Le ruban de Möbius comme représentation d'un idéal non principal

Daniel Ferrand
Mars 2005

Introduction

Sur votre bande de papier calque, de forme rectangulaire assez allongée, tracez une droite parallèle aux deux grands côtés et équidistante d'iceux ; en chaque point de cette droite pensez à, ou tracez, un segment perpendiculaire, que vous imaginerez de longueur infinie. Collez les petits côtés du rectangle, aprés avoir effectué le demi-tour fatidique. La droite tracée devient un cercle. Cette chose, la bande de Möbius, devrait vous faire penser à une famille de droites paramétrée par le cercle, famille radicalement différente de celle fournie par un cylindre... et pourtant il suffit de les couper, i.e. d'enlever à chacune de ces surfaces une droite verticale pour qu'elles deviennent évidemment isomorphes.

Cet objet géométrique a un analogue algébrique. Considérez l'anneau $\mathbf{R}[X,Y]/(X^2+Y^2-1)$ des applications polynomiales définies sur le cercle, à valeurs réelles. C'est un anneau intégralement clos, son complexifié est principal, et cependant l'idéal de cet anneau engendré par $1+x$ et y *n'est pas principal.*

Dans cette note, je donne un modèle mathématique très simple du ruban de Möbius. Il permet d'expliquer les liens entre le ruban et l'idéal. J'espère que cela éclairera l'un et l'autre.

J'ai explicité - au-delà, sans doute, du nécessaire - les passages entre le géométrique et l'algébrique. Après les avoir compris, l'étudiant élaguera les digressions devenues superflues. Le paragraphe 3 donne *trois* démonstrations de la non factorialité de A. Chacune méritait d'être exposée, et chacune peut conduire à un développement original qui aurait sa place dans les leçons suivantes :

- Exemples d'application des idéaux d'un anneau commutatif unitaire
- Anneaux principaux
- Groupe des nombres complexes de module 1
- Applications des nombres complexes à la géométrie

Ce qui suit est considéré, par les spécialistes, et depuis quarante ans, comme plus ou moins évident, au point, semble-t-il, de n'avoir pas été rédigé complètement. L'article de Swan [5] contient quelques lignes (p.273) qui m'ont aidé.

1. Géométrie : le ruban de Möbius.

Dans toute cette note, le symbole $\mathbf{U}$ désigne le groupe des nombres complexes de module 1, vu, géométriquement, comme le cercle unité.

1.1. Définition

On définit le ruban de Möbius comme un sous-espace topologique de $\mathbf{U} \times \mathbf{C}$, à savoir :

$$\mathbf{M} \;=\; \{(u,z) \in \mathbf{U} \times \mathbf{C}, u\bar{z} = z.\}$$

On utilisera constamment la

Remarque-clé 1.1.1. *Si $v \in \mathbf{U}$, alors la relation $v^2\bar{z} = z$ équivaut à $z = \mu v$, avec $\mu \in \mathbf{R}$.*

En effet, la relation en question s'écrit aussi $\overline{(z/v)} = z/v$.

La première projection $\mathbf{U} \times \mathbf{C} \longrightarrow \mathbf{U}$ induit une application continue

$$p : \mathbf{M} \quad \longrightarrow \quad \mathbf{U}, \qquad (u,z) \mapsto u.$$

Pour tout $u \in \mathbf{U}$, la fibre $\mathbf{M}_u = p^{-1}(u)$ est un $\mathbf{R}$-espace vectoriel de dimension 1. En effet, $\mathbf{C}$ étant algébriquement clos, tout complexe admet une racine carrée, et si on choisit une racine carrée de u, soit un élément $v \in \mathbf{U}$ tel que $v^2 = u$, alors, d'après 1.1.1, on a

$$\mathbf{M}_u \;=\; \mathbf{R}v \subset \mathbf{C}.$$

La droite $\mathbf{M}_u$ est donc la bissectrice de l'angle $\widehat{(1,u)}$. Ainsi, l'application $p : \mathbf{M} \longrightarrow \mathbf{U}$ conduit à voir $\mathbf{M}$ comme une famille de droites vectorielles dans le plan, paramétrée par le cercle unité, et qui « tournent deux fois moins vite » que le paramètre.

Avant de faire le lien entre cette définition et la bande de Möbius « concrète », il faut indiquer comment on obtient le ruban de Möbius comme quotient du cylindre $\mathbf{U} \times \mathbf{R}$ par l'action d'un groupe d'ordre 2.

Lemme 1.1.2. *Le carré suivant est cartésien, i.e il permet d'identifier $\mathbf{U} \times \mathbf{R}$ au sous-ensemble de $\mathbf{U} \times \mathbf{M}$ formé des couples (v,m) tels que $v^2 = p(m)$.*

$$\begin{array}{ccc} \mathbf{U} \times \mathbf{R} & \xrightarrow{(v,\mu)\mapsto(v^2,\mu v)} & \mathbf{M} \\ {\scriptstyle \mathrm{pr}_1}\downarrow & & \downarrow{\scriptstyle p} \\ \mathbf{U} & \xrightarrow[v\mapsto v^2]{} & \mathbf{U} \end{array}$$

De plus, l'application indiquée $\mathbf{U} \times \mathbf{R} \to \mathbf{M}$, $(v,\mu) \mapsto (v^2, \mu v)$ permet d'identifier $\mathbf{M}$ avec le quotient de $\mathbf{U} \times \mathbf{R}$ sous l'involution $(v,\mu) \mapsto (-v,-\mu)$.

