



Calcul exact des formes de Jordan et de Frobenius d'une matrice

Patrick Ozello

► To cite this version:

Patrick Ozello. Calcul exact des formes de Jordan et de Frobenius d'une matrice. Modélisation et simulation. Université Joseph-Fourier - Grenoble I, 1987. Français. NNT: . tel-00323705

HAL Id: tel-00323705

<https://theses.hal.science/tel-00323705>

Submitted on 23 Sep 2008

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

THESE

présentée par **Patrick OZELLO**

pour obtenir le titre de **DOCTEUR de l'UNIVERSITE SCIENTIFIQUE
TECHNOLOGIQUE et MEDICALE de GRENOBLE .**

(arrêté ministériel du 5 Juillet 1984)

en **INFORMATIQUE et MATHEMATIQUES APPLIQUEES .**

CALCUL EXACT DES FORMES DE JORDAN ET DE FROBENIUS D'UNE MATRICE .

Thèse soutenue le 29 Janvier 1987 devant la commission d'examen .

Président : D. Lazard

Examineurs : F. Robert
J. Della Dora
K. Geddes
D. Duval
M. Giusti

Thèse préparée au sein du laboratoire TIM3

UNIVERSITE SCIENTIFIQUE ET MEDICALE DE GRENOBLE

Année universitaire 1982-1983

Président de l'Université : M. TANCHE

MEMBRES DU CORPS ENSEIGNANT DE L'U.S.M.G.

(RANG A)

SAUF ENSEIGNANTS EN MEDECINE ET PHARMACIE

PROFESSEURS DE 1ère CLASSE

ARNAUD Paul	Chimie organique
ARVIEU Robert	Physique nucléaire I.S.N.
AUBERT Guy	Physique C.N.R.S.
AYANT Yves	Physique approfondie
BARBIER Marie-Jeanne	Electrochimie
BARBIER Jean-Claude	Physique expérimentale C.N.R.S. (labo de magnétisme)
BARJON Robert	Physique nucléaire I.S.N.
BARNOUD Fernand	Biosynthèse de la cellulose-Biologie
BARRA Jean-René	Statistiques - Mathématiques appliquées
BELORISKY Elie	Physique
BENZAKEN Claude (M.)	Mathématiques pures
BERNARD Alain	Mathématiques pures
BERTRANDIAS Françoise	Mathématiques pures
BERTRANDIAS Jean-Paul	Mathématiques pures
BILLET Jean	Géographie
BONNIER Jean-Marie	Chimie générale
BOUCHEZ Robert	Physique nucléaire I.S.N.
BRAVARD Yves	Géographie
CARLIER Georges	Biologie végétale
CAUQUIS Georges	Chimie organique
CHIBON Pierre	Biologie animale
COLIN DE VERDIERE Yves	Mathématiques pures
CRABBE Pierre (détaché)	C.E.R.M.O.
CYROT Michel	Physique du solide
DAUMAS Max	Géographie
DEBELMAS Jacques	Géologie générale
DEGRANGE Charles	Zoologie
DELOBEL Claude (M.)	M.I.A.G. Mathématiques appliquées
DEPORTES Charles	Chimie minérale
DESRE Pierre	Electrochimie
DOLIQUE Jean-Michel	Physique des plasmas
DUCROS Pierre	Cristallographie
FONTAINE Jean-Marc	Mathématiques pures
GAGNAIRE Didier	Chimie physique

.../...

GASTINEL Noel	Analyse numérique - Mathématiques appliquées
GERBER Robert	Mathématiques pures
GERMAIN Jean-Pierre	Mécanique
GIRAUD Pierre	Géologie
IDELMAN Simon	Physiologie animale
JANIN Bernard	Géographie
JOLY Jean-René	Mathématiques pures
JULLIEN Pierre	Mathématiques appliquées
KAHANE André (détaché DAFCO)	Physique
KAHANE Josette	Physique
KOSZUL Jean-Louis	Mathématiques pures
KRAKOWIAK Sacha	Mathématiques appliquées
KUPTA Yvon	Mathématiques pures
LACAZE Albert	Thermodynamique
LAJZEROWICZ Jeannine	Physique
LAJZEROWICZ Joseph	Physique
LAURENT Pierre	Mathématiques appliquées
DE LEIRIS Joël	Biologie
LLIBOUTRY Louis	Géophysique
LOISEAUX Jean-Marie	Sciences nucléaires I.S.N.
LOUP Jean	Géographie
MACHE Régis	Physiologie végétale
MAYNARD Roger	Physique du solide
MICHEL Robert	Minéralogie et pétrographie (géologie)
MOZIERES Philippe	Spectrométrie - Physique
OMONT Alain	Astrophysique
OZENDA Paul	Botanique (biologie végétale)
PAYAN Jean-Jacques (détaché)	Mathématiques pures
PEBAY PEYROULA Jean-Claude	Physique
PERRIAUX Jacques	Géologie
PERRIER Guy	Géophysique
PIERRARD Jean-Marie	Mécanique
RASSAT André	Chimie systématique
RENARD Michel	Thermodynamique
RICHARD Lucien	Biologie végétale
RINAUDO Marguerite	Chimie CERMAV
SENGEL Philippe	Biologie animale
SERGERAERT Francis	Mathématiques pures
SOUTIF Michel	Physique
VAILLANT François	Zoologie
VALENTIN Jacques	Physique nucléaire I.S.N.
VAN CUTSEN Bernard	Mathématiques appliquées
VAUQUOIS Bernard	Mathématiques appliquées
VIALON Pierre	Géologie

PROFESSEURS DE 2ème CLASSE

ADIBA Michel	Mathématiques pures
ARMAND Gilbert	Géographie

.../...

AURIAULT Jean-Louis	Mécanique
BEGUIN Claude (M.)	Chimie organique
BOEHLER Jean-Paul	Mécanique
BOITET Christian	Mathématiques appliquées
BORNAREL Jean	Physique
BRUN Gilbert	Biologie
CASTAING Bernard	Physique
CHARDON Michel	Géographie
COHENADDAD Jean-Pierre	Physique
DENEUVILLE Alain	Physique
DEPASSEL Roger	Mécanique des fluides
DOUCE Roland	Physiologie végétale
DUFRESNOY Alain	Mathématiques pures
GASPARD François	Physique
GAUTRON René	Chimie
GIDON Maurice	Géologie
GIGNOUX Claude (M.)	Sciences nucléaires I.S.N.
GUITTON Jacques	Chimie
HACQUES Gérard	Mathématiques appliquées
HERBIN Jacky	Géographie
HICTER Pierre	Chimie
JOSELEAU Jean-Paul	Biochimie
KERCKOVE Claude (M.)	Géologie
LE BRETON Alain	Mathématiques appliquées
LONGEQUEUE Nicole	Sciences nucléaires I.S.N.
LUCAS Robert	Physiques
LUNA Domingo	Mathématiques pures
MASCLE Georges	Géologie
NEMOZ Alain	Thermodynamique (CNRS - CRTBT)
OUDET Bruno	Mathématiques appliquées
PELMONT Jean	Biochimie
PERRIN Claude (M.)	Sciences nucléaires I.S.N.
PFISTER Jean-Claude (détaché)	Physique du solide
PIBOULE Michel	Géologie
PIERRE Jean-Louis	Chimie organique
RAYNAUD Hervé	Mathématiques appliquées
ROBERT Gilles	Mathématiques pures
ROBERT Jean-Bernard	Chimie physique
ROSSI André	Physiologie végétale
SAKAROVITCH Michel	Mathématiques appliquées
SARROT REYNAUD Jean	Géologie
SAXOD Raymond	Biologie animale
SOUTIF Jeanne	Physique
SCHOOL Pierre-Claude	Mathématiques appliquées
STUTZ Pierre	Mécanique
SUBRA Robert	Chimie
VIDAL Michel	Chimie organique
VIVIAN Robert	Géographie

