Remerciements

Je remercie tout d'abord mon Dieu qui m'a donné la force pour terminer ce modeste travail. Je tiens à remercier mon promoteur: Mr.N. MIDOUNE pour la confiance qu'il m'a témoignée en me proposant ce sujet, ses encouragements et sa patience. Les discussions scientifiques qu'il a su générer, ses remarques et ses suggestions qui m'ont permis de finaliser ce modeste travail. Je souhaite lui transmettre ma reconnaissance et ma plus profonde gratitude.

Je remercie aussi tous les membres du Jury pour l'honneur qu'ils m'ont fait, en acceptant de juger ce travail.

Je ne peux pas clôturer mes remerciements sans se retourner vers les êtres qui me sont les plus chers; ma famille qui ont eu un rôle essentiel et continu dans ma réussite.

Merci

Table des matières

Introduction

Les courbes cubiques elliptiques généralisées (CCEG) forment une classe de structure combinatoires introduites récemment par F.Buekenhout [Bue01].
On se donne une famille de triplets de points $((x, y, z))$ qui généralise la situation géométrique des courbes elliptiques ; pour tout couple de points x, y, on a un seul troisiéme point aligné

$$z = x \cdot y$$

chaque point étant éventuellement répété (deux fois pour les points de tangence, et trois fois pour les points d'inflexion).
A tout choix d'une origine u, on sait alors associer une loi réguliére $x *_u y = u \cdot (x \cdot y)$ de neutre u. Mais est-ce une loi de groupe abélien comme dans les courbes elliptiques ?. Pas toujours, à moins qu'on ait l'entropie (au sens que : $(x \cdot y) \cdot (z \cdot t) = (x \cdot z) \cdot (y \cdot t)$ identiquement)

Nous étendrons certains théorémes de structure des CCEG entropiques à la catégorie plus générale des CCEG térentropiques.
Elles sont en correspondance avec les boucles de Moufang coummutatives. Dans cette catégorie, nous avons des théorémes des classification sur deux situations extrêmales :

1. celles où tout point est d'inflextion : les Courbes Cubiques Généralisées de Hall (CCGH)

2. et celles qui sont de classe 2, c'est-à-dire celles où l'associateur vérifie l'identité suivante: $(x \cdot x', y, z) = (x, y, z) \cdot (x', y, z)$

Chapitre 1

Courbes cubiques elliptiques généralisées

Soit G un ensemble. Un triplet non ordonné de G, noté $((x, y, z))$ ou $((xyz))$, est la classe d'équivalence du triplet (x, y, z) incluant tous les triplets (x', y', z') obtenus par permutation x', y', z' des points x, y, z.

Définition 1.0.1 *[Bue01]*

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.

Définition 1.0.2

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 $a \cdot x = b$ (resp $y \cdot a = b$) admette une solution unique dans G. Si de plus la loi admet un neutre bilatére e, on dit qu'on a une boucle.

Soit (G, T) une CCEG**.** On définit une loi sur G, dite "loi milieu" $x, y \longrightarrow x \cdot y = z$, 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 $*_u$, qui à x, y de G fait correspondre $x *_u y = u \cdot (x \cdot y)$. On déduit de la définition de la loi milieu que

$$x \cdot y = y \cdot x \text{ et } u \cdot (x \cdot u) = x$$

Par suite G organisé par la loi binaire qui à x, y fait correspondre $(x *_u y)$ est une boucle commutative de neutre u, dite "boucle associée d'origine u ".

Remarque 1.0.1

- *Toute loi milieu d'une CCEG vérifie la totale symétrie, au sens que toute égalité de forme $x \cdot y = z$ demeure vraie sous permutation arbitraire des trois lettres x, y, z.*
- *Une loi totalement symétrique est une loi de quasigroupe.*
- *Tout quasigroupe totalement symétrique provient d'une CCEG unique.*

Définition 1.0.3

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'inflextion" 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 systéme générateur des sous-ensembles de G de cardinal r.

