▷ C'est un corollaire de (3.4.23) et (3.4.3). ◁

Nous terminons cette section en indiquant deux questions ouvertes :

Question 3.4.25. En utilisant la construction de [CW 99] peut-on obtenir un groupe minimal de degré de transcendance infini n'ayant comme endomorphismes que les éléments de $\mathbb{F}_p$?

L'étude de la classe suivante de groupe ainsi que le lemme 3.4.27 ont été suggérés par T. Scanlon.

Soit $\theta \in K\{\alpha\}$. On définit

$$\theta^\sharp := \bigcap_{n \in \omega} \theta^n(L).$$

On suppose que $\theta = \sum_{i \geq 1} a_i \alpha^i$. Sinon pour tout $l \in L$, $P_\theta - l$ est séparable, donc $\theta(L) = L$ et dans ce cas $\theta^\sharp = L$.

Alors $\theta^\sharp$ est de rang de transcendance 1 : en effet pour tout $x \in \theta^\sharp$ et $n \in \omega$, il existe y tel que $x = \theta^n(y)$ et donc $K(x_{\leq n}) \subseteq K(y)$. D'où pour tout n, $\mathrm{RT}(x_{\leq n}/K) \leq 1$.

T. Scanlon a posé la question suivante :

Question 3.4.26 (de T. Scanlon). Soit θ tel que $\theta^\sharp$ est localement modulaire. A-t-on pour tout r quasi-endomorphisme de $\theta^\sharp$, une puissance de θ qui commute avec r ?

Remarque. Soit $n \in \omega$. Le groupe G_n est égal à $\theta_n^\sharp$ pour $\theta_n = \alpha + b\alpha^{n+1}$.

Les groupes G_n permettent de voir que θ ne commute pas nécessairement avec tous les endomorphismes définissables. En effet, tout $n \geq 2$, par (3.4.17),

$$\mathrm{End}_K(\theta_n^\sharp) = \mathbb{F}_{p^n}\{\theta_n, \theta_n^{-1}\}$$

et donc si $a \in \mathbb{F}_{p^n}$ alors $\theta_n \circ a = a^p \circ \theta_n$. Mais en revanche, θ_n^n lui commute avec tous les endomorphismes.

Terminons par une caractérisation des groupes localement modulaires de la forme $\theta^\sharp$.

Lemme 3.4.27. *Si $\theta^\sharp$ est minimal alors $\theta^\sharp$ est non localement modulaire si et seulement si il existe $a \in K^*$ tel que $a^{-1}\theta a \in K^p\{\alpha\}$.*

$\triangleright$ S'il existe $a \in K^*$ tel que $a^{-1}\theta a \in K^p\{\alpha\}$ alors $(a^{-1}\theta a)(L) \subseteq L^p$ d'où $(a^{-1}\theta a)^\sharp \subseteq L^{p^\infty}$ et par minimalité de L^{p^∞}, $(a^{-1}\theta a)^\sharp = L^{p^\infty}$. On conclut car $\theta^\sharp = a(a^{-1}\theta a)^\sharp$.

Sinon, soit $x \in \theta^\sharp$ et $y \in \theta^\sharp$ tel que $x = \theta(y)$. Soit N tel que $\deg P_\theta = p^N$. Si x est transcendant sur K alors y aussi et on a $[K(y) : K(x)] = \deg P_\theta = p^N$.

On va d'abord montrer qu'il existe R un p-polynôme de $K[Y]$ de degré inférieur ou égal à p^{N-2} tel que $R(y) \in K[x_{\leq 1}]$. En effet pour tout $i \in p^\nu$, $x_i = \theta_i(y)$ avec $\deg P_{\theta_i} \leq p^{N-1}$.

Ou bien il existe i tel que $\theta_i \neq 0$ et $\deg P_{\theta_i} < p^{N-1}$. Dans ce cas on pose $R = P_{\theta_i}$.

Ou bien pour tout i, $\deg P_{\theta_i} = p^{N-1}$ ou $\theta_i = 0$. Alors il existe deux P_{θ_i} non colinéaires (et une combinaison de ces deux polynômes donne R). Sinon il existerait i_0 et des $c_i \in K$ tels que pour tout i, $\theta_i = c_i\theta_{i_0}$. Dans ce cas il existe $c \in K$ tel que $\theta = c\alpha\theta_{i_0}$. En prenant $a \in K$ tel que $a^{p-1} = c^{-1}$, on a alors $a^{-1}\theta a = \alpha\theta'$ d'où $a^{-1}\theta a \in K^p\{\alpha\}$.

On a donc

$$R(Y) = \sum_{i=n_0}^{N-2} d_i Y^{p^i}.$$

On peut supposer que $d_{n_0} = 1$. En considérant

$$S(Y) = \sum_{i=n_0}^{N-2} d_{i,\bar{0}(n_0)} Y^{p^{i-n_0}},$$

on obtient que $S(y) \in K[x_{\leq n_0+1}]$ d'où $[K(x_{\leq n_0+1}, y) : K(x_{\leq n_0+1})] \leq p^{N-n_0-2}$ et pour tout $m \in \omega$, $y_{\leq m} \in K[x_{\leq n_0+1+m}, y]$.

On peut remarquer que n_0 ne dépend pas du choix de x.

On montre par récurrence sur $m \in \omega$ que $[K(x_{\leq m(n_0+1)}) : K(x)] \geq p^{m(n_0+2)}$ pour tout $x \in \theta^\sharp$ tel que $\mathrm{RT}(x/K) = 1$.

Pour $m = 0$ il n'y a rien à montrer.

On suppose le résultat vrai pour m. Soit $x \in \theta^\sharp$ tel que $\mathrm{RT}(x/K) = 1$. Il existe $y \in \theta^\sharp$ tel que $\theta(y) = x$.

Alors y est aussi transcendant sur K. On peut donc appliquer l'hypothèse de récurrence à y. Donc
$$[K(y_{\leq m(n_0+1)} : K(y)] \geq p^{m(n_0+2)}.$$
D'après ce qui précède, $y_{\leq m(n_0+1)} \in K[x_{\leq (m+1)(n_0+1)}, y]$. D'où
$$[K(x_{\leq (m+1)(n_0+1)}, y) : K(y)] \geq p^{m(n_0+2)}$$
et donc
$$[K(x_{\leq (m+1)(n_0+1)}, y) : K(x)] \geq p^{N+m(n_0+2)}.$$
On a aussi,
$$[K(x_{\leq (m+1)(n_0+1)}, y) : K(x_{\leq (m+1)(n_0+1)})] \leq p^{N-n_0-2}$$
d'où
$$[K(x_{\leq (m+1)(n_0+1)}) : K(x)] \geq p^{(m+1)(n_0+2)}.$$
Par (3.4.9), on conclut. En effet si pour $x \in \theta^\sharp$ tel que $\mathrm{RT}(x/K) = 1$, le type de x n'était pas orthogonal à L^{p^∞} alors il existerait $k \in \omega$ tel que $[K(x_{\leq n}) : K(x)] \leq kp^n$. Ce qui est impossible d'après ce qui précède. $\lhd$

3.5 Quasi-endomorphismes

Dans cette partie L est à nouveau un modèle fixé de $T_{p,\nu}$ et $k_0 \preccurlyeq K \preccurlyeq L$ sont des sous-structures élémentaires de L. De plus nous supposons L $|K|^+$-saturé. Les sous-groupes additifs seront supposés définissables sur k_0 (en général $k_0 = \mathbb{F}_p(B)^{sep}$) et les quasi-endomorphismes définissables sur K. Rappelons que dans le cas d'un sous-groupe minimal localement modulaire définissable sur k_0, tout quasi-endomorphisme définissable sur K l'est sur k_0 (1.3.5).

La notion de quasi-endomorphisme (1.3.4) se généralise aux groupes abéliens stables $\bigwedge$-définissables et dans ce cadre l'ensemble des quasi-endomorphismes est toujours muni d'une structure d'anneau (qui n'est pas nécessairement un corps) [Wa 97, Bu 96].

Dans le paragraphe qui suit, nous considérons uniquement les quasi-endomorphismes de groupes abéliens stables connexes $\bigwedge$-définissables et nous écrivons une preuve (nous n'en avons pas trouvé dans la littérature) du fait que les anneaux de quasi-endomorphismes sont stables par isogénie définissable (3.5.2).

Nous en déduisons que tout sous-groupe additif définissable connexe a un anneau de quasi-endomorphismes qui s'exprime simplement en fonction de l'anneau des quasi-endomorphismes de $(L, +)$ (3.5.5). De plus comme les sous-groupes minimaux additifs non localement modulaires sont définissablement isogènes à $(L^{p^\infty}, +)$ (3.1.25), nous en déduisons qu'ils ont même corps de quasi-endomorphismes et que l'on peut voir la locale modularité sur ce corps (3.5.9).

D'autre part nous montrons que tout quasi-endomorphisme d'un sous-groupe connexe $\bigwedge$-définissable de $(L,+)$ est la trace d'un quasi-endomorphisme de $(L,+)$ (3.5.6).

Nous construisons ensuite un sous-groupe additif minimal localement modulaire dont le corps de quasi-endomorphismes n'est pas un corps de fractions de l'anneau des endomorphismes définissables (3.5.16). Nous terminons par une construction de $2^{\aleph_0}$ sous-groupes minimaux additifs définis sur le vide et de rang de transcendance 1 dont le corps de quasi-endomorphismes est $\mathbb{F}_p$ et dont la structure induite est exactement la structure correspondante de $\mathbb{F}_p$-espace vectoriel et est donc $\aleph_0$-catégorique (3.5.20).

3.5.1 Isogénies

On se place dans une structure M stable et saturée et on fixe un ensemble de paramètres A de cardinal strictement inférieur à celui de M. Dans toute la suite de cette sous-section, les définissables (resp. les $\bigwedge$-définissables) seront supposés définissables (resp. $\bigwedge$-définissables) sur $\mathrm{acl}^{eq}(A)$.

On fixe deux groupes abéliens G et H $\bigwedge$-définissables connexes. Comme M est stable ils sont intersections de groupes définissables.

L'hypothèse supplémentaire de connexité permet de donner une définition des quasi-endomorphismes (équivalente à celles données dans [Wa 97] ou [Bu 96])) qui n'utilise pas de relation d'équivalence :

Définition 3.5.1. Un sous-groupe S relativement définissable de $G \times H$ est un quasi-homomorphisme de G dans H si l'image de la projection de S sur G, $\pi_1(S)$, est G, si le conoyau de S ($\mathrm{coker}(S) = \{y \in H;\ (0,y) \in S\}$) est fini et si S est connexe.

Un quasi-endomorphisme de G est un quasi-homomorphisme de G dans G.

On note $\mathrm{QsH}(G,H)$ l'ensemble des quasi-homomorphismes de G dans H et $\mathrm{QsE}(G)$ l'ensemble des quasi-endomorphismes de G.

Les ensembles $\mathrm{QsH}(G,H)$ et $\mathrm{QsE}(G)$ sont munis respectivement d'une structure de groupe et d'une structure d'anneau par les opérations $+^0$ et $*^0$ que l'on peut définir de la manière suivante dans notre cadre (et que nous notons différemment de l'addition et multiplication usuelles afin de ne pas les confondre avec l'addition et la multiplication de sous-groupes) :

Définition. On définit les opérations $+^1$ et $+^0$ sur les sous groupes de $G \times H$, de la manière suivante : $S +^1 T := \{(x,y) \in (G,H);\ \exists y_1 y_2\ (y = y_1 + y_2) \wedge ((x,y_1) \in S) \wedge ((x,y_2) \in T)\}$ et $S +^0 T := (S +^1 T)^0$ (la composante connexe de $(S +^1 T)$).

