

Le Groupe $P1$ et ses Sous-Groupes.

I. Outillage Mathématique: Automorphisme et Factorisation Matricielle

PAR YVES BILLIET

*Chimie et Symétrie, Laboratoire de Chimie Inorganique Moléculaire, Université de Bretagne Occidentale,
6 avenue Le Gorgeu, 29283 Brest, France**

(Reçu le 24 mars 1978; accepté le 13 décembre 1978)

Abstract

Nowadays there is a good knowledge of space subgroups but, curiously, the subgroups of the simplest space group $P1$ are poorly known. This is due to the fact that $P1$ is the sole space group possessing only isosymbolic subgroups while more complicated space groups possess extra *translationengleich*, *klassengleich* and other subgroups whose derivation is easier than that of isosymbolic subgroups. Thus the examination of the subgroups of $P1$ has been undertaken. This problem is connected to a large extent with matrix transformations and automorphisms which constitute the mathematical tools developed in this first paper. The subgroups of $P1$ are connected with changes of the unit cell, *i.e.* with matrices having integer coefficients. Such matrices can be decomposed into the products of simpler matrices and reduced to diagonal matrices having integer coefficients. The results of these theoretical considerations will be applied, in a following paper, to subgroups of $P1$.

Les sous-groupes spatiaux après être restés très longtemps dans l'ombre connaissent actuellement un grand intérêt car ils sont à la base de la construction théorique de modèles pour les structures dérivées telles que structures ordonnées, structures déformées, structures pseudosymétriques, *etc.* Grâce aux travaux récemment parus (Bertaut, 1976*a,b*; Billiet, 1973; Billiet, Sayari & Zarrouk, 1978; Boyle & Lawrenson, 1972*a,b*; Neubüser & Wondratschek, 1966*a,b*; Sayari & Billiet, 1977; Sayari, Billiet & Zarrouk, 1978; *etc.*) on sait maintenant dériver sans trop de difficulté de nombreux sous-groupes. Mais curieusement les sous-groupes du groupe spatial le plus simple $P1$ sont mal connus contrairement aux groupes les plus compliqués dont les sous-groupes sont relativement bien connus. Ceci provient du fait que $P1$ est le seul groupe d'espace à ne posséder que des sous-groupes isosymboliques (Billiet,

1973) alors que tous les autres groupes d'espace possèdent en plus des sous-groupes *translationengleich*, des sous-groupes *klassengleich* non isosymboliques (Hermann, 1929) et d'autres types de sous-groupes dont la dérivation est souvent plus aisée que celle des sous-groupes isosymboliques.

Comme le réseau de tout groupe spatial est en quelque sorte le groupe d'espace $P1$, les études sur les sous-groupes *klassengleich* – c'est-à-dire, qui conservent la classe de symétrie d'orientation du groupe de départ – sont nécessairement en relation avec la détermination des 'réseaux dérivés' d'un réseau, † c'est-à-dire, avec les sous-groupes de $P1$. C'est pourquoi nous nous sommes attachés à leur étude.

Malgré plusieurs tentatives négatives dans des directions plus attrayantes, il semble malheureusement que la détermination des sous-groupes de $P1$ doive faire intervenir des notions mathématiques extrêmement abstraites. Toute maille élémentaire d'un sous-groupe est une maille multiple de $P1$ dont les propriétés sont mises en évidence lors de la factorisation de matrices de passage à coefficients entiers; cette branche de la théorie des nombres entiers est particulièrement rebutante pour le physicien et le chimiste (Bourbaki, 1962; *Encyclopaedia Britannica*, 1969). Quant au classement des sous-groupes de $P1$, il repose sur les propriétés des automorphismes du groupe $P1$ et, de l'aveu même d'un algébriste spécialiste de la théorie des groupes 'l'investigation du groupe de tous les automorphismes d'un groupe donné est d'ordinaire très difficile' (Kurosh, 1960).

Aussi invitons-nous le lecteur à s'armer de stoïcisme pour affronter ce premier mémoire où sera mis en place l'outillage mathématique: nous avons essayé de le rendre digestible en multipliant les exemples et en rendant la lecture plus facile par l'utilisation d'abrégés

† Historiquement, pour des raisons venant essentiellement de la diffraction des rayons X, les réseaux 'dérivés' ont d'abord été appelés 'sur-réseaux' (superlattices) alors qu'il aurait mieux valu les appeler 'sous-réseaux' car ils correspondent à un sous-ensemble de noeuds du réseau de départ. Pour éviter toute confusion et toute querelle de langage, nous avons préféré utiliser l'expression 'réseau dérivé' dont l'origine semble due à Buerger (1947).

* English translations, not 'refereed', may be obtained from the author upon request.

viations appelées dans le Tableau 1. Dans un autre mémoire nous utiliserons cet outillage pour énumérer et classer les sous-groupes de $P1$.

Tableau 1. *Abréviations utilisées et propriétés caractéristiques des matrices*

MAOE: matrice d'affinité orthogonale élémentaire; un vecteur de la base est remplacé par un vecteur k fois plus grand (k entier supérieur à 1); le déterminant est égal à k .
 MAOG: matrice d'affinité orthogonale généralisée; produit de MAOE; le déterminant est un entier supérieur à 1.
 MCBE: matrice de changement de base élémentaire; produit de MTBE; la valeur du déterminant est 1.
 MCBG: matrice de changement de base généralisée; produit de MCBE et de MRBG; le déterminant est égal à ± 1 .
 MRBE: matrice de réorientation de base élémentaire; on échange deux vecteurs de la base ou on remplace un vecteur de la base par son opposé; le déterminant vaut -1 .
 MRBG: matrice de réorientation de base généralisée; produit de MRBE; le déterminant vaut ± 1 .
 MRCE: matrice régulière à coefficients entiers; le déterminant est un entier non nul.
 MTBE: matrice de transformation de base élémentaire; on ajoute à un vecteur de la base un multiple entier d'un autre vecteur de la base; le déterminant est égal à 1.
 MTE: matrice de transformation élémentaire; les MAOE, les MRBE et les MTBE sont des MTE.
 MUCE: matrice unimodulaire à coefficients entiers; le déterminant est égal à ± 1 .
 p.g.c.d.: plus grand commun diviseur.

Exemples

$$\text{MTBE: } \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 3 & 0 & 1 \end{bmatrix}; \text{MRBE: } \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}; \begin{bmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix};$$

$$\text{MAOE: } \begin{bmatrix} 1 & 0 & 0 \\ 0 & 5 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

I. Le groupe spatial $P1$

Le groupe spatial tridimensionnel $P1$ est bien connu des cristallographes et des mathématiciens: nous ne rappellerons, dans le détail, les propriétés classiques de ce groupe, qu'afin de mieux préciser le cadre mathématique de cette étude. Pour les mathématiciens, le groupe spatial $P1$ est plus exactement le groupe abélien libre de rang 3 ou encore le \mathbb{Z} -module libre \mathbb{Z}^3 , cas particulier des modules libres \mathbb{Z}^n qui sont des groupes commutatifs à opérateurs sur l'anneau des nombres entiers relatifs \mathbb{Z} . Les propriétés – dont nous parlerons spécialement à propos du groupe $P1$ – sont vraies du groupe spatial bidimensionnel $p1$ et d'une façon générale des modules \mathbb{Z}^n ($n \geq 2$).

1. Les automorphismes de $P1$ et les changements de maille élémentaire

Une maille élémentaire de $P1$ – l'origine n'intervenant pas dans la question – est essentiellement un

repère constitué de trois vecteurs de translations de $P1$, non coplanaires, (A, B, C) , tels que le vecteur V de toute translation de $P1$ puisse s'exprimer par:

$$V = AP + BQ + CR, \quad (1)$$

P , Q et R étant trois nombres entiers relatifs. Le passage à une autre maille élémentaire (A', B', C') et le passage inverse sont caractérisés par une matrice M et son inverse M^{-1} :

$$(A', B', C') = (A, B, C) M$$

$$\text{et } (A, B, C) = (A', B', C') M^{-1}.$$

Les matrices M et M^{-1} sont des matrices régulières à coefficients entiers; leurs déterminants sont des entiers relatifs dont le produit est égal à 1; ces déterminants sont donc égaux à ± 1 ; les matrices M et M^{-1} sont plus précisément des MUCE (Tableau 1). Inversement une maille élémentaire (A, B, C) et une MUCE M quelconques étant connues, le repère (A', B', C') donné par $(A', B', C') = (A, B, C) M$ est une maille élémentaire. En effet, la matrice M^{-1} , inverse d'une MUCE, est une MUCE car:

$$(a) \det M^{-1} = 1/\det M = \pm 1;$$

(b) tout coefficient de M^{-1} est égal, au signe près puisque $\det M = \pm 1$, au cofacteur du terme homologue de la matrice transposée de M , c'est-à-dire, à un nombre entier.

