DÉCRYPTAGE CONSTRUCTIF DES PREUVES CLASSIQUES, UN CAS D'ÉCOLE: LE THÉORÈME D'ARTIN EN THÉORIE DE GALOIS

par

Henri Lombardi & Claude Quitté

Résumé. — Nous traitons avec le théorème d'Artin un « cas d'école » pour le décryptage constructif des preuves classiques qui utilisent le principe du tiers exclu et l'axiome du choix.

***Abstract* (Constructive Deciphering of Artin Theorem in Galois Theory)**
We give a constructive deciphering of a standard proof of Artin Theorem in Galois theory.

Table des matières

Introduction

Dans cette note nous examinons le théorème d'Artin en théorie de Galois et sa version « anneaux commutatifs ». Nous montrons comment décrypter certaines preuves classiques usuelles (qui utilisent le principe du tiers exclu et l'axiome du choix) en des preuves constructives.

Nous nous inspirons à la fois de [**3**] et [**4**].

Il s'agit ici d'un « cas d'école » pour le décryptage des preuves classiques, dans la mesure où une preuve constructive élémentaire du théorème le plus fort peut être obtenue de façon beaucoup plus directe (voir section 3).

1. Le lemme de Dedekind et le théorème d'Artin

On prendra les notations suivantes.

Notations 1. — $(\mathbf{L}, +, -, ., 0, 1)$ est un corps, $(M, ., 1)$ un monoïde, σ_i, $i = 1 \dots, n$ sont des homomorphismes du monoïde M dans le monoïde multiplicatif du corps. Des éléments x^{ij}, $1 \leq i < j \leq n$ témoignent du fait que les homomorphismes sont deux à deux distincts : on pose $s_{ij} = \sigma_i(x^{ij}) - \sigma_j(x^{ij})$ et on a $s_{ij} \neq 0$ pour tous $i < j$. Dans le cas où $M = \mathbf{L}$ et où les σ_i forment un groupe fini G d'automorphismes de $\mathbf{L}$ on note $\mathbf{K}$ le sous-corps de $\mathbf{L}$ fixé par G : $\mathbf{K} = \{x \in \mathbf{L}\,;\, \sigma(x) = x,\ \forall \sigma \in G\}$.

Rappelons tout d'abord la théorie et la preuve usuelles.

***Classification mathématique par sujets* (2000).** — 03F65, 13C15.
Mots clefs. — Théorème d'Artin, Mathématiques constructives, Décryptage de preuves classiques.

Proposition 2. — (Lemme de Dedekind-Artin)
Avec les notations 1 :

1. *Les homomorphismes σ_i sont $\mathbf{L}$-linéairement indépendants*
2. *Plus précisément, il existe n éléments $y^1, \dots, y^n$ de M tels que la matrice $(\sigma_i(y^j))_{1\leq i,j\leq n}$ soit inversible.*

Démonstration. — On prouve le point 1 par induction, sous la forme suivante

$$\forall \alpha_1, \dots, \alpha_n \in \mathbf{L}, \quad \sum\nolimits_{i=1}^{n} \alpha_i \, \sigma_i = 0 \implies \alpha_1 = \cdots = \alpha_n = 0.$$

Pour $n = 1$, si $\alpha_1 \, \sigma_1 = 0$ alors $\alpha_1 = \alpha_1 \, \sigma_1(1) = 0$. Supposons l'assertion vraie pour $n-1$ et montrons là pour n. Soit une relation de dépendance linéaire

$$\sum\nolimits_{i=1}^{n} \alpha_i \, \sigma_i = 0 \tag{1}$$

Soit $x \in \mathbf{L}$ tel que $\sigma_1(x) \neq \sigma_n(x)$. On a alors pour tout $z \in \mathbf{L}$,

$$\sum_{i=1}^{n} \alpha_i \, \sigma_i(xz) = \sum\nolimits_{i=1}^{n} \alpha_i \, \sigma_i(x) \, \sigma_i(z) = 0$$

ce qui donne

$$\sum_{i=1}^{n} \alpha_i \, \sigma_i(x) \, \sigma_i = 0 \tag{2}$$

Par combinaison linéaire des égalités 1 et 2 on obtient

$$\sum\nolimits_{i=1}^{n-1} \alpha_i \, (\sigma_n(x) - \sigma_i(x)) \, \sigma_i = 0 \tag{3}$$

Par hypothèse de récurrence cela donne $\alpha_i \, (\sigma_n(x) - \sigma_i(x)) = 0$ pour $i = 1, \dots, n-1$. En particulier, puisque $\sigma_1(x) \neq \sigma_n(x)$, $\alpha_1 = 0$. Donc $\sum_{i=2}^{n} \alpha_i \, \sigma_i = 0$ et par hypothèse de récurrence $\alpha_2 = \cdots = \alpha_n = 0$.

Passons au point 2.
Pour $n = 1$ on choisit $1 \in M$, on a bien $\Delta_1 = \left| \ \sigma_1(1) \ \right| = 1 \neq 0$. Pour $n = 2$, si $\sigma_1(x) = x_1 \neq \sigma_2(x) = x_2$ on choisit 1, x et on a bien $\Delta_2 = \begin{vmatrix} 1 & x_1 \\ 1 & x_2 \end{vmatrix} \neq 0$. Supposons maintenant avoir trouvé $n-1$ éléments $1, x, \dots, u$ avec

$$\Delta_{n-1} = \begin{vmatrix} 1 & x_1 & \cdots & u_1 \\ \vdots & \vdots & & \vdots \\ 1 & x_{n-1} & \cdots & u_{n-1} \end{vmatrix} \neq 0$$

(on a posé $x_i = \sigma_i(x), \dots, u_i = \sigma_i(u)$). En un point t arbitraire de M, si on évalue le déterminant

$$\begin{vmatrix} 1 & x_1 & \cdots & u_1 & \sigma_1(t) \\ \vdots & \vdots & & \vdots & \vdots \\ 1 & x_n & \cdots & u_n & \sigma_n(t) \end{vmatrix}$$

en développant selon la dernière colonne, on trouve $\delta_{n,1}\sigma_1(t) + \cdots + \delta_{n,n}\sigma_n(t)$ avec $\delta_{n,n} = \Delta_{n-1} \neq 0$. Mais, d'après le point 1, puisque $\delta_{n,n} \neq 0$ on doit avoir $\delta_{n,1}\sigma_1 + \cdots + \delta_{n,n}\sigma_n \neq 0$. Cela implique qu'il existe un $v \in M$ tel que $\delta_{n,1}\sigma_1(v) + \cdots + \delta_{n,n}\sigma_n(v) \neq 0$, ce qui donne

$$\Delta_n = \begin{vmatrix} 1 & x_1 & \cdots & u_1 & v_1 \\ \vdots & \vdots & & \vdots & \vdots \\ 1 & x_n & \cdots & u_n & v_n \end{vmatrix} \neq 0 \,.$$

□

On a alors comme corollaire.

Théorème 1. — (théorème d'Artin)
Toujours avec les notations 1, dans le cas d'un groupe fini d'automorphismes de $\mathbf{L}$, *les* y^j *donnés dans le point 2 de la proposition 2 forment une base de* $\mathbf{L}$ *sur* $\mathbf{K}$.