On définit les opérations $*^1$ et $*^0$ sur les sous-groupes de $G \times G$, de la manière suivante : $S *^1 T := \{(x,z) \in (G,G);\ \exists y\ ((x,y) \in S) \wedge ((y,z) \in T)\}$ et $S *^0 T := (S *^1 T)^0$.

Nous vérifions maintenant que les isogénies définissent des isomorphismes entre les anneaux de quasi-endomorphismes :

Proposition 3.5.2. *Soient G, G', H et H' quatre groupes $\bigwedge$-définissables et connexes. Si G est définissablement isogène à G' et si H est définissablement isogène à H' alors les groupes* $\mathrm{QsH}(G,H)$ *et* $\mathrm{QsH}(G',H')$ *sont isomorphes et les anneaux* $\mathrm{QsE}(G)$ *et* $\mathrm{QsE}(G')$ *sont isomorphes.*

$\triangleright$ Soient ϕ une isogénie définissable de G sur G' et ψ une isogénie définissable de H sur H'. Montrons que (ϕ, ψ) induit un isomorphisme de groupes entre $\mathrm{QsH}(G, H)$ et $\mathrm{QsH}(G', H')$ et que (ϕ, ϕ) induit un isomorphisme d'anneaux entre $\mathrm{QsE}(G)$ et $\mathrm{QsE}(G')$. Soient $S \in \mathrm{QsH}(G, H)$ et $T := (\phi, \psi)(S)$. Vérifions que $T \in \mathrm{QsH}(G', H')$. Comme *phi* est une isogénie, $\pi_1(T) = G'$. De plus

$$\mathrm{coker} T = \{t \in H';\ \exists (x, y) \in G \times H\ \phi(x) = 0 \wedge t = \psi(y)\}.$$

Donc $\mathrm{coker}T$ est fini puisque $\ker \phi$ et $\mathrm{coker}S$ sont fini. Montrons que T est connexe : soient U d'indice fini dans T et $V := (\phi, \psi)^{-1}(U) := \{(x, y);\ (\phi(x), \psi(y)) \in U\}$. On voit facilement que $V \cap S$ est d'indice fini dans S. Comme S est connexe, $S \subseteq V$ et donc $T = U$.

La fonction (ϕ, ψ) induit donc une application de $\mathrm{QsH}(G, H)$ dans $\mathrm{QsH}(G', H')$.

Pour S et T sous-groupes de $G \times H$, il est simple de vérifier que $(\phi, \psi)(S +^1 T) = ((\phi, \psi)(S)) +^1 ((\phi, \psi)(T))$.

Supposons de plus S et T dans $\mathrm{QsH}(G, H)$, alors

$$(\phi, \psi)(S +^0 T) = ((\phi, \psi)(S +^1 T))^0 = ((((\phi, \psi)(S)) +^1 ((\phi, \psi)(T)))^0.$$

Donc (ϕ, ψ) est un homomorphisme de groupes.

Soit $S \in \mathrm{QsH}(G, H)$. Si $(\phi, \psi)(S) = G' \times \{0\}$ alors $S \subseteq G \times \ker \psi$ d'où $S = G \times \{0\}$. Donc le noyau de cet homomorphisme est réduit à 0.

Soit $T \in \mathrm{QsH}(G', H')$. Soit $U = (\phi, \psi)^{-1}(T)$ alors $\pi_1(U) = G$, $\mathrm{coker}U$ est fini et $(\phi, \psi)(U^0) = T$.

Donc (ϕ, ψ) induit un isomorphisme de groupe de $\mathrm{QsH}(G, H)$ dans $\mathrm{QsH}(G', H')$ dont l'application inverse associe à $T \in \mathrm{QsH}(G', H')$, $((\phi, \psi)^{-1}(T))^0$.

Il reste à vérifier que (ϕ, ϕ) est un morphisme d'anneaux : si D est la diagonale de $G \times G$ alors $(\phi, \phi)(D)$ est la diagonale de $G' \times G'$. On vérifie facilement que pour tous sous-groupes S et T de $G \times G$, $(\phi, \phi)(S *^1 T) = \phi(S) *^1 \phi(T)$ et on en déduit de la même façon que pour l'addition ci-dessus que pour tous éléments S et T de $\mathrm{QsE}(G)$, $(\phi, \phi)(S *^0 T) = \phi(S) *^0 \phi(T)$. $\triangleleft$

Terminons ce paragraphe avec un lemme simple mais un peu pénible à vérifier :

Lemme 3.5.3. *Soient G et H deux groupes $\bigwedge\!\!\!\bigwedge$-définissables et connexes. Le groupe $\mathrm{QsH}(G^{\times k}, H^{\times l})$ est isomorphe au groupe de matrices $\mathcal{M}_{k,l}(\mathrm{QsH}(G, H))$ et l'anneau $\mathrm{QsE}(G^{\times m})$ est isomorphe à l'anneau de matrices $\mathcal{M}_{m,m}(\mathrm{QsE}(G))$. Le premier isomorphisme θ se définit de la manière suivante : pour $S \in \mathrm{QsH}(G^{\times k}, H^{\times l})$ on associe $(S^0_{i,j})$ tel que*

$$S_{i,j} = \{(x, y);\ \exists \bar{y}, \bar{y}'\ (0, \dots, 0, x, 0, \dots, 0, \bar{y}, y, \bar{y}') \in S\}.$$

Réciproquement à $(T_{i,j}) \in \mathcal{M}_{k,l}(\mathrm{QsH}(G, H))$ on associe $\tilde{T}^0$ tel que

$$\tilde{T} = \{(\bar{x}, \bar{y});\ \exists (y_{i,j})\ y_j = \sum_i y_{i,j} \text{ et } (x_i, y_j) \in T_{i,j}\}.$$

▷ Notons pour cette preuve, $\mathrm{QsH}^1(G,H)$ l'ensemble des sous-groupes $\mathcal{M}$-définissables de $G\times H$ vérifiant les deux premières propriétés des quasi-homomorphismes (on enlève la propriété de connexité). Notons de même $\mathrm{QsH}^1(G^{\times k},H^{\times l})$.

Si $T\in\mathrm{QsH}^1(G^{\times k},H^{\times l})$ alors pour tout (i,j) $T_{i,j}\in\mathrm{QsH}^1(G,H)$ car $\mathrm{coker}T_{i,j}=\pi_j(\mathrm{coker}T)$.

Si S est un sous-groupe d'indice fini de T dans $\mathrm{QsH}^1(G^{\times k},H^{\times l})$ alors chaque $S_{i,j}$ est d'indice fini dans $T_{i,j}$.

Il est aussi facile de vérifier que pour tous S et T dans $\mathrm{QsH}^1(G^{\times k},H^{\times l})$,

$$(S+^1T)_{i,j}=S_{i,j}+^1T_{i,j}.$$

De ce qui précède on déduit que θ est un morphisme de groupes.

Si S est dans le noyau de ce morphisme alors chaque $S_{i,j}\subseteq G\times\mathrm{coker}S_{i,j}=G\times\pi_j(\mathrm{coker}S)$. On en déduit que $S\subseteq G^{\times k}\times\prod_j\pi_j(\mathrm{coker}S)$. Ce morphisme θ est donc injectif.

Pour montrer la surjectivité, on peut vérifier la relation suivante :
pour tout $(T_{i,j})\in\mathcal{M}_{k,l}(\mathrm{QsH}(G,H))$,

$$T_{i,j}\subseteq\tilde{T}_{i,j}\subseteq T_{i,j}+\{0\}\times\sum_{s\neq i}\mathrm{coker}T_{s,j}.$$

Donc $\tilde{T}^0$ est antécédent de $(T_{i,j})$.

Il reste à montrer que l'on a un morphisme d'anneaux entre les anneaux $\mathrm{QsE}(G^{\times m})$ et $\mathcal{M}_{m,m}(\mathrm{QsE}(G))$. Pour D la diagonale de $G^{\times m}\times G^{\times m}$ on a $D_{i,j}$ qui est la diagonale de $G\times G$.

Le plus pénible à vérifier est que $(S*^1T)_{i,j}$ et $\sum_s{}^1(S_{i,s}*^1T_{s,j})$ sont commensurables. Il est assez simple de voir que $\sum_s{}^1(S_{i,s}*^1T_{s,j})$ est d'indice fini dans $(S*^1T)_{i,j}$: on montre que

$$(S*^1T)_{i,j}\subseteq\sum_s{}^1(S_{i,s}*^1T_{s,j})+\{0\}\times\pi_j(\mathrm{coker}T).$$

En effet si $(x_i,z_j)\in(S*^1T)_{i,j}$, il existe $\bar{z}$ tel que z_j est le j-ème élément de $\bar{z}$ et tel que $(\bar{0},x_i,\bar{0},\bar{z})\in S*^1T$. Il existe alors $\bar{y}$ tel que $(\bar{0},x_i,\bar{0},\bar{y})\in S$ et $(\bar{y},\bar{z})\in T$. Pour chaque y_s il existe $\bar{z}_s$ tel que $(\bar{0},y_s,\bar{0},\bar{z}_s)\in T$. On a donc $(x,y_s)\in S_{i,s}$ et $(y_s,\bar{z}_{s,j})\in T_{s,j}$. D'autre part on voit facilement que $z_j-\sum_s\bar{z}_{s,j}\in\pi_j(\mathrm{coker}T)$.

Le second sens : soit $B=T(\prod_s\pi_s(\mathrm{coker}S))$ (c'est-à-dire l'ensemble des $\bar{z}$ tel qu'il existe $\bar{y}\in\prod_s\pi_s(\mathrm{coker}S)$ tel que $(\bar{y},\bar{z})\in T$).

On vérifie que

$$\sum_s{}^1(S_{i,s}*^1T_{s,j})\subseteq(S*^1T)_{i,j}+\pi_j(B).$$

En effet si $(x,z)\in\sum_s{}^1(S_{i,s}*^1T_{s,j})$, il existe $z_1,\dots,z_s$ et $y_1,\dots,y_s$ tels que $z=\sum_s z_s$, $(x,y_s)\in S_{i,s}$ et $(y_s,z_s)\in T_{s,j}$. Il existe alors $\bar{y}'$ tel que $\bar{y}'_1=y_1$ et $(\bar{0},x,\bar{0},\bar{y}')\in S$. Pour tout s, $\bar{y}'_s-y_s\in\pi_s(\mathrm{coker}S)$. Il existe $\bar{z}'$ tel que $(\bar{y}',\bar{z}')\in T$. On a alors $(x,\bar{z}'_j)\in(S*^1T)_{i,j}$ et $z-\bar{z}'\in B$. ◁

3.5.2 Quasi-endomorphismes de sous-groupes additifs

Le corps K joue ici le rôle de l'ensemble de paramètres A de la partie précédente. Comme K est une sous-structure élémentaire de L, tout définissable sur $\mathrm{acl}^{eq}(K)$, l'est sur K.

Nous montrons que comme pour les endomorphismes, tout quasi-endomorphisme d'un sous-groupe additif est restriction d'un quasi-endomorphisme du groupe additif entier (3.5.6).

Dans [BD2] E. Bouscaren et F. Delon montrent le lemme suivant :

Lemme 3.5.4. *Soit G un sous-groupe λ_0-fermé de $(L^{\times k}, +)$ défini sur K. Alors il existe une isogénie ϕ définissable sur K de $(L^{\times k}, +)$ tel que $\phi(G) = L^{\times m} \times \{0\}^{\times(k-m)}$ ($m = dim(\bar{G})$).*

Remarque. On peut remarquer que l'isogénie est définie par des p-polynômes mais par contre on n'a pas a priori $G = \phi^{-1}(L^{\times m} \times \{0\}^{\times(k-m)})$.

