Forme normale de Smith

Introduction

N.B. on présente ici une version un peu tirée par les cheveux de l'algo car on s'interdit d'utiliser des matrices de permutation, afin que c'est possible, et que l'algorithme fonctionne aussi à l'intérieur de $\mathrm{SL}_n(R)$. Cela permet d'en déduire que $\mathrm{SL}_n(R)$ est engendré par les transvections dès que R est euclidien.

Attention cependant : Le recasage en 108 est impossible. En effet, si on veut seulement prouver que $\mathrm{SL}_n(R)$ est engendré par les transvections, il suffit d'échelonner la première colonne uniquement. En effet, le déterminant de A étant 1, il vient que a_{11} est inversible. Donc on peut échelonner le reste gratuitement puis recommencer, cela ne demande qu'une toute partie de l'algorithme de Smith.

I. L'algorithme

Le « stathme minimal » sur une portion de M est le minimum des stathmes des coefficients non nuls de cette portion.

Le but d'une « itération » est de transformer A en une matrice diagonale par blocs, l'un de taille 1×1, a_{11}, divisant l'autre bloc.

A Entrée dans l'algorithme, préparation de la première colonne

Début de l'itération. Si M est nulle, alors on a fini. On suppose donc ici que $M\neq 0$. Dans le cas où la colonne 1 est entièrement nulle, ça veut dire qu'il existe un $a_{ij}\neq 0$ dans la matrice, qu'on transvecte vers la colonne 1. Si $a_{11}=0$, alors il y a, autre part sur la colonne 1, un a_{i1} non nul. Par une transvection de coefficient 1 de L_i vers L_1, on obtient que a_{11} est non nul.

Aller en B.

B Trouver un pivot non nul de stathme minimal sur la colonne 1 et simplifier la colonne

Ici, on sait que $a_{11}\neq 0$. Si a_{11} est de stathme minimal sur la colonne, aller en B.ii. Sinon, aller en B.i.

B.i Si $a_{11}\neq 0$ n'est pas de stathme minimal

Si on est ici, c'est que a_{11} n'est pas de stathme minimal sur la colonne 1. Alors il y a un a_{i1} non nul, qui, lui, est de stathme minimal. Par une transvection, on peut remplacer a_{11} par son reste modulo a_{i1}. Dans le cas où le nouveau a_{11} est nul, on retransvecte un petit coup L_i vers L_1 pour que $a_{11}=a_{i1}$. Maintenant, a_{11} est non nul de stathme minimal sur sa colonne.le stathme de a_{11} a strictement baissé ici.

Aller en B.ii.

B.ii a_{11} est de stathme minimal : abîmer la colonne

On peut abîmer la première colonne. Utiliser ce pivot pour diminuer strictement les stathmes via division euclidienne[1] de toute la première colonne via des transvections de lignes. Si des coefficients en-dessous de a_{11} sont non nuls, alors il faut revenir en B.i. S'ils sont bien nuls, aller en C.

1. C'est bien de détailler une fois le calcul effectué.

C Trouver un pivot non nul de stathme minimal sur la ligne 1 et simplifier cette ligne

Nous savons ici que la colonne 1 est nulle mais pas a_{11}. Si a_{11} est de stathme minimal pour la ligne 1, aller en C.ii. Sinon on va en C.i.

C.i Minimiser le stathme sur la ligne

Si on est ici, alors on sait que a_{11} n'est pas de stathme minimal sur sa ligne. On prend un a_{1i} non nul, choisi de stathme minimal sur la ligne 1. Par une transvection, on peut remplacer a_{11} par son reste modulo a_{1i}. Dans le cas où le reste est nul, on fait une transvection supplémentaire pour que a_{11} soit égal à a_{1i} donc non nul. Le stathme de a_{11} est maintenant minimal sur cette ligne et a strictement baissé.

Suite à cette opération, la colonne 1 n'est plus forcément nulle, et il faut retourner en B pour s'en assurer. Dans le cas contraire, on peut aller en C.ii.

C.ii Abîmer la ligne

On peut faire baisser strictement le stathme de tous les éléments de la première ligne par des transvections vers les autres colonnes. Si la ligne n'est pas annulée, il faut retourner en C.i en sachant que a_{11} n'est pas de stathme minimal (puisque sur la ligne, il y a des restes non nuls de DE par lui). Si elle est annulée, alors puisque a_{11} est le seul non nul sur sa ligne et sa colonne, on peut aller en D.

