ALGÈBRES DE LIE

Nous allons construire quelques algèbres de LIE centrales simples sur k = $\mathbb{Z}/2\mathbb{Z}$ dans ce chapitre

DEFINITION 3.0.22. (NOBUSAWA). Un ensemble S muni d'une opération binaire $\circ$ est **symétrique** si, pour tout a, b, c $\in$ S, on a :

(i) $a \circ a = a$;
(ii) $(b \circ a) \circ a = b$;
(iii) $(b \circ c) \circ a = (b \circ a) \circ (c \circ a)$.

Il est. facile de voir que $\vartheta : b \to b \circ a$ est une bijection pour tout a $\in$ S ; en effet, c'est un automorphisme du système (S , $\circ$) d'ordre 2.

DEFINITION 3.0.23. Un **espace alterné** est un espace vectoriel sur k = $\mathbb{Z}/2\mathbb{Z}$ muni d'une forme bilinéaire alternée (dégénérée ou pas).

Si G est un graphe, on définit k{G}, l'espace vectoriel sur k = $\mathbb{Z}/2\mathbb{Z}$ de base G. La matrice d'adjacence de G munit V d'une forme bilinéaire alternée, et nous nommerons k{G} l'espace alterné de G.

Il est facile de vérifier qu'un sous-ensemble S d'un espace alterné V clos sous l'opération $a \circ b = a + (a,b)b$ est un ensemble symétrique. On appelle un tel sous-ensemble S un ensemble **symétrique abélien** .

Une propriété remarquable des ensembles symétriques abéliens, qui n'est pas vraie en général pour les ensembles symétriques, est que

$a \circ b \neq a \Rightarrow a \circ b = b \circ a$

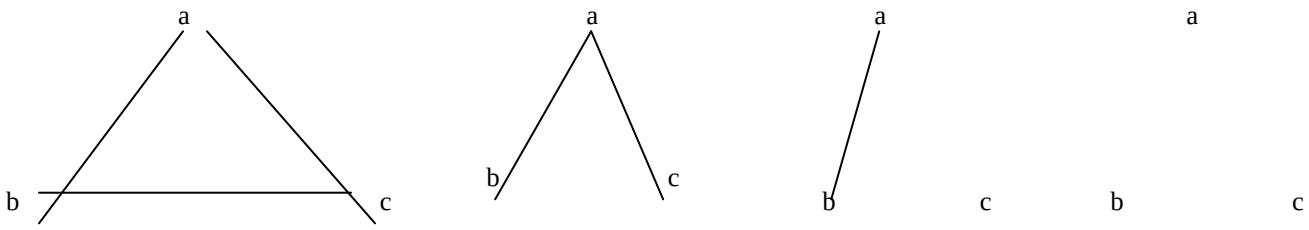
LEMME 3.0.24. (KAPLANSKY) Soit S un ensemble abélien symétrique, et soit L(S) l'espace vectoriel sur k de base $\{e_a : a \in S\}$.

Définissons la multiplication dans L(S) par $e_a e_b = (a, b)e_{a \circ b}$. Ainsi, L(S) est une algèbre de LIE de dimension |S| sur k.

DEMONSTRATION . La commutativité de la multiplication vient du fait que S est un ensemble abélien symétrique : (a,b) = 1, alors $a \circ b = b \circ a$.

Nous munissons , L(S) d'une forme bilinéaire alternée $(e_a,e_b) =(a, b)$ pour tout a, b $\in$ S.

Il y a quatre cas pour vérifier l'identité de Jacobi pour e_a, e_b, e_c, illustré ci-dessous (une arête a et b signifie que (a,b) = 1; aucune arête n'est définie ailleurs).



Cas 1 Cas 2 Cas 3 Cas 4

Chacun des cas ci dessus est simple, vérifions par exemple le cas 2:
(a,b) = 1, (a,c) = 1 et (b,c) = 0.

$e_a e_b . e_c + e_c e_a . e_b + e_b e_c . e_a = e_{a \circ b} e_c + e_{c \circ a} e_b + e_{b \circ c} e_a = e_{a \circ b} e_c + e_{c \circ a} e_b$
(car (b,c) = 0).
Par conséquent,
$a \circ b = a + b$ et $(a \circ b,c) = (a +b,c) = (a,c) + (b,c) = 1+0=1$.
D' où $e_{a \circ b} e_c = e_{(a \circ b)} e_c$

