REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE

Université Mohamed Boudiaf de M'sila
Faculté des Mathématiques et de l'Informatique
Département de Mathématiques

Mémoire de Master

Domaine : Mathématiques et Informatique
Filière : Mathématiques
Option : Algèbre et Mathématiques Discrètes

Thème

Formes trilinéaire alternées et (CCEG ou BMC)

Présenté par :
SABKHA Fatiha

Devant le jury composé de :

M^r *MIHOUBI* Douadi	Pr,	Université de M'sila	**Président**.
M^r *MIDOUNE* Nourdine	M.CA,	Université de M'sila	**Encadreur**.
M^r *HABOB* Lakhdar	M.CB,	Université de M'sila	**Examinateur**.

Année universitaire 2020/2021

Remerciements

Avant tout je remercie **Allah**, le tout puissant d'avoir, éclaire ma vie, renforce mon courage et ma volanté pour finir ce travail.

J'exprime mes meilleurs remerciement à mon encadreur **Midoune Noureddine**, qui a accepté de diriger ce mémoir en témoignant sa confiance.

Je tient aussi à exprimer mes vifs remerciement les membres du jury : Monsieur **Mihoubi Douadi** et Monsieur **Habob Lakhdar** d'avoir accepté d'examiner cette mémoire.

J'accorde tout mes respect à ceux qui m'ont soutenus, en particulier à mes chers parents, mes soeurs, mes frères et mes amies.

Table des matières

Introduction

Soit E un espace vectoriel de dimension finie n sur un corps commutatif K.

La classification des trivecteurs (ou formes trilinéaires alternées), c'est-à-dire la détermination des orbites, et un représentant typique de chaque orbite, est l'étude de l'action du groupe linéaire $GL(E)$ sur l'espace vectoriel des trivecteurs $\Lambda^3 E$ (ou des formes trilinéaires alternées $Alt_3(E)$).

De l'isomorphisme $\Lambda^3 E^* \simeq (\Lambda^3 E)^* \simeq Alt_3(E)$, on parle indifféremment des formes trilinéaires alternées et des trivecteurs .

Plusieurs auteurs ont étudié les formes trilinéaires alternées. Il n'y a qu'un nombre fini d'orbites pour $n \leq 8$ dont la liste est donnée dans [4], [6], [8],

[11] et [10].

Pour classifier les trivecteurs, on utilise le plus souvent les invariants algébriques, par exemple, le groupes d'automorphisme d'un trivecteur ω, $Aut(\omega)$, car, deux trivecteurs ω_1 et ω_2 sont équivalents si et seulement si leurs groupes d'automorphismes $Aut(\omega_1)$ et $Aut(\omega_2)$ le sont.

Si $Aut(\omega_1)$ et $Aut(\omega_2)$ ne sont pas isomorphes, alors, leurs trivecteurs ω_1 et ω_2 ne le sont pas.

Donc, pour classifier les trivecteurs, il est indisponsable de déterminer les groupes d'automorphismes de chaque trivecteur sur un corps algébriquement clos de caractéristique quelconque.

Dans ce mémoire, nous rappelons l'essentiel des résultats connus sur la classification des trivecteurs de rang $n \leq 7$, puis nous déterminons les groupes d'automorphismes de chaque trivecteur sur un corps algébriquement clos, pour $n \leq 6$.

Dans le premier chapitre, on donne des généralités sur le produit tensoriel, produit exterieure, scindabilité, invariants, groupe d'automorphismes, commutant et parties stables.

Le deuxième chapitre est consacré à la relation entre les formes trilinéaires alternées et les courbes cubiques elleptiques generalisées (CCEG). De plus nous donnons les proprietés de ses courbes.

Après avoir donné la classification des trivecteurs pour $n \leqslant 7$, nous déterminons les CCEG de Hall.

Chapitre 1

Préliminaires

1.1 Produit tensoriel

Définition 1.1 Soit E un espace vectoriel sur un corps commutatif K.

Il existe un espace vectoriel sur K, notée $E \otimes E$ qui se lit E tenseur E et une forme bilinéaire

$$\begin{array}{rccc} \varphi_1 : & E \times E & \rightarrow & E \otimes E \\ & (u, v) & \rightarrow & \varphi_1 (u, v) \end{array}$$

tel que, pour toute forme bilinéaire

$$\begin{array}{rccc} \varphi_2 : & E \times E & \rightarrow & E \otimes E \\ & (u, v) & \rightarrow & \varphi_2 (u, v) \end{array}$$

il existe une unique forme linéaire $\varphi : E \otimes E \rightarrow K$ telle que $\varphi_2 = \varphi \circ \varphi_1$.

$$\begin{array}{ccc} E \times E & \overset{\forall \varphi_2}{\longrightarrow} & K \\ \exists \varphi_1 \downarrow & \nearrow_{\exists ! \varphi} & \\ E \otimes E & & \end{array}$$

l'ensemble des formes bilinéaires de $E \times E$ dans K, s'identifie à l'ensemble des formes linéaires de $E \otimes E$ dans K

$$\begin{array}{rcl} \varphi_1(E,E;K) & \simeq & (E\otimes E;K) \\ \varphi_2 & \to & \varphi \end{array}$$

et cette propriété caractérise $E\otimes E$. Les éléments de $E\otimes E$ sont les $x_i\otimes x_j$.
On pose $T^3(E)=E\otimes E\otimes E=\otimes^3 E$.

1.2 produit extérieure

Définition 1.2 On note $\Lambda^3 E$ le quotient de $T^3(E)$ par le sous-espace vectoriel engendré par les éléments $x_1\otimes x_2\otimes x_3$ où $x_i=x_j$ pour 2 indices $i\neq j$. On appelle $\Lambda^3 E$ la puissance extérieure 3−ième de E.

On note $x_{_1}\wedge x_2\wedge x_3=\overline{x_1\otimes x_2\otimes x_3}$ qui se lit x_1 extèrieur x_2 extèrieur x_3.

1. La puissance extérieure $\Lambda^3 E$ est défininissable d'une manière analogue au produit tensoriel.

$$\begin{array}{ccc} \omega : E\times E\times E & \overset{\forall\omega_1}{\to} & K \\ (x_1,x_2,x_3) & \to & \omega(x_1,x_2,x_3) \\ \omega_2\downarrow & \nearrow_{\exists!\omega} & \\ \Lambda^3\omega & & \end{array}$$

$$\omega_1=\omega\circ\omega_2$$

$$\omega(x_1,x_2,x_3)=x_{_1}\wedge x_2\wedge x_3$$

$$\omega(x_{_1}\wedge x_2\wedge x_3)=\omega(x_1,x_2,x_3)$$

2.

$$\begin{array}{rcl} (x+y)\wedge(x+y) & = & 0 \\ & = & x\wedge x+y\wedge y+x\wedge y+y\wedge x \\ x\wedge y & = & -y\wedge x. \end{array}$$

1.2.1 Support et Rang

On appelle support de ω et on note S_ω le plus petit sous-espace F de E tel que $\omega \in \Lambda^3 F$; la dimension de S_ω s'appelle le rang de ω qu'on note $rg(\omega)$.

Exemple Si $\omega = e_1 \wedge e_2 \wedge e_3$, $rg(\omega) = 3$.

1.2.2 Radical

Soit $\omega \in \Lambda^3 E^*$ une forme trilinéaire alterneé, le radical de ω est l'ensemble

$$Rad(\omega) = \{x \in E / \omega(x, y, z) = 0, \forall y, z \in E\}$$

Si $Rad\ \omega = \{0\}$, on dit que ω est non dégénérée ou de rang maximal.

1.2.3 Vecteure décomposable

Un trivecteur non nul ω est appelé décomposable s'il existe x, y, z dans E tel que $\omega = x \wedge y \wedge z$. Un trivecteur est somme de trivecteurs décomposables :

Si $\dim E = n$ et $\{e_1, ..., e_n\}$ une base de E, $\omega = \sum \alpha_{ijk} e_i e_j e_k$ et $\dim \Lambda^3 E = C_n^3$.

Remarque 1.1 On écrit souvent $x_1 x_2 x_3$ ou lieu de $x_1 \wedge x_2 \wedge x_3$.