Démonstration. — Soit $a \in \mathbf{L}$, on veut l'écrire sous la forme $\sum_{j=1}^n a_j y^j$ avec les a_j dans $\mathbf{K}$. Ceci implique $\sigma_i(a) = \sum_{j=1}^n a_j \sigma_i(y^j)$ pour $i = 1 \ldots, n$. Ceci peut être vu comme un système linéaire de n équations à n inconnues a_i dans $\mathbf{L}$. Par construction ce système linéaire admet une solution unique $(a_1, \ldots, a_n)$ dans $\mathbf{L}^n$. Si on transforme le système linéaire au moyen de l'un quelconque des automorphismes σ dans G, on obtient le même système (seul l'ordre dans lequel sont écrites les équations a changé). Donc, par unicité, $(a_1, \ldots, a_n) = (\sigma(a_1), \ldots, \sigma(a_n))$. Et les a_i sont bien dans $\mathbf{K}$. □

Il est remarquable (et bien connu) que ce théorème assure déjà « la moitié » de la correspondance galoisienne entre sous $\mathbf{K}$-extensions de $\mathbf{L}$ et sous-groupes de G : l'égalité entre le degré de l'extension et l'ordre du groupe d'une part, le caractère injectif de l'application « sous-groupe $\mapsto$ sous $\mathbf{K}$-extension » d'autre part.

Analyse de la preuve du lemme de Dedekind. — Tout d'abord, nous pouvons énoncer précisément un lemme qui correspond à la récurrence dans la preuve du point 1 de la proposition 2. Disons qu'une partie X de M *sépare* $\{\sigma_1, \ldots, \sigma_n\}$ si $\sigma_1|_X, \ldots, \sigma_n|_X$ sont linéairement indépendants. On a démontré le lemme suivant :

Lemme 3. — *Si* X *sépare* $\{\sigma_1, \ldots, \sigma_k\}$, *si* Y *sépare* $\{\sigma_2, \ldots, \sigma_{k+1}\}$ *et si* $\{a\}$ *sépare* $\{\sigma_1, \sigma_{k+1}\}$, *alors* $X \cup a\,X \cup Y$ *sépare* $\{\sigma_1, \ldots, \sigma_{k+1}\}$.

Voyons maintenant pourquoi la preuve de la proposition 2 pose problème du point de vue constructif.

Dans la preuve de la proposition 2, l'indépendance linéaire est vue sous forme négative dans le point 1, tandis que dans le point 2, les y^j forment un système qui témoigne de cette indépendance sous forme positive : l'inversibilité d'une matrice (c'est-à-dire celle de son déterminant).

Le point 2 qui est sous forme positive est obtenu par l'intermédiaire d'un raisonnement par l'absurde et donc les y^j ne sont pas donnés par la preuve sous forme explicite. En effet on a prouvé au point 1 :

$$\forall \alpha_1, \ldots, \alpha_n \in \mathbf{L}, \quad \Big(\forall t \in M \ \ \sum\nolimits_{i=1}^n \alpha_i\, \sigma_i(t) = 0\Big) \implies \alpha_1 = \cdots = \alpha_n = 0.$$

mais on a utilisé pour montrer le point 2 quelque chose d'un peu plus précis :

$$\forall \alpha_1, \ldots, \alpha_n \in \mathbf{L}, \quad \alpha_n \neq 0 \implies \exists v \in M \ \ \sum\nolimits_{i=1}^n \alpha_i\, \sigma_i(v) \neq 0.$$

Par ailleurs dans le fonctionnement de la preuve nous voyons que le monoïde M n'intervient pas directement. Il peut être avantageusement remplacé par son image dans $\mathbf{L}^n$ qui est un monoïde pour la loi multiplicative produit.

Le lemme de Dedekind peut alors être reformulé comme suit, uniquement dans le corps $\mathbf{L}$. Nous supposerons que nous avons un test d'égalité à 0 dans le corps $\mathbf{L}$ (on dit alors que le corps est *discret*).

Lemme 4. — (lemme de Dedekind-Artin, reformulé)
Soit $\mathbf{L}$ *un corps discret. On considère l'espace des vecteurs colonnes* $\mathbf{L}^n$ *comme un monoïde multiplicatif pour la loi produit*

$$^{\mathrm{t}}(a_1, \ldots, a_n) \cdot {}^{\mathrm{t}}(b_1, \ldots, b_n) = {}^{\mathrm{t}}(a_1 b_1, \ldots, a_n b_n).$$

Soit C *une partie finie de* $\mathbf{L}^n$ *qui contient la colonne* $\mathbf{1}$ *et qui « sépare les lignes » (i.e., pour* $1 \leq i < j \leq n$ *il y a une* $c \in C$ *telle que* $c_i \neq c_j$. *Alors dans le monoïde engendré par* C *il y a* n *colonnes linéairement indépendantes.*

Un cas particulièrement simple est fourni si une seule colonne $a = {}^{\mathrm{t}}(a_1, \ldots, a_n)$ sépare toutes les lignes. Alors les colonnes $\mathbf{1}$, a, $a^2, \ldots, a^{n-1}$ forment une matrice de Vandermonde dont le déterminant est clairement non nul. Le lemme de Dedekind peut donc être compris comme une généralisation des déterminants de Vandermonde.

Preuve constructive du lemme 4. — Nous allons maintenant « extraire » de la preuve « par l'absurde » de la proposition 2 donnée précédemment, une preuve constructive explicite du lemme 4.

Puisque le corps est discret, pour démontrer qu'au moins un élément du corps, dans une liste donnée, est inversible, il suffira de réduire à l'absurde l'hypothèse que tous les éléments de la liste sont nuls.

Nous procédons par récurrence sur n. Mais plutôt que de traiter directement le cas général nous regarderons fonctionner les premières étapes.

On notera que nous faisons fonctionner ici une version forte du lemme 3, dans laquelle l'indépendance linéaire est certifiée par un mineur inversible dans une matrice convenable.

Pour $n = 1$ la colonne $\mathbf{1}$ convient.

Pour $n = 2$, soit $c^{1,2}$ une colonne qui sépare les lignes 1 et 2. Les colonnes $\mathbf{1}$ et $x = c^{1,2}$ conviennent :

$$\begin{vmatrix} 1 & x_1 \\ 1 & x_2 \end{vmatrix} = x_2 - x_1 \neq 0$$

Désormais nous notons $c^{i,j}$ une colonne qui sépare les lignes i et j (la notation est ambigüe puisque n n'est pas précisé).

De même nous notons $C^{i,j}$ l'ensemble fini sélectionné comme indiqué à l'étape précédente, lorsqu'on considère les lignes i et j.

Pour $n = 3$: voici un ensemble fini $C^{1,2,3}$ convenable de colonnes : une matrice carrée d'ordre 3 extraite, pour les lignes $1, 2, 3$, est certainement inversible ($x_1 \neq x_2$, $y_1 \neq y_3$, $z_2 \neq z_3$).

$$C^{1,2,3} = C^{1,2} \cup c^{1,3} \cdot C^{1,2} \cup C^{2,3} = \begin{bmatrix} 1 & x_1 & y_1 & x_1y_1 & z_1 \\ 1 & x_2 & y_2 & x_2y_2 & z_2 \\ 1 & x_3 & y_3 & x_3y_3 & z_3 \end{bmatrix}$$

(si une colonne apparaît deux fois dans cette matrice on peut évidemment supprimer sa deuxième occurence). Dans cette matrice nous pouvons garantir que l'un des trois mineurs suivants

$$\begin{vmatrix} 1 & x_1 & y_1 \\ 1 & x_2 & y_2 \\ 1 & x_3 & y_3 \end{vmatrix}, \quad \begin{vmatrix} 1 & x_1 & x_1y_1 \\ 1 & x_2 & x_2y_2 \\ 1 & x_3 & x_3y_3 \end{vmatrix}, \quad \begin{vmatrix} 1 & x_1 & z_1 \\ 1 & x_2 & z_2 \\ 1 & x_3 & z_3 \end{vmatrix},$$

est certainement non nul.

