Jean Fresnel, 21/04/2018

Prolongement d'une colonne unimodulaire en une matrice inversible
Prolongement d'une matrice 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 $\det M \in A^\times$, i.e. $\det M$ 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 $A = x_1A + x_2A + \dots + x_nA$. En effet, si ce n'était pas le cas, il existerait un idéal maximal $\mathfrak{M}$ de A avec $x_1A + x_2A + \dots + x_nA \subset \mathfrak{M}$, alors en calculant $\det A$ selon le développement avec la première colonne, on aurait $\det A \in \mathfrak{M}$, ce qui contredit le fait que $\det M \in A^\times$.
Une colonne $x := {}^t(x_1, x_2, \dots, x_n)$ de A^n telle que $A = x_1A + x_2A + \dots + x_nA$ est appelée *unimodulaire*.

La question est donc de savoir si réciproquement, une colonne unimodulaire peut être la première colonne d'une matrice inversible.
Plus généralement, on dira que l'anneau A satisfait le prolongement de la colonne unimodulaire si toute colonne unimodulaire à coefficients dans A peut être la première colonne d'une matrice inversible à coefficients dans A.

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

La réponse est aussi toujours positive si A est un anneau principal.
Sans changer une virgule, la démonstration s'adapte au cas d'un anneau de Bézout, i.e. d'un anneau intègre dans lequel tout idéal de type fini est principal.

Il y a aussi une large famille d'anneaux définie en 1961 par H. Bass (([B], p. 14.)) qui donne une réponse positive. C'est ce qui suit.
Soit A un anneau commutatif, unitaire. On dit que A satisfait *la propriété "stable range 2"* , si pour tout $s \geq 2$ et pour tout $a_1, a_2, \dots, a_s, a_{s+1} \in A$ avec $a_1A + a_2A + \dots + a_sA + a_{s+1}A = A$, il existe $b_1, b_2, \dots, b_s \in A$ avec

$$(a_1 + b_1 a_{s+1})A + (a_2 + b_2 a_{s+1})A + \dots + (a_s + b_s a_{s+1})A = A .$$

On écrit de façon abrégée cette propriété sous la forme SR(A) ≤ 2 .
De façon élémentaire, cette famille généralise les anneaux principaux.
Si A est un anneau avec SR(A) ≤ 2 , alors A satisfait le prolongement de la colonne unimodulaire.

Toutefois, on est loin d'obtenir tous les anneaux satisfaisant le prolongement de la colonne unimodulaire, puisque la réponse est toujours positive si $A = K[X_1, X_2, \ldots, X_n]$ lorsque K est un corps commutatif, c'est un résultat de Quillen et Suslin, 1976 ([**La**] p. 848).

Il y a deux généralisations du prolongement de la colonne unimodulaire.
La première consiste à considérer une matrice $M \in M_{k,n}(A)$ avec $1 \leq k < n$ telle que l'idéal engendré par les mineurs d'ordre k de M est A. Alors on peut montrer que si A satisfait prolongement de la colonne unimodulaire, il existe une matrice de $G\ell_n(A)$ dont les k premières colonnes sont celles de M.

La seconde consiste à considérer une matrice $M \in M_{k,n}(A)$ avec $1 \leq k < n$ dont $\mathfrak{A}$ est l'idéal engendré par les mineurs d'ordre k de M. Soit $d \in \mathfrak{A}$, on souhaite savoir s'il existe une matrice N de $M_n(A)$ dont les k premières colonnes sont celles de M et dont le déterminant est d. La réponse est positive si l'anneau A est de Dedekind, c'est un théorème de Steinitz.

On sait que tout anneau satisfait la propriété de prolongement de la colonne unimodulaire pour $n = 2$. En revanche, on a un contre-exemple pour $n = 3$, en considérant l'anneau

$$A := \frac{\mathbb{R}[X,Y,Z]}{(X^2+Y^2+Z^2-1)\mathbb{R}[X,Y,Z]} = \mathbb{R}[x,y,z]$$

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

$$A := \frac{K[X,Y,Z]}{(P(X,Y,Z)-1)K[X,Y,Z]} = K[x,y,z]$$

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) .