De plus, quelle que soit la translation de vecteur V (cf. relation 1):

$$V = A'P' + B'Q' + C'R' = (A', B', C') \begin{bmatrix} P' \\ Q' \\ R' \end{bmatrix}$$

$$= (A, B, C) M \begin{bmatrix} P' \\ Q' \\ R' \end{bmatrix},$$

$$V = AP + BQ + CR = (A, B, C) \begin{bmatrix} P \\ Q \\ R \end{bmatrix},$$

$$\begin{bmatrix} P' \\ Q' \\ R' \end{bmatrix} = M^{-1} \begin{bmatrix} P \\ Q \\ R \end{bmatrix};$$

et les nombres P' , Q' , R' sont donc des entiers.

L'application de $P1$ sur lui-même qui fait correspondre au vecteur de translation $V = AP + BQ + CR$, le vecteur de translation $V' = A'P' + B'Q' + C'R'$, est un automorphisme de $P1$ car cette application est bijective et, si V_1 et V_2 correspondent à V'_1 et V'_2 , $(V_1 + V_2)$ correspond bien à $(V'_1 + V'_2)$. Inversement considérons la maille élémentaire (A, B, C) et un automorphisme de $P1$; A' , B' et C' désignant les images de A , B et C , par

cet automorphisme, le transformé de $V = AP + BQ + CR$ est $V' = A'P + B'Q + C'R$, quels que soient P, Q et R ; (A', B', C') est bien une maille élémentaire. Donc, à chaque automorphisme de $P1$ correspondent et réciproquement, d'une part, un changement de maille élémentaire et, d'autre part, une MUCE. Si φ_1 et φ_2 sont les automorphismes associés aux changements de maille élémentaire $(A', B', C') = (A, B, C) M_1$ et $(A'', B'', C'') = (A', B', C') M_2$, $\varphi_1 \varphi_2$ est l'automorphisme associé au changement de maille élémentaire $(A'', B'', C'') = (A, B, C) M_1 M_2$. Le groupe des automorphismes de $P1$ est donc isomorphe du groupe \mathcal{S} des MUCE (produit matriciel) et du groupe des changements de maille élémentaire (compositions successives).

2. Les changements de maille quelconque et les sous-groupes du groupe spatial $P1$

Une maille multiple (a, b, c) de $P1$ est un repère constitué par trois vecteurs de translations de $P1$, non coplanaires, tels que (a, b, c) ne soit pas une maille élémentaire. Le passage d'une maille élémentaire (A, B, C) à la maille multiple (a, b, c) peut être caractérisé par une MRCE S (Tableau 1): $(a, b, c) = (A, B, C) S$ et $(A, B, C) = (a, b, c) S^{-1}$. La matrice S n'est pas unimodulaire, son déterminant est, en valeur absolue, un nombre entier supérieur à 1: c'est la multiplicité de (a, b, c) . La matrice inverse S^{-1} est régulière mais son déterminant est un nombre rationnel différent d'un nombre entier. Tout vecteur V de translation s'exprime ainsi (cf. relation 1):

$$V = ap + bq + cr \quad \text{et} \quad \begin{bmatrix} p \\ q \\ r \end{bmatrix} = S^{-1} \begin{bmatrix} P \\ Q \\ R \end{bmatrix};$$

il existe donc des vecteurs de translations pour lesquels un, au moins, des nombres p, q et r est un rationnel non entier. Réciproquement, toute MRCE non unimodulaire S définit une maille multiple donnée par $(a, b, c) = (A, B, C) S$ car les vecteurs a, b , et c ne sont pas coplanaires ($\det S \neq 0$) et ne constituent pas une maille élémentaire ($\det S \neq \pm 1$). Le passage d'une maille élémentaire à une maille quelconque est donc associé et réciproquement à une MRCE unimodulaire ou non. L'ensemble \mathcal{S} des MRCE n'est pas un groupe vis-à-vis de la multiplication matricielle. C'est un semi-groupe ou demi-groupe simplifiable; il manque à \mathcal{S} pour être un groupe les inverses des MRCE non unimodulaires qui sont des matrices à coefficients rationnels dont un au moins n'est pas entier. Par contre le semi-groupe \mathcal{S} contient comme partie stable le groupe \mathcal{E} des MUCE.

Nous allons maintenant nous intéresser aux seuls sous-groupes de $P1$ qui soient des groupes spatiaux tridimensionnels. Ces sous-groupes sont isomorphes de $P1$: les isomorphismes qui appliquent $P1$ sur ses sous-groupes sont des endomorphismes injectifs. L'ensemble

de ces sous-groupes est un treillis modulaire. Ces sous-groupes admettent le même symbole international ($P1$). Afin d'éviter toute ambiguïté, désignons par Γ le groupe spatial $P1$ de maille élémentaire (A, B, C) et dont (a, b, c) est une maille multiple. Considérons tous les vecteurs de translations de Γ pour lesquels les composantes p, q et r sur le repère (a, b, c) sont des entiers, $v = ap + bq + cr$. L'ensemble γ des translations correspondantes est bien un groupe de translations tridimensionnel dont (a, b, c) est une maille élémentaire. Le groupe γ est un sous-groupe propre de Γ car il existe des vecteurs de translations de Γ pour lesquels une, au moins, des composantes sur (a, b, c) n'est pas un entier. Réciproquement, à tout sous-groupe propre tridimensionnel γ correspond, au moins, une maille multiple de Γ : toute maille élémentaire (a, b, c) de γ est une maille de Γ ; si (a, b, c) était élémentaire dans Γ , γ serait confondu avec Γ . Deux mailles élémentaires de γ sont deux mailles de Γ de même multiplicité égale à l'indice i de γ dans Γ ; elles se correspondent par automorphisme de γ : $(a', b', c') = (a, b, c) M$, M étant une MUCE. Les MRCE qui expriment le passage de la maille élémentaire (A, B, C) de Γ aux deux mailles élémentaires (a, b, c) et (a', b', c') de γ sont liées entre elles:

$$\begin{aligned} (a, b, c) &= (A, B, C) S; & (a', b', c') &= (A, B, C) S' \\ &= (A, B, C) SM \text{ d'où } S' = SM, S^{-1} S' = M, \\ & & (S \text{ et } S' = \text{MRCE}, M = \text{MUCE}). \end{aligned}$$

Deux MRCE qui vérifient cette relation sont dites associées à gauche par une MUCE. L'association à gauche \mathcal{A}_G est une relation d'équivalence dans \mathcal{S} . Toutes les matrices d'une même classe à gauche conduisent et réciproquement, par changement de repère à partir d'une maille élémentaire donnée (A, B, C) de Γ , à toutes les mailles élémentaires du même sous-groupe γ . Dans cette optique, chaque classe à gauche conduit, et réciproquement, à un seul sous-groupe γ , aux automorphismes près de celui-ci. Il existe donc une bijection de l'ensemble quotient $\mathcal{S} / \mathcal{A}_G$ vers le treillis \mathcal{E} des sous-groupes γ de Γ .