. De manière analogue, on a $e_{c\circ a}e_b = e_{(c\circ a)\circ b,}$ et leur somme est nulle (car k est de caractéristique 2).
Définissons une structure de graphe sur un espace vectoriel alterné V comme suit: pour
a, b ∈ V on dira que:
a et b sont adjacents ssi (a,b) = 1.
Nous pouvons considérer tout sous-ensemble S de V comme un sous-graphe fermé de V (deux sommets de S sont adjacents dans S ssi ils sont adjacents dans V).
DEFINITION 3.0.25. Soit σ,τ deux sommets d'un graphe G. Un sommet ρ sépare σ de τ si ρ est adjacent à exactement un d'entre eux.
Un graphe G est séparable si toute paire de sommets peut être séparée.
D'après le lemme 1.0.10 (ii) le graphe F est séparable.
Notons que si σ et τ sont adjacents, alors tout autre sommet les sépare; si dist(σ , τ) ≥ 3, alors tout sommet adjacent à l'un les sépare. Donc, la séparation est une propriété sur les sommets de distance 2. Il est facile par conséquent de voir qu'un graphe connexe est séparable ssi $\bar{a} = \bar{b} \Rightarrow$ a = b
(rappelons que $\bar{a}$ est l'ensemble de tous les sommets adjacents à a) .
THEOREME 3.0.26. Si S est un ensemble symétrique abélien dont le graphe est connexe et séparable, alors L(S) est une algèbre de LIE centrale simple sur $\mathbb{Z}/2\mathbb{Z}$.
DEMONSTRATION . Tout h ∈ L(S) a une valeur λ (h), à savoir, le nombre de e_a nécessaire pour l'exprimer comme une combinaison linéaire . Soit I ≠ 0 un idéal de L(S), et choisissons
h ∈ I de longueur positive minimale de l. Nous faisons une induction sur l ≥ 1 que I = L(S).
Si l = 1, alors h = e_a pour un certain a ∈ S. Si b ∈ S, alors $e_ae_b = (a,b)e_{(a\circ b)}$. S'il existe une arête dans S joignant a et b, alors $e_ae_b = e_{a+b} \in I$ et $e_{a+b}e_a = e_b \in I$. Plus généralement, s'il existe un chemin dans S de a à b, alors $e_a \in I$ entraîne que $e_b \in I$. Puisque le graphe est connexe, $e_b \in S$ pour tout b ∈ S, et donc I = L(S).
Si l ≻ 1, alors h = $\sum_A r_a e_a$ avec |A| ≥ 2 et $r_a =$ 1 pour tout a ∈ A. Si b ∈ S, alors

$$he_b = \sum_{A\cap\bar{b}} r_a e_{a\circ b} \qquad \text{où}$$

$\bar{b}$ = { s ∈ S : (s,b) =1 }. Notons que si a et a' sont des éléments distincts de A, alors
a ∘ b ≠ a' ∘ b . Donc $\lambda(he_b) = |A\cap\bar{b}|$, d'où $he_b \neq 0$.
Si $A\cap\bar{b} \neq \varnothing$. Choisissons a, a' ∈ A avec a ≠ a'. Puisque S est séparable, il existe b ∈ S qui les sépare. Alors $A\cap\bar{b} \neq \varnothing$, donc $he_b \neq 0$ et $|A\cap\bar{b}| < |A|$. D' où l'hypothèse d'induction s'applique et I = L(S).
Soit K une extension du corps k, et soit J un idéal non nul de K⊗L(S). Choisissons h ∈ J, h ≠0 ; alors,

$$h = \sum_A r_a e_a$$

où $A \subset S$ et tous les $r_a \in S$ sont non nuls. Si |A| ≥ 2 et a,b ∈ A, la séparabilité fournit un
c ∈ S avec (a,c) = 1 et (b,c) = 0. L'élément he_c est un élément non nul de J de longueur minimale. Donc, nous pouvons supposer que J contient r_ae_a pour un certain a ∈ S et un élément non nul $r_a \in K$; puisque K est un corps, nous pouvons supposer que $e_a \in J$. La connectivité de S nous montre que J contient { e_a : a ∈ S}, qui est une K – base , et donc
J = K⊗L(S).

NOBUSAWA définit un ensemble symétrique simple S, comme ne contenant aucun sous-ensemble symétrique propre B avec |B| ≥ 2 et (B ∘ c) ∩ B = B ou ∅ pour tout c ∈ S.

THEOREME 3.0.27. Un ensemble symétrique S est simple si, et seulement s'il est connexe et séparable

DEMONSTRATION . Si S est connexe et séparable, alors S est simple.
(Dans l'article de N. NOBUSAWA, SIMPLE SYMMETRIC SETS AND SIMPLE GROUPS, OSAKA J. MATH , la transitivité de NOBUSAWA donne la connectivité, et son autre hypothèse est la séparabilité).
Supposons que S est simple. Si B est une composante de S, alors a,b ∈ B implique que
a ∘ b ∈ B, d'où B est sous-ensemble symétrique de S. Si c ∉ B ; alors (b,c) = 0 pour tout
b ∈ B, et b ∘ c = b ; d'où B ∘ c = B. Si avec |B| = 1, on a aussi B ∘ c = B. Si c ∈ B et |B| alors
B connexe entraîne qu'il existe b ∈ B avec (b,c) = 1. Par conséquent, b ∘ c = b + c ∈ B car (b+c,b) = (c,b) = 1.
Donc B ∘ c ⊂ B (finalement, B ∘ c = B car l'application $\vartheta_c : S \to S$ définie par s → s ∘ c est une bijection). Puisque S est simple, B = S et donc S est connexe.

Si S n'est pas séparable, alors il existe $a,b \in S$ qui ne peuvent pas être séparés nous pouvons supposer que a et b sont adjacents .
Définissons B={a,b} tel qu'il soit un sous-ensemble symétrique de S.
Si $c \in$ ={a,b}, alors $B \circ c = B$. D'autre part, c est adjacent à a et à b. Donc, $b \circ c = b + c$ et $a \circ c = a + c$. Supposons $(B \circ c) \cap B \neq \varnothing$; soit $a + c \in B$. Alors soit , $a + c = a$, soit $a + c = b$. Dans le premier cas, on a $c = 0$, cela contredit $(a,c) \neq 0$. Dans le second cas, on a forcément $b+ c = a$, et donc $B \circ c = B$. L'un ou l'autre cas contredit la simplicité de S.