Exemple 1.0.1

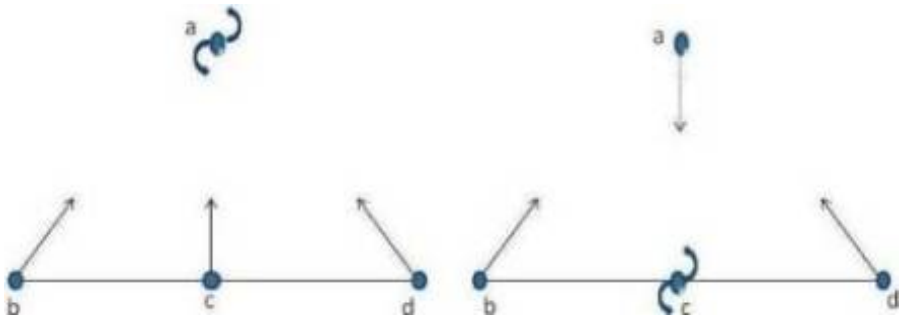
Sur un ensemble $G = \{a, b, c, d\}$ de cardinal 4, il y a essentiellement deux structures de CCEG, on peut les représenter par les familles de triplets non ordonnés

$$T = \{((bcd)),\ ((bba)),\ ((cca)),\ ((dda)),\ ((aaa))\} \text{ et}$$

$$U = \{((bcd)),\ ((bba)),\ ((ccc)),\ ((dda)),\ ((aac))\}.$$

Leurs rangs sont 2 et 1 respectivement. Chaque CCEG on la représente dans une figure où on utilise les conventions standard : chaque point est représenté par un cercle, le triplet par une droite, le point d'inflexion par le symbole S et la fléche d'origine un point b joint le tangentiel de b :

(G,T) (G,U)



FIG, (01)

Définition 1.0.4

Les CCEG entropiques sont celles où

$$(x \cdot y) \cdot (z \cdot t) = (x \cdot z) \cdot (y \cdot t) \quad identiquement$$

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

1.1 Théorémes de structure des CCEG

L'énoncé qui suit met en évidence le fait que, en quelque sorte, les CCEG entropiques sont aux groupes abéliens ce que les espaces affines sont aux espaces vectoriels. Il formalise à un niveau de généralité naturel une propriété bien connue dans le cas des CCEG issues de courbes cubiques.

Proposition 1.1.1

1. *Soit* $(Q,\ T)$ *une CCEG entropique et* u *un élément arbitraire de* Q*, alors* $(Q,\ *_u)$ *est un groupe abélien.*

2. *Pour tout couple* $u,\ v$ *d'éléments de la CCEG entropique* $(Q,\ T)$*, les deux groupes* $(Q,\ *_u)$ *et* $(Q,\ *_v)$ *sont isomorphes.*

Preuve.

1. La loi $x,\ y \longrightarrow x *_u y = u \cdot xy$ est cmmutative; elle admet u comme neutre.
   En outre $x' = u^2 x$ est l'inverse de x car :

$$x *_u u^2 x = u \cdot \left(x \cdot u^2 x\right) = u \cdot u^2 = u$$

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

$$(u \cdot xy) \cdot z = x \cdot (u \cdot yz) \text{ .....} \mathbf{(1.1.1)}$$

   On multiplie les deux membres de (1.1.1) par u on obtient $(x *_u y) *_u z = x *_u (y *_u z)$, ainsi $(Q,\ *_u)$ est un groupe abélien.

2. Posons

$$f(x) = x *_u v = u \cdot xv, \text{ on a alors :}$$

$$f(x) *_v f(y) = v((u \cdot vx)(u \cdot vy)) = v\left(u^2 \cdot \left(v^2.xy\right)\right)$$

$$= vu^2 \cdot (x \cdot y) = u \cdot (v \cdot (u \cdot xy)) = f(x *_u y)$$

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

Théorème 1.1.1

Si $(A, +)$ est un groupe 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 abélien unique à un isomorphisme prés (et isomorphe à $(G, *_u)$ pour tout u de G).

Preuve.