En utilisant la proposition 3.5.2, on déduit immédiatement le corollaire suivant :

Corollaire 3.5.5. *Soit G un sous-groupe connexe λ_0-fermé de $(L^{\times k}, +)$ défini sur K. Alors* $\mathrm{QsE}(G)$ *est isomorphe à* $\mathrm{QsE}((L^{\times m}, +)) = \mathcal{M}_{m,m}(\mathrm{QsE}((L, +)))$ *où $m = dim(\bar{G})$.*

Du lemme précédent, on déduit un autre résultat :

Corollaire 3.5.6. *Soit G un sous-groupe connexe λ-fermé de $(L, +)$ défini sur K. Alors tout quasi-endomorphisme de G se prolonge en un quasi-endomorphisme de $(L, +)$.*

$\triangleright$ Soit $S \in \mathrm{QsE}(G)$. Le groupe S est connexe et est une intersection décroissante de sous-groupes définissables S_i de $(L \times L, +)$. Par compacité on peut supposer que $\mathrm{coker} S_0 = \mathrm{coker} S$. De même G est une intersection décroissante de sous-groupes définissables G_j de $(L, +)$. Par la proposition 3.1.20 on peut supposer les G_j connexes.

Par compacité il existe j tel que que $\pi_1(S_0) \supseteq G_j$.
Soit $T = (S_0 \cap (G_j \times L))^0$. Alors $T \supseteq S$ et $T \in \mathrm{QsH}(G_j, L)$.

Il existe un entier n tel que G_j est λ_n-fermé.
Soit $H = \lambda_n(G_j)$ et $U = (\lambda_n, id)(T)$.

Le groupe H est un sous-groupe λ_0-fermé de $(L^{\times p^{\nu n}}, +)$. Donc il existe une isogénie définissable ϕ de $(L^{\times p^{\nu n}}, +)$ qui envoie H sur $L^{\times k} \times \{0\}^{\times p^{\nu n} - k}$ (3.5.4). Ainsi on a une isogénie définissable ψ de H dans $(L^{\times k}, +)$. Soit $V = (\psi, id)(U)$. Donc $V \in \mathrm{QsH}(L^{\times k}, L)$. Soit $W \in \mathrm{QsH}(L^{\times p^{\nu n}}, L)$ défini par $W = \{(x, z, y);\ (x, y) \in V \text{ et } z \in L^{\times p^{\nu n} - k}\}$. Soit $X = (\phi, id)^{-1}(W)$. On a $X \supseteq U$.

Enfin soit $Y = (\lambda_n, id)^{-1}(X)$. Alors $Y \supseteq T \supseteq S$ et $Y \in \mathrm{QsE}((L, +))$. $\triangleleft$

Dans le cas particulier du groupe $(L, +)$ on a le petit lemme suivant :

Lemme 3.5.7. *Pout tout $S \in \mathrm{QsE}((L, +))$ il existe un endomorphisme T de $(L, +)$ tel que $S *^0 T$ est un endomorphisme de $(L, +)$. De plus cet endomorphisme T est défini par un p-polynôme de $K[X]$ (c'est-à-dire $T \in K\{\alpha\}$).*

$\triangleright$ coker$S$ est un sous-groupe fini définissable sur K de $(L, +)$. Le p-polynôme P qui définit coker$S$ est dans $K[X]$. Soit T le graphe de ce p-polynôme. On a alors $\mathrm{coker}(S *^0 T) = \{0\}$. $\triangleleft$

On a le même lemme pour le groupe $(L^{p^\infty}, +)$ avec la même démonstration.

Lemme 3.5.8. $\mathrm{QsE}((L^{p^\infty}, +))$ *est égal à* $= K^{p^\infty}\{\alpha, \alpha^{-1}\}$*, c'est à dire l'unique corps de fractions de* $\mathrm{End}_K((L^{p^\infty}, +))$.

$\triangleright$ Pout tout $S \in \mathrm{QsE}((L^{p^\infty}, +))$ il existe un endomorphisme T de $(L^{p^\infty}, +)$ tel que $S *^0 T$ est un endomorphisme de $(L^{p^\infty}, +)$. De plus cet endomorphisme T est défini par un p-polynôme de $K^{p^\infty}[X]$.

Comme $(L^{p^\infty}, +)$ est minimal $\mathrm{QsE}((L^{p^\infty}, +))$ est un corps et donc un corps de fractions de $\mathrm{End}_K((L^{p^\infty}, +)) = K^{p^\infty}\{\alpha, \alpha^{-1}\}$.

$K^{p^\infty}\{\alpha\}$ est un anneau de Ore à gauche car principal à gauche (en fait comme K^{p^∞} est un corps parfait $K^{p^\infty}\{\alpha\}$ est aussi principal à droite donc de Ore à droite). On en déduit que $K^{p^\infty}\{\alpha, \alpha^{-1}\}$ est aussi un anneau de Ore à gauche : en effet si g et h sont deux éléments non nuls de $K^{p^\infty}\{\alpha, \alpha^{-1}\}$ alors il existe m tel que $\alpha^m g$ et $\alpha^m h$ sont deux éléments non nuls de $K^{p^\infty}\{\alpha\}$, d'où

$$K^{p^\infty}\{\alpha, \alpha^{-1}\}g \cap K^{p^\infty}\{\alpha, \alpha^{-1}\}h \supseteq K^{p^\infty}\{\alpha\}\alpha^m g \cap K^{p^\infty}\{\alpha\}\alpha^m h \neq \{0\}.$$

$K^{p^\infty}\{\alpha, \alpha^{-1}\}$ étant un anneau de Ore, il a un unique corps de fraction [Co 71]. $\triangleleft$

Proposition 3.5.9. *Soit G un sous-groupe minimal additif $\bigwedge\!\!\!\bigwedge$-définissable sur K. Si $|K| > \aleph_0$ alors le corps des quasi- endomorphismes définissables sur K de G est isomorphe au corps de fractions de $K^{p^\infty}\{\alpha, \alpha^{-1}\}$ si et seulement si G est non localement modulaire.*

$\triangleright$ Si G est non localement modulaire alors G est isogène à $(L^{p^\infty}, +)$ (3.1.25), donc par (3.5.2), $\mathrm{QsE}_K(G)$ est isomorphe à $\mathrm{QsE}_K(L^{p^\infty}, +)$.

Le groupe G est un λ-fermé. Il existe donc un sous-corps K_0 dénombrable de définition de G (3.1.7).

Si G est localement modulaire alors $\mathrm{QsE}_K(G) = \mathrm{QsE}_{K_0}(G)$ (1.3.5).
Donc $\mathrm{QsE}_K(G)$ est dénombrable ce qui n'est pas le cas de $\mathrm{QsE}_K(L^{p^\infty}, +)$. $\triangleleft$

3.5.3 Corps des quasi-endomorphismes et anneaux des endomorphismes

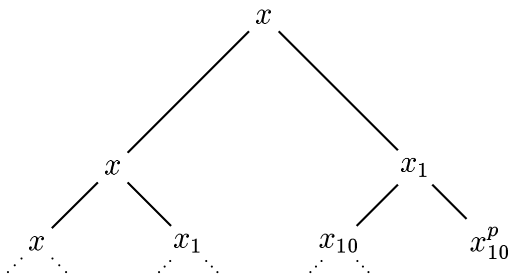
Remarque 3.5.10. Soit $G = \{x;\ \exists y \in L^{p^\infty},\ x = x^p + by^p\}$ le groupe considéré dans la proposition 3.4.3. Le groupe G est définissablement isogène à $(L^{p^\infty}, +)$ donc a même corps de quasi-endomorphismes (3.1.25). Par contre l'anneau des endomorphismes définissables de G est réduit à $\mathbb{F}_p$ (3.4.3). Donc G est un exemple de groupe minimal non localement modulaire dont le corps de quasi-endomorphismes n'est pas un corps de fractions de son anneau d'endomorphismes.

Nous allons voir qu'il existe aussi des exemples localement modulaires. Ceci est plus intéressant. Cela signifie qu'il existe un sous-groupe H de $(L,+)$ localement modulaire dont la structure induite est plus riche que sa structure de module sur son anneau d'endomorphismes.

Remarque. On peut choisir ce groupe H $\bigwedge\!\!\!\bigwedge$-définissable sur le vide (3.5.16) et donc par (3.3.3 et 3.3.5) ce groupe est $\bigwedge\!\!\!\bigwedge$-définissable dans la structure de module $L_{\mathbb{F}_p(B)^{sep}-mod}$ et la structure induite sur H par L est identique à celle induite par $L_{\mathbb{F}_p(B)^{sep}-mod}$. Ce contre exemple se réalise donc dans une structure de module.

Définition. Soit $H := \{x;\ \exists y \in G_1,\ x = x^p + by^p\}$ où G_1 est le sous-groupe de $(L,+)$ de la proposition 3.4.17, $G_1 = \{x \in L;\ x_{\bar{0}(n)} = x^p_{\bar{0}(n+1)} + x^{p^2}_{\bar{0}(n+1)}b$ pour tout $n \in \omega\}$, et b est le premier élément de la p-base.

Donc H est un sous-groupe de $(L,+)$ définissablement isogène à G_1.



Groupe H

Nous allons montrer que H est minimal et que son anneau d'endomorphismes est réduit à $\mathbb{F}_p$.

Soient la suite Q_n de polynômes de $K[Y]$ définie par

$$Q_0(Y) = Y^p \text{ et } Q_{n+1}(Y) = Q_n(Y^p + bY^{p^2})$$

et la suite P_n de polynômes de $K[X,Y]$ définie par

$$P_n(X,Y) = X^p - X + bQ_n(Y).$$

Il est simple de voir que $x \in H$ si et seulement si pour tout $n \in \omega$, $P_n(x, x_{1\bar{0}(n)}) = 0$.

Les lemmes suivants montrent que les polynômes P_n sont irréductibles.

Lemme 3.5.11. *Pour tout n, il existe $(s_{i,n}) \in \mathbb{F}_p(B)$ et $t_n \in \omega$ tels que $Q_n(Y) = \sum_{0\le i\le n} s_{i,n} Y^{p^{n+1+i}}$ et $s_{n,n} = b^{pt_n}$*

$\triangleright$ On fait la preuve par induction sur n.

Pour $n = 0$, $t_0 = 0$.

Supposons le résultat vrai pour n.

$$\begin{array}{rcl} Q_{n+1}(Y) & = & Q_n(Y^p + bY^{p^2}) \\ & = & \sum_{i=0}^{n} s_{i,n}(Y^{p^{(n+2)+i}} + b^{p^{n+1+i}} Y^{p^{(n+2)+1+i}}). \end{array}$$

En particulier $s_{n+1,n+1} = s_{n,n} b^{p^{2n+1}}$. Donc $s_{n+1,n+1} = b^{p(t_n + p^{2n})}$ et $t_{n+1} = t_n + p^{2n}$. ◁

Corollaire 3.5.12. *Pour tout n, il n'existe pas de polynôme A dans $\bar{K}[Y]$ tel que $A - A^p = bQ_n(Y)$.*

▷ Si pour un n, on a un tel polynôme A. Alors A est un p-polynôme car la dérivée de Q_n est nulle.

Donc $A(Y) = \sum_{i=0}^{n-1} c_i Y^{p^{n+1+i}}$ et $bQ_n(Y) = \sum_{i=0}^{n-1}(c_i Y^{p^{n+1+i}} - c_i^p Y^{p^{n+2+i}})$. Il suit que $bs_{0,n} = c_0$, pour $0 < i < n$, $bs_{i,n} = c_i - c_{i-1}^p$ et $bs_{n,n} = -c_{n-1}^p$.