En effet, notons $\delta_{2,1}, \delta_{2,2}, \delta_{2,3}$ les trois mineurs 2×2 extraits sur les deux premières colonnes, de sorte que les mineurs 3×3 ci-dessus sont respectivement égaux à

$$\begin{array}{rcccccc} \alpha & = & \delta_{2,1}\, y_1 & + & \delta_{2,2}\, y_2 & + & \delta_{2,3}\, y_3 \\ \beta & = & \delta_{2,1}\, x_1y_1 & + & \delta_{2,2}\, x_2y_2 & + & \delta_{2,3}\, x_3y_3 \\ \gamma & = & \delta_{2,1}\, z_1 & + & \delta_{2,2}\, z_2 & + & \delta_{2,3}\, z_3 \end{array}$$

Notons aussi que par construction

$$\begin{array}{rcccccccc} \delta & = & \delta_{2,1} & + & \delta_{2,2} & + & \delta_{2,3} & = & 0 \\ \eta & = & \delta_{2,1}\, x_1 & + & \delta_{2,2}\, x_2 & + & \delta_{2,3}\, x_3 & = & 0 \end{array}$$

Par hypothèse de récurrence on sait que $\delta_{2,3} \neq 0$. Si on avait $\alpha = \beta = \gamma = \delta = \eta = 0$, on en déduirait :

$$\begin{array}{rcccccc} \alpha - y_3\delta & = & 0 & = & (y_1 - y_3)\delta_{2,1} & + & (y_2 - y_3)\delta_{2,2} \\ \beta - y_3\eta & = & 0 & = & (y_1 - y_3)\delta_{2,1}x_1 & + & (y_2 - y_3)\delta_{2,2}x_2 \end{array}$$

c'est-à-dire encore

$$\begin{bmatrix} 0 & 0 \end{bmatrix} = \begin{bmatrix} (y_1 - y_3)\delta_{2,1} & y_2 - y_3)\delta_{2,2} \end{bmatrix} \cdot \begin{bmatrix} 1 & x_1 \\ 1 & x_2 \end{bmatrix}.$$

D'où on déduit $(y_1-y_3)\delta_{2,1}=0$ puis $\delta_{2,1}=0$. On a alors $\gamma=\delta_{2,2}z_2+\delta_{2,3}z_3=0$ et $\delta=\delta_{2,2}+\delta_{2,3}=0$, c'est-à-dire

$$\begin{bmatrix} 0 & 0 \end{bmatrix} = \begin{bmatrix} \delta_{2,2} & \delta_{2,3} \end{bmatrix} \cdot \begin{bmatrix} 1 & z_2 \\ 1 & z_3 \end{bmatrix},$$

ce qui implique par hypothèse de récurrence $\delta_{2,2}=\delta_{2,3}=0$, ce qui est absurde.

De la même manière pour $n=4$ nous pouvons prendre une matrice ayant pour colonnes :

$$C^{1,2,3,4} = C^{1,2,3} \cup c^{1,4} \cdot C^{1,2,3} \cup C^{2,3,4}$$

Plus précisément :

$$\begin{bmatrix} 1 & x_1 & y_1 & x_1y_1 & z_1 & u_1 & u_1x_1 & u_1y_1 & u_1x_1y_1 & u_1z_1 & v_1 & v_1z_1 & w_1 \\ 1 & x_2 & y_2 & x_2y_2 & z_2 & u_2 & u_2x_2 & u_2y_2 & u_2x_2y_2 & u_2z_2 & v_2 & v_2z_2 & w_2 \\ 1 & x_3 & y_3 & x_3y_3 & z_3 & u_3 & u_3x_3 & u_3y_3 & u_3x_3y_3 & u_3z_3 & v_3 & v_3z_3 & w_3 \\ 1 & x_4 & y_4 & x_4y_4 & z_4 & u_4 & u_4x_4 & u_4y_4 & u_4x_4y_4 & u_4z_4 & v_4 & v_4z_4 & w_4 \end{bmatrix}$$

où $c^{1,4} = {}^{\mathrm{t}}(u_1,\ldots,u_4)$ avec $u_1 \neq u_4$, $c^{2,4} = {}^{\mathrm{t}}(v_1,\ldots,v_4)$ avec $v_2 \neq v_4$, $c^{3,4} = {}^{\mathrm{t}}(w_1,\ldots,w_4)$ avec $w_3 \neq w_4$.

Nous garantissons que l'un des mineurs extraits qui vont apparaître dans le raisonnement qui suit est certainement non nul. Nous sélectionnons dans $C^{1,2,3}$ (c'est-à-dire parmi les cinq premières colonnes de la matrice ci-dessus) trois colonnes, $\mathbf{1}, x, c$, telles que le mineur 3×3 sur les trois premières lignes est non nul, conformément à l'hypothèse de récurrence.
De même nous sélectionnons dans $C^{2,3,4}$ (c'est-à-dire parmi les colonnes $1, 5, 11, 12, 13$ de la matrice ci-dessus) trois colonnes, $\mathbf{1}, z, e$, telles que le mineur 3×3 sur les trois dernières lignes est non nul, conformément à l'hypothèse de récurrence.
Nous notons $\delta_{3,1}, \delta_{3,2}, \delta_{3,3}, \delta_{3,4}$ les quatre mineurs 3×3 extraits sur les colonnes $\mathbf{1}, x, c$, de sorte que les mineurs 4×4 du type $|\mathbf{1}, x, c, t|$ sont égaux à $\delta_{3,1}t_1+\delta_{3,2}t_2+\delta_{3,3}t_3+\delta_{3,4}t_4$ (avec $\delta_{3,4}=\Delta_3\neq 0$).
On prend pour t les colonnes suivantes : $\mathbf{1}$, x, c, u, $u\cdot x$, $u\cdot c$, z, e.
Si on appelle L_i la i-ème ligne de la matrice obtenue en gardant ces colonnes et si on suppose tous les mineurs $|\mathbf{1}, x, c, t|$ nuls, cela donne $\delta_{3,1}L_1+\delta_{3,2}L_2+\delta_{3,3}L_3+\delta_{3,4}L_4=0$.
Montrons que cette supposition est absurde. Les trois mineurs avec $t=\mathbf{1}, x$ ou c sont nuls par construction. Les trois mineurs avec $t=u$, $u\cdot x$, $u\cdot c$ étant supposés nuls, on obtient par combinaisons linéaires convenables, comme dans le cas $n=3$:

$$\begin{bmatrix} 0 & 0 & 0 \end{bmatrix} = \begin{bmatrix} (u_1-u_4)\delta_{3,1} & (u_2-u_4)\delta_{3,2} & (u_3-u_4)\delta_{3,3} \end{bmatrix} \cdot \begin{bmatrix} 1 & x_1 & c_1 \\ 1 & x_2 & c_2 \\ 1 & x_3 & c_3 \end{bmatrix}.$$

D'où on déduit $(u_1-u_4)\delta_{3,1}=0$, puis $\delta_{3,1}=0$, et donc $\delta_{3,2}L_2+\delta_{3,3}L_3+\delta_{3,4}L_4=0$. En particulier

$$\begin{bmatrix} 0 & 0 & 0 \end{bmatrix} = \begin{bmatrix} \delta_{3,2} & \delta_{3,3} & \delta_{3,4} \end{bmatrix} \cdot \begin{bmatrix} 1 & z_2 & e_2 \\ 1 & z_3 & e_3 \\ 1 & z_4 & e_4 \end{bmatrix}.$$

d'où $\delta_{3,2}=\delta_{3,3}=\delta_{3,4}=0$, ce qui est absurde.

