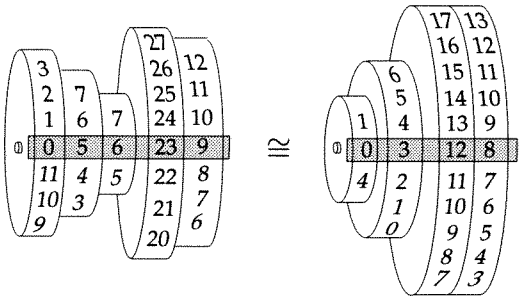
CES GROUPES OU CES ANNEAUX SONT-ILS ISOMORPHES ?

Raymond SÉROUL



Parmi les trois groupes ou anneaux

$$A = \mathbb{Z}_{12} \oplus \mathbb{Z}_{35} \oplus \mathbb{Z}_{45}, \quad B = \mathbb{Z}_{15} \oplus \mathbb{Z}_{1260}, \quad C = \mathbb{Z}_{30} \oplus \mathbb{Z}_{630},$$

lesquels sont isomorphes ? et comment construire un isomorphisme explicite ?

1. L'ANNEAU DES ENTIERS MODULO N

• Soient $a, n > 0$ deux entiers. L'équation homogène

$$ax = 0, \quad x \in \mathbb{Z}_n,$$

possède $d = \text{pgcd}(a, n)$ solutions. En effet, si on pose $a = da'$ et $n = dn'$, on sait que a' et n' sont premiers entre eux. La condition $ax = kn$ équivaut à $a'x = kn'$, d'où l'on déduit $x = hn'$ en vertu du lemme de Gauss. En revenant dans $\mathbb{Z}_n$, cela donne les solutions $x_1 = n', x_2 = 2n', \ldots, x_d = dn' = 0$.

Soient $a, b > 0$ et λ des entiers ; intéressons-nous aux applications de $\mathbb{Z}_a$ dans $\mathbb{Z}_b$.

• La formule $\Phi(x) = \lambda x$ définit une application $\Phi : \mathbb{Z}_a \to \mathbb{Z}_b$ si et seulement si on a $\Phi(x + ak) = \Phi(x)$, ce qui équivaut à $\lambda a \equiv 0$ modulo b.

• Lorsque a, b, λ vérifient la congruence précédente, $\Phi : \mathbb{Z}_a \to \mathbb{Z}_b$ respecte la multiplication si et seulement si λ est un *idempotent* de $\mathbb{Z}_b$, c'est-à-dire $\lambda^2 = \lambda$.

• Considérons les applications $\Phi_i : \mathbb{Z}_a \to \mathbb{Z}_b$ définies par $\Phi_i(x) = \lambda_i x$, les λ_i satisfaisant bien entendu les relations $\lambda_i a \equiv 0 \text{ mod } b$. Alors l'application

$$\Phi = \Phi_1 + \cdots + \Phi_k : \mathbb{Z}_a \longrightarrow \mathbb{Z}_b$$

est un homomorphisme d'anneaux si et seulement si les λ_i sont des idempotents de $\mathbb{Z}_b$ deux à deux orthogonaux :

$$\lambda_i^2 = \lambda_i, \quad \lambda_i\lambda_j = 0, \quad 1 \leq i, j \leq k, \ i \neq j.$$

Plus généralement, on peut associer à un homomorphisme de groupes additifs

$$\Phi : \mathbb{Z}_{a_1} \oplus \cdots \oplus \mathbb{Z}_{a_p} \longrightarrow \mathbb{Z}_{b_1} \oplus \cdots \oplus \mathbb{Z}_{b_q}$$

une matrice

$$\mathcal{M}_\Phi = \begin{pmatrix} m_{11} & m_{12} & \dots & m_{1p} \\ m_{21} & m_{22} & \dots & m_{2p} \\ \dots & \dots & \dots & \dots \\ m_{q1} & m_{q2} & \dots & m_{qp} \end{pmatrix}$$

dont les coefficients satisfont les conditions $a_j m_{ij} \equiv 0$ modulo b_i. On remarquera que la i-ième ligne de cette matrice n'est définie que modulo b_i puisque, en posant $y = Mx$, on trouve

$$y_i = m_{i1}x_1 + m_{i2}x_2 + \cdots + m_{ip}x_p \in \mathbb{Z}_{b_i}.$$

L'application Φ est un homomorphisme d'anneaux (*i.e.* Φ respecte la multiplication) si et seulement si, pour $i = 1, \dots, q$, la i-ième ligne de M contient des idempotents deux à deux orthogonaux de $\mathbb{Z}_{b_i}$.

Théorème chinois. — *Soient $a, b > 1$ deux entiers étrangers. Alors l'application canonique*

$$\Phi : \mathbb{Z}_{ab} \longrightarrow \mathbb{Z}_a \oplus \mathbb{Z}_b$$

définie par $\Phi(z) = (z, z)$ est un isomorphisme d'anneaux. En outre, si u, v sont choisis tels que $au + bv = 1$, l'isomorphisme réciproque est

$$\Phi^{-1}(x, y) = bvx + auy.$$

Démonstration. — Commençons par montrer que

$$\Psi(x, y) = bvx + auy$$

définit un homomorphisme de l'anneau $\mathbb{Z}_a \oplus \mathbb{Z}_b$ dans l'anneau $\mathbb{Z}_{ab}$.

- Cette application est bien définie puisque $a(bv) \equiv b(au) \equiv 0$ modulo ab.
- Il est clair que bv et au sont orthogonaux dans $\mathbb{Z}_{ab}$.
- Si nous multiplions $au+bv = 1$ par au ou bv, nous obtenons aussitôt $(au)^2 = au$ et $(bv)^2 = bv$ dans $\mathbb{Z}_{ab}$, ce qui prouve que au et bv sont deux idempotents de $\mathbb{Z}_{ab}$.

On déduit immédiatement de $\Psi(\Phi(z)) = bvz + auz = z$ que Φ et Ψ sont des isomorphismes réciproques. □

2. LES MÉTAMORPHOSES D'UNE SOMME DIRECTE

Le théorème chinois est l'outil rêvé pour répondre aux questions d'isomorphisme qui nous préoccupent. Il est facile de prouver que les anneaux A et B du début sont isomorphes :

$$\begin{aligned} A = \mathbb{Z}_{12} \oplus \mathbb{Z}_{35} \oplus \mathbb{Z}_{45} &\cong \mathbb{Z}_3 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_7 \oplus \mathbb{Z}_{45} \\ &\cong (\mathbb{Z}_3 \oplus \mathbb{Z}_5) \oplus (\mathbb{Z}_4 \oplus \mathbb{Z}_7 \oplus \mathbb{Z}_{45}) \\ &\cong \mathbb{Z}_{15} \oplus \mathbb{Z}_{1260} = B. \end{aligned}$$

En outre, la seconde partie du théorème chinois nous offre la possibilité de rendre explicite cet isomorphisme.

