Algorithme des facteurs invariants

Arnaud Girand

19 juin 2012

Référence :
- [BMP05], p. 285–288

On se propose de démontrer de façon algorithmique l'existence [1] de la décomposition suivante :

Proposition 1
Soit $(\mathbb{A}, \delta)$ un anneau euclidien.
Soit $U \in \mathcal{M}_{m,n}(\mathbb{A})$.
Alors il existe $d_1, \dots, d_s \in \mathbb{A}^*$ tels que $\forall i \in [s-1]$, $d_i | d_{i+1}$ et $(P, Q) \in GL_m(\mathbb{A}) \times GL_n(\mathbb{A})$ tels que :

$$U = PDQ, \text{ où } D := \begin{pmatrix} d_1 & & & (0) \\ & \ddots & & \\ & & d_s & \\ (0) & & & (0) \end{pmatrix}$$

On considère donc l'algorithme [2] suivant :

Algorithme 1 (Facteurs invariants)
`Entrée` : *$U \in \mathcal{M}_{m,n}(\mathbb{A})*
`Sortie` : *$D \in \mathcal{M}_{m,n}(\mathbb{A})$ correspondant à la réduction de U donnée dans la proposition 1.*
On suit alors les étapes suivantes :

1. `Si` *$U = 0$, renvoyer U.* `Sinon`, *passer à l'étape 2.*
2. Choix d'un pivot. *Sélectionner $(i_0, j_0) \in [m] \times [n]$ tel que $\delta(u_{i_0,j_0}) = inf\{\delta(u_{i,j}) \,|\, u_{i,j} \neq 0\}$. Effectuer ensuite les opérations élémentaires suivantes :*

$$C_1 \leftrightarrow C_{j_0} \tag{1}$$
$$L_1 \leftrightarrow L_{i_0} \tag{2}$$

3. Traitement de la première colonne. *Initialiser un compteur $i \leftarrow 2$.*
   (a) *Par division euclidienne, on peut écrire (dans $\mathbb{A}$) :*

$$u_{i,1} = u_{1,1}q + r_i, \text{ avec } r_i = 0 \text{ ou } \delta(r_i) < \delta(u_{1,1})$$

   Effectuer alors l'opération suivante :

$$L_i \leftarrow L_i - qL_1 \tag{3}$$

   On a ainsi remplacé $u_{i,1}$ par r_i.
   (b) `Si` *$r_i \neq 0$, effectuer l'opération suivante :*

$$L_i \leftrightarrow L_1 \tag{4}$$

   Retourner ensuite en 3.(a).
   (c) `Si` *$r_i = 0$ et $i < m$, incrémenter i ($i \leftarrow i + 1$) et retourner en 3.(a).*

1. Le lecteur averti aura remarqué qu'on peut également énoncer un résultat d'unicité de cette dernière. On peut d'ailleurs en trouver une démonstration dans [BMP05], p. 289.
2. On ne se privera donc pas de faire usage des conventions d'écriture propres à l'algorithmique, par exemple en continuant de noter U notre matrice quelques soient les sévices que nous lui ferons subir.

(d) `Sinon` *passer à l'étape* 4. *On a désormais :*

$$C_1 = \begin{pmatrix} u_{1,1} \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

4. Traitement de la première ligne. *Initialiser un compteur* $j \leftarrow 2$.

(a) Par division euclidienne on a :

$$u_{1,j} = u_{1,1}q + s_j, \text{ avec } s_j = 0 \text{ ou } \delta(s_j) < \delta(u_{1,1})$$

Effectuer ensuite l'opération suivante :

$$C_j \leftarrow C_j - qC_1 \tag{5}$$

On a ainsi remplacé $u_{1,j}$ *par* s_j.

(b) `Si` $s_j \neq 0$, *effectuer l'opération suivante :*

$$C_j \leftrightarrow C_1 \tag{6}$$

Retourner ensuite en 4.(*a*).

(c) `Si` $s_j = 0$ *et* $j < n$, *incrémenter* j *et retourner en* 4.(*a*).

(d) `Sinon` *passer à l'étape* 5. *On a désormais :*

$$U = \begin{pmatrix} u_{1,1} & 0 & \dots & 0 \\ 0 & & & \\ \vdots & & & \\ \vdots & & (*) & \\ 0 & & & \end{pmatrix}$$

5. Vérification de la divisibilité.

(a) `Si` *il existe* $i_1, j_1 \geq 2$ *tels que* $u_{1,1} \nmid u_{i_1,j_1}$, *effectuer l'opération suivante :*

$$C_1 \leftarrow C_1 + C_{j_1} \tag{7}$$

Retourner ensuite en 3.

