Proceedings of the Edinburgh Mathematical Society (1986) 29, 187–197 ©

SUR LES ALGEBRES GAMETIQUES

par ARTIBANO MICALI et PHILIPPE REVOY

(Reçu le 17 Janvier 1985)

1. Préliminaires

Soient K un anneau commutatif à élément unité, P un K-module unitaire, $S_K(P)$ l'algèbre symétrique de P et $S_K^m(P)$ le sous-K-module de $S_K(P)$ des éléments homogènes de degré $m \geqq 0$. Rappelons que si P est un K-module libre de rang $n+1$, l'algèbre $S_K(P)$ est isomorphe à l'algèbre des polynômes $K[X_0, X_1, \ldots, X_n]$ en les indéterminées $X_0, X_1, \ldots, X_n$ à coefficients dans K et $S_K^m(P)$ est le K-module libre dont une base est formée par les monômes $X_0^{i_0} X_1^{i_1} \ldots X_n^{i_n}$ tels que $\sum_{k=0}^n i_k = m$, i.e., par les monômes homogènes de degré m.

On rappelle ici que l'*algébre gamétique* d'une population multiallélique, i.e., avec $n+1$ allèles et polyploïde, c'est-à-dire, $2m$-ploïde est le K-module libre $S_K^m(P)$, où P est un K-module libre de rang $n+1$, muni de la structure d'algèbre commutative et non associative dont la table de multiplication relativement à la base canonique s'écrit

$$(X_0^{i_0} X_1^{i_1} \ldots X_n^{i_n}) * (X_0^{j_0} X_1^{j_1} \ldots X_n^{j_n}) = \binom{2m}{m}^{-1} \sum_{k_0 + \cdots + k_n = m} \binom{i_0 + j_0}{k_0} \ldots \binom{i_n + j_n}{k_n} X_0^{k_0} X_1^{k_1} \ldots X_n^{k_n}$$

quelles que soient les suites d'entiers $(i_0, \ldots, i_n)$ et $(j_0, \ldots, j_n)$ vérifiant $\sum_{k=0}^n i_k = m$ et $\sum_{k=0}^n j_k = m$, où l'on suppose que K soit un $\mathbb{Q}$-espace vectoriel. En la base de $S_K^m(P)$ formée par les monômes $X_0^{i_0}(X_0 - X_1)^{i_1} \ldots (X_0 - X_n)^{i_n}$ avec $\sum_{k=0}^n i_k = m$, cette table de multiplication s'écrit

$$(X_0^{i_0}(X_0 - X_1)^{i_1} \ldots (X_0 - X_n)^{i_n}) * (X_0^{j_0}(X_0 - X_1)^{j_1} \ldots (X_0 - X_n)^{j_n})$$

$$= \binom{2m}{m}^{-1} \binom{i_0 + j_0}{m} X_0^{i_0 + j_0 - m}(X_0 - X_1)^{i_1 + j_1} \ldots (X_0 - X_n)^{i_n + j_n}$$

quelles que soient les suites d'entiers $(i_0, \ldots, i_n)$ et $(j_0, \ldots, j_n)$ vérifiant $\sum_{k=0}^n i_k = m$ et $\sum_{k=0}^n j_k = m$. Or, à un changement de base près, cette table de multiplication peut encore s'écrire

$$(X_0^{i_0} X_1^{i_1} \ldots X_n^{i_n}) * (X_0^{j_0} X_1^{j_1} \ldots X_n^{j_n}) = \binom{2m}{m}^{-1} \binom{i_0 + j_0}{m} X_0^{i_0 + j_0 - m} X_1^{i_1 + j_1} \ldots X_n^{i_n + j_n},$$

quelles que soient les suites d'entiers $(i_0, \ldots, i_n)$ et $(j_0, \ldots, j_n)$ vérifiant $\sum_{k=0}^n i_k = m$ et $\sum_{k=0}^n j_k = m$. Si, maintenant, on désigne par fg le produit ordinaire de deux polynômes f

et g dans l'algèbre $K[X_0, X_1, \ldots, X_n]$, la structure d'algèbre de $S_K^m(P)$ est donnée par

$$f * g = \frac{m!}{(2m)!} \frac{\partial^m}{\partial X_0^m}(fg),$$

quels que soient les polynômes f et g dans $S_K^m(P)$, où $\partial/\partial X_0$ désigne la dérivée partielle relativement à la variable X_0.

Cette construction nous guidera, par la suite. On remarque tout simplement que si l'on pose $d = \partial/\partial X_0$, la formule ci-dessus peut encore s'écrire

$$f * g = \binom{2m}{m}^{-1} \sum_{r+s=m} \frac{1}{r!s!} d^r(f) d^s(g)$$

quels que soient les polynômes f et g dans $S_K^m(P)$.

2. Algèbres gamétiques

Soient K un anneau commutatif à élément unité, P un K-module unitaire et $d: P \to K$ une application K-linéaire surjective laquelle se prolonge en une K-dérivation de degré -1, notée encore d, de l'algèbre symétrique $S_K(P)$. On définit sur le K-module $S_K^m(P)$ une structure de K-algèbre commutative non associative, en posant

$$x * y = \binom{2m}{m}^{-1} \sum_{r+s=m} \frac{1}{r!s!} d^r(x) d^s(y)$$

quels que soient x et y dans $S_K^m(P)$, où l'on note $d^r = d \circ \cdots \circ d$, r fois. Notons que $d^r(x)d^s(y)$ désigne le produit dans l'algèbre symétrique $S_K(P)$ et que l'on suppose que K est un $\mathbb{Q}$-espace vectoriel. On note $S_K^m(P, d)$ cette algèbre.