I. Le cas d'un anneau principal

Proposition *Soient* A *un anneau principal,* $n\geq 2$, $x:={}^t(x_1,x_2,\dots,x_n)$ *avec* $x_k\in A$ *pour* $1\leq k\leq n$ et $A=x_1A+x_2A+\dots+x_nA$. *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* $\varepsilon_1:={}^t(1,0,\dots,0)$ *; 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 $A=x_1A+x_2A$, il suit qu'il existe $u,v\in A$ avec $ux_1+vx_2=1$.
Soit $N:=\begin{bmatrix} u & v \\ -x_2 & x_1 \end{bmatrix}$, on a $\det N=1$ 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 $dA=x_2A+x_3A+\dots+x_nA$, il suit alors de la relation $A=x_1A+x_2A+\dots+x_nA$ que $A=x_1A+dA$.
Comme $x_i\in dA$, il existe $y_i\in A$ avec $x_i=dy_i$ pour $i\geq 2$. On a donc $A=y_2A+y_3A+\dots+y_nA$, il suit de l'hypothèse de récurrence qu'il existe $P\in S\ell_{n-1}(A)$ avec $Py=e_1$ où $y:={}^t(y_2,y_3,\dots,y_n)$ et $e_1:={}^t(1,0,\dots,0)$ et $(1,0,\dots,0)\in A^{n-1}$. Il suit de cela que

$$Pz=de_1 \text{ , si } z:={}^t(x_2,x_3,\dots,x_n) .$$

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

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

De la relation $A=x_1A+dA$, 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 $\det T=1$ 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

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

ce qui montre la proposition.

Description du procédé algorithmique
Comme A est principal, il existe $d_{n-1}\in A$ avec $d_{n-1}A=x_{n-1}A+x_nA$. 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 $\det T=1$ 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 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 ${}^t(x_1, x_2, \dots, x_n)$.

Remarque Sans changer une virgule, la démonstration ci-dessus s'adapte au cas d'un anneau de **Bézout**, i.e. d'un anneau intègre dans lequel tout idéal de type fini est principal.

II. La propriété "stable range 2" et prolongement de la colonne unimodulaire

Définition (*la propriété "stable range 2"*) Soit A un anneau commutatif, unitaire. On dit que A satisfait *la propriété "stable range 2"*, si pour tout $s \geq 2$ et pour tout $a_1, a_2, \dots, a_s, a_{s+1} \in A$ avec $a_1A + a_2A + \dots + a_sA + a_{s+1}A = A$, il existe $b_1, b_2, \dots, b_s \in A$ avec

$$(a_1 + b_1a_{s+1})A + (a_2 + b_2a_{s+1})A + \dots + (a_s + b_sa_{s+1})A = A.$$

On écrit de façon abrégée cette propriété sous la forme SR(A) ≤ 2.

Cette propriété est déjà évoquée par H. Bass en 1961 ([B], p. 14.) On la retrouve aussi chez D. Estes et J. Ohm en 1966 ([E-O], p. 14.). Remarquons que chez Bass la propriété ci-dessus est notée SR(A) ≤ 3 ; nous adoptons la notation SR(A) ≤ 2 qui semble être maintenant la plus courante.

Quelques exemples d'anneaux A avec SR(A) ≤ 2
0. Une limite inductive A d'anneau A_i avec SR(A_i) ≤ 2 satisfait SR(A) ≤ 2
1. Si pour tout $x \in A - \Re$, le nombre d'idéaux maximaux qui contiennent x est fini, on a SR(A) ≤ 2 ; $\Re$ est le radical de Jacobson de A, i.e. l'intersection des idéaux maximaux de A (lemme ci-après).
2. Si l'anneau A a un nombre fini d'idéaux maximaux, alors SR(A) ≤ 2 (c'est une conséquence de 1.).
3. Si A est anneau principal, ou de Dedekind, on a SR(A) ≤ 2 (c'est une conséquence de 1.).
4. Si A est un anneau entier sur $\mathbb{Z}$ ou sur $\mathbb{F}_p[T]$, on a SR(A) ≤ 2 (c'est une conséquence de 0. et 1.).
5. Si A est une algèbre de type fini sur un corps commutatif, intègre et de dimension de Krull au plus 1, on a SR(A) ≤ 2 (c'est une conséquence de 1.).

Lemme *Soient A un anneau commutatif, unitaire, $\Re$ le radical de* Jacobson *de A*, i.e. *l'intersection des idéaux maximaux de A. On suppose que pour tout $x \in A - \Re$, le nombre d'idéaux maximaux qui contiennent x est fini.*
Alors l'anneau A satisfait SR(A) ≤ 2 .

Démonstration
Soient donc $n > 2$, $a_1, a_2, \ldots, a_n \in A$ avec $a_1 A + a_2 A + \ldots + a_n A = A$, il s'agit de montrer qu'il existe $b_1, b_2, \ldots, b_{n-1} \in A$ avec

$$(a_1 + b_1 a_n) A + (a_2 + b_2 a_n) A + \ldots + (a_{n-1} + b_{n-1} a_n) A = A .$$

1) On suppose que $a_1 A + a_2 A + \ldots + a_{n-2} A = A$, alors $b_1 = b_2 = \ldots = b_{n-2} = 0$ et b_{n-1} quelconque conviennent.