(En termes savants - et tout-à-fait inutiles pour la suite - on énoncerait que le ruban de Möbius est un fibré en droites sur $\mathbf{U}$, trivialisé par le revêtement $v \mapsto v^2$; « trivialisé » veut dire : rendu isomorphe au cylindre $\mathbf{U} \times \mathbf{R}$.)

La première assertion du lemme répète la remarque-clé. Pour vérifier la seconde, considérons des éléments (v,μ) et (v',μ') de $\mathbf{U}\times\mathbf{R}$ ayant la même image dans $\mathbf{M}$; on a donc $v^2 = v'^2$, d'où $v' = \varepsilon v$, avec $\varepsilon = \pm 1$, et $\mu v = \mu' v' = \mu'\varepsilon v$; d'où $(v',\mu') = \varepsilon(v,\mu)$.

1.2. Reconnaître la bande de Möbius

Rappelons la définition classique du ruban de Möbius comme quotient du plan $\mathbf{R}^2$ par l'action d'un groupe Γ (GODBILLON, p.43 ; STILLWELL p.25, où la *bande* de Möbius est nommée "Möbius strip", tandis que son *ruban* est nommé "twisted cylinder", ce qui est très évocateur).

On considère la « symétrie glissée » ("glide reflection") $\gamma : \mathbf{R}^2 \to \mathbf{R}^2$ définie par $\gamma(\lambda,\mu) = (\lambda+1, -\mu)$, et le groupe Γ (isomorphe à $\mathbf{Z}$) engendré par γ.

On remarque que $\gamma^2(\lambda,\mu) = (\lambda+2,\mu)$; il est donc naturel de passer d'abord au quotient par le sous-groupe engendré par γ^2 puisqu'il n'agit que par translation sur le premier facteur ; l'exponentielle donne un homéomorphisme

$$\mathbf{R}^2/<\gamma^2> \quad \widetilde{\longrightarrow} \quad \mathbf{U}\times\mathbf{R}, \qquad (\lambda,\mu)\mapsto(e^{i\pi\lambda},\mu).$$

Comme $e^{i\pi} = -1$, la symétrie glissée γ induit sur le quotient l'application $(u,\mu)\mapsto(-u,-\mu)$; c'est précisément l'involution considérée dans le lemme précédent, et ce lemme implique donc qu'on a un homéomorphisme

$$\mathbf{R}^2/\Gamma \quad \widetilde{\longrightarrow} \quad \mathbf{M}.$$

Pour remonter du *ruban* (surface non compacte, sans bord, non immergeable dans l'espace) à la *bande* (surface compacte, à bord, mais qu'on peut fabriquer et voir), on se restreint au rectangle $D = [0,1]\times[-1,1] \subset \mathbf{R}^2$; les seuls points de D que γ envoie dans D sont les points du bord $(0,\mu)$, et $\gamma(0,\mu) = (1,-\mu)$; en identifiant pour chaque $\mu\in[-1,1]$, les points $(0,\mu)$ et $(1,-\mu)$ on trouve la fameuse bande.

1.3. Les sections

Une *section* de p est, par définition, une application continue $s : \mathbf{U}\to\mathbf{M}$ telle que $p\circ s = id_{\mathbf{U}}$. Il est habituel d'écrire ces applications verticalement :

$$\begin{array}{ccc} & & \mathbf{M} \\ & {\scriptstyle s}\uparrow \;\; \downarrow{\scriptstyle p} & \\ & \mathbf{U} & \end{array}$$

La donnée d'une section peut être vue comme la donnée, pour chaque u, d'un point sur la droite $\mathbf{M}_u$, point qui varie continûment avec u.
La *section nulle* est l'application $s_0 : \mathbf{U}\to\mathbf{M}$ définie par $s_0(u) = (u,0)$.

Proposition 1.3.1. *Toute section rencontre la section nulle.*

Raisonnons par l'absurde en supposant qu'il existe une application continue $s : \mathbf{U}\to\mathbf{M}$ telle que $p\circ s = id_{\mathbf{U}}$ et telle que pour tout $u\in\mathbf{U}$, $s(u)\neq(u,0)$. La section s'écrit $s(u) = (u, f(u))$, où f s'obtient par composition avec la projection dans $\mathbf{C}$,

$$\begin{array}{ccccc} \mathbf{M} & \longrightarrow & \mathbf{U}\times\mathbf{C} & \xrightarrow{\mathrm{pr}_2} & \mathbf{C} \\ {\scriptstyle s}\uparrow & & & \nearrow_{f} & \\ \mathbf{U} & & & & \end{array}$$

L'application $f : \mathbf{U}\to\mathbf{C}$ est continue, comme s, et ne s'annule pas. Comme $(u,f(u))\in\mathbf{M}$, on a, pour tout $u\in\mathbf{U}$, $u\overline{f(u)} = f(u)$, ce qui s'écrit aussi, puisque $f(u)$ n'est jamais nul, $u = f(u)^2/\overline{f(u)}f(u)$. Si on

pose $\varphi(u) = f(u)/|f(u)|$, on a donc $u = \varphi(u)^2$. Or,

Proposition 1.3.2 *Il n'existe pas d'application continue* $\varphi : \mathbf{U} \to \mathbf{U}$ *telle que* $u = \varphi(u)^2$ *pour tout* $u \in \mathbf{U}$.