En revanche, et bien qu'ayant le même nombre d'éléments, les anneaux B et C ne sont pas isomorphes car on trouve dans B un élément d'ordre 1260 alors que l'on a $630x = 0$ pour tout élément de C.

Nous allons voir comment généraliser ces idées de manière à déboucher sur un algorithme que nous pourrons programmer.

2.1. Forme réduite d'une somme directe

Il est facile de modifier l'aspect d'une somme directe grâce au théorème chinois. Pour inhiber ces métamorphoses, il faut considérer des groupes dont les ordres ne sont jamais étrangers, ce qui conduit naturellement à la définition suivante.

Définitions

• *Nous dirons que les entiers positifs $d_1, d_2, \ldots, d_n$ vérifient la condition $(\mathcal{D})$ si d_i divise d_{i+1} pour $i = 1, \ldots, n-1$, soit en symboles :*

$$(\mathcal{D}) \qquad d_1 \mid d_2 \mid \cdots \mid d_n.$$

• *Nous dirons que la somme $\mathbb{Z}_{d_1} \oplus \cdots \oplus \mathbb{Z}_{d_n}$ est* réduite *lorsque $d_1, d_2, \ldots, d_n$ vérifient la condition $(\mathcal{D})$.*

Théorème. — *Soient $a_1, \ldots, a_n$ et $b_1, \ldots \ldots b_m$ des entiers > 1 et considérons les groupes ou les anneaux*

$$A = \mathbb{Z}_{a_1} \oplus \mathbb{Z}_{a_2} \oplus \cdots \oplus \mathbb{Z}_{a_n}, \quad B = \mathbb{Z}_{b_1} \oplus \mathbb{Z}_{b_2} \oplus \cdots \oplus \mathbb{Z}_{b_m}.$$

Si les suites $(a_1, \ldots, a_n)$ et $(b_1, \ldots \ldots b_m)$ vérifient la propriété $(\mathcal{D})$, on a l'équivalence

$$A \cong B \iff (a_1, \ldots, a_n) = (b_1, \ldots \ldots b_m).$$

(L'isomorphisme est, au choix, un isomorphisme de groupes ou d'anneaux.)

Démonstration. — Supposons A et B isomorphes ; alors :

- ils ont même cardinal, ce qui s'écrit $a_1 \cdots a_n = b_1 \cdots b_m$;
- l'équation $\alpha x = 0$ possèdent le même nombre de racines dans A et dans B ; sachant que cette équation possède $(\alpha, \beta) = \text{pgcd}(\alpha, \beta)$ racines dans $\mathbb{Z}_\beta$, nous avons ici

$$(1) \qquad (\alpha, a_1)(\alpha, a_2) \cdots (\alpha, a_n) = (\alpha, b_1)(\alpha, b_2) \cdots (\alpha, b_m).$$

Supposons un instant que l'on ait $n < m$. Le dénombrement des racines de l'équation $b_1 x = 0$ montre que l'on a

$$(2) \qquad b_1^m = (b_1, a_1) \cdots (b_1, a_n) \leq b_1^n,$$

ce qui est incompatible avec l'hypothèse $b_1 > 1$. La symétrie du problème interdisant $n > m$, nous concluons que $n = m$.

Nous pouvons aller un peu plus loin : la relation (2) nous apprend que la majoration $(b_1, a_i) \leq b_1$ est en fait une égalité pour $i = 1, \ldots, n$; en particulier, $(b_1, a_1) = b_1$ montre que b_1 divise a_1. Comme les a_i et les b_i jouent le même rôle, on en déduit que l'on a $a_1 = b_1$.

Le dénombrement des racines de l'équation $b_2 x = 0$ montre que l'on a

$$(3) \qquad b_2^{n-1} = (b_2, a_1) \cdots (b_2, a_n).$$

Les majorations $(b_2, a_i) \leq b_2$ et (3) exigent alors $(b_2, a_i) = b_2$ pour $i = 1, \ldots, n-1$. En particulier, $(b_2, a_2) = b_2$ montre que b_2 divise a_2. On montre pareillement que a_2 divise b_2, ce qui prouve que $a_2 = b_2$.

On prouve ainsi de proche en proche que l'on a $a_i = b_i$ pour tous les indices. □

Remarque

Décomposons chaque d_i en facteurs premiers

$$d_i = p_1^{\varepsilon_{i1}} p_2^{\varepsilon_{i2}} \cdots p_k^{\varepsilon_{ik}}, \quad \varepsilon_{i_j} \geq 0,$$

et considérons la matrice des exposants

$$\begin{array}{cccc} \varepsilon_{11} & \varepsilon_{12} & \ldots & \varepsilon_{1k} \\ \varepsilon_{21} & \varepsilon_{22} & \ldots & \varepsilon_{2k} \\ \vdots & \vdots & & \vdots \\ \varepsilon_{n1} & \varepsilon_{n2} & \ldots & \varepsilon_{nk} \end{array} \qquad \begin{array}{c} (\text{exposants de } d_1) \\ (\text{exposants de } d_2) \\ \vdots \\ (\text{exposants de } d_n). \end{array}$$

La condition $(\mathcal{D})$ impose aux colonnes de cette matrice d'être des suites croissantes.

Lorsque $(d_1, d_2, d_3, d_4) = (2, 12, 120, 1800)$, les ε_{ij} sont par exemple

2	3	5	$d_i = 2^\alpha 3^\beta 5^\gamma$
1	0	0	$d_1 = 2$
2	1	0	$d_2 = 12$
3	1	1	$d_3 = 120$
3	2	2	$d_4 = 1800$

2.2. Un algorithme de décomposition-recomposition

Pour répondre à la question de l'isomorphisme des groupes

$$A = \mathbb{Z}_{a_1} \oplus \mathbb{Z}_{a_2} \oplus \cdots \oplus \mathbb{Z}_{a_n} \quad \text{et} \quad B = \mathbb{Z}_{b_1} \oplus \mathbb{Z}_{b_2} \oplus \cdots \oplus \mathbb{Z}_{b_m},$$

il ne nous reste plus qu'à apprendre à mettre ceux-ci sous forme réduite

Isomorphisme d'une somme directe de deux groupes

Théorème d'échange. — *Soient $a, b > 1$ deux entiers quelconques, $d = \mathrm{pgcd}(a, b)$ et $m = \mathrm{ppcm}(a, b)$. On a un isomorphisme de groupes (et même d'anneaux)*

$$\mathbb{Z}_a \oplus \mathbb{Z}_b \cong \mathbb{Z}_d \oplus \mathbb{Z}_m.$$

Démonstration. — Commençons par fixer les notations.