2) On suppose que $a_1 A + a_2 A + \ldots + a_{n-2} A \subset \Re$, alors

$$(a_1 + a_n) A + a_2 A + \ldots + a_{n-2} A + a_{n-1} A = A .$$

En effet, s'il existe un idéal maximal $\mathfrak{M}$ avec $(a_1 + a_n) A + a_2 A + \ldots + a_{n-2} A + a_{n-1} A \subset \mathfrak{M}$, cela implique que $a_1 + a_n \in \mathfrak{M}$ et comme $a_1 \in \Re \subset \mathfrak{M}$, on a $a_n \in \mathfrak{M}$; par ailleurs $a_1, a_2, \ldots, a_{n-2} \in \Re \subset \mathfrak{M}$, il suit donc que $a_{n-1} \in \mathfrak{M}$; ce qui est impossible puisque

$$a_1 A + a_2 A + \ldots + a_n A = A .$$

3) Si 1) et 2) ne sont pas vérifiés, on a donc $a_1 A + a_2 A + \ldots + a_{n-2} A \not\subset \Re$ et $a_1 A + a_2 A + \ldots + a_{n-2} A \neq A$.
Il suit qu'il existe un nombre fini d'idéaux maximaux qui contiennent $a_1 A + a_2 A + \ldots + a_{n-2} A$ et que ce nombre n'est pas nul.

Appelons $\{\mathfrak{M}_1, \mathfrak{M}_2, \ldots, \mathfrak{M}_s\}$ l'ensemble des idéaux maximaux qui contiennent $a_1A + a_2A + \ldots + a_{n-2}A$ avec $\mathfrak{M}_i \neq \mathfrak{M}_j$ si $i \neq j$.

3.1) Si $a_n \notin \mathfrak{M}_1 \cup \mathfrak{M}_2 \cup \ldots \cup \mathfrak{M}_s$, il existe donc $x_i \in A$ avec $a_{n-1} - x_i a_n \in \mathfrak{M}_i$ pour $1 \leq i \leq s$. Par le théorème des restes chinois, il existe $b \in A$ tel que $b - (x_i - 1) \in \mathfrak{M}_i$ pour $1 \leq i \leq s$. Il suit de cela que $a_{n-1} + b\,a_n \notin \mathfrak{M}_i$ pour $1 \leq i \leq s$.
Il reste à montrer que $a_1A + a_2A + \ldots + a_{n-2}A + (a_{n-1} + b\,a_n)A = A$.
Supposons le contraire, il existe un maximal $\mathfrak{M}$ avec $a_1A + a_2A + \ldots + a_{n-2}A + (a_{n-1} + b\,a_n)A \subset \mathfrak{M}$. Cela implique que $a_1A + a_2A + \ldots + a_{n-2}A \subset \mathfrak{M}$. Ainsi il existe i avec $1 \leq i \leq s$ et $\mathfrak{M} = \mathfrak{M}_i$. Comme $a_{n-1} + b\,a_n \notin \mathfrak{M}_i$, cela donne une contradiction.

3.2) Si $a_n \in \mathfrak{M}_1 \cap \mathfrak{M}_2 \cap \ldots \cap \mathfrak{M}_s$, il suit de l'inclusion $a_1A + a_2A + \ldots + a_{n-2}A \subset \mathfrak{M}_1 \cap \mathfrak{M}_2 \cap \ldots \cap \mathfrak{M}_s$ et de l'égalité $a_1A + a_2A + \ldots + a_{n-1}A + a_nA = A$ que $a_{n-1} \notin \mathfrak{M}_1 \cup \mathfrak{M}_2 \cup \ldots \cup \mathfrak{M}_s$ et donc que $a_{n-1} - a_n \notin \mathfrak{M}_1 \cup \mathfrak{M}_2 \cup \ldots \cup \mathfrak{M}_s$. En utilisant la méthode de 3.1), il suit de cela que $a_1A + a_2A + \ldots + a_{n-2}A + (a_{n-1} - a_n)A = A$.

3.3) Si les hypothèses de 3.1) et 3.2) ne sont pas vérifiées, quitte à changer les indices, on peut supposer qu'il existe $1 \leq t < s$ avec $a_n \notin \mathfrak{M}_1 \cup \mathfrak{M}_2 \cup \ldots \cup \mathfrak{M}_t$ et que $a_n \in \mathfrak{M}_{t+1} \cap \mathfrak{M}_{t+2} \cap \ldots \cap \mathfrak{M}_s$. Il existe donc $x_i \in A$ avec $a_{n-1} - x_i a_n \in \mathfrak{M}_i$ pour $1 \leq i \leq t$. Par le théorème des restes chinois, il existe $b \in A$ tel que $b - (x_i - 1) \in \mathfrak{M}_i$ pour $1 \leq i \leq t$.
Pour $i > t$, on a $a_n \in \mathfrak{M}_i$, sachant $a_1, a_2, \ldots, a_{n-2} \in \mathfrak{M}_i$ et que $a_1A + a_2A + \ldots + a_nA = A$, il suit que $a_{n-1} + b\,a_n \notin \mathfrak{M}_i$.
En résumé $a_{n-1} + b\,a_n \notin \mathfrak{M}_i$ pour $1 \leq i \leq s$.
Alors la méthode utilisée en 3.1) permet de montrer que