Plus généralement on peut prendre :

$$C^{1,\ldots,n+1} = C^{1,\ldots,n} \cup c^{1,n+1} \cdot C^{1,\ldots,n} \cup C^{2,\ldots,n+1}$$

avec un système convenable de mineurs extraits. Le nombre de colonnes dans la matrice $C^{1,\ldots,n}$ peut être facilement majoré, par exemple par $2\times 3^{n-2}$, et on pourrait trouver une majoration de même style pour le nombre de mineurs concernés.

Nous laissons le soin au lecteur sceptique d'écrire en détail l'étape de récurrence, par exemple en démontrant directement la version forte du lemme 3.

2. Utilisation non triviale de l'anneau trivial

La preuve précédente vaut dans la théorie formelle des corps discrets (les corps avec test d'égalité à 0). On peut l'interpréter en disant que l'hypothèse « les s_{ij} sont inversibles[(1)], mais les mineurs sélectionnés dans la matrice $C^{1,\dots,n}$ sont nuls » conduit à une contradiction dans la théorie des corps.

Un théorème important affirme que lorsqu'un système d'hypothèses de ce type conduit à une contradiction, cela est confirmé par un « certificat algébrique » de type Nullstellensatz (pour un traitement constructif voir par exemple [**1**]). Précisément, si on remplace $\mathbf{L}$ par un anneau commutatif arbitraire $\mathbf{B}$, si on note S le monoïde engendré par les s_{ij} $(1 \leq i < j \leq n)$ et J l'idéal engendré par les mineurs sélectionnés, on a $S \cap J \neq \emptyset$. Ou encore : l'anneau $S^{-1}(\mathbf{B}/J)$ est trivial. Ce résultat est plus général et il implique en particulier que dans le cas des corps, le résultat reste vrai sans l'hypothèse que le corps est discret.

En fait la preuve constructive que nous venons de donner pour le lemme 4, « par l'absurde » en supposant que $\mathbf{L}$ est un corps discret, peut être relue comme une preuve que l'anneau $S^{-1}(\mathbf{B}/J)$ est trivial. L'absurdité dans le corps, c'est que $1 = 0$, mais $1 = 0$ dans $S^{-1}(\mathbf{B}/J)$, c'est justement un résultat concret : on a explicité un élément dans $S \cap J$! C'est ce que Richman [**4**] appelle une utilisation non triviale de l'anneau trivial.

Nous aurons besoin dans le cas général du lemme de recollement suivant. Ce lemme peut être vu comme un cas particulier d'un principe local-global concret qui sert de substitut constructif à un principe local-global abstrait (cf. [**3**]).

Lemme 5. — (Lemme de recollement)
Soit $\mathbf{C}$ *un anneau et* $\alpha_1, \dots, \alpha_n$ *des éléments* comaximaux*, c'est-à-dire tels que*

$$\langle \alpha_1, \dots, \alpha_n \rangle = \langle 1 \rangle .$$

Alors $\mathbf{C}$ *est trivial si et seulement si chacun des anneaux localisés* $\mathbf{C}[1/\alpha_i]$ *est trivial.*

Démonstration. — L'hypothèse signifie une égalité $\alpha_1\beta_1 + \cdots + \alpha_n\beta_n = 1$. Dire que $\mathbf{C}[1/\alpha_i]$ est trivial c'est dire que α_i est nilpotent dans $\mathbf{C}$. A fortiori chaque $\alpha_i\beta_i$ est nilpotent dans $\mathbf{C}$. Enfin une somme d'éléments nilpotents est un élément nilpotent. Donc 1 est nilpotent dans $\mathbf{C}$, donc $1 = 0$ dans $\mathbf{C}$. □

Il peut sembler étonnant qu'une telle suite d'évidences concernant l'anneau trivial puisse avoir une efficacité dans un calcul ou une preuve. C'est pourtant le cas.

C'est l'objet des paragraphes qui suivent.

Pour simplifier l'exposé nous commençons par le cas d'un anneau local, où le lemme de recollement n'est pas nécessaire.

Le lemme de Dedekind pour les anneaux locaux. — Rappelons que la définition constructive d'un anneau local (équivalente en mathématiques classiques à la définition classique) : c'est un anneau dans lequel pour tout x, x ou $1 + x$ est inversible.

De plus un corps arbitraire (comme le corps des réels, ou celui des p-adiques) est toujours un anneau local, même s'il n'est pas discret.

Le théorème suivant sur les anneaux locaux s'applique donc en particulier pour les corps non discrets.

Théorème 2. — (lemme de Dedekind-Artin, version anneaux locaux)
Soit $\mathbf{B}$ *un anneau local,* $(M, ., 1)$ *un monoïde,* σ_i*,* $i = 1 \dots, n$ *des homomorphismes du monoïde* M *dans le monoïde multiplicatif de l'anneau. On suppose que pour* $1 \leq i < j \leq n$ *il existe* $x^{i,j} \in M$ *tel que* $\sigma_i(x^{i,j}) - \sigma_j(x^{i,j})$ *est inversible. Alors il existe* n *éléments* $y^1, \dots, y^n$ *de* M *tels que la matrice* $(\sigma_i(y^j))_{1 \leq i,j \leq n}$ *soit inversible.*

(1) Voir les notations 1

En mathématiques classiques on obtient le théorème 2 en considérant le corps résiduel de l'anneau local et en appliquant la proposition 2.

Pour la preuve constructive, nous ne pouvons appliquer simplement le lemme 4 puisque nous ne supposons pas ici le corps résiduel discret. Nous allons voir néanmoins qu'une très légère modification de la preuve du lemme 4 fournit une preuve constructive du théorème 2.

Nous reformulons d'abord un peu plus précisément le théorème 2, dans le style du lemme 4.