1.2.4 Vecteur divisible

Soit ω un trivecteur non nul, ω est un trivecteur divisible s'il existe un

$$x \in E - \{0_E\} \quad \text{et } u \in \Lambda^2 E_2 \quad \text{tel que} \quad E = Kx \oplus E_2 \text{ et } \omega = x \wedge u.$$

1.2.5 L'action d'un groupe sur un ensemble

Définition 1.3 L'action du groupe linéaire $GL(E)$ sur l'ensemble des formes trilinéaires alternées $Alt_3(E)$, est définie par :

Pour $f \in GL(E)$ et $\omega : E \times E \times E \to K$ une forme trilinéaire alternée, on a $f.\omega(x, y, z) = \omega(f(x), f(y), f(z))$ satisfaisant aux conditions suivantes :

pour tous $f_1, f_2 \in GL(E)$, ω une forme trilinéaire alternée

1. $(f_1 \circ f_2).\omega = f_1.(f_2.\omega)$
2. $Id_E.\omega = \omega$.

Définition 1.4 L'action du groupe linéaire $GL(E)$ sur l'espace vectoriel $\Lambda^3 E$, est définie par : pour tous $f \in GL(E)$, $\omega \in \Lambda^3 E$, $f.\omega = (\Lambda^3 f)(\omega)$ où $\Lambda^3 f$ est un endomorphisme de $\Lambda^3 E$, définie par : $\Lambda^3 f(x \wedge y \wedge z) = f(x) \wedge f(y) \wedge f(z)$.

D'après l'isomorphisme $\Lambda^3 E^* \simeq (\Lambda^3 E)^*$, on emploi les deux définitions.

1.2.6 Formes trilinéaires alternées

L'espace vectoriel $\Lambda^3 E$ peuvent être défini d'une autre manière en utilisant les formes trilinéaires alternées. Pour tout espace vectoriel E sur un corps commutatif K, l'ensemble $Alt_3(E)$ des formes trilinéaires alternées $h : E \times E \times E \longrightarrow K$ est lui-même un K espace vectoriel pour les opérations terme à terme habituelles.

Définition 1.5 Une forme trillinéaire

$$\begin{array}{rccc} \omega : & E \times E \times E & \to & K \\ & (x,y,z) & \to & \omega(x,y,z) \end{array}$$

est dite alternée si $\omega(x,y,z) = 0$ dèsque $x_i = x_j$; pour un couple d'indices $i \neq j$.

Pour chaque application linéaire

$$\begin{array}{rccc} f : & E & \to & E \\ \Lambda^3 f : & \wedge^3 E & \to & \wedge^3 E \\ & x_1 \wedge x_2 \wedge x_3 & \to & \Lambda^3 f(x_1 \wedge x_2 \wedge x_3) \\ & & = & f(x_1) \wedge f(x_2) \wedge f(x_3). \end{array}$$

1.2.7 Parties stables

Lemme 1.1 *Soit E un espace vectoriel sur le corps K et considérons la forme bilinéaire alternée définie par :*

$\omega^x(y,z) = \omega(x,y,z)$, ω une forme trilinéaire alternée.

Alors, l'ensemble $R_i = \{x \in E / rg\omega^x = 2i\}$ $(0 \leq 2i \leq n)$ est stable par $Aut(\omega)$, c'est-a-dire $f(R_i(\omega)) \subset R_i(\omega)$ pour $f \in Aut(\omega)$.

Preuve. Remarque. On utilise les parties stables pour déterminer les groupes d'automorphismes. ■

Lemme 1.2 *Soit E un espace vectoriel sur le corps K, de dimension finie, V_1 et V_2 deux sous-espace de E différents et tel que $\dim V_1 = \dim V_2$. Si f est un endomorphisme de E qui laissent stable la réunion de V_1 et V_2, c'est-a-dire $f(V_1 \cup V_2) \subset V_1 \cup V_2$, alors on a $[f(V_1) \subset V_1$ et $f(V_2) \subset V_2]$ ou $[f(V_1) \subset V_2$ et $f(V_2) \subset V_1]$.*

Preuve. Comme $f(V_1 \cup V_2) \subset V_1 \cup V_2$, on obtient :

$$\begin{cases} f(V_1) \subset V_1 \cup V_2 \\ f(V_2) \subset V_1 \cup V_2 \end{cases} \Rightarrow \begin{cases} f(V_1) \cap (V_1 \cup V_2) = f(V_1) \\ f(V_2) \cap (V_1 \cup V_2) = f(V_2) \end{cases}$$

$$\Rightarrow \begin{cases} (f(V_1) \cap V_1) \cup (f(V_1) \cap V_2) = f(V_1) \ \textbf{I} \\ (f(V_2) \cap V_1) \cup (f(V_2) \cap V_2) = f(V_2) \ \textbf{II} \end{cases}$$

Or, la réunion de deux sous-espaces vectoriels est un sous espaces vectoriel si et seulement si l'un est inclus dans l'autre, ainsi :

$$\begin{cases} ((f(V_1) \cap V_1) \subset (f(V_1) \cap V_2)) \text{ ou } ((f(V_1) \cap V_2) \subset (f(V_1) \cap V_1)) \\ \text{et} \\ ((f(V_2) \cap V_1) \subset (f(V_2) \cap V_2)) \text{ ou } ((f(V_2) \cap V_2) \subset (f(V_2) \cap V_1)) \end{cases}$$

On remplace dans I et II on obtient :

$$\begin{cases} ((f(V_1) \cap V_1) = f(V_1)) \text{ ou } ((f(V_1) \cap V_2) = f(V_1)) \\ \text{et} \\ ((f(V_2) \cap V_1) = f(V_2)) \text{ ou } ((f(V_2) \cap V_2) = f(V_2)) \end{cases}$$

Ce qui implique que :

$$\begin{cases} (f(V_1) \subset V_1) \text{ ou } (f(V_1) \subset V_2) \\ \text{et} \\ (f(V_2) \subset V_1) \text{ ou } (f(V_2) \subset V_2) \end{cases}$$

On a quatre cas qui figurent :

$$\begin{cases} (f(V_1) \subset V_1 \text{ et } f(V_2) \subset V_2) \text{ ou } (f(V_1) \subset V_2 \text{ et } f(V_2) \subset V_1) \\ \text{et} \\ (f(V_1) \subset V_1 \text{ et } f(V_2) \subset V_1) \text{ ou } (f(V_1) \subset V_2 \text{ et } f(V_2) \subset V_2) \end{cases}$$

Les deux derniers cas sont impossibles car par exemple :

Si $f(V_1) \subset V_1$ et $f(V_2) \subset V_1$ comme $\dim f(V_1) = \dim V_1$

et $\dim f(V_2) = \dim V_2$.

D'où $f(V_1) = V_1$ et $f(V_2) = V_1 \Rightarrow V_1 = V_2$ (f injective) ce qui est absurde car $V_1 \neq V_2$. ■

1.2.8 Eléments scindables

Soient E_1 et E_2 deux sous-espaces supplémentaires de E, $\Lambda^3 E$ s'identifie à :

$$\bigoplus_{k=0}^{k=3} \left(\Lambda^k E_1 \otimes \Lambda^{3-k} E_2\right).$$

Un élément $\omega \in \Lambda^3 E$ est dit scindabl, s'il existe une décomposition $E = E_1 \oplus E_2$ telle que : $\omega \in E_1 \otimes \Lambda^2 E_2$ vu comme facteur direct de $\Lambda^3 E$. Si $\dim E_1 = r$, on dit que ω est r-scindable. La scindabilité est une généralisation de la divisibilité. en effet ω est divisible si et seulement si ω est 1-scindable, propriété qui ne dépend pas du corps de base car c'est équivalent à dire que l'application :

$$\begin{array}{ccc} E & \longrightarrow & \Lambda^4 E \\ x & \longrightarrow & x\omega \end{array} \quad \text{n'est pas injective.}$$

Soit ω un élément r-scindable et $\{e_1, ..., e_r\}$ une base de E_1, $\omega = \sum_{i=1}^{r} e_i u_i$ où $u_i \in \Lambda^2 E_2$. Les u_i sont déterminés de façon unique par la base $e_1, ..., e_r$ de E_1. Alors ω est déterminé par le sous-espace vectoriel F de $\Lambda^2 E_2$ engendré par les u_i, en effet, si on change de base dans E_1, et si la nouvelle base f_j est donnée par :

$$e_i = \sum_{j=1}^{r} a_{ij} f_j,$$

$$\omega = \sum_{1}^{r} e_i u_i = \sum_{j=1}^{r} f_j \left(\sum_{j=1}^{r} a_{ij} u_i \right) = \sum_{j=1}^{r} f_j v_j,$$

les v_j s'obtiennent donc à partir des u_i par le changement de base contragrédient de celui qui fait passer de la base $\{f_j\}$ à la base $\{e_i\}$. Cela se voit aussi en utilisant l'isomorphisme naturel entre $E_1 \otimes \Lambda^2 E_2$ et $Hom\left(E_1^*, \Lambda^2 E_2\right)$, si φ est l'élément de $Hom\left(E_1^*, \Lambda^2 E_2\right)$ canoniquement associé à ω, F n'est autre que $\varphi\left(E_1^*\right)$.