COROLLAIRE 3.0.28. (CHARNES). Si S est un ensemble symétrique abélien simple, alors L(S) est une algèbre de LIE centrale simple sur $\mathbb{Z}/2\mathbb{Z}$

DEMONSTRATION . Elle est immédiate à partir du théorème.

DEFINITION 3.0.29. Si V est un espace alterné, toute intersection de sous-ensembles symétriques abéliens est aussi; si B est un sous-ensemble quelconque de V, sa clôture $B*$ est le sous-ensemble symétrique abélien engendré par B.
Si $B \subset V$ est un sous-ensemble, on définit $B \circ B = \{x + (x,y)y : x, y \in B\}$.
Remarquons que $B \subset B \circ B$, pour $x = x + (x,x)x$.

DEFINITION 3.0.30. Si $B \subset V$, où V est un espace alterné, on définit $B^0 = B$ et $B^{r+1} = B^r \circ B^r$. Remarquons que $B^r \subset B^{r+1}$.
LEMME 3.0.31. Soit $B \subset V$, où V est un espace alterné. Si $B*$ désigne sa clôture, alors

$$B* = \bigcup_{r \geq 0} B^r.$$

DEMONSTRATION .Il est clair que $B*$ contient l'union $\cup$. D'autre part, U est un ensemble Symétrique : si $\alpha, \beta \in U$, alors il existe $r \geq 0$ avec $\alpha, \beta \in B^r$, et $\alpha \circ \beta \in B^{r+1} \subset U$.

LEMME 3.0.32. Si B est un sous-ensemble connexe d'un espace alterné V, alors sa clôture $B*$ est aussi connexe

DEMONSTRATION . Au sens du lemme précédent, il suffit de prouver que si B est connexe alors $B \circ B$ l'est aussi. Chaque nouveau élément de $B \circ B$ (i.e, qui n'est pas dans B) est de la forme $a + (a,b)b$, où $a,b \in B$ et $(a,b) = 1$. D'où $(a +b,b) = 1$, et il existe une arête joignant $a + (a,b)b$ et a. Donc, $B \circ B$ est connexe.

DEFINITION 3.0.33. Un graphe connexe régulier est bien régulier si $|\bar{a} \cap \bar{b}|$ ne dépend pas des sommets adjacents a et b. Un graphe bien régulier est fortement régulier si $|\bar{a} \cap \bar{b}|$ ne dépend pas du choix des sommets distincts non-adjacents a et b.
Si H est bien régulier, posons $\lambda = |\bar{a} \cap \bar{b}|$ lorsque a et b sont adjacents ; si H est fortement régulier, posons $\mu = |\bar{a} \cap \bar{b}|$ lorsque a et b ne sont adjacents.

THEOREME 3.0.33.

(i) Si est un ensemble symétrique connexe abélien, alors S est un graphe bien régulier avec $k = 2\lambda$.
(ii) Si, de plus, S est séparable et n'est pas un graphe complet, alors il est fortement régulier et $\lambda = 0 \mod 4$.

DEMONSTRATION .

(i) D'après la connectivité, il suffit de prouver que si a et $b \in S$ et $(a,b) = 1$, alors $|\bar{a}| = |\bar{b}|$. Si $x \in \bar{a}$, alors $x + a \in S$ et la fonction $\vartheta_a : x \to x+a$ est une bijection de $\bar{a} \to \bar{a}$

(qui est son propre inverse) . Si $x \in \bar{a} \cap \bar{b}$, alors

$(x,b) = 1$, $(x + a, b) = (x,b) + (a,b) = 1+1 = 0$,

et $x \in \bar{a} - \bar{b}$; si $x \in \bar{a} - \bar{b}$, alors $(x + a, b) = 0 + 1 = 1$

et $x + a \in \bar{a} \cap \bar{b}$. Il s'ensuit que $\vartheta_a(\bar{a} \cap \bar{b}) = \bar{a} - \bar{b}$ et $\vartheta_a(\bar{a} - \bar{b}) = \bar{a} \cap \bar{b}$. Donc

$|\bar{a} \cap \bar{b}| = |\bar{a} - \bar{b}|$ et $|\bar{a}| = 2|\bar{a} \cap \bar{b}|$. En échangeant les rôles de a et b on obtient

$|\bar{a}| = |\bar{b}|$. Puisque $|\bar{a}| = k$ et $|\bar{a} \cap \bar{b}| = \lambda$, nous avons montré que S est régulier et que

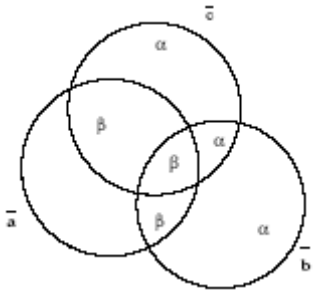
$k = 2\lambda$. D'où, S est bien régulier.