Théorème 2 (reformulé)
Soit $\mathbf{B}$ *un anneau local. On considère le* $\mathbf{B}$*-module des vecteurs colonnes* $\mathbf{B}^n$ *comme un monoïde multiplicatif pour la loi produit*

$$ {}^{\mathrm{t}}(a_1,\dots,a_n)\cdot {}^{\mathrm{t}}(b_1,\dots,b_n) = {}^{\mathrm{t}}(a_1b_1,\dots,a_nb_n). $$

Soit C *une partie finie de* $\mathbf{B}^n$ *qui contient la colonne* $\mathbf{1}$ *et qui « sépare les lignes » : i.e., pour* $1 \le i < j \le n$ *il y a une colonne* $c \in C$ *telle que* $c_i - c_j$ *soit inversible. Alors dans le monoïde engendré par* C *il y a* n *colonnes dont le déterminant* $n \times n$ *est inversible.*

Preuve constructive. — Pour $n = 1$ ou 2 il n'y a rien à faire.
Cas $n = 3$:
Considérons trois colonnes x, y, z de C, telles que $x_1 - x_2$, $y_1 - y_3$ et $z_2 - z_3$ sont inversibles. Notons $J_{1,2,3}$ l'idéal engendré par les trois mineurs respectivement basés sur les colonnes $(\mathbf{1}, x, y)$, $(\mathbf{1}, x, xy)$, $(\mathbf{1}, x, z)$. Alors la preuve écrite page 46 peut être vue comme une preuve du fait que l'anneau $\mathbf{C} = \mathbf{B}/J_{1,2,3}$ est trivial. Pour la lectrice sceptique, nous réécrivons la chose. L'idéal $J_{1,2,3}$ est engendré par les trois mineurs suivants

$$ \begin{vmatrix} 1 & x_1 & y_1 \\ 1 & x_2 & y_2 \\ 1 & x_3 & y_3 \end{vmatrix}, \quad \begin{vmatrix} 1 & x_1 & x_1y_1 \\ 1 & x_2 & x_2y_2 \\ 1 & x_3 & x_3y_3 \end{vmatrix}, \quad \begin{vmatrix} 1 & x_1 & z_1 \\ 1 & x_2 & z_2 \\ 1 & x_3 & z_3 \end{vmatrix}, $$

qui sont nuls dans $\mathbf{C}$. Notons $\delta_{2,1}, \delta_{2,2}, \delta_{2,3}$ les trois mineurs 2×2 extraits sur les deux premières colonnes, de sorte que les mineurs 3×3 ci-dessus sont respectivement égaux à $\alpha = \delta_{2,1}y_1 + \delta_{2,2}y_2 + \delta_{2,3}y_3$, $\beta = \delta_{2,1}x_1y_1 + \delta_{2,2}x_2y_2 + \delta_{2,3}x_3y_3$ et $\gamma = \delta_{2,1}z_1 + \delta_{2,2}z_2 + \delta_{2,3}z_3$. Notons aussi que par construction $\eta = \delta_{2,1}x_1 + \delta_{2,2}x_2 + \delta_{2,3}x_3 = 0$ et $\delta = \delta_{2,1} + \delta_{2,2} + \delta_{2,3} = 0$. On sait que $\delta_{2,3}$ est inversible. Puisque $\alpha = \beta = \gamma = \delta = \eta = 0$ dans $\mathbf{C}$, on en déduit :

$$ \begin{array}{rcl} \alpha - y_3\delta & = & 0 \quad = \quad (y_1 - y_3)\delta_{2,1} \quad + \quad (y_2 - y_3)\delta_{2,2} \\ \beta - y_3\eta & = & 0 \quad = \quad (y_1 - y_3)\delta_{2,1}x_1 \quad + \quad (y_2 - y_3)\delta_{2,2}x_2 \end{array} $$

c'est-à-dire encore

$$ \begin{bmatrix} 0 & 0 \end{bmatrix} = \begin{bmatrix} (y_1 - y_3)\delta_{2,1} & y_2 - y_3)\delta_{2,2} \end{bmatrix} \cdot \begin{bmatrix} 1 & x_1 \\ 1 & x_2 \end{bmatrix}. $$

D'où on déduit $(y_1 - y_3)\delta_{2,1} = 0$ (parce que $\delta_{2,3}$ est inversible) puis $\delta_{2,1} = 0$ (parce que $(y_1 - y_3)$ est inversible). On a alors $\gamma = \delta_{2,2}z_2 + \delta_{2,3}z_3 = 0$ et $\delta = \delta_{2,2} + \delta_{2,3} = 0$, c'est-à-dire

$$ \begin{bmatrix} 0 & 0 \end{bmatrix} = \begin{bmatrix} \delta_{2,2} & \delta_{2,3} \end{bmatrix} \cdot \begin{bmatrix} 1 & z_2 \\ 1 & z_3 \end{bmatrix}, $$

ce qui implique, puisque $\begin{vmatrix} 1 & z_2 \\ 1 & z_3 \end{vmatrix}$ est inversible, que $\delta_{2,2} = \delta_{2,3} = 0$, or $\delta_{2,3}$ est inversible, donc $\mathbf{C}$ est trivial.
Ainsi il existe $\alpha, \beta, \gamma \in \mathbf{B}$ avec $\alpha\,|\mathbf{1}, x, y| + \beta\,|\mathbf{1}, x, xy| + \gamma\,|\mathbf{1}, x, z| = 1$. Puisque l'anneau est local cela implique que l'un des trois mineurs $|\mathbf{1}, x, y|$, $|\mathbf{1}, x, xy|$, $|\mathbf{1}, x, z|$ est inversible.

Cas $n = 4$:
Soient x, y, z, u, v, w six colonnes de C, telles que les éléments $x_1 - x_2$, $y_1 - y_3$, $z_2 - z_3$, $u_1 - u_4$, $v_2 - v_4$ et $w_3 - w_4$ sont inversibles. D'après ce qu'on a vu pour le cas $n = 3$, un des 3 générateurs de $J_{1,2,3}$ (celui correspondant aux colonnes $\mathbf{1}, x, c$) et l'un des 3 générateurs de $J_{2,3,4}$ (celui correspondant aux colonnes $\mathbf{1}, z, e$) sont inversibles. Notons alors $J_{1,2,3,4}$ l'idéal engendré par les mineurs 4×4

correspondant aux 4 premières lignes et aux colonnes $\mathbf{1}, x, c, t$ où on prend pour t les colonnes suivantes : $\mathbf{1}$, x, c, u, $u \cdot x$, $u \cdot c$, z, e. Alors la preuve page 47 montre que l'anneau $\mathbf{C} = \mathbf{B}/J_{1,2,3,4}$ est trivial. Pour le lecteur sceptique, nous réécrivons la chose.
On appelle L_i la i-ème ligne de la matrice obtenue en gardant les colonnes citées ci-dessus et puisque tous les mineurs $|\mathbf{1}, x, c, t|$ sont nuls dans $\mathbf{C}$, cela donne $\delta_{3,1}L_1 + \delta_{3,2}L_2 + \delta_{3,3}L_3 + \delta_{3,4}L_4 = 0$.
En considérant les mineurs avec $t = \mathbf{1}$, x, c et ceux avec $t = u$, $u \cdot x$, $u \cdot c$, on obtient par combinaisons linéaires convenables :

$$\begin{bmatrix} 0 & 0 & 0 \end{bmatrix} = \begin{bmatrix} (u_1 - u_4)\delta_{3,1} & (u_2 - u_4)\delta_{3,2} & (u_3 - u_4)\delta_{3,3} \end{bmatrix} \cdot \begin{bmatrix} 1 & x_1 & c_1 \\ 1 & x_2 & c_2 \\ 1 & x_3 & c_3 \end{bmatrix}.$$

