Jean Fresnel, 12/03/2018

Prolongement d'une colonne unimodulaire en une matrice inversible

Soient A un anneau commutatif, $M \in G\ell_n(A)$, i.e. il existe $N \in M_n(A)$ avec $MN = I_n$. Il suit de cela que $\text{dét} M \in A^\times$, i.e. $\text{dét} M$ est un inversible de A . Si $x := {}^t(x_1, x_2, \dots, x_n)$ est la première colonne de M , il suit de cela que $A = x_1 A + x_2 A + \dots + x_n A$. En effet, si ce n'était pas le cas, il existerait un idéal maximal $\mathfrak{M}$ de A avec $x_1 A + x_2 A + \dots + x_n A \subset \mathfrak{M}$, alors en calculant $\text{dét} A$ selon le développement avec la première colonne, on aurait $\text{dét} A \in \mathfrak{M}$, ce qui contredit le fait que $\text{dét} M \in A^\times$.
Une colonne $x := {}^t(x_1, x_2, \dots, x_n)$ de A^n telle que $A = x_1 A + x_2 A + \dots + x_n A$ est appelée *unimodulaire*.

La question est donc de savoir si réciproquement, une colonne unimodulaire peut être la première colonne d'une matrice inversible.

La réponse est toujours positive si $n = 2$, en effet si $u x_1 + v x_2 = 1$, alors $\text{dét}\begin{bmatrix} x_1 & u \\ x_2 & -v \end{bmatrix} = 1$.

La réponse est aussi toujours positive si A est un anneau principal.

On a un contre-exemple pour $n = 3$, en considérant l'anneau $A := \dfrac{\mathbb{R}[X, Y, Z]}{(X^2 + Y^2 + Z^2 - 1)\mathbb{R}[X, Y, Z]} = \mathbb{R}[x, y, z]$ et la colonne ${}^t(x, y, z)$. Le résultat repose essentiellement sur le théorème de la boule chevelue qui dit qu'un champ de vecteurs tangent à la sphère réelle de dimension 2 s'annule en au moins un point. Cet exemple a été mis en évidence en 1961 par [**Sa**], proposition 10, p. 169 et en 1962 par [**Sw**], theorem 3, p. 270.

En revanche si K est un corps commutatif avec $\mathrm{car} K \neq 2$ et si $A := \dfrac{K[X, Y, Z]}{(P(X, Y, Z) - 1)K[X, Y, Z]} = K[x, y, z]$ où $P(X, Y, Z)$ est un polynôme homogène de degré 2 qui admet un zéro non trivial dans K^3, alors la colonne ${}^t(x, y, z)$ peut être complétée en un élément de $G\ell_3(A)$ ([**Sa**], proposition 10, p. 169, [**To**]1979) .

Enfin, la réponse est aussi toujours positive si $A = K[X_1, X_2, \dots, X_n]$ lorsque K est un corps commutatif, c'est un résultat de Quillen et Suslin, 1976 ([**La**] p. 848)

I. Le cas d'un anneau principal

Proposition *Soient* A *un anneau principal,* $n \geq 2$, $x := {}^t(x_1, x_2, \ldots, x_n)$ *avec* $x_k \in A$ *pour* $1 \leq k \leq n$ et $A = x_1 A + x_2 A + \ldots + x_n A$. *Alors il existe* $M \in S\ell_n(A)$ *tel que* x *soit la première colonne de* M *; ce qui veut aussi dire que* $x = M\varepsilon_1$ *où* $\varepsilon_1 := {}^t(1, 0, \ldots, 0)$ *; ce qui veut aussi dire qu'il existe* $N \in S\ell_n(A)$ *tel que* $Nx = \varepsilon_1$.

Démonstration
La démonstration sera par récurrence sur n .

1) Le cas $n = 2$ (on remarquera que dans ce cas, on n'utilise pas le fait que A est principal).
De la relation $A = x_1 A + x_2 A$, il suit qu'il existe $u, v \in A$ avec $u x_1 + v x_2 = 1$.
Soit $N := \begin{bmatrix} u & v \\ -x_2 & x_1 \end{bmatrix}$, on a $\text{dét} N = 1$ et $N \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$; il suit donc que la proposition est satisfaite.

2) On suppose que $n \geq 3$ et que la proposition est satisfaite pour $n-1$.
Comme A est principal, il existe $d \in A$ avec $dA = x_2 A + x_3 A + \ldots + x_n A$, il suit alors de la relation $A = x_1 A + x_2 A + \ldots + x_n A$ que $A = x_1 A + dA$.
Comme $x_i \in dA$, il existe $y_i \in A$ avec $x_i = d y_i$ pour $i \geq 2$. On a donc $A = y_2 A + y_3 A + \ldots + y_n A$, il suit de l'hypothèse de récurrence qu'il existe $P \in S\ell_{n-1}(A)$ avec $Py = e_1$ où $y := {}^t(y_2, y_3, \ldots, y_n)$ et $e_1 := {}^t(1, 0, \ldots, 0)$ et $(1, 0, \ldots, 0) \in A^{n-1}$. Il suit de cela que

$$Pz = d e_1 \text{ , si } z := {}^t(x_2, x_3, \ldots, x_n) .$$

Soit B la matrice qui est le tableau diagonal (I_1, P) , alors on a

$$B\,{}^t(x_1, x_2, \ldots, x_n) = {}^t(x_1, d, 0, \ldots, 0) \text{ avec } \text{dét}(B) = 1 .$$