Soit e dans P tel que $d(e) = 1$. Notons Ke le sous-K-module de P formé des K-multiples de e. On peut alors écrire $P = Ke \oplus \operatorname{Ker}(d)$, d'où l'isomorphisme de K-modules:

$$S_K^m(P) \approx \bigoplus_{i+j=m} S_K^i(Ke) \bigotimes_K S_K^j(\operatorname{Ker}(d)).$$

Ceci nous montre que pour tout élément x dans $S_K^m(P)$, il existe des éléments $x_0, x_1, \ldots, x_m$ dans $S_K(P)$, uniques, $x_i \in S_K^i(\operatorname{Ker}(d))$ $(i = 0, 1, \ldots, m)$ tels que $x = \sum_{i=0}^m x_i e^{m-i}$. On a alors

$$e^m * (x_{m-k} e^k) = \binom{2m}{m}^{-1} \sum_{r+s=m} \frac{1}{r!s!} \frac{m!}{r!} \frac{k!}{s!} x_{m-k} e^k$$

$$= \binom{2m}{m}^{-1} \sum_{r+s=m} \binom{m}{r} \binom{k}{s} x_{m-k} e^k$$

$$= \binom{2m}{m}^{-1} \binom{m+k}{m} x_{m-k} e^k \quad (k = 0, 1, \ldots, m).$$

Notons

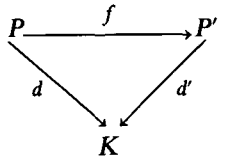
$$\rho_k=\binom{2m}{m}^{-1}\binom{2m-k}{m} \quad (k=0,1,\ldots,m).$$

Il s'agit d'une suite décroissante de nombres rationnels avec

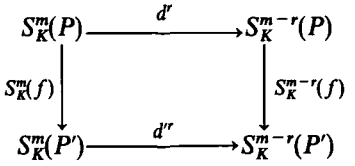
$$\rho_0=1, \rho_1=\tfrac{1}{2},\ldots,\rho_m=\binom{2m}{m}^{-1},\ldots;$$

ce sont les *t-racines* (train roots) de l'*algèbre gamétique* $S_K^m(P,d)$.

La construction ci-dessus d'une algèbre gamétique est fonctorielle. En effet, considérons la catégorie dont les *objets* sont les couples (P,d) où P est un K-module et $d:P\to K$ une application K-linéaire surjective. Un *morphisme* $f:(P,d)\to(P',d')$ est une application K-linéaire $f:P\to P'$ rendant commutatif le diagramme:



De plus, si (P,d) est un objet de la catégorie, l'application K-linéaire $d:P\to K$ se prolonge en une dérivation $d:S_K^m(P)\to S_K^{m-1}(P)$ de degré -1 donc, pour tout morphisme $f:(P,d)\to(P',d')$ et pour tout entier $r\geqq 1$, le diagramme suivant est commutatif



où $S_K^m(f):S_K^m(P)\to S_K^m(P')$ désigne l'extension de $f:P\to P'$ à l'algèbre symétrique. Il est clair que $S_K^m(f)$ est une application K-linéaire mais, en fait, il s'agit d'un morphisme d'algèbres pour les structures d'algèbres gamétiques. En effet, quels que soient x et y dans $S_K^m(P,d)$, on a

$$S_K^m(f)(x*y)=\binom{2m}{m}^{-1}\sum_{r+s=m}\frac{1}{r!s!}S_K^{m-r}(f)(d^r(x))S_K^{m-s}(f)(d^s(y))$$

$$=\binom{2m}{m}^{-1}\sum_{r+s=m}\frac{1}{r!s!}d'^r(S_K^m(f)(x))d'^s(S_K^m(f)(y))=S_K^m(f)(x)*S_K^m(f)(y).$$

Notons que si $f:(P,d)\to(P',d')$ est un morphisme surjectif, il en est de même du morphisme d'algèbres gamétiques $S_K^m(f):S_K^m(P,d)\to S_K^m(P',d')$ et le noyau de $S_K^m(f)$ est l'idéal de $S_K^m(P,d)$ engendré par le noyau de f où, plus précisément, $\mathrm{Ker}(S_K^m(f))=$

$\mathrm{Ker}(f)S_K(P) \cap S_K^m(P,d)$. Ceci découle des propriétés bien connues de l'algèbre symétrique (cf. [1], chapitre 3, section 6, nombre 2, proposition 4). Par contre, l'injectivité de $f:(P,d)\to(P',d')$, ou encore, le fait que l'application K-linéaire $f:P\to P'$ soit injective n'entraîne pas que le morphisme d'algèbres gamétiques $S_K^m(f):S_K^m(P,d)\to S_K^m(P',d')$ le soit aussi.

Exemple 2.1. Soit $f:P\to P'$ une application K-linéaire injective telle que l'application K-linéaire $S_K^m(f):S_K^m(P)\to S_K^m(P')$ ne soit pas injective. De tels exemples d'applications K-linéaires sont bien connus. Si $d:K\oplus P\to K$ et $d':K\oplus P'\to K$ désignent les projections sur le premier facteur, alors $\mathrm{id}+f:(K\oplus P,d)\to(K\oplus P',d')$ est un morphisme injectif mais le morphisme d'algèbres gamétiques $S_K^m(\mathrm{id}+f):S_K^m(K\oplus P,d)\to S_K^m(K\oplus P',d')$ n'est pas injectif, car $S_K^m(\mathrm{id}+f)=\sum_{i=0}^m S_K^i(f)$ (somme directe) contient une composante non injective qui est $S_K^m(f)$.