REMERCIEMENTS

Je tiens à remercier ici Monsieur D. Lazard , Professeur à Paris VI et président du GRECO , pour l'honneur qu'il me fait en présidant le jury de cette thèse . J'ai eu la chance , dès le début de ce travail , de pouvoir bénéficier de ses conseils .

J'adresse toute ma gratitude à Monsieur F. Robert , Professeur à l'ENSIMAG. L'intérêt qu'il a manifesté pour ce travail , et par là , pour le calcul formel , est pour moi la meilleure récompense .

Je remercie aussi vivement Monsieur J. Della Dora , Professeur à l'ENSIMAG , d'avoir dirigé cette thèse . J'ai pu apprécier sa compétence scientifique , mais aussi son humour et sa chaleur humaine .

Mes remerciements vont également à Madame D. Duval , Maître de conférence à Grenoble I , pour l'attention et l'intérêt avec laquelle elle a suivi ce travail . Ses encouragements constants , ont énormément contribué à l'accomplissement de cette thèse .

Que soient remerciés aussi Messieurs K. Geddes , Professeur à Waterloo (Canada) , et M. Giusti , chargé de recherche au CNRS , pour avoir accepté de faire partie de ce jury .

Je tiens également à remercier Mademoiselle C. Dicrescenzo et Monsieur A. Eberhard , dont les conseils en informatique m'ont été d'une grande utilité .

Je ne peux oublier les membres de l'équipe calcul formel , ainsi que les joyeux ex-titulaires ou titulaires du bureau 58 de la tour IRMA , J.M. Muller , D. Pellegrin , R. Ruiz , L. Deshpande , et P. Klein ; qu'ils soient remerciés pour leur gentillesse et leur bonne humeur .

Je remercie aussi le personnel du service de reprographie de l'IMAG pour la réalisation matérielle de ce travail .

Je remercie également le Ministère de la Recherche et de la Technologie , le GRECO de calcul formel et le laboratoire TIM3 ; sans eux , cette thèse n'aurait pu voir le jour .

L'observation des valeurs approchées des couples (λ_1, λ_2) , (λ_3, λ_4) , et (λ_5, λ_6) , laisse penser que nous avons au moins trois valeurs propres de multiplicité 2. Pourtant il n'en est rien, toutes les valeurs propres de cette matrice sont distinctes.

On pourrait aussi donner des exemples de matrice ayant des valeurs propres multiples, et dont les valeurs approchées, données par les algorithmes, sont très différentes. Kagstrom et Ruhe étudient une méthode pour reconnaître des valeurs propres multiples, et donnent des algorithmes pour le calcul de la forme de Jordan [Kagstrom, Ruhe, 1980], [Ruhe, 1970].

Afin d'écartier les problèmes d'instabilité numérique, nous proposons dans cette thèse, de nouveaux algorithmes de calcul formel, particulièrement intéressants lorsque les données (coefficients de la matrice) sont exactes.

On peut utiliser, pour calculer formellement la forme de Jordan, les algorithmes 1) et 2) suivants :

- 1) - Calcul du polynôme caractéristique de A .
 - Factorisation du polynôme caractéristique.
 - Pour chaque valeur propre λ et chaque entier k inférieur à l'ordre de multiplicité de λ , calcul d'une base du sous espace $(A - \lambda I)^k$.
- 2) - Calcul de la forme d'Hermite, puis de la forme de Smith S de $A - XI$, ainsi que des matrices U et V telles que $S = U(A - XI)V$

Kannan et Bachem donnent un algorithme polynomial pour le calcul de la forme de Smith d'une matrice à coefficients entiers, et Krishnamoorthy et Saunders montrent dans le cas de matrice à coefficients dans $\mathbb{Q}[X]$, que cet algorithme est aussi polynomial [Kannan, Bachem, 1979], [Krishnamoorthy, Saunders, 1985].

Ces deux algorithmes utilisent largement l'arithmétique des polynômes: addition, multiplication, quotient, PGCD, et même factorisation dans le premier cas. Or, avec les systèmes actuels de calcul formel, et les architectures des machines qui les supportent, ces opérations s'avèrent coûteuses, et il est souvent préférable de ne travailler qu'avec les entiers relatifs.

C'est pourquoi nous avons recherché des algorithmes qui utilisent essentiellement les opérations arithmétiques des entiers, et éventuellement des rationnels. Ceci nous a conduit à envisager une autre forme normale de matrice: la forme de Frobenius ou forme rationnelle, qui est une matrice diagonale par blocs, chaque bloc étant une matrice compagnon.

L'objet du premier chapitre , et de montrer que l'on peut déduire de la forme de Frobenius d'une matrice , la forme de Jordan , une matrice de passage et son inverse avec un minimum de calcul .

Nous donnons dans les chapitres II et III , deux algorithmes pour le calcul de la forme de Frobenius d'une matrice à coefficients rationnels .

Le premier (chapitre II) , présente l'avantage d'être facile à programmer ; mais les coefficients de la matrice de passage , en général rationnels , peuvent être assez grands .

Le second (chapitre III) est un algorithme de complexité polynomiale . On démontre que si A est une matrice d'ordre n à coefficients rationnels , le nombre des opérations est borné par $O(n^4)$, et compte tenu de la croissance des coefficients , le temps de calcul est borné par $O(n^8 \log^2 \|A\|)$. De plus , la croissance des coefficients étant contrôlée , on obtient une matrice de passage souvent plus intéressante que celle obtenue par le premier algorithme .

On s'intéresse dans le chapitre IV , au cas où les coefficients de la matrice sont des nombres algébriques sur \mathbb{Q} . Ce qui nous conduira à présenter les avantages , et les limites , du nouveau système D5 de maniement des nombres algébriques , développé par J. Della Dora , C. Dicrescenzo , et D. Duval .