(ii) Supposons maintenant que, a, b, u, v satisfont (a,b) = (u,v) = 0

(Cela est possible car nous sommes dans le cas où S n'est pas complet) ; il suffit de montrer que $|\bar{a} \cap \bar{b}| = |\bar{u} \cap \bar{v}|$ • Notons d'abord que pour a, $x \in S$, $\vartheta_x(\bar{a}) = \overline{\vartheta x(a)}$; aussi, puisque ϑ_x est une bijection, $|\bar{a} \cap \bar{b}| = |\vartheta_x \bar{a} \cap \vartheta_x \bar{b}|$. Maintenant, prenons un chemin de u à a ; les applications itérées de ϑ_x pour x dans le chemin donne $|\bar{a} \cap \bar{b}| = |\bar{a} \cap \bar{c}|$ pour un certain sommet c. Ainsi, il suffit de montrer que $|\bar{a} \cap \bar{b}| = |\bar{a} \cap \bar{c}|$ lorsque (a,b) = (a,c) = 0.

Les preuves suivantes reposent sur l'analyse de diagrammes de Venn.

1er cas (b,c) = 1 [(a,b) = (a,c) = 0] :



Supposons d'abord que $\bar{b} \cap \bar{c} - \bar{a} \neq \varnothing$. Si $x \in \bar{b} \cap \bar{c} - \bar{a}$, alors $b + c \in S$. Le produit interne de b + x avec a, b, c montre que $b + x \in \bar{b} - \bar{a} - \bar{c}$; d' où $|\bar{b} \cap \bar{c} - \bar{a}| = |\bar{b} - \bar{a} - \bar{c}|$. En échangeant les rôles de b et c, on obtient $|\bar{b} \cap \bar{c} - \bar{a}| = |\bar{c} - \bar{a} - \bar{b}|$; désignons leur valeur commune par α. Nos arguments précédents montrent que $|\bar{b} \cap \bar{c}| = \lambda$ (car (b,c) = 1).

Si $\beta = |\bar{a} \cap \bar{b} \cap \bar{c}|$, alors $\lambda = \alpha + \beta$; puisque $|\bar{b}| = 2\lambda = |\bar{c}|$, il s'ensuit que

$|\bar{a} \cap \bar{c} - \bar{b}| = \beta = |\bar{a} \cap \bar{b} - \bar{c}|$. Donc, $= |\bar{a} \cap \bar{b}| = 2\beta = |\bar{a} \cap \bar{c}|$.

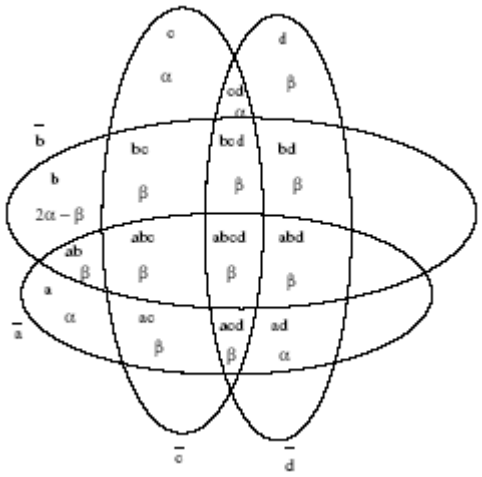
Si $|\bar{b} \cap \bar{c} - \bar{a}| = \varnothing$, alors $\alpha = 0$ et $\bar{c} \subset \bar{a}$; par régularité, $|\bar{c}| = |\bar{a}|$, et donc $\bar{c} = \bar{a}$, ce qui contredit la séparabilité de S.

2e cas (b,c) = 0 et [(a,b) = (a,c) = 0] :

Puisque S est séparable, il existe $d \in S$ avec (a,d) = 1 et (b,d) = 0.

Il y a maintenant deux sous cas dépendant soit de (c,d) = 1, soit de (c,d).

Sous-cas (i). (c,d) = 1. Nous adoptons la notation $ac = \bar{a} \cap \bar{c} - \bar{b} - \bar{d}$, etc., pour les 15 régions possibles du diagramme de Venn déterminé par les quatre ensembles $\bar{a}$, $\bar{b}$, $\bar{c}$, $\bar{d}$:



Si x ∈ abd, alors en effectuant le produit interne de x + d avec a, b, c, d on montre que ϑ_d transforme abd en bcd ; notons β leur taille commune ; nous simplifions cela en disant que ϑ_d donne | abc| = | bcd| . Par conséquent ϑ_a donne | abc| = | bcd| = β ; ϑ_a donne | ab| = | **a**bd| =β ;

ϑ_c donne | bc| = | bcd| = β ; ϑ_d donne | bd| = | abc| = β ; ϑ_d donne | bd| = |abcd| = β. Une analyse du diagramme de Venn montre que | $\bar{a} \cap \bar{b}$ | = 4β = | $\bar{b} \cap \bar{c}$ |.