Pour chaque x et $y \in A$, il existe un seul z vérifiant :

$$z = x \circ_c y = c - x - y \in A \text{ et } ((xyz)) \in T$$

$$\text{Puisque } x \circ_c y = y \circ_c x \text{ et } x \circ_c (y \circ_c x) = y$$

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, T) 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 ..**(1.1.1)**.. alors on réobtient

$$x \cdot y = x \circ_c y \text{ en choisissant } c = u^2 = u \cdot u$$

Donc toute CCEG entropique (A, T) s'obtient ainsi à partir d'un groupe abélien unique à un isomorphisme prés (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 1.1.1

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

Exemple 1.1.1

Soit $\mathbb{Z}_n$ l'ensemble des restes modulo n où n est un entier $\succ 0$. Les familles de triplets non ordonnés

$$T_1 = \{((x, y, 1 - x - y))\} \text{ et } T_0 = \{((x, y, -x - y))\}$$

définissent deux structures de CCEG entropiques non isomorphes si n est multiple de 3 ($n = 3k$), (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 1.1.1

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

$$\begin{array}{rccc} f_i : & (Q, \cdot) & \longrightarrow & (R, \circ) \\ & a & \longrightarrow & f(a) = a^\alpha \end{array}$$

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

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

Théorème 1.1.2 ***(Bruck)***

Si deux groupes sont isotopes, alors ils sont aussi isomorphes.

Preuve. [Bru58]

On peut voir facilement que la CCEG entropique (Q,T) et le groupe $(Q,\star_u)$ dans la proposition ..**(1.1.1)**..sont isotopes. Donc d'aprés le théoréme **(1.1.2)** chaque CCEG entropique est isotope à un groupe abélien, qui est unique à un isomorphisme prés. 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 [Schw95] 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 1.1.1

On a l'isomorphisme 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 ou chacune s'obtient à partir d'un groupe cyclique.

Théorème 1.1.3

Soint G un groupe cyclique isomorphe à $\mathbb{Z}_m$ on a les isomorphismes suivants :

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* $(G,T_0)\cong(G,T_1)$. *(i e* $|G|=3k-1$ *ou* $|G|=3k-2$*)*

Preuve.

L'application $\alpha : (G, T_e) \longrightarrow (G, T_{e+3})$

définie par $\alpha(a) = a + 1$ est un homorphisme puisque pour tous $x, u \in G$ on a :

$$\alpha(x \cdot y) = \alpha(e - x - y) = e - x - y + 1, \text{ et } \alpha(x) \cdot \alpha(y) = e + 3 - \alpha(x) - \alpha(y)$$

$$= e + 3 - (x + 1) - (y + 1) = e - x - y + 1$$

La preuve que α est bijective est évidente.

On considére 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 :

$$\beta(x \cdot y) = \beta(1 - x - y) = x + y, \text{ et } \beta(x) \cdot \beta(y) = (-x + 1) \cdot (-y + 1)$$

$$= 2 - (-x + 1) - (-y + 1) = x + y$$

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

1. Soit $3k - 1$ avec k un entier, dans ce cas on utilise l'application bijective

   $$\gamma_1 : a \longrightarrow a + k$$

   on vérifie aisément que γ_1 est un homorphisme.

2. Soit $3k - 2$ en utilisant

   $$\gamma_2 : a \longrightarrow a + (2k - 1)$$

   on trouve la démonstration de **(3)**.

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

Théorème 1.1.4

Soit $(A, +)$ un groupe abélien d'ordre non divisible par 3.

Il existe à un isomorphisme prés une seule CCEG entropique isotope à $(A, +)$.

Définition 1.1.2

Etant donné une CCEG (Q,T) de loi milieu $x\cdot y$, étant donné un élément a de Q, notons : $a^{(1)}=a$, $a^{(2)}=a\cdot a$, ..., $a^{(i+1)}=a^{(i)}\cdot a$.

Si $a^{(n-1)}=a\neq a^{(i)}$ pour chaque i tel que $1\preceq i\prec n-1$, on dit que la suite $\left(a,a^{(2)},a^{(3)},...,a^{(n-1)}\right)$ et un cercle de longueur n et n est l'ordre multiplicatif de a.