La construction de l'algèbre gamétique d'un module commute à l'extension de l'anneau des scalaires. En effet, soient K un anneau commutatif à élément unité, P un K-module, $d:P\to K$ une application K-linéaire surjective et $K\to K'$ un morphisme d'anneaux commutatifs à élément unité. L'application K'-linéaire $d':P\bigotimes_K K'\to K'$ définie par $x\otimes\lambda'\mapsto d(x)\lambda'$ est surjective car $d'(e\otimes 1')=1'$ où $1'$ est l'élément unité de K' et e est un élément de P vérifiant $d(e)=1$. Si l'on considère sur le K'-module $S_K^m(P,d)\bigotimes_K K'$ la structure d'algèbre définie par $(x\otimes\lambda')*(y\otimes\mu')=(x*y)\otimes(\lambda'\mu')$, quels que soient x et y dans $S_K^m(P,d)$ et quels que soient λ' et μ' dans K', alors $S_K^m(P,d)\bigotimes_K K'$ devient une algèbre gamétique via l'isomorphisme de K-algèbres $S_K^m(P,d)\bigotimes_K K'\approx S_{K'}^m(P\bigotimes_K K',d')$.

Cet isomorphisme nous montre, en particulier, que des résultats locaux sur les algèbres gamétiques peuvent être globalisés. En effet, pour tout idéal premier ou maximal $\mathscr{P}$ de K, il existe un isomorphisme de $K_{\mathscr{P}}$-algèbres gamétiques $S_K^m(P,d)_{\mathscr{P}}\approx S_{K_{\mathscr{P}}}^m(P_{\mathscr{P}},d_{\mathscr{P}})$ où $d_{\mathscr{P}}:P_{\mathscr{P}}\to K_{\mathscr{P}}$ est l'application $K_{\mathscr{P}}$-linéaire surjective définie par $(x/s)\mapsto(d(x)/s)$. Ainsi, les propriétés des algèbres gamétiques classiques, c'est-à-dire, d'algèbres gamétiques de modules libres peuvent être étendues au case d'algèbres gamétiques de modules projectifs.

D'autres propriétés fonctorielles comme, par exemple, le fait que le foncteur S_K^m commute aux limites inductives filtrantes, sont faciles à établir.

On remarque, finalement, que nous avons procédé, ci-dessus, à la construction de l'algèbre gamétique commutative, d'un module. Mais une construction analogue peut se faire dans le cas non commutatif, en remplaçant l'algèbre symétrique par l'algèbre tensorielle.

3. Détermination des idempotents

Soient K un anneau commutatif à élément unité, (P,d) un K-module et $S_K^m(P,d)$ ou, si aucune confusion n'est à craindre, $S_K^m(P)$ son algèbre gamétique. On voit facilement que pour tout élément e dans P tel que $d(e)=1$, e^m est un idempotent de l'algèbre gamétique $S_K^m(P)$, c'est-à-dire, $e^m * e^m = e^m$. Le théorème ci-dessous nous dit que, essentiellement, les idempotents de $S_K^m(P)$ sont tous de cette forme et, pour ce faire, nous supposerons que l'anneau de base soit *connexe*, i.e., ses seuls idempotents sont 0 et 1.

Théorème 3.1. *Soient K un anneau commutatif à élément unité et connexe, P un K-module et $m \geqq 0$ un nombre entier. L'ensemble des idempotents non nuls de la K-algèbre gamétique $S_K^m(P,d)$ coïncide avec l'ensemble des puissances m-ièmes dans l'algèbre symétrique $S_K(P)$ des éléments t dans P tels que $d(t)=1$.*

Dans un sens, c'est clair, car si t est dans P et si $d(t)=1$, alors $t^m * t^m = t^m$. Réciproquement, soient u dans $S_K(P)$ un idempotent de l'algèbre gamétique $S_K^m(P,d)$ et e dans P tel que $d(e)=1$. On peut alors écrire $u=\sum_{i=0}^{m} x_i e^{m-i}$ où les x_i sont des éléments de $S_K(P)$, uniques, vérifiant $x_i \in S_K^i(\mathrm{Ker}(d))$ $(i=0,1,\ldots,m)$. Puisque

$$e^i * e^j = \binom{2m}{m}^{-1} \binom{i+j}{m} e^{i+j-m} \quad (i,j=0,1,\ldots,m),$$

alors

$$u * u = \binom{2m}{m}^{-1} \sum_{i,j=0}^{m} \binom{i+j}{m} x_{m-i} x_{m-j} e^{i+j-m}$$

et la condition $u*u=u$ entraîne $x_0^2 = x_0$ donc $x_0=0$ ou $x_0=1$, car K est connexe.

Supposons, tout d'abord, que $x_0=0$ et que $u \neq 0$ et soit $k \neq 0$ le plus petit entier tel que $x_k \neq 0$. On a alors $u = x_k e^{m-k} + \cdots + x_m$ et

$$u * u = \binom{2m}{m}^{-1} \binom{2m-2k}{m} x_k^2 e^{m-2k} + \cdots,$$

c'est-à-dire, $u*u$ commence par un terme dont le degré en e est $m-2k$, soit strictement plus petit que $m-k$. Donc, on ne peut avoir $u*u=u$ que si $u=0$, ce qui est à exclure.

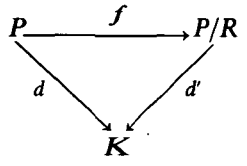
L'unique possibilité est alors que $x_0=1$ donc $u = e^m + x_1 e^{m-1} + \cdots + x_m$. Supposons que $x_1=0$ et que $u \neq e^m$ et soit $k \neq 0, 1$ le plus petit entier tel que $x_k \neq 0$, soit $u = e^m + x_k e^{m-k} + \cdots + x_m$. On a $u*u = e^m + 2\rho_k x_k e^{m-k} + \cdots$ et la condition $u*u=u$ entraîne $2\rho_k x_k = x_k$. Or, le K-module $S_K^k(\mathrm{Ker}(d))$ étant aussi muni d'une structure de $\mathbb{Q}$-espace vectoriel, la condition $(2\rho_k - 1)x_k = 0$ entraîne $\rho_k = \frac{1}{2}$ ou bien $x_k = 0$, l'un ou l'autre de ces cas étant impossibles. On se ramène ainsi au cas où $x_1 \neq 0$ et soit $e' = e + (1/m)x_1$. On a $e'^m = e^m + x_1 e^{m-1} + \cdots$, c'est-à-dire, $u \equiv e'^m (\mathrm{mod}\, e^{m-2})$, d'où $u = e'^m$.