$$a_1A + a_2A + \ldots + a_{n-2}A + (a_{n-1} + b\,a_n)A = A$$

Théorème (prolongement de la colonne unimodulaire)
Soit A *un anneau tel que* $\mathrm{SR}(A) \leq 2$. *Soit* $n \geq 1$, $a_1, a_2, \ldots, a_n \in A$ *tels que* $a_1A + a_2A + \ldots + a_nA = A$. *Soit* $x := {}^t(a_1, a_2, \ldots, a_n)$, *alors il existe* $M \in G\ell_n(A)$ *tel que* x *soit la première colonne de la matrice* M , *c'est équivalent à, il existe* $S \in G\ell_n(A)$ *tel que* $Sx = \varepsilon$ *où* $\varepsilon := {}^t(1, 0, \ldots, 0)$ *avec* $(1, 0, \ldots, 0) \in A^n$.

Démonstration
1) Le cas $n = 1$ ou $n = 2$ est trivial.

On suppose maintenant que $n \geq 3$ *et que le théorème est vrai pour* $n-1$.

2) Sachant que SR(A) ≤ 2 , on sait qu'il existe $b_1, b_2, \ldots, b_{n-1} \in A$ avec

$$(a_1 + b_1 a_n)A + (a_2 + b_2 a_n)A + \ldots + (a_{n-1} + b_{n-1} a_n)A = A .$$

Soit $R := \begin{bmatrix} 1 & . & . & . & b_1 \\ 0 & 1 & 0 & . & b_2 \\ . & . & . & . & . \\ . & . & . & 1 & b_{n-1} \\ 0 & . & . & . & 1 \end{bmatrix} \in G\ell_n(A)$, alors on a

$$Rx = {}^t(a_1 + b_1 a_n, a_2 + b_2 a_n, \ldots, a_{n-1} + b_{n-1} a_n, a_n) .$$

Il suit de l'hypothèse de récurrence qu'il existe $S \in G\ell_{n-1}(A)$ tel que $S\,{}^t(a_1 + b_1 a_n, a_2 + b_2 a_n, \ldots, a_{n-1} + b_{n-1} a_n) = \theta$ avec $\theta := {}^t(1, 0, \ldots, 0)$ où $(1, 0, \ldots, 0) \in A^{n-1}$.

Si donc T est le tableau diagonal (S, I_1) , on a

$$T\,{}^t(a_1 + b_1 a_n, a_2 + b_2 a_n, \ldots, a_{n-1} + b_{n-1} a_n, a_n) = {}^t(1, 0, \ldots, 0, a_n)$$

où $(1, 0, \ldots, 0, a_n) \in A^n$

Soit maintenant $U := \begin{bmatrix} 1 & 0 & . & . & 0 \\ 0 & 1 & . & . & . \\ . & . & 1 & . & . \\ 0 & . & . & . & . \\ -a_n & 0 & . & 0 & 1 \end{bmatrix} = I_n - a_n E_{n,1}$ où $E_{n,1}$ est la matrice dont tous les coefficients sont nuls sauf celui en position $(n, 1)$. Alors on a $U\,{}^t(1, 0, \ldots, 0, a_n) = {}^t(1, 0, \ldots, 0)$ où $(1, 0, \ldots, 0) \in A^n$.

Ainsi $URx = \varepsilon := {}^t(1, 0, \ldots, 0)$ où $(1, 0, \ldots, 0) \in A^n$ avec $UR \in G\ell_n(A)$.

III. Prolongement d'une matrice

Proposition *Soit* A *un anneau qui satisfait le prolongement de la colonne unimodulaire. Soient* $n \geq 2$, $1 \leq k < n$, $M \in M_{n,k}(A)$. *On suppose que l'idéal engendré par les mineurs d'ordre* k *de* M *est* A . *Alors il existe* $N \in G\ell_n(A)$ *dont les* k *premières colonnes sont celles de* M .

Démonstration

Si $n = 2$ c'est trivial.

On suppose maintenant que $n > 2$.

1) *L'objectif est de monter qu'il existe* $S \in G\ell_n(A)$ *tel que* $SM = \begin{bmatrix} U \\ 0 \end{bmatrix}$, *où* $U \in M_k(A)$ *est triangulaire supérieure avec des* 1 *sur la diagonale, et* 0 *est la matrice nulle de* $M_{n-k,k}(A)$.