un même trivecteur peut être scindable pour plusieurs valeurs de l'entier r comme le montre l'exemple :

$\omega_{7,3} = e_1 e_2 e_3 + e_3 e_4 e_5 + e_5 e_6 e_7$ qui est 2 et 3−scindable :

$\omega_{7,3} = e_3 \left(e_1 e_2 + e_4 e_5\right) + \left(e_5 e_6\right) e_7 = e_1 \left(e_2 e_3\right) + e_4 \left(e_5 e_3\right) + \left(e_5 e_6\right) e_7.$

1.2.9 Suite exacte

Définition 1.6 Soit $G' \xrightarrow{f} G \xrightarrow{g} G''$ une suite d'homomorphismes de groupes. Nous dirons que cette suite est exacte si

$$\operatorname{Im} f = \ker g.$$

Exemple 1.1 Si H est un sous groupe distingué de G, la suite

$$H \xrightarrow{j} G \xrightarrow{\varphi} G/H$$

est exacte (j étant l'injection et φ la projection canonique).

Remarque 1.2 Dire, la suite

$$1 \longrightarrow G' \xrightarrow{f} G \xrightarrow{g} G'' \longrightarrow 1$$

est exacte, signifie que f est injectif, que $\operatorname{Im} f = \ker g$ et que g est surjectif .

1.2.10 Invariant et trivecteurs : l'invariant $Aut\left(\omega\right)$

Le groupe des automorphismes de ω, $Aut\left(\omega\right)$ est le stabilisateur de ω dans l'action de $GL\left(E\right)$, c'est à dire le sous-groupe de $GL\left(E\right)$ des automorphismes de E qui laissent

ω invariant

$Aut\,(\omega) = \{f \ / \ f \in GL(E) \text{ et } \Lambda^3 f(\omega) = \omega\} = \{f \ \ / f \in GL(E) \text{ et } f \cdot \omega = \omega\}$.

L'orbite de ω par $GL(E)$ est alors en bijection avec l'ensemble des classes à gouche $GL(E)/Aut(\omega)$.

Chapitre 2

Courbes cubiques elliptiques généralisées

Définition 2.1 Une courbe cubique elliptique généralisée ($CCEG$) est un couple (G, T) formé d'un ensemble G et d'une famille T de triplets non ordonnés tel que, pour chaque x et y dans G il existe un seul z de G tel que $((xyz)) \in T$.

Pour travailler algébriquement, nous devons introduire les quasigroupes associés à une $CCEG$. Rappellons qu'un quasigroupe est un ensemble G muni d'une loi de composition interne, disons $x, y \longrightarrow x \cdot y$, telle que toute équation de la forme $\alpha \cdot x = b$ (resp. $y \cdot \alpha = b$) admette une solution unique dans G. Si de plus la loi admet un neutre bilatère e, on dit qu'on a une boucle.

Soit (G, T) une $CCEG$. On définit une loi sur G, dit "loi milieu" $x, y \longmapsto x \cdot y = z$, en décidant que z est l'unique point caractérisé par $((xyz)) \in T$. Pour tout u fixé dans G, on peut organiser G par une loi, notée $\star_u$, qui à x, y de G fait correspondre $x \star_u y = u \cdot (x \cdot y)$.

On déduit de la définition de la loi milieu que $x \cdot y = y \cdot x$ et $u \cdot (x. \cdot u) = x$. Par suite G organisé par la loi binaire qui à x, y fait correspondre $(x \star_u y)$ est une boucle commutative de neutre u, dite "boucle associée d'origine u".

Reprenons quelques notations de nature géométrique

Définition 2.2 Pour tout point $x \in G$ le tangentiel de x est l'unique point t pour lequel $((xxt)) \in T$. Si $t = x$ on dit que x est "point d'inflexion" de G. L'ensemble $I(G)$ des points d'inflexion est celui des idempotents de la loi milieu. Le rang d'une

$CCEG$ est le plus petit cardinal r pour lequel il existe un système générateur de cardinal r.

Définition 2.3 Une boucle L est appelée boucle de moufang commutative (BMC) si

1. $x \cdot y = y \cdot x$
2. $x^2 \cdot (y \cdot z) = (x \cdot y)(x \cdot z)$

pour tout x, y et $z \in L$.

Définition 2.4 Les $CCEG$ entropiques sont celles où

$$(x \cdot y) \cdot (z \cdot t) = (x \cdot z)\,(y \cdot t) \text{ identiquement.}$$

Quand l'entropicité est seulement vérifiée dans tout sous-système de rang ≤ 3 on dit que (G, T) est une $CCEG$ terentropique ($CCEGT$). Plus particulièrement une $CCEGT$ où tout point est d'inflexion est une $CCEG$ de Hall ($CCGH$).

2.1 Théorèmes de structure des CCEG

Proposition 2.1 **i)** *soit (Q, T) une $CCEG$ entropique et u un élément arbitraire de Q, alors $(Q, \star_u)$ est un groupe abélien.*

ii) *Pour tout couple u, v d'élements de la $CCEG$ entropique (Q, T), les deux groupes $(Q, \star_u)$ et $(Q, \star_v)$ sont isomorphes.*

Preuve.

i) la loi $x, y \longrightarrow x \star_u y = u \cdot xy$ est commutative ; elle admet u comme neutre. En outre $x' = u^2 x$ est l'inverse de x car :

$x \star_u u^2 x = u \cdot (x \cdot u^2 x) = u \cdot u^2 = u.$

Quel que soit $x, y, z \in Q$, nous avons $xy \cdot uz = xu \cdot yz$ en en multipliant les deux memberes par u^2, on trouve :

$$(u \cdot xy) \cdot z = x \cdot (u \cdot yz)\,. \tag{2.1}$$

On multiplie les deux membres de 2.1 par u on obtient

$$(x \star_u y) \star_u z = x \star_u (y \star_u z),$$

ainsi $(Q, \star_u)$ est un groupe abélien.

ii) Posons $f(x) = x \star_u v = u \cdot xv$, on a alors :

$$\begin{aligned} f(x) \star_v f(y) &= v((u \cdot vx)(u \cdot vy)) \\ &= v(u^2 \cdot (v^2 \cdot xy)) \\ &= vu^2 \cdot (x \cdot y) \\ &= u \cdot (v \cdot (u \cdot xy)) \\ &= f(x \star_u y). \end{aligned}$$

Donc f est un morphisme et comme f est une permutation de Q, nous avans bien un isomorphisme. On peut donc définir le groupe associé au $CCEG$ entropique (Q, T) comme étant l'un quelconque des gropes $(Q, \star_u)$. ■

Théorème 2.1 *Si $(A, +)$ est un grope abélien, pour chaque c de A la famille T_c des triplets non ordonnés $((x, y, z))$ caractérisés par $x+y+z = c$ font de A une $CCEG$ entropique. Toute $CCEG$ entropique (G, T) s'obtient ainsi à partir d'un groupe obélien unique à un isomorphisme près (et isomorphe à $(G, \star_u)$ pour tout u de G).*

Preuve. Pour chaque x et $y \in A$, il existe un seul z vérifiant $z = x \circ_c y = c - x - y \in A$ et $((xyz)) \in T$. Puisque $x \circ_c y = y \circ_c x$ et $x \circ_c (y \circ_c x) = x$ donc (A, T) est une $CCEG$ et comme $(A, +)$ est un groupe, on en déduit :

$$(x \circ_c y) \circ_c (z \circ_c t) = (x \circ_c z) \circ_c (y \circ_c t).$$

Donc $(A, +)$est une $CCEG$ entropique.

Si $(A, +)$ n'est autre que le groupe $(A, \star_u)$ de neutre u associé au $CCEG$ entropique (A, T) de la proposition 2.1 alors on réobtient $x \cdot y = x \circ_c y$ en choisissant $c = u^2 = u \cdot u$.