D Ramener un nouveau pivot

Ici, on a correctement échelonné notre matrice pour la première ligne et la première colonne ! On sait aussi que $a_{11} \neq 0$. Si a_{11} divise tout le bloc qui reste, se rendre à l'étape D.ii. Supposons que a_{11} ne divise pas tout le monde dans le bloc qui reste. Dans ce cas, aller en D.i.

D.i Si a_{11} ne divise pas tout le bloc

Si a_{ij} est dans ce bloc et non divisible par a_{11}, alors on le transvecte vers la première colonne de M. On fait une division euclidienne de ce a_{ij} par a_{11}. Comme a_{11} ne le divise pas, le reste est non nul, et de stathme strictement inférieur à a_{11}. Ainsi, a_{11} n'est plus de stathme minimal sur sa colonne, on peut donc revenir en B.i.

D.ii Récurrer

L'itération actuelle est terminée.Il faut réappliquer l'algorithme depuis le début, non pas à M mais au bloc $n-1 \times n-1$ en bas à droite.

II. La terminaison

Plaçons notre point de vue dans une et une seule itération de cet algorithme.

Lemme II.1.
Les étapes A et D.ii ne peuvent s'exécuter qu'une seule fois.

Preuve. A n'est appelée qu'au début. Si D.ii s'exécute, alors c'est la fin de l'itération. □

Lemme II.2.
Chacune des étapes B.ii et C.ii ne fait pas augmenter le stathme de a_{11}.

Preuve. L'étape B.ii n'altère pas a_{11}.
L'étape C.ii n'altère pas a_{11}.

□

Lemme II.3.
Les étapes B.i et C.i font strictement baisser le stathme de a_{11}.

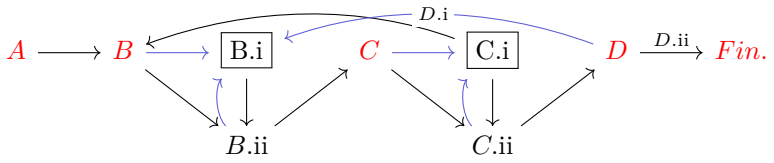
Preuve. L'étape B.i consiste à remplacer a_{11} par son reste modulo une DE par un élément de stathme strictement plus petit, ou par cet élément de stathme strictement plus petit.

L'étape C.i diminue le stathme explicitement de la même façon. □

Proposition II.4. Terminaison
Si on commence l'itération au début, i.e. à l'étape A, alors on atteindra un jour l'étape D.ii.

Preuve.

Dans le diagramme suivant, les cases encadrées sont celles où on est sûr qu'à chaque passage, $\varphi(a_{11})$ va diminuer strictement. On ne peut donc passer qu'un nombre fini de fois par ces cases. Les flèches bleues sont les flèches menant à ces cases : elles ne peuvent être empruntées qu'un nombre fini de fois. Alors à partir d'un certain nombre d'itération, on n'utilisera que les flèches noires, qui ne font pas de boucle.



□

III. L'unicité

On note μ_k le pgcd des mineurs de taille k. On va montrer que si $M \sim \mathrm{diag}(d_1, \dots, d_n)$ où $d_1 \mid \cdots \mid d_n$, alors $d_k = \frac{\mu_k}{\mu_{k-1}}$ (où $\mu_0 = 1$). On le voit directement sur la diagonale, mais il va falloir prouver que $\mu_k(M)$ est invariant par équivalence. Une façon de plier le calcul rapidement est d'appiquer la formule de Cauchy-Binet :

Théorème III.1. Cauchy-Binet
Soit $A, B \in \mathcal{M}_n(R)$ où R est un anneau commutatif. Alors en notant $m_{I,J}(A)$ le déterminant de sa matrice extraite par dont les lignes sont I et les colonnes sont J, où $|I| = |J| = k$. On a : $m_{I,J}(AB) = \sum_{|K|=k} m_{I,K}(A) m_{K,J}(B)$.