1.1) On suppose que ${}^t(a_1, a_2, \dots, a_n)$ est la première colonne de M. Montrons que $a_1A + a_2A + \dots + a_nA = A$.
Sinon, il existe un maximal $\mathfrak{M}$ avec $a_1A + a_2A + \dots + a_nA \subset \mathfrak{M}$. Il suit facilement de cela que tous les mineurs d'ordre k de M sont dans $\mathfrak{M}$, ce qui est impossible.

1.2) Comme A satisfait le prolongement de la colonne unimodulaire, cela veut dire qu'il existe $S_1 \in G\ell_n(A)$ tel que $S_1 {}^t(a_1, a_2, \dots, a_n) = {}^t(1, 0, \dots, 0)$. Il suit de cela que $S_1M = \begin{bmatrix} 1 & V \\ 0 & N \end{bmatrix}$ où $V \in M_{1,k-1}(A)$, 0 est l'élément nul de $M_{n-1,1}(A)$ et $N \in M_{n-1,k-1}(A)$.

1.3) On sait que l'idéal engendré par les mineurs de M d'ordre k est aussi l'idéal engendré par les mineurs d'ordre k de S_1M ([Fr2] lemme 1.2.4.2. p. 60). Ainsi l'idéal engendré par les mineurs d'ordre k de S_1M est A. Si un mineur d'ordre k de S_1M est le déterminant d'une sous-matrice qui ne contient pas la première ligne de S_1M, il est nul. Il suit facilement de cela que l'idéal engendré par les mineurs d'ordre $k-1$ de N est A.

1.4) Par hypothèse de récurrence sur k, il existe $T \in G\ell_{n-1}(A)$ tel que $TN = \begin{bmatrix} W \\ 0 \end{bmatrix}$, où $W \in M_{k-1}(A)$ est triangulaire supérieure avec des 1 sur la diagonale, et 0 est la matrice nulle de $M_{n-k+1,k-1}(A)$.
Soit S_2 la matrice qui est le tableau diagonal de (I_1, T), il suit que $S_2(S_1M) = \begin{bmatrix} U \\ 0 \end{bmatrix}$, où $U \in M_k(A)$ est triangulaire supérieure avec des 1 sur la diagonale, et 0 est la matrice nulle de $M_{n-k,k}(A)$.
Ainsi 1) est montré avec $S = S_2S_1$.

2) Soit $R = \begin{bmatrix} U & 0_1 \\ 0_2 & I_{n-k} \end{bmatrix}$, où U est défini en 1), 0_1 est l'élément nul de $M_{k,n-k}(A)$, 0_2 est l'élément nul de $M_{n-k,k}(A)$; bien entendu $R \in G\ell_n(A)$.
Facilement $S^{-1}R = [\, M\, N' \,]$, où $N' := S^{-1}\begin{bmatrix} 0_1 \\ I_{n-k} \end{bmatrix}$. Ainsi $S^{-1}R \in G\ell_n(A)$ et les k premières colonnes de $S^{-1}R$ sont celles de M.

Théorème ([S])*Soient* A *un anneau de Dedekind,* $1 \leq k \leq n$, $M \in M_{k,n}(A)$. *Soient* $\mathfrak{A}$ *l'idéal de* A *engendré par les mineurs d'ordre* k *de* M *et* $d \in \mathfrak{A}$. *Alors il existe* $N \in M_n(A)$ *dont les* k *premières lignes sont celles de* M *et tel que* $\det N = d$.

Démonstration (c'est la démonstration de [G-M-R])
1) Si $k = n$, il n'y a rien à montrer.

2) *On suppose que* $1 \leq k < n$ *et que* $M = [D\ 0]$ *où* $D \in M_{k,k+1}(A)$ *et* 0 *est la matrice nulle de* $M_{k,n-k-1}(A)$.
Soient $1 \leq i \leq k+1$, d_i le mineur qui est le déterminant de la sous-matrice de M obtenu à partir de M en supprimant la i-ème colonne et les colonnes de $k+2$ à n . Facilement l'idéal $d_1A + d_2A + ... + d_{k+1}A$ est l'idéal engendré par les mineurs d'ordre k de M . Il suit de cela qu'il existe $\lambda_1, \lambda_2, \ldots, \lambda_{k+1} \in A$ avec $d = \lambda_1 d_1 + \lambda_2 d_2 + \ldots + \lambda_{k+1} d_{k+1}$.
Soit $\Delta \in M_{k+1}(A)$ dont les k premières lignes sont celles de D et dont la $k+1$-ème ligne est $(\mu_1, \mu_2, \ldots, \mu_{k+1})$ avec $\mu_i := (-1)^{k+i} \lambda_i$. Il suit de cela que $\det \Delta = d$.
Soit maintenant $N := \begin{bmatrix} \Delta & 0_1 \\ 0_2 & I_{n-k-1} \end{bmatrix}$, où 0_1 est la matrice nulle de $M_{k,n-k-1}(A)$ et 0_2 est la matrice nulle de $M_{n-k-1,k+1}(A)$. Facilement, on a $\det N = d$ et les k premières lignes de N sont celles de M .