Nous avons donc montré que β ≠ 0. Un chemin de a vers b, passant par les sommets (adjacents) a, r, s, …, b réduit si sa longueur dépasse 2 : il suffit de remplacer simplement r et s par r + s. Il s'ensuit que $\bar{a} \cap \bar{b} \neq 0$ et β ≠ 0. Notons que, si d existe, alors il existe un d' tel que (a,d') = 1 = (b,d') et (c,d') = 0 ; ainsi, $\bar{a} \cap \bar{b} - \bar{c} \neq 0$, car | $\bar{a} \cap \bar{b} - \bar{c}$ | = 2β ≠ 0. En répétant l'argument ci-dessus avec d' à la place de d, on a : | $\bar{a} \cap \bar{c}$ | = | $\bar{b} \cap \bar{c}$ |, le résultat souhaité.

Sous-cas (ii). (c,d) = 0 pour tout séparateur d. L'hypothèse est que tout d tel que (a,d) = 1 et (b,d) = 0 doit satisfaire (c,d) = 0 ; en d'autres termes, $\bar{a} \cap \bar{b} - \bar{c} = \varnothing$. Comme nous l'avons remarqué dans le cas précédent, cela entraîne forcément que $\bar{a} \cap \bar{b} - \bar{c} = \varnothing$. Mais dans ces conditions, on a | $\bar{a} \cap \bar{b}$ | = | $\bar{a} \cap \bar{b} \cap \bar{c}$ | = | $\bar{a} \cap \bar{c}$ | .

Nous avons montré que S est fortement régulier avec k = 2λ. Il reste à montrer que μ est un multiple de 4 (Cela serait, si nous savions que le cas (ii) reste valable). Soient a et b deux sommets non adjacents, et soit c ∈ $\bar{a} \cap \bar{b}$. Par conséquent, (a,b) = 0, et donc c + a + b ∈ S car (c + a , b) = 0 + 1 = 1 . Il est facile de voir que c, c + b, c + a et c + a + b sont tous les quatre des éléments de $\bar{a} \cap \bar{b}$. S'il en existe un autre élément, notons le d (dans $\bar{a} \cap \bar{b}$). Alors il est facile de voir que les ensembles {c, c + a, c + b, c + a + b} et {d, d + a, d + b, d + b + a} sont disjoints ; et le résultat en découle.

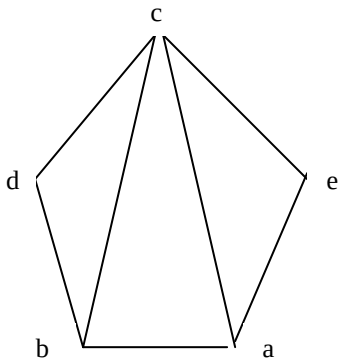
COROLLAIRE 3.0.35. Si G est un graphe connexe, alors G∗ est bien régulier avec k = 2λ.

DEMONSTRATION .

Il découle immédiatement du théorème et du lemme 3.0.31.

EXEMPLE 3.0.36. Le graphe formé de deux sommets et d'une arête entre eux est connexe et séparable.

EXEMPLE 3.0.37. Considérons le graphe connexe et séparable G suivant :



Soit k{G} l'espace alterné de G. Les éléments de $G^1 = G$ o G sont a + b, a + c, a + d,

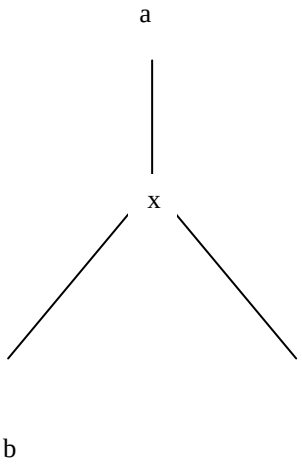
b +c, b + e, c + d, c + e, et l' on montre facilement qu' il est impossible de séparer a + b et c. Donc, G o G n'est pas séparable. En effet, $G^2 = G^1$ o G^1 possède les nouveaux éléments

a + b + d, a + b +e, a + c + e, b + c +d, c + d + e, a + b + c+ d, a + b + c + e, a + b + c + e, et

l'on ne peut non plus séparer a +b et c.n poussant le développement, on a $G^3 = G^2oG^2 = G^2$, donc $G* = G^2$ n'est pas séparable. Notons que = |G∗| = 20, donc c'est un sous-ensemble propre de V – {0} (remarquons que si B est un sous-ensemble d'un espace alterné, alors

$0 \in B*$ ssi $0 \in B$).

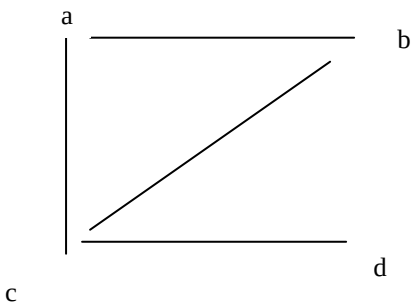
EXEMPLE 3.0.38.



Soit G le graphe constitué de trois sommets non adjacents tous connectés à un quatrième sommet ; comme le montre la figure ci-dessus, et soit V = k{G}, où k = **Z**/2**Z**. On montre que

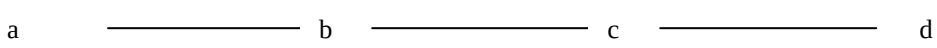
$G* = G^3 = V-\{0\}$, et donc la clôture de G requiert trois étapes. Maintenant G∗ est connexe mais non séparable ; de plus, L(G∗) n'est pas simple car $(e_a + e_b)$ est un idéal propre. Donc, l'hypothèse de séparabilité du théorème 3.0.25 est nécessaire.