(Cette impossibilité devrait être bien connue ; un étudiant qui la rencontrerait pour la première fois devrait d'abord vérifier que $\varphi(e^{i\alpha}) = e^{i\alpha/2}$ ne marche pas.)

Première démonstration. Si une telle application φ existait, l'application $\psi(u) = \varphi(u)\varphi(\bar{u})$ vérifierait

$$\psi(u)^2 \;=\; \varphi(u)^2\varphi(\bar{u})^2 \;=\; u\bar{u} \;=\; 1.$$

Elle ne prendrait donc que deux valeurs : 1 et -1. Mais elle serait aussi continue, et $\mathbf{U}$ est connexe, donc ψ serait constante ; or, $\psi(-1) = -1$ et $\psi(1) = 1$.

Deuxième démonstration. Elle donne le cas général, à savoir : pour $n \geq 2$, il n'y a pas d'application continue telle que $u = \varphi(u)^n$. Supposons qu'une telle application existe et montrons d'abord que les ensembles $\omega\varphi(\mathbf{U})$ forment une partition de $\mathbf{U}$, lorsque ω parcourt l'ensemble μ_n des racines n-ièmes de l'unité.

Soit $u \in \mathbf{U}$; on a $u^n = \varphi(u^n)^n$, donc il existe $\omega \in \mu_n$ tel que $u = \omega\varphi(u^n)$; la réunion des ensembles $\omega\varphi(\mathbf{U})$ est donc égale à $\mathbf{U}$. Leurs intersections deux à deux sont vides puisque si on a $\omega\varphi(u) = \omega'\varphi(u')$, alors $u = (\omega\varphi(u))^n = (\omega'\varphi(u'))^n = u'$, d'où aussi $\omega = \omega'$.

Mais $\mathbf{U}$ est compact ; la continuité de φ entraîne donc que $\varphi(\mathbf{U})$ est compact donc fermé dans $\mathbf{U}$. Comme $\mathbf{U}$ est connexe il n'admet pas de partition finie en n sous-ensembles fermés, lorsque $n \geq 2$.

Conclusion 1.3.3 *Le ruban de Möbius n'est pas isomorphe à un cylindre.*

Montrons-le par l'absurde en supposant qu'il existe un homéomorphisme $h : \mathbf{U} \times \mathbf{R} \xrightarrow{\sim} \mathbf{M}$ compatible avec les projections

$$\begin{array}{ccc} \mathbf{U}\times\mathbf{R} & \xrightarrow{\;h\;} & \mathbf{M} \\ & {\scriptstyle \mathrm{pr}_1}\searrow \quad \swarrow{\scriptstyle p} & \\ & \mathbf{U} & \end{array}$$

et induisant sur chaque fibre un isomorphisme de $\mathbf{R}$-espaces vectoriels $\mathbf{R} \xrightarrow{\sim} \mathbf{M}_u$. Comme, pour u fixé, $\lambda \mapsto h(u,\lambda)$ est linéaire, on a $h(u,\lambda) = \lambda h(u,1)$, donc $h(u,1) \neq 0$. L'application $s : \mathbf{U} \to \mathbf{M}$ définie par $s(u) = h(u,1)$ serait donc une section (continue) de p partout non nulle ; on a vu que c'est impossible.

2. Traduction en termes algébriques

2.1. L'espace $\mathbf{M}$ a été défini comme l'ensemble des points de $\mathbf{U} \times \mathbf{C}$ qui sont fixes sous l'involution

$$r : \mathbf{U} \times \mathbf{C} \;\to\; \mathbf{U} \times \mathbf{C}, \quad (u,z) \mapsto (u, u\bar{z}),$$

donc comme un sous-ensemble de points soumis à une relation. Il est souvent plus commode, quand c'est possible, de travailler avec un objet « paramétré », c'est-à-dire défini plutôt comme *image* d'une application (dont la source devient donc l'ensemble des paramètres). Lorsque la relation est une involution, il est très facile de passer d'un point de vue à l'autre : on introduit le projecteur associé, soit, ici, l'application $q = \frac{1}{2}(r+1)$, précisement :

$$q(u,z) \;=\; (u, \frac{1}{2}(u\bar{z} + z)).$$

Une vérification immédiate montre que $q^2 = q$, et que $\mathrm{Im}(q) = \mathbf{M}$.