De la relation $A = x_1 A + dA$, il suit qu'il existe $\alpha, \beta \in A$ avec $\alpha x_1 + \beta d = 1$.
Soit $T := \begin{bmatrix} \alpha & \beta \\ -x_1 & d \end{bmatrix}$, on a $\text{dét} T = 1$ et $T \begin{bmatrix} x_1 \\ d \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$. Soit la matrice C qui est le tableau diagonal (T, I_{n-2}) , on a donc

$$CB\,{}^t(x_1, x_2, \ldots, x_n) = \varepsilon_1 \text{ avec } \text{dét}(CB) = 1 ;$$

ce qui montre la proposition.

Description du procédé algorithmique
Comme A est principal, il existe $d_{n-1} \in A$ avec $d_{n-1} A = x_{n-1} A + x_n A$. On a donc $x_{n-1} = d_{n-1} y_{n-1}$, $x_n = d_{n-1} y_n$; il existe donc $\alpha, \beta \in A$ avec $\alpha y_n + \beta y_{n-1} = 1$. Soit $T := \begin{bmatrix} \beta & \alpha \\ -y_n & y_{n-1} \end{bmatrix}$, on a $\text{dét} T = 1$ et

$T\begin{bmatrix} y_{n-1} \\ y_n \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$ et donc $T\begin{bmatrix} x_{n-1} \\ x_n \end{bmatrix} = \begin{bmatrix} d_{n-1} \\ 0 \end{bmatrix}$. Si donc N_{n-1} est la matrice qui est le tableau diagonal (I_{n-2}, T) , on a

$$N_{n-1}{}^t(x_1, x_2, \dots, x_n) = {}^t(x_1, x_2, \dots, x_{n-2}, d_{n-1}, 0) .$$

Comme A est principal, il existe $d_{n-2} \in A$ avec $d_{n-2}A = x_{n-2}A + d_{n-1}A$, i.e. $d_{n-2}A = x_{n-2}A + x_{n-1}A + x_nA$. Alors en utilisant la méthode précédente, alors il existe $R \in S\ell_2(A)$ tel que

$$R\begin{bmatrix} x_{n-2} \\ d_{n-1} \end{bmatrix} = \begin{bmatrix} d_{n-2} \\ 0 \end{bmatrix}.$$

Si donc N_{n-2} est la matrice qui est le tableau diagonal (I_{n-3}, R, I_1) , on a $\text{dét}(N_{n-2}) = 1$ et

$$N_{n-2}N_{n-1}{}^t(x_1, x_2, \dots, x_n) = {}^t(x_1, x_2, \dots, x_{n-3}, d_{n-2}, 0, 0) .$$

On continue le processus en choisissant $d_k \in A$ tel que $d_kA = x_kA + x_{k+1}A + \dots + x_nA$ pour $k \geq 2$ et $d_1 = 1$. Il suit alors que

$$N_1N_2 \dots N_{n-2}N_{n-1}{}^t(x_1, x_2, \dots, x_n) = {}^t(1, 0, \dots, 0, 0) .$$

Cela montre aussi que la matrice $M := (N_1N_2 \dots N_{n-2}N_{n-1})^{-1}$ est un élément de $G\ell_n(A)$ dont la première colonne est ${}^t(x_1, x_2, \dots, x_n)$.

II. Un contre-exemple avec $n=3$

Proposition *Soient* $A := \dfrac{\mathbb{R}[X,Y,Z]}{(X^2+Y^2+Z^2-1)\mathbb{R}[X,Y,Z]}$ *et* $\rho : \mathbb{R}[X,Y,Z] \to A$ *la surjection canonique avec* $x := \rho(X)$, $y := \rho(Y)$, $z := \rho(Z)$. *On a donc* $x^2+y^2+z^2=1$ *, ce qui implique que le vecteur* (x,y,z) *de* A^3 *est unimodulaire. Alors, il n'existe pas de matrice* $N \in G\ell_3(A)$ *dont* ${}^t(x,y,z)$ *est la première colonne.*

Démonstration

1) *Soit* $M := \{(a,b,c) \in A^3 \mid xa+yb+zc=0\}$. *Alors on a*

$$A^3 = A(x,y,z) \oplus M .$$

Montrons que $A^3 = A(x,y,z) + M$. Soit $(a,b,c) \in A^3$ et $\alpha := xa+yb+zc$. on a donc $(a,b,c) = \alpha(x,y,z) + (a-\alpha x, b-\alpha y, z-\alpha z)$; sachant que $x^2+y^2+z^2=1$, on a bien $(a-\alpha x, b-\alpha y, z-\alpha z) \in M$. Cela montre que bien que $A^3 = A(x,y,z) + M$.