Chapitre I

**Lien entre forme de Frobenius et forme de Jordan
d'une matrice .**

I.1. Rappels.

Nous allons dans le début de ce chapitre, rappeler les théorèmes fondamentaux concernant les formes de Jordan et de Frobenius d'une matrice. Nous en profiterons pour préciser quelques notations qui seront employées dans plusieurs chapitres (polynôme minimal , matrice compagnon).

Nous donnerons ensuite un exemple de matrice de passage entre les formes de Jordan et de Frobenius.

I.1.a Forme de Jordan.

Considérons deux matrices carrées A et B d'ordre n , dont les éléments appartiennent à un corps \mathbb{K} .

On dit que ces deux matrices sont semblables s'il existe une matrice P inversible telle que $AP = PB$.

Cette relation de similitude est une relation d'équivalence.

On appelle polynôme caractéristique de A le polynôme

$$P_A(X) = \det(X \cdot \text{Id} - A).$$

C'est un polynôme unitaire de degré n , dont les racines $\lambda_1 \dots \lambda_k$ appartiennent à la clôture algébrique de \mathbb{K} . Si A et B sont semblables, alors $P_A = P_B$.

Notons $J_r(\lambda_i)$ le bloc d'ordre r , appelé bloc de Jordan :

$$J_r(\lambda_i) = \begin{pmatrix} \lambda_i & 1 & 0 & \dots & \dots & \dots & 0 \\ 0 & \lambda_i & 1 & \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots & \dots & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \lambda_i & 1 \\ 0 & \dots & \dots & \dots & \dots & 0 & \lambda_i \end{pmatrix}$$

Théorème : 1) A est semblable à une matrice bloc-diagonale

$$J = \text{diag} (J_{r_1}(\lambda_1), \dots, J_{r_j}(\lambda_1), \dots, J_{r_p}(\lambda_i), \dots, J_{r_q}(\lambda_k))$$

$$\text{avec } \sum_{p=1}^q r_p = n.$$

2) J est unique à une permutation près des blocs $J_r(\lambda_i)$.

J est appelée forme de Jordan de A .

On pourra trouver une démonstration de ce théorème dans [Gantmacher, 1966]

1.1.b Polynôme minimal d'un vecteur.

Soient A une matrice de $M_n(\mathbb{K})$, où \mathbb{K} est un corps,

$\mathfrak{E} = \mathbb{K}^n$ l'espace vectoriel sur \mathbb{K} de dimension n ;

(e_1, \dots, e_n) la base canonique.

* On notera A aussi bien la matrice que l'endomorphisme qui lui est associé dans la base canonique.

* \mathfrak{E} peut être considéré comme un module sur l'anneau principal $\mathbb{K}[X]$. Si $\alpha \in \mathbb{K}[X]$, $\alpha = a_m X^m + \dots + a_0$ et $e \in \mathfrak{E}$
alors $\alpha e = (a_m A^m + \dots + a_0 I) e$.

* Si e est un vecteur, on note $(e)_A$ le sous-module de \mathfrak{E} engendré par e .

$$(e)_A = \{ \alpha e, \alpha \in \mathbb{K}[X] \}$$

* On note π_e le polynôme minimal de e : c'est le polynôme unitaire de plus bas degré tel que $\pi_e(e) = 0$.

Théorème $(e)_A$ est un sous espace vectoriel de \mathfrak{E} , et $\dim (e)_A = \deg \pi_e$.

1.1.c Matrices compagnons.

Une matrice compagnon est une matrice carrée de la forme suivante:

$$C = \begin{pmatrix} 0 & \cdots & 0 & -a_0 \\ 1 & & & -a_1 \\ 0 & \ddots & & \vdots \\ \vdots & & \ddots & 0 \\ 0 & \cdots & 0 & 1 & -a_{n-1} \end{pmatrix}$$

On associera à C le polynôme $P = X^n + a_{n-1}X^{n-1} + \dots + a_0$.

Réciproquement, on associera à tout polynôme unitaire P de degré n , une unique matrice compagnon d'ordre n .

Théorème. :

Soient C une matrice compagnon, et P le polynôme associé à C . Si P_C et Π_C désignent respectivement le polynôme caractéristique et le polynôme minimal de C , alors $P_C = \Pi_C = P$.

La démonstration fait appel à la notion de polynôme minimal d'un vecteur.

Soit (e_1, e_2, \dots, e_n) la base canonique de \mathbb{K}^n , et ϵ l'endomorphisme associé à C .

Nous avons

$$\begin{aligned} \epsilon(e_1) &= e_2 \\ \epsilon(e_2) &= e_3 \\ &\vdots \\ \epsilon(e_n) &= -a_0 e_1 + \dots - a_{n-1} e_n \end{aligned}$$

donc $(e_1, \epsilon(e_1), \epsilon^2(e_1), \dots, \epsilon^{n-1}(e_1))$ est une base de \mathbb{K}^n .

Si π_{e_1} est le polynôme minimal de e_1 , on a alors $\deg(\pi_{e_1}) \geq n$.

Comme $\epsilon^n(e_1) = -a_0 e_1 + \dots - a_{n-1} \epsilon^{n-1}(e_1)$ on en déduit $P = \pi_{e_1}$.

Nous savons d'autre part (théorème d'Hamilton Cayley) que le polynôme caractéristique P_C est un multiple du polynôme minimal Π_C , et que Π_C est un multiple de π_{e_1} . Ces polynômes étant tous de degré n , ils sont donc égaux à un coefficient multiplicatif près. Si de plus on les choisit unitaires on a finalement :

$$P_C = \Pi_C = \pi_{e_1} = P .$$

Corollaire: [Wilkinson , 1965]

Si $P = P_1 \star P_2^2 \star \dots \star P_k^k$ est la décomposition sans carrés de P ,
(les P_i étant premiers entre eux deux à deux et sans facteurs carrés), et si $\lambda_{i,1}, \dots, \lambda_{i,d_i}$ sont les d_i racines distinctes de P_i alors la forme de Jordan de la matrice compagnon associée à P est :

$$J = \text{diag} \left(J_i (\lambda_{i,j}) \right) \\ \begin{matrix} i = 1 \text{ à } k \\ j = 1 \text{ à } d_i \end{matrix}$$

$$J_i (\lambda_{i,j}) = \begin{vmatrix} \lambda_{i,j} & 1 & 0 & \dots & 0 \\ 0 & \lambda_{i,j} & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & \dots & 0 & 1 & \lambda_{i,j} \end{vmatrix}$$

Exemple : $P = (X^2 - 2) \star (X^2 + X + 1)^3$; $\mathbb{K} = \mathbb{Q}$

pour simplifier les notations notons μ_1, μ_2 les racines de $X^2 - 2$,

et λ_1, λ_2 les racines de $X^2 + X + 1$.