Définition 1.1.3

Etant donné une CCEG entropique (Q,T_e), on définit le graphe orienté simple associé en posant :

1. *que son ensemble de sommets est l'ensemble Q des points de la CCEG.*
2. *que ses arcs sont les couples de forme $(a,a\circ a)$, avec $a\circ a=e-2a$.*

L'ordre multiplicatif de (-2) modulo 3^r c'est-à-dire de (-2) dans le groupe multiplicatif $\mathbb{Z}_{3^r}^*$ des éléments inversibles de l'anneau $\mathbb{Z}_{3^r}$, joue un rôle important dans la détermination des CCEG entropiques non isomorphes deux à deux bien qu'isotopes à un méme groupe abélien $(\mathbb{Z}_{3^r},+)$.

Lemme 1.1.2

L'ordre multiplicatif de (-2) dans le groupe cyclique $(\mathbb{Z}_{3^r}^*,\cdot)$ est 3^{r-1}.

Théorème 1.1.5

Dans le graphe orienté simple associé à $(\mathbb{Z}_{3^r},T_0)$ chaque élément de la forme $y=3^sx$ avec $p\gcd(x,3)=1$ se trouve dans un cercle de longueur 3^{r-s-1} .

Preuve.

Considérons la suite :

$$y_0=y,\ y_1=y\circ y=-2y,\ ...,\ y_{n+1}=y_n\circ y_n=(-2)^{n+1}y,\ \ (n\in\mathbb{N})$$

On a $y_m = (-2)^m y = y \bmod 3^r$ si et seulement si $(-2)^m = 1 \bmod 3^{r-s}$.

Supposons $(-2)^m \equiv 1 \bmod 3^{r-s}$ alors :

$$y_m = \left(3^{r-s}z + 1\right) 3^s x \text{ avec } z \text{ un entier}$$

$$y_m = 3^r zx + 3^r x \equiv y \bmod 3^r$$

Si $y_m \equiv y \bmod 3^r$, on a $y_m = (-2)^m y = y + z3^r = 3^s x + z3^r = 3^s x\left(1 + 3^{r-s}z'\right)$

donc on a $(-2)^m = 1 - 3^{r-s}z' \equiv 1 \bmod 3^{r-s} \Longrightarrow (-2)^m = 1 \bmod 3^{r-s}$

donc la longueur m du cercle est égale à l'ordre multiplicatif de $-2 \bmod 3^{r-s}$ qui est 3^{r-s-1}.

Lemme 1.1.3

Le graphe orienté simple associé à $(\mathbb{Z}_{3^r}, T_1)$ se réduit à un seul cercle de longueur 3^r.

Preuve.

Dans la CCEG entropique $(\mathbb{Z}_m, T_e)$ on montre par récurrence :

$\overbrace{\left(\left(\left(a^2\right)^2\right)^2 ...\right)^2}^{n} = a^{2^n} = e \cdot \sum_{k=0}^{n-1} (-2)\, k + a\,(-2)^n \bmod m$, de plus on a :

$$3\sum_{k=0}^{n-1} (-2)^k = 1 - (-2)^n .$$

Donc dans la CCEG entropique $(\mathbb{Z}_{3^r}, T_1)$:

$$a^{2^n} = a \bmod 3^r \Longleftrightarrow 3^{-1}\left(1 - (-2)^n\right) + a\,(-2)^n = a + \beta 3^r$$

$$\Longleftrightarrow (1 - (-2)^n) + 3a\,(-2)^n = 3a + \beta 3^{r+1}$$

$$\Longleftrightarrow (3a - 1)\left((-2)^n - 1\right) = \beta 3^{r+1}$$

$$\Longleftrightarrow 0 = (3a - 1)\left(1 - (-2)^n\right) \bmod 3^{r+1}$$

Mais $pgcd\,(3a-1,3)=1$ donc $1-(-2)^n=0 \bmod 3^{r+1}$, par conséquent la longueur n de a est égale à 3^r.

Donc le graphe orienté simple associé à $(\mathbb{Z}_{3^r},T_1)$ contient un seul cercle de longueur 3^r.

Lemme 1.1.4

Soint (G,T) et (H,T') deux CCEG entropiques, $e\in G$ et $f\in H$ se trouvent dans des cercles de longueurs m et n respectivement, alors (e,f) se trouve dans un cercle de longueur $ppcm\,(m,n)$.

Preuve.