Donc toute $CCEG$ entropique (A, T) s'obtient ainsi à partir d'un groupe abélien unique à un isomorphisme près (et isomorphe à $(A, \star_u)$ pour tout u). Donc si (Q, T) est une $CCEG$ et u un élément arbitraire de Q, alors (Q, T) est entropique

si et seulement si $(Q, \star_u)$ est un groupe abélien. Dans ce cas, le groupe $(Q, \star_u)$ est essentiellement indépendant du choix de u. ■

Remarque 2.1 A différents choix de c dans $(A, +)$ correspondent des $CCEG$ entropiques non nécessairement isomorphes.

Exemple 2.1 Soit $\mathbb{Z}_n$ l'ensemble des restes modulo n où n est un entier > 0. Les familles de triplets non ordonnés $T_1 = \{((x, y, 1 - x - y))\}$ et $T_0 = \{((x, y, -x - y))\}$ définissent deux structures de $CCEG$ entropiques non isomorphes si n est multiple de 3, (car seule $(\mathbb{Z}_n, T_0)$ admet un point d'inflexion), bien qu'ayant même groupe associé $(\mathbb{Z}_n, +)$.

Afin de préciser la nature de la classe des différentes $CCEG$ entropiques associées à un même groupe, il faut introduire une notion qui généralise la notion d'isomorphisme.

Définition 2.5 On dit que deux quasigroupes $(Q, \cdot)$ et $(R, \circ)$ sont isotopes s'il existe un triplet (α, β, γ) de bijections de Q sur R tel que :

$$a^\alpha \circ b^\beta = (a \cdot b)^\gamma \qquad \text{pour tous } a, b \in Q.$$

La relation d'isotopie est une relation d'équivalence dans la famille des quasigroupes.

Théorème 2.2 *Si deux groupes sont isotopes, alors ils sont aussi isomorphes.*

Preuve. On peut voir facilement que la $CCEG$ entropique (Q, T) et le groupe $(Q, \star_u)$ dans la proposition 2.1 sont isotopes. Donc d'après le théorème 2.2 chaque $CCEG$ entropique est isotope à un groupe abélien, qui est unique à un isomorphisme près. Autrement dit dans chaque classe d'isotopie des $CCEG$ entropiques, on trouve un seul groupe abélien.

Ainsi il existe une correspondance biunivoque entre les classes d'isotopie des $CCEG$ entropiques et les classes d'isomorphismes de groupes abéliens.

Schwenk a donné une classification de $CCEG$ entropiques non isomorphes deux à deux dont la boucle associée est isotope à un groupe abélien donné. On va reprendre ses résultats. ■

Lemme 2.1 *On a l'isomorrphisme suivant* $(G,T_e)\times(H,T_f)\cong\left(G\times H,T_{(e,f)}\right)$.

Ce lemme nous permet de construire toutes les $CCEG$ entropiques à partir des $CCEG$ entropiques où chacune s'obtient à partir d'un groupe cyclique.

Théorème 2.3 *Soit* G *un groupe cyclique isomorphe à* $\mathbb{Z}_m$ *on à les isomorphismes siuvants :*

1. $(G,T_e)\cong(G,T_{e+3})$;
2. $(G,T_1)\cong(G,T_2)$;
3. *Si* $p\gcd(|G|,3)=1$, *alors* $(G,T_0)\cong(G,T_1)$.

Preuve. L'application $\alpha:(G,T_e)\longrightarrow(G,T_{e+3})$ définie par $\alpha(a)=a+1$ est un homorphisme puisque pour tous $x,y\in G$ on a :

$$\begin{cases}\alpha(x\cdot y) &= \alpha(e-x-y)\\ &= e-x-y+1,\end{cases}\quad\text{et}\quad\begin{cases}\alpha(x)\cdot\alpha(y) &= e+3-\alpha(x)-\alpha(y)\\ &= e+3-(x+1)-(y+1)\\ &= e-x-y+1.\end{cases}$$

La preuve que α est bijective est évidente.

On considère l'application $\beta:(G,T_1)\longrightarrow(G,T_2)$ définie par $\beta(a)=-a+1$. β est bijective. De plus β est un homorphisme :

$$\begin{cases}\beta(x\cdot y) &= \beta(1-x-y)\\ &= x+y,\end{cases}\quad\text{et}\quad\begin{cases}\beta(x)\cdot\beta(y) &= (-x+1)\cdot(-y+1)\\ &= 2-(-x+1)-(-y+1)\\ &= x+y.\end{cases}$$

Pour (3), on a l'ordre de G :

• Soit $3k-1$ avec k un entier, dans ce cas on utilise l'application bijective γ_1 : $a\longmapsto a+k$, on vérifie aisément que $\gamma_1$est un homorphisme.

• Soit $3k-2$ en utilisant $\gamma_2:a\longmapsto a+(2k-1)$, on trouve la démonstration de(3). ■

Maintenant on est en mesure d'énoncer le théorème suivant :

Théorème 2.4 *Soit* $(A,+)$ *un groupe abélien d'ordre non divisible par* 3. *Il existe à un isomorphisme près une seule CCEG entropique isotope à* $(A,+)$.

Lemme 2.2 *Soit* $G\cong Z_{3^r}$ *et* $H\cong Z_{3^s}$ *avec* $r\leq s$, *alors :*

$$\left(G\times H,T_{(0,1)}\right)\cong\left(G\times H,T_{(1,1)}\right).$$

Preuve. On note $y \equiv x \ MOD \ n$ pour $y \equiv x \bmod n$ et $0 \leq y < n$. considérons l'application :

$$\alpha : \left(G \times H, T_{(0,1)}\right) \longrightarrow \left(G \times H, T_{(1,1)}\right)$$

$$(a, b) \longrightarrow ((a + b) \, MOD \ 3^r, b)$$

tout d'abord α est bijective car l'inverse de α est défini par

$$\alpha^{-1}((a, b) := (a - b) \ \ MOD \ 3^r, b).$$

L'image du milieu de deux point est :

$$\begin{aligned} \alpha((a_1, b_1) \cdot (a_2, b_2)) &= \alpha((0, 1) - (a_1, b_1) - (a_2, b_2)) \\ &= \alpha(-a_1 - a_2, 1 - b_1 - b_2) \\ &= ((1 - a_1 - a_2 - b_1 - b_2) \ \ MOD \ 3^r, 1 - b_1 - b_2). \end{aligned}$$

Et on a :

$$\begin{aligned} \alpha(a_1, b_1) \cdot \alpha(a_2, b_2) &= (1, 1) - ((a_1 + b_1) \ \ MOD \ 3^r, b_1) - ((a_2 + b_2) \ \ MOD \ 3^r, b_2) \\ &= (1 - (a_1 + b_1) \ \ MOD \ 3^r - (a_2 + b_2) \ \ MOD \ 3^r, 1 - b_1 - b_2) \\ &= (1 - (a_1 + a_2 + b_1 + b_2) \ MOD \ 3^r, 1 - b_1 - b_2) \\ &= ((1 - a_1 - a_2 - b_1 - b_2) \ \ MOD \ 3^r, 1 - b_1 - b_2). \end{aligned}$$

Donc α est isomorphisme. ■

Théorème 2.5 (**Schwenk**) *Soient $(A, +)$un groupe abélien d'ordre fini $3^n m$ avec m non divisible par 3, et H son sous-groupe d'ordre 3^n, isomorphe à*

$(\mathbb{Z}_{3^{r_1}})^{l_1} \times (\mathbb{Z}_{3^{r_2}})^{l_2} \times .... \times (\mathbb{Z}_{3^{r_k}})^{l_k}$ *avec* $l_1 r_1 + l_2 r_2 + ... + l_k r_k = n$ *et* $r_1 < .... < r_k$.

Alors il existe exactement $k + 1$ CCEG entropiques non isomorphes associées à $(A, +)$.

Théorème 2.6 *Soit G un groupe abélien de type fini, mais d'ordre infini. Alors*

1. *G est isomorphe à un produit direct de forme : $Z^t \times A$ où A est un groupe abélien d'ordre fini et t un entier ≥ 1.*
2. *Si A vérifie les hypothéses du théorème 2.5, c'est-à-dire s'il y a exactement k facteurs directs de A non isomorphes et de forme $\mathbb{Z}_{3^{r_i}}$, alors il y a très exactement $k + 2$ CCEG non isomorphes associées à $(G, +)$.*

Théorème 2.7 *[2](**classification de Buekenhout**) Il y a à un isomorphisme près 26 CCEG d'ordre ≤ 8, dont 13 sont entropiques ; parmi celles-ci il y en a 12 qui*

proviennent d'une courbe cubique elliptique.