D'où on déduit $(u_1 - u_4)\delta_{3,1} = 0$, et puisque $(u_1 - u_4)$ est inversible, $\delta_{3,1} = 0$. Donc $\delta_{3,2}L_2 + \delta_{3,3}L_3 + \delta_{3,4}L_4 = 0$. En particulier

$$\begin{bmatrix} 0 & 0 & 0 \end{bmatrix} = \begin{bmatrix} \delta_{3,2} & \delta_{3,3} & \delta_{3,4} \end{bmatrix} \cdot \begin{bmatrix} 1 & z_2 & e_2 \\ 1 & z_3 & e_3 \\ 1 & z_4 & e_4 \end{bmatrix}.$$

Or le déterminant de la matrice carrée ci-dessus est inversible (dans $\mathbf{B}$ donc a fortiori dans $\mathbf{C}$) et donc $\delta_{3,2} = \delta_{3,3} = \delta_{3,4} = 0$. Or

$$\delta_{3,4} = \begin{vmatrix} 1 & x_1 & c_1 \\ 1 & x_2 & c_2 \\ 1 & x_3 & c_3 \end{vmatrix}$$

est inversible dans $\mathbf{C}$, donc $\mathbf{C}$ est trivial.
Puisque l'anneau est local cela implique que l'un des mineurs $|\mathbf{1}, x, c, t|$ où t est l'une des colonnes u, $u \cdot x$, $u \cdot c$, z, e est inversible.

La preuve complète peut se faire par récurrence, mais nous laissons ce soin à la lectrice courageuse. □

Une forme générale du lemme de Dedekind. — En mathématiques classiques on déduit facilement du lemme de Dedekind (proposition 2) le théorème suivant, au moyen d'une zornette. C'est une généralisation de l'identité algébrique que nous avons signalée au début de la section 2.

Théorème 3. — (lemme de Dedekind-Artin, version anneaux commutatifs)
Soit $\mathbf{B}$ *un anneau commutatif,* $(M, ., 1)$ *un monoïde,* σ_i, $i = 1 \dots, n$ *des homomorphismes du monoïde* M *dans le monoïde multiplicatif de l'anneau. On suppose que pour* $1 \leq i < j \leq n$ *l'idéal* $I_{i,j}$ *engendré par les* $\sigma_i(x) - \sigma_j(x)$ *(lorsque* x *parcourt* M*) contient* 1*. Considérons l'idéal* J *engendré par les déterminants de* n *colonnes du type* ${}^{\mathrm{t}}(\sigma_1(x), \dots, \sigma_n(x))$*. Cet idéal contient* 1*.*

Preuve classique. — Si $1 \notin J$ soit $\mathfrak{m}$ un idéal maximal contenant J. Dans le corps $\mathbf{B}/\mathfrak{m}$ les hypothèses de la proposition 2 sont vérifiées. Donc l'idéal J contient un élément inversible dans $\mathbf{B}/\mathfrak{m}$. Ceci est en contradiction avec $J \subset \mathfrak{m}$. □

Voici maintenant la même preuve, mais constructive.

Démonstration. — La « même » preuve, constructive
Nous reformulons un peu plus précisément le théorème précédent, dans le style du lemme 4.

Théorème 3 (reformulé)
Soit $\mathbf{B}$ *un anneau commutatif. On considère le* $\mathbf{B}$*-module des vecteurs colonnes* $\mathbf{B}^n$ *comme un monoïde multiplicatif pour la loi produit* (${}^{\mathrm{t}}(a_1, \dots, a_n) \cdot {}^{\mathrm{t}}(b_1, \dots, b_n) = {}^{\mathrm{t}}(a_1b_1, \dots, a_nb_n)$*). Soit* C *une partie finie de* $\mathbf{B}^n$ *qui contient la colonne* $\mathbf{1}$ *et qui « sépare les lignes » : i.e.,* $\langle c_i - c_j \,;\, c \in C \rangle = \mathbf{B}$ *(pour* $1 \leq i < j \leq n$*). Alors dans le monoïde engendré par* C *on peut extraire une matrice finie dont les mineurs* $n \times n$ *sont comaximaux.*

Remarques. — 1) Une telle matrice est souvent appelée unimodulaire, l'unimodularité est équivalente à la surjectivité de l'application linéaire correspondante.
2) Dans la preuve qui suit on va voir que dans le monoïde engendré par C, on n'utilise que les éléments qui sont produits d'au plus $n-1$ éléments de C.

Pour $n = 1$ ou 2 il n'y a rien à faire.
Pour $n \geq 3$ on va reprendre la preuve donnée dans le cas local en utilisant le lemme de recollement 5). Comme dans le cas local nous ne traiterons en détail que les cas $n = 3$ et $n = 4$.
Tout d'abord avec $n = 3$.
Considérons d'abord le cas où x, y, z sont trois colonnes de C, telles que $x_1 - x_2$, $y_1 - y_3$ et $z_2 - z_3$ sont inversibles. Notons $J_{1,2,3}$ l'idéal engendré par les trois mineurs respectivement basés sur les colonnes $(\mathbf{1}, x, y)$, $(\mathbf{1}, x, xy)$, $(\mathbf{1}, x, z)$. Alors la preuve du cas analogue pour un anneau local fonctionne sans changement aucun comme une preuve du fait que l'anneau $\mathbf{C} = \mathbf{B}/J_{1,2,3}$ est trivial.
Dans le cas général pour chaque colonne x qui intervient pour certifier que l'idéal engendré par les $x_1 - x_2$ contient 1, pour chaque colonne y qui intervient pour certifier que l'idéal enegendré par les $y_1 - y_3$ contient 1, et pour chaque colonne z qui intervient pour certifier que l'idéal engendré par les $z_2 - z_3$ contient 1, on note $J_{1,2,3}^{x,y,z}$ l'idéal engendré par les trois mineurs respectivement basés sur les colonnes $(\mathbf{1}, x, y)$, $(\mathbf{1}, x, xy)$, $(\mathbf{1}, x, z)$. D'après le cas particulier examiné en premier, si $\mathbf{B}_{1,2,3}^{x,y,z} = \mathbf{B}[1/(x_1 - x_2)(y_1 - y_3)(z_2 - z_3)]$ on sait que $\mathbf{B}_{1,2,3}^{x,y,z}/J_{1,2,3}^{x,y,z}$ est trivial. Si nous définissons $J_{1,2,3}$ comme la somme des $J_{1,2,3}^{x,y,z}$, nous avons a fortiori l'anneau $\mathbf{B}_{1,2,3}^{x,y,z}/J_{1,2,3}$ qui est trivial. Enfin puisque par hypothèse les $(x_1 - x_2)(y_1 - y_3)(z_2 - z_3)$ sont comaximaux (lorsqu'on fait parcourir à x, y et z les colonnes convenables), le lemme de recollement nous dit que l'anneau $\mathbf{B}/J_{1,2,3}$ est trivial.