- Les lettres grecques $\alpha, \beta, \lambda, \ldots$ désignent des multi-indices, c'est-à-dire des éléments $\alpha = (\alpha_1, \ldots \ldots \alpha_k)$ de $\mathbb{N}^k$.
- Si α, β sont deux multi-indices de $\mathbb{N}^k$, on dit que l'on a $\alpha < \beta$ (resp. $\alpha \leq \beta$) si l'on a $\alpha_i < \beta_i$ (resp. $\alpha_i \leq \beta_i$) pour $i = 1, \ldots, k$
- Si $\alpha = (\alpha_1, \ldots \ldots \alpha_k)$ et $p = (p_1, \ldots, p_k)$, on note enfin $p^\alpha = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$.

Décomposons maintenant a et b en facteurs premiers (notations condensées) :

$$a = p^{\alpha'} q^{\alpha''} r^\lambda, \quad b = p^{\beta'} q^{\beta''} r^\lambda, \quad \alpha' > \beta', \quad \alpha'' < \beta''.$$

Leur pgcd et leur ppcm sont

$$d = p^{\beta'} q^{\alpha''} r^\lambda, \quad m = p^{\alpha'} q^{\beta''} r^\lambda.$$

On arrive au résultat en appliquant deux fois de suite le théorème chinois :

$$\begin{aligned} \mathbb{Z}_a \oplus \mathbb{Z}_b &= \mathbb{Z}_{p^{\alpha'} q^{\alpha''} r^\lambda} \oplus \mathbb{Z}_{p^{\beta'} q^{\beta''} r^\lambda} \\ &\cong \mathbb{Z}_{p^{\alpha'} r^\lambda} \oplus \mathbb{Z}_{q^{\alpha''}} \oplus \mathbb{Z}_{p^{\beta'} r^\lambda} \oplus \mathbb{Z}_{q^{\beta''}} \\ &\cong \mathbb{Z}_{p^{\beta'} q^{\alpha''} r^\lambda} \oplus \mathbb{Z}_{p^{\alpha'} q^{\beta''} r^\lambda} = \mathbb{Z}_d \oplus \mathbb{Z}_m. \quad \square \end{aligned}$$

Corollaire. — *Les groupes ou les anneaux* $\mathbb{Z}_{a_1} \oplus \mathbb{Z}_{b_1}$ *et* $\mathbb{Z}_{a_2} \oplus \mathbb{Z}_{b_2}$ *sont isomorphes si et seulement si on a* $a_1 b_1 = a_2 b_2$ *et* $\mathrm{pgcd}(a_1, b_1) = \mathrm{pgcd}(a_2, b_2)$.

Isomorphisme d'une somme directe de plusieurs groupes

Commençons par examiner le cas particulier d'une suite $(d_1, \ldots, d_{n-1})$ qui vérifie $(\mathcal{D})$; on se donne $\delta = d_n \geq 2$ et on cherche à définir la nouvelle suite $(d'_1, \ldots, d'_n,)$ qui satisfait encore la condition $(\mathcal{D})$ et

$$\mathbb{Z}_{d_1} \oplus \cdots \oplus \mathbb{Z}_{d_{n-1}} \oplus \mathbb{Z}_{\delta} \cong \mathbb{Z}_{d'_1} \oplus \cdots \oplus \mathbb{Z}_{d'_{n-1}} \oplus \mathbb{Z}_{d'_n}.$$

• Le théorème d'échange appliqué aux entiers d_{n-1} et δ nous garantit qu'en posant $d'_n = \mathrm{ppcm}(d_{n-1}, \delta)$ et $\delta' = d'_{n-1} = \mathrm{pgcd}(d_{n-1}, \delta)$, nous avons

$$\mathbb{Z}_{d_1} \oplus \cdots \oplus \mathbb{Z}_{d_{n-1}} \oplus \mathbb{Z}_{\delta} \cong \mathbb{Z}_{d_1} \oplus \cdots \oplus \mathbb{Z}_{d_{n-2}} \oplus \mathbb{Z}_{\delta'} \oplus \mathbb{Z}_{d'_n}$$

• Nous sommes ainsi ramenés à la même situation avec la suite $(d_1, \ldots, d_{n-2})$ et l'entier δ'. En posant $d'_{n-1} = \mathrm{ppcm}(d_{n-2}, \delta')$ et $\delta'' = d'_{n-2} = \mathrm{pgcd}(d_{n-2}, \delta')$, nous avons l'isomorphisme

$$\mathbb{Z}_{d_1} \oplus \cdots \oplus \mathbb{Z}_{d_{n-1}} \oplus \mathbb{Z}_{\delta} \cong \mathbb{Z}_{d_1} \oplus \cdots \oplus \mathbb{Z}_{d_{n-3}} \oplus \mathbb{Z}_{\delta''} \oplus \mathbb{Z}_{d'_{n-1}} \oplus \mathbb{Z}_{d'_n}.$$

Nous sommes certains que $d'_{n-1} = \mathrm{ppcm}(d_{n-2}, \delta')$ divise $d'_n = \mathrm{ppcm}(d_{n-1}, \delta)$ parce que d_{n-2} divise d_{n-1} et δ' divise δ.

La nouvelle suite $(d'_1, \ldots, d'_n, d'_{n+1})$ s'obtient de proche en proche, ce qui revient à employer l'algorithme :

(A_1)

for $i := n$ **downto** 2 **do begin**
  $a := d[i]$;
  $b := d[i-1]$;
  $d[i] := ppcm(a, b)$;
  $d[i-1] := pgcd(a, b)$
end

Lorsque $n = 2$, cet algorithme se réduit au théorème d'échange.

Si nous partons maintenant d'une suite $(d_1, \ldots, d_n)$ *quelconque*, nous commençons par appliquer le théorème d'échange au couple (d_1, d_2) de manière que d_1 divise d_2 ; cela fait, nous appliquons l'algorithme précédent à (d_1, d_2) et d_3, puis nous recommençons avec (d_1, d_2, d_3) et d_4, et ainsi de suite.