Exemple 3.2. Soit P un K-module libre de rang $n+1$ et supposons que le prolongement de l'application K-linéaire surjective $d: P \to K$ à l'algèbre symétrique soit la dérivation $d = (\partial/\partial X_0): S_K^m(P) \to S_K^{m-1}(P)$. Alors, les idempotents non nuls de l'algèbre gamétique $S_K^m(P,d)$ sont les éléments de la forme $(X_0 + \sum_{k=1}^{n} a_k X_k)^m$ où les a_k sont dans K. Si le prolongement de l'application K-linéaire surjective $d: P \to K$ à l'algèbre symétrique est la dérivation $d = \sum_{i=0}^{n} (\partial/\partial X_i): S_K^m(P) \to S_K^{m-1}(P)$, alors les idempotents non nuls de l'algèbre gamétique $S_K^m(P,d)$ sont les éléments de $S_K^m(P)$ de la forme $(\sum_{k=0}^{n} a_k X_k)^m$, où les a_k sont dans l'anneau K et vérifient $\sum_{k=0}^{n} a_k = 1$.

4. Le groupe des automorphismes

Nous montrerons ici que le groupe des K-automorphismes de l'algèbre gamétique $S_K^m(P,d)$ est le groupe affine du K-module $\mathrm{Ker}(d)$.

En effet, soient K un anneau commutatif à élément unité, (P,d) un K-module et R un sous-K-module de P tel que $R \subset \mathrm{Ker}(d)$. Il existe alors une application K-linéaire surjective $\bar{d}: P/R \to K$, unique, faisant commuter le diagramme



où $f: P \to P/R$ est la surjection canonique. Si K est un $\mathbb{Q}$-espace vectoriel, on est déduit un morphisme surjectif d'algèbres gamétiques $S_K^m(f): S_K^m(P,d) \to S_K^m(P/R,\bar{d})$ et, de plus, $\mathrm{Ker}(S_K^m(f)) = RS_K(P) \cap S_K^m(P,d)$.

En particulier, si $R = \mathrm{Ker}(d)$, il existe un isomorphisme de K-modules $P/R \approx K$, donc de K-algèbres gamétiques $S_K^m(P/R,\bar{d}) \approx K$, où K est muni du produit habituel en tant que K-algèbre. L'isomorphisme de K-algèbres $S_K^m(P,d)/\mathrm{Ker}(S_K^m(f)) \approx K$ nous montre alors que $\mathrm{Ker}(S_K^m(f))$ est un idéal maximal de l'algèbre gamétique $S_K^m(P,d)$, *si K est un corps.* On a, en fait, le résultat suivant:

Théorème 4.1. *Soient K un corps commutatif de caractéristique zéro, P un K-espace vectoriel, $d: P \to K$ une application K-linéaire non nulle et $m \geqq 1$ un nombre entier. Alors l'algèbre gamétique $S_K^m(P,d)$ est une algèbre locale dont l'unique idéal maximal est $M = \mathrm{Ker}(d)S_K(P) \cap S_K^m(P,d)$.*

Montrons que $M = RS_K(P) \cap S_K^m(P,d)$, où $R = \mathrm{Ker}(d)$, est l'unique idéal maximal de l'algèbre $S_K^m(P,d)$ et, pour ce faire, il suffit de montrer que si x est un élément de $S_K^m(P,d)$, $x \notin M$, alors l'idéal I de $S_K^m(P,d)$ engendré par x est égal à $S_K^m(P,d)$.

Considérons un élément e dans P tel que $d(e) = 1$ et écrivons $x = x_0 e^m + x_1 e^{m-1} + \cdots + x_m$ où les x_i sont des éléments de $S_K(P)$, x_i $S_K^i(\mathrm{Ker}(d))$ $(i = 0, 1, \ldots, m)$. Comme $x \notin M$, alors $x_0 \neq 0$, donc on peut supposer que $x_0 = 1$ et montrons, tout d'abord, que l'élément e^m est dans l'idéal I. En effet, soit $k \neq 0$ le plus petit entier tel que $x_k \neq 0$ et écrivons $x = e^m + x_k e^{m-k} + \cdots + x_m$, donc $x * (e^m - x_k e^{m-k}) = e^m + x'_{k+1} e^{m-k-1} + \cdots$ est dans l'idéal I. Par une suite de multiplications, on peut supprimer tous les termes non nuls qui suivent e^m dans l'expression de x et ceci nous montre que $e^m \in I$. Si, maintenant, $u = \sum_{k=0}^m y_k e^{m-k}$ est un élément quelconque de l'algèbre $S_K^m(P,d)$, l'élément $e^m * \sum_{k=0}^m (y_k/\rho_k) e^{m-k} = u$ est dans I, d'où, $I = S_K^m(P,d)$. Ceci nous dit que M est l'unique idéal maximal de l'algèbre $S_K^m(P,d)$.