3) Soient maintenant $1 \leq k < n$, $M \in M_{k,n}(A)$, $\mathfrak{A}$ l'idéal de A engendré par les mineurs d'ordre k de M et $d \in \mathfrak{A}$. Il suit du lemme ci-après qu'il existe $S \in G\ell_n(A)$ tel que $MS = = [D\ 0]$ où $D \in M_{k,k+1}(A)$ et 0 est la matrice nulle de $M_{k,n-k-1}(A)$. On sait que $\mathfrak{A}$ est aussi l'idéal de A engendré par les mineurs d'ordre k de $[D\ 0]$ ([Fr2] lemme 1.2.4.2. p. 60). Il suit alors de 2) qu'il existe une matrice $N \in M_n(A)$ avec $\det N = d$ et les k premières lignes de N sont celles de $[D\ 0]$. Il suit facilement de cela que les k premières lignes de NS^{-1} sont celles de M et que $\det NS^{-1} = \det(N) \det(S)^{-1}$.
Soit alors N' la matrice dont les $n-1$ premières lignes sont celles de NS^{-1} et dont la n-ème ligne est celle de NS^{-1} multipliée par $\det(S)$. Il est alors immédiat que N' satisfait le théorème.

Lemme *Soient* A *un anneau de Dedekind,* $1 \leq k < n$, $M \in M_{k,n}(A)$ *avec* $\operatorname{rang} M = k$. *Alors il existe* $S \in G\ell_n(A)$ *telle que la matrice* MS *soit une matrice de la forme* $[D\ 0]$ *où* $D \in M_{k,k+1}(A)$ *et* 0 *est la matrice nulle de* $M_{k,n-k-1}(A)$.

Démonstration

Soit $f : A^n \to A^k$ l'application linéaire définie par $f(X) := MX$.

Il suit d'abord que $f(A^n)$ est un A-module de type fini. Comme $f(A^n) \subset A^k$, il suit que $f(A^n)$ est sans torsion. Sachant que A est un anneau de Dedekind, on sait alors que $f(A^n)$ est un A-module projectif ([Bk1] prop. 21, p. 78).

On sait alors que $f(A^n)$ est isomorphe à un facteur direct L de A^n ([Bk2] prop. 4, partie d), A.II.39p. 78). On a donc

(1) $$A^n = L \oplus \ker f .$$

Bien entendu $\operatorname{rang}(L) = k$ et $\operatorname{rang}(\ker f) = n - k.$

Il suit de la structure des modules sur un anneau de Dedekind que

(2) $$L \simeq A^{k-1} \oplus I \text{ , } \ker f \simeq A^{n-k-1} \oplus J$$

où I et J sont des idéaux de A . Par ailleurs, on sait que $I \oplus J \simeq A \oplus (IJ)$ ([Bk1] prop. 24, p. 79) . Ainsi, il suit de (1) et (2) que

(3) $$A^n = L \oplus \ker f \simeq (A^{k-1} \oplus I) \oplus (A^{n-k-1} \oplus J) \simeq (A^{n-2} \oplus (I \oplus J) ,$$

ainsi

(4) $$A^n \simeq A^{n-1} \oplus (IJ).$$

Il suit de l'unicité de la factorisation ([Bk1] prop. 24, p. 79) que $IJ \simeq A$ et donc que $I \oplus J \simeq A^2$.

Ainsi

(5) $$L \simeq L_1 \oplus I \text{ où } L_1 = A^{k-1} \text{ , } \ker f \simeq L_2 \oplus J \text{ où } L_2 = A^{n-k-1} ;$$

cela implique en particulier que $\ker f$ contient un sous-module $L_3 \simeq A^{n-k-1}$.

Par ailleurs, on a

(6) $$A^n \simeq (L_1 \oplus I \oplus J) \oplus (L_2) \simeq (L_1 \oplus A^2) \oplus (L_2) \simeq (L_1 \oplus A^2) \oplus (L_3) ,$$

il suit facilement de cela que A^n contient un sous-module L_4 avec

(7) $$A^n = L_4 \oplus L_3 \text{ et } L_4 \simeq A^{k+1} .$$

Il existe donc une base $(e_1, e_2, \ldots, e_n)$ de A^n telle que $(e_1, e_2, \ldots, e_{k+1})$ soit une base de L_4 et que $(e_{k+2}, e_{k+3}, \ldots, e_n)$ soit une base de L_3 .