Si $e^{2^m}=e$ et $f^{2^n}=f$, alors le plus petit entier k tel que

$$\left(e^{2^k},f^{2^k}\right)=(e,f)\ \text{ est } ppcm(m,n).$$

Donc on a la liste suivante, en supposant que $G\cong Z_{3^r}$ et $H\cong Z_{3^s}$ et $r\leq s$:

CCEG entropique	le graphe orienté simple associé
(G,T_0)	cercles de longueur $1,3...,3^{r-1}$
(G,T_1)	cercle de longueur 3^r
(H,T_0)	cercles de longueur $1,3,...,3^{s-1}$
(H,T_1)	cercle de longueur 3^s
$\left(G\times H,T_{(0,0)}\right)$	cercles de longueur $1,3,...,3^{s-1}$
$\left(G\times H,T_{(0,1)}\right)$	cercle de longueur 3^s
$\left(G\times H,T_{(1,0)}\right)$	cercles de longueur $1,3,...,3^{s-1}$
$\left(G\times H,T_{(1,1)}\right)$	cercle de longueur 3^s

Lemme 1.1.5

Soit $G\cong\mathbb{Z}_{3^r}$ et $H\cong\mathbb{Z}_{3^s}$ 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 $y \equiv x \bmod n$ pour $y \equiv x \bmod n$ et $0 \preceq y \prec n$.

Considérons l'application :

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

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

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

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

Limage du milieu de deux points est :

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

Et on a :

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

Donc α est un isomorphisme.

Théorème 1.1.6 ***(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 $\left(\mathbb{Z}_{3^{r_1}}\right)^{l_1} \times \left(\mathbb{Z}_{3^{r_2}}\right)^{l_2} \times ... \times \left(\mathbb{Z}_{3^{r_k}}\right)^{l_k}$ avec

$$l_1 r_1 + l_2 r_2 + ... + l_k r_k = n \text{ et } r_1 \prec ... \prec r_k$$

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

Preuve.

Par le lemme précédent si on choisit $c_{r_j} = 1$ pour la composante $\mathbb{Z}_{3^{r_j}}$ et on met 1 ou 0 dans les autres composantes $\mathbb{Z}_{3^{r_i}}$ pour $r_i \leq r_j$ on va avoir la méme classe d'isomorphisme. Donc pour avoir tous les CECG entropiques non isomorphes deux à deux isotopes à $(A, +)$, on choisit $j \in \{1, ..., k\}$ et on met 1 dans le cyclique composant $\mathbb{Z}_{3^{r_j}}$ et 0 pour les autres composantes et enfin on ajoute la classe d'isomorphisme $\left(A, T_{\left(0^{l_1}, 0^{l_2}, ..., 0^{j_k}\right)}\right)$.

Théorème 1.1.7

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 théoréme (2.15), 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 trés exactement $k+2$ CECG non isomorphes associées à $(G, +)$.

Théorème 1.1.8 ***(classification de Buekenhout)***

Il y a à un isomorphisme prés 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 $p \succ 0$ 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 vecteriel 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 $|G| = 4$ (resp 8), on obtient l'exemple (P, T) de **(1.3)** (resp.l'unique CCEG entropique d'ordre ≤ 8 qui ne provient d'aucune courbe elliptique).*

Théorème 1.1.9

Soit (G,T) une CCEG de loi milieu $x \cdot y$; posons $x^2 = x^{(2)} = x \cdot x$.

Les 3 conditios suivantes sont équivalentes :

1. $x^2 \cdot yz = xy \cdot xz$
2. $x^2 z \cdot y = (xy \cdot z)\, x$
3. $x \cdot yz = x^2 z \cdot xy$

Preuve.

En multipliant les deux membres de (1) par z^2 :

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

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

par symétrie

$$z \cdot yz = y \text{ et } z \cdot xz = x$$

ainsi l'galité (2) est vérifiée.

On passe de (2) à (3) en faisant $xy = Y$ on obtient

$$x^2 z \cdot xY = Yz \cdot x$$

qui est équivalente à (3). En multipliant les deux membres de (3) par xy

on obtient

$$xy \cdot (x \cdot yz) = x^2 y$$

et en faisant $yz = Z$; on trouve (1).

Remarque 1.1.2

Chacune des identités $(1), (2)$ *et* (3) *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 1.1.10

Soit (G,T) une CCEG terentropique de loi miliex $x \cdot y$.