Voyons maintenant le cas $n = 4$.
Commençons par examiner le cas particulier où x, y, z, u, v, w sont six colonnes de C, telles que les éléments $x_1 - x_2$, $y_1 - y_3$, $z_2 - z_3$, $u_1 - u_4$, $v_2 - v_4$ et $w_3 - w_4$ sont inversibles. Supposons aussi que l'un des 3 générateurs de $J_{1,2,3}$ (celui correspondant aux colonnes $\mathbf{1}, x, c$) et l'un des 3 générateurs de $J_{2,3,4}$ (celui correspondant aux colonnes $\mathbf{1}, z, e$) sont inversibles. Notons alors $J_{1,2,3,4}$ l'idéal engendré par les mineurs 4×4 correspondant aux 4 premières lignes et aux colonnes $\mathbf{1}, x, c, t$ où on prend pour t les colonnes suivantes : $\mathbf{1}$, x, c, u, $u \cdot x$, $u \cdot c$, z, e. Alors la preuve donnée dans la cas d'un anneau local fonctionne sans changement aucun pour montrer que l'anneau $\mathbf{C} = \mathbf{B}/J_{1,2,3,4}$ est trivial. Enfin, comme dans le cas $n = 3$, le cas général se déduit de l'étude du cas particulier en utilisant le lemme de recollement et l'hypothèse de récurrence. □

Une version du théorème d'Artin valable pour les anneaux commutatifs (algèbres galoisiennes). — Elle est obtenue comme corollaire du théorème 3 de la même manière que le théorème d'Artin pour les corps était un corollaire de la proposition 2.

Théorème 4. — (théorème d'Artin, version anneaux commutatifs : algèbres galoisiennes)
Soit $\mathbf{B}$ *un anneau commutatif,* σ_i, $i = 1 \ldots, n$ *des automorphismes de* $\mathbf{B}$*, avec* $\sigma_1 = \mathrm{Id}$*, qui forment un groupe fini* G *« séparant », au sens suivant : pour* $2 \leq i \leq n$ *l'idéal engendré par l'image de l'application* $\sigma_i - \mathrm{Id}$ *contient* 1*. On note* $\mathbf{A}$ *le sous-anneau de* $\mathbf{B}$ *fixé par* G *:* $\mathbf{A} = \{x \in \mathbf{B}\,;\, \sigma(x) = x,\ \forall \sigma \in G\}$*. Alors* $\mathbf{B}$ *est un* $\mathbf{A}$*-module projectif de type fini de rang constant* n *et* $\mathbf{A}$ *est facteur direct dans* $\mathbf{B}$*.*

Remarque. — Une étude des *algèbres galoisiennes*, c'est-à-dire des triplets $(\mathbf{A}, \mathbf{B}, G)$ comme ci-dessus est faite dans [**2**].

Démonstration. — On a une combinaison $\mathbf{B}$-linéaire de mineurs qui est égale à 1, selon le théorème 3. Par construction chacun de ces mineurs δ vérifie $\sigma(\delta) = \pm\delta$ pour chaque $\sigma \in G$.
Donnons d'abord la preuve dans le cas où les σ induisent tous par translation des permutations paires de G (c'est-à-dire l'ordre de G est impair ou, s'il est pair, les 2-Sylow de G ne sont pas cycliques). Les mineurs sont alors dans $\mathbf{A}$. En fait ils ne sont pas seulement comaximaux dans $\mathbf{B}$,

ils le sont aussi dans $\mathbf{A}$. Pour s'en convaincre il suffit de transformer la combinaison linéaire par les $\sigma \in G$ et de faire le produit des combinaisons linéaires obtenues :
Supposons en effet qu'on ait une égalité $\sum_{i=1}^{\ell} b_i\delta_i = 1$, considérons le polynome

$$\prod_{\sigma\in G}\sum_{i=1}^{\ell}\sigma(b_i)X_i = \sum_{m_1+\cdots+m_\ell=|G|} a_{m_1,\ldots,m_\ell}X_1^{m_1}\cdots X_\ell^{m_\ell}\,.$$

Par construction les coefficients $a_{m_1,\ldots,m_\ell}$ sont fixés par G, donc dans $\mathbf{A}$. Il est alors simple de réorganiser la somme

$$1 = \sum_{m_1+\cdots+m_\ell=|G|} a_{m_1,\ldots,m_\ell}\delta_1^{m_1}\cdots\delta_\ell^{m_\ell}\,,$$

dont tous les termes sont dans $\mathbf{A}$, en une somme $\sum_{i=1}^{\ell}\alpha_i\delta_i = 1$, avec les $\alpha_i \in \mathbf{A}$.
Enfin lorsqu'on rend un de ces mineurs inversibles, $\mathbf{B}$ devient libre de rang n sur $\mathbf{A}$ (même preuve que pour le théorème 1).
Donc $\mathbf{B}$ est un $\mathbf{A}$-module projectif de type fini de rang constant n.
Pour voir que $\mathbf{A}$ est facteur direct dans le $\mathbf{A}$-module $\mathbf{B}$, il suffit de le vérifier localement pour chacun des anneaux localisés $\mathbf{A}[1/\delta]$. Or ceci est clair puisque la première colonne de la matrice qui donne le mineur δ est justement la colonne $\mathbf{1}$.
Enfin s'il arrive que $\sigma(\delta) = -\delta$ pour certains $\sigma \in G$, on se débrouille en considérant les δ^2. □

3. Plus simplement

Nous indiquons ici rapidement des preuves constructives élémentaires plus faciles des résultats précédents.

Preuve directe constructive simple du théorème 3. — Comme nous l'avons déjà signalé, les mineurs d'ordre n d'une matrice $M \in \mathbf{B}^{m\times n}$ avec $m \leq n$ engendrent l'idéal $\langle 1\rangle$ si et seulement si la matrice est surjective (une fois qu'on sait que la matrice M est surjective, on peut l'inverser à droite et le fait que ses mineurs $n\times n$ sont comaximaux résulte alors de la formule de Binet-Cauchy).

Nous donnons ici une preuve directe de surjectivité « à la Lagrange ».

Théorème 3 (encore reformulé)
Soit $\mathbf{B}$ *un anneau commutatif. On considère les vecteurs colonnes* $\mathbf{B}^n$ *comme formant une* $\mathbf{B}$*-algèbre (la loi produit est* $({}^{\mathrm{t}}(a_1,\ldots,a_n)\cdot {}^{\mathrm{t}}(b_1,\ldots,b_n) = {}^{\mathrm{t}}(a_1b_1,\ldots,a_nb_n)$*). Soit* C *une partie finie de* $\mathbf{B}^n$ *qui « sépare les lignes » : i.e.,* $\langle c_i - c_j\,;\, c\in C\rangle = \mathbf{B}$ *(pour* $1 \leq i < j \leq n$*). Alors la* $\mathbf{B}$*-algèbre engendrée par* C *est égale à* $\mathbf{B}^n$*.*

La remarque fondamentale est que dans le $\mathbf{B}$-module engendré par $x = {}^{\mathrm{t}}(x_1,\ldots,x_n)$ et $\mathbf{1}$ il y a le vecteur $x - x_2\,\mathbf{1}$ qui est du type ${}^{\mathrm{t}}(x_1 - x_2, 0, \times, \ldots, \times)$ et le vecteur $-x + x_1\,\mathbf{1}$ qui est du type ${}^{\mathrm{t}}(0, x_1 - x_2, \times, \ldots, \times)$. Donc lorsqu'on suppose que l'idéal $I_{1,2}$ engendré par les $x_1 - x_2$ contient 1, cela implique que dans le $\mathbf{B}$-module engendré par C il y a un vecteur $g^{1,2}$ du type ${}^{\mathrm{t}}(1, 0, g_3^{1,2}, \ldots g_n^{1,2})$ et un vecteur $g^{2,1}$ du type ${}^{\mathrm{t}}(0, 1, g_3^{2,1}, \ldots g_n^{2,1})$. Même chose en remplaçant 1 et 2 par deux entiers $i < j \leq n$.