Corollaire 4.2. *Pour tout automorphisme σ de l'algèbre $S_K^m(P,d)$, on a $\sigma(M^k) = M^k$ pour tout entier $k \geqq 1$.*

Comme σ est un automorphisme de $S_K^m(P,d)$, l'image par σ de l'idéal maximal M de

$S_K^m(P,d)$ est encore un idéal maximal de $S_K^m(P,d)$, donc $\sigma(M)=M$. On déduit aussi que $\sigma(M^2)\subset M^2$ et comme $\sigma^{-1}(M^2)\subset M^2$, alors $\sigma(M^2)=M^2$. Le corollaire s'ensuit.

Note 4.3. *L'algèbre des nombres presque duaux.* Soit K un anneau commutatif à élément unité, $S_K^m(P,d)$ l'algèbre gamétique du K-module (P,d) et soit e un élément de P tel que $d(e)=1$. Tout élément de $S_K^m(P,d)$ s'écrit sous la forme $\sum_{i=0}^m x_i e^{m-i}$ avec x_i dans $S_K^i(\mathrm{Ker}(d))$ $(i=0,1,\ldots,m)$. Si $M=\mathrm{Ker}(d)S_K(P)\cap S_K^m(P,d)$ est l'idéal de l'algèbre $S_K^m(P,d)$ engendré par le K-module $\mathrm{Ker}(d)$, les éléments $x_i e^{m-i}$ sont dans M^2 pour $i\geqq 2$ d'où un isomorphisme de K-algèbres $S_K^m(P,d)/M^2\simeq K\oplus\mathrm{Ker}(d)$ donné par $\bar{x}\mapsto(x_0,x_1)$ si $x=\sum_{i=0}^m x_i e^{m-i}$. La structure de K-algèbre de $K\oplus\mathrm{Ker}(d)$ est donnée par $(\lambda,x)(\mu,y)=(\lambda\mu,\frac{1}{2}(\lambda y+\mu x))$, quels que soient λ et μ dans K et x et y dans $\mathrm{Ker}(d)$, à condition de supposer que K soit un $\mathbb{Q}$-espace vectoriel. On dira que $S_K^m(P,d)/M^2$ est *l'algèbre des nombres presque duaux*. (cf. Note 4.6).

Voyons maintenant comment on calcule les automorphismes de l'algèbre des nombres presque duaux $A=K\oplus\mathrm{Ker}(d)$. Or, on sait que les idempotents de A sont les éléments de la forme $(1,x)$ avec x dans $\mathrm{Ker}(d)$ plus l'idempotent trivial $(0,0)$ et l'image d'un idempotent de A par un automorphisme est encore un idempotent de A. Ainsi, pour tout élément (λ,x) de A, on a $(\lambda,x)=\lambda(1,0)+(0,x)$ donc pour tout automorphisme σ de A, $\sigma(\lambda,x)=\lambda\sigma(1,0)+\sigma(0,x)=\lambda(1,x_\sigma)+(0,u(x))=(\lambda,\lambda x_\sigma+u(x))$, où $\sigma(1,0)=(1,x_\sigma)$ avec x_σ dans $\mathrm{Ker}(d)$ et où u est la restriction de σ à $\mathrm{Ker}(d)$. L'application $\mathrm{Aut}(K\oplus\mathrm{Ker}(d))\to\mathrm{Aff}(\mathrm{Ker}(d))$ définie par $\sigma\mapsto(x_\sigma,u)$ est un isomorphisme du groupe des automorphismes de A sur le groupe affine de $\mathrm{Ker}(d)$. En effet, il suffit de voir que $\sigma'\sigma\mapsto(x_{\sigma'}+u'(x_\sigma),u'u)=(x_{\sigma'},u')(x_\sigma,u)$, i.e., que la flèche ci-dessus définie est un morphisme pour les structures de groupes de $\mathrm{Aut}(A)$ et du groupe affine de $\mathrm{Ker}(d)$. Cela nous permet de déterminer les automorphismes de l'algèbre gamétique $S_K^m(P,d)$. En effet, on a le résultat suivant:

Théorème 4.4. *Soient K un corps commutatif de caractéristique zéro, P un K-espace vectoriel, $d:P\to K$ une application K-linéaire non nulle et $m\geqq 1$ un nombre entier. Le groupe des K-automorphismes de l'algèbre gamétique $S_K^m(P,d)$ est alors isomorphe au groupe affine du K-espace vectoriel* $\mathrm{Ker}(d)$.

En effet, le Théorème 4.1 nous dit que tout automorphisme σ de $S_K^m(P,d)$ donne, par passage aux quotients, un automorphisme $\bar{\sigma}$ de l'algèbre $S_K^m(P,d)/M^2$. On a donc un morphisme surjectif de groupes $\mathrm{Aut}(S_K^m(P,d))\to\mathrm{Aff}(\mathrm{Ker}(d))$ défini par $\sigma\mapsto\bar{\sigma}$ et il suffira de démontrer que ce morphisme est injectif. Montrons, pour cela, que si $\sigma\in\mathrm{Aut}(S_K^m(P,d))$ et si $\bar{\sigma}$ $(=\sigma$ modulo $M^2)$ est l'identité dans l'algèbre des nombres presque duaux $S_K^m(P,d)/M^2$, alors $\sigma=\mathrm{id}$. Or, pour tout idempotent e^m de l'algèbre gamétique $S_K^m(P,d)$, $\sigma(e^m)=e'^m$ est un idempotent de $S_K^m(P,d)$ donc, d'après l'hypothèse, $e'^m=e^m(\mathrm{mod}\,M^2)$. Si l'on écrit $e=e+x$ avec x dans $\mathrm{Ker}(d)$, on a $e'^m-e^m\equiv mxe^{m-1}(\mathrm{mod}\,M^2)$ d'où $x=0$, c'est-à-dire, $e'^m=e^m$. Ainsi, σ laisse fixe tout idempotent de l'algèbre gamétique $S_K^m(P,d)$ et comme celle-ci est additivement engendrée par ses idempotents, alors $\sigma=\mathrm{id}$.