Montrons que la somme est directe. Si $\beta(x,y,z) = (a,b,c)$ avec $xa+yb+zc=0$, il suit que $\beta(x^2+y^2+z^2)=0$ et comme $x^2+y^2+z^2=1$, on a bien $\beta=0$. Ainsi la somme est directe.

On suppose désormais que la proposition est fausse.

2) Cela veut dire qu'il existe $(P_2, Q_2, R_2) \in A^3$, $(P_3, Q_3, R_3) \in A^3$, de façon que $\begin{bmatrix} x & P_2 & P_3 \\ y & Q_2 & Q_3 \\ z & R_2 & R_3 \end{bmatrix} \in G\ell_3(A)$. Cela veut dire que si

$$e := (x, y, z) \ , \ e' := (P_2, Q_2, R_2) \ , \ e'' := (P_3, Q_3, R_3) \ ,$$

alors (e, e', e'') est une base du A-module A^3 .
On a donc par 1) , $\dfrac{A^3}{Ae} \simeq M$ et par ci-dessus $\dfrac{A^3}{Ae} \simeq Ae' \oplus Ae''$, i.e. $M \simeq Ae' \oplus Ae''$. En conclusion M admet une base (f, g) avec $f = (U_2, V_2, W_2)$, $g = (U_3, V_3, W_3)$.

3) Soit $p := (\alpha, \beta, \gamma) \in \mathbb{R}^3$ tel que $\alpha^2 + \beta^2 + \gamma^2 = 1$, alors l'application $P(X, Y, Z) \mapsto P(\alpha, \beta, \gamma)$ induit un homomorphisme $\rho_p : A^3 \to \mathbb{R}$ tel que $\rho_p(\rho(P(X, Y, Z)) = P(\alpha, \beta, \gamma)$.
Soient $p = (\alpha, \beta, \gamma) \in \mathbb{R}^3$ tel que $\alpha^2 + \beta^2 + \gamma^2 = 1$, $u_p : A^3 \to \mathbb{R}^3$ défini par $u_p(a, b, c) := (\rho_p(a), \rho_p(b), \rho_p(c))$.
Montrons que $(u_p(e), u_p(f), u_p(g))$ est une base du $\mathbb{R}$-espace vectoriel $\mathbb{R}^3$. Il suffit de montrer que $(u_p(e), u_p(f), u_p(g))$ engendre $\mathbb{R}^3$. En effet, il existe $r, s, t \in A$ avec

$$(1, 0, 0) = re + sf + tg \ .$$

Alors

$$(1, 0, 0) = u_p(1, 0, 0) = \rho_p(r)\, u_p(e) + \rho_p(s)\, u_p(f) + \rho_p(t)\, u_p(g) \ .$$

Ainsi $(u_p(e), u_p(f), u_p(g))$ engendre $(1, 0, 0)$. De même $(u_p(e), u_p(f), u_p(g))$ engendre $(0, 1, 0)$ et $(0, 0, 1)$. Cela montre que $(u_p(e), u_p(f), u_p(g))$ est une base de $\mathbb{R}^3$.

4) Il suit en particulier de 3) que pour tout $p = (\alpha, \beta, \gamma) \in \mathbb{R}^3$ tel que $\alpha^2 + \beta^2 + \gamma^2 = 1$, on a $u_p(f) \neq (0, 0, 0)$; i.e. $u_p(U_2, V_2, W_2) \neq (0, 0, 0)$. Cela veut dire que pour tout $p = (\alpha, \beta, \gamma) \in \mathbb{R}^3$ tel que $\alpha^2 + \beta^2 + \gamma^2 = 1$, on a

(1) $\qquad (\rho_p(U_2), \rho_p(V_2), \rho_p(W_2)) \neq (0, 0, 0)$.

Et comme $(U_2, V_2, W_2) \in M$, on a $0 = xU_2 + yV_2 + zW_2$, et en appliquant ρ_p à cette égalité, on a

(2) $\qquad 0 = \alpha\, \rho_p(U_2) + \beta\, \rho_p(V_2) + \gamma\, \rho_p(W_2)$.

Ainsi, pour tout $p = (\alpha, \beta, \gamma) \in \mathbb{R}^3$ tel que $\alpha^2 + \beta^2 + \gamma^2 = 1$, le vecteur $(\rho_p(U_2), \rho_p(V_2), \rho_p(W_2))$ de $\mathbb{R}^3$ est non nul et il est orthogonal à (α, β, γ).
Sachant par ailleurs que U_2, V_2, W_2 sont des fonctions polynomiales en x, y, z à coefficients dans $\mathbb{R}$, il suit que l'application

(3) $p=(\alpha,\beta,\gamma)\mapsto(\rho_p(U_2),\rho_p(V_2),\rho_p(W_2))$ est continue.
Cela définit bien un champ de vecteurs tangents à la sphère $S^2=\{(\alpha,\beta,\gamma)\in\mathbb{R}^3 \mid \alpha^2+\beta^2+\gamma^2=1\}$ et de plus ce champ de vecteurs ne s'annulle jamais.
Cela est en contradiction avec le théorème de la boule chevelue (en IV, ci-après), en conséquence la proposition ne peut être fausse.