EXEMPLE 3.0.39. Considérons le graphe G suivant



Il est facile de prouver que, dans V = {G} (où k = **Z**/2**Z**), que G∗ = G ² et |G∗| = 10.

EXEMPLE 3.0.40. Si G est le graphe linéaire



On montre facilement que |G∗| = 10.

EXEMPLE 3.0.41. Si G = K_4, le graphe complet sur quatre sommets, on montre aussi facilement que |G∗| = 10.

Les trois exemples précédents de G∗ sont isomorphes (chacun d'eux est en fait le complément du graphe de Petersen).

Nous remarquons que le graphe de base symplectique est une union disjointe d'arêtes qui sont très loin d'être connectées.

LEMME 3.0.42. Supposons que V est un espace alterné dont la forme bilinéaire est non dégénérée. Si S est un sous-ensemble de V qui contient une base de V, alors S est un sous-graphe séparable.

DEMONSTRATION. Autrement, il existerait deux sommets distincts a et b dans S avec $\overline{a} = \overline{b}$. D'où pour tout x ∈ S on aurait (a,x) = (b,x) ; ainsi (a + b,x) = 0 pour tout x ∈ S. Comme S contient une base de V, et que (a + b,x) = 0 pour tout x ∈ V, cela qui contredit la dégénérescence de la forme.

COROLLAIRE 3.0.43. Pour tout n ≥ 1, il existe une algèbre de LIE centrale simple sur **Z** /2**Z** de dimension 4^n – 1.

DEMONSTRATION. Soit V un espace vectoriel sur **Z**/2**Z** de dimension 2n muni d'une forme bilinéaire alternée non dégénérée. Il est facile de voir que S = V – {0} est un ensemble symétrique abélien qui est connexe (choisissons une base symplectique de V ; tout vecteur non nul est adjacent à un certain vecteur de la base, et tout vecteur de base est adjacent au vecteur dont toutes les cordonnées valent 1) et séparable (lemme ci-dessus) ; et le résultat découle du théorème 3.0.25.

DEFINITION 3.0.44. Un graphe est dit non dégénéré lorsque sa matrice d'adjacence est de déterminant impair ; c'est à dire si sa matrice d'adjacence est non singulière mod 2.

Une matrice symétrique formée de 0 et de 1 ayant des 0 sur la diagonale, comme une matrice d'adjacence, est antisymétrique lorsqu'on le considère modulo 2. Mais si une matrice d'adjacence antisymétrique m×m est non singulière, alors m doit être pair. Donc, seuls les graphes dont le nombre total de sommets est pair peuvent être non dégénéré. En particulier, le graphe séparable de l'exemple 3.0.36. est dégénéré car il possède cinq sommets. Tous les autres exemples sont les plus petits graphes connexes non dégénérés. Si n est pair, alors K_n, le graphe complet sur n sommets, est non dégénéré : si J est un n×n-matrice tel que chaque terme soit égal à 1, alors J^n= nJ

= 0 mod 2 (puisque n est pair) ; mais la matrice de K_n mod 2 est J + I, et il est non singulier car c'est la somme de la matrice d'identité et d'une matrice nilpotente.

COROLLAIRE 3.0.45. Si G est un graphe connexe non dégénéré ayant plus de deux sommets, alors G* est un graphe fortement régulier avec $k = 2\lambda$ et $\mu = 0 \bmod 4$.

DEMONSTRATION. Si G n'est pas complet, alors il ;existe deux sommets a et b dans G tels que (a,b) = 0, et cette équation reste valable dans G* ; d'où G* n'est pas complet. Si G est une arête, alors G* est le graphe complet sur trois sommets. Si G est complet sur plus de deux sommets, il contient trois sommets distincts a, b et c. Par conséquent, G* contient a et b + c, et ceux-là ne sont pas adjacents car (a, b + c) = 1 + 1 = 0 ; donc, G* n'est pas complet. Par suite, on a le résultat avec le théorème 3.0.35. et le lemme 3.0.41.

THEOREME 3.0.46. Soit G un graphe connexe non dégénéré, et soit G* sa clôture dans espace alterné k{G}. Alors L(G*) est une algèbre de LIE centrale simple sur **Z**/2**Z**.

DEMONSTRATION. D'après le lemme 3.0.31, la connectivité de G entraîne celle de G* ; d'après le lemme 3.0.41, la non dégénérescence de G entraîne la séparabilité de G* . Donc, le théorème 3.0.25 nous donne la simplicité de L(G*).

Rappelons que la dimension de L(G*) est |G*| = n, et la forte régularité de G∗ donne la formule suivante : $k(k - \lambda - 1) = \mu(n - k - 1)$ ainsi, n est déterminé par trois paramètres. En réalité, $k = 2\lambda$ permet de déterminer n à partir de deux de ces paramètres.

On peut assimiler G à un ″diagramme de DYNKIN ″ pour L(G*) en ce sens que l'on peut construire l'algèbre à partir de ce graphe.

Le graphe de l'exemple 3.0.35 nous fournit une algèbre de LIE centrale simple de dimension 3, et les exemples 3.0.37, 3.0.38, 3.0.39, des algèbres de LIE centrales simples de dimension 10.