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

2. Les triplets $((xyz))$ de T sont caractérisés par l'égalité

$$x \star_u y \star_u z = u^2$$

Preuve.

La loi $x, y \longrightarrow x \star_u y = u \cdot xy$ 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 avons:

$$(x \star_u y) \star_u x'$$

$$= u\left((u \cdot xy) \cdot u^2 x\right)$$

$$= u\left(u \cdot (xy \cdot x)\right) = y$$

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

$$(a \star_u a) \star_u (x \star_u y) = u \cdot [ua^2 \cdot (u \cdot xy)]$$

$$= u \cdot \{u^2 \cdot \left(a^2 \cdot xy\right)\}$$

$$= u \cdot [u^2 (ax \cdot ay)] = u \cdot \{u \cdot ax \cdot (u \cdot ay)\}$$

$$= (a \star_u x) \star_u (a \star_u y)$$

Ainsi $(G, \star_u)$ est une boucle de Moufang commutative; son centre associatif $Z(G, \star_u)$ est l'ensemble des éléments 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

$$xy \cdot u = u^2 y \cdot ux$$

ainsi $u^2 \in Z(G, \star_u)$.

Nous avons 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 :

$$u^2 - (x \star_u y) = u \cdot \left(u^2 \left(u^2 (u \cdot xy)\right)\right) = xy$$

$$\text{Donc} \qquad x \star_u y \star_u z = u^2$$

Théorème 1.1.11

Pour tout couple u, v d'éléments de la CCEG terentropique (G, T), les deux boucles de Moufang $(E, \star_u)$ et $(E, \star_v)$ sont isomorphes par

$$x \longrightarrow x \star_u v = u \cdot (vx)$$

Preuve.

Posons $f(x) = x \star_u v$. On a $f(x \star_u y) = (x \star_u y) \star_u v = u \cdot (v \cdot (u \cdot xy)) = u^2 v \cdot xy$.

Par ailleurs $f(x) \star_v f(y) = (x \star_u v) \star_v (y \star_u v) = v \cdot ((u \cdot xv) \cdot (uyv)) = v \cdot (u^2 \cdot (xv \cdot yv)) = v \cdot (u^2 \cdot (v^2 \cdot xy)) = A$ car (G, T) est terentropique; en outre il résulte que

$$A = vu^2 \cdot xy$$

Nous avons 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 avons 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 1.1.12

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 ordonnés de la forme : $((x, y, c - x - y))$ est une CCEGT. Toute CCEGT s'obtient ainsi.

2. La boucle de Moufang de neutre e associée à (G, T_c) n'est autre que $(G, +)$.

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

$$x \cdot (x \cdot y) = c - x - (c - x - y) = y$$

Par ailleurs

$$a \cdot a + x \cdot y = 2c - 2a - x - y = a \cdot x + a \cdot y$$

$$\text{donc } (a \cdot a) \cdot (x \cdot y) = (a \cdot x) \cdot (a \cdot y)$$

Ainsi $(E, \cdot) = (E, \circ_c)$ est bien une CCEGT. Toute CCEGT peut être reconstruite par ce procédé : il suffit de prendre $c = u^2$ dans $(G, \star_u)$.
En outre, si on fait $u = e$, alors $u^2 = u \cdot u = c - 2e = c$

$$\text{et } x \star_e y = e \circ_c (x \circ_c y) = e \circ_c (c - x - y) = c - e - (c - x - y) = x + y$$

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

Exemple 1.1.2

Soit $(G,+)$ un 3-groupe abélien élémentaire.

Les triplets non ordonnés $((xyz))$ caractérisés par

$$x+y+z=0$$

font de G une CCEG de Hall. Toute CCEG de Hall s'obtient 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 1.1.13

Les CCEGT possédant au 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 éléments de la forme

$$3x=x+x+x$$

constitue 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:

$$x\cdot y=u^2-_{\star_u}(x\star_u y)=u-_{\star}(x\star_u y)=-(x\star_u y).$$

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

Proposition 1.1.2

Si $(E,+)$ est une une BMC de neutre e, alors les CCEGT (E,T_c) obtient en prenant c dans $\theta(E,+)$ forment une classe compléte d'isomorphie dont le représentant le plus simple est évidemment (E,T_e).
Les CCEGT répondant à cette description sont trés exactement celles qui possédent un point d'inflexion.