La forme de Jordan J de la matrice compagnon associée à P est :

$$J = \begin{pmatrix} \mu_1 & & & & & \\ & \mu_2 & & & & \\ & & \lambda_1 & 1 & 0 & \\ & & 0 & \lambda_1 & 1 & \\ & & 0 & 0 & \lambda_1 & \\ & & & & & \lambda_2 & 1 & 0 \\ & & & & & 0 & \lambda_2 & 1 \\ & & & & & 0 & 0 & \lambda_2 \end{pmatrix}$$

1.1.d. Forme de Frobenius.

Théorème : Si A est une matrice de $M_n(\mathbb{K})$ alors il existe :

- 1) une unique matrice F de $M_n(\mathbb{K})$ telle que $F = \text{diag}(C_1, \dots, C_k)$ où les C_i sont des matrices compagnons et les polynômes P_i associés aux blocs C_i vérifient la propriété : P_{i+1} divise P_i pour $i = 1$ à $k-1$.
- 2) une matrice $P \in M_n(\mathbb{K})$ inversible telle que $AP = PF$.

F est appelée forme de Frobenius de A . Ajoutons que les polynômes P_i dans l'énoncé du théorème sont appelés diviseurs élémentaires de A . On trouvera une démonstration dans [Gantmacher, 1966], [Newman, 1972], [Gastinel, 1966].

Si l'on n'impose pas aux polynômes P_i de vérifier la propriété de divisibilité, P_{i+1} divise P_i pour $i = 1$ à $k-1$, on parlera de forme faible de Frobenius. Cette forme n'est pas unique en général.

Dans la suite de ce chapitre, nous allons décrire une matrice de passage Q entre forme de Jordan et forme faible de Frobenius ($QF = JQ$) et une méthode pour calculer Q^{-1} . Mais avant il faut dire pourquoi on s'intéresse à cette forme de Frobenius. Nous supposons que A est une matrice de $M_n(\mathbb{K})$. En pratique nous considérerons soit $\mathbb{K} = \mathbb{Q}$ le corps des nombres rationnels, soit $\mathbb{K} = \mathbb{F}_p$ un corps fini à p éléments.

Dans ces deux situations, \mathbb{K} n'est pas un corps algébriquement clos. Les éléments de la matrice de Jordan de A , ainsi que ceux de la matrice de passage sont généralement des nombres algébriques, racines du polynôme caractéristique, qui seront représentés par des polynômes à coefficients dans \mathbb{K} , de degrés inférieurs ou égaux à n . Afin d'éviter de nombreuses opérations arithmétiques avec les nombres algébriques, nous proposons la méthode suivante qui se divise en deux étapes :

- 1) Déterminer la forme de Frobenius F de A (ou éventuellement une forme faible) , ainsi qu'une matrice de passage P telle que $AP = PF$.
- 2) En déduire la forme de Jordan J et la matrice de passage R telle que $AR = RJ$ ($R = PQ^{-1}$).

En ce qui concerne la première partie, nous donnerons deux algorithmes dans les chapitres suivants. Nous développons maintenant la deuxième partie.

1.2. Description d'une matrice de passage entre la forme de Frobenius et la forme de Jordan, et de son inverse.

1.2. a. Réduction du problème au cas d'une matrice compagnon.

Supposons qu'une forme faible de Frobenius F de A soit formée de plusieurs matrices compagnons.

$$F = \text{diag} (C_1, \dots, C_k).$$

On peut alors associer à chaque C_i sa forme de Jordan J_i ainsi qu'une matrice de passage Q_i telle que $Q_i C_i = J_i Q_i$. Alors la forme de Jordan de F est:

$$J = \text{diag} (J_1, \dots, J_k)$$

et la matrice de passage Q telle que $QF = JQ$ est

$$Q = \text{diag} (Q_1, \dots, Q_k).$$

De plus l'inverse de Q est $Q^{-1} = \text{diag} (Q_1^{-1}, \dots, Q_k^{-1}).$

1.2.b Calcul de la matrice de passage.

Supposons maintenant que F soit une matrice compagnon. Nous avons déjà donné dans les rappels la forme de Jordan de F . Si λ_i est une racine du polynôme caractéristique de F , d'ordre de multiplicité r alors on trouvera un seul bloc de Jordan $J_r(\lambda_i)$, d'ordre r , associé à la valeur propre λ_i .

Lorsque nous parlons de la forme de Jordan, celle-ci est unique à une permutation des blocs près. Si $P = P_1 \cdot P_2^2 \cdot \dots \cdot P_k^k$ est la décomposition sans carrés du polynôme associé à F , nous pouvons ranger les valeurs propres de la façon suivante:

$$(\lambda_{1,1}, \dots, \lambda_{1,d_1}, \dots, \lambda_{i,1}, \dots, \lambda_{i,d_i}, \dots, \lambda_{k,d_k})$$

d_i étant égal au degré de P_i et $\lambda_{i,j}$ $1 \leq j \leq d_i$ les racines de P_i .

Nous prendrons alors comme matrice de Jordan la matrice :

$$J = \text{diag} \left(J_i(\lambda_{i,j}) \right) \\ i = 1 \text{ à } k \\ j = 1 \text{ à } d_i$$

La matrice de passage Q peut alors être décrite de la façon suivante :
[Wilkinson, 1965]

$$Q = \begin{pmatrix} Q_1 \\ \vdots \\ Q_i \\ \vdots \\ Q_k \end{pmatrix} \quad \text{avec} \quad Q_i = \begin{pmatrix} L_i(\lambda_{i,1}) \\ \vdots \\ L_i(\lambda_{i,j}) \\ \vdots \\ L_i(\lambda_{i,d_i}) \end{pmatrix}$$

Les matrices $L_i(\lambda_{i,j})$ sont des matrices à i lignes et n colonnes (i est l'ordre de multiplicité de $\lambda_{i,j}$ dans le polynôme caractéristique) et les matrices Q_i ont $i \cdot d_i$ lignes et n colonnes.

Description de $L_i(X)$:

$$L_i(X) = \begin{pmatrix} 0 & . & . & 0 & 1 & . & . & C_{i-1}^{n-2} X^{n-i-1} & C_{i-1}^{n-1} X^{n-i} \\ . & . & . & . & . & . & . & . & . \\ 0 & 1 & 2X & . & . & . & . & C_1^{n-2} X^{n-3} & C_1^{n-1} X^{n-2} \\ 1 & X & X^2 & . & . & . & . & X^{n-2} & X^{n-1} \end{pmatrix}$$

si on note $\alpha_{i,h,k}$ le terme de la $h^{\text{ième}}$ ligne et de la $k^{\text{ième}}$ colonne de $L_i(X)$

$$\text{on a : } \alpha_{i,h,k}(X) = C_{i-h}^{k-1} X^{k-1+h-i}$$

Exemple : Nous considérons à nouveau $P = (X^2 - 2) \cdot (X^2 + X + 1)^3$

μ_1 et μ_2 les racines de $X^2 - 2$,

λ_1 et λ_2 les racines de $X^2 + X + 1$.