III Le cas d'un anneau défini par un polynôme homogène

Soit K un corps commutatif avec $\mathrm{car} K\neq 2$. Soit $P(X,Y,Z)$ un polynôme homogène de degré 2 . On sait que
(1) $$X\frac{\partial P}{\partial X}(X,Y,Z)+Y\frac{\partial P}{\partial Y}(X,Y,Z)+Z\frac{\partial P}{\partial Z}(X,Y,Z)=2P(X,Y,Z) .$$
Soit
(2) $$A:=\frac{K[X,Y,Z]}{(P(X,Y,Z)-1)K[X,Y,Z]} \quad \text{et} \quad \rho:K[X,Y,Z]\to A$$
la surjection canonique et $x:=\rho(X)$, $y:=\rho(Y)$, $z:=\rho(Z)$.
Soient $U:=\rho(\frac{\partial P}{\partial X}(X,Y,Z))$, $V:=\rho(\frac{\partial P}{\partial Y}(X,Y,Z))$, $W:=\rho(\frac{\partial P}{\partial Z}(X,Y,Z))$.
Il suit de (1) que
(3) $$Ux+Vy+Wz=2 .$$
Ainsu, le vecteur (x,y,z) est unimodulaire.

Lemme *Soit* $M:=\{\ (a,b,c)\in A^3 \mid Ua+Vb+Wc=0\ \}$. *Alors on a* $A^3=A\,(x,y,z)\oplus M$. *Il suit de cela que* M est un A- *module projectif de rang* 2.

Démonstration
1) Montrons que $A^3=A\,(x,y,z)+M$.
Soit $\alpha:=Ua+Vb+Wc$. On a donc
$(a,b,c)=\frac{\alpha}{2}(x,y,z)+(a-\frac{\alpha}{2}x,b-\frac{\alpha}{2}y,c-\frac{\alpha}{2}z)$. Compte tenu de la relation (2) on a bien
$U(a-\frac{\alpha}{2}x)+V(b-\frac{\alpha}{2}y)+W(c-\frac{\alpha}{2}z)=0$.
Cela montre bien que $A^3=A\,(x,y,z)+M$.
2) Montrons que la somme est directe.
Si $\beta(x,y,z)=(a,b,c)$ avec $Ua+Vb+Wc$, il suit $\beta\,(Ux+Vy+Wz)=0$ et compte tenu de (3) que $\beta=0$. Cela montre bien que la somme est directe.

Proposition *Soit* A *l'anneau défini en* (2). *On suppose qu'il existe* $(r,s,t)\in K^3-\{(0,0,0)\}$ *tel que* $P(r,s,t)=0$. *Il suit que le vecteur unimodulaire* ${}^t(x,y,z)$ *est le premier vecteur d'une matrice* N *de* $G\ell_3(A)$ *et aussi que le* A*-module* M *est libre de rang* 2 .

Démonstration

Le polynôme P définit sur K^3 une forme quadratique, l'hypothèse sur P veut dire qu'il existe un vecteur isotrope non nul pour cette forme quadratique.

1) Si le rang de la forme quadratique est 1 , cela veut dire qu'après un changement linéaire des variables, on peut supposer que $P(X,Y,Z)=uX^2$ avec $u\in K-\{0\}$. Ainsi $M=\{(a,b,c)\in A^3 \mid 2uxa=0\}$; ce qui veut dire que $M=A(0,1,0)\oplus A(0,0,1)$.

On a donc dét $\begin{bmatrix} x & 0 & 0\\ y & 1 & 0\\ z & 0 & 1\end{bmatrix}=x$, or $ux^2=1$; ce qui montre que ${}^t(x,y,z)$ est le premier vecteur d'une matrice de $G\ell_3(A)$.

2) Si le rang de la forme quadratique est 2 , cela veut dire qu'après un changement linéaire des variables, on peut supposer que $P(X,Y,Z)=uX^2+vY^2$. Ainsi $M:=\{(a,b,c)\in A^3 \mid 2uxa+2vyb=0\}$. Facilement $e':=(vy,-ux,0)$ et $e'':=(0,0,1)$ sont des éléments de M . Si $e:=(x,y,z)$, on a $\text{dét}(e,e',e'')=-1$.

Ce qui montre que ${}^t(x,y,z)$ est le premier vecteur d'une matrice de $G\ell_3(A)$ et aussi que (e,e',e'') est une base du A-module A^3 .