COROLLAIRE 3.0.47. Soit X un plan projectif d'ordre pair. Si F est le graphe résultant du drapeau de X, alors L(F*) est une algèbre de LIE centrale simple sur **Z**/2**Z**.

DEMONSTRATION. L'espace alterné de F est H(X). Le résultat découle du lemme 1.0.9 et du théorème 1.0.7

KAPLANSKY donne quatre classes des algèbres de LIE centrales simples sur **Z**/2**Z,** la première d'elle résulte d'un espace vectoriel muni d'une forme bilinéaire non alternée. La classe II est précisément L(S) lorsque S = V –{0} (corollaire 3.0.42). La classe III est de dimension n(n –1)/2 (elle s'avère être L(K*), où K_n est le graphe complet sur n sommets). Enfin, soit V un n-espace alterné non dégénéré, et soit Q une forme quadratique associée à la forme bilinéaire. Alors, S = { v ∈ V : Q(v) = 1} est un ensemble symétrique qui est connexe et séparable, et L(S) donne des algèbres de KAPLANSKY de classe IV.

Jusque-là, nous avons travaillé avec des algèbres de LIE munies de formes bilinéaires ; une question naturelle est le cas où il n'y aurait pas de connectivité avec les formes de KILLING :

$$f(e_a, e_b) = Tr((ada)(adb)).$$

COROLLAIRE 3.0.48. La forme de KILLING sur L(G*) est identiquement nulle.

DEMONSTRATION.Soient a et b ∈ Vert(G). Pour tout c dans Vert(G) on a,
$e_c e_a . e_b = (c,a)e_{c\,o\,a}e_b = (c,a)(coa, b)e_{(c\,o\,a)o\,b} = (c,a)(c + (c, a)a, b)e_{c+(c,a)a+(c+(c,a)a,b)b.}$
Par consequent,

$$(coa)ob = c \text{ ssi } (c,a)a = [(c,b) + (c,a)(a,b)]b.$$

Si $(coa)ob \neq c$, alors c ne contribue pas à la trace de (ada)(adb) ;
Si (coa)ob = c, alors soit (c,a) = 0, d'où (c,b) = 0, et la contribution est nulle, soit (c,a) = 1 auquel cas a = b. Calculons $Tr((ade_a)^2)$;
$e_c e_a . e_a = (c,a)e_{c\,o\,a}e_a = (c,a)(coa, a)e_{(c\,o\,a)o\,a} = (c,a)e_c$

car (c,a)a = (c + (c,a)a,a) = (c,a) et (coa)oa = c . D'où

$$Tr((ade_a)^2) = \sum_{c \in \overline{a}} (c,a) = |\overline{a}|.$$

Nous avons montré que $f(e_a, e_b) = 0$ si $a \neq b$ et $f(e_a, e_b) = |\overline{a}| \bmod 2$ si $a = b$. D'après le corollaire 3.0.34, G* est un graphe régulier de valence paire k, et donc $|\overline{a}| = 0 \bmod 2$ pour tout sommet $a \in G$

Nous remarquons que les algèbres de LIE L(S) ne sont jamais restreintes, pour la dérivation, $(ade_a)^2$ n'est pas nécesaire interne. Supposons que, pour tout $b \in S$, $e_b(ade_a)^2 = e_b x$ pour un certain $x = \Sigma r_c e_c \in L(S)$ (un tel x est parfois noté $e_a^{[2]}$). Par conséquent, $e_b e_a . e_a = (b,a) e_b$, comme nous venons juste de le voir. D'autre part, $e_b \Sigma r_c e_c = \Sigma r_c(b,c) e_{b\,o\,c}$. Puisque $boc = b + (b,c)c$, alors $e_{b\,o\,c} = e_b$ ssi $(b,c) = 0$. Maintenant, choisissons b tel que $(b,a) = 1$. Alors $e_b = \Sigma r_c(b,c) e_{b\,o\,c}$;
mais seuls les termes de droite impliquant e_b doivent avoir leur coefficient $(b,c) = 0$, et contradiction avec les éléments de base $\{ e_c : c \in S\}$.
J.J. ROTMAN une interprétation de la non dégénérescence de la théorie des graphes de P.M. WEICHSEL.

DEFINITION 3.0.49 Une l-factorisation (ou distribution parfaite) d'un graphe G est une partition de ces sommets en deux sous-ensembles $\{ a_i, b_i \}$ avec a_i et b_i adjacents pour tout i.

THEOREME 3.0.50. (WEICHSEL) Soit G un graphe fini de la matrice d'adjacence A. Si μ est le nombre de l-factorisations de G, alors $\det A \equiv \mu \bmod$.

DEMONSTRATION. Il existe une interprétation de la théorie des graphes pour les coefficients du polynôme caractéristique de A ; en particulier, il y a une interprétation du déterminant de A. Rappelons qu'un circuit dans un graphe est un sous-graphe régulier connexe de valence 2 ; une figure de base dans un graphe est un sous-graphe dont les composantes sont soit, des circuits, soit des arêtes. La formule

$$\det A = \sum_{U} (-1)^{p(U)} 2^{c(U)}$$

est vérifiée. Ici U est une figure de base impliquant tous les sommets de G, p(U) est le nombre de composantes de U, et c(U) est le nombre de circuits de U. Puisque non seulement intéressé par la parité du det A, nous avons besoin seulement de ces figures de base U telles que

c(U) = 0 ; c'est à dire, les sous-graphes dont les composantes sont des arêtes. Mais un tel sous-graphe est simplement une l-factorisation.