L'algorithme employé est donc :

(A_2)

```
for k := 2 to n do begin
  for i := k downto 2 do begin
    a := d[i] ;
    b := d[i − 1] ;
    d[i] := ppcm(a, b) ;
    d[i − 1] := pgcd(a, b)
  end
end
```

Voici une trace de cet algorithme avec la suite $(36, 70, 120, 150)$:

k	i	36	70	120	150
2	2	2	1260	120	150
3	3	2	60	2520	150
3	2	2	60	2520	150
4	4	2	60	30	12600
4	3	2	30	60	12600
4	2	2	30	60	12600

Exemple
L'algorithme (A_2) transforme $(4, 6, 15, 21)$ en $(1, 3, 6, 420)$ et $(15, 21, 24)$ en $(3, 3, 840)$. On a donc les isomorphismes

$$A = \mathbb{Z}_4 \oplus \mathbb{Z}_6 \oplus \mathbb{Z}_{15} \oplus \mathbb{Z}_{21} \cong \mathbb{Z}_3 \oplus \mathbb{Z}_6 \oplus \mathbb{Z}_{420},$$
$$B = \mathbb{Z}_{15} \oplus \mathbb{Z}_{21} \oplus \mathbb{Z}_{24} \qquad \cong \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_{840}.$$

On notera que l'on a éliminé le groupe $\mathbb{Z}_1 = \{0\}$ de la forme réduite de A. On conclut que les groupes (ou les anneaux) A et B, bien qu'ayant le même cardinal, ne sont pas isomorphes puisque leurs formes réduites ne sont pas identiques.

3. RECHERCHE EXPLICITE DES ISOMORPHISMES

Nous nous sommes contentés jusqu'à présent de répondre par *oui* ou par *non* à la question : «les sommes directes A et B sont-elles isomorphes ?» Mais lorsque la réponse à cette question est positive, nous sommes bien en peine d'exhiber un isomorphisme...

L'examen de la démonstration du théorème d'échange, $\mathbb{Z}_a \oplus \mathbb{Z}_b \cong \mathbb{Z}_d \oplus \mathbb{Z}_m$, montre qu'il est possible d'expliciter l'isomorphisme au prix de la décomposition en facteurs premiers de a et b. Mais comme cette opération est algorithmiquement très coûteuse, nous allons apprendre à la contourner.

Définition. — Soient a_1, a_2, b_1, b_2 quatre entiers > 0. Nous dirons que (a_1, a_2) et (b_1, b_2) sont *bi-étrangers* si tout entier d'indice 1 est étranger à tout entier d'indice 2, c'est-à-dire si

$$\begin{aligned}\operatorname{pgcd}(a_1, a_2) = \operatorname{pgcd}(a_1, b_2) = 1,\\ \operatorname{pgcd}(b_1, a_2) = \operatorname{pgcd}(b_1, b_2) = 1.\end{aligned}$$

Une application immédiate du théorème chinois fournit le résultat suivant.

Théorème d'échange (deuxième version). — *Si les factorisations $a = a_1a_2$ et $b = b_1b_2$ sont bi-étrangères, on a des isomorphismes d'anneaux*

$$\mathbb{Z}_{a_1a_2} \oplus \mathbb{Z}_{b_1b_2} \longrightarrow \mathbb{Z}_{a_1} \oplus \mathbb{Z}_{a_2} \oplus \mathbb{Z}_{b_1} \oplus \mathbb{Z}_{b_2} \longrightarrow \mathbb{Z}_{a_1b_2} \oplus \mathbb{Z}_{b_1a_2}.$$

Plus précisémment, si les entiers u, v, w, t sont choisis tels que l'on ait

$$a_1u + b_2v = 1, \quad a_2w + b_1t = 1,$$

le composé des deux isomorphismes est l'application

$$(x, y) \longmapsto (b_2vx + a_1uy, b_1tx + a_2wy).$$

3.1. Détermination d'une factorisation bi-étrangère

Nous allons maintenant apprendre à calculer les factorisations $a = a_1a_2$ et $b = b_1b_2$ telles que $d = \operatorname{pgcd}(a, b) = a_1b_2$, $m = \operatorname{ppcm}(a, b) = a_2b_1$ et (a_1, a_2), (b_1, b_2) bi-étrangers sans être obligés de décomposer a et b en facteurs premiers.

Définition. — Nous dirons que la boucle

(A_3)

```
d := pgcd(a,b) ;
while d > 1 do begin
|  a := a/d ;
|  b := b * d ;
|  d := pgcd(a,b)
end
```

réalise le *transfert des diviseurs communs* de a vers b.

Exemple

Soient p, q, r trois nombres premiers distincts et α, β deux entiers non divisibles par l'un des nombres p, q ou r ; considérons les entiers

$$a = p^6q^4r^2\alpha, \quad b = pq^2r^5\beta.$$

La boucle (A_3) transfère des diviseurs communs de a vers b de la manière suivante (la troisième colonne contient le diviseur commun d qui se déplace de a vers b) :

$$\begin{aligned} a &= \alpha p^6 q^4 r^2, & b &= p q^2 r^5 \beta, & d &= p q^2 r^2, \\ a &= \alpha p^5 q^2, & b &= p^2 q^4 r^7 \beta, & d &= p^2 q^2, \\ a &= \alpha p^3, & b &= p^4 q^6 r^7 \beta, & d &= p^3, \\ a &= \alpha, & b &= p^7 q^6 r^7 \beta, & d &= 1. \end{aligned}$$

Insistons : l'algorithme de transfert n'utilise que la fonction pgcd ; les nombres premiers ne figurent ici que pour faciliter la compréhension de la dynamique des calculs.

Soient $a, b > 1$ deux entiers, $m = \mathrm{ppcm}(a, b)$ et $d = \mathrm{pgcd}(a, b)$; posons

$$a = d a_2, \quad b = d b_2. \tag{1}$$

Nous savons que a_2 et b_2 sont étrangers ; cependant, ces décompositions en facteurs ne conviennent pas encore car (d, a_2) d'une part et (d, b_2) d'autre part ne sont pas étrangers en général.