Corollaire 1.1.1

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

Remarque 1.1.3

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 $(E,+)$.

Chapitre 2

Quelques exemples de CCEGT et de BMC non entropiques

1. Soient $\mathcal{F}_3 = \mathbb{Z}_3$ le corps à trois éléments et $L_3 = \mathcal{F}_3^4$ l'espace vectoriel des quadruplets de la forme $X = (x_1, x_2, x_3, x_4)$ avec $x_i \in \mathcal{F}_3$. A tout couple X, Y d'éléments de L_3, associons le scalaire

$$\delta(X, Y) = (x_1 - y_1)(x_2 y_3 - x_3 y_2) \text{ modulo } 3$$

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 L_3 une BMC.

On vérifie aisément qu'il y a deux CCEGT non isomorphes dont $(L_3, \star)$ est la BMC associée.

En effet : La BMC $(L_3, \star)$ admet pour neutre $e = (0,0,0,0)$, et que $\alpha = (0,0,0,1)$ y est un élément central.

Tout élément X de L_3 vérifie :

$$X \star X \star X = e \neq \alpha$$

Donc la CCEGT (L_3, T_α) n'admet aucun point d'inflexion, contrairement à (L_3, T_e) où tout point est d'inflexion.

2. Soit toujours $\mathcal{F}_3 = \mathbb{Z}_3$.

   Posons $\mathbb{Z}_9$ et désignons par $\mathbb{N}_3$ le produit cartésien $\mathcal{F}_3^2 \times \mathbb{Z}_9$, de terme générique $X = (x_1, x_2, x_3)$ avec x_1 et x_2 dans $\mathcal{F}_3$ 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 recéle 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.

2.1 Théorèmes de 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 étre non entropique [CH88].
Dans le cas particulier des CCEG issues des hypersurfaces cubiques, le sous-systéme $I(G)$ est une CCGH et on a :

Théorème 2.1.1

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

1. Tout tangentiel est un point d'inflexion c'est-à-dire $((xxz)) \in T$ entraîne $((zzz)) \in T$.
2. (G,T) admet un point d'inflexion et la BMC associée est d'exposant 6.
3. (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 $x + y = u \cdot xy$ alors $x \cdot y = -x - y$ donc $x^2 = -2x$.

- Si (1) est vérifiée on a : $x^2 \cdot x^2 = x^2$, on déduit que tout x^2 est point d'inflexion, est de plus :

$$2x^2 = x^2 + x^2 = u \cdot x^2x^2 = u \cdot x^2$$

$$= u \cdot xx = x + x = 2x,$$

alors $2x = 2x^2 = 2(-2x) = -4x$

donc $6x = u$ et $(G, \star)$ d'exposant 6, ce qui prouve (2).

- Si (2) est vérifiée avec u point d'inflexion, l'application

$$P : x \longrightarrow x^2 = -2x$$

vérifie $-2(x+y) = -2x - 2y$, c'est un endomorphisme idempotent de $(G,+)$ puisque

$$P(P(x)) = \left(x^2\right)^2 = 4x = -2x = x^2 = P(x)$$

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 $x \cdot y = -x - y = a_x \cdot b_y - x^2 - y^2 = a_x \cdot b_y + x^2 \cdot y^2$.

L'application :

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

$$x \quad \longrightarrow \quad \left(a_x, x^2\right)$$

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 $(G^2, \cdot)$.

- Si (3) est vérifiée $x = a_x + d$, $a_x \in A$ et $d \in G^2$ alors

$$x^2 = 2a_x + \left(x^2\right)^2 = 0_A + \left(x^2\right)^2 = \left(x^2\right)^2$$

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

Corollaire 2.1.1

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

Remarque 2.1.1 ***(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 2.1.2

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 $(G, \star_u)$ à une telle CCEGT est toujours d'exposant 3 puisque :

$$(x \star_u x) \star_u x = u \cdot ((u \cdot xx) \cdot x) = u\,(ux \cdot x) = uu = u$$

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 2.1.1

Toute BMC non associative est d'ordre divisible par 81, et il y a exactement deux BMC non isomorphes d'ordre 81, à savoir $(L_3, \star)$ et $(\mathbb{N}_3, \star)$.