L'application $z \mapsto \frac{1}{2}(u\bar{z} + z)$ est donc un projecteur ($\mathbf{R}$-linéaire) du $\mathbf{R}$-espace vectoriel $\mathbf{C}$, dépendant du paramètre u. Donnons-en sa matrice.

Si on écrit $u = x + iy$, avec la contrainte $x^2 + y^2 = 1$, et $z = a + ib$, on trouve $\frac{1}{2}(u\bar{z} + z) = \frac{1}{2}[((1+x)a + yb) + i(ya + (1-x)b)]$. Dans l'espace fibre ($= \mathbf{C}$) au dessus de $u = x + iy$, la matrice de q est donc

$$\boxed{Q \;=\; \frac{1}{2}\begin{pmatrix} 1+x & y \\ y & 1-x \end{pmatrix}}$$

2.2. Posons $A = \mathbf{R}[X,Y]/(X^2 + Y^2 - 1)$.

Il faut voir A comme l'anneau des fonctions continues $f : \mathbf{U} \to \mathbf{R}$ qui sont polynomiales au sens suivant : il existe un polynôme $F(X,Y) \in \mathbf{R}[X,Y]$ tel que, pour $u = \xi + i\eta \in \mathbf{U}$, on ait $f(u) = F(\xi, \eta)$. Bien évidemment F n'est défini par f qu'à un multiple près de $X^2 + Y^2 - 1$, et c'est pourquoi l'on passe au quotient.

Désignons désormais par x et y les classes de X et de Y dans l'anneau quotient A, et considérons maintenant la matrice

$$Q \;=\; \frac{1}{2}\begin{pmatrix} 1+x & y \\ y & 1-x \end{pmatrix}$$

comme une matrice à coefficients dans A. Le théorème de Hamilton-Cayley s'écrit

$$Q^2 - \mathrm{Tr}(Q)Q + \det(Q) = 0.$$

Comme $\mathrm{Tr}(Q) = 1$ et $\det(Q) = 0$, on a

$$Q^2 \;=\; Q.$$

Cette matrice définit une application A-linéaire $Q : A^2 \to A^2$. On pose

$$M \;=\; \mathrm{Im}(Q) \;=\; \mathrm{Ker}(1-Q).$$

Ce module M est l'analogue algébrique du ruban de Möbius.

Précisons cette assertion en montrant comment associer à un élément de M une section (polynomiale) de $p : \mathbf{M} \to \mathbf{U}$. À un élément $\binom{a}{b} \in A^2$, c'est-à-dire à un couple d'éléments de A, vus comme applications polynomiales de $\mathbf{U}$ dans $\mathbf{R}$, on associe l'application $f : \mathbf{U} \to \mathbf{C}$ définie par $f = a + ib$. Si $\binom{a}{b}$ est dans $M = \mathrm{Ker}(1-Q)$, alors $Q\binom{a}{b} = \binom{a}{b}$, ce qui s'écrit aussi

$$\begin{pmatrix} x & y \\ y & -x \end{pmatrix}\begin{pmatrix} a \\ b \end{pmatrix} \;=\; \begin{pmatrix} a \\ b \end{pmatrix}.$$

Si on utilise l'écriture complexe, cela donne $(x+iy)(a-ib) = a+ib$, soit $u\overline{f(u)} = f(u)$; bref, $(u, f(u)) \in \mathbf{M}$, et $u \mapsto (u, f(u))$ est la section annoncée.

2.3. Montrons que le A-module M n'est pas isomorphe à A, contrairement à ce que tout laisse penser (En termes savants, M est projectif de rang 1, mais n'est pas libre).

Si on pose $M' = \mathrm{Im}(1-Q)$, on obtient une décomposition en somme directe de A-modules

$$M \oplus M' \;=\; A^2.$$

La vérification de cela, classique pour les espaces vectoriels, est exactement la même pour les modules ; elle utilise seulement le fait que l'endomorphisme Q est idempotent. Je ne la recopie pas.

Soit K le corps des fractions de A (on verra plus bas que A est intègre). Notons Q_K l'endomorphisme du K-espace vectoriel K^2 de matrice Q, et posons $V = \mathrm{Im}(Q_K)$ et $V' = \mathrm{Im}(1 - Q_K)$. Ces K-espaces vectoriels donnent la décomposition

$$V \oplus V' = K^2.$$

Comme les matrices Q et $1-Q$ sont non nulles, on a $\dim_K(V) = \dim_K(V') = 1$; V et V' sont, par suite, isomorphes à K et ne peuvent donc pas contenir de partie libre sur A ayant 2 éléments. Enfin, l'inclusion $A^2 \subset K^2$ entraîne les suivantes : $M \subset V$ et $M' \subset V'$.

Si l'anneau A était principal, M et M' seraient libres (comme sous-modules du module libre A^2), donc libres de rang 1 comme sous-modules de V et V', et on pourrait encore conclure que M est isomorphe à A. Malheureusement, on va voir que M n'est pas libre, ce qui entraînera que A n'est pas principal.