Ceci donne l'équation suivante :

$$\sum_{i=0}^{n} (bs_{i,n})^{p^{n-i}} = 0.$$

Par (3.5.11), on obtient l'équation $a^p + bb^{pt_n} = 0$ en posant $a = \sum_{i=0}^{n-1}(bs_{i,n})^{p^{n-1-i}}$ ce qui est impossible car b n'appartient pas à L^p. ◁

Corollaire 3.5.13. *Les polynômes P_n sont irréductibles dans $\bar{K}[X, Y]$.*

▷ On considère $P_n(X)$ comme polynôme de $\bar{K}(Y)[X]$. Si $P_n(X)$ est réductible sur $\bar{K}(Y)$ alors d'après le théorème d'Artin-Schreier $P_n(X) = X^p - X + bQ_n(Y)$ a une racine dans $\bar{K}(Y)$. (Un polynôme de la forme $X^p - X - c$ sur un corps de caractéristique p est soit irréductible soit scindé.) Comme $\bar{K}[Y]$ est factoriel, cette racine est dans $\bar{K}[Y]$. Ceci est impossible d'après le corollaire 3.5.12. Donc les polynômes P_n sont irréductibles. ◁

Proposition 3.5.14. *Le groupe H est minimal et son anneau d'endomorphismes est réduit à $\mathbb{F}_p$.*

▷ Montrons que H est minimal.

Le groupe H est de $\mathrm{RU} = 1$ car il est définissablement isogène à G_1 qui est minimal. Il reste à montrer qu'il est connexe.

Soit J l'idéal de $K[X_\infty]$ engendré par les polynômes P_n et I^0. On sait que $H = V(J)$ et il suffit donc de montrer que J est premier séparable. Considérons pour cela les idéaux J_{n+1} de $K[X_{\leq n+1}]$ engendré par $I^0_{\leq n+1}$ et P_n, et montrons que ces idéaux sont premiers séparables.

Pour tout $n \in \omega$,

$$K[X_{\leq n+1}]/J_{n+1} \simeq K[X/J_{n+1}, X_{1\bar{0}(n)}/J_{n+1}].$$

Or $Z := X_{1\bar{0}(n)}/J_{n+1}$ est transcendant sur K et $T := X/J_{n+1}$ est séparablement algébrique sur $K[Z]$ par le polynôme $P_n(T, Z) = T - T^p + bQ_n(Z)$ qui est irréductible dans $K[Z, T]$ (3.5.13) et séparable en la variable T.

Montrons maintenant qu'un endomorphisme de H est nécessairement un élément de $\mathbb{F}_p$. Posons pour cela, pour tout $n \in \omega$, $H_n := V(I(H)_{\leq n})$ et montrons le petit lemme suivant :

Lemme 3.5.15. *Soit $n \in \omega$. Posons $Y := X_{1\bar{0}(n)}$. Soit R un p-polynôme dans $K[X,Y] \cap I(H)_{\leq n+1}$. Alors $R \in < P_n >$ et en particulier ou bien $\deg_Y R \geq \deg Q_n$, ou bien R est nul.*

$\triangleright$ [Preuve de 3.5.15] Soient x réalisant le générique de H_n sur K, $y := x_{1\bar{0}(n)}$ et R un p-polynôme dans $K[X,Y] \cap I(H)_{\leq n+1}$.

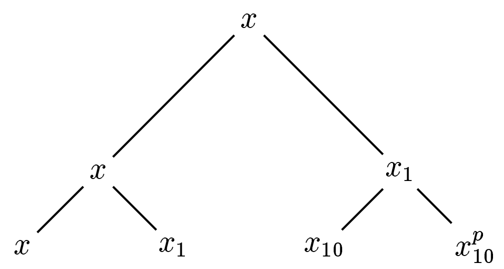
Montrons par induction sur $\deg_X R$ qu'il existe $S \in K[X,Y]$ tel que $\deg_X(R - SP_n) \leq 1$: supposons que $\deg_X R = p^{n+1}$. Alors il existe $R' \in K[X,Y]$ tel que $\deg_X R' \leq p^n$ et $R(X,Y) = R'(X,Y) + aX^{p^{n+1}}$. Or $(X^p)^{p^n} = (X + P_n(X,Y) - bQ_n(Y))^{p^n}$. D'où

$$R(X,Y) = R'(X,Y) + a(X + P_n(X,Y) - bQ_n(Y))^{p^n}$$

et donc $\deg_X(R - aP_n^{p^n}) \leq p^n$.

Soit $S \in K[X,Y]$ tel que $\deg_X(R - SP_n) \leq 1$. Alors $R - SP_n = 0$ puisque $(R - SP_n)(x,y) = 0$, $x \notin K[y]$ et $y \notin \bar{K}$. $\triangleleft$

Reprenons la preuve de (3.5.14) : soit τ un endomorphisme non nul de H. D'après la proposition 3.4.4 τ s'étend en un endomorphisme de $(L,+)$.
Par compacité il existe $m > 0$ tel que $\tau(H_m) \subseteq H_2$.



Groupe H_2

Par ailleurs il existe $n \geq m$ et R un p-polynôme de $K[X_{=n+1}]$, tels que pour tout $x \in L$, $\tau(x) = R(x_{=n+1})$ (3.3.1).

On a alors S un p-polynôme de $K[X,Y]$ tel que pour tout $x \in H_{n+1}$, $\tau(x) = S(x,y)$ où $y := x_{1\bar{0}(n)}$. Par le même type de preuve que celle de (3.5.15), on peut supposer que $\deg_Y(S) < \deg_Y(P_n)$.

Ceci donne pour tout $x \in H_{n+1}$

$$\tau(x) = \sum_{i=0}^{l} a_i x^{p^i} + \sum_{j=0}^{k} c_j y^{p^j} \text{ tel que } p^k < \deg Q_n.$$

Par ailleurs comme $\tau(H_{n+1}) \subseteq H_1$ on a sur H_{n+1}

$$\tau = \tau^p + b(f_1 \circ \tau)^p.$$

D'où

$$f_0 \circ \tau = \tau \text{ et}$$
$$f_i \circ \tau = 0 \text{ pour tout } i \in p^\nu \setminus \{0,1\}.$$

D'autre part (cela ne nous servira que pour $p = 2$), comme $\tau(H_{n+1}) \subseteq H_2$ et par définition de G_1, on a sur H_{n+1}

$$f_1 \circ f_1 \circ \tau = (f_0 \circ f_1 \circ \tau)^p.$$

On se place sur H_{n+2}, de façon que $y\ (= x_{1\bar{0}(n)}) = y_0^p + by_0^{p^2}$ et $x = x^p + bx_1^p$.

On calcule $f_0 \circ \tau$: pour tout $x \in H_{n+2}$,

$$f_0 \circ \tau(x) = a_{0,0}x + a_{0,p-1}bx_1 + \sum_{i=1}^{l} a_{i,0}x^{p^{i-1}} + c_{0,0}y_0 + c_{0,p-1}by_0^p + \sum_{j=1}^{k} c_{j,0}y^{p^{j-1}}.$$

(Ce sont toujours les notations suivantes : $a_{0,0} = f_0(a_0)$, $a_{0,p-1} = f_{p-1}(a_0)$,.... (voir 3.1.2)).

Il existe $Q'_{n+1} \in K[Y]$ tel que $Q_{n+1}(Y) = Q_0(Q'_{n+1}(Y)) = (Q'_{n+1}(Y))^p$. Ainsi x_1 $(= f_1(x)) = Q'_{n+1}(y_0)$.

En remplaçant, y par $y_0^p + by_0^{p^2}$ et x_1 par $Q'_{n+1}(y_0)$, on obtient :

$$\begin{aligned} f_0 \circ \tau(x) &= a_{0,0}x + a_{0,p-1}bQ'_{n+1}(y_0) + \sum_{i=1}^{l} a_{i,0}x^{p^{i-1}} \\ &\quad + b_{0,0}y_0 + c_{0,p-1}by_0^p + \sum_{j=1}^{k} c_{j,0}(y_0^p + by_0^{p^2})^{p^{j-1}}. \end{aligned}$$

Alors du fait que $f_0 \circ \tau = \tau$, on en déduit que pour tout $x \in H_{n+2}$,

$$T(x, x_{1\bar{0}(n+1)}) = 0$$

avec

$$\begin{aligned} T(X,Y) &= \sum_{i=0}^{l} a_i X^{p^i} - (a_{0,0}X + \sum_{i=1}^{l} a_{i,0}X^{p^{i-1}}) \\ &\quad + \sum_{j=0}^{k} c_j (Y^p + bY^{p^2})^{p^j} \\ &\quad - (a_{0,p-1}bQ'_{n+1}(Y) + c_{0,0}Y + c_{0,p-1}bY^p + \sum_{j=1}^{k} c_{j,0}(Y^p + bY^{p^2})^{p^{j-1}}). \end{aligned}$$

Comme $p^k < \deg Q_n$, on a $\deg_Y(T) \leq \max\{p^{k+2}, \deg Q'_{n+1}\} < \deg(Q_{n+1}) = p^2 \deg(Q_n)$ donc T est nul (3.5.15).

La nullité de T implique que pour tout $x \in H_{n+2}$, $\tau(x) = a_0 x + \sum_{j=0}^{k} c_j y^{p^j}$ avec $a_0 = a_{0,0}$.

Nous allons maintenant montrer que $a_{0,p-1}$ est nul ainsi la nullité de T impliquera que $\tau(x) = a_0 x$.

Pour $p > 2$, c'est très simple : il suffit de considérer $f_{p-1} \circ \tau$ qui est nul. On a pour pour tout $x \in H_{n+2}$,

$$f_{p-1} \circ \tau(x) = a_{0,p-1}x + a_{0,p-2}x_1 + \text{termes en } y_0 \text{ de degré } < \deg(Q_{n+1}).$$

Toujours par (3.5.15) $a_{0,p-1} = 0$.

Pour $p = 2$, on se place sur H_{n+3}, ainsi on a $y_0 = y_{00}^p + by_{00}^{p^2}$ et on utilise la relation suivante :

$$f_1 \circ f_1 \circ \tau = (f_0 \circ f_1 \circ \tau)^p.$$

On a

$$f_1 \circ \tau(x) = a_{0,1}x + a_{0,0}x_1 + c_{0,1}y_0 + c_{0,0}y_0^p + \sum_{j=1}^{k} c_{j,1} y^{p^{j-1}}.$$

En remplaçant, y par $y_0^p + by_0^{p^2}$ et x_1 par $Q'_{n+1}(y_0)$ on obtient :

$$f_1 \circ \tau(x) = a_{0,1}x + S(y_0)$$

où S est un p-polynôme de $K[Y]$ de degré strictement inférieur à celui de Q_{n+1}. On calcule $f_1 \circ f_1 \circ \tau$ en remplaçant y_0 par $y_{00}^p + by_{00}^{p^2}$, on obtient ainsi :

$$f_1 \circ f_1 \circ \tau(x) = a_{0,11}x + a_{0,10}x_1 + S_1(y_{00}).$$

avec $p \deg(S_1) < \deg(Q_{n+2})$. De même on a :

$$f_0 \circ f_1 \circ \tau(x) = a_{0,10}x + a_{0,11}bx_1 + S_0(y_{00}).$$

avec $p \deg(S_0) < \deg(Q_{n+2})$. D'où

$$(f_0 \circ f_1 \circ \tau(x))^p = a_{0,10}^p x^p + a_{0,11}^p b^p x_1^p + S_0^p(y_{00}).$$

On a d'une part $x_1 = Q'_{n+2}(y_{00})$ avec $\deg(Q_{n+2}) = p \deg(Q'_{n+2})$ et d'autre part $bx_1^p = x - x^p$. Avec ces relations et l'équation $f_1 \circ f_1 \circ \tau = (f_0 \circ f_1 \circ \tau)^p$ on en déduit l'équation suivante sur H_{n+3} :

$$a_{0,11}x + a_{0,10}Q'_{n+2}(y_{00}) + S_1(y_{00}) = a_{0,10}^p x^p + ba_{0,11}^p(x - x^p) + S_0^p(y_{00}).$$

Les degrés des polynômes Q'_{n+2}, S_1 et S_0^p sont strictement inférieurs à celui de Q_{n+2}, donc le polynôme $a_{0,11}X - a_{0,10}^p X^p - ba_{0,11}^p(X - X^p)$ est nul. D'où $a_{0,10}^p = ba_{0,11}^p$ (3.5.15).