On a donc $A^3=Ae\oplus(Ae'\oplus Ae'')$ et comme par le lemme $A^3=Ae\oplus M$ et que $Ae'\oplus Ae''\subset M$, il suit que $M=Ae'\oplus Ae''$. En effet si $m\in M$, on a $m=\lambda e+(\lambda' e'+\lambda'' e'')$, soit $0=\lambda e+(\lambda' e'+\lambda'' e''-m)$, sachant que $\lambda' e'+\lambda'' e''-m\in M$, il suit que $\lambda' e'+\lambda'' e''-m=0$, i.e. $M=Ae'\oplus Ae''$.

3) Si le rang de la forme quadratique est 3 , sachant que l'espace quadratique contient un vecteur isotrope non nul, cela veut dire que K^3 est somme directe orthogonale d'un plan hyperbolique et d'une droite définie. Cela veut dire qu'après un changement linéaire des variables, on peut supposer que $P(X,Y,Z)=XY+uZ^2$.

On a donc $M=\{(a,b,c)\in A^3 \mid ya+xb+2uzc=0\}$. Facilement $e':=(-2uz,0,y)$ et $e'':=(x^2,-1,\frac{1}{2}xz)$ sont des éléments de M .

Par ailleurs, si $e:=(x,y,z)$, on a $\text{dét}(e,e',e'')=2$.

Ce qui montre que ${}^t(x,y,z)$ est le premier vecteur d'une matrice de $G\ell_3(A)$ et aussi que (e,e',e'') est une base du A-module A^3 . Comme en 2) on déduit que $M=A\,e'\oplus A\,e''$.

IV Le théorème de la boule chevelue ([**Br**], 1912)

Théorème *Soit* $S^2:=\{(x_1,x_2,x_3)\in\mathbb{R}^3 \mid (x_1)^2+(x_2)^2+(x_3)^2=1\}$. *Soit* $u:S^2\to\mathbb{R}^3$ *une application continue avec la propriété que pour tout* $(x_1,x_2,x_3)\in S^2$ *, le vecteur* $u((x_1,x_2,x_3))$ *est orthogonal à* (x_1,x_2,x_3) *;* i.e. u *est un champ de vecteurs tangents à la sphère* S^2 *. Alors il existe* $(a_1,a_2,a_3)\in S^2$ *tel que* $u((a_1,a_2,a_3))=(0,0,0)$.

Démonstration
On suppose le théorème faux.

1) Ce qui veut dire que pour tout $(x_1,x_2,x_3)\in S^2$, on a $u((x_1,x_2,x_3))\neq(0,0,0)$, alors l'application $(x_1,x_2,x_3)\mapsto \dfrac{u((x_1,x_2,x_3))}{\| u((x_1,x_2,x_3))\|}$ possède les mêmes propriétés que u .
On peut donc supposer désormais que pour tout $(x_1,x_2,x_3)\in S^2$ on a $\| u((x_1,x_2,x_3))\|=1$.

2) *Contruction d'un repère "mobile" orthonormé du plan tangent et construction de lacets.*
Soit $x:[0,2\pi]\times[-\frac{\pi}{2},\frac{\pi}{2}]\to\mathbb{R}^3$, l'application définie par

(1) $$x(\theta,\varphi):=(\cos\theta\cos\varphi\ ,\ \sin\theta\cos\varphi,\sin\varphi)\ .$$

Facilement, on a $x([0,2\pi]\times[-\frac{\pi}{2},\frac{\pi}{2}])=S^2$.
Soient $(\theta,\varphi)\in[0,2\pi]\times[-\frac{\pi}{2},\frac{\pi}{2}]$, on définit $e_1(\theta,\varphi)$, $e_2(\theta,\varphi)$ par

(2) $$e_1(\theta,\varphi):=(-\sin\theta\ ,\cos\theta,0)\ ,$$
$$e_2(\theta,\varphi):=(-\sin\varphi\cos\theta\ ,-\sin\varphi\sin\theta,\ \cos\varphi).$$

Alors $(e_1(\theta,\varphi),e_2(\theta,\varphi))$ est une base orthonormée de l'orthogonal de $x(\theta,\varphi)$ dans $\mathbb{R}^3$. Sachant que $u(x(\theta,\varphi))$ est orthogonal à $x(\theta,\varphi)$, on a $u(x(\theta,\varphi))=v_1(\theta,\varphi)\,e_1(\theta,\varphi)+v_2(\theta,\varphi)\,e_2(\theta,\varphi)$ avec

(3) $$v_1(\theta,\varphi)=(\ u(x(\theta,\varphi))\mid e_1(\theta,\varphi))\ ,\ v_2(\theta,\varphi)=(\ u(x(\theta,\varphi))\mid e_2(\theta,\varphi))$$

où $(.\,|\,.)$ est le produit scalaire canonique de $\mathbb{R}^3$.

(4) Il suit de (3) que $v_1(\theta,\varphi)$ et $v_2(\theta,\varphi)$ sont des fonctions continues sur $[0,2\pi]\times[-\frac{\pi}{2},\frac{\pi}{2}]$.