La matrice Q est de la forme suivante :

$$\left. \begin{array}{l} \left. \begin{array}{l} \left. \begin{array}{l} 1 \quad \mu_1 \quad \mu_1^2 \quad \mu_1^3 \quad \mu_1^4 \quad \mu_1^5 \quad \mu_1^6 \quad \mu_1^7 \\ 1 \quad \mu_2 \quad \mu_2^2 \quad \mu_2^3 \quad \mu_2^4 \quad \mu_2^5 \quad \mu_2^6 \quad \mu_2^7 \\ 0 \quad 0 \quad 1 \quad 3\lambda_1 \quad 6\lambda_1^2 \quad 10\lambda_1^3 \quad 15\lambda_1^4 \quad 21\lambda_1^5 \\ 0 \quad 1 \quad 2\lambda_1 \quad 3\lambda_1^2 \quad 4\lambda_1^3 \quad 5\lambda_1^4 \quad 6\lambda_1^5 \quad 7\lambda_1^6 \\ 1 \quad \lambda_1 \quad \lambda_1^2 \quad \lambda_1^3 \quad \lambda_1^4 \quad \lambda_1^5 \quad \lambda_1^6 \quad \lambda_1^7 \\ 0 \quad 0 \quad 1 \quad 3\lambda_2 \quad 6\lambda_2^2 \quad 10\lambda_2^3 \quad 15\lambda_2^4 \quad 21\lambda_2^5 \\ 0 \quad 1 \quad 2\lambda_2 \quad 3\lambda_2^2 \quad 4\lambda_2^3 \quad 5\lambda_2^4 \quad 6\lambda_2^5 \quad 7\lambda_2^6 \\ 1 \quad \lambda_2 \quad \lambda_2^2 \quad \lambda_2^3 \quad \lambda_2^4 \quad \lambda_2^5 \quad \lambda_2^6 \quad \lambda_2^7 \end{array} \right\} \begin{array}{l} L_1(\mu_1) \\ L_1(\mu_2) \\ L_3(\lambda_1) \\ L_3(\lambda_2) \end{array} \right\} Q_1 \\ \left\{ Q_3 \right. \end{array} \right\} Q_3$$

Remarque : les éléments de cette matrice sont bien sûr des nombres algébriques, mais dans une ligne donnée, chaque élément s'écrit comme une expression polynomiale en une seule racine.

1.2.c Calcul de l'inverse de la matrice de passage.

L'idée de l'algorithme est de se ramener au calcul de l'inverse d'une matrice de Vandermonde. Tout d'abord, nous pouvons "réduire" les coefficients en degré en utilisant le fait que chaque nombre algébrique $\lambda_{i,j}$ est racine d'un polynôme P_i de degré d_i ; ainsi $(\lambda_{i,j})^k$ s'écrit comme un polynôme en $\lambda_{i,j}$ de degré $d_i - 1$ au plus. Ce qui donne sur notre exemple :

$$Q = \begin{pmatrix} 1 & \mu_1 & 2 & 2\mu_1 & 4 & 4\mu_1 & 8 & 8\mu_1 \\ 1 & \mu_2 & 2 & 2\mu_2 & 4 & 4\mu_2 & 8 & 8\mu_2 \\ 0 & 0 & 1 & 3\lambda_1 & -6\lambda_1^{-6} & 10 & 15\lambda_1 & -21\lambda_1^{-21} \\ 0 & 1 & 2\lambda_1 & -3\lambda_1^{-3} & 4 & 5\lambda_1 & -6\lambda_1^{-6} & 7 \\ 1 & \lambda_1 & -\lambda_1^{-1} & 1 & \lambda_1 & -\lambda_1^{-1} & 1 & \lambda_1 \\ 0 & 0 & 1 & 3\lambda_2 & -6\lambda_2^{-6} & 10 & 15\lambda_2 & -21\lambda_2^{-21} \\ 0 & 1 & 2\lambda_2 & -3\lambda_2^{-3} & 4 & 5\lambda_2 & -6\lambda_2^{-6} & 7 \\ 1 & \lambda_2 & -\lambda_2^{-1} & 1 & \lambda_2 & -\lambda_2^{-1} & 1 & \lambda_2 \end{pmatrix}$$

Théorème :

Q se factorise en un produit $Q = S \cdot M$, où M est une matrice à coefficients dans \mathbb{K} et S une matrice bloc-diagonale

$$S = \text{diag} (S_1, \dots, S_k) \quad \text{les } S_i \text{ étant des blocs d'ordre } i \cdot d_i.$$

$$\text{avec } S_i = \begin{pmatrix} BS_i(\lambda_{i,1}) \\ \vdots \\ BS_i(\lambda_{i,j}) \\ \vdots \end{pmatrix} \quad j=1 \text{ à } d_i$$

et $BS_i(X)$ une matrice à i lignes, et $d_i + i$ colonnes :

$$BS_i(X) = \begin{pmatrix} 1 & X & \dots & X^{d_i-1} & 0 & \dots & \dots & \dots & \dots & \dots & 0 \\ 0 & \dots & \dots & \dots & 1 & X & \dots & X^{d_i-1} & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & \dots & \dots & \dots & \dots & \dots & \dots & \dots & 1 & X & \dots & X^{d_i-1} \end{pmatrix}$$

Exemple : si Q est la matrice de l'exemple précédent alors :

$$S = \left[\begin{array}{cc|cccccccc} 1 & \mu_1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & \mu_2 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 1 & \lambda_1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & \lambda_1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & \lambda_1 & 0 \\ 0 & 0 & 1 & \lambda_2 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & \lambda_2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & \lambda_2 & 0 \end{array} \right] \left\{ \begin{array}{l} BS_1(\mu_1) \\ BS_1(\mu_2) \\ \vdots \\ BS_3(\lambda_1) \\ BS_3(\lambda_2) \end{array} \right\} \begin{array}{l} S_1 \\ \\ S_3 \end{array}$$

$$M = \begin{pmatrix} 1 & 0 & 2 & 0 & 4 & 0 & 8 & 0 \\ 0 & 1 & 0 & 2 & 0 & 4 & 0 & 8 \\ 0 & 0 & 1 & 0 & -6 & 10 & 0 & -21 \\ 0 & 0 & 0 & 3 & -6 & 0 & 15 & -21 \\ 0 & 1 & 0 & -3 & 4 & 0 & -6 & 7 \\ 0 & 0 & 2 & -3 & 0 & 5 & -6 & 0 \\ 1 & 0 & -1 & 1 & 0 & -1 & 1 & 0 \\ 0 & 1 & -1 & 0 & 1 & -1 & 0 & 1 \end{pmatrix}$$

démonstration :

1) Chaque matrice $L_i(\lambda_{i,j})$ se factorise en $BS_i(\lambda_{i,j}) * M_i$ avec M_i une matrice à coefficients dans \mathbb{K} à $d_i * i$ lignes et n colonnes.