Notons que le module $M = \mathrm{Im}(Q)$ contient les éléments $Q\binom{1}{0} = \binom{1+x}{y}$ et $Q\binom{0}{1} = \binom{y}{1-x}$. Si M admettait une base, elle serait réduite à un élément puisque M est un sous-module de V ; notons $\binom{a}{b}$ ce générateur libre ; il existerait des éléments $c, d \in A$ tels que $\binom{1+x}{y} = c\binom{a}{b}$, et $\binom{y}{1-x} = d\binom{a}{b}$; en particulier, on aurait $1+x = ca$ et $1-x = db$ donc $2 = ca + db$. Mais alors les applications a et b ne pourraient s'annuler simultanément, et la section $u \mapsto (u, f(u))$ associée, comme ci-dessus, à $\binom{a}{b}$ serait partout non nulle. On a vu que c'est impossible.

3. Algèbre : l'anneau $A = \mathbf{R}[X,Y]/(X^2+Y^2-1)$

Ce paragraphe aborde plusieurs aspects de la non factorialité de A ; on montre, en particulier, que l'idéal $(1+x, y)$ n'est pas principal.

Il semble que le livre de D. Perrin [2] reste un des exposés de ces propriétés arithmétiques les mieux adaptés à l'agrégation. Nous supposerons connus les paragraphes 1 et 3 du chapitre II de ce livre.

3.1 L'extension de degré deux $\mathbf{R}[X] \to A$.

Pour établir certaines propriétés de l'anneau $A = \mathbf{R}[X,Y]/(X^2+Y^2-1)$ on utilise ici l'analogue algébrique de la projection du cercle unité $\mathbf{U}$ sur l'axes des X. Toute fonction polynomiale sur cet axe, i.e. tout polynôme $F(X)$, fournit, en la composant avec la projection (la partie réelle), une application polynomiale définie sur $\mathbf{U}$, à savoir $u \mapsto F(\Re u)$.

Notons, comme plus haut, par x et y les classes dans A de X et de Y. En écrivant

$$A = \mathbf{R}[X][Y]/(Y^2 - (1-X^2)),$$

on fait apparaître A comme l'anneau obtenu en adjoignant à $\mathbf{R}[X]$ une racine carrée de $1-X^2$; cela montre déja que *tout élément de A s'écrit de façon unique sous la forme $p(x) + yq(x)$.*

Par ailleurs, le critère d'Eisenstein, appliqué avec l'élément premier $X-1$ de $\mathbf{R}[X]$ entraîne que $Y^2 - (1-X^2)$ est irréductible, donc que A est *intègre.*

Pour aller plus loin, on introduit l'application norme (déja utilisée dans la première démonstration de 1.3.2). Soit $\sigma : A \to A$ l'automorphisme de $\mathbf{R}[X]$-algèbres défini par $\sigma(y) = -y$ (C'est bien un automorphisme puisque $-y$ est une racine de $Y^2 - (1-X^2)$). Posons, pour $a \in A$,

$$N(a) = a\sigma(a).$$

Comme σ respecte la multiplication, il en est de même de N ; on a donc $N(ab) = N(a)N(b)$, et, si a ne dépend pas de y, $N(a) = a^2$.

Si on écrit a sur la base $(1, y)$, on trouve

$$N(p(x) + yq(x)) = p(x)^2 - y^2 q(x)^2 = p(x)^2 + (x^2-1)q(x)^2.$$

C'est un polynôme en X, dont on peut considérer le degré.

$$\mathbf{R}[X] \xrightleftarrows{N} A$$

Lemme 3.1.1 *Pour tout* $a \in A$, $\deg N(a) \neq 1$.

En effet, le polynôme à coefficients réels $p(X)^2 + (X^2-1)q(X)^2$ prend des valeurs ≥ 0 pour $x < -1$, et pour $x > 1$, ce qu'un polynôme de degré 1 ne peut faire.

3.2. Un élément de A irréductible et non premier

Le lemme précédent implique immédiatement que y est un élément irréductible de A : en effet, l'égalité $y = ab$, avec $a, b \in A$, entraîne que $X^2-1 = N(y) = N(a)N(b)$; comme $N(a)$ et $N(b)$ sont des polynômes en X de degré $\neq 1$, l'un des deux est constant, donc a ou b est inversible [1].
L'irréductibilité de y dans A est liée à la topologie de $\mathbf{R}$. On verra en effet plus bas (3.5) que y n'est plus irréductible dans l'anneau $\mathbf{C}[X,Y]/(X^2+Y^2-1)$, car on peut le décomposer en $y = \frac{1}{2i}(1-x+iy)(1+x+iy)$.

On constate ensuite que l'idéal yA n'est pas premier, puisque l'anneau quotient $A/yA = \mathbf{R}[X,Y]/(X^2+Y^2-1, Y) \simeq \mathbf{R}[X]/(X^2-1)$ n'est pas intègre (la classe $\bar{x}$ de X est distincte de ± 1 et vérifie la relation $(\bar{x}-1)(\bar{x}+1) = 0$).

Cela montre que l'anneau A n'est pas factoriel, et a fortiori qu'il n'est pas principal (PERRIN II 3.19 et 3.21) (Voir aussi ci-dessous 4.2 pour les relations entre « factoriel » et « principal »).