Soit G un groupe abélien fini et $p > 0$ un entier premier.

Quand $pG = \{px; x \in G\} = \{0\}$, on dit que $(G, \cdot)$ est un p-groupe abélien élémentaire ; c'est le groupe abélien sous-jacent d'un espace vectoriel sur $\mathbb{Z}_p$, il est donc isomorphe à un $(\mathbb{Z}_p)^l$, et admet 1 (resp 2) CCEG isotopes quand $p \neq 3$ (resp. $p = 3$).

Dans un 2-groupe abélien élémentaire $(G, +)$, la famille de triplets non ordonnés de forme $((x, y, x + y))$ définit une structure de CCEG entropique, dite "binaire". Pour $|G| = 4$, on obtient l'exemple (P, T)de 2.1

(resp. l'unique CCEG entropique d'ordre ≤ 8 qui ne provient d'aucune courbe elliptique).

Théorème 2.8 *Soit (G, T) une CCEG de loi milieu $x \cdot y$; posons $x^2 = x^{(2)} = x \cdot x$. Les 3 conditions suivantes sont équivalentes :*

i) $x^2 \cdot yz = xy \cdot xz$;

ii) $x^2 z \cdot y = (xy \cdot z)\, x$;

iii) $x \cdot yz = x^2 z \cdot xy$.

Preuve. En multipliant les deux membres de (i) pa z^2 :

$z^2 (x^2 \cdot yz) = z^2 (xy \cdot xz)$

$zx^2 \cdot (z \cdot yz) = (z \cdot xy) \cdot (z \cdot xz)$ par symetrie $z \cdot yz = y$ et $z \cdot xz = x$ ainsi l'égalité (ii) est vérifiée.

On passe de (ii) à (iii) en faisant $xy = Y$ on obtient $x^2 z \cdot xY = Yz \cdot x$, qui est équivalente à(iii).

En multipliant les deux membres de (iii) par xy on obtient $xy \cdot (x \cdot yz) = x^2 y$, et en faisant $yz = Z$; on trouve (i).

Chacune des identités (i),(ii) et (iii) caractérise, parmi les $CCEG$, ceux qui sont des $CCEG$ terentropiques.

Nous allons voir que la correspondance entre $CCEG$ terentropiques et Boucles de Moufang Commutatives (BMC) généralise la correspondance entre $CCEG$ entropiques et groupes abéliens. ■

Théorème 2.9 *Soit (G, T) une CCEG terentropique de loi milieu $x \cdot y$.*

1. *Pour chaque $u \in G$, $(G, \star_u)$ est une boucle de Moufang commutative ; elle admet u^2 comme élément central.*

2. Les triples $((xyz))$ de T sont caractérisés par l'égalité $x \star_u y \star_u z = u^2$.

Preuve. La loi $x, y \longmapsto x \star_u y = u \cdot xy$ est commutative puisque $xy = yx$, elle admet u comme neutre car $u \cdot ux = x$. En outre si $x' = u^2 x$, pour tout y nous avans :

$$\begin{aligned}(x \star_u y) \star_u x' &= u\left((u \cdot xy) \cdot u^2 x\right) \\ &= u\left(u \cdot (xy \cdot x)\right) \\ &= y,\end{aligned}$$

en vertu du théorème 2.8 et de la symétrie.

Enfin puisque (G, T) est une $CCEG$ terentropique on a :

$$\begin{aligned}(a \star_u a) \star_u (x \star_u y) &= u \cdot \{ua^2 \cdot (u \cdot xy)\} \\ &= u \cdot \{u^2 \cdot (a^2 \cdot xy)\} \\ &= u \cdot \{u^2 (ax \cdot ay)\} \\ &= u \cdot \{u \cdot ax \cdot (u \cdot ay)\} \\ &= (a \star_u x) \star_u (a \star_u y).\end{aligned}$$

Ainsi $(G, \star_u)$ est une boucle de Moufang commutative ; son centre associatif $Z(G, \star_u)$ est l'ensemble des élément c vérifiant : $(u \cdot xy) \cdot c = (u \cdot cy) \cdot x$ pour tout x, y de G ou encore : $xy \cdot uc = cy \cdot ux$ pour tout x et y de G.

Or si $c = u \cdot u = u^2$ alors $uc = u$ et nous savons que $xy \cdot u = u^2 y \cdot ux$ identiquement 2.8 ; ainsi $u^2 \in Z(G, \star_u)$.

Nous avans vu que chaque x de $(G, \star_u)$ avait pour opposé $-x = u^2 x$. En particulier si $x = x \star_u y$, nous avons $-x = u^2 (u \cdot xy)$ et donc

$$\begin{aligned}u^2 - (x \star_u y) &= u \cdot (u^2 (u^2 (u \cdot xy))) \\ &= xy.\end{aligned}$$

Donc $x \star_u y \star_u z = u^2$. ■

Théorème 2.10 *Avec les conventions du théorème précédent, pour tout couple u, v d'élement de la $CCEG$ terentropique (G, T), les deux boucles de Moufang $(E, \star_u)$ et $(E, \star_v)$ son isomorphes par $x \longrightarrow x \star_u v = u \cdot (vx)$.*

Preuve. Posons $f(x) = x \star_u v$. On a

$$\begin{aligned} f(x \star_u y) &= (x \star_u y) \star_u v \\ &= u \cdot (v \cdot (u \cdot xy)) \quad \text{d'après le théorème 2.8.} \\ &= u^2 v \cdot xy, \end{aligned}$$

Par ailleurs

$$\begin{aligned} f(x) \star_v f(y) &= (x \star_u v) \star_v (y \star_u v) \\ &= v \cdot ((u \cdot xv) \cdot (\,\mathrm{u}yv)) \\ &= v \cdot (u^2 \cdot (xv \cdot yv)) \\ &= v\,(u^2 \cdot (v^2 \cdot xy)) \\ &= A \end{aligned}$$

car (G,T) est terentropique, en outre il résulte du théorème 2.8 que $A = vu^2 \cdot xy$. Nous avans montré que f est un morphisme de $(G, \star_u)$ sur $(G, \star_u)$. Comme f est une permutation de E (c'est une translation d'une boucle), nous avans bien un isomorphisme.

On peut donc définir "la boucle de Moufang commutative associée au $CCEG$ terentropique (G,T)" comme étant l'une quelconque des boucles $(G, \star_u)$. ■

Théorème 2.11 *Soient $(G,+)$ une BMC de neutre e et c un élément central de G, alors :*

1. *L'ensemble G organisé par la famille T_c des triplets non ordonnes de la forme $((x,y,c-x-y))$ est une $CCEGT$. Tout $CCEGT$ s'obtient ainsi.*
2. *La boucle de Moufang de neutre e associée à (G,T_c) n'est autre que $(G,+)$.*

Preuve. Posons ici $x \cdot y = x \circ_c y$. Cette loi est commutative puisque l'addition l'est.

En outre

$$\begin{aligned} x \cdot (x \cdot y) &= c - x - (c - x - y) \\ &= y. \end{aligned}$$

Par ailleurs

$$\begin{aligned} a \cdot a + x \cdot y &= 2c - 2a - x - y \\ &= a \cdot x + a \cdot y, \end{aligned}$$

donc $(a \cdot a) \cdot (x \cdot y) = (a \cdot x) \cdot (a \cdot y)$. Ainsi $(E, \cdot) = (E, \circ_c)$ est bien une $CCEGT$.

Toute $CCEGT$ peut être reconstruire par ce procédé : il suffit de prendre $c = u^2$ dans $(G, \star_u)$.

En outre, si on fait

$$u = e, \text{ alors } \begin{cases} u^2 &= u.u \\ &= c - 2e \\ &= c \end{cases} \text{ et } \begin{cases} x \star_e y &= e \circ_c (x \circ_c y) \\ &= e \circ_c (c - x - y) \\ &= c - e - (c - x - y) \\ &= x + y, \end{cases}$$

de sorte que $(G, +)$ coïncide avec la M-boucle $(G, \star_e)$ de neutre e associée à (G, T_c). ■

Exemple 2.2 Soit $(G, +)$ un 3-groupe abélien élémentaire. Les triples non ordonnés $((xyz))$ caractérisés par $x + y + z = 0$ font de G une $CCEG$ de Hall. Toute $CCEG$ de Hall s'abtient ainsi.