On peut également définir l'association à droite \mathcal{A}_D de deux MRCE S et S'' par une MUCE M : $S'' = MS$, $S'' S^{-1} = M$. C'est, bien sûr, une relation d'équivalence dans \mathcal{S} . En voici une interprétation: (A, B, C) étant une maille élémentaire de Γ , l'automorphisme de Γ associé à M transforme (A, B, C) en une autre maille élémentaire (A'', B'', C'') de Γ : $(A'', B'', C'') = (A, B, C) M$. Les deux mailles multiples (a, b, c) et (a'', b'', c'') construites par la même matrice S à partir des deux mailles élémentaires présentent les relations suivantes:

$$\begin{aligned} (a, b, c) &= (A, B, C) S; & (a'', b'', c'') &= (A'', B'', C'') S; \\ (a'', b'', c'') &= (A, B, C) MS = (A, B, C) S''. \end{aligned}$$

Si S et S'' sont à la fois associées à droite et à gauche – c'est-à-dire si les deux produits $S^{-1} S''$ et $S'' S^{-1}$ sont des MUCE – les mailles (a, b, c) et (a'', b'', c'') sont deux

mailles élémentaires du même sous-groupe se correspondant à la fois par un automorphisme de Γ et un automorphisme du sous-groupe. Si S et S'' sont seulement associées à droite – c'est-à-dire, si $S''S^{-1}$ est une MUCE et si $S^{-1}S''$ n'est pas une MUCE – les mailles (a, b, c) et (a'', b'', c'') sont respectivement des mailles élémentaires de deux sous-groupes différents de même indice se correspondant par un automorphisme de Γ . De ce point de vue, chaque classe à droite conduit aux sous-groupes de même indice qui se correspondent par les automorphismes de Γ .

Enfin, on peut définir 'l'équivalence classique' \mathcal{R} entre matrices de \mathcal{S} . Deux MRCE S et T sont équivalentes modulo \mathcal{R} si et seulement s'il existe deux MUCE M et N telles que $T = MSN$. Chaque classe d'équivalence, modulo \mathcal{R} , permet de passer d'une maille élémentaire donnée (A, B, C) de Γ à toutes les mailles élémentaires de tous les sous-groupes de même indice qui se correspondent par les automorphismes de Γ . Notons que l'équivalence \mathcal{R} est moins fine que les associations \mathcal{A}_G et \mathcal{A}_D , lesquelles sont moins fines que l'association bilatère (association à droite et à gauche). Remarquons que deux matrices congrues au sens de l'une quelconque de ces équivalences ont des déterminants nécessairement égaux au signe près.

Exemples divers. Quelles relations d'équivalence présentent les six MRCE suivantes?

$$S_1 = \begin{bmatrix} 1 & -1 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}; \quad S_2 = \begin{bmatrix} -1 & -1 & 0 \\ 5 & 3 & 0 \\ 0 & 0 & -1 \end{bmatrix};$$

$$S_3 = \begin{bmatrix} 1 & 0 & 2 \\ 1 & 0 & 0 \\ 0 & -1 & 0 \end{bmatrix}; \quad S_4 = \begin{bmatrix} 2 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix};$$

$$S_5 = \begin{bmatrix} 0 & 2 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}; \quad S_6 = \begin{bmatrix} 4 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 3 \end{bmatrix}.$$

Le déterminant de chacune des matrices est respectivement égal à 2, -2, -2, 2, 2, 24; il en résulte immédiatement que S_6 n'est équivalente à aucune des cinq autres MRCE: S_6 ne peut donc pas conduire à une maille élémentaire du même sous-groupe que l'une quelconque des cinq autres MRCE. Voici maintenant les matrices inverses S_1^{-1} et S_4^{-1} :

$$S_1^{-1} = \begin{bmatrix} \frac{1}{2} & \frac{1}{2} & 0 \\ -\frac{1}{2} & \frac{1}{2} & 0 \\ 0 & 0 & 1 \end{bmatrix}; \quad S_4^{-1} = \begin{bmatrix} \frac{1}{2} & 0 & 0 \\ -\frac{1}{2} & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

Le lecteur pourra constater sans difficulté que les produits $S_1^{-1}S_2$, $S_1^{-1}S_3$, $S_4^{-1}S_5$ sont des MUCE. Les MRCE S_1 , S_2 , S_3 – étant associées à gauche – conduisent à des mailles élémentaires d'un même sous-groupe γ_1 d'indice 2. Pour la même raison, S_4 et S_5 conduisent à des mailles élémentaires d'un même sous-groupe γ_2 d'indice 2, différent du précédent car $S_1^{-1}S_4$ n'est pas une MUCE. Le produit $S_2S_1^{-1}$ est une MUCE; les deux mailles élémentaires de γ_1 définies par S_1 et S_2 se correspondent donc à la fois par automorphisme de Γ et par automorphisme de γ_1 tandis que la maille élémentaire de γ_1 définie par S_3 ne correspond aux précédentes que par automorphisme de γ_1 car $S_3S_1^{-1}$ n'est pas une MUCE. Et comme, de même, $S_5S_4^{-1}$ n'est pas une MUCE, les mailles élémentaires de γ_2 définies par S_5 et S_4 ne se correspondent que par automorphisme de γ_2 . Mais la maille élémentaire de γ_1 définie par S_1 et la maille élémentaire de γ_2 définie par S_4 se correspondent par automorphisme de Γ car $S_4S_1^{-1}$ est une MUCE. Le produit $S_5S_1^{-1}$ n'est pas une MUCE; il n'existe donc aucun automorphisme de Γ qui fasse correspondre les mailles élémentaires de γ_1 et γ_2 auxquelles S_1 et S_5 conduisent respectivement. Or nous venons de voir que γ_1 et γ_2 se correspondent par au moins un automorphisme de Γ , c'est donc que les matrices S_1 et S_5 sont équivalentes au sens de \mathcal{R} ; on a en effet:

$$S_5 = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} S_1 \begin{bmatrix} 0 & 1 & 0 \\ 0 & -1 & 1 \\ 1 & 0 & 0 \end{bmatrix}.$$

S_6 conduit évidemment à une maille élémentaire d'un troisième sous-groupe d'indice 24 qui ne peut correspondre à γ_1 et γ_2 par aucun automorphisme de Γ ; il est impossible à la matrice S_6 d'être congrue, modulo \mathcal{R} , à l'une quelconque des cinq autres matrices.

Avant de poursuivre l'étude des sous-groupes de Γ , il est nécessaire d'établir quelques propriétés des matrices MRCE.

II. La factorisation des matrices régulières à coefficients entiers

Nous allons montrer dans cette partie que toute MRCE, unimodulaire ou non, est décomposable en un produit fini de matrices à coefficients entiers extrêmement simples appelées matrices de transformation élémentaire. De plus, nous verrons que toute MRCE non unimodulaire est équivalente, modulo \mathcal{R} , à une matrice diagonale à coefficients entiers. Il faut auparavant rappeler certaines propriétés remarquables des nombres entiers.

1. L'algorithme d'Euclide* et le théorème de Bezout

Considérons deux nombres entiers positifs, α et β , premiers entre eux, α étant le plus grand. Effectuons la division euclidienne de α par β , c'est-à-dire, soustrayons de α le plus grand multiple possible de β : $\alpha - k\beta = \gamma$. Le reste de la division euclidienne vérifie les relations $\alpha > \beta > \gamma > 0$; de plus, ou bien γ est égal à 1 ou bien γ est premier avec β ; en effet, si $\gamma \neq 1$ n'était pas premier avec β , on aurait $\beta = xq$, $\gamma = yq$ (q étant le p.g.c.d., c'est-à-dire, le plus grand commun diviseur, de β et γ) et $\alpha = k\beta + \gamma = (kx + y)q$; α ne serait pas premier avec β , ce qui est contradictoire aux hypothèses. Donc si $\gamma \neq 1$, β et γ sont premiers entre eux et le reste δ de la division euclidienne de β par γ est égal à 1 ou premier avec γ et ainsi de suite. En poursuivant l'algorithme d'Euclide, on est amené à trouver une suite: $\alpha > \beta > \gamma > \delta > \dots > \lambda > \mu = 1$. Les nombres adjacents sont premiers entre eux, la suite est finie et le dernier terme est égal à 1. En effet, s'il n'en était pas ainsi, on pourrait trouver un autre nombre ρ reste de la division euclidienne de λ par μ et μ ne serait pas le dernier terme de la suite. Les nombres de la suite sont des combinaisons linéaires à coefficients entiers de α et β ; en particulier, il existe une combinaison linéaire à coefficients entiers de α et β égale à 1 (théorème de Bezout). L'algorithme d'Euclide et le théorème de Bezout connaissent trois généralisations importantes. Si on considère deux nombres entiers positifs non premiers entre eux, désignés par αp et βp (p étant leur p.g.c.d. et $\alpha > \beta$), on obtient une suite de multiple de p : $\alpha p > \beta p > \gamma p > \delta p > \dots > \lambda p > \mu p = p$. Les nombres adjacents admettent p comme p.g.c.d. et le dernier est égal à p . Tous ces nombres et en particulier le p.g.c.d. sont des combinaisons linéaires à coefficients entiers des deux premiers. On peut aussi généraliser au cas de deux nombres entiers de signe quelconque; si les nombres de départ ont des signes opposés, il faut remplacer la soustraction par l'addition dans l'algorithme d'Euclide et la suite est composée de nombres dont les signes alternent; dans tous les cas, le dernier nombre est égal, au signe près, au p.g.c.d. des deux nombres de départ et les autres propriétés sont conservées. Enfin on peut étendre au cas de plusieurs nombres entiers quelconques: en réalisant l'algorithme d'Euclide de deux d'entre eux, on aboutit à leur p.g.c.d.; on réalise ensuite l'algorithme d'Euclide de ce p.g.c.d. et d'un troisième nombre et on aboutit au p.g.c.d. des trois nombres et ainsi de suite.*

Exemple. Trouver par l'algorithme d'Euclide le p.g.c.d. des trois nombres: (-3780) , (462) et (165) .