Comme $\| u(x(\theta,\varphi))\| = 1$, on a $(v_1(\theta,\varphi))^2 + (v_2(\theta,\varphi))^2 = 1$, par suite

(5) $$v(\theta,\varphi) := v_1(\theta,\varphi) + i\, v_2(\theta,\varphi)$$

est un élément de $\mathbb{T} := \{z \in \mathbb{C} \mid z\,\overline{z} = 1\}$.

Soit $\varphi \in [-\frac{\pi}{2}, \frac{\pi}{2}]$, alors l'application $\theta \mapsto v(\theta,\varphi)$ de $[0, 2\pi]$ dans $\mathbb{T}$ est continue et de plus $v(0,\varphi) = v(2\pi,\varphi)$.

Ainsi l'application $\theta \mapsto v(\theta,\varphi)$ de $[0, 2\pi]$ dans $\mathbb{T}$ est un lacet défini sur $[0, 2\pi]$ à valeurs dans $\mathbb{T}$ que l'on notera $v(.,\varphi)$.

3) *Le calcul du nombre d'enroulement du lacet* $v(.,\varphi)$.

Soit $w(v(.,\varphi))$ le nombre d'enroulement du lacet $v(.,\varphi)$ (corollaire 1 et définition ci-après) . Il suit de (4) et du corollaire 2 ci-après que l'application $\varphi \to w(v(.,\varphi))$ est une application localement constante sur $[-\frac{\pi}{2}, \frac{\pi}{2}]$; sachant que $[-\frac{\pi}{2}, \frac{\pi}{2}]$ est connexe, il suit que l'application $\varphi \to w(v(.,\varphi))$ est constante.

Nous allons montrer que $w(v(., \frac{\pi}{2})) = -1$ et $w(v(., -\frac{\pi}{2})) = 1$.

Cela montrera que l'hypothèse le "théorème est faux" est à rejeter.

Calculons $w(v(., \frac{\pi}{2}))$. Comme $x(\theta, \frac{\pi}{2}) = (0,0,1)$, sachant que $u(x(\theta, \frac{\pi}{2}))$ est orthogonal à $(0,0,1)$, on a

$$u(x(\theta, \tfrac{\pi}{2})) = (a_1, a_2, 0) \ \text{ avec } \ (a_1)^2 + (a_2)^2 = 1 .$$

Il suit alors de (3) que

(6) $$v(\theta, \tfrac{\pi}{2}) = (-a_1 \sin\theta + a_2 \cos\theta) + i\,(-a_1 \cos\theta - a_2 \sin\theta) .$$

Par ailleurs, il existe $\alpha \in \mathbb{R}$ avec $a_1 = \sin\alpha$, $a_2 = \cos\alpha$. Ainsi (6) s'écrit

(7) $$v(\theta, \tfrac{\pi}{2}) = \cos(\alpha+\theta) - i \sin(\alpha+\theta) = e^{-i(\alpha+\theta)} .$$

On sait alors par le corollaire 1 que

$$w(v(., \tfrac{\pi}{2})) = \frac{-(\alpha+2\pi) + (\alpha+0)}{2\pi} = -1 .$$

Par une méthode analogue, on montre que $w(v(\theta, -\frac{\pi}{2})) = -1$.

Lemme (de relèvement)

Soient $\mathbb{T} := \{z \in \mathbb{C} \mid z\,\overline{z} = 1\}$, $a : [0,1] \to \mathbb{T}$ *une application continue. Soit* $t_0 \in \mathbb{R}$ *tel que* $e^{\,i\,t_0} = a(0)$. *Alors il existe une unique application continue* $b : [0,1] \to \mathbb{R}$ *telle que pour tout* $t \in [0,1]$, $e^{\,i\,b(t)} = a(t)$ *et* $b(0) = t_0$.

$$\begin{tikzcd} & \mathbb{R} \arrow[d, "\lambda"] \\ {[0,1]} \arrow[ur, "b"] \arrow[r, "a"'] & \mathbb{T} \end{tikzcd}$$

Il suit que si $c : [0,1] \to \mathbb{R}$ *est une application continue telle que pour tout* $t \in [0,1]$, $e^{\,i\,c(t)} = a(t)$, *alors il existe* $k \in \mathbb{Z}$ *tel que pour tout* $t \in [0,1]$, *on a* $c(t) = b(t) + 2\,k\,\pi$.

Démonstration

1) *Soient* $x \in [0,1]$, V *un voisinage de* x *contenu dans* $[0,1]$, $a : V \to \mathbb{T}$ *une application continue. Soit* $y \in \mathbb{R}$ *tel que* $e^{\,i\,y} = a(x)$. *Montrons qu'il existe un voisinage* W *de* x *avec* $W \subset V$ *et* $b : W \to \mathbb{R}$, *une application continue avec pour tout* $t \in W$, $e^{\,i\,b(t)} = a(t)$ *et* $b(x) = y$.