Preuve. Les deux membres sont n-linéaires par rapport aux colonnes de B et n-alternés par rapport aux lignes de A. Il est donc suffisant de prouver la formule pour la base canonique de $(\mathbb{R}^n)^n$. Ils sont même en fait n-alternés : il suffit de le prouver pour $A = B = I_n$. □

Corollaire III.2.
Si $P \in \mathrm{GL}_n(R)$, alors $\mu_k(M) = \mu_k(PM) = \mu_k(MP)$.

Preuve. On note $\mathcal{I}_k(M)$ l'idéal engendré par les mineurs de taille k de M. Un mineur de PM s'écrit comme une somme de produits de mineurs de P et de mineurs de M de taille k donc $\mathcal{I}_k(PM) \subset \mathcal{I}_k(P)\mathcal{I}_k(M) \subset \mathcal{I}_k(M)$. En appliquant à P^{-1} et PM, on trouve que $\mu_k(PM) \subset \mu_k(M)$. Faire la même chose à l'envers, ou bien appliquer le résultat à M^T pour avoir l'autre sens.

□

IV. N'en faire que des 1 !

Si on souhaite trouver des générateurs à $\mathrm{SL}_n(R)$, il suffit d'appliquer l'algorithme suivant :

M est maintenant diagonale avec des coefficients nommés ε_i sur sa diagonale. Supposons que M était au départ dans $\mathrm{SL}_n(R)$. Alors notre diagonale de ε_i vérifie $\prod_i \varepsilon_i = 1$. Voyons comment n'avoir que des 1 en faisant des transvections. Sauf si $n = 1$, auquel cas $\varepsilon_1 = 1$, on peut supposer $n \geqslant 2$, auquel cas on peut

voir notre matrice comme une diagonale par blocs : le bloc $\begin{pmatrix}\varepsilon_1 & \\ & \varepsilon_2\end{pmatrix}$, et le bloc des autres ε_i. On ne va s'intéresser qu'au premier puisque les transvections qu'on fait dessus n'affecte jamais l'autre bloc, et car les coefficients sur les deux premières lignes à partir du 3ème sont nuls, et sur les 2 premières colonnes à partir du 3ème sont nuls.
On transvecte L_1 vers L_2 pour obtenir $\begin{pmatrix}\varepsilon_1 & 0\\ \varepsilon_1 & \varepsilon_2\end{pmatrix}$. Soit $\lambda \in R$ tel que $\varepsilon_1 + \lambda\varepsilon_1 = 1$ (existe car ε_1 est inversible). On transvecte alors λ fois L_2 vers L_1 pour obtenir $\begin{pmatrix}1 & \lambda\varepsilon_2\\ \varepsilon_1 & \varepsilon_2\end{pmatrix}$. Alors, par des transvections évidentes, notre 1 peut tuer ses deux voisins pour trouver $\begin{pmatrix}1 & 0\\ 0 & \varepsilon_2\end{pmatrix}$. Il suffit de recommencer l'opération pour rendre ε_2 égal à 1 et ainsi de suite. On garde un invariant qui est le produit des coefficients diagonaux vaut 1. Donc, quand on aura changé ε_{n-1} pour 1, le dernier sera automatiquement un 1.

Applications

Proposition IV.1.
Soit R un anneau. Si $n \geqslant 3$, toutes les transvections sont des commutateurs.

Preuve. Soit $\lambda \in R$, $i \neq j$ entre 1 et n, montrons que $I_n + E_{ij}\lambda$ (une transvection quelconque. E_{ij} n'a que le coefficient ij non nul) est un commutateur. Soit k différent de i, j. Idée : L_j se donne $(\times -1)$ à L_k, qui s'en sert pour embêter L_i $(\times\lambda)$. Effarée, L_j remet L_k à sa position initiale ($\times 1$, l'opération exacte inverse qu'au début). L_k, honteux et confus, essaye de réparer ce qu'il a infligé à L_i (en faisant l'action contraire : $\times\lambda$), mais comme L_k a changé entre temps, le résultat sur L_i ne sera jamais le même : il a pris un λ sur sa colonne j. Cqfd car, en partant de l'identité, les opérations sur L_k se sont annulées, par contre L_i a été changée à vie et s'est pris un λ en i, j. On vient d'obtenir $I_n + E_{ij}$ comme produit d'un commutateur de transvections et de l'identité. □

Attention, si $n = 2$, alors toutes les transvections ne sont pas des commutateurs. En effet, sinon, on aurait $D(\mathrm{SL}_n(\mathbb{Z})) = \mathrm{SL}_n(\mathbb{Z})$ et (Conrad) il existe une surjection de $\mathrm{SL}_n(\mathbb{Z})$ vers $\mathbb{Z}/12\mathbb{Z}$!