* Le procédé connu sous le nom 'd'Algorithme d'Euclide' remonte vraisemblablement aux Pythagoriciens (cinquième siècle avant Jésus-Christ). Nous avons repris dans un langage mieux adapté à notre époque la démonstration que donne (*Les Oeuvres d'Euclide, Eléments*; Peyrard, 1966).

L'algorithme d'Euclide des deux premiers aboutit à leur p.g.c.d., le nombre 42. Voici la suite obtenue: -3780 , 462 , -84 , 42 . On remarquera que le théorème de Bezout est vérifié:

$$\begin{aligned} 42 &= 1 \times (462) + 5 \times (-84) = 1 \times (462) \\ &+ 5 \times (-3780 + 8 \times 462), \\ 42 &= 5 \times (-3780) + 41 \times (462). \end{aligned}$$

L'algorithme de (165) et (42) conduit au p.g.c.d. des trois nombres de départ, le nombre 3. En voici la suite: 165 , 42 , 39 , 3 . Le théorème de Bezout est bien vérifié car l'on:

$$\begin{aligned} 3 &= 1 \times (42) - 1 \times (39) = 1 \times (42) \\ &- 1 \times (165 - 3 \times 42) = 4 \times (42) - 1 \times (165), \\ 3 &= 20 \times (-3780) + 164 \times (462) - 1 \times (165). \end{aligned}$$

2. Les matrices de transformation élémentaire

Les transformations matricielles élémentaires sont de trois types: échange de deux lignes (ou de deux colonnes), multiplication des termes d'une ligne (ou d'une colonne) par un scalaire, addition aux termes d'une ligne (ou d'une colonne) de k fois les termes correspondants d'une autre ligne (ou d'une autre colonne). Les MTE (cf. Tableau 1) sont les matrices qui résultent de l'application d'une transformation élémentaire à la matrice identité: leurs propriétés caractéristiques sont résumées dans le Tableau 1. L'intérêt fondamental des MTE réside dans le fait qu'il suffit, pour effectuer une transformation élémentaire sur les lignes (ou sur les colonnes) d'une matrice quelconque, de multiplier à gauche (ou à droite) la matrice en question par la MTE correspondante (*Encyclopaedia Britannica*, 1969).

Exemple. Supposons que l'on veuille additionner quatre fois la première colonne à la dernière colonne de la matrice J suivante; il suffira pour cela de multiplier à droite J par la MTE correspondante, c'est-à-dire, par la matrice unité dans laquelle on aura au préalable additionné quatre fois la première colonne à la dernière colonne; on obtiendra ainsi la matrice transformée J' .

$$J = \begin{bmatrix} 1 & 8 & 6 \\ 4 & 2 & 5 \\ 7 & 9 & 3 \end{bmatrix}; \quad J' = J \begin{bmatrix} 1 & 0 & 4 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 8 & 10 \\ 4 & 2 & 21 \\ 7 & 9 & 31 \end{bmatrix}.$$

Il revient au même de dire que la matrice de départ J est égale à la matrice transformée J' multipliée à droite par la MTE *inverse*, c'est-à-dire, par la matrice unité dans laquelle on aura au préalable soustrait quatre fois la première colonne de la dernière colonne.

$$J = J' \begin{bmatrix} 1 & 0 & -4 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

La remarque précédente est générale; elle s'étend à toutes les transformations matricielles élémentaires. Lorsqu'une matrice a subi une transformation élémentaire portant sur une ligne (ou une colonne), il suffit pour retrouver la matrice de départ de multiplier à gauche (ou à droite) la matrice transformée par la MTE *inverse*, c'est-à-dire, la matrice unité ayant subi la transformation élémentaire *opposée*. Cette remarque est capitale pour une bonne compréhension de la méthode de réduction matricielle.

3. Réduction d'une MRCE d'ordre n à une MRCE d'ordre $(n - 1)^*$

Par une suite de transformations élémentaires, une MRCE d'ordre n est toujours décomposable en le produit – de gauche à droite – d'une MCBE (cf. Tableau 1), d'une MRCE particulière et d'une MCBE; la MRCE particulière présente alors une sous-matrice carrée d'ordre $(n - 1)$ bordée par une ligne et une colonne nulles à l'exception du terme commun. La méthode s'applique aussi aux MRCE présentant déjà une (plusieurs) ligne(s) et une (plusieurs) colonne(s) nulles à l'exception du (des) terme(s) commun(s): on rendra nulles, dans la MRCE particulière, une ligne et une colonne supplémentaires à l'exception du terme commun. Quatre cas peuvent se présenter.

Cas A. La MRCE d'ordre m , $S = [s_{ab}]$, présente au moins un coefficient égal à ± 1 , soit le coefficient s_{ij} . Pour rendre nul le k ème terme s_{ik} ($k \neq j$) de la i ème ligne, on retranche, des termes de la k ème colonne de S , s_{ik}/s_{ij} fois les termes correspondants de la j ème colonne, ce qui revient à avoir multiplié, à droite, la matrice de départ S par une MTBE (cf. Tableau 1). Afin de conserver l'égalité avec la matrice S , on porte à droite de la matrice ainsi transformée la MTBE inverse, c'est-à-dire, celle où $m_{jk} = s_{ik}/s_{ij}$; le produit de ces deux matrices est bien égal à S . On procède de même avec les autres colonnes ($b \neq j$). A ce stade, la matrice S est décomposée en le produit, écrit de gauche à droite, d'une matrice S' (MRCE) où tous les termes s'_{ib} de la i ème ligne sont nuls sauf $s'_{ij} = s_{ij} = \pm 1$, et de $(n - 1)$ MTBE inverses (moins, si un ou plusieurs coefficients s_{ib} étaient déjà nuls dans la matrice S); la première MTBE apparue dans la décomposition se trouve à l'extrême droite, la seconde immédiatement à gauche de la première, etc. Le produit des MTBE est une MCBE (cf. Tableau 1).

Exemple 1. On annule les premier et deuxième termes de la première ligne de σ_1 .

* Ce procédé de réduction matricielle offre des points communs avec la 'méthode d'élimination à Gauss' fréquemment utilisée en théorie des espaces vectoriels (Gantmacher, 1966).

$$\sigma_1 = \begin{bmatrix} 2 & 66 & -1 \\ 86 & -6 & 152 \\ -6 & 33 & 3 \end{bmatrix} = \begin{bmatrix} 0 & 66 & -1 \\ 390 & -6 & 152 \\ 0 & 33 & 3 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ -2 & 0 & 1 \end{bmatrix},$$

$$\sigma_1 = \begin{bmatrix} 0 & 0 & -1 \\ 390 & 10026 & 152 \\ 0 & 231 & 3 \end{bmatrix} \times \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & -66 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ -2 & 0 & 1 \end{bmatrix},$$

$$\sigma_1 = \begin{bmatrix} 0 & 0 & -1 \\ 390 & 10026 & 152 \\ 0 & 231 & 3 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ -2 & -66 & 1 \end{bmatrix}$$

De la même manière, tous les termes de la j ème colonne de S' vont être transformés en zéro sauf s'_{ij} . Pour rendre nul le terme s'_{lj} ($l \neq i$), on retranche, de la l ème ligne, s'_{lj}/s'_{ij} fois la i ème ligne de S' et on porte, à gauche de la matrice ainsi transformée, la MTBE où $m_{li} = s'_{lj}/s'_{ij}$, etc. On aboutit finalement à décomposer S' en le produit, de gauche à droite, d'au plus $(n - 1)$ MTBE et d'une matrice S'' (MRCE) où tous les termes de la i ème ligne et de la j ème colonne sont nuls sauf $s''_{ij} = s_{ij} = \pm 1$; la première MTBE apparue figure à l'extrême gauche, la seconde immédiatement à droite de la première, etc. Le produit de ces MTBE est une MCBE. La matrice S est donc décomposée en le produit de trois matrices: la matrice S'' (MRCE) encadrée des deux MCBE.