Preuve.

Pour la démonstration de ce lemme on renvoit le lecteur au [**Ben81**].

Nous allons en déduire le :

Théorème 2.1.2

Toute 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 :
(L_3, T_α), (L_3, T_e) et $(\mathbb{N}_3, T)$.

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 $\mid E \mid = 81$, alors$(E, +)$ est isomorphe soit à $(L_3, \star)$, soit à $(\mathbb{N}_3, \star)$. Or, si $(E, +) \cong (\mathbb{N}_3, \star)$, alors nécessairement $(E, T) \cong (\mathbb{N}_3, T)$,d'aprés

la proposition **(1.1.1)**, car on vérifie que le centre de $(\mathbb{N}_3, \star)$ se réduit à $\theta(\mathbb{N}_3, \star)$. Par contre si $(E, +) \approxeq (L_3, \star)$, 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 calculé dans $(L_3, \star)$ avec $c \in \mathbb{Z}(L_3, \star) = \{-\alpha, e, \alpha\}$. Or les éventualités : $c = -\alpha$ et $c = \alpha$ donnent des CCEGT isomorphes

par l'involution $x \longrightarrow -x$. Par contre lorsque $c = e$, tout élément de la CCEGT correspondant (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 $(L_3, \star)$ et $(\mathbb{N}_3, \star)$ sont non isomorphes, aucune des deux CCEGT correspondant à $(L_3, \star)$ ne peut être isomorphe à $(\mathbb{N}_3, \star)$, seule la CCEGT associée à $(\mathbb{N}_3, \star)$.

Ceci termine la preuve.

Théorème 2.1.3 ***(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 entropique, et 3 sont terentropiques et non entropiques. Si $(L_3, \star)$ 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 $(L_3, \star)$ 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 $\left(\mathbb{Z}_3^4, T_{(1,1,1,1)}\right)$
$(\mathbb{Z}_3^2 \times \mathbb{Z}_9, +)$	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 $(\mathbb{Z}_{81}, T_1)$
$(L_3, \star)$	2 : (L_3, T_u) et (L_3, T_c)
$(\mathbb{N}_3, \star)$	1 : $(\mathbb{N}_3, T_v)$

Conclusion

Ce mémoire comporte des théorèmes de
classification nouveaux concernant les
courbes cubiques elliptiques généralisés (CCEG)
Quelques exemples de CCEG ont été donnés

Bibliographie

[1] [Ben81] L. Bénéteau. Ordre minimum des boucles de Moufang commutatives de classe 2 (res. 3), Ann. Fac. Sc. Toulouse Math. (5) 3,1981.

[2] [BL88] L.Bénéteau et J.Lacaze. Symplectic trilinear form and related designs and quasigroups. Communications in Algebra, 16(5), (1988), 1035-1051.

[3] [BR88] L. Bénéteau et G. Razafimanantsoa. Boucles de Moufang k-nilpotentes minimales. C.R.Acad.Sci.Paris, tome 306, Série I, (1988), 743-746.

[4] [Bru58] R.H. Bruck. A survey of binary systems. Springer-Verlag, 1958.

[5] [Bue01] F. Buekenhout. Generalized elliptic cubic curves. Part 1, Finite geometries, (2001), 35-48.

[6] [CPS90] O. Chein, H.O. Pflugfelder et J.DH. Smith. Quasigroups and loops; Theory and Applications. Sigma Series in Pure Mathematics, vol. 8, Heldermann, Berlin, 1990.

[7] [CH88] A. Cohen et A. Helminck. Trilinear alternating forms on a vector space of dimension 7. Communications in Algebra, 16(1), (1988), 1-25.

[8] [Ful69] W.Fultan. Algebric curve, Benjamin, New-York-Amsterdam, 1969.

[9] [Man74] Yu. I.Manin. Cubic forms. algebra, geometry, arithmetic, North-holland, Amsterdam, London, 1974.

[10] [Schw95] J. Schwenk. A classification of abelian quasigroups. Rend. Math. App. (7) 15 (2), (1995), 161-172.