Les différentes $CCEGT$ correspondant à une BMC donnée forment une classe d'isotopie. Les différents choix de l'élément central c peuvent conduire à des $CCEGT$ non isomorphes, c'était déjà le cas, nous l'avons vu, dans la sous-classe des $CCEG$ entropiques.

Théorème 2.12 *Les $CCEGT$ possédant ou moins un point d'inflexion sont les $CCEGT$ dont la loi milieu s'écrit $x \cdot y = 3d - x - y$ dans une BMC convenable G où d est un élément arbitraire.*

Preuve. Supposons que $(E, +)$ est une BMC. On sait que l'ensemble $\theta(E, |)$ des élément de la forme $3x = x + x + x$ consitue un sous-groupe du centre $Z(E, |)$. Si $c \in Z(E, +)$, alors le $CCEGT$ (E, T_c) admet un point d'inflexion x si et seulement si $c = 3x$.

La loi milieu $x \cdot y$ d'une $CCEGT$ possédant un point d'inflexion u peut s'écrire sous la forme :

$$\begin{aligned} x \cdot y &= u^2 -_{\star_u} (x \star_u y) \\ &= u -_{\star_u} (x \star_u y) \\ &= -(x \star_u y). \end{aligned}$$

Et comme la BMC de neutre e associée à (E, T_c) n'est autre que $(E, +)$, on a : $x \cdot y = -x - y$. ■

Proposition 2.2 *[2]Si $(E, +)$ est une BMC de neutre e, alors les $CCEGT$ (E, T_c) que l'on obtient en prenant c dans $\theta(E, +)$ forment une classe complète d'isomorphie dont le représentant le plus simple est évidemment (E, T_e). Les $CCEGT$ répondant à cette description sont très exactement celles qui possèdent un point d'inflexion.*

Corollaire 2.1 *Si $(E, +)$ est une BMC où $\theta(E, +)$ coïncide avec le centre, alors il y a une seule $CCEGT$ associée à un isomorphisme près, à savoir (E, T_e).*

Remarque 2.2 ceci généralise le résultat de Schwenk sur l'unicité de la $CCEG$ associée à un groupe abélien fini d'ordre premier avec 3. Noter qu'on a toujours $\theta(E, +) \subseteq Z(E, +)$ dans toute BMC. Lorsque cette inclusion est stricte, il y a plusieurs $CCEG$ non isomorphes associées à $(E, +)$.

2.2 Examples de CCEGT et de BMC non entropiques

a) Soient $\mathbb{F}_3 = \mathbb{Z}_3$ le corps à trois élèments et $\mathbb{L}_3 = \mathbb{F}_3^4$ l'espace vectoriel des quadruplets de la forme $X = (x_1, x_2, x_3, x_4)$ avec $x_i \in \mathbb{F}_3$. A tout couple X, Y d'éléments de L_3, associons le scalaire $\delta(X, Y) = (x_1 - y_1)(x_2 y_3 - x_3 y_2)$ modulo 3.

L'ensemble L_3 organisé par la famille T des triplets non ordonnés de la forme :

$$((X, Y, (-x_1 - y_1, -x_2 - y_2, -x_3 - y_3, -x_4 - y_4 - \delta(X, Y)))),$$

est une $CCEGT$, tandis que la loi :

$$X \star Y = (x_1 + y_1, x_2 + y_2, x_3 + y_3, x_4 + y_4 + \delta(X, Y)),$$

fait de $\mathbb{L}_3$ une BMC.

On vérifie aisément qu'il y a deux $CCEGT$ non isomorphes dont $(\mathbb{L}_3, \star)$ est la BMC associée. En effet :

La BMC $(\mathbb{L}_3, \star)$ admet pour neutre $e = (0,0,0,0)$ et que $\alpha = (0,0,0,1)$ y est un élément central. Tout élément X de $\mathbb{L}_3$ vérifie $X \star X \star X = e \neq \alpha$. Danc la $CCEGT\,(\mathbb{L}_3, T_\alpha)$ n'admet aucun point d'inflexion, contrairement à $(\mathbb{L}_3, T_e)$ où tout point est point d'inflexion.

b) Soit toujours $\mathbb{F}_3 = \mathbb{Z}_3$. Posons $\mathbb{Z}_9$ et désignons par $\mathbb{N}_3$ le produit cartésien $\mathbb{F}_3^2 \times \mathbb{Z}_9$,

de terme générique $X = (x_1, x_2, x_3)$ avec x_1 et x_2 dans $\mathbb{F}_3$ et x_3 dans $\mathbb{Z}_9$. Etant donnés deux éléments X et Y de $\mathbb{N}_3$, nous désignons ici par $\delta\,(X,Y)$ l'élément $3\,((x_1 - y_1)\,(x_2 y_3 - x_3 y_2))$, considéré ici comme appartenant à $\mathbb{Z}_9$. La définition de cet entier modulo 9 ne recèle aucune ambiguïté, bien que x_1, y_1, x_2 et y_2 soient des entiers modulo 3. L'ensemble $\mathbb{N}_3$ organisé par la famille T des triplets non ordonnés de la forme :

$$(X, Y, (-x_1 - y_1, -x_2 - y_2, -x_3 - y_3 - \delta\,(X,Y)))\,,$$

est une $CCEGT$, et par ailleurs la loi définie par :

$$X \star Y = (x_1 + y_1, x_2 + y_2, x_3 + y_3 + \delta\,(X,Y))\,,$$

fait de $\mathbb{N}_3$ une BMC.

2.2.1 Théorèmes de la classification

Toute $CCEGT$ finie peut être décomposée en produit de $CCEGT$ d'ordre une puissance d'un premier, et seule la 3-composante peut éventuellement être non entropique. Dans le cas particulier des $CCEG$ issues des hypersurfaces cubiques, le sous-système $I\,(G)$ est une $CCGH$ et on a :

Théorème 2.13 *Soit (G,T) une $CCEGT$. Les trois conditions suivantes sont équivalentes :*

i) Tout tangentiel est un point d'inflexion c'est-à-dire $((xxz)) \in T$ entraîne $((zzz)) \in T$.

ii) (G,T) admet un point d'inflesion et la BMC associée est d'exposant 6.

iii) (G,T) est le produit direct d'un 2-groupe abélien élémentaire et d'une BMC d'exposant 3.

Preuve. Supposons que u soit un point d'inflexion, on a : $u^2 = u$ et si $x + y = u.xy$ alors $x \cdot y = -x - y$ donc $x^2 = -2x$.

• Si (i) est vérifiée on a : $x^2 \cdot x^2 = x^2$, on déduit que tout x^2 est point d'inflexion, est de plus :

$$\begin{aligned} 2x^2 &= x^2 + x^2 \\ &= u \cdot x^2 x^2 \\ &= u \cdot x^2 \\ &= u \cdot xx \\ &= x + x \\ &= 2x, \end{aligned}$$

alors

$$\begin{aligned} 2x = 2x^2 &= 2(-2x) \\ &= -4x, \end{aligned}$$

danc $6x = u$ et $(G, *)$ d'exenposant 6, ce qui prouve (ii).

• Si (ii) est vérifiée avec u point d'inlexion, l'application $P : x \longmapsto x^2 = -2x$ vérifie $-2(x + y) = -2x - 2y$, c'est un endomorphisme idempotent de $(G, +)$ puisque

$$\begin{aligned} P(P(x)) = (x^2)^2 &= 4x \\ &= -2x \\ &= x^2 \\ &= P(x). \end{aligned}$$

Pour $x \in G$, $x = a_x + d$ où $d = x^2 \in \mathrm{Im}(P)$ et $a_x = x - x^2 \in \ker(P)$, cette écriture est unique. Or une BMC où tout élément non nul a pour ordre une puissance de $p \neq 3$ est un p-groupe abélien.

Donc $(A = \ker(P), +)$ est un 2-groupe abélien. On a aussi pour tout $y = x^2$ de G^2, l'égalité $y^2 = y$ qui se traduit par $-2y = y$, soit $3y = u$. Donc $(G^2, \cdot)$ est une BMC d'exposant 3.

Pour $x = a_x + x^2$, et $y = b_y + y^2$ on a : a_x et $b_y \in \ker(P)$ donc $a_x \cdot b_y = \pm(a_x + b_y)$ et

$$\begin{aligned} x \cdot y &= -x - y \\ &= a_x \cdot b_y - x^2 - y^2 \\ &= a_x \cdot b_y + x^2 \cdot y^2. \end{aligned}$$

L'application :

$$f : (G, T) \longrightarrow (A, \cdot) \times \left(G^2, \cdot\right)$$

$$x \longmapsto \left(a_x, x^2\right)$$

est donc un isomorphisme, et (G, T) est isomorphe au produit direct d'un 2-groupe abélien $(A, \cdot)$ et d'une BMC d'exposant 3, à savoir $(G^2, \cdot)$.