Exemple 1 (suite). Traitement de la troisième colonne

$$\begin{bmatrix} 0 & 0 & -1 \\ 390 & 10026 & 152 \\ 0 & 231 & 3 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ -152 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ -3 & 0 & 1 \end{bmatrix} \begin{bmatrix} 0 & 0 & -1 \\ 390 & 10026 & 0 \\ 0 & 231 & 0 \end{bmatrix}$$

$$\text{et } \sigma_1 = \begin{bmatrix} 1 & 0 & 0 \\ -152 & 1 & 0 \\ -3 & 0 & 1 \end{bmatrix} \\ \times \begin{bmatrix} 0 & 0 & -1 \\ 390 & 10026 & 0 \\ 0 & 231 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ -2 & -66 & 1 \end{bmatrix}.$$

Cas B. La MRCE d'ordre n , $S = [s_{ab}]$, ne présente aucun coefficient égal à ± 1 , mais au moins un terme, par exemple s_{ij} , divise tous les termes de sa ligne, la i ème ligne, et tous les termes de sa colonne, la j ème colonne. Le cas *B* n'est qu'une extension du cas précédent *A* et on procède de la même manière.

Exemple 2. Traitement de la deuxième colonne et de la deuxième ligne de σ_2 .

$$\sigma_2 = \begin{bmatrix} 0 & 0 & -1 \\ 1950 & 3 & 0 \\ -780 & 45 & 0 \end{bmatrix} \\ = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 15 & 1 \end{bmatrix} \begin{bmatrix} 0 & 0 & -1 \\ 1950 & 3 & 0 \\ -30030 & 0 & 0 \end{bmatrix}, \\ \sigma_2 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 15 & 1 \end{bmatrix} \begin{bmatrix} 0 & 0 & -1 \\ 0 & 3 & 0 \\ -30030 & 0 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 650 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

Cas C. Les conditions requises pour le traitement des cas *A* et *B* ne sont pas remplies, mais le p.g.c.d. des termes d'une colonne, au moins, est égal à 1; soit la j ème cette colonne. S'il existe au moins deux termes s_{ij} et s_{kj} , de cette colonne, dont le p.g.c.d. est égal à 1, on combine entre elles les lignes i et k plusieurs fois de manière à ce que les coefficients s_{ij} et s_{kj} prennent les valeurs successives données par l'algorithme d'Euclide de leurs valeurs de départ, la dernière valeur étant nécessairement 1; on est ramené au cas *A*. Si le p.g.c.d. des deux termes s_{ij} et s_{ik} est toujours différent de 1, quels que soient i et k , la combinaison des lignes i et k selon l'algorithme d'Euclide des valeurs initiales des termes s_{ij} et s_{ik} conduit au p.g.c.d. de celles-ci α_{ik} . En combinant la ligne du terme ainsi réduit à α_{ik} (ligne i ou ligne k) avec une troisième ligne, la ligne m , on arrive par l'algorithme d'Euclide au p.g.c.d. des valeurs de départ des coefficients s_{ij} , s_{kj} et s_{mj} . En continuant ainsi, on aboutit nécessairement à transformer l'un des termes de la j ème colonne en 1; le problème se ramène au cas *A*. Evidemment, il ne faut pas oublier, pour garder

l'égalité avec la matrice de départ S , de porter à gauche de la matrice transformée les MTBE inverses associées aux différentes étapes de la réduction, la première étant à l'extrême gauche. D'une manière tout à fait analogue, on peut se ramener au cas *A* si le p.g.c.d. des termes d'une ligne, au moins, est égal à 1; bien sûr les MTBE caractéristiques sont portées à droite, la première figurant à l'extrême droite. Quelle que soit la réduction effectuée, les produits de MTBE sont des MCBE.

Exemple 3. Traitement de la troisième colonne de σ_3 .

$$\sigma_3 = \begin{bmatrix} 22 & 33 & -11 \\ 86 & -6 & 152 \\ -14 & 0 & 7 \end{bmatrix} \\ = \begin{bmatrix} 1 & 0 & -1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 8 & 33 & -4 \\ 86 & -6 & 152 \\ -14 & 0 & 7 \end{bmatrix}, \\ \sigma_3 = \begin{bmatrix} 1 & 0 & -1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ -1 & 0 & 1 \end{bmatrix} \begin{bmatrix} 8 & 33 & -4 \\ 86 & -6 & 152 \\ -6 & 33 & 3 \end{bmatrix} \\ \sigma_3 = \begin{bmatrix} 1 & 0 & -1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ -1 & 0 & 1 \end{bmatrix} \\ \times \begin{bmatrix} 1 & 0 & -1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 2 & 66 & -1 \\ 86 & -6 & 152 \\ -6 & 33 & 3 \end{bmatrix} \\ \text{et } \sigma_3 = \begin{bmatrix} 2 & 0 & -3 \\ 0 & 1 & 0 \\ -1 & 0 & 2 \end{bmatrix} \begin{bmatrix} 2 & 66 & -1 \\ 86 & -6 & 152 \\ -6 & 33 & 3 \end{bmatrix}.$$

Cas D. Aucune des conditions requises dans les cas *A*, *B* et *C* n'est satisfaite. Dans ces conditions, les termes de la i ème ligne (ou de la i ème colonne) ont pour p.g.c.d. p_i . Par combinaisons successives des colonnes (ou des lignes) selon les algorithmes d'Euclide caractéristiques, on peut rendre un des termes de la i ème ligne (ou de la i ème colonne) égal à p_i , les autres termes de la i ème ligne (ou de la i ème colonne) étant des multiples, au sens large, de p_i ; soit s'_{ij} (ou s'_{ji}) ce terme. Les coefficients de la j ème colonne (ou de la j ème ligne) ont alors pour p.g.c.d. p'_j . Trois possibilités se présentent:

(a) $p'_j = 1$, le problème est ramené au cas *C*.

Exemple 4. Traitement de la première ligne de σ_4 ($p = 11$).

$$\sigma_4 = \begin{bmatrix} 55 & 33 & -143 \\ 20 & -6 & 26 \\ -35 & 0 & 91 \end{bmatrix}$$

$$= \begin{bmatrix} 55 & 33 & -33 \\ 20 & -6 & 66 \\ -35 & 0 & 21 \end{bmatrix} \begin{bmatrix} 1 & 0 & -2 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix},$$

$$\sigma_4 = \begin{bmatrix} 22 & 33 & -33 \\ 86 & -6 & 66 \\ -14 & 0 & 21 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ -1 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & -2 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix},$$

$$\sigma_4 = \begin{bmatrix} 22 & 33 & -11 \\ 86 & -6 & 152 \\ -14 & 0 & 7 \end{bmatrix} \begin{bmatrix} 1 & 0 & -1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

$$\times \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ -1 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & -2 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

$$\text{et } \sigma_4 = \begin{bmatrix} 22 & 33 & -11 \\ 86 & -6 & 152 \\ -14 & 0 & 7 \end{bmatrix} \begin{bmatrix} 2 & 0 & -5 \\ 0 & 1 & 0 \\ -1 & 0 & 3 \end{bmatrix}.$$

(b) $p'_j = p_i$, le problème se ramène au cas B .