Soit maintenant $(\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_k)$ la base canonique de A^k , alors on a $\operatorname{Mat}(f; (e_i), (\varepsilon_j)) = [D\ 0]$ où $D \in M_{k,k+1}(A)$ et 0 est la matrice nulle de

$M_{k,n-k-1}(A)$ puisque $f(e_i)=0$ pour $k+2\le i\le n$. Cela veut bien dire qu'il existe $S\in G\ell_n(A)$ tel que $MS=[D\ 0]$.

IV. 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) $\qquad0=\alpha\rho_p(U_2)+\beta\rho_p(V_2)+\gamma\rho_p(W_2)$.

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) $\quad p=(\alpha,\beta,\gamma)\mapsto(\rho_p(U_2),\rho_p(V_2),\rho_p(W_2))$ 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.

V. Le cas d'un anneau défini par un polynôme homogène de degré 2

Soit K un corps commutatif avec $\mathrm{car}K\neq2$. Soit $P(X,Y,Z)$ un polynôme homogène de degré 2. On sait que

(1) $\qquad X\frac{\partial P}{\partial X}(X,Y,Z)+Y\frac{\partial P}{\partial Y}(X,Y,Z)+Z\frac{\partial P}{\partial Z}(X,Y,Z)=2P(X,Y,Z)$.

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) $$Ux + Vy + Wz = 2 \ .$$

Ainsi, 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 (3) on a bien

$$U(a - \frac{\alpha}{2}x) + V(b - \frac{\alpha}{2}y) + W(c - \frac{\alpha}{2}z) = 0 \ ,$$

ce qui veut dire que $(a - \frac{\alpha}{2}x, b - \frac{\alpha}{2}y, c - \frac{\alpha}{2}z) \in M$.
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 que $\beta(Ux + Vy + Wz) = 0$ 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 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. Il existe donc un changement linéaire des variables qui permet de 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 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 $M = Ae' \oplus Ae''$.

VI. 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 $(x_1, x_2, x_3) \mapsto \frac{u((x_1, x_2, x_3))}{\| u((x_1, x_2, x_3)) \|}$ 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 $(. \mid .)$ 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

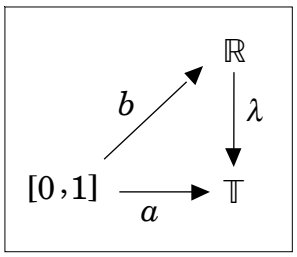
(7) $$v(\theta, \tfrac{\pi}{2}) = \cos(\alpha+\theta) - i\sin(\alpha+\theta) = e^{-i(\alpha+\theta)} .$$

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* $e^{it_0} = a(0)$. *Alors il existe une unique application continue* $b : [0,1] \to \mathbb{R}$ *telle que pour tout* $t \in [0,1]$, $e^{ib(t)} = a(t)$ *et* $b(0) = t_0$.



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

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* $e^{iy} = a(x)$. *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* $t \in W$, $e^{ib(t)} = a(t)$ *et* $b(x) = y$.

Notons $\lambda : \mathbb{R} \to \mathbb{T}$ l'application définie par $\lambda(t) := e^{it}$. 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) $e^{i\mu(z)}=z$ 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 $e^{ib(t)}=a(t)$ 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 $t\in V$, $e^{ib(t)}=a(t)$ et $e^{ib'(t)}=a(t)$. On suppose qu'il existe $t_0\in V$ avec $b(t_0)=b'(t_0)$. Montrons que $b=b'$.*

En effet, on a $e^{ib(t)-b'(t)}=1$, 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 $t\in[0,r[$, $e^{ib(t)}=a(t)$ 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 $a : [x,y] \to \mathbb{T}$, 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 $\mathbb{T} := \{z \in \mathbb{C} \mid z\,\overline{z} = 1\}$, $a : [0,1] \to \mathbb{T}$ (resp. $a' : [0,1] \to \mathbb{T}$) *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 $b : [0,1] \to \mathbb{R}$ (resp. $b' : [0,1] \to \mathbb{R}$) 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 $\lambda : \mathbb{R} \to \mathbb{T}$ l'application définie par $\lambda(t) := e^{it}$. On sait que λ induit un homéomorphisme $\lambda'' :]-\frac{\pi}{2}, \frac{\pi}{2}[\to \{z \in \mathbb{T} \mid |z - 1| < \sqrt{2}\}$. 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 $c(t) := \mu(\frac{a'(t)}{a(t)})$, 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 $w(a') = w(a)$.