Pour tout $i \in 2^\nu \setminus \{0,1\}$, en calculant $f_i \circ f_1 \circ \tau$ on obtient $a_{0,1\frown i} = 0$ (3.5.15). Ainsi $a_{0,1} = a_{0,10}^p + ba_{0,11}^p = 2a_{0,10}^p = 0$.

On a donc montré que pour tout p, $a_{0,p-1} = 0$ et donc que le terme en x_1 (qui vaut $a_{0,p-1}bx_1 = a_{0,p-1}bQ'_{n+1}(y_0)$) dans $f_0 \circ \tau$ disparaît. On en déduit par nullité de T que $\tau(x) = a_0 x$ sur H_{n+2} avec $a_0 = a_{0,0}$.

Maintenant nous utilisons le fait que $\tau = \tau^p + b(f_1 \circ \tau)^p$ sur H_{n+2} :

$$\begin{aligned} a_0 x &= (a_0 x)^p + b(a_{0,1}x + a_{0,0}x_1)^p \\ &= a_0^p x^p + ba_{0,1}^p x^p + a_0^p(bx_1^p) \\ &= a_0^p x^p + ba_{0,1}^p x^p + a_0^p(x - x^p). \end{aligned}$$

D'où $a_0 = a_0^p$ et donc $a_0 \in \mathbb{F}_p$. ◁

Corollaire 3.5.16. *Le groupe H est un exemple de sous-groupe additif minimal $\bigwedge\!\!\bigwedge$-définissable sur $\emptyset$ localement modulaire dont le corps des quasi-endomorphismes n'est pas un corps de fractions de l'anneau des endomorphismes.*

▷ Le groupe H est définissablement isogène à G_1 donc il est localement modulaire et a même corps de quasi-endomorphismes (3.5.2). Par (3.4.17), ce corps est infini (il contient $\mathbb{F}_p(X)$) alors que l'anneau des endomorphismes définissables de H est réduit à $\mathbb{F}_p$ (3.5.14). ◁

Tout sous-groupe minimal additif non localement modulaire est définissablement isogène à $(L^{p^\infty}, +)$ (3.1.25) dont le corps de quasi- endomorphismes est l'unique corps de fractions de l'anneau d'endomorphismes. Voici un résultat du même type pour tous les sous-groupes minimaux additifs dont la clôture algébrique du vide est finie :

Proposition 3.5.17. *Soit G un sous-groupe minimal additif $\bigwedge\!\!\bigwedge$-définissable sur k_0. Si $G_{k_0} = G \cap k_0$ est fini alors il existe un sous-groupe minimal additif H tel que G est définissablement isogène à H et tel que $\mathrm{QsE}_{k_0}(H) = \mathrm{End}_{k_0}(H)$.*

▷ G_{k_0} est fini donc k_0-définissable. Soit P le polynôme ayant comme ensemble de racines G_{k_0}. Alors P est un p-polynôme de $k_0[X]$ (3.2.4). Soit $H := P(G)$. Le p-polynôme P définit une isogénie ϕ de G sur H. Donc H est minimal et $H_{k_0} = \{0\}$ car $G_{k_0} = \ker \phi$. Donc $\mathrm{QsE}_{k_0}(H) = \mathrm{End}_{k_0}(H)$. ◁

Question 3.5.18. Nous ne savons pas si les hypothèses de la proposition précédente sont nécessaires et donc si tout sous-groupe additif minimal est définissablement isogène à un sous-groupe additif minimal dont le corps de quasi-endomorphismes est un corps de fractions de l'anneau des endomorphismes ?

3.5.4 Construction de sous-groupes minimaux additifs et $\aleph_0$-catégoriques

Nous reprenons la construction de groupes de RT $= 1$ de la proposition 3.4.18. Le lemme suivant montre que l'on peut choisir ψ tel que $\mathrm{acl}(\emptyset) \cap G_\psi = \{0\}$, ainsi $\mathrm{QsE}(G_\psi) = \mathbb{F}_p$, et par (1.3.6), la structure induite sur G_ψ est exactement sa structure de $\mathbb{F}_p$-espace vectoriel, et donc G_ψ est $\aleph_0$-catégorique.

Lemme 3.5.19. *Il existe une application ϕ de ω dans ω telle que si ψ est une autre application de ω dans ω telle que $\psi(n) \neq \phi(n)$ pour tout $n \in \omega$ alors* $\mathrm{acl}(\emptyset) \cap G_\psi = \{0\}$.

▷ Soit (a_n) une énumération de $\mathrm{acl}(\emptyset) = \mathbb{F}_p(B)^{sep}$. On construit ϕ par induction : pour $n \in \omega$, on suppose que ϕ est construit sur l'ensemble n.

Ou bien $a_{n,\bar{0}(n)01} = 0$ et dans ce cas on définit $\phi(n) = 0$.

Ou bien $a_{n,\bar{0}(n)01} \neq 0$. Alors il existe au plus un entier l tel que $a_{n,\bar{0}(n)1} = a_{n,\bar{0}(n)0}^{p^l}$. Sinon si pour $l_1 < l_2$, $a_{n,\bar{0}(n)1} = a_{n,\bar{0}(n)0}^{p^{l_1}} = a_{n,\bar{0}(n)0}^{p^{l_2}}$ alors $a_{n,\bar{0}(n)0} = a_{n,\bar{0}(n)0}^{p^{l_2-l_1}}$ d'où $a_{n,\bar{0}(n)01} = 0$. Si l existe on pose $\phi(n) = l$ sinon on pose $\phi(n) = 0$.

Soit ψ une application de ω dans ω. Si il existe n tel que $a_n \in G_\psi$, alors $a_{n,\bar{0}(n)01} = 0$ ou $a_{n,\bar{0}(n)1} = a_{n,\bar{0}(n)0}^{p^{\phi(n)}}$. Si $a_{n,\bar{0}(n)01} = 0$ on vérifie alors que $a_{n,\bar{0}(n)00} = 0$ et donc par induction que $a_n = 0$. Sinon $\psi(n) = \phi(n)$. ◁

Corollaire 3.5.20. *Pour tout entier $m > 0$, il existe $2^{\aleph_0}$ sous-groupes minimaux additifs $\bigwedge\!\!\!\bigwedge$-définissables sur $\emptyset$ $\aleph_0$-catégoriques et deux à deux orthogonaux qui ont tous exactement comme structure induite, une structure de $\mathbb{F}_{p^m}$-espace vectoriel et qui ont tous une clôture algébrique du vide triviale.*

▷ Reprenons la preuve de (3.4.23) en ajoutant la condition supplémentaire suivante sur les suites p_n et q_n : pour tout entier n, $p_n > \phi(n)$ et $q_n > \phi(n)$ (où ϕ est l'application du lemme 3.5.19).

Les $G_{m\psi_\alpha}$ sont des sous-groupes minimaux deux à deux orthogonaux dont l'anneau des endomorphismes est réduit à F_{p^m}. Par (3.5.19) pour tout α, $G_{m\psi_\alpha} \cap \mathrm{acl}(\emptyset) = \{0\}$. Donc pour tout α le corps de quasi-endomorphismes de G_{ψ_α} est réduit à $\mathbb{F}_{p^m}$ et par (1.3.6) $G_{m\psi_\alpha}$ a pour structure induite une structure de $\mathbb{F}_{p^m}$-espace vectoriel. ◁

Remarque. Deux groupes minimaux localement modulaires de clôture algébrique du vide réduite à $\{0\}$ sont non orthogonaux si et seulement si ils sont définissablement isomorphes (1.3.9). Le corollaire précédent est donc équivalent à l'existence de $2^{\aleph_0}$ sous-groupes non définissablement isomorphes de $(L, +)$ ayant ces propriétés.

3.6 Sous-groupes additifs de rang ω

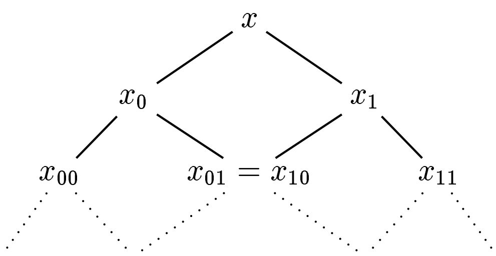
Dans [CCSSW] il est construit des types triviaux dans L de rang U égal à ω. Nous donnons ici une construction de types non triviaux dans L de rang U égal à ω. On utilise pour cela un sous-groupe de $(L, +)$ que l'on appelle le grill et qui est d'ailleurs un candidat possible pour un tel type mais dont on ne sait s'il est rangé.

Notre construction montre qu'il existe une infinité de sous-groupes additifs de rang U égal à ω dont les types génériques sont deux à deux orthogonaux (3.6.6). Certains sont 1-basés d'autres non (3.6.7 et 3.6.8). Il existe ainsi pour tous entiers n et m des sous-groupes additifs de rang égal à $\omega \cdot n + m$ (3.6.10). Par contre nous ne savons pas en construire de rang égal à ω^2.

Nous fixons pour cette partie une sous-structure élémentaire dénombrable K de L sur laquelle tous les groupes et types seront définis. On peut prendre pour K le modèle premier $\mathbb{F}_p(B)^{sep}$.

Définition. Le grill est défini de la manière suivante : $x \in \mathit{Grill}$ si et seulement si pour tout n, pour tout $i \in (p^\nu)^{<\omega}$, $x_{i01} = x_{i10}$ et si i n'est pas une suite de $0, 1 \in p^\nu$ alors $x_i = 0$ (c'est-à-dire si $i \notin \{0,1\}^{<\omega}$). (Rappelons que $x_i = f_i(x)$, $x_{i01} = f_1 \circ f_0(x_i)$ et $x_{i10} = f_0 \circ f_1(x_i)$ (3.1.2).)

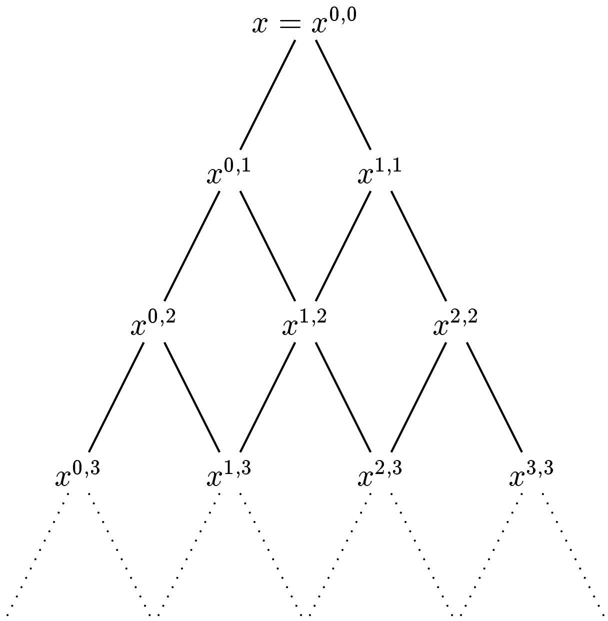
Grill :



Par la définition du grill, pour tout $n \in \omega$ et pour tout $i \in p^{\nu n}$, si $x \in \mathit{Grill}$ alors ou bien $x_i = 0$, ou bien x_i est égal à l'un des éléments $f_1^j \circ f_0^{n-j}(x)$ pour $j \leq n$.