$\cdot$ Si (iii) est vérifiée $x = a_x + d, a_x \in A$ et $d \in G^2$, alors

$$\begin{aligned} x^2 &= 2a_x + (x^2)^2 \\ &= 0_A + (x^2)^2 \\ &= (x^2)^2, \end{aligned}$$

donc tout tangentiel x^2 est un point d'inflexion si et seulement si $a_x = 0_A$. ■

Corollaire 2.2 *Toute $CCEGT$ où tout tangentiel est un point d'inflexion est décomposable d'une manière canonique en produit direct $A \times B$ d'une $CCGH$ A est isomorphe à $I(G)$ et d'une $CCEG$ binaire B.*

Remarque 2.3 (**sur l'ordre de** A et B) Avec les notations ci-dessus si de plus G est fini, alors $|A|$ (resp. $|B|$) est puissance de 3 (resp. 2).

Corollaire 2.3 *une $CCEGT$ où tout tangentiel est un point d'inflexion est non entropique si et seulement si A est non entropique.*

Par ailleurs, si tout point d'une $CCEGT$ est un point d'inflexion, alors la BMC associée $(G, *_u)$ à une telle $CCEGT$ est toujours d'exposant 3 puisque :

$$\begin{aligned} (x *_u x) *_u x &= u \cdot ((u \cdot xx) \cdot x) \\ &= u\,(ux \cdot x) \\ &= \text{u}u \\ &= u. \end{aligned}$$

Toute $CCEGT$ finie peut être décomposée en produit de $CCEGT$ d'ordre une puissance d'un premier, et seule la 3-composante peut éventuellement être non entropique.

Lemme 2.3 *[2]Tout BMC non associative est d'ordre divisible par* 81*, et il y a exactement deux BMC non isomorphes d'ordre* 81*, à savoir* $(\mathbb{L}_3, \star)$ *et* $(\mathbb{N}_3, \star)$*.*

Théorème 2.14 *Tout CCEGT finie non entropique est d'ordre divisible par* 81*, et il y a exactement trois CCEGT non entropiques et non isomorphes d'ordre* 81*, à savoir :* $(\mathbb{L}_3, T_\alpha), (\mathbb{L}_3, T_e), (\mathbb{N}_3, T)$*.*

Preuve. Soit (E, T) une $CCEGT$ finie non entropique. La BMC associée $(E, +)$ est non associative, et donc son ordre est multiple de 81. Si $|E| = 81$, alors $(E, +)$ est isomorphe soit à $(\mathbb{L}_3, \star)$, soit à $(\mathbb{N}_3, \star)$. Or, si $(E, +) \cong (\mathbb{N}_3, \star)$, alors nécessairement $(E, T) \cong (\mathbb{N}_3, T)$, d'après la proposition 2.2, car on vérifie que le centre de $(\mathbb{N}_3, \star)$ se réduit à $\theta(\mathbb{N}_3, \star)$. Par contre si $(E, +) \cong (\mathbb{L}_3, \star)$, alors la loi de la $CCEGT$ (E, T_c) peut s'écrire : $x \cdot y = x \circ_c y = c - x - y$, le dernier membre étant dans $(\mathbb{L}_3, \star)$ avec $c \in Z(\mathbb{L}_3, *) = \{-\alpha, e, \alpha\}$. Or les éventualités : $c = -\alpha$ et $c = \alpha$ donnent des $CCEGT$ isomorphes par l'involution $x \longmapsto -x$. Par centre lorsque $c = e$, tout élément de la $CCEGT$ correspondant $(\mathbb{L}_3, T_e)$ est point d'inflexion, tandis que $c = \alpha$ donne une $CCEGT$ sans point d'inflexion ($\alpha \notin \theta(L_3, \star) = \{e\}$). Comme les BMC $(\mathbb{L}_3, \star)$ et $(\mathbb{N}_3, \star)$ sont non isomorphes, aucune des deux $CCEGT$ correspondant à $(\mathbb{L}_3, \star)$ ne peut être isomorphes, à $(\mathbb{N}_3, \star)$, seule la $CCEGT$ associée à $(\mathbb{N}_3, \star)$. Ceci termine la preuve. ■

Théorème 2.15 *[2](**de l'ordre minimum**) Toute CCEGT non entropique est d'ordre multiple de* 81*. Il y a exactement* 15 *CCEGT non isomorphes d'ordre* 81*, dont* 12 *sont entropiques, et* 3 *sont terentropiques et non entropiques. Si* $(\mathbb{L}_3, \star)$ *et* $(\mathbb{N}_3, \star)$ *sont les BMC non associatives d'ordre* 81*, d'exposants* 3 *et* 9 *respectivement et de neutres u et v, avec c élément central de* $(\mathbb{L}_3, \star)$ *distinct de u, alors la correspondance entre CCEGT d'une part et leurs groupes ou boucles associés d'autre part, est comme suit :*

Groupes et BMC d'ordre 81	*CCEG* (G, T_c) *associées : nombre et description*
$(\mathbb{Z}_3^4, +)$	$2 : \left(\mathbb{Z}_3^4, T_{(0,0,0,0)}\right)$ *et* $\left(\mathbb{Z}_3^4 \times T_{(1,1,1,1)}\right)$
$(\mathbb{Z}_3^2 \times \mathbb{Z}_9, +)$	$3 : \left(\mathbb{Z}_3^2 \times \mathbb{Z}_9, T_{(0,0,0)}\right), \left(\mathbb{Z}_3^2 \times \mathbb{Z}_9, T_{(1,1,0)}\right)$ *et* $\left(\mathbb{Z}_3^2 \times \mathbb{Z}_9, T_{(0,0,1)}\right)$
$(\mathbb{Z}_9^2, +)$	$2 : \left(\mathbb{Z}_9^2, T_{(0,0)}\right)$ *et* $\left(\mathbb{Z}_9^2, T_{(1,1)}\right)$
$(\mathbb{Z}_3 \times \mathbb{Z}_{27}, +)$	$3 : \left(\mathbb{Z}_3 \times \mathbb{Z}_{27}, T_{(0,0)}\right), \left(\mathbb{Z}_3 \times \mathbb{Z}_{27}, T_{(1,0)}\right)$ *et* $\left(\mathbb{Z}_3 \times \mathbb{Z}_{27}, T_{(0,1)}\right)$
$(\mathbb{Z}_{81}, +)$	$2 : (\mathbb{Z}_{81}, T_0)$ *et* $(\mathbb{Z}_{81}, T_1)$
$(\mathbb{L}_3, \star)$	$2 : (\mathbb{L}_3, T_u)$ *et* $(\mathbb{L}_3, T_c)$
$(\mathbb{N}_3, \star)$	$1 : (\mathbb{N}_3, T_v)$

2.3 Cubiques Généralisées de Hall et formes trilinéaires alternées

Soit (E, T) une courbe cubique généralisée de Hall de 3-ordre 3^{n+1} et de rang $n+1$ engendrée par $e_0, e_1, ..., e_n$. Notons $(E, +)$ la BMC associée de neutre e_0, où l'associateur est la forme trilinéaire ω.

2.3.1 Construction de CCGH et des BMC d'exposant 3 et de classe 2

Soient $V = V(n, \mathbb{F}_3)$,de base e_i, $i = 1, 2, ..., n$, et R un sous-espace vectoriel arbitraire de codimension 1 dans $\Lambda^3 V$. Le quotient $W = \Lambda^3 V / R$ a pour système générateur l'ensemble des $\binom{n}{3}$ classes modulo R des trivecteurs $e_i e_j e_k$, pour $i < j < k$, notés $\overline{e_{ijk}}$

Tout vecteur x de $E = V \oplus W$ s'écrit

$$x = \sum_{i=1,2,..,n} x_i e_i + \sum_{1 \leq i < j < k \leq n} x_{ijk} \overline{e_{ijk}} \text{ où } x_i, x_{ijk} \in \mathbf{F}_3.$$

on définit dans E de manière intrinsèque une loi de BMC d'exposant 3 de forme :

$$x * y = x + y + \sum_{1 \leq i < j < k \leq n} (x_i y_i - y_i x_i)(x_k - y_k) \overline{e_{ijk}},$$

$(E, *)$ est de classe 2. Les triplets définis par $x * y * z = 0$ munissent E d'une structure de $CCEH$ de ciasse 2, l'associateur factorisé est :

$$\omega(\overline{x}, \overline{y}, \overline{z}) = \sum_{1 \leq i < j < k \leq n} e^*_{ijk}(x, y, z)\, \overline{e_{\widehat{ijk}}}.$$

Théorème 2.16 *[2]* ***(de correspondance)*** *Pour $n \geq 3$ on a correspondance biunivoque entre :*

1. d'une part les classes des formes trilinéaires alternées $AlT(n, \mathbb{F}_3)$ et
2. d'autre part les classes d'isomorphie des $CCGH$ (resp. des BMC d'exposant 3) de rang $n+1$ (resp. n), et de 3-ordre $n+1$, et de classe 2.