Bibliographie

[B] **Bass H.** *K-theory and stable algebra* *Publ. Inst. Hautes Etudes Sci. 22 (1964) p. 1-60.*

[Bk1] **Bourbaki N.** *Algèbre commutative ch. 7.* *Hermann (1965)*

[Bk2] **Bourbaki N.** *Algèbre ch. 1, 2, 3* *Hermann (1970)*

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

[E-O] **Estes D. , Ohm J.** *Stable Range in Commutative Rings* *Journal of Algebra 7, 343-362 (1967)*

[Fr1] **Fresnel Jean** *Anneaux* *Hermann* 2001

[Fr2] **Fresnel Jean** *Algèbre des matrices* *Hermann* 2011

[G-M-R] **Gustafson W., Moore M., Reiner I.** *Matrice completion over Dedekind Rings* *Linear and Multilinear Algebra, 1981, Vol. 10, pp. 141-144.*

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

[L-M] **Micheli G., Weger V.** *On rectangular unimodular matrices over the ring of algabraic integers,* arXiv : 1803.08785v1 [math.NT] 23 Mar 2018

[R1] **Reiner I. Completion of primitive matrices** *The American Mathematical Monthly Vol. 73, N° 4 (Apr.;1966) pp. 380-381*

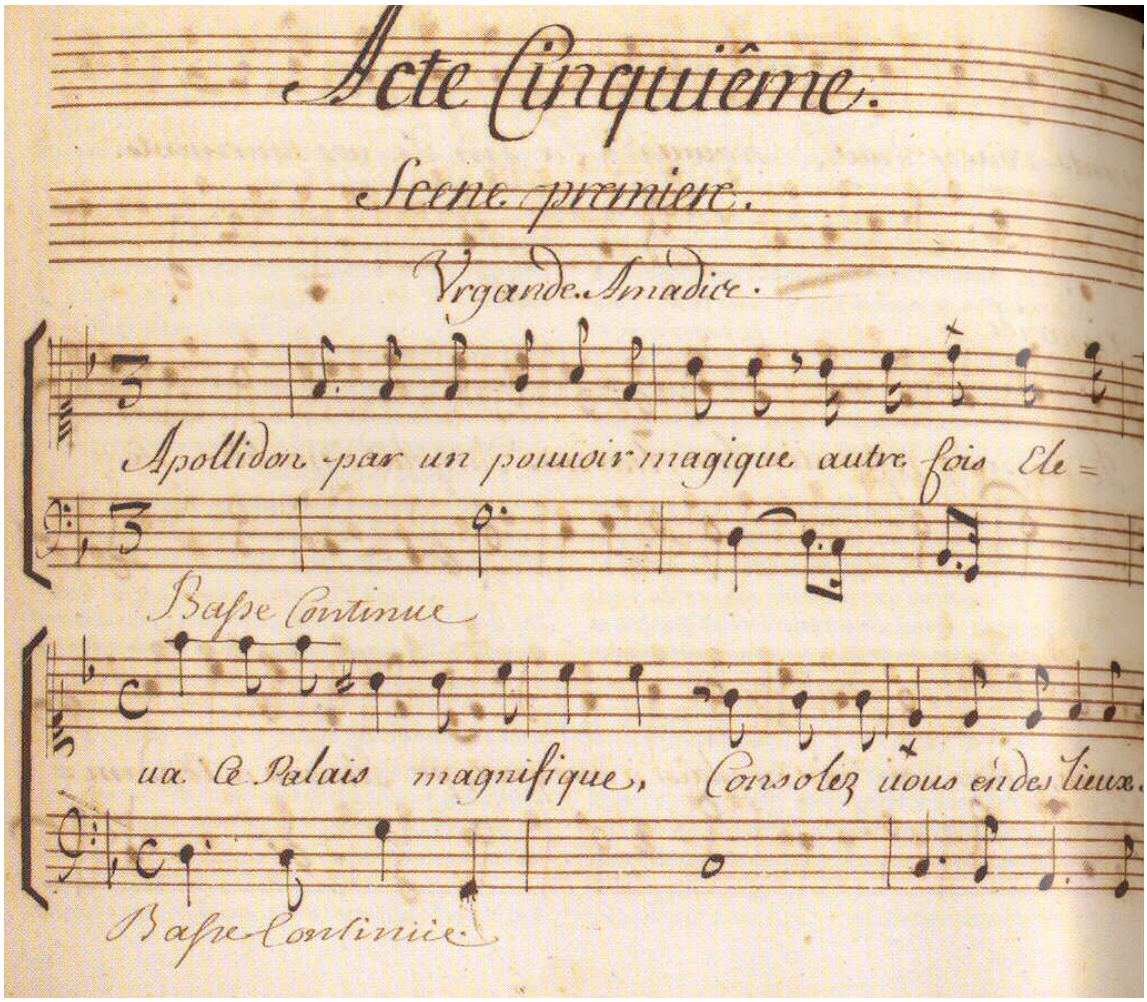
[R2] **Reiner I.** *Unimodular complements* *The American Mathematical Monthly Vol. 63, N° 4 (Apr.;1956) pp. 246-247*

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

[S] **Steinitz E.** *Rechteckige Systeme und Moduln in algebraischen Zahlenkörpern,* *Math. Ann. 71 (1911) 328-354.*

[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*



Adamis de Lully