Nous avons donné page 17, l'expression de $\alpha_{i,h,k}(X)$, le terme de la $h^{\text{ième}}$ ligne et de la $k^{\text{ième}}$ colonne de $L_i(X)$.

$$\alpha_{i,h,k}(X) = C_{i-h}^{k-1} X^{k-1+h-i} = \sum_{p=0}^{d_i-1} a_{i,h,k}^{(p)} X^p \quad \text{modulo } P_i(X)$$

les $a_{i,h,k}^{(p)}$ étant des éléments du corps \mathbb{K} .

les coefficients de la matrice M_i sont alors définis par :

$$m_{1+p+h d_i, k} = a_{i,h,k}^{(p)} \quad \text{avec } 0 \leq h \leq i-1 \quad \text{et } 0 \leq p \leq d_i-1.$$

$$2) \quad \text{la matrice } Q_i = \begin{pmatrix} L_i(\lambda_{i,1}) \\ \vdots \\ L_i(\lambda_{i,i}) \\ \vdots \end{pmatrix} \quad j = 1, \dots, d_i.$$

se factorise en $S_i \star M_i$ (M_i la même matrice qu'en 1).

$$\text{et } M = \begin{pmatrix} & M_1 & & \\ & \cdot & \cdot & \cdot \\ & \cdot & \cdot & \cdot \\ & \cdot & \cdot & \cdot \\ & M_k & & \end{pmatrix}$$

fin de la démonstration .

Après avoir factorisé la matrice Q , l'algorithme se poursuivra en inversant les matrices S et M , puis en effectuant le produit $M^{-1} \star S^{-1}$.

- * Le calcul de M^{-1} pourra être fait éventuellement à l'aide de la méthode de Gauss .
- * On utilisera pour le calcul de S^{-1} un résultat sur l'inverse d'une matrice de Vandermonde .

Supposons que $P = X^d + a_{d-1}X^{d-1} + \dots + a_0$ soit un polynôme à coefficients dans \mathbb{K} et sans facteurs carrés. Notons alors μ_1, \dots, μ_d ses d racines distinctes. La matrice de Vandermonde associée à P est décrite ci-dessous :

$$V = \begin{vmatrix} 1 & \mu_1 & \dots & \mu_1^{d-1} \\ \vdots & & & \\ \vdots & & & \\ 1 & \mu_d & \dots & \mu_d^{d-1} \end{vmatrix}$$

Théorème: V est inversible et V^{-1} peut être décrite colonne par colonne :

$$V^{-1} = \begin{pmatrix} & \cdot & \cdot & \\ & \cdot & \cdot & \\ C(\mu_1) & \dots & C(\mu_d) & \\ & \cdot & \cdot & \end{pmatrix}$$

$$\text{avec } C(X) = \frac{1}{P'(X)} \begin{pmatrix} X^{d-1} + a_{d-1} X^{d-2} + \dots + a_1 \\ \dots \\ X^2 + a_{d-1} X + a_{d-2} \\ X + a_{d-1} \\ 1 \end{pmatrix}$$

démonstration : Considérons F_V la matrice compagnon associée au polynôme P ; alors μ_1, \dots, μ_d sont les valeurs propres de F_V . De plus les μ_i étant distinctes, F_V est diagonalisable et donc sa forme de Jordan J est diagonalisable.

D'après le paragraphe 1.2.b. on a $V \cdot F_V = J \cdot V$.

On en déduit $F_V \cdot V^{-1} = V^{-1} \cdot J$; les colonnes de V^{-1} sont donc formées par des vecteurs propres de F_V .

Calculons un vecteur propre de F_V associé à une valeur propre μ .

Le système $F_V(X_\mu) = \mu X_\mu$ avec $X_\mu = {}^t(x_1, \dots, x_d)$ donne les relations :

$$\left\{ \begin{array}{l} -a_0 x_d = \mu x_1 \\ x_1 - a_1 x_d = \mu x_2 \\ \dots \\ x_{d-1} - a_{d-1} x_d = \mu x_d \end{array} \right.$$

L'ensemble des solutions de ce système est une droite vectorielle engendrée par le vecteur :

$$X_\mu = \begin{pmatrix} \mu^{d-1} + a_{d-1} \mu^{d-2} + \dots + a_1 \\ \dots \\ \mu^2 + a_{d-1} \mu + a_{d-2} \\ \mu + a_{d-1} \\ 1 \end{pmatrix}$$

La matrice V^{-1} est donc de la forme :

$$V^{-1} = (f_{\mu_1} X_{\mu_1}, \dots, f_{\mu_d} X_{\mu_d}) \quad \text{les } f_{\mu_i} \text{ étant des coefficients non nuls.}$$

Comme $V \cdot V^{-1} = \text{Id}$ nous avons :

$$\begin{aligned} (1, \mu, \dots, \mu^{d-1}) f_{\mu} X_{\mu} &= 1 \\ \text{or } (1, \mu, \dots, \mu^{d-1}) X_{\mu} &= P'(\mu) \end{aligned}$$

$$\text{donc } f_{\mu} = \frac{1}{P'(\mu)} \quad \text{et } C(\mu) = \frac{1}{P'(\mu)} X_{\mu}$$

Nous pouvons maintenant finir d'expliquer le calcul de S^{-1} .

La matrice S étant bloc-diagonale $S = \text{diag}(S_1, \dots, S_k)$ nous aurons $S^{-1} = \text{diag}(S_1^{-1}, \dots, S_k^{-1})$. Chaque matrice S_i de taille $d_i \times i$ peut s'écrire comme un produit $S_i = P_i \cdot S V_i$ où P_i est une matrice de permutation et

$$S V_i = \underbrace{\text{diag}(V_i, \dots, V_i)}_{i \text{ blocs}}$$

V_i étant la matrice de Vandermonde, d'ordre d_i , associée au polynôme P_i . Les matrices V_i^{-1} se calculent en utilisant le dernier théorème, et $S_i^{-1} = S V_i^{-1} \cdot P_i^{-1}$.

Exemple : toujours le même.

μ_1 et μ_2 racines de $P_1(X) = X^2 - 2$.