C'est pour cette raison que nous transférons les diviseurs communs de d vers a_2 et de d vers b_2 à l'aide de boucle (A_3), ce qui donne

$$a = a_1 a_2', \quad b = b_1 b_2'. \tag{2}$$

Si $d_1, \ldots, d_k$ sont les diviseurs communs qui se déplacent de d vers a_2, nous avons $a_1 = d/(d_1 \cdots d_k)$ et $a_2' = d_1 \cdots d_k a_2$. Les notations b_1, b_2' sont analogues (on notera toutefois que ce ne sont pas forcément les mêmes diviseurs qui se déplacent de d vers b_2). Comme a_2 a reçu des nombres qui le divisent et comme il en est de même de b_2, nous sommes certains que a_2' et b_2' sont étrangers. En outre, a_1 est étranger à a_2' et b_1 est étranger à b_2'.

Mais il ne s'agit pas encore d'une factorisation bi-étrangère car, si nous échangeons les facteurs a_2' et b_2' dans a et b, nous obtenons les entiers $a_1 b_2'$ et $b_1 a_2'$; or a_1 et b_2' n'ont aucune raison d'être étrangers. Pour remédier à ce dernier défaut, posons $\delta = \mathrm{pgcd}(a_1, b_1)$, ce qui permet d'écrire

$$a = a_1' \delta a_2', \quad b = b_1' \delta b_2'. \tag{3}$$

Lemme. — *Avec les notations précédentes, les décompositions*

$$a = a_2'(a_1' \delta), \quad b = b_1'(\delta b_2')$$

sont bi-étrangères. En outre, après échange des derniers facteurs dans a et b, l'un des entiers $a_2'(\delta b_2')$ ou $b_1'(a_1' \delta)$ est le pgcd de a et b, l'autre étant leur ppcm.

Démonstration. — Décomposons a et b en facteurs premiers (notations condensées)

$$a = p^{\alpha'} q^{\alpha''} r^{\lambda}, \quad b = p^{\beta'} q^{\beta''} r^{\lambda}, \quad \alpha' > \beta', \quad \alpha'' < \beta''.$$

Leur pgcd est $d = p^{\beta'} q^{\alpha''} r^{\lambda}$ et (1) devient

$$(1') \qquad a = (p^{\beta'} q^{\alpha''} r^{\lambda})(p^{\alpha'-\beta'}), \quad b = (p^{\beta'} q^{\alpha''} r^{\lambda})(q^{\beta''-\alpha''}).$$

Comme $\alpha' - \beta' > 0$, les diviseurs communs qui passent de $p^{\beta'} q^{\alpha''} r^{\lambda}$ dans $p^{\alpha'-\beta'}$ sont ceux du produit $p^{\beta'}$; de manière analogue, le transfert déplace $q^{\alpha''}$ du premier facteur de b au second facteur

$$(2') \qquad a = (q^{\alpha''} r^{\lambda})(p^{\alpha'}), \quad b = (p^{\beta'} r^{\lambda})(q^{\beta''}).$$

Le pgcd des premiers facteurs de a et b étant r^{λ}, il vient

$$(3') \qquad a = (q^{\alpha''})(r^{\lambda})(p^{\alpha'}), \quad b = (p^{\beta'})(r^{\lambda})(q^{\beta''}).$$

Il résulte alors de ce calcul que les décompositions

$$a = p^{\alpha'}(q^{\alpha''} r^{\lambda}), \quad b = p^{\beta'}(r^{\lambda} q^{\beta''}).$$

sont bi-étrangères. Le pgcd et le ppcm s'obtiennent bien par échange des derniers facteurs $q^{\alpha''} r^{\lambda}$ et $r^{\lambda} q^{\beta''}$ puisque $m = p^{\alpha'}(r^{\lambda} q^{\beta''})$ et $d = p^{\beta'}(q^{\alpha''} r^{\lambda})$. □

Exemple

Considérons les entiers

$$a = 1\,792\,929\,600 = 2^6 \times 3^3 \times 5^2 \times 7^3 \times 11^2,$$
$$b = 32\,683\,612\,500 = 2^2 \times 3^2 \times 5^5 \times 7^4 \times 11^2,$$

les décompositions en facteurs premiers facilitant la compréhension des calculs. Le pgcd de a et b est $d = 37\,352\,700 = 2^2 \times 3^2 \times 5^2 \times 7^3 \times 11^2$, d'où les décompositions

$$a = 37\,352\,700 \times 48 = (2^2 \times 3^2 \times 5^2 \times 7^3 \times 11^2)(2^4 \times 3),$$
$$b = 37\,352\,700 \times 7 = (2^2 \times 3^2 \times 5^2 \times 7^3 \times 11^2)(7).$$

Transférons les diviseurs 2 et 3 du pgcd vers le second facteur de a et les diviseurs 7 du pgcd vers le second facteur de b :

$$a = 1\,037\,575 \times 1\,728 = (5^2 \times 7^3 \times 11^2)(2^6 \times 3^3),$$
$$b = 108\,900 \times 2\,401 = (2^2 \times 3^2 \times 5^2 \times 11^2)(7^4).$$

Isolons enfin le pgcd $3\,025 = 5^2 \times 11^2$ des premiers facteurs de a et b :

$$a = 343 \times 3\,025 \times 1\,728 = (7^3)(5^2 \times 11^2)(2^6 \times 3^3),$$
$$b = 36 \times 3\,025 \times 2\,401 = (2^2 \times 3^2)(5^2 \times 11^2)(7^4).$$

Les factorisations bi-étrangères recherchées s'obtiennent en échangeant le premier et le dernier facteur de a puis en effectutant le produit des deux derniers facteurs :

$$a = 1\,728 \times (343 \times 3\,025) = 1\,728 \times 1\,037\,575 = (2^6 \times 3^3)(5^2 \times 7^3 \times 11^2),$$
$$b = 36 \times (3\,025 \times 2\,401) = 900 \times 7\,263\,025 = (2^2 \times 3^2)(5^2 \times 7^4 \times 11^2).$$

Vérification : nous obtenons bien le pgcd et le ppcm en échangeant les derniers facteurs :

$$12\,550\,507\,200 = 1\,728 \times 7\,263\,025 = (2^6 \times 3^3)(5^2 \times 7^4 \times 11^2),$$
$$37\,352\,700 = 36 \times 1\,037\,575 = (2^2 \times 3^2)(5^2 \times 7^3 \times 11^2).$$

3.2. Implémentation du théorème d'échange pour deux anneaux

Le programme qui construit explicitement l'isomorphisme entre $\mathbb{Z}_a \oplus \mathbb{Z}_b$ et $\mathbb{Z}_d \oplus \mathbb{Z}_m$ est donc le suivant :