Exemple 5. Traitement de la deuxième colonne de σ_5 ($p_2 = 3 = p'_2$).

$$\sigma_5 = \begin{bmatrix} 0 & 0 & -1 \\ 390 & 10026 & 0 \\ 0 & 231 & 0 \end{bmatrix}$$

$$= \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 43 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 0 & 0 & -1 \\ 390 & 93 & 0 \\ 0 & 231 & 0 \end{bmatrix},$$

$$\sigma_5 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 43 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 2 & 1 \end{bmatrix} \begin{bmatrix} 0 & 0 & -1 \\ 390 & 93 & 0 \\ -780 & 45 & 0 \end{bmatrix},$$

$$\sigma_5 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 43 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 2 & 1 \end{bmatrix}$$

$$\times \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 0 & 0 & -1 \\ 1950 & 3 & 0 \\ -780 & 45 & 0 \end{bmatrix}$$

$$\text{et } \sigma_5 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 87 & 217 \\ 0 & 2 & 5 \end{bmatrix} \begin{bmatrix} 0 & 0 & -1 \\ 1950 & 3 & 0 \\ -780 & 45 & 0 \end{bmatrix}.$$

(c) p'_j est différent de 1 et de p_i ; p'_j est donc plus petit que p_i et divise p_i . Par combinaisons des lignes (ou des colonnes) selon les algorithmes d'Euclide adéquats, on peut rendre un des termes de la j ème colonne (ou de la j ème ligne) égal à p'_j , soit s''_{kj} (ou s''_{jk}) ce terme; les autres termes de la j ème colonne (ou de la j ème ligne) sont des multiples, au sens large, de p'_j . Les termes de la k ème ligne (ou de la k ème colonne) ont alors pour p.g.c.d. p''_k . De nouveau, on est en présence des possibilités (a), (b) ou (c). Dans l'hypothèse où on se trouverait de nouveau devant la possibilité (c), il faut remarquer que p''_k est plus petit que p'_j et le divise. Il est donc plus petit que p_i et le divise. Les nombres p'_j et p''_k appartiennent donc à une suite de sous-multiples stricts de p_i , chaque terme de la suite divisant strictement ceux qui le précèdent; cette suite est forcément finie et se termine par 1. Il en résulte, qu'en procédant alternativement sur les lignes et les colonnes, on aboutira nécessairement aux possibilités (a) ou (b) après un certain nombre de manipulations. Comme pour les cas A , B et C , il ne faut pas oublier, pour garder l'invariance avec la matrice de départ, de porter, à droite ou à gauche de la matrice transformée, selon que l'on combine les colonnes ou les lignes, les MTBE inverses associées aux différentes étapes de la réduction, on aboutit à une MRCE réduite encadrée de deux MCBE. La MRCE de départ de départ est équivalente, modulo \mathcal{R} , à la MRCE réduite et a même déterminant.

4. Réduction totale d'une MRCE d'ordre n

Evidemment, on peut procéder de la même façon que précédemment avec le bloc d'ordre $(n - 1)$ et ainsi de suite. La MRCE est donc finalement équivalente par deux MCBE à une MRCE totalement réduite, c'est-à-dire une MRCE dont tous les termes sont nuls à l'exception d'un seul terme par ligne et par colonne; la

MRCE totalement réduite a le même déterminant que la matrice de départ. Les exemples précédents pris dans l'ordre 4, 3, 1, 5, 2 constituent la réduction totale de la MRCE σ_4 , d'ordre 3. Les premières étapes (exemples 4, 3, 1) sont relatives à la réduction à un bloc d'ordre 2, les étapes suivantes (exemples 5, 2) à la réduction de ce bloc. La réduction totale fait intervenir 15 étapes, 6 transformations élémentaires portant sur les colonnes et 9 portant sur les lignes. On peut écrire en effectuant les produits de MTBE:

$$\sigma_4 = \begin{bmatrix} 11 & -231 & -15 \\ -152 & 3342 & 217 \\ -7 & 154 & 10 \end{bmatrix} \times \begin{bmatrix} 0 & 0 & -1 \\ 0 & 3 & 0 \\ -30030 & 0 & 0 \end{bmatrix} \begin{bmatrix} 2 & 0 & -5 \\ 1300 & 1 & -3250 \\ -5 & -66 & 13 \end{bmatrix}.$$

Il faut noter que la réduction n'est pas unique: le résultat dépend de l'ordre adopté dans le choix des différentes étapes, en général.

Insistons pour conclure sur la généralité de cette méthode de réduction matricielle. Elle ne fait intervenir que des notions mathématiques particulièrement simples: transformations matricielles élémentaires (les MTBE essentiellement) et algorithme d'Euclide. La méthode s'applique non seulement aux MRCE d'ordre 3 mais à toutes celles d'ordre fini, quelque grand que soit cet ordre. Toutes les MRCE peuvent être réduites y compris les MUCE; dans le cas de celles-ci, la réduction ne passe que par les cas A et C et la matrice réduite est unimodulaire.

5. Equivalence d'une MRCE à une MAOG

Une MRCE totalement réduite ne diffère d'une matrice diagonale que par la permutation éventuelle de plusieurs lignes et de plusieurs colonnes. Il en résulte qu'en procédant par échanges successifs des lignes (ou des colonnes) et, en portant à gauche (ou à droite) les MRBE (cf. Tableau 1) associées à ces échanges, on aboutira à une matrice diagonale équivalente. Si cette dernière présente des coefficients négatifs, on peut en changer le signe à condition de porter à droite ou à gauche la MRBE associée. Donc toute MRCE totalement réduite est équivalente à une MAOG (cf. Tableau 1) par deux MRBG (cf. Tableau 1). Et plus généralement toute MRCE est décomposable entièrement en un produit fini de MTE à coefficients entiers; toute MRCE est équivalente par deux MCBG (cf. Tableau 1) à une MAOG de même déterminant, au signe près.

Exemple.

$$\begin{bmatrix} 0 & 0 & -1 \\ 0 & 3 & 0 \\ -30030 & 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix} \times \begin{bmatrix} 30030 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{bmatrix} \\ \sigma_4 = \begin{bmatrix} -15 & -231 & 11 \\ 217 & 3342 & -152 \\ 10 & 154 & -7 \end{bmatrix} \times \begin{bmatrix} 30030 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} -2 & 0 & 5 \\ 1300 & 1 & -3250 \\ 5 & 66 & -13 \end{bmatrix}.$$

Dans le cas particulier d'une MUCE, la MAOG est en fait confondue avec la matrice unité; de sorte que toute MUCE est finalement une MCBG, c'est-à-dire, un produit fini de MTBE et de MRBE.

6. Equivalence et non-équivalence des MRCE

Deux MRCE S et S' sont équivalentes si et seulement s'il existe deux MUCE M et N telles que S' = MSN; ce qui implique $|\det S'| = |\det S|$. Deux MRCE dont les déterminants ne sont pas égaux, au signe près, ne peuvent pas être équivalentes. Par contre deux MRCE dont les déterminants sont égaux, en valeur absolue, peuvent être équivalentes ou non. Signalons tout de suite deux cas où S et S' sont équivalentes; premier cas: le produit $S^{-1}S' = K$ est une MUCE: en effet, S' = SK, S' et S sont associées à gauche et donc équivalentes modulo \mathcal{R} ; deuxième cas: le produit $S'S^{-1} = L$ est une MUCE, S' et S sont associées à droite donc équivalentes modulo \mathcal{R} . Dans le cas général, le problème se ramène à l'équivalence de deux matrices diagonales; car, comme nous l'avons vu, S et S' sont respectivement équivalentes à deux MAOG D et D' par des MCBG P, Q et P', Q': S = PDQ et S' = P'D'Q'; l'équivalence D' = M₀DN₀ entraîne l'équivalence S' = P'M₀P⁻¹SQ⁻¹N₀Q'. Deux MAOG sont toujours équivalentes dans les deux cas suivants:

Cas I. Les deux MAOG ne diffèrent l'une de l'autre que par l'ordre des valeurs des coefficients diagonaux. Remarquons que l'échange des lignes d'indices i et k suivi de l'échange des colonnes d'indices i et k aboutit à l'échange des coefficients diagonaux d'indices i et k. Par itération, on peut donc transformer D en D': D' est équivalente à D par deux MRBG d'ailleurs inverses l'une de l'autre.