Théorème 2.17 *[2]*(***du nombre de classes d'isomorphie***). *Pour $n \geq 3$, le nombre maximum des classes $AlT(n, 1, \mathbb{F}_3)$ non équivalentes coïncide avec le nombre maximun de $CCGH$ de rang $n+1$, de 3-ordre $n+1$ et de classe 2 qui sont non isomorphes deux à deux. Parmi ces $CCGH$, celles qui sont de rang maximal forment.*

Théorème 2.18 *[2]*(***Classifications et descriptions implicites***) *Il y a exactement 11 classes d'isomorphie de $CCGH$ de rang 8 (resp. de BMC déexposant 3 de rang 7) et d'ordre 3^8, dont 6 sont centralement irréductibles et d'associateurs factorisés : f_5, f_6, f_7, f_8, f_9.*

f_i	$\Phi_{f_i}(x,y)$
$f_1 = e_{123}$	$(x_2y_3 - x_3y_2)(x_1 - y_1)$
$f_2 = e_{123} + e_{145}$	$(x_2y_3 - x_3y_2 + x_4y_5 - x_5y_4)(x_1 - y_1)$
$f_3 = e_{123} + e_{145}$	$(x_2y_3 - x_3y_2 + x_4y_5 - x_5y_4)(x_1 - y_1)$
$f_4 = e_{162} + e_{243} + e_{135}$	$(x_6y_2 - x_2y_6 + x_3y_5 - x_5y_3)(x_1 - y_1)$ $+ (x_4y_3 - x_3y_4)(x_2 - y_2)$
$f_5 = e_{123} + e_{456} + e_{147}$	$(x_2y_3 - x_3y_2 + x_4y_7 - x_7y_4)(x_1 - y_1)$ $+ (x_5y_6 - x_6y_5)(x_4 - y_4)$
$f_6 = e_{152} + e_{147} + e_{163} + e_{243}$	$(x_5y_2 - x_2y_5 + x_4y_7 - x_7y_4 + x_6y_3 - x_3y_6)(x_1 - y_1)$ $+ (x_4y_3 - x_3y_4)(x_2 - y_2)$
$f_7 = e_{146} + e_{157} + e_{245} + e_{367}$	$(x_4y_6 - x_6y_4 + x_5y_7 - x_7y_5)(x_1 - y_1)$ $+ (x_4y_5 - x_5y_4)(x_2 - y_2) + (x_6y_7 - x_7y_6)(x_3 - y_3)$
$f_8 = e_{123} + e_{145} + e_{167}$	$(x_2y_3 - x_3y_2 + x_4y_5 - x_5y_4 + x_6y_7 - x_7y_6)(x_1 - y_1)$
$f_9 = e_{123} + e_{456} + e_{147} + e_{257} + e_{367}$	$(x_2y_3 - x_3y_2 + x_4y_7 - x_7y_4)(x_1 - y_1)$
	$+ (x_5y_7 - x_7y_5)(x_2 - y_2) + (x_6y_7 - x_7y_6)(x_3 - y_3)$ $+ (x_5y_6 - x_6y_5)(x_4 - y_4)$

Preuve. cette classification résulte du théorème 2.16. ■

Exemple 2.3 $CCGH$ d'associateur factorisé f_9 :

soit $V = V(7, F_3)$ et R l'hyperplan de $\Lambda^3 V$ engendré par : $e_{123} - e_{456}, e_{123} - e_{147}, e_{123} - e_{257}, e_{123} - e_{367}$ et tous les e_{ijk} pour $i < j < k$ et pour (i,j,k) diffférents de : $(1,2,3), (4,5,6), (1,4,7), (2,5,7), (3,6,7)$.

Le quotient $E(f_9) = V \oplus (\Lambda^3 V/R)$ est engendré par $e_i, i = 1,...,7$ et le composé au sens de la boucle est

$$x * y = x + y + \Phi(x,y).u$$

avec

$\Phi_{f_9}(x,y) = (x_2y_3 - x_3y_2 + x_4y_7 - x_7y_4)(x_1 - y_1) + (x_5y_7 - x_7y_5)(x_2 - y_2)$
$+ (x_6y_7 - x_7y_6)(x_3 - y_3) + (x_5y_6 - x_6y_5)(x_4 - y_4)$.

De même, pour $\Phi_{f_i}(x, y\ ), i = 1, 2, ...8$.

Conclusion

L'étude présenté dans ce mémoire s'articule essentiellement sur la classification des trivecteurs de rang ≤ 7.

Cette classification est interprétable pour décrire certaines classifications des courbes cubiques elliptiques généralisées. Notons que l'application des courbes elliptiques à la cryptographie est relativement récente, d'où l'importance de cette classification en cryptographie. Notons aussi que cette classification aide à résoudre certains problèmes en théorie des codes.

Bibliographie

[1] **A.Cohen et A.Helminck**, Trilinear alternating forms on a vector space of dimension 7, Communications in Algebra 16(1), 1988, p.1-25.

[2] **Abou Hashih, M., Bénéteau, L.** (2004) Analternative way to classify some Generalized elliptic

[3] **B.Kahn**, Sommes de tenseurs décomposables, Prépublication de l'université Paris VII, Mai 1991, 28p.

[4] **D.Djokovic's**, Classification of trivectors of an eight dimensional real vector space, Linear and multilinear Algebra, 13(3), 1983, p.3-39.

[5] **E.M. Rains, J.A. Sloane**, Self-dual codes, Handbook of Coding Theory, pless V.S. Huffman W.C (editors), Elsevier, Amsterdam, 1998, p.177-294.

[6] **G.B.Gurevitch**, Theory of algebraic invariants. P.Noordhof LTD, Groningen, the Netherland, 1964

[7] **L.Noui et Ph.Revoy**, Formes multilinéaires alternées, Ann.Math.Blaise Pascal Vol 1, n°2, 1994, p.43-69

[8] **L.Noui**, Classification des trivecteurs par l'action du groupe linéaire, Thèse de Doctorat, Université de Montpellier II, France, 1995.

[9] **N.Bourbaki**, Algèbre, chapitres 1 à 3, Hermann, Paris.

[10] **Ph.Revoy**, Formes trilinéaires alternées de Rang 7, Bul.Sc. Math.112,1988, p.357-368.

[11] **Ph.Revoy**, Trivecteurs de rang 6, in coll. Sur les formes quadratiques, Bulletin SMF, 59, 1979, p.141-155.

[12] **Rakdi .M.A. et Midoune N.** Weights of the Fq-forms of 2-step splitting trivectors of rank 8 over a finite field, Carpathian Mathematical Publications,Vol. 11 No. 2 (2019).

[13] **S.Lang**, Algebra, second edition, Addisson-Wesley publishing company Inc, California 1984.

[14] **V.L.Popov, E.B.Vinberg**, Invariant theory, Algebraic Geometry IV, Encyclopaedia of Mathematical Sciences, Volume 55, Springer-Verlag.

Résume

L'étude présenté dans ce mémoire s'articule essentiellement sur la classification des trivecteurs (ou formes trilinéaires alternées).

Cette classification est interprétabl pour décrire certains classification des CCEG (courbes cubiques elliptiques)

Abstract

The study presented in this memoir is essentially about the classification of trivectors (or alterate trilinear forms).

This classification can be interpeted to describe certain classification of CCEG (generalized elliptical cubic curves).

ملخص

تعتمد الدراسة المقدمة في هذه الأطروحة أساسًا على تصنيف الأشعة لثلاثية (أو الأشكال ثلاثية المتناوبة).

يمكن تفسير التصنيف لوصف تصنيف معين لمنحنيات مكعبة بيضاوية معممة.