- On calcule $d = \mathrm{pgcd}(a, b)$, ce qui définit $a = d \times a_2$ et $b = d \times b_2$, puis on transfère les diviseurs communs de d vers a_2 et b_2 (nous avons à la sortie $a = \delta a_1 \times a_2$ et $b = \delta b_1 \times b_2$) :

$d := pgcd(a, b)$;
$da := d$; $a_2 := a$ **div** da ;
$transfert\_diviseurs\_communs(da, a_2)$;
$db := d$; $b_2 := b$ **div** db ;
$transfert\_diviseurs\_communs(db, b_2)$;

- On isole ensuite le pgcd δ de da et db de manière à obtenir les factorisations $a = a_1 \times \delta \times a_2$ et $b = b_1 \times \delta \times b_2$. Cela fait, on échange les contenus de a_1 et a_2, de sorte que les factorisation bi-étrangères désirées sont maintenant $a = a_1 \times \delta a_2$ et $b = b_1 \times \delta b_2$:

$delta := pgcd(da, db)$;
$a_1 := da$ **div** $delta$; $b_1 := db$ **div** $delta$;
$swap(a_1, a_2)$;
$a_2 := delta * a_2$; $b_2 := delta * b_2$;

- On définit $d = a_1 b_2$ et $m = a_2 b_1$, qui sont, à transposition près, le pgcd et le ppcm de a de b; on recherche u, v, w, t tels que $a_1 u + b_2 v = a_2 w + b_1 t = 1$, ce qui permet de définir la matrice (m_{ij}) de l'isomorphisme $\mathbb{Z}_a \oplus \mathbb{Z}_b \to \mathbb{Z}_d \oplus \mathbb{Z}_m$:

$d := a_1 * b_2$; $m := b_1 * a_2$;
$Bezout(a_1, b_2, u, v)$; $Bezout(b_1, a_2, w, t)$;
$m_{11} := b_2 * v$; $m_{12} := a_1 * u$;
$m_{21} := b_1 * w$; $m_{22} := a_2 * t$;

- Lorsque d ne divise pas m, ce qui correspond au cas $d = \mathrm{ppcm}(a, b)$ et

$m = \text{pgcd}(a, b)$, on échange les contenus de d et m, ce qui a pour effet d'échanger les lignes de la matrice des (m_{ij}) :

if m **mod** $d > 0$ **then** *transposition* := *true* **else** *transposition* := *false* ;
if *transposition* **then begin**
  $swap(d, m)$;
  $swap(m_{11}, m_{21})$;
  $swap(m_{12}, m_{22})$;
end ;

L'isomorphisme d'anneaux cherché est

$$\Phi : \mathbb{Z}_a \oplus \mathbb{Z}_b \longrightarrow \mathbb{Z}_d \oplus \mathbb{Z}_m,$$

$$(x, y) \longmapsto (m_{11}x + m_{12}y, m_{21}x + m_{22}y)$$

- L'isomorphisme réciproque

$$\Psi = \Phi^{-1} : \mathbb{Z}_d \oplus \mathbb{Z}_m \to \mathbb{Z}_a \oplus \mathbb{Z}_b$$
$$(x, y) \longmapsto (M_{11}x + M_{12}y, M_{21}x + M_{22}y)$$

s'obtient en déterminant u, v, w, t tels que $a_1u + a_2v = b_1w + b_2t = 1$:

$Bezout(a_1, a_2, u, v)$; $Bezout(b_1, b_2, w, t)$;
$M_{11} := a_2 * v$; $M_{12} := a_1 * u$;
$M_{21} := b_1 * w$; $M_{22} := b_2 * t$;
if *transposition* **then begin**
  $swap(M_{11}, M_{12})$;
  $swap(M_{21}, M_{22})$
end

Exemple

Lorsque $a = 350$ et $b = 980$, on obtient les isomorphismes d'anneaux :

$$\Phi : \mathbb{Z}_{350} \oplus \mathbb{Z}_{980} \longrightarrow \mathbb{Z}_{70} \oplus \mathbb{Z}_{4900},$$
$$(x, y) \longmapsto (15x - 14y, 1176x - 1175y)$$

$$\Psi = \Phi^{-1} : \mathbb{Z}_{70} \oplus \mathbb{Z}_{4900} \longrightarrow \mathbb{Z}_{350} \oplus \mathbb{Z}_{980},$$
$$(x, y) \longmapsto (-125x + 126y, 196x - 195y)$$

3.3. Isomorphisme entre deux sommes directes quelconques

Nous savons maintenant que deux sommes directes de groupes ou d'anneaux sont isomorphes si et seulement si leurs formes réduites le sont. Ce résultat nous autorise donc à nous contenter d'expliciter les isomorphismes (direct et réciproque) entre une somme directe et sa forme réduite. Considérons par exemple l'anneau

$$\mathbb{Z}_{36} \oplus \mathbb{Z}_{120} \oplus \mathbb{Z}_{150}.$$

L'algorithme (A_2) tranforme la suite $(36, 120, 150)$ en la suite $(6, 60, 1800)$ en passant par les suites intermédiaires $(12, 360, 150)$ et $(12, 30, 1800)$ et le théorème d'échange fournit les isomorphismes

$$\begin{aligned}\Phi_A &: \mathbb{Z}_{36} \oplus \mathbb{Z}_{120} \oplus \mathbb{Z}_{150} \longrightarrow \mathbb{Z}_{12} \oplus \mathbb{Z}_{360} \oplus \mathbb{Z}_{150},\\ \Phi_B &: \mathbb{Z}_{12} \oplus \mathbb{Z}_{360} \oplus \mathbb{Z}_{150} \longrightarrow \mathbb{Z}_{12} \oplus \mathbb{Z}_{30} \oplus \mathbb{Z}_{1800},\\ \Phi_C &: \mathbb{Z}_{12} \oplus \mathbb{Z}_{30} \oplus \mathbb{Z}_{1800} \longrightarrow \mathbb{Z}_{6} \oplus \mathbb{Z}_{60} \oplus \mathbb{Z}_{1800},\end{aligned}$$

de matrices respectives

$$\Phi_A = \begin{pmatrix} -3 & 4 & 0 \\ -80 & 81 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad \Phi_B = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 6 & 5 \\ 0 & -575 & 576 \end{pmatrix}, \quad \Phi_C = \begin{pmatrix} -2 & 3 & 0 \\ -15 & 16 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

L'isomorphisme composé

$$\Phi = \Phi_C \circ \Phi_B \circ \Phi_A : \mathbb{Z}_{36} \oplus \mathbb{Z}_{120} \oplus \mathbb{Z}_{150} \longrightarrow \mathbb{Z}_{6} \oplus \mathbb{Z}_{60} \oplus \mathbb{Z}_{1800}$$

a donc pour matrice associée

$$\Phi = \Phi_C\Phi_B\Phi_A = \begin{pmatrix} -1434 & 1450 & -15 \\ -7635 & 7716 & -80 \\ 46000 & -46575 & 576 \end{pmatrix} \equiv \begin{pmatrix} 0 & 4 & 3 \\ 45 & 36 & 40 \\ 1000 & 225 & 576 \end{pmatrix}$$

puisque, la première ligne est définie modulo 6, la seconde modulo 60 et la troisième modulo 1800.