Exemple.

$$\begin{bmatrix} 3 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 30030 \end{bmatrix} = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix} \begin{bmatrix} 30030 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}.$$

Cas II. Les MAOG D et D' sont équivalentes si la valeur commune des déterminants de D et D' est un produit de nombres premiers tous différents. Cette propriété repose sur l'étude de l'équivalence des matrices bidimensionnelles:

$$V = \begin{bmatrix} ac & 0 \\ 0 & b \end{bmatrix} \quad \text{et} \quad W = \begin{bmatrix} a & 0 \\ 0 & bc \end{bmatrix} \quad (a, b, c: \text{entiers}).$$

Pour que V et W soient équivalentes, il faut et il suffit qu'il existe deux MUCE F et G telles que $FV = WG$, soit:

$$\begin{bmatrix} f_{11} & f_{12} \\ f_{21} & f_{22} \end{bmatrix} \begin{bmatrix} ac & 0 \\ 0 & b \end{bmatrix} = \begin{bmatrix} a & 0 \\ 0 & bc \end{bmatrix} \begin{bmatrix} g_{11} & g_{12} \\ g_{21} & g_{22} \end{bmatrix}$$

ou encore

$$\begin{bmatrix} f_{11}ac & f_{12}b \\ f_{21}ac & f_{22}b \end{bmatrix} = \begin{bmatrix} g_{11}a & g_{12}a \\ g_{21}bc & g_{22}bc \end{bmatrix}.$$

Les matrices F et G doivent donc être de la forme:

$$F = \begin{bmatrix} f_{11} & k_1a/p \\ k_2b/p & g_{22}c \end{bmatrix} \quad \text{et} \quad G = \begin{bmatrix} f_{11}c & k_1b/p \\ k_2a/p & g_{22} \end{bmatrix}$$

avec

p : p.g.c.d. de a et b , k et k_2 entiers et $\det F = \det G = f_{11}g_{22}c - k_1k_2ab/p_2 = \pm 1$.

Discussion

(1) Si le p.g.c.d. de ab/p^2 et c est $d \neq 1$, $ab/p^2 = xd$ et $c = yd$; $\det F = (f_{11}g_{22}y - k_1k_2x)d$ est toujours différent de ± 1 et V ne peut pas être équivalente à W .

(2) Si ab/p^2 et c sont premiers entre eux, le théorème de Bezout stipule l'existence de deux entiers, au moins, λ et μ tels que $\lambda ab/p^2 + \mu c = 1$ (λ et μ peuvent être trouvés en réalisant l'algorithme d'Euclide de ab/p^2 et c). On peut choisir $f_{11} = 1$, $k_1 = -1$, $k_2 = \lambda$ et $g_{22} = \mu$; les matrices F et G sont alors des MUCE et les matrices V et W sont bien équivalentes. Le raisonnement peut être étendu sans difficulté à une matrice d'ordre quelconque et il en résulte la propriété générale suivante: deux MAOG sont équivalentes, si et seulement si, pour chaque facteur premier figurant dans la décomposition de la valeur du déterminant, la distribution des puissances de ce facteur le long de la

diagonale est la même, à l'ordre près, pour les deux MAOG.

Exemple. Les matrices D_1 et D_3 sont équivalentes entre elles car d'une part les facteurs premiers 2, 5, 7, 11 et 13 ne figurent qu'une seule fois dans la décomposition de la valeur du déterminant et peuvent être distribués indifféremment et d'autre part le facteur premier 3 figure une fois dans chacun des premier et second termes de D_1 et une fois dans chacun des second et troisième termes de D_3 . Par contre la matrice D_2 n'est pas équivalente aux matrices D_1 et D_3 puisque le nombre 3 figure au carré dans le premier coefficient de D_2 .

$$D_1 = \begin{bmatrix} 30030 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 1 \end{bmatrix}; \quad D_2 = \begin{bmatrix} 90090 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix};$$

$$D_3 = \begin{bmatrix} 22 & 0 & 0 \\ 0 & 273 & 0 \\ 0 & 0 & 15 \end{bmatrix}.$$

On peut vérifier que:

$$D_3 = \begin{bmatrix} 801 & -2002 & -1364 \\ -801 & 2002 & 1365 \\ -2 & 5 & 0 \end{bmatrix} \times D_1 \begin{bmatrix} 5 & 62 & 1 \\ 20020 & 248248 & 4005 \\ 22 & 273 & 0 \end{bmatrix}.$$

Pour conclure sur l'équivalence des MAOG, on peut dire que deux MAOG dont la valeur commune du déterminant est un produit d'entiers premiers tous différents sont toujours équivalentes.

Enfin on peut déduire quelles sont les classes d'équivalence modulo \mathcal{R} des matrices MRCE dont le déterminant a pour valeur absolue un entier positif quelconque donné par avance. Si cet entier est premier ou s'il est le produit de nombres premiers tous différents, il existe une seule classe modulo \mathcal{R} . Si le même facteur figure plusieurs fois dans la décomposition, il existe nécessairement plusieurs classes.

Exemples. Si la valeur absolue du déterminant est le nombre $90090 = 1 \times 2 \times 3^2 \times 5 \times 7 \times 11 \times 13$, il y a deux classes différentes de MRCE d'ordre 3 puisqu'il existe deux façons de distribuer le nombre 3. Les matrices D_1 et D_2 sont respectivement des représentants de ces deux classes. Le nombre de classes est lié à l'ordre des matrices: ainsi, il y a six classes de MRCE d'ordre 3 et quatre classes de MRCE d'ordre 2 ayant un déterminant de valeur absolue égale à 72.

III. Quelques propriétés caractéristiques des sous-groupes de P1

L'étude de la factorisation des MRCE et des équivalences qu'elles présentent est d'une grande conséquence pour les propriétés des sous-groupes tridimensionnels du groupe spatial Γ (P1). C'est en développant et en utilisant systématiquement ces propriétés que nous pourrions ultérieurement (Billiet & Rolley-Le Coz, 1979) construire les sous-groupes de Γ , les classer et en dresser la liste jusqu'à des indices relativement élevés.

Pour terminer le présent mémoire nous donnons maintenant un aperçu rapide des propriétés qui découlent de la réduction des MRCE et de leurs équivalences. Rappelons (cf. I.2) qu'une MRCE définit et réciproquement le passage d'une maille élémentaire (A,B,C) de Γ à une maille élémentaire (a,b,c) d'un sous-groupe γ : (a,b,c) = (A,B,C)S. Or nous avons montré que S, comme toute MRCE, est équivalente par deux MCBG, M et m, à une matrice diagonale (MAOG) Δ ; ce qui s'exprime par $S = M\Delta m$. En voici l'interprétation: le passage de la maille élémentaire (A,B,C) de Γ à la maille élémentaire (a,b,c) du sous-groupe γ est équivalente à la succession des trois opérations suivantes:

– passer de la maille élémentaire (A,B,C) à une autre maille élémentaire (A₀,B₀,C₀) du groupe de départ Γ par une MCBG M:

$$(A_0, B_0, C_0) = (A, B, C) M.$$

– passer de la maille (A₀,B₀,C₀) du groupe de départ Γ à une maille élémentaire (a₀,b₀,c₀) du sous-groupe γ par une MAOG Δ , c'est-à-dire, par une affinité:

$$(a_0, b_0, c_0) = (A_0, B_0, C_0) \Delta,$$

– passer de la maille élémentaire (a₀,b₀,c₀) à une autre maille élémentaire du même sous-groupe γ par une MCBG m:

$$(a, b, c) = (a_0, b_0, c_0) m.$$

Autrement dit, quel que soit le sous-groupe γ (P1) de Γ (P1) il existe toujours au moins une maille élémentaire (a₀,b₀,c₀) de γ et une maille élémentaire (A₀,B₀,C₀) de Γ telles que (a₀,b₀,c₀) se déduise de (A₀,B₀,C₀) par une affinité (Fig. 1), c'est-à-dire, de telle sorte que l'un au moins des vecteurs a₀, b₀, c₀ de γ soit multiple entier du vecteur correspondant A₀, B₀, C₀ de Γ et que chacun des deux autres vecteurs de γ soit multiple entier ou confondu avec le vecteur correspondant de Γ :

$$a_0 = pA_0, \quad b_0 = qB_0, \quad c_0 = rC_0$$

(p, q, r entiers égaux ou supérieurs à 1); l'indice i du sous-groupe γ étant égal au produit pqr.