Par la suite on ne s'interesse donc qu'aux indices dans $\{0,1\}^{<\omega}$. Pour tout $x \in \mathit{Grill}$ et toute hauteur n, on note $x^{0,n}, \ldots, x^{n,n}$ les $n+1$ composantes (de gauche à droite) de x à hauteur n susceptibles d'être algébriquement indépendantes : c'est-à-dire pour tout $j \leq n$, $x^{j,n} := f_1^j \circ f_0^{n-j}(x)$. En fait le grill n'impose pas de relation algébrique entre les éléments $x^{0,n}, \ldots, x^{n,n}$.

Voici l'arbre des composantes du grill avec ces notations :



Par les remarques précédentes, on voit facilement que l'idéal de $K[X_\infty]$, $I(\mathit{Grill})$ correspond au type complet p_{Grill} au-dessus de K, défini par $x \in \mathit{Grill}$ et pour tout n, les composantes $x^{0,n}, \ldots, x^{n,n}$ sont algébriquement indépendantes au-dessus de K. Le grill est donc un groupe connexe dont le type générique est p_{Grill}.

Remarque 3.6.1. Soit $a \models p_{Grill}$. Pour tout $n \in \omega$, les éléments $a^{0,n}, \ldots, a^{n,n}$ sont algébriquement indépendants mais ne sont pas indépendants au sens de la théorie des modèles si $n \geq 3$. En effet pour tout $0 \leq j \leq j' \leq n$,

$$a^{j,n}, \ldots, a^{j',n} \in K\!<\!a^{j,n}, a^{j',n}\!>$$

et en fait que pour tout $m \geq n$ et $k \in \{j, \ldots, j'+m-n\}$,

$$a^{k,m} \in K\!<\!a^{j,n}, a^{j',n}\!>.$$

Par contre on peut démontrer, par un simple argument de compacité, que pour tout $0 \leq j < j' \leq n$, $a^{j,n}$ n'est pas algébrique au sens de la théorie des modèles sur $K \cup \{a^{j+1,n}, \ldots, a^{n,n}\}$ et $a^{j',n}$ n'est pas non plus algébrique au sens de la théorie des modèles sur $K \cup \{a^{0,n}, \ldots, a^{j'-1,n}\}$.

Lemme 3.6.2. *Le grill n'est pas de rang U fini et pour tout $a \models p_{Grill}$ et tout $0 \leq j \leq j' \leq n$, $\mathrm{RU}(a/K \cup \{a^{j,n}, a^{j',n}\}) = n - (j'-j) = \mathrm{RT}(a/K\!<\!a^{j,n}, a^{j',n}\!>)$*

▷ Soit $n \in \omega$ et $a \models p_{Grill}$.
Par (3.6.1), pour tout $m \geq n$,

$$\deg tr(K(a_{=m})/K\!<\!a^{j,n}, a^{j',n}\!>) \leq n - (j'-j).$$

Donc

$$\mathrm{RU}(a/K \cup \{a^{j,n}, a^{j',n}\}) \leq \mathrm{RT}(a/K\!<\!a^{j,n}, a^{j',n}\!>\}) \leq n - (j'-j).$$

Réciproquement montrons par induction sur $0 \leq n - j' \leq n$ que

$$\mathrm{RU}(a/K, a^{0,n}, \ldots, a^{j',n}) \geq n - j'.$$

Pour $n - j' = 0$ c'est évident. Supposons le résultat vrai pour $n - j' < n$. Comme $a^{j',n}$ est définissable sur a mais n'est pas algébrique (au sens de la théorie des modèles) sur $K \cup \{a^{0,n}, \ldots, a^{j'-1,n}\}$ (3.6.1), par symétrie de la déviation, $\mathrm{tp}(a/K, a^{0,n}, \ldots, a^{j',n})$ dévie sur $K, a^{0,n}, \ldots, a^{j'-1,n}$. Donc

$$\mathrm{RU}(a/K, a^{0,n}, \ldots, a^{j'-1,n}) > \mathrm{RU}(a/K, a^{0,n}, \ldots, a^{j',n}) \geq n - j'.$$

Donc pour tout $j' \leq n$, $\mathrm{RU}(a/K, a^{0,n}, \ldots, a^{j',n}) \geq n - j'$. Par le même type d'induction on obtient que pour tout $j \leq j' \leq n$, $\mathrm{RU}(a/K \cup \{a^{j,n}, \ldots, a^{j',n}\}) \geq n - (j'-j)$. ◁

Remarque 3.6.3. a réalise une extension déviante de p_{Grill} si et seulement si pour un n il y a une relation algébrique entre les éléments $a^{0,n}, \ldots, a^{n,n}$. Pour montrer que le *grill* est de rang U égal à ω, il suffirait donc d'après ce qui précède de montrer que si on a une telle relation alors un $a^{j,m}$ est algébrique.

Pour obtenir un groupe de rang U égal à ω, on va se baser sur le grill mais en ajoutant des étapes de construction telles que l'on ait la propriété ci-dessus. C'est l'idée que l'on trouve dans [CCSSW, section 4 Theorem 1] : les auteurs construisent un type de rang U égal à ω à partir d'un seul type minimal de rang de transcendance 1 qui est "fortement" trivial (c'est-à-dire sa prégéométrie correspond à celle de l'ensemble infini avec comme seule structure l'égalité). Ils utilisent cette dernière propriété. On ne peut donc pas faire exactement le même preuve pour obtenir un groupe. Nous allons utiliser une infinité de types additifs de rang de transcendance 1 et deux à deux orthogonaux.

Nous avons besoin du petit lemme suivant :

Lemme 3.6.4. *Soient $p_0, \ldots, p_n$ des types minimaux de rang de transcendance 1 et deux à deux orthogonaux.*

Alors pour tout $Q \in K[X_0, \ldots, X_n, \bar{Y}]$ on a

$$p_0(x_0) \bigwedge \cdots \bigwedge p_n(x_n) \ \vdash \ \Big(Q(X_0, \ldots, X_n, \bar{y}) \neq 0 \bigwedge Q(x_0, \ldots, x_n, \bar{y}) = 0\Big) \Rightarrow \bigvee_{i=0}^{n} "x_i \in \operatorname{acl}(\bar{y})".$$

Ci-dessus il suffit d'une formule pour témoigner de l'algébricité de x_i sur $\bar{y}$, car la disjonction (infinie) de formules "$x_i \in \operatorname{acl}(\bar{y})$" est équivalente dans un fermé à une seule formule.

Par compacité il existe $m(Q)$ tel que l'on ait la même propriété en remplaçant les p_i par $p_{i,m(Q)}$ (voir notation 3.1.9).

Afin d'avoir par la suite une description simple des déviations du type de $\mathrm{RU} = \omega$ construit, on remarque aussi que l'on peut choisir $m(Q)$ tel que pour tout $I \subseteq \{1, \ldots, n\}$ l'on ait :

$$\bigwedge_{i \in I} p_{i,m(Q)}(x_i) \ \vdash \ \Big(Q((X_i)_{i\in I}, (x_j)_{j\notin I}, \bar{y}) \neq 0 \bigwedge Q(x_0, \ldots, x_n, \bar{y}) = 0\Big) \Rightarrow \bigvee_{i \in I} "x_i \in \operatorname{acl}(\bar{y} \cup \{x_j / j \notin I\})".$$

(La notation $Q((X_i)_{i\in I}, (x_j)_{j\notin I}, \bar{y})$ signifie que l'on considère le polynôme Q où l'on a remplacé pour tout $j \notin I$, la variable X_j par la constante x_j et les variables $\bar{Y}$ par les constantes $\bar{y}$.)

$\triangleright$ On ne doit démontrer que la première assertion. La suite est une conséquence immédiate du fait que être algébrique s'écrit par une disjonction de formules.

On montre par induction sur $j \leq n$ que si aucun des x_i n'est dans $\operatorname{acl}(\bar{y})$ alors $x_0, \ldots, x_j$ est une suite indépendante au-dessus de $\bar{y}$: en effet du fait de l'orthogonalité des types si $x_0, \ldots, x_j$ est une suite indépendante au-dessus de $\bar{y}$ alors $\operatorname{tp}(x_0, \ldots, x_j/\bar{y})$ est orthogonal à $\operatorname{tp}(x_{j+1}/\bar{y})$. $\triangleleft$

Proposition 3.6.5. *A partir d'une infinité de types minimaux de rang de transcendance 1 et deux à deux orthogonaux on peut construire un type de rang U égal à ω. De plus si ces types sont additifs la construction donne un type additif qui sera le générique d'un sous-groupe de $(L, +)$ de rang U égal à ω. Du fait qu'il existe une infinité de types* *minimaux additifs de rang de transcendance* 1 *deux à deux orthogonaux, il existe donc des sous-groupes de* $(L,+)$ *de rang* U *égal à* ω.

$\triangleright$ Nous pourrions écrire la preuve de la même façon que celles de [CW 99], en remplaçant l'étape qui consiste à relier les éléments algébriquement indépendants par une étape du grill.

Pour simplifier on suppose que l'on part d'une infinité $(p_j)_{j\in\omega}$ de types minimaux sur K de RT $= 1$ et 2 à 2 orthogonaux tels que pour tout $j, n \in \omega$, si $x \models p_j$ alors pour tout $i \in (p^\nu)^{\leq n}$, $x_i \in K[x_{\bar{0}(n)}]$.
Cela ne pose pas de problème car les exemples que l'on a construits sont ainsi (3.4.15).

Cette hypothèse supplémentaire permet de commencer par définir simplement un type dépendant d'un paramètre tel que quelque soit la valeur de ce paramètre ce type ait des propriétés analogues à celle du type générique du grill dans le lemme 3.6.2, et ensuite de définir par induction ce paramètre tel que l'on ait alors la propriété supplémentaire de la remarque précédente (3.6.3).

Pour tout $j, n \in \omega$, on note $p_{j,n}$ le type p_j restreint à la hauteur n (voir 3.1.9).