Interlude

Comme les calculs deviennent compliqués, rassurons-nous en vérifiant *directement* que cette matrice définit bien un isomorphisme d'anneaux :

- Les congruences $a_j m_{ij} \equiv 0$ modulo b_i sont respectées, ce qui montre que Φ est une application.
- L'application Φ est un homomorphisme d'anneaux puisque :
  — 4 et 3 sont des idempotents orthogonaux de $\mathbb{Z}_6$;
  — 45, 36 et 40 sont des idempotents deux à deux orthogonaux de $\mathbb{Z}_{120}$;
  — 1000, 225 et 576 sont des idempotents deux à deux orthogonaux de $\mathbb{Z}_{1800}$.
- Comme $\mathbb{Z}_{36} \oplus \mathbb{Z}_{120} \oplus \mathbb{Z}_{150}$ et $\mathbb{Z}_{6} \oplus \mathbb{Z}_{60} \oplus \mathbb{Z}_{1800}$ ont le même cardinal, nous pouvons nous contenter de vérifier que Φ est injective pour nous assurer que c'est un isomorphisme d'anneaux. Si $\Phi(x, y, z) = (0, 0, 0)$, on voit facilement que :
  — $4y + 3z = 6k$ implique $y \equiv 0 \pmod 3$ et $z \equiv 0 \pmod 2$;
  — $45x + 36y + 40z = 60h$ implique $x \equiv 0 \pmod 4$, $y \equiv 0 \pmod 5$ et $z \equiv 0 \pmod 3$;
  — $1000x + 225y + 576z = 1800\ell$ implique $x \equiv 0 \pmod 9$, $y \equiv 0 \pmod 8$ et $z \equiv 0 \pmod{25}$.

Par conséquent, on a $x \equiv 0 \pmod{36}$, $y \equiv 0 \pmod{120}$ et $z \equiv 0 \pmod{150}$.

Le théorème d'échange nous fournit aussi, en même temps que les isomorphisme directes Φ_A, Φ_B, Φ_C, les isomorphisme réciproques

$$\begin{aligned}
\Psi_A &: \mathbb{Z}_{12} \oplus \mathbb{Z}_{360} \oplus \mathbb{Z}_{150} \longrightarrow \mathbb{Z}_{36} \oplus \mathbb{Z}_{120} \oplus \mathbb{Z}_{150},\\
\Psi_B &: \mathbb{Z}_{12} \oplus \mathbb{Z}_{30} \oplus \mathbb{Z}_{1800} \longrightarrow \mathbb{Z}_{12} \oplus \mathbb{Z}_{360} \oplus \mathbb{Z}_{150},\\
\Psi_C &: \mathbb{Z}_{6} \oplus \mathbb{Z}_{60} \oplus \mathbb{Z}_{1800} \longrightarrow \mathbb{Z}_{12} \oplus \mathbb{Z}_{30} \oplus \mathbb{Z}_{1800},
\end{aligned}$$

dont les matrices associées sont

$$\Psi_A = \begin{pmatrix} 9 & -8 & 0 \\ 40 & -39 & 0 \\ 0 & 0 & 1 \end{pmatrix},\ \Psi_B = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -144 & 145 \\ 0 & 25 & -24 \end{pmatrix},\ \Psi_C = \begin{pmatrix} 4 & -3 & 0 \\ 15 & -14 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

L'isomorphisme composé est donc

$$\Psi = \Psi_A\Psi_B\Psi_C : \mathbb{Z}_6 \oplus \mathbb{Z}_{60} \oplus \mathbb{Z}_{1800} \longrightarrow \mathbb{Z}_{36} \oplus \mathbb{Z}_{120} \oplus \mathbb{Z}_{150}$$

et sa matrice est

$$\Psi = \Psi_A\Psi_B\Psi_C \equiv \begin{pmatrix} 0 & 9 & 28 \\ 40 & 96 & 105 \\ 75 & 100 & 126 \end{pmatrix}.$$

Pour contrôler ce résultat, on vérifie que l'on a $\Psi\Phi \equiv I$ ainsi que $\Phi\Psi \equiv I$ (ne pas oublier que les lignes de la matrice $\Psi\Phi$ sont définies modulo 36, 120 et 150 alors que celles de la matrice $\Phi\Psi$ sont définies modulo 6, 60 et 1800).

3.4. Le programme

La transformation en programme de l'exemple que nous venons de traiter ne présente pas de difficulté particulière. On commence par saisir le nombre n de facteurs puis le vecteur $d_1, \ldots, d_n$. La détermination des isomorphismes s'obtient en greffant à l'intérieur de l'algorithme (A_2), qui transforme la suite $d_1, \ldots, d_n$, le calcul de la matrice (a_{ij}) de la matrice de l'isomorphisme d'échange

$$\mathbb{Z}_\alpha \oplus \mathbb{Z}_\beta \longrightarrow \mathbb{Z}_\delta \oplus \mathbb{Z}_\mu,$$

avec $\alpha = d_{i-1}$, $\beta = d_i$, $\delta = \mathrm{pgcd}(a, b)$, $\mu = \mathrm{ppcm}(a, b)$ et celle de la matrice (aa_{ij}) de l'isomorphisme réciproque.

On enchasse ensuite les matrices (a_{ij}) et (aa_{ij}) dans des matrices unités de dimension n pour trouver les matrices Φ_A et Ψ_A des isomorphismes partiels

$$\mathbb{Z}_{d_1} \oplus \cdots \mathbb{Z}_\alpha \oplus \mathbb{Z}_\beta \oplus \cdots \mathbb{Z}_{d_n} \underset{\Psi_A}{\overset{\Phi_A}{\rightleftharpoons}} \mathbb{Z}_{d_1} \oplus \cdots \mathbb{Z}_\delta \oplus \mathbb{Z}_\mu \oplus \cdots \mathbb{Z}_{d_n}.$$

On compose ces isomorphismes partiels, en multipliant au fur et à mesure les matrices correspondantes. Il y a un petit piège à éviter : si nous examinons notre

exemple, nous constatons que nous obtenons les couples de matrices (Φ_A, Ψ_A), (Φ_B, Ψ_B), (Φ_C, Ψ_C) *dans cet ordre*; comme nous désirons calculer $\Phi_C\Phi_B\Phi_A$ et $\Psi_A\Psi_B\Psi_C$, nous devons réfléchir un peu à l'ordre des multiplications.