Notons $\lambda : \mathbb{R} \to \mathbb{T}$ l'application définie par $\lambda(t) := e^{\,i\,t}$. On sait que λ induit un homéomorphisme $\lambda' :]\,y - \pi, y + \pi\,[\to \mathbb{T} - \{-\lambda(y)\}$, i.e. un homéomorphisme $\lambda' :]\,y - \pi, y + \pi\,[\to \mathbb{T} - \{-a(x)\}$. Soit $\mu := (\lambda')^{-1}$, on a donc pour tout $z \in \mathbb{T} - \{-a(x)\}$,

(1) $\qquad e^{\,i\,\mu(z)} = z$ et en particulier $\mu(a(x)) = y$.

Il existe un voisinage W de x avec $W \subset V$ et $a(W) \subset \mathbb{T} - \{-a(x)\}$. Alors il suit de (1) que pour tout $t \in W$, $e^{\,i\,\mu(a(t))} = a(t)$. Soit b défini par $b(t) := \mu\,a(t)$, alors on a $e^{\,i\,b(t)} = a(t)$ et $b(x) = y$.

2) *Soient* V *un ouvert connexe de* $[0,1]$, $a : V \to \mathbb{T}$ *une application continue,* $b : V \to \mathbb{R}$, $b' : V \to \mathbb{R}$ *des applications continues avec pour tout* $t \in V$, $e^{\,i\,b(t)} = a(t)$ *et* $e^{\,i\,b'(t)} = a(t)$. *On suppose qu'il existe* $t_0 \in V$ *avec* $b(t_0) = b'(t_0)$. *Montrons que* $b = b'$.

En effet, on a $e^{\,i\,b(t)\,-\,b'(t)} = 1$, il suit que $t \mapsto b(t) - b'(t)$ est une application continue à valeurs dans $2\,\pi\,\mathbb{Z}$, elle est constante puisque V est connexe et elle s'anulle en t_0 , il suit que $b = b'$.

3) (existence et unicité du relèvement)

Il suit de 1) qu'il existe $r > 0$ et une application continue $b : [\,0, r\,[\to \mathbb{R}$ telle que pour tout $t \in [0, r\,[$, $e^{\,i\,b(t)} = a(t)$ et $b(0) = t_0$. De même s'il existe $r' > r$ et une application continue $b' : [\,0, r'[\to \mathbb{R}$ telle que pour tout

$t \in [0, r'[$, $e^{ib'(t)} = a(t)$ et $b'(0) = t_0$, alors il suit de 2) que b et b' coïncident sur $[0, r[$.
Soit donc s le maximum des r qui satisfont la propriété ci-dessus. On a donc une application continue $b : [0, s[\to \mathbb{R}$ telle que pour tout $t \in [0, s[$, $e^{ib(t)} = a(t)$ et $b(0) = t_0$.
Montrons d'abord que $s = 1$.
Supposons $s < 1$, alors par 1) il existe $0 < u < s < w < 1$, une application continue $c :]u, w[\to \mathbb{R}$ telle que pour tout $t \in]u, w[$, $e^{ic(t)} = a(t)$. Soit v tel que $u < v < s$. Comme $e^{ic(v)} = a(v) = e^{ib(v)}$, il existe $k \in \mathbb{Z}$ avec $b(v) = c(v) + 2\pi k$. Alors il suit de 2) que l'application b et l'application $t \mapsto c(t) + 2\pi k$ coïncident sur $]u, s[$. Cela permet de prolonger l'application b à $[0, w[$; et comme s est maximum, il suit que $s = 1$.
La méthode précédente permet de prolonger b à 1 .
Cela montre l'existence de b avec $b(0) = t_0$.
L'unicité est conséquence de 2).

4) Soit $c : [0, 1] \to \mathbb{R}$ est une application continue telle que pour tout $t \in [0, 1]$, $e^{ic(t)} = a(t)$. On a donc $a(0) = e^{it_0} = e^{ic(0)}$, alors il existe $k \in \mathbb{Z}$ tel que $c(0) - 2k\pi = t_0$. Si donc $c' : [0, 1] \to \mathbb{R}$ est l'application définie par $c'(t) := c(t) - 2k\pi$, on a bien $e^{ic(t)} = e^{ic'(t)} = a(t)$ et $c'(0) = t_0$, alors l'unicité en 3) montre que $c' = b$ et ainsi pour tout $t \in [0, 1]$, on a $c(t) = b(t) + 2k\pi$.