Soit β une application de ω dans ω. Nous allons définir à partir de la famille des p_j un type p_β : on commence par $x \models p_{0,\beta(0)}$, ensuite on ajoute une première étape du grill, on impose ensuite aux deux nouveaux éléments y, z que $y \models p_{0,\beta(1)}$ et $z \models p_{1,\beta(1)}$ et ainsi de suite. Plus précisément, à partir de β, définissons pour tout $l \leq n$, $\gamma(l,n) \in \{0,1\}^{<\omega}$. Soit $\gamma(0,0) = \emptyset$ et pour $l \leq n$, $\gamma(l,n+1) = \gamma(l,n)\ \bar{0}(\beta(n)+1)$ et $\gamma(n+1,n+1) = \gamma(n,n)\ \bar{0}(\beta(n))\ 1$.

p_β est défini par les relations suivantes :
pour tout $l \leq n$,

$$x_{\gamma(l,n)} \models p_{l,\beta(n)} \text{ et } x_{\gamma(l,n)\bar{0}(\beta(n))} = x^p_{\gamma(l,n+1)} + bx^p_{\gamma(l+1,n+1)},$$

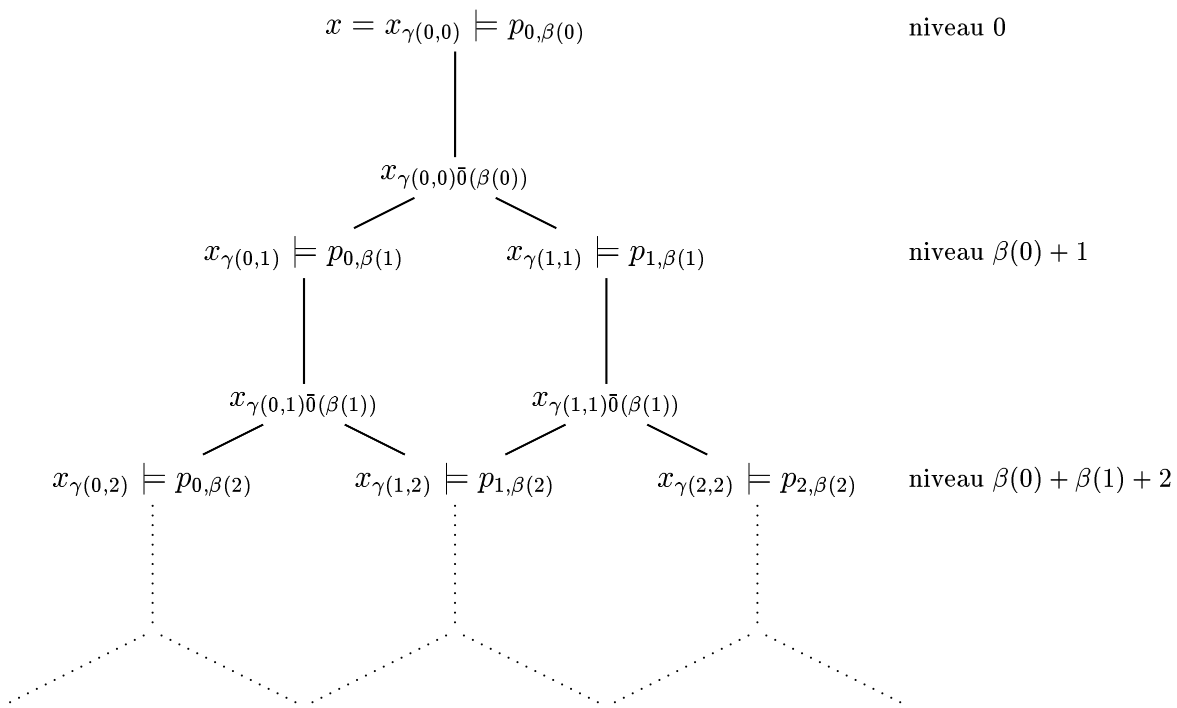
et pour tout n,

$$x_{\gamma(0,n)}, \dots, x_{\gamma(n,n)} \text{ sont algébriquement indépendants sur K.}$$

Remarquons que par la dernière hypothèse sur la famille des p_i, pour tout $l \leq n$ et $i \in (p^\nu)^{\leq\beta(n)}$,

$$x_{\gamma(l,n)i} = f_i(x_{\gamma(l,n)}) \in K[x_{\gamma(l,n)\bar{0}(n)}].$$

Voici l'arbre des p-composantes de p_β :



Dans le cas où tous les types p_j sont additifs alors p_β est le type générique du sous-groupe G_β défini simplement par les relations suivantes :
pour tout $l \leq n$,

$$x_{\gamma(l,n)} \in V(I(p_{l,\beta(n)})) \text{ et } x_{\gamma(l,n)\bar{0}(\beta(n))} = x^p_{\gamma(l,n+1)} + b x^p_{\gamma(l+1,n+1)}.$$

En fait, pour $x \models p_\beta$, les éléments $x_{\gamma(0,n)}, \ldots , x_{\gamma(n,n)}$ jouent le même rôle que les éléments $x^{0,n}, \ldots , x^{n,n}$ dans le grill : pour tout $a \models p_\beta$ et tout $j \leq j' \leq n$, $\mathrm{RU}(a/K \cup \{a_{\gamma(j,n)}, a_{\gamma(j',n)}\}) = n - (j' - j) = \mathrm{RT}(a/K < a_{\gamma(l,n)}, a_{\gamma(j',n)} >)$ et donc $\mathrm{RU}(p_\beta) \geq \omega$.

La preuve est la même que celle du lemme 3.6.2.

Nous allons voir maintenant que l'on peut définir une application β par induction de façon que $\mathrm{RU}(p_\beta) \leq \omega$.

On note p^n_β le type p_β restreint à la hauteur $\sum_{i=0}^{n-1}(\beta(i) + 1)$ (qui est égale à la longueur de $\gamma(0, n)$). (Avec la notation 3.1.9, $p^n_\beta = p_{\beta,\sum_{i=0}^{n-1}(\beta(i)+1)}$.)

On remarque tout d'abord que p^n_β ne dépend que de la valeur de $\beta_{|n}$ et que pour tout $l \leq m \leq n$, il existe $Q_{\beta_{|n},l,m} \in K[X_0, \ldots , X_n]$ tel que pour tout $x \models p^n_\beta$

$$x_{\gamma(l,m)} = Q_{\beta_{|n},l,m}(x_{\gamma(0,n)}, \ldots , x_{\gamma(n,n)}).$$

Nous voulons construire β tel que s'il y a une relation algébrique à un niveau de l'arbre alors il existe $l \leq n$ tel que $a_{\gamma(l,n)}$ est algébrique. Soit $\bar{Y}$ un uple infini dénombrable de variables et $(P_n)_{n\in\omega}$ une énumération de l'ensemble dénombrable de polynômes

$$\bigcup_{m\in\omega} K[X_{0,m}, \ldots , X_{m,m}, \bar{Y}].$$

On choisit cette énumération telle que pour tout entier n,

$$P_n \in K[X_{0,m}, \dots, X_{m,m}, \bar{Y}] \text{ avec } m \leq n.$$

On définit alors β par induction de telle manière que pour tout $n \in \omega$, $\bar{c} \in L$, et $a \models p_\beta^{n+1}$, si $P_n(a_{\gamma(0,m)}, \dots, a_{\gamma(m,m)}, \bar{c}) = 0$ et $P_n(X_{0,m}, \dots, X_{m,m}, \bar{c}) \neq 0$ alors il existe $l \leq n$ tel que $a_{\gamma(l,n)}$ est algébrique sur $K(\bar{c})$.

Pour 0 il n'y a rien à faire, on peut choisir $\beta(0) = 0$.
Supposons β défini jusqu'à $n-1$ et définissons $\beta(n)$: on utilise

$$R_n(X_0, \dots, X_n, \bar{Y}) := P_n(Q_{\beta_{|n},0,m}(X_0, \dots, X_n), \dots, Q_{\beta_{|n},m,m}(X_0, \dots, X_n), \bar{Y}).$$

et l'orthogonalité des types $p_0, \dots, p_n$. On pose $\beta(n) = m(R_n)$ défini par le lemme 3.6.4.

On vérifie que si $a \models p_\beta^{n+1}$ tel que

$$P_n(a_{\gamma(0,m)}, \dots, a_{\gamma(m,m)}, \bar{c}) = 0 \text{ et } P_n(X_{0,m}, \dots, X_{m,m}, \bar{c}) \neq 0$$

alors il existe $l \leq n$ tel que $a_{\gamma(l,n)}$ est algébrique sur $K(c)$. En effet dans ce cas on a d'une part $R_n(a_{\gamma(0,n)}, \dots, a_{\gamma(n,n)}, \bar{c}) = 0$ et d'autre part $R_n(X_0, \dots, X_n, \bar{c}) \neq 0$ car si a' réalise p_β^{n+1} tel que $a'_{\gamma(0,m)}, \dots, a'_{\gamma(m,m)}$ sont algébriquement indépendants au-dessus de $K(\bar{c})$ alors

$$R_n(a'_{\gamma(0,n)}, \dots, a'_{\gamma(n,n)}, \bar{c}) = P_n(a'_{\gamma(0,m)}, \dots, a'_{\gamma(m,m)}, \bar{c}) \neq 0.$$

On peut donc appliquer le lemme 3.6.4.

β ainsi défini, p_β est de RU $\leq \omega$. En effet si a réalise une extension déviante de p_β sur L, alors il existe un entier m tel qu'il y a une relation algébrique entre $a_{\gamma(0,m)}, \dots, a_{\gamma(m,m)}$ au-dessus de L.

Donc il existe $n \geq m$ et $\bar{c} \in L$ tel que $P_n(a_{\gamma(0,m)}, \dots, a_{\gamma(m,m)}, \bar{c}) = 0$.

On en déduit donc par la définition de β qu'il existe $l \leq n$ tel que $a_{\gamma(l,n)}$ est algébrique sur $K, \bar{c}$ et donc que $a_{\gamma(l,n)} \in L$. D'où

$$\mathrm{RU}(a/L) \leq \mathrm{RU}(a/K, a_{\gamma(l,n)}) \leq n.$$

Le type p_β est donc de rang U égal à ω. Rappelons que si l'on a choisit pour famille des p_i des types additifs, alors p_β est un type additf et est le génerique du groupe G_β connexe de rang ω.

Donnons maintenant une description des extensions déviantes de p_β, en utilisant la condition supplémentaire sur $m(R_n)$ définie dans le lemme 3.6.4. On montre alors que pour tout ensemble de paramètres C algébriquement clos et toute réalisation a de p_β, la description du type de a sur C est la donnée des éléments $a_{\gamma(l,n)}$ appartenant à C. Pour les types dans G_β (si nous partons de types additifs) on a la même description.

Soient a et b deux réalisations de p_β et C algébriquement clos, tels que pour tout $l \leq n$, $a_{\gamma(l,n)} \in C$ si et seulement si $b_{\gamma(l,n)} \in C$ et dans ce cas $a_{\gamma(l,n)} = b_{\gamma(l,n)}$. Supposons que a et b n'ont pas même type au-dessus de C. Dans ce cas il existe $\bar{c} \in C$ et P_n tels que $P_n(a_{\gamma(0,m)}, \dots, a_{\gamma(m,m)}, \bar{c}) = 0$ et $P_n(b_{\gamma(0,m)}, \dots, b_{\gamma(m,m)}, \bar{c}) \neq 0$.

Soit R_n le polynôme associé à P_n et $I := \{i;\ a_{\gamma(i,n)} \notin C\}$.
On a

$$R_n(a_{\gamma(0,n)}, \dots, a_{\gamma(n,n)}, \bar{c}) = P_n(a_{\gamma(0,m)}, \dots, a_{\gamma(m,m)}, \bar{c}) = 0$$

et

$$R_n((X_{i,n})_{i \in I}, (a_{\gamma(i,n)})_{i \notin I}, \bar{c}) \neq 0$$

car

$$R_n(b_{\gamma(0,n)}, \dots, b_{\gamma(n,n)}, \bar{c}) = P_n(b_{\gamma(0,m)}, \dots, b_{\gamma(m,m)}, \bar{c}) \neq 0.$$

D'après le lemme 3.6.4, il existe $i \in I$ tel que $a_{\gamma(i,n)} \in \mathrm{acl}(C \cup \{a_{\gamma(j,n)};\ j \notin I\} = C$. Ce qui est impossible par définition de I. $\triangleleft$

Proposition 3.6.6. *Il existe une infinité de sous-groupes additifs définis sur le vide de rang U égal à ω dont les types génériques sont deux à deux orthogonaux.*

$\triangleright$ Il suffit de considérer une partition infinie d'un ensemble infini de types additifs de $RT = 1$, deux à deux orthogonaux et définis sur le vide (3.4.15), et ainsi de construire une infinité de types $(p_{\beta_s})_{s \in \omega}$ de la même manière que dans la proposition 3.6.5. Dans cette construction on peut alors imposer à l'aide du lemme 3.6.4 (et en utilisant le même procédé que dans la preuve de (3.6.5)) la condition suivante : pour tout $s, s' \in \omega$ et tout ensemble de paramètres C, si a_s réalise p_{β_s}, $a_{s'}$ réalise $p_{\beta_{s'}}$ et s'il y a une relation algébrique à hauteur m entre a_s et $a_{s'}$ au-dessus de C, alors une des composantes de a_s ou $a_{s'}$ est algébrique sur C. Ainsi si a_s réalise l'extension non déviante de p_{β_s} et $a_{s'}$ réalise l'extension non déviante de $p_{\beta_{s'}}$ alors a_s et $a_{s'}$ sont indépendants au-dessus de C. $\triangleleft$

Corollaire 3.6.7. *Il existe des sous-groupes de $(L, +)$ de rang U égal à ω non 1-basés.*

$\triangleright$ Si dans la proposition 3.6.5 p_0 est le type générique de $(L^{p^\infty}, +)$ alors L^{p^∞} est un sous-groupe de G_β et donc G_β n'est pas 1-basé. $\triangleleft$

Proposition 3.6.8. *Il existe des sous-groupes de $(L, +)$ de rang U égal à ω et 1-basés.*

Pour montrer cette dernière proposition, nous allons utiliser une infinité de sous-groupes minimaux de $(L, +)$ de RT $= 1$, deux à deux orthogonaux, localement modulaires tels que leurs clôtures algébriques du vide sont réduites à $\{0\}$ et leurs corps de quasi-endomorphismes sont réduits à $\mathbb{F}_p$. Nous fixons pour la suite une suite infinie $(H_i)_{i \in \omega}$ de tels groupes, en prenant ces groupes parmi ceux du corollaire 3.5.20. Pour tout i soit p_i le type générique de H_i. Le lemme suivant qui est une généralisation du lemme 3.6.4 permet de montrer la proposition.