λ_1 et λ_2 racines de $P_3(X) = X^2 + X + 1$

$$V_1 = \begin{pmatrix} 1 & \mu_1 \\ 1 & \mu_2 \end{pmatrix} \quad \text{et} \quad V_1^{-1} = \begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{\mu_1}{4} & \frac{\mu_2}{4} \end{pmatrix}$$

$$V_3 = \begin{pmatrix} 1 & \lambda_1 \\ 1 & \lambda_2 \end{pmatrix} \quad \text{et} \quad V_3^{-1} = \begin{pmatrix} \frac{1}{3} - \frac{1}{3} \lambda_1 & \frac{1}{3} - \frac{1}{3} \lambda_2 \\ -\frac{1}{3} - \frac{2}{3} \lambda_1 & -\frac{1}{3} - \frac{2}{3} \lambda_2 \end{pmatrix}$$

$$S^{-1} = \begin{vmatrix} a(\mu_1) & a(\mu_2) & 0 & 0 & 0 & 0 & 0 & 0 \\ b(\mu_1) & b(\mu_2) & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & c(\lambda_1) & 0 & 0 & c(\lambda_2) & 0 & 0 \\ 0 & 0 & d(\lambda_1) & 0 & 0 & d(\lambda_2) & 0 & 0 \\ 0 & 0 & 0 & c(\lambda_1) & 0 & 0 & c(\lambda_2) & 0 \\ 0 & 0 & 0 & d(\lambda_1) & 0 & 0 & d(\lambda_2) & 0 \\ 0 & 0 & 0 & 0 & c(\lambda_1) & 0 & 0 & c(\lambda_2) \\ 0 & 0 & 0 & 0 & d(\lambda_1) & 0 & 0 & d(\lambda_2) \end{vmatrix}$$

$$\text{avec} \quad \begin{cases} a(x) = \frac{1}{2} \\ b(x) = \frac{x}{4} \\ c(x) = \frac{1}{3} - \frac{1}{3} x \\ d(x) = -\frac{1}{3} - \frac{2}{3} x \end{cases}$$

Puis $Q^{-1} = M^{-1} \cdot S^{-1}$

Q^{-1} pouvant être décrite de la manière suivante :

$$Q^{-1} = [U(\mu_1), U(\mu_2), X(\lambda_1), Y(\lambda_1), Z(\lambda_1), X(\lambda_2), Y(\lambda_2), Z(\lambda_2)]$$

les coefficients des vecteurs $U(x), X(x), Y(x), Z(x)$ étant des polynômes de degré au plus 1. Nous donnons les composantes de ces vecteurs page suivante.

$$U(x) = \frac{1}{1372} \begin{pmatrix} -58x + 90 \\ -129x + 212 \\ -213x + 366 \\ -136x + 282 \\ -33x + 134 \\ 96x - 78 \\ 77x - 84 \\ 45x - 58 \end{pmatrix}$$

$$X(x) = \frac{1}{63} \begin{pmatrix} 8x - 2 \\ 26x + 4 \\ 40x + 11 \\ 33x + 18 \\ 6x + 9 \\ -13x - 2 \\ -14x - 7 \\ -5x - 4 \end{pmatrix}$$

$$Y(x) = \frac{1}{441} \begin{pmatrix} -142x - 248 \\ -108x - 582 \\ -45x - 708 \\ 130x - 421 \\ 100x + 38 \\ 12x + 228 \\ -21x + 189 \\ -25x + 64 \end{pmatrix}$$

$$Z(x) = \frac{1}{3087} \begin{pmatrix} -2894x - 106 \\ -7442x - 4198 \\ -7127x - 4387 \\ -4929x - 3099 \\ -109x - 356 \\ 2531x + 1441 \\ 2198x + 1288 \\ 897x + 579 \end{pmatrix}$$

Résumons l'algorithme de calcul de Q^{-1} .

- 1) Réduction " en degré " des coefficients de Q .
- 2) Construction des matrices S et M telles que $Q = S \cdot M$.
- 3) Calcul de M^{-1} .
- 4) Calcul de S^{-1} .
- 5) $Q^{-1} = M^{-1} \cdot S^{-1}$.

Conclusion :

Bien que les éléments de Q^{-1} appartiennent à l'extension $\mathbb{K}(\lambda_{1,1}, \dots, \lambda_{i,j}, \dots, \lambda_{k,d_k}) \quad i = 1, \dots, k, \quad j = 1, \dots, d_i$, nous avons montré que dans une colonne donnée de Q^{-1} , chaque élément s'exprime comme une expression polynomiale en un seul des nombres $\lambda_{i,j}$. De plus, on peut effectuer tous les calculs en utilisant les opérations arithmétiques de \mathbb{K} et de $\mathbb{K}[X]$.

Chapitre II

Premier algorithme pour le calcul de la forme de Frobenius
d'une matrice .

II. 1 Introduction.

Comme nous l'avons déjà dit dans le chapitre précédent, la forme de Frobenius d'une matrice A présente un grand intérêt pour deux raisons.

D'abord, il est facile à partir de cette forme d'en déduire la forme de Jordan de A ainsi qu'une matrice de passage. Pour certaines applications, la forme de Frobenius sera tout à fait satisfaisante, le passage à la forme de Jordan s'avérant inutile (calcul des diviseurs élémentaires par exemple).

Le deuxième avantage est que si A est une matrice à coefficients dans un corps \mathbb{K} , alors sa forme de Frobenius l'est aussi, et il existe des matrices de passage dont tous les coefficients sont des éléments de \mathbb{K} .

Plusieurs auteurs ont depuis longtemps proposé des méthodes constructives de la forme de Frobenius encore appelée forme rationnelle d'une matrice [Dixon, 1926], [Bennett, 1931], [Browne, 1940]. Si nous avons emprunté un grand nombre d'idée à ces auteurs, nous n'avons pas implanté leurs algorithmes qui ont une complexité supérieure aux deux algorithmes que nous proposons.

L'algorithme que nous présentons dans cette partie consiste à effectuer une suite de transformations élémentaires de "type semblable", chacune de ces transformations n'effectuant que des opérations arithmétiques dans le corps \mathbb{K} .

Il faut dire avant de continuer, que nous commettons un abus en prétendant que cet algorithme calcule la forme de Frobenius de A . On obtiendra en général, une forme faible de Frobenius, que nous avons définie dans le paragraphe 1.1.d.

Toutefois si l'on souhaite obtenir la forme de Jordan, la méthode exposée dans le chapitre I, s'applique encore.

Nous commençons par définir les transformations élémentaires.

II. 2 Transformations élémentaires "type semblable".

Elles transforment une matrice en une matrice qui lui est semblable.

- * $P_{i,j}$ permute les lignes i et j , ainsi que les colonnes i et j .
- * $M_{i,a}$ $a \neq 0$ multiplie la $i^{\text{ème}}$ ligne par a , et la $i^{\text{ème}}$ colonne par $1/a$.
- * $L_{i,a,j}$ remplace la $i^{\text{ème}}$ ligne par $i^{\text{ème}} + a * j^{\text{ème}}$ ligne, puis la $j^{\text{ème}}$ colonne par $j^{\text{ème}} - a * i^{\text{ème}}$ colonne.
- * $C_{i,a,j}$ remplace la $i^{\text{ème}}$ colonne par $i^{\text{ème}} + a * j^{\text{ème}}$ colonne, puis la $j^{\text{ème}}$ ligne par $j^{\text{ème}} - a * i^{\text{ème}}$ ligne.