Rappelons aussi (cf. I.2) que des MRCE équivalentes conduisent à des mailles élémentaires du même sous-groupe ou appartenant à des sous-groupes qui se

correspondent par les automorphismes de Γ . Tous les sous-groupes d'un même indice premier i se correspondent par les automorphismes de Γ car toutes les MRCE ayant pour déterminant le même nombre premier i, au signe près, sont équivalentes. Et évidemment seul l'un des vecteurs est multiplié par i dans l'affinité de passage au sous-groupe. Lorsque l'indice n'est pas premier, les situations peuvent être très différentes.

Exemple A. L'indice est égal à $2 \times 3 = 6$. Toutes les MRCE de déterminant égal à ± 6 sont équivalentes car les facteurs premiers de 6 sont tous différents (cf. II.5). Il en résulte que tous les sous-groupes d'indice 6 se correspondent par les automorphismes de Γ . De plus l'on rencontrera pour chacun de ces sous-groupes deux types d'affinité dans les passages groupe – sous-groupe (Fig. 1):

(i) Seul l'un des vecteurs A₀, B₀, C₀ est sextuplé, les autres étant conservés.

(ii) L'un des vecteurs est triplé, un autre est doublé et le troisième est conservé.

Et voici une conséquence, valable pour chacun des sous-groupes d'indice 6 au niveau des familles de plans réticulaires: il existe quatre types de familles (Fig. 1):

Type I. Un plan sur six est entièrement conservé par le sous-groupe, les cinq autres plans ne conservant aucun noeud de Γ .

Type II. Un plan sur trois est à demi conservé, les deux autres plans ne conservant aucun noeud de Γ .

Type III. Un plan sur deux est au tiers conservé, l'autre ne conservant aucun noeud de Γ .

Type IV. Tous les plans conservent un noeud sur six noeuds de Γ .

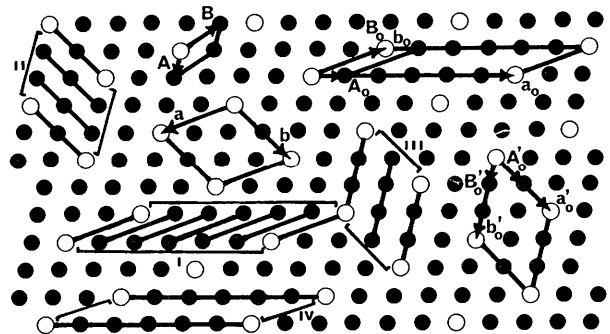


Fig. 1. Analogie bidimensionnelle de l'exemple A. Les sous-groupes isomorphes d'indice 6 de Γ (p1) sont tous équivalents par les automorphismes de Γ . Dans le cas présent le sous-groupe γ est défini par $a = -A - 2B$, $b = 4A + 2B$. Il est possible de trouver deux affinités de passage de Γ à γ : ($a_0 = 6A_0$, $b_0 = B_0$) et ($a'_0 = 2A'_0$, $b'_0 = 3B'_0$). Il existe quatre type de familles de rangées réticulaires: (I) une rangée sur six rangées de Γ est conservée par γ , (II) une rangée sur trois est à demi conservée, (III) une rangée sur deux est au tiers conservée, (IV) chaque rangée conserve un noeud sur six.

Exemple B. L'indice est égal à $2 \times 2 = 4$. Les MRCE de déterminant égal à ± 4 forment deux classes d'équivalence car le nombre 2 figure plusieurs fois dans la décomposition du nombre 4 en facteurs premiers (cf. II.5). Il en résulte deux classes de sous-groupes d'indice 4 dont les propriétés diffèrent beaucoup.

Première classe. Un seul type d'affinité conduit du groupe Γ à l'un quelconque des sous-groupes de cette classe: seul l'un des vecteurs A_0, B_0, C_0 est quadruplé, les autres étant inchangés (Fig. 2a). Il existe pour ces sous-groupes trois types de familles de plans réticulaires:

Type I. Un plan sur quatre est entièrement conservé, les trois autres plans ne conservant aucun noeud de Γ .

Type II. Un plan sur deux est à demi conservé, l'autre ne conservant aucun noeud de Γ .

Type III. Chaque plan conserve un noeud sur quatre noeuds de Γ .

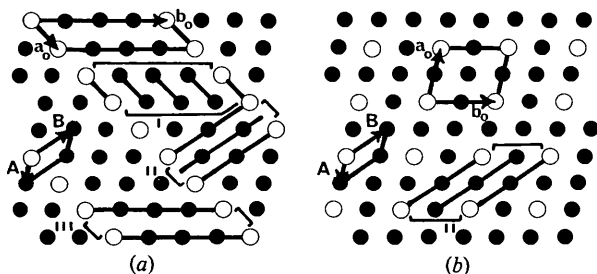


Fig. 2. Analogie bidimensionnelle de l'exemple B. (a) La première classe des sous-groupes d'indice 4 se caractérise par l'affinité de passage $a_0 = A_0, b_0 = 4B_0$. Il existe trois types de rangées réticulaires: (I) une rangée sur quatre est conservée, (II) une rangée sur deux est à demi conservée, (III) chaque rangée conserve le quart des noeuds. (b) La seconde classe des sous-groupes d'indice 4 se caractérise par l'affinité de passage $a_0 = 2A_0, b_0 = 2B_0$. Il n'existe qu'un seul type de rangées réticulaires: (II) une rangée sur deux est à demi conservée.

Deuxième classe. Un seul type d'affinité, différent du cas de la 1ère classe, conduit aux sous-groupes de la seconde classe: deux des vecteurs A_0, B_0, C_0 sont doublés, le troisième étant inchangé (Fig. 2b). Quant aux familles de plans réticulaires, elles n'appartiennent qu'à un seul type: un plan sur deux est à demi conservé, l'autre ne conservant aucun noeud de Γ (type II).

Toutes ces questions seront reprises dans un autre mémoire (Rolley-Le Coz & Billiet, 1979).

Références

- BERTAUT, E. F. (1976a). *Acta Cryst.* A32, 380–387.
 BERTAUT, E. F. (1976b). *Acta Cryst.* A32, 976–983.
 BILLIET, Y. (1973). *Bull. Soc. Fr. Minéral. Cristallogr.* 96, 327–334.
 BILLIET, Y. & ROLLEY-LE COZ, M. (1979). En préparation.
 BILLIET, Y., SAYARI, A. & ZARROUK, H. (1978). *Acta Cryst.* A34, 414–421.
 BOURBAKI, N. (1962). *Eléments de Mathématique, II Algèbre, 2 Algèbre linéaire*. Paris: Hermann.
 BOYLE, L. L. & LAWRENSON, J. E. (1972a). *Acta Cryst.* A28, 485–489.
 BOYLE, L. L. & LAWRENSON, J. E. (1972b). *Acta Cryst.* A28, 489–493.
 BUERGER, M. J. (1947). *J. Chem. Phys.* 15, 1–16.
Encyclopaedia Britannica (1969). Tome 24, pp. 1113–1114. Chicago: William Benton.
 GANTMACHER, F. R. (1966). *Théorie des Matrices* (traduction française). Paris: Dunod.
 HERMANN, C. (1929). *Z. Kristallogr.* 69, 533–541.
 KUROSH, A. G. (1960). *The Theory of Groups*, 2ème éd., Tome I, p. 88. New York: Chelsea Publishing Co.
 NEUBÜSER, J. & WONDRAČSHEK, H. (1966a). *Krist. Tech.* 4, 529–543.
 NEUBÜSER, J. & WONDRAČSHEK, H. (1966b). *Liste de sous-groupes maximaux des groupes spatiaux*. Communication privée.
 PEYRARD, F. (1966). *Les Oeuvres d'Euclide* (traduction française), *Eléments*, Livre VII, Propositions II et III. Paris: Librairie Scientifique et Technique Albert Blanchard.
 ROLLEY-LE COZ, M. & BILLIET, Y. (1979). En préparation.
 SAYARI, A. & BILLIET, Y. (1977). *Acta Cryst.* A33, 985–986.
 SAYARI, A., BILLIET, Y. & ZARROUK, H. (1978). *Acta Cryst.* A34, 553–555.