En général, le groupe dérivé de $\mathrm{SL}_2(\mathbb{K})$ c'est quoi ?

Ok une application : prouver que $\mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z})$ est un quotient (euh en fait c'est que le cas où R est un corps qui sert là... mais dans ce cas on peut remplacer 3 par n'importe quel nombre euh oui mais non c'est pas euclidien) ! Et il admet $\mathbb{Z}/3\mathbb{Z}$ comme quotient !

Ok : s'il n'y a qu'un seul 2-Sylow dans $\mathrm{SL}_2(\mathbb{Z}/3\mathbb{Z})$ (cardinal 24), alors quotienter par lui, on a une surjection vers $\mathbb{Z}/3\mathbb{Z}$, alors son groupe dérivé ne peut pas être égal à lui-même. Et sinon, il y a 3 2-Sylow A,B,C, et en étudiant l'action du groupe sur eux : $\mathrm{Stab}_A = A$ (car de cardinal 8), $A \cap B \cap C$ le Ker de l'action, et surtout le noyau est au moins de cardinal 4 car c'est un morphisme d'un groupe de cardinal 24 vers $\mathfrak{S}_3$ de cardinal 6. Donc un sous-groupe non égal à 1 de $\mathfrak{S}_3$ est un quotient de G. Mais soit ce sous-groupe est strict, auquel cas c'est $\mathbb{Z}/2\mathbb{Z}$ ou $\mathbb{Z}/3\mathbb{Z}$, soit c'est $\mathfrak{S}_3$, mais $\mathfrak{S}_3$ admet pour quotient $\mathbb{Z}/2\mathbb{Z}$. Dans tous les cas, on arrive à montrer qu'un truc abélien est un quotient de G donc G n'est pas de dérivée égale à G. En fait il n'y a qu'un seul 2-sylow, il suffit de compter les éléments d'ordre 8.

En fait le dérivé de ce $\mathrm{SL}_2(\mathbb{F}_3)$ c'est le groupe des quaternions... voir olivier serman (taper sur everything). Résumé de la preuve : $PGL_2(\mathbb{F}_3) \simeq \mathfrak{S}_4$ (par permutation des droites). Donc évidemment $PSL_2(\mathbb{F}_3) \simeq \mathfrak{A}_4$. Donc $\mathfrak{A}_4$ est un quotient d'indice 2 de $\mathrm{SL}_2(\mathbb{F}_3)$. Mais $\mathfrak{A}_4/V_4$ est d'ordre 3 donc cyclique donc $\mathbb{Z}/3\mathbb{Z}$ est un quotient abélien de $\mathrm{SL}_2(\mathbb{F}_3)$) donc il existe un sous-groupe d'ordre 8 contenant le groupe dérivé. Montrons que c'est le sous-groupe dérivé.

La surjection $\mathrm{SL}_2(\mathbb{F}_3) \to \mathfrak{A}_4$ dont le noyau K est de cardinal 2 se restreint en une surjection $D(\mathrm{SL}_2(\mathbb{F}_3)) \to V_4$ dont le noyau est égal à l'intersection de K avec $D(\mathrm{SL}_2(\mathbb{F}_3))$, de cardinal 1 ou 2. Si le groupe dérivé n'est pas d'ordre 8, alors le noyau de ce morphisme est de cardinal 1 donc on aurait $D(\mathrm{SL}_2(\mathbb{F}_3)) = V_4 \simeq Z/2Z^2$ et on a 3 involutions. Le hic c'est que :

Lemme IV.2.
Les seules involutions de $\mathrm{SL}_2(\mathbb{F}_3)$ *sont* $\pm I_2$.

Preuve. Elles sont annulées par $(X-1)(X+1)$ qui est scindé à racines simples. Leur déterminant étant 1, c'est fini. □

Cela montre le cardinal du groupe dérivé, c'est pas mal. Utiliser le lemme suivant ainsi que la classification des groupes d'ordre 8 pour conclure que c'est $\mathbb{H}_8$.