Les boucles terminées, on affiche les matrices trouvées modulo les valeurs initiales *init_d* et finales *d*.

```
init_d := d ; Phi := unite(n) ; Psi := unite(n) ;
for k := 2 to n do begin
  for i := k downto 2 do begin
    α := d[i − 1] ; β := d[i] ;
    δ := pgcd(a, b) ; μ := ppcm(α, β) ;
    d[i] := μ ; d[i − 1] := δ ;
    {— théorème d'échange —}
    echange(α, β, δ, μ, a11, a12, a21, a22, aa11, aa12, aa21, aa22) ;
    {— insertion des (a_ij) dans une matrice unité —}
    Phi_A := unite(n) ;
    Phi_A[i − 1, i − 1] := a11 ; Phi_A[i − 1, i] := a12 ;
    Phi_A[i, i − 1] := a21 ; Phi_A[i, i] := a22 ;
    {— insertion des (aa_ij) dans une matrice unité —}
    Psi_A := unite(n) ;
    Psi_A[i − 1, i − 1] := aa11 ; Psi_A[i − 1, i] := aa12 ;
    Psi_A[i, i − 1] := aa21 ; Psi_A[i, i] := aa22 ;
    {— composition des isomorphismes —}
    Phi := mult_mat(Phi_A, Phi) ;
    Psi := mult_mat(Psi, Psi_A) ;
  end
end ;
afficher_iso(Phi, init_d, d) ;
afficher_iso(Psi, d, init_d)
```

Exemple

Considérons les anneaux

$$\mathbb{Z}_9 \oplus \mathbb{Z}_{12} \oplus \mathbb{Z}_{25} \oplus \mathbb{Z}_{40} \quad \text{et} \quad \mathbb{Z}_{24} \oplus \mathbb{Z}_{45} \oplus \mathbb{Z}_{100}.$$

Le programme précédent fournit les isomorphismes

$$\mathbb{Z}_9 \oplus \mathbb{Z}_{12} \oplus \mathbb{Z}_{25} \oplus \mathbb{Z}_{40} \xrightarrow{\Phi_1} \mathbb{Z}_{60} \oplus \mathbb{Z}_{1800} \xrightarrow{\Psi_2} \mathbb{Z}_{24} \oplus \mathbb{Z}_{45} \oplus \mathbb{Z}_{100}$$

de matrices respectives

$$\Phi_1 = \begin{pmatrix} 0 & 25 & 0 & 36 \\ 1000 & 0 & 576 & 225 \end{pmatrix}, \quad \Psi_2 = \begin{pmatrix} 16 & 9 \\ 36 & 10 \\ 25 & 76 \end{pmatrix}.$$

L'isomorphisme composé

$$\mathbb{Z}_9 \oplus \mathbb{Z}_{12} \oplus \mathbb{Z}_{25} \oplus \mathbb{Z}_{40} \xrightarrow{\Psi_2 \circ \Phi_1} \mathbb{Z}_{24} \oplus \mathbb{Z}_{45} \oplus \mathbb{Z}_{100}$$

a donc pour matrice

$$\Psi_2\Phi_1 = \begin{pmatrix} 9000 & 400 & 5184 & 2601 \\ 10000 & 900 & 5760 & 3546 \\ 76000 & 625 & 43776 & 18000 \end{pmatrix} \equiv \begin{pmatrix} 0 & 16 & 0 & 9 \\ 10 & 0 & 0 & 36 \\ 0 & 25 & 76 & 0 \end{pmatrix}.$$

On trouve de même les isomophismes d'anneaux

$$\mathbb{Z}_{24} \oplus \mathbb{Z}_{45} \oplus \mathbb{Z}_{100} \xrightarrow{\Phi_2} \mathbb{Z}_{60} \oplus \mathbb{Z}_{1800} \xrightarrow{\Psi_1} \mathbb{Z}_9 \oplus \mathbb{Z}_{12} \oplus \mathbb{Z}_{25} \oplus \mathbb{Z}_{40}$$

de matrices respectives

$$\Phi_2 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \\ 0 & 1 \\ 16 & 25 \end{pmatrix}, \quad \Psi_1 = \begin{pmatrix} 40 & 36 & 45 \\ 225 & 1000 & 576 \end{pmatrix},$$

ce qui donne l'isomorphisme composé

$$\mathbb{Z}_{24} \oplus \mathbb{Z}_{45} \oplus \mathbb{Z}_{100} \xrightarrow{\Psi_1 \circ \Phi_2} \mathbb{Z}_9 \oplus \mathbb{Z}_{12} \oplus \mathbb{Z}_{25} \oplus \mathbb{Z}_{40}$$

de matrice

$$\Psi_1\Phi_2 = \begin{pmatrix} 225 & 1000 & 576 \\ 40 & 36 & 45 \\ 225 & 1000 & 576 \\ 6265 & 25576 & 15120 \end{pmatrix} \equiv \begin{pmatrix} 0 & 1 & 0 \\ 4 & 0 & 9 \\ 0 & 0 & 1 \\ 25 & 16 & 0 \end{pmatrix}.$$

Remarques

• On peut facilement contrôler que les matrices définissent des homomorphismes d'anneaux à l'aide des résultats suivants :

anneau	*idempotents*	*anneau*	*idempotents*
$\mathbb{Z}_9$	$0, 1$	$\mathbb{Z}_{24}$	$0, 1, 9, 16$
$\mathbb{Z}_{12}$	$0, 1, 4, 9$	$\mathbb{Z}_{45}$	$0, 1, 10, 36$
$\mathbb{Z}_{25}$	$0, 1$	$\mathbb{Z}_{100}$	$0, 1, 25, 76$
$\mathbb{Z}_{40}$	$0, 1, 16, 25$		

• Il est facile de s'assurer que les matrices $\Psi_2\Phi_1\Psi_1\Phi_2$ et $\Psi_1\Phi_2\Psi_2\Phi_1$ sont des matrices unités.