Corollaire 1 et définition du nombre d'enroulement
Soient $\mathbb{T} := \{z \in \mathbb{C} \mid z\,\overline{z} = 1\}$, $a : [0, 1] \to \mathbb{T}$ *une application continue telle que* $a(0) = a(1)$; i.e. *a est un lacet défini sur* $[0, 1]$ *à valeurs dans* $\mathbb{T}$. *Soit* $b : [0, 1] \to \mathbb{R}$ *une application continue telle que pour tout* $t \in [0, 1]$, $e^{ib(t)} = a(t)$ (*le lemme dit que l'application* b *existe*). *Alors on a*

$$\frac{b(1) - b(0)}{2\pi} \in \mathbb{Z}$$

et cet entier ne dépend pas du choix de b .
Ce nombre $\frac{b(1) - b(0)}{2\pi}$ s'appelle *le nombre d'enroulement du lacet* a . *On le notera* $w(a)$ *(widing number).*

Démonstration
L'existence de b est assurée par le lemme. Si b et c satisfont les hypothèses du corollaire 1, on sait par le lemme qu'il existe $k \in \mathbb{Z}$ tel que $b(t) = c(t) + 2\pi k$ pour tout $t \in [0, 1]$. Cela montre bien que

$$\frac{c(1) - c(0)}{2\pi} = \frac{b(1) - b(0)}{2\pi} .$$

Remarque On pourrait aussi définir un lacet comme une application continue $a\colon [x,y] \to \mathbb{T}$, avec $x, y \in \mathbb{R}$, $x<y$ et $a(x)=a(y)$. Alors on définirait le nombre d'enroulement du lacet a par $w(a) := \frac{b(y)-b(x)}{2\pi}$, si $a(t)=e^{ib(t)}$.

Corollaire 2 (la continuité du nombre d'enroulements)
Soient $\mathbb{T} := \{z \in \mathbb{C} \mid z\overline{z}=1\}$, $a\colon[0,1]\to\mathbb{T}$ (resp. $a'\colon[0,1]\to\mathbb{T}$) *une application continue telle que* $a(0)=a(1)$ (resp. $a'(0)=a'(1)$) ; i.e. a (resp. a') *est un lacet défini sur* $[0,1]$ *à valeurs dans* $\mathbb{T}$. *On suppose que pour tout* $t\in[0,1]$ *on a* $|a(t)-a'(t)|<\sqrt{2}$. *Alors on a* $w(a)=w(a')$, i.e. a *et* a' *ont le même nombre d'enroulement.*

Démonstration
Par le lemme, il existe $b\colon[0,1]\to\mathbb{R}$ (resp. $b'\colon[0,1]\to\mathbb{R}$) une application continue telle que pour tout $t\in[0,1]$, $e^{ib(t)}=a(t)$ (resp. $e^{ib'(t)}=a'(t)$). Il suit de cela que
$$e^{i(b'(t)-b(t))}=\frac{a'(t)}{a(t)}.$$
De plus, pour tout $t\in[0,1]$, on a $\left|\frac{a'(t)}{a(t)}-1\right|<\sqrt{2}$.
Notons $\lambda\colon\mathbb{R}\to\mathbb{T}$ l'application définie par $\lambda(t):=e^{it}$. On sait que λ induit un homéomorphisme $\lambda''\colon]-\frac{\pi}{2},\frac{\pi}{2}[\to\{z\in\mathbb{T} \mid |z-1|<\sqrt{2}\}$. Soit $\mu:=(\lambda'')^{-1}$, on a donc pour tout $z\in\mathbb{T}$ avec $|z-1|<\sqrt{2}$, $e^{i\mu(z)}=z$. Soit alors $c(t):=\mu\left(\frac{a'(t)}{a(t)}\right)$, il suit donc que $e^{ic(t)}=\frac{a'(t)}{a(t)}$. Il suit du lemme qu'il existe $k\in\mathbb{Z}$ tel que pour tout $t\in[0,1]$, on a $c(t)=b'(t)-b(t)+2k\pi$. Ainsi
$$\frac{c(1)-c(0)}{2\pi}=\frac{b'(1)-b'(0)}{2\pi}-\frac{b(1)-b(0)}{2\pi}.$$
Comme $-\frac{\pi}{2}<c(t)<\frac{\pi}{2}$, il suit que $-\frac{1}{4}<\frac{c(1)-c(0)}{2\pi}<\frac{1}{4}$, ainsi $-\frac{1}{4}<w(a')-w(a)<\frac{1}{4}$; sachant que $w(a'), w(a)\in\mathbb{Z}$, on a bien $w(a')=w(a)$.

[Br] **Brouwer L.E.J.** *Über Abbildung von Mannigfaltigkeiten* *Mathematische Annalen 1912 p. 97-115*

[Fr] **Fresnel Jean** *Anneaux* *Hermann* 2001

[La] **Lang Serge** *Algebra* *Addison-Wesley publisching company* 1993 ou *Graduate Texts in Mathematics Springer-Verlag* 2002

[Sa] **Samuel Pierre** *Sur les anneaux factoriels* *Bull. Soc. math. France, 89*, 1961, p. 155-173

[Sw] **Swan Richard** *Vector bundles and projective modules* *Trans. Amer. Math. Soc. 105 (1962) 264-277*

[To] **Towber Jacob** *Tangent Bundles of Affine Quadric Surfaces on Local and Global Fields* *Communications in algebra 7(5), 525-532, 1979*