3.3. L'idéal $(1+x)A + yA$.

Notons I cet idéal de A

3.2.1. On va montrer que *le module M introduit en 2.2 est isomorphe à I*, ce qui justifie de considérer ici cet idéal. Plus précisément, on va montrer que la projection

$$\mathrm{pr}_1 : A^2 \to A$$

induit un isomorphisme de M sur I. En effet, l'idéal I est engendré par la première ligne de la matrice Q, c'est-à-dire par les premières coordonnées de $Q\binom{1}{0}$ et $Q\binom{0}{1}$. Or, $\mathrm{Im}(Q) = M$; par suite,

$$I \;=\; \mathrm{pr}_1(M).$$

Il reste à montrer que $\mathrm{Ker}(\mathrm{pr}_1) \cap M = 0$, c'est-à-dire, puisque $\mathrm{Ker}(\mathrm{pr}_1) = 0 \times A$, que l'on a $M \cap (0 \times A) = 0$. Or, si $\binom{0}{a} \in M$, alors $Q\binom{0}{a} = \binom{0}{a}$, ce qui équivaut à : $ya = 0$ et $(1-x)a = a$, d'où $xa = 0$; mais alors $a = (x^2+y^2)a = 0$.

On a montré en 2.3, par voie géométrique, que le A-module M n'est pas libre, cela entraîne donc que l'idéal I n'est pas principal.

On va retrouver ce résultat presqu'algébriquement, c'est-à-dire en réduisant les inévitables arguments topologiques au seul lemme 3.1.1 ci-dessus. Les numéros 3.2.2 et 3.2.3 ne dépendent pas logiquement de la remarque 3.2.1 qui précède.

3.2.2. Montrons que I^2 est principal, engendré par $1+x$.
L'idéal I^2 est engendré par les éléments $(1+x)^2, (1+x)y$, et $y^2 = (1+x)(1-x)$; mettant $1+x$ en facteur, il suffit de voir que l'idéal engendré par $1+x$, y et $1-x$ est égal à A ; or, il contient $(1+x)+(1-x) = 2$,

[1] Cet argument me semble plus compréhensible que celui proposé dans [1], p.72 et 73. D'ailleurs, en général, la considération d'applications normes - parce qu'elles sont multiplicatives - est particulièrement indiquée dans les questions d'irréductibilité.

qui est un élément inversible.

3.2.3. L'idéal I n'est pas principal.

Raisonnons par l'absurde en supposant que $I = aA$. On a alors $(1+x)A = I^2 = a^2A$; en particulier, il existe des éléments b et c dans A tels que $a^2 = (1+x)b$ et $1+x = a^2c$. Ces éléments sont inverses l'un de l'autre puisque $1+x = (1+x)bc$, et que A est intègre.

Prenant les normes des deux membres de l'égalité $a^2 = (1+x)b$, on trouve

$$N(a)^2 = (1+x)^2 N(b).$$

Comme b est inversible, $N(b)$ est un élément inversible de $\mathbf{R}[X]$, c'est-à-dire une constante non nulle ; par suite, $N(a)$ est un polynôme de degré 1. C'est impossible.

3.4. L'analogue algébrique du revêtement $v \mapsto v^2$

Dans ce paragraphe et le suivant on indique comment rendre l'idéal I principal en passant de A à un sur-anneau un peu plus gros. Une première méthode consiste à algébriser le lemme 1.1.2 qui montre que l'application $v \mapsto v^2$ transforme le ruban de Möbius en un cylindre. En termes des coordonnées réelles (x, y) (de sorte que $v = x + iy$), cette application s'écrit

$$(x, y) \longmapsto (x^2 - y^2, 2xy).$$

Cela indique ce qu'il faut faire.

Pour définir le morphisme de $\mathbf{R}$-algèbres $\alpha : A \to A$ correspondant à $v \mapsto v^2$, il est plus clair d'écrire, dans le second anneau, l'anneau « but », ξ et η, à la place de x et de y. On pose alors

$$\alpha(x) = \xi^2 - \eta^2, \qquad \alpha(y) = 2\xi\eta.$$

Cela définit bien un morphisme de $\mathbf{R}$-algèbres puisque l'image de $x^2 + y^2 - 1$ est $(\xi^2 - \eta^2)^2 + 4\xi^2\eta^2 - 1 = (\xi^2 + \eta^2)^2 - 1 = 0$. L'idéal engendré par $\alpha(I)$ est engendré par $\alpha(1+x) = 1 + \xi^2 - \eta^2 = 2\xi^2$ et $\alpha(y) = 2\xi\eta$; comme l'idéal engendré par ξ et η est égal à A (puisqu'il contient $1 = \xi^2 + \eta^2$), on voit que

$$\alpha(I)A = \xi A.$$

3.5. Complexifier A

3.4.1. Considérons l'anneau A comme un sous-anneau de $B = \mathbf{C}[X, Y]/(X^2 + Y^2 - 1)$.

L'anneau B est principal. En effet, l'isomorphisme de $\mathbf{C}$-algèbres

$$\mathbf{C}[X, Y] \longrightarrow \mathbf{C}[Z, Z'], \qquad X \mapsto \frac{1}{2}(Z + Z'),\ Y \mapsto \frac{1}{2i}(Z - Z'),$$

donne par passage aux quotients un isomorphisme

$$\mathbf{C}[X, Y]/(X^2 + Y^2 - 1) \quad \widetilde{\longrightarrow} \quad \mathbf{C}[Z, Z']/(ZZ' - 1).$$

Ainsi B est isomorphe à l'anneau de fractions $\mathbf{C}[Z]_Z$ (Voir, par exemple, [1], p. 55 et 71, ou bien, plus bas, 4.1.3).