Corollaire 4.5. *Soient K un anneau commutatif à élément unité, P un K-module, $d:P\to K$ une application K-linéaire surjective et $m\geqq 1$ un nombre entier. Si K est un $\mathbb{Q}$-espace vectoriel et si K est un anneau régulier au sens de Von Neumann, alors le groupe des K-automorphismes de l'algèbre gamétique $S_K^m(P,d)$ est isomorphe au groupe affine du K-module* Ker(d).

Note 4.6. L'algèbre des nombres duaux (cf. [1], page AIII.15) sur un anneau K commutatif à élément unité se définit en posant $(\lambda,\mu)(\lambda',\mu')=(\lambda\lambda',\lambda\mu'+\lambda'\mu)$, quels que soient λ, μ, λ', μ' dans K. On a ainsi sur $K\times K$ une structure de K-algèbre commutative et associative à élément unité, appelée *algèbre des nombres duaux* ou *algèbre quadratique de type* $(0,0)$. Plus généralement, si K est un anneau commutatif à élément unité et M un K-module, l'algèbre des nombres duaux $K\oplus M$ est définie en posant $(\lambda,x)(\mu,y)=(\lambda\mu,\lambda y+\mu x)$ pour λ, μ dans K et x, y dans M. Le K-module M devient ainsi un idéal de la K-algèbre commutative et associative $K\oplus M$ à élément unité tel que $M^2=0$. De plus, il existe un isomorphisme de K-algèbres $K\oplus M/M\approx K$. Ces considérations nous ont conduit à définir la notion d'algèbre des nombres presque duaux, cette algèbre étant commutative mais non associative et n'ayant pas non plus d'élément unité. On vérifie facilement que *l'algèbre des nombres presque duaux est une algèbre de Jordan commutative.*

5. Dérivations

Soient K un anneau commutatif à élément unité, (P,d) un K-module, $m\geqq 1$ un nombres entier, $u:P\to P$ une application K-linéaire telle que $du=0$ et $\delta_u:S_K(P)\to S_K(P)$ la K-dérivation de degré zéro de l'algèbre symétrique $S_K(P)$ qui prolonge u. On supposera, de plus, que K soit un $\mathbb{Q}$-espace vectoriel.

Lemme 5.1. *Pour toute application K-linéaire $u:P\to P$ telle que $du=0$, δ_u est une K-dérivation de l'algèbre gamétique $S_K^m(P,d)$.*

On observe, tout d'abord, que la condition $du=0$ signifie que les dérivations δ_u et d de l'algèbre symétrique $S_K(P)$ commutent, donc δ_u et d^r commutent pour tout entier $r\geqq 1$. On a alors, quels que soient les éléments x et y dans l'algèbre gamétique $S_K^m(P,d)$,

$$\delta_u(x*y)=\binom{2m}{m}^{-1}\sum_{r+s=m}\frac{1}{r!s!}\delta_u(d^r(x)d^s(y))$$

$$=\binom{2m}{m}^{-1}\sum_{r+s=m}\frac{1}{r!s!}(\delta_u(d^r(x))d^s(y)+d^r(x)\delta_u(d^s(y)))$$

$$=\binom{2m}{m}^{-1}\sum_{r+s=m}\frac{1}{r!s!}d^r(\delta_u(x))d^s(y)+\binom{2m}{m}^{-1}\sum_{r+s=m}\frac{1}{r!s!}d^r(x)d^s(\delta_u(y))$$

$$=\delta_u(x)*y+x*\delta_u(y).$$

Lemme 5.2. *Soient K un anneau commutatif à élément unité, (P,d) un K-module et $m\geqq 1$ un nombre entier. Pour toute K-dérivation δ de l'algèbre gamétique $S_K^m(P,d)$, l'image de δ est contenue dans l'idéal $M=\mathrm{Ker}(d)S_K(P)\cap S_K^m(P,d)$.*

Comme l'algèbre gamétique $S_K^m(P,d)$ est K-linéairement engendrée par ses idempotents, il suffit de démontrer le résultat pour un idempotent e^m de $S_K^m(P,d)$. De la relation $e^m * e^m = e^m$ on a $\delta(e^m)*e^m=\frac{1}{2}\delta(e^m)$ et si l'on écrit $\delta(e^m)=\sum_{i=0}^m x_i e^{m-i}$ avec $x_i\in S_K^i(\mathrm{Ker}(d))$ $(i=0,1,\ldots,m)$, alors $\delta(e^m)*e^m=\sum_{i=0}^m \rho_i x_i e^{m-i}$ donc $\rho_i x_i=\rho_1 x_i$ $(i=0,1,\ldots,m)$, où $\rho_1=\frac{1}{2}$. Ceci nous dit que $x_i=0$ pour $i\neq 1$ donc $\delta(e^m)=x_1 e^{m-1}$. Le lemme est démontré.

On en déduit que si $t\in M^2$, alors $\delta(t)\in M^2$ pour toute dérivation δ de l'algèbre gamétique $S_K^m(P,d)$. En effet, si $t=\sum_i x_i * y_i$ (somme finie) où les x_i et les y_i sont dans M, alors $\delta(t)=\sum_i(\delta(x_i)*y_i+x_i*\delta(y_i))\in M^2$, i.e., $\delta(M^2)\subset M^2$. Plus généralement, pour toute dérivation δ de $S_K^m(P,d)$ et pour tout entier $k\geqq 1$, $\delta(M^k)\subset M^k$. Par passage aux quotients, δ induit une dérivation de l'algèbre des nombres presque duaux $S_K^m(P,d)/M^2$ donc un morphisme d'algèbres de Lie $\Delta:\mathrm{Der}_K(S_K^m(P,d))\to\mathrm{Der}_K(S_K^m(P,d)/M^2)$. On a:

Proposition 5.3. *Soient K un anneau commutatif à élément unité, (P,d) un K-module et $m\geqq 1$ un nombre entier. L'algèbre de Lie des K-dérivations de la K-algèbre $S_K^m(P,d)/M^2$ est isomorphe à l'algèbre de Lie du groupe affine du K-module* $\mathrm{Ker}(d)$.