(b) `Sinon` *retourner en* 1 *avec* $U \leftarrow (u_{i,j})_{2 \leq i \leq m, 2 \leq j \leq n}$ *(i.e on finit le traitement de façon récursive).*

TERMINAISON : L'idée est ici de montrer que chaque retour en arrière fait strictement décroître l'entier $\delta(u_{1,1})$. On conclura alors qu'il n'est possible d'effectuer qu'un nombre fini d'étapes et donc que l'algorithme termine.

Les étapes 1 et 2 ne posent pas de problèmes [3]. Lors de l'étape 3, on ne rebrousse chemin que si $r_i \neq 0$ (étape 3.(*b*)) et alors on remplace $u_{1,1}$ par r_i ce que implique une décroissance stricte de $\delta(u_{1,1})$. Ceci ne pouvant de facto arriver qu'un nombre fini de fois, on passera [4] nécessairement à l'étape 4.

Durant l'étape 4, on ne retournera en arrière qu'à l'expresse condition que $s_j \neq 0$ (4.(*b*)). Comme précédemment, on en déduit qu'on passera nécessairement à l'étape 5.

Passer de l'étape 5 à une étape antérieure (en l'occurence 3) requière qu'il $i_1, j_1 \geq 2$ tels que $u_{1,1} \nmid u_{i_1,j_1}$. On remplace alors C_1 par $C_1 + C_{j_1}$ ce qui, au vu de l'état de notre matrice U, laisse $u_{1,1}$ inchangé et remplace $u_{i_1,1}$ par u_{i_1,j_1} et donc $r_{i_1} \neq 0$. Ainsi ce passage par l'étape 3 verra strictement décroître $\delta(u_{1,1})$; on ne pourra donc se permettre qu'un nombre fini de telles excentricités, entraînant que l'algorithme termine.

3. Ou alors c'est que vous vous y prenez *très* mal ...
4. Un jour ...

Correction : Au bout d'une itération de l'algorithme (i.e avant de poursuivre récursivement) on obtient une matrice U' de la forme suivante [5] :

$$U' = \begin{pmatrix} u'_{1,1} & 0 & \dots & 0 \\ 0 & & & \\ \vdots & & & \\ \vdots & & U_1 & \\ 0 & & & \end{pmatrix}$$

L'étape 5 nous assure par ailleurs que $u'_{1,1}$ divise tous les coefficients de U_1. Chaque étape de notre algorithme n'étant au final, une fois les tests conditionnels et autres fioritures éliminées, qu'une succession d'opérations élémentaires sur les lignes et colonnes, il existe $(P, Q) \in GL_m(\mathbb{A}) \times GL_n(\mathbb{A})$ telles que $U = PU'Q$.

De même, il va exister $(P_1, Q_1) \in GL_{m-1}(\mathbb{A}) \times GL_{n-1}(\mathbb{A})$ telles que $U_1 = P_1 U'_1 Q_1$, où :

$$U'_1 = \begin{pmatrix} u''_{2,2} & 0 & \dots & 0 \\ 0 & & & \\ \vdots & & & \\ \vdots & & U_2 & \\ 0 & & & \end{pmatrix}$$

Ainsi, si on pose :

$$P'_1 = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & & & \\ \vdots & & P_1 & \\ 0 & & & \end{pmatrix} \qquad \text{et} \qquad Q'_1 = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & & & \\ \vdots & & Q_1 & \\ 0 & & & \end{pmatrix}$$

On a :

$$U = PP'_1 \begin{pmatrix} u'_{1,1} & 0 & \dots & 0 \\ 0 & u''_{2,2} & & \\ \vdots & & & \\ \vdots & & U_2 & \\ 0 & & & \end{pmatrix} Q'_1 Q$$

Comme nous n'avons effectué que des opérations élémentaires que que $u_{1,1}$ divisait tous les coefficients de U_1 il divise tous ceux de U_2 ainsi que $u''_{2,2}$. De plus l'étape 5 (itération 2) nous assure que $u''_{2,2}$ divise tous les coefficients de U_2. Par récurrence (utiliser l'invariant de boucle que l'on vient d'énoncer concernant la divisibilité), l'algorithme est correct.

Références

[BMP05] Vincent Beck, Jérôme Malick, and Gabriel Peyré. *Objectif Agrégation (2e édition)*. H & K, 2005.

5. Ce paragraphe contenant un raisonnement mathématique, il n'est plus réellement tolérable de continuer à la noter U. Ceci étant, chacun reste libre d'en faire à sa guise.