D'ailleurs, il est clair que l'élément $b = 1 + x + iy \in IB$ engendre cet idéal puisque

$$1 + x = \frac{1}{2}(1 + x - iy)(1 + x + iy), \qquad \text{et} \qquad y = \frac{1}{2i}(1 - x + iy)(1 + x + iy).$$

3.4.2. On va préciser les relations entre A et B. Notons que $B = A[i]$ (ce qui justifie le titre du paragraphe) : en effet, chaque élément de B s'écrit de façon unique sous la forme $p(x) + yq(x)$, où p et q sont des polynômes à coefficients complexes ; on peut donc les décomposer en $p = p' + ip''$, et $q = q' + iq''$, où

les quatres polynômes écrits sont à coefficients réels ; mais alors, $p + yq = (p' + yq') + i(p'' + yq'')$.

On peut donc définir un automorphisme de conjugaison $b \mapsto \bar{b}$, qui ne porte que sur les coefficients des divers polynômes, et qui laisse invariants x et y ; avec cette notation, on a pour tout $b \in B$, l'équivalence $b \in A \Leftrightarrow b = \bar{b}$.

Introduisons les corps des fractions K et L, respectivement de A et B ; on a le diagramme commutatif de morphismes d'inclusion :

$$\begin{array}{ccc} A & \longrightarrow & B \\ \downarrow & & \downarrow \\ K & \longrightarrow & L \end{array}$$

Montrons l'égalité $K \cap B = A$.

Il est - ou devrait - être clair que $K[i] = L$, donc que K est le sous-corps de L formé des éléments invariants sous la conjugaison invoquée ci-dessus ; si un tel élément est aussi dans B, alors il est dans A.

Cela implique, en particulier, que A est *intégralement clos*, autrement dit qu'un élément de K qui est racine d'un polynôme unitaire $F(T) \in A[T]$ est dans A : en effet, un tel élément, vu dans L est dans B puisque B est principal, donc intégralement clos (PERRIN, p.61).

4. Compléments

4.1. Sur certains anneaux principaux

Proposition 4.1.1. *Soient A un anneau principal de corps des fractions K, et B un sous-anneau de K contenant A : $A \subset B \subset K$. Alors B est principal.*

Montrons d'abord que tout élément $b \in B$ s'écrit sous la forme $b = a/s$, où s est un élément de A qui admet un inverse dans B : comme A est principal, on peut choisir une écriture de b comme une fraction a/s « réduite », c'est-à-dire telle que a et s soient premiers entre eux ; le théorème de Bézout affirme alors l'existence de u et v dans A tels que $au + sv = 1$, ce qui s'écrit aussi : $(bu + v)s = 1$; l'élément $bu + v \in B$ est donc l'inverse de s.

Montrons que tout idéal J de B est principal. L'idéal $J \cap A$ de A est principal, engendré, disons, par a. Pour un élément $b \in J$ il existe, d'après ce qui précède, un $s \in A \cap B^\times$ tel que $sb \in A \cap J = aA$, c'est-à-dire $sb = at$, avec $t \in A$. On a donc $b = a.\frac{t}{s}$, et $\frac{t}{s}$ est dans B puisque s est inversible dans B. Donc $J = aB$.

Proposition 4.1.2. *Soit A un anneau intègre, de corps des fractions K. Considérons un élément non nul $t \in A$, et le morphisme de A-algèbres $A[T] \longrightarrow K$, $\quad P(T) \mapsto P(1/t)$. Alors le noyau de ce morphisme est l'idéal engendré par $tT - 1$, et son image, notée A_t, est le sous-anneau de K formé des factions de la forme a/t^m.*

Soit $P(T) = a_n T^n + \cdots + a_0$ un polynôme tel que $P(1/t) = 0$, c'est-à-dire tel que $a_n + a_{n-1}t + \cdots + a_0 t^n = 0$; en regroupant les n derniers termes, on peut écrire $a_n = tb$, avec $b \in A$. Mais alors le polynôme $P(T) - bT^{n-1}(tT - 1)$ est encore dans le noyau et son degré est $\leq n - 1$; on conclut par récurrence sur le degré.

Corollaire 4.1.3. *Pour tout corps k, l'anneau $k[X, Y]/(XY - 1)$ est principal.*

En effet, il est isomorphe au sous-anneau $k[X]_X \subset k(X)$, lequel est principal d'après 4.1.1.