On en déduit que ${}^{\mathrm{t}}(1, 0, 0, \ldots, 0) = g^{1,2}\cdot g^{1,3}\cdots g^{1,n}$, est dans la $\mathbf{B}$-algèbre engendrée par C. De même, chaque vecteur de la base canonique de $\mathbf{B}^n$ sera dans la $\mathbf{B}$-algèbre engendrée par C. □

Preuve directe constructive simple du théorème 4. — Les éléments du groupe G sont $\sigma_1 = \mathrm{Id}, \sigma_2, \ldots, \sigma_n$. On note pour $x \in \mathbf{B}$, $\mathrm{Tr}_G(x) = \mathrm{Tr}(x) = \sum_{\sigma\in G}\sigma(x)$. Il est clair que $\mathrm{Tr} : \mathbf{B} \to \mathbf{A}$ est $\mathbf{A}$-linéaire. Puisque les σ_i sont des automorphismes de $\mathbf{B}$, la $\mathbf{B}$-algèbre engendrée par les ${}^{\mathrm{t}}(\sigma_1(x),\ldots,\sigma_n(x))$ est égale au $\mathbf{B}$-module engendré par ces mêmes vecteurs.

D'après la preuve du paragraphe précédent il existe un entier N et des éléments $x_1, \dots, x_N$, $y_1, \dots, y_N \in \mathbf{B}$ tels que

$$\sum_{i=1}^{N} x_i \begin{bmatrix} y_i \\ \sigma_2(y_i) \\ \vdots \\ \sigma_n(y_i) \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix}$$

C'est-à-dire encore, pour $\sigma \in G$

$$\sum_{i=1}^{N} x_i \sigma(y_i) = \begin{cases} 1 & \text{si } \sigma = \mathrm{Id} \\ 0 & \text{sinon} \end{cases} \tag{4}$$

On en déduit que pour tout $z \in \mathbf{B}$, $z = \sum_{i=1}^{N} \mathrm{Tr}(zy_i)\, x_i$. En effet

$$\begin{aligned} \textstyle\sum_{i=1}^{N} \mathrm{Tr}(zy_i)\, x_i &= \textstyle\sum_{i=1}^{N} \sum_{j=1}^{n} \sigma_j(zy_i) x_i \\ &= \textstyle\sum_{j=1}^{n} \sigma_j(z) \left(\sum_{i=1}^{N} \sigma_j(y_i) x_i \right) \\ &= \sigma_1(z) \times 1 + \textstyle\sum_{j=2}^{n} \sigma_j(z) \times 0 \quad = \quad z. \end{aligned}$$

Notons $y_i^\star$ la forme $\mathbf{A}$-linéaire $z \mapsto \mathrm{Tr}(zy_i)$. On a établi que le système

$$((x_1, \dots, x_N), (y_1^\star, \dots, y_N^\star))$$

est un « système de coordonnées » (certains auteurs disent une base) pour le $\mathbf{A}$-module $\mathbf{B}$. Celui-ci est donc projectif de type fini, isomorphe à l'image de la matrice de projection

$$P = (p_{ij})_{1 \le i,j \le N} = (y_i^\star(x_j))_{1 \le i,j \le N} = (\mathrm{Tr}(y_i x_j))_{1 \le i,j \le N}\,.$$

Voyons que ce module projectif de type fini est bien de rang constant n.

D'après (4) on a aussi pour $\sigma, \tau \in G$

$$\sum_{i=1}^{N} \tau(x_i)\sigma(y_i) = \begin{cases} 1 & \text{si } \sigma = \tau \\ 0 & \text{sinon} \end{cases} \tag{5}$$

Posons alors :

$$X = \begin{bmatrix} x_1 & x_2 & \cdots & x_N \\ \sigma_2(x_1) & \sigma_2(x_2) & \cdots & \sigma_2(x_N) \\ \vdots & \vdots & & \vdots \\ \sigma_n(x_1) & \sigma_n(x_2) & \cdots & \sigma_n(x_N) \end{bmatrix}$$

$$Y = \begin{bmatrix} y_1 & y_2 & \cdots & y_N \\ \sigma_2(y_1) & \sigma_2(y_2) & \cdots & \sigma_2(y_N) \\ \vdots & \vdots & & \vdots \\ \sigma_n(y_1) & \sigma_n(y_2) & \cdots & \sigma_n(y_N) \end{bmatrix}$$

D'après (5) on a $X\,{}^{\mathrm{t}}Y = \mathrm{I}_n$. On retrouve que $P = {}^{\mathrm{t}}YX$ est une matrice de projection. En outre P est de rang n, puisque

$$\det(\mathrm{I}_N + \lambda P) = \det(\mathrm{I}_N + \lambda\, {}^{\mathrm{t}}YX) = \det(\mathrm{I}_n + \lambda\, X\, {}^{\mathrm{t}}Y) = (1+\lambda)^n\,,$$

(l'égalité du milieu peut se montrer facilement en complétant les matrices X et Y par des lignes nulles pour en faire des matrices carrées d'ordre N). Enfin la trace Tr est une application $\mathbf{A}$-linéaire surjective de $\mathbf{B}$ sur $\mathbf{A}$ puisque le déterminant de $\mathrm{I}_N + \lambda P$ a le coefficient de degré n égal à 1 (et ce coefficient est clairement dans l'image de la trace puisque les p_{ij} y sont). Soit $b \in \mathbf{B}$ tel que $\mathrm{Tr}(b) = 1$, la forme linéaire $f : \mathbf{B} \to \mathbf{A}$, $z \mapsto \mathrm{Tr}(bz)$ est surjective et $f(1) = 1$. Donc $\mathbf{B} = \mathbf{A} \oplus \mathrm{Ker}\ f$.

□

Références

[1] Coste M., Lombardi H., Roy M.-F. *Dynamical method in algebra : Effective Nullstellensätze.* Annals of Pure and Applied Logic **111**, (2001) 203–256.

[2] Demeyer F., Ingraham E. *Separable algebras over commutative rings*. Springer Lecture Notes in Mathematics 181 (1971).

[3] Lombardi H., Quitté C. *Constructions cachées en algèbre abstraite (2) Le principe local global*. dans : Commutative ring theory and applications. Eds : Fontana M., Kabbaj S.-E., Wiegand S. Lecture notes in pure and applied mathematics vol 131. M. Dekker. (2002) 461–476.

[4] Richman F. *Non trivial uses of trivial rings.* Proc. Amer. Math. Soc., **103** (1988), 1012–1014.

---

8 novembre 2006

Henri Lombardi, Laboratoire de Mathématiques, UMR CNRS 6623, UFR des Sciences et Techniques, Université de Franche-Comté, 25030 Besançon cedex, France • *E-mail :* `henri.lombardi@univ-fcomte.fr`
Url : `http://hlombardi.free.fr/`

Claude Quitté, Laboratoire de Mathématiques,, SP2MI, Boulevard 3, Teleport 2, BP 179,, 86960 Futuroscope Cedex, France • *E-mail :* `quitte@mathlabo.univ-poitiers.fr`