Soit $A=K\oplus\mathrm{Ker}(d)$ l'algèbre des nombres presque duaux et $\delta:A\to A$ une K-dérivation de A. Pour tout élément (λ,x) de A, on a $\delta(\lambda,x)=\lambda\delta(1,0)+\delta(0,x)$ et si l'on écrit $\delta(1,0)=(\mu,x_\delta)$, la condition $(1,0)^2=(1,0)$ nous donne $2(1,0)\delta(1,0)=\delta(1,0)$ d'où $\mu=0$. Si u désigne la restriction de δ à $\mathrm{Ker}(d)$, alors u est un endomorphisme de $\mathrm{Ker}(d)$ et δ s'écrit $\delta(\lambda,x)=(0,\lambda x_\delta+u(x))$ pour tout (λ,x) dans A où x_δ est un vecteur de $\mathrm{Ker}(d)$ qui dépend de δ. L'application $\mathrm{Der}_K(A)\to\mathrm{Ker}(d)\times_{\mathrm{s.d.}}\mathrm{gl}(\mathrm{Ker}(d))$ définie par $\delta\mapsto(x_\delta,u)$ est alors un morphisme d'algèbres de Lie car $[\delta,\delta']\mapsto(u(x_{\delta'})-u'(x_\delta),[u,u'])=[(x_\delta,u),(x_{\delta'},u')]$. Ce morphisme est, de toute évidence, injectif et étant donnés y dans $\mathrm{Ker}(d)$ et v un endomorphisme de $\mathrm{Ker}(d)$, alors l'application $A\to A$ définie par $(\lambda,y)\mapsto(0,\lambda y+v(x))$ est une dérivation de A. On a ainsi montré que l'application $\mathrm{Der}_K(A)\to\mathrm{Ker}(d)\times_{\mathrm{s.d.}}\mathrm{gl}(\mathrm{Ker}(d))$ est un isomorphisme d'algèbres de Lie.

Lemme 5.4. *Le morphisme $\Delta:\mathrm{Der}_K(S_K^m(P,d))\to\mathrm{Der}_K(S_K^m(P,d)/M^2)$ est un isomorphisme d'algèbres de Lie.*

Ce morphisme est surjectif car si u est une K-dérivation de l'algèbre des nombres presque duaux, δ_u est une K-dérivation de l'algèbre gamétique $S_K^m(P,d)$ et $\Delta(\delta_u)=u$. Montrons que Δ est injectif, c'est-à-dire, si δ est une K-dérivation de l'algèbre gamétique $S_K^m(P,d)$ et si $\delta(S_K^m(P,d))\subset M^2$, alors $\delta=0$. Or, pour tout idempotent e^m de $S_K^m(P,d)$, il existe un élément z dans $\mathrm{Ker}(d)$ tel que $\delta(e^m)=ze^{m-1}$ et $\delta(e^m)$ appartient à M^2 si et seulement si $z=0$. Comme l'algèbre gamétique $S_K^m(P,d)$ est linéairement engendrée par ses idempotents, nécessairement on a $\delta=0$.

Théorème 5.5. *L'application $u\mapsto\delta_u$ définie dans l'algèbre de Lie des opérateurs linéaires de P dans P tels que $du=0$ est un isomorphisme de l'algèbre de Lie du groupe affine de* $\mathrm{Ker}(d)$ *sur l'algèbre de Lie des K-dérivations de la K-algèbre gamétique $S_K^m(P,d)$.*

En effet, on remarque que l'ensemble des endomorphismes u de P tels que $du=0$ forment une sous-algèbre de Lie de l'algèbre de Lie $\mathrm{gl}(P)$ du groupe linéaire de P. De plus, cette sous-algèbre est naturellement isomorphe à l'algèbre de Lie $\mathrm{aff}(\mathrm{Ker}(d))=\mathrm{Ker}(d)\times_{\mathrm{s.d.}}\mathrm{gl}(\mathrm{Ker}(d))$ du groupe affine de $\mathrm{Ker}(d)$. En effet, si l'on fixe une décomposition $P=Ke\oplus\mathrm{Ker}(d)$ de P avec $d(e)=1$, il suffit de considérer l'application $u\mapsto(u(e),u|_{\mathrm{Ker}(d)})$. Elle nous fournit l'isomorphisme ci-dessus mentionné. Par ailleurs, la formule $\delta_{uv-vu}=\delta_u\delta_v-\delta_v\delta_u$ étant vraie dans l'algèbre symétrique $S_K(P)$, car elle l'est en degré 1 (et ceci, quels que soient les endomorphismes u et v de P tels que $du=0$ et $dv=0$), alors l'application composée $u\mapsto\delta_u\mapsto\bar{\delta}_u$, où la barre désigne le passage au quotient par l'idéal M^2, est un isomorphisme de K-algèbres de Lie. Le théorème en résulte aussitôt.