COROLLAIRE 3.0.51. Tout graphe non dégénéré possède une l-factorisation.
NOBUSAWA a montré comment considérer tout groupe G comme un sous-ensemble symétrique.
Désignons le produit du groupe de G par la juxtaposition, et une opération binaire sur G par :
$aoc = ba^{-1}b$.
Il est facile de prouver que (G,o) est un ensemble symétrique.

LEMME 3.0.52.

(i) Soit S un ensemble symétrique, et soient $a,b \in S$. Alors $aob \neq a$ ssi $boa \neq b$

(ii) Un ensemble symétrique S est un graphe si l'on définit : $a,b \in S$ sont adjacents ssi $aob \neq a$.

DEMONSTRATION. (i) Autrement, $boa = a$. Mais dans ce cas on aurait
$aob = (aoa)o(boa) = (aob)oa$, ce qui entraînerait que $a = aob$ car $x \rightarrow xob$ est une bijection ; ce qui contredirait l'hypothèse.
(ii) Pour tout $a \in S$, nous avons $aoa = a$; c'est à dire, a n'est pas adjacent à lui même. La partie (i) montre que l'adjacence est une relation symétrique.

Si G est un groupe, on peut le considérer comme un ensemble symétrique, et par conséquent comme un graphe. Il existe un foncteur γ : groupes $\rightarrow$ graphes, où $Vert(\gamma G) = G$ et, si $a,b \in G$, alors a et b sont adjacents ssi $ba^{-1}b \neq a$; c'est à dire, $(a^{-1}b)^2 \neq 1$.
Nous noterons $a \sim b$ si a et b sont adjacents dans γG.

LEMME 3.0.53.

(i) Si G est un groupe et a, b, c des éléments de G, les expressions suivantes sont équivalentes dans γG :

$a \sim b$; $ac \sim bc$; $ca \sim cb$

(ii) Si G est un groupe, alors γG est un graphe régulier de valence d, où

$d = |\{x \in G : x^2 \neq 1\}|$.

DEMONSTRATION

(i) Trivial, on utilise le fait que $a \sim b$ ssi $(a^{-1}b)^2 \neq 1$

(ii)La régularité de γG vient de la traduction de $1 \sim b$, comme dans (i) ; par conséquent, la valeur de d représente le nombre d'éléments adjacents à 1.

Le résultat (négatif) suivant montre que cette approche ne produit pas d'algèbres de simple.

THEOREME 3.0.54. (ROTMAN ET WEICHSEL). Tout groupe fini G est dégénéré.

DEMONSTRATION. Soit A une matrice d'adjacence de γG. Maintenant G est un graphe régulier de valence $d = |G| - |\{x \in G : x^2 = 1\}|$.

Un théorème de FROBENIUS donne $|\{x \in G : x^2 = 1\}|$ un multiple de $(|G|, 2)$, donc d est toujours pair. Mais tout graphe régulier de valence d admet d comme valeur propre ; d'où

$\det A \equiv 0 \bmod 2$.

WEICHSEL a montré que si $E = \{x \in G : x^2 \neq 1\}$, alors $| G - E| < 1/2| G|$ implique que γG est un graphe régulier connexe de diamètre 2 ; de plus, G est engendré par E et γG est le graphe de CALEY de G relatif à l'ensemble générateur E.

On voit donc que l'espace alterné d'un graphe peut s'avérer être un outil puissant dans l'étude des graphes

THEOREME 3.0.55. Si G est un graphe connexe non dégénéré ayant n sommets, alors Aut(G) peut être plongé comme un sous-groupe de Sp(n, 2). En effet Aut(G) est le stabilisateur de G sous l'action de Sp(n, 2) sur $k\{G\}$.

DEMONSTRATION. Nous savons que G est une base de $V = k\{G\}$ (où $k = \mathbf{Z}/2\mathbf{Z}$), un ,espace alterné de dimension n. Si φ est un automorphisme de graphe de G, alors φ conserve le produit interne, donc il est simplectique.

Conclusion

Je finis par ces quelques remarques à propos du sujet. C'est un sujet que, personnellement, je trouve particulièrement riche et intéressant. Il m'a permis à la fois de renforcer mes connaissances théoriques sur l'algèbre classique et bilinéaire que j'utilise dans ce document mais aussi et surtout de me familiariser avec la théorie des graphes. Ce qui est particulièrement instructif et qui m'a permis de consulter pas mal d'œuvres, c'est la géométrie projective. Dans ce document, je n'ai eu à parler que de plans projectifs qui constituent une partie de cette discipline.

Je pense qu'une étude intéressante peut être lancée pour la recherche dans le domaine de la géométrie projective et de l'application de l'algèbre dans cet environnement. Ce document constitue un premier pas dans la recherche et je pense qu'il ne sera pas aussi parfait comme je le voudrais ou comme le souhaiteraient mes encadreurs. Néanmoins, on dit qu'il faut un début à tout et j'apprendrai avec le temps.