Lemme 3.6.9. *Pour tout $Q \in K[X_0^0, \dots, X_0^l, \dots, X_n^0, \dots, X_n^l, \bar{Y}]$ on a*

$$\bigwedge_{j \in \{0,\dots,l\}} \bigwedge_{i \in \{0,\dots,n\}} p_i(x_i^j) \vdash \big(Q((X_i^j), \bar{y}) \neq 0 \bigwedge Q((x_i^j), \bar{y}) = 0\big)$$

$$\Rightarrow \bigvee_{i=0}^{n} "CL(x_i^0, \dots, x_i^l) \in \mathrm{acl}(\bar{y})".$$

"$CL(x^0,\dots,x^l)\in \mathrm{acl}(\bar y)$" signifie qu'il existe une combinaison linéaire non nulle de $x^0,\dots,x^l$ appartenant à $\mathrm{acl}(\bar y)$, c'est à dire il existe $(\lambda_0,\dots,\lambda_l)\in\mathbb{F}_p^{l+1}\setminus\{(0,\dots,0)\})$ tels que $\lambda_0x^0+\ldots+\lambda_lx^l\in\mathrm{acl}(\bar y)$. Par compacité il existe $k(Q)$ tel que l'on ait la même propriété en remplaçant les p_i par $p_{i,k(Q)} := p_{i|k(Q)}$.

En fait il nous faut plus pour montrer la proposition.

On choisit par compacité $k(Q)$ tel que pour tout $J_0\subseteq\{0,\dots,l\},\dots,J_n\subseteq\{0,\dots,l\}$ et tout $\lambda_{i,j,j'}\in\mathbb{F}_p$ pour $i\in\{0,\dots,n\}$, $j'\in J_i$ et $j\in\{0,\dots,l\}\setminus J_i$, si l'on note $Q'((Z_i^j),\bar Y)$ le polynôme Q où l'on a remplacé les variables X_i^j par Z_i^j si $j\in J_i$ et par $Z_i^j+\sum_{j'\in J_i}\lambda_{i,j,j'}Z_i^{j'}$ sinon, alors :

$$\bigwedge_{i=0}^n\bigwedge_{j\in J_i}p_{i,k(Q)}(z_i^j)\vdash\big(Q'((Z_i^j)_{i\in I,j\in J_i},(z_i^j)_{i\in I,j\notin J_i},\bar y)\neq 0\bigwedge Q'((z_i^j),\bar y)=0\big)$$

$$\Rightarrow\bigvee_{i=0}^n\text{"}CL((z_i^j)_{j\in J_i})\in\mathrm{acl}(\bar y\cup\{z_k^j/k\in\{0,\dots,n\}\ \textit{et}\ j\notin J_k\})\text{"}.$$

On peut remarquer que si $l=0$ c'est simplement le lemme 3.6.4

$\triangleright$ La preuve se fait de la même manière que dans le lemme 3.6.4. Si on suppose que pour tout i il n'y a pas de combinaison linéaire non nulle de $x_i^0,\dots,x_i^l$ dans $\mathrm{acl}(\bar y)$ alors par le choix des types p_i, pour tout i, les $x_i^0,\dots,x_i^l$ sont indépendants au-dessus de $\mathrm{acl}(\bar y)$ et donc les types $\mathrm{tp}(x_i^0,\dots,x_i^l/\bar y)$ sont deux à deux orthogonaux. Ils ne peut donc pas y avoir de relations algébriques entre eux.

Pour le choix de $k(Q)$ c'est une simple coséquence du fait que les deuxièmes parties sont des disjonctions. $\triangleleft$

$\triangleright$ **Preuve de la proposition 3.6.8**

Nous conservons les notations de la preuve de la proposition 3.6.5. Nous commençons par la même construction de types p_β qui sont génériques de groupes G_β.

Pour définir β par induction, nous prenons ici une énumération $(P_n)_{n\in\omega}$ de l'ensemble dénombrable de polynômes

$$\bigcup_{l\in\omega}\bigcup_{m\in\omega}K[X_{0,m}^0,\dots,X_{0,m}^l,\dots,X_{m,m}^0,\dots,X_{m,m}^l,\bar Y]$$

On choisit cette énumération telle que pour tout entier n,

$$P_n\in K[X_{0,m}^0,\dots,X_{0,m}^l,\dots,X_{m,m}^0,\dots,X_{m,m}^l,\bar Y]\text{ avec }m\le n\text{ et }l\in\omega.$$

On définit alors β par induction de la façon suivante :

On pose $\beta(0):=k(P_0)$ défini par le lemme 3.6.9.

Si β est défini sur n on pose $\beta(n):=k(R_n)$ défini par le lemme 3.6.9, où R_n est le polynôme P_n dans lequel on a remplacé les variables $X_{i,m}^j$ par

$$Q_{\beta_{|n},i,m}(X_0^j,\dots,X_n^j).$$

De la même façon que dans la proposition 3.6.5, on montre que p_β est de RU $=\omega$, mais avec les conditions imposées par le lemme 3.6.9, on a, pour tout $l\in\omega$, une description simple des types dans $(G_\beta)^{l+1}$. Nous montrons que si $(a^0, \dots, a^l) \in G_\beta$ et C est un ensemble de paramètres algébriquement clos alors le type de $(a^0, \dots, a^l)$ sur C est donné par la connaissance, pour tout $n \in \omega$ et $i \in \{0, \dots, n\}$, des $\mathbb{F}_p$-espace vectoriels engendrés par $a^0_{\gamma(i,n)}, \dots, a^l_{\gamma(i,n)}$ au-dessus de C (la connaissance signifie la connaissance des relations linéaires au-dessus de C entre les $a^0_{\gamma(i,n)}, \dots, a^l_{\gamma(i,n)}$). En effet si on a $a = (a^0, \dots, a^l) \in (G_\beta)^{l+1}$ et $b = (b^0, \dots, b^l) \in (G_\beta)^{l+1}$ ayant des espaces vectoriels se correspondant au-dessus de C et si on suppose qu'ils n'ont pas même type au-dessus de C alors il existe par exemple une relation algébrique au-dessus de C satisfaite par a_∞ et non satisfaite par b_∞. Donc il existe $n \in \omega$ et $\bar{c} \in C$ tels que $P_n((a^j_{\gamma(i,m)}), \bar{c}) = 0$ et $P_n((b^j_{\gamma(i,m)}), \bar{c}) \neq 0$. Considérons le polynôme R_n associé à P_n. Donc $R_n((a^j_{\gamma(i,n)}), \bar{c}) = 0$ et $R_n((b^j_{\gamma(i,n)}), \bar{c}) \neq 0$. Pour tout $i \in \{0, \dots, n\}$, soit $J_i \subseteq \{0, \dots, l\}$ tel que $(a^j_{\gamma(i,n)})_{j \in J_i}$ est une base de l'espace vectoriel engendré par $a^0_{\gamma(i,n)}, \dots, a^l_{\gamma(i,n)}$ au-dessus de C. Donc pour tout $i \in \{0, \dots, n\}$, $(b^j_{\gamma(i,n)})_{j \in J_i}$ est une base de l'espace vectoriel engendré par $b^0_{\gamma(i,n)}, \dots, b^l_{\gamma(i,n)}$ au-dessus de C. De plus il existe $\lambda_{i,j,j'} \in \mathbb{F}_p$ pour $i \in \{0, \dots, n\}$, $j' \in J_i$ et $j \in \{0, \dots, l\} \setminus J_i$ tels que pour tout i et $j \notin J_i$,

$$a^j_{\gamma(i,n)} - \sum_{j' \in J_i} \lambda_{i,j,j'} a^{j'}_{\gamma(i,n)} = b^j_{\gamma(i,n)} - \sum_{j' \in J_i} \lambda_{i,j,j'} b^{j'}_{\gamma(i,n)} = c^j_i \in C.$$

Maintenant on utilise la définition de R'_n correspondant à R_n dans le lemme 3.6.9.

Si l'on définit pour tout $i \in \{0, \dots, n\}$ et $j \in \{0, \dots, l\}$, a'^j_i par $a^j_{\gamma(i,n)}$ si $j \in J_i$ et par c^j_i sinon, et de la même manière (b'^j_i), on a alors

$$R'_n((a'^j_i), \bar{c}) = P_n((a^j_{\gamma(i,m)}), \bar{c}) = 0$$

et

$$R'_n((b'^j_i), \bar{c}) = P_n((b^j_{\gamma(i,m)}), \bar{c}) \neq 0.$$

On peut donc appliquer le lemme et on en déduit qu'il y a pour un i une combinaison linéaire non nulle de $(a^j_{\gamma(i,n)})_{j \in J_i}$ dans C. Ce qui contredit la définition de J_i.

Cette description des types implique que pour tout $a \in (G_\beta)^{l+1}$ et tout C ensemble de paramètres, la base canonique du type de a sur C est dans la clôture algébrique de a. Le groupe G_β est donc 1-basé (1.1.9). $\lhd$

Remarque. A un type p de rang U égal à ω, on peut associer une prégéométrie : il suffit de prendre comme relation de dépendance la déviation. Dans le cas où p est 1-basé alors la prégéométrie est nécessairement localement modulaire. Dans la construction précédente du groupe 1-basé G_β, la prégéométrie associée à p_β est la suivante : une suite $a^0, \dots, a^l$ n'est pas libre si et seulement si il existe des entiers $i \leq n$ tels que la suite $a^0_{\gamma(i,n)}, \dots, a^l_{\gamma(i,n)}$ est linéairement dépendante sur $\mathbb{F}_p$. Cette prégéométrie est donc une "limite" d'espaces vectoriels sur $\mathbb{F}_p$.

Proposition 3.6.10. *Pour tout entier n et m il existe des sous- groupes additifs de rang U égal à $\omega \cdot n + m$.*

$\triangleright$ Il suffit d'utiliser un sous-groupe additif G de rang égal à ω et un sous-groupe additif H de rang égal à 1. Alors $G^{\times n} \times H^{\times m}$ est de rang $\omega \cdot n + m$. A l'aide des bijections λ_k, on peut se ramener à un sous-groupe de $(L, +)$. $\triangleleft$

Question 3.6.11. Existe-il des groupes de rang U égal à ω^2 ?