4.2. Sur certains anneaux factoriels

Un anneau principal est factoriel (PERRIN II 3.21), et il existe des anneaux factoriels qui ne sont pas principaux, par exemple $\mathbf{Z}[X]$.

Voici une situation où un anneau factoriel est nécessairement principal ; ce n'est pas la plus générale, mais c'est la situation plus fréquemment rencontrée au niveau de l'agrégation.

Proposition *Soient R un anneau principal contenu dans un anneau A ; on suppose que A est un R-module libre de rang fini. Alors, si A est factoriel, il est principal.*

Un idéal I de A est, en particulier, un sous-R-module du R-module libre de type fini A ; c'est donc un R-module (libre et) de type fini ; en particulier c'est un idéal de A de type fini. Pour montrer qu'il est principal, on peut donc se ramener, par récurrence, au cas où il est engendré par deux éléments a et b ; soit d un plus grand diviseur commun (A est supposé factoriel) ; écrivons $a = da'$ et $b = db'$, de sorte que a' et b' n'ont pas de diviseur commun non inversible ; on a $aA + bA = d(a'A + b'A)$.

Il reste donc à démontrer que si deux éléments a et b de A n'ont pas de diviseur commun non inversible, alors $aA + bA = A$.

Si a est inversible, $aA = A$ et on a fini ; sinon, a est un produit d'éléments irréductibles de A. Or, si l'on peut décomposer a en un produit $a = a'a''$ tel que $a'A + bA = A$ et $a''A + bA = A$; alors on peut conclure $aA + bA = A$. En effet, par hypothèse, on a des relations de le forme $a'x' + by' = 1$ et $a''x'' + by'' = 1$, d'où, par produit, $a'a''x'x'' + b(a'x'y'' + a''x''y' + by'y'') = 1$. Par récurrence sur le nombre de facteurs irréductibles de a, il suffit donc de traiter le cas où a est irréductible ; l'hypothèse sur a et b signifie alors que a ne divise pas b, c'est-à-dire que $b \notin aA$, et il faut conclure que $aA + bA = A$; autrement dit, il faut montrer que l'idéal aA est *maximal*. En changeant la notation, et en utilisant le fait que dans un anneau factoriel, un élément irréductible est premier, on est ramené à démontrer ceci : *si p est un élément premier non nul de A, alors l'idéal pA est maximal, i.e A/pA est un corps.*

Montrons d'abord que l'idéal $pA \cap R$ est non nul. L'application $u : A \to A,\ a \mapsto pa$ est un endomorphisme R-linéaire du R-module libre A ; la « transposée de la comatrice » fournit un endomorphisme v tel que $u(v(a)) = \det(u)a$; pour $a = 1$ on a $\det(u) = u(v(1)) = pv(1) \in pA \cap R$; mais u est injectif puisque A est intègre, donc $\det(u)$ est non nul[2]

En passant aux quotients, on obtient un homomorphisme *injectif* d'anneaux

$$R/pA \cap R \longrightarrow A/pA.$$

Comme pA est premier, l'anneau A/pA est intègre, donc son sous-anneau $R/pA \cap R$ l'est aussi ; l'idéal $pA \cap R$ est donc premier, et par suite maximal puisqu'il est non nul et que R est principal ; bref, $R/pA \cap R$ est un corps, et l'anneau intègre A/pA apparaît comme un espace vectoriel de dimension finie sur ce corps ; on en déduit que A/pA est un corps, en invoquant le lemme classique suivant.

Lemme *Un anneau intègre S qui est un espace vectoriel de dimension finie sur un sous-corps K, est lui-même un corps.*

En effet, si $s \in S$ est un élément non nul, la multiplication par s est un endomorphisme injectif de S, puisque S est intègre, donc bijectif car S est un vectoriel de dimension finie sur le sous-corps K ; l'élément unité 1 est donc dans l'image de cet endomorphisme ; ainsi s admet un inverse.

[2]Soit K le corps des fractions de R, et soit $(e_1, \ldots, e_m)$ une base du R-module A. La matrice $M = (a_{ij}) \in \mathbf{M}(m, R) \subset \mathbf{M}(m, K)$ de u permet de définir un endomorphisme de K^m qui est encore injectif, comme on le voit en réduisant au même dénominateur les coordonées d'un vecteur de son noyau. Cet endomorphisme de K^m est donc bijectif ; par suite son déterminant est non nul.

Références

[1] S. FRANCINOU et H. GIANELLA. *Exercices de mathématiques pour l'agrégation, Algèbre 1*, Paris, Masson,1997.
[2] D. PERRIN. *Cours d'algèbre*, Paris, Ellipses, 1996.
[3] C. GODBILLON. *Éléments de topologie algébrique*, Paris, Hermann, 1971.
[4] J. STILLWELL. *Geometry of Surfaces*, New York, Springer-Verlag, 1992.
[5] R. SWAN. *Vector Bundles and Projective Modules*, Trans. Amer. Math. Soc., Vol. 105, No 2 (Nov. 1962), 264-277.