Note 5.6. L'algèbre de Lie du groupe affine du K-module $\mathrm{Ker}(d)$ n'est, en général, ni résoluble ni semi-simple. Si P est projectif de type fini et de rang 1, $\mathrm{Ker}(d)=0$ et cette algèbre est réduite à zéro. Si P est projectif de type fini et de rang 2, $\mathrm{Ker}(d)$ est projectif de rang 1 et l'algèbre de Lie du groupe affine de $\mathrm{Ker}(d)$ est résoluble. Si P est projectif de type fini et de rang $\geqq 3$, $\mathrm{Ker}(d)$ est projectif de rang $\geqq 2$ et, dans ce cas, l'algèbre de Lie dérivée de l'algèbre de Lie du groupe affine de $\mathrm{Ker}(d)$ est l'algèbre $\mathrm{Ker}(d)\times_{\mathrm{s.d.}}\mathrm{sl}(\mathrm{Ker}(d))$ (décomposition de Levi), où $\mathrm{sl}(\mathrm{Ker}(d))$ est l'algèbre des endomorphismes de trace nulle de $\mathrm{Ker}(d)$. Si la caractéristique de K vaut 2 et si le rang de P est trois, cette algèbre de Lie est nilpotente et l'algèbre de Lie du groupe affine de $\mathrm{Ker}(d)$ est alors résoluble. Pour voir que l'algèbre dérivée de l'algèbre de Lie $\mathrm{aff}(\mathrm{Ker}(d))=\mathrm{Ker}(d)\times_{\mathrm{s.d.}}\mathrm{gl}(\mathrm{Ker}(d))$ n'est jamais nilpotente si $\mathrm{Ker}(d)\neq 0$, on procède comme suit. On considère le couple $e=(0,\mathrm{id}_{\mathrm{Ker}(d)})$ et, pour tout x dans $\mathrm{Ker}(d)$, on a $[e,(x,0)]=(x,0)$, donc ad_e n'est jamais nilpotent. Il suffit d'appliquer ici le théorème d'Engel.

Note 5.7. *L'algèbre gamétique* $S_K^1(P,d)$. L'algèbre quotient $S_K^m(P,d)/M^2$ n'est autre, à isomorphisme près, que l'algèbre gamétique $S_K^1(P,d)$ munie du produit $*$. En effet, quels que soient les éléments x et y dans $S_K^1(P,d)=P$, on a $x*y=\frac{1}{2}(d(y)x+d(x)y)$ et soit e dans P tel que $d(e)=1$. L'application K-linéaire $P\to K\oplus\mathrm{Ker}(d)$ définie par $x\mapsto(d(x),x-d(x)e)$ est alors un isomorphisme de K-modules et, par transport de structure, le produit $*$ donne, sur le K-module $K\oplus\mathrm{Ker}(d)$, la structure d'algèbre des nombres presque duaux (cf. Note 4.3).

Note 5.8. *La pondération.* Comme les idempotents de l'algèbre gamétique $S_K^m(P,d)$ engendrent $S_K^m(P,d)$ en tant que K-module, l'unique pondération possible de $S_K^m(P,d)$ est l'application K-linéaire $\omega: S_K^m(P,d)\to K$ définie par $\omega=(1/m!)d^m$. Pour tout idempotent e^m de $S_K^m(P,d)$ on a $\omega(e^m)=1$ et on vérifie immédiatement que $\omega(x*y)=\omega(x)\omega(y)$, quels que soient x et y dans $S_K^m(P,d)$. On a alors $\mathrm{Ker}(\omega)=M$ et le Lemme 5.2 nous dit que pour toute dérivation δ de $S_K^m(P,d)$ on a $\omega\delta=0$. La réciproque est, en général, fausse car $\mathrm{Ker}(\omega)$ est bien trop grand, comparé à $\mathrm{Ker}(d)$. Elle n'est, en faite, vraie que si $m=1$ et, dans ce cas, $\omega=d$ et une application K-linéaire $u: P\to P$ est une K-dérivation de l'algèbre gamétique $S_K^1(P,d)=P$ si et seulement si $du=0$ (cf. [4], Lemme 2.1).

Note 5.9. *L'algèbre gamétique d'une population ayant une infinité de formes alleliques.* La construction donnée ci-dessus de l'algèbre gamétique d'un K-module (P,d) ne fait

intervenir aucune hypothèse sur la finitude du K-module P. Si $K=\mathbb{R}$ et si P est un $\mathbb{R}$-espace vectoriel de dimension finie, cet entier désigne le nombre d'allèles intervenant dans la population. Mais il est clair que dans la construction de l'algèbre gamétique $S_K^m(P,d)$, le nombre de formes allèliques n'intervient pas. Ceci répond à une question qui nous a été posée récemment par Philip Holgate concernant la construction d'algèbres gamétiques d'une population à une infinité d'allèles.

Note 5.10. Nous rappelons ici que l'utilisation de dérivations pour exprimer la multiplication gamétique a été faite pour la première fois par 0. Reiersøl dans son article de 1962 (cf. [5]).

Nous remercions très vivement le Referee dont les remarques nous ont permis d'améliorer la rédaction.

BIBLIOGRAPHIE

1. N. Bourbaki, *Algèbre* I, *chapitres* 1 à 3 (Hermann, Paris, 1970).

2. H. Gonshor, Special train algebra arising in genetics II, *Proc. Edinburgh Math. Soc.* (2) **14** (1965), 333–338.

3. P. Holgate, Genetic algebras arising in polyploidy, *Proc. Edinburgh Math. Soc.* (2) **15** (1966), 1–9.

4. A. Micali, T. M. M. Campos, M. C. Costa e Silva et S. M. M. Ferreira, *Dérivations dans les algèbres gamétiques* II, *Linear Algebra and its applications* **64** (1985), 175–181.

5. O. Reiersøl, Genetic algebras studied recursively and by means of differential operators, *Math. Scand.* **10** (1962), 25–44.

Institut de Mathématiques
Université de Montpellier II
Place Eugène Bataillon
34060 Montpellier, France