Nous avons le théorème fondamental suivant :

Théorème : *L'ensemble des transformations élémentaires "type semblable" engendre le groupe des transformations $A \rightarrow P^{-1} \cdot A \cdot P$.*

Ce théorème nous assure l'existence d'une suite finie de transformations élémentaires qui conduise à la forme de Frobenius de A .

Complexité :

Le nombre d'opérations arithmétiques nécessaires pour chaque transformation élémentaire effectuée sur une matrice d'ordre n , est égal à :

- * $P_{i,j}$ aucune opération arithmétique.
- * $M_{i,a}$ 1 calcul d'inverse et $2n$ multiplications.
- * $L_{i,a,j}$ et $C_{i,a,j}$ $2*(n-1)$ additions et $2n$ multiplications.

II.3 La procédure "polyminel".

On utilise la méthode de Danilewski ([Danilewski , 1937] , [Gastinel , 1966] en faisant une suite de transformations élémentaires sur une matrice A d'ordre n , afin d'obtenir une matrice semblable bloc-diagonale $B = \text{diag} (F_1 , D_1)$, où F_1 est une matrice compagnon de dimension d , et D_1 une matrice quelconque. En termes géométriques, si \mathfrak{A} désigne l'endomorphisme associé à A , il faut trouver deux sous espaces \mathfrak{F} et \mathfrak{G} vérifiant les propriétés (\mathfrak{P}) suivantes :

- * \mathfrak{F} et \mathfrak{G} sont stables par \mathfrak{A} .
- * \mathfrak{F} est un sous espace cyclique $\mathfrak{F} = (f_1 , \dots , \mathfrak{A}^{d-1} (f_1))$
- * \mathfrak{F} et \mathfrak{G} sont en somme directe.

La première étape est de faire apparaître une matrice compagnon C_1 de dimension $d_1 \times d_1$ dans la partie située en haut et à gauche de la matrice (figure 1 ci-dessous) .

$$(1) \quad \left(\begin{array}{cc|cc} & & & \\ & C_1 & & B_1 \\ \hline 0 & & 0 & \\ & & & B_2 \\ 0 & & 0 & \end{array} \right)$$

C'est la procédure "polyminel" qui exécute ce travail . Si on note B la matrice transformée par "polyminel" il est facile de connaître une matrice P telle que $A \cdot P = P \cdot B$. Il suffit pour cela d'initialiser une matrice à l'identité , puis d'effectuer les mêmes transformations sur les colonnes de cette matrice que sur celles de A . En pratique , si l'on désire obtenir la matrice de passage, on travaillera avec la matrice

A
Id

à $2n$ lignes et n colonnes

On pourrait également obtenir P^{-1} en initialisant une matrice à l'identité , et effectuer sur les lignes de cette matrice les mêmes transformations que sur celles de A .

Avant de décrire en détail la procédure "polyminel" , examinons la procédure "chercheli" qui est appelée par "polyminel" .

Cette procédure recherche dans la colonne j d'une matrice B un terme non nul dont l'indice ligne est supérieur ou égal à $j + 1$. Si tous les $b_{i,j}$ avec $i \geq j$ sont nuls , "chercheli" retourne $n + 1$.

procedure **chercheli** (B , j)

entrées : une matrice B , et j un entier $j \leq n$.
sortie : un entier .

begin

$k := j + 1$;
while ($k \leq n$ and $b_{k,j} \neq 0$) *do* $k := k + 1$;
return k ;

end ;

procedure **polymine1** (B , j)

entrées : une matrice B (de dimension $n \cdot n$ ou $2n \cdot n$) , j un entier $j \leq n$
sortie : l'entier d (égal à la dimension de la matrice compagnon C_1)
effet : transforme la matrice B en une matrice de la forme (1) .

begin

$k := \text{chercheli} (B , j)$;

while $k \leq n$ *do*

begin

if $k \neq j+1$ *then* $P_{k,j+1}$; (ainsi $b_{j+1,j} \neq 0$)

$M_{j+1, \frac{1}{b_{j+1,j}}}$; (ainsi $b_{j+1,j} = 1$)

for $i=1$ *to* n *do*

if $i \neq j+1$ *then* $L_{i, -b_{i,j}, j+1}$; (ainsi $b_{i,j} = 0$ si $i \neq j+1$)

$j = j + 1$;

$k := \text{chercheli} (B , j)$;

end ;

$d := j$;

return d ;

end ;

Exemple 1:

Prenons pour A la matrice Mat - 6 (définie dans l'annexe), et $\mathbb{K} = \mathbb{Q}$.

polyminel (A , 1) ;

A est transformée en une matrice B décrite ci-dessous :

$$\begin{pmatrix} 0 & -5 & \frac{-12}{5} & \frac{2}{5} & \frac{1}{5} & 0 \\ 1 & 4 & \frac{7}{5} & \frac{-2}{5} & \frac{-1}{5} & 0 \\ 0 & 0 & \frac{1}{5} & \frac{4}{5} & \frac{2}{5} & 0 \\ 0 & 0 & \frac{-3}{5} & \frac{3}{5} & \frac{9}{5} & 0 \\ 0 & 0 & \frac{-2}{5} & \frac{-8}{5} & \frac{21}{5} & 0 \\ 0 & 0 & \frac{-1}{5} & \frac{-4}{5} & \frac{3}{5} & 3 \end{pmatrix}$$

Nous énonçons maintenant un théorème qui justifiera le nom de cette procédure "polyminel" .

Théorème 1. *Le polynôme associé à la matrice compagnon C_1 est le polynôme minimal du vecteur e_1 .*

Dans le dernier exemple ce polynôme est $x^2 - 4x + 5$.

démonstration: Intéressons nous à la matrice de passage P et supposons que la matrice compagnon C_1 soit de dimension $d \times d$.

Si on note \mathfrak{B} la base canonique (e_1, \dots, e_n) de \mathbb{K}^n et \mathfrak{A} l'endomorphisme associé à la matrice A dans la base \mathfrak{B} , on peut dire que la matrice B est la matrice de \mathfrak{A} dans une nouvelle base $\mathfrak{B}' = (f_1, \dots, f_n)$. Les vecteurs de cette nouvelle base étant représentés par les colonnes de la matrice de passage P . Or , la première colonne de P représente le vecteur e_1 de \mathfrak{B} (en effet , la procédure "polyminel" ne modifie jamais la première colonne de P).

Des relations :

$$\mathfrak{A}(f_1) = f_2, \quad \mathfrak{A}(f_2) = f_3, \quad \dots, \quad \mathfrak{A}(f_{d-1}) = f_d$$

$$\mathfrak{A}(f_d) = -a_0 f_1 - \dots - a_{d-1} f_d$$

$$\text{on déduit } f_2 = \mathfrak{A}(f_1), \quad \dots, \quad f_d = \mathfrak{A}^{d-1}(f_1)$$

$$\mathfrak{A}^d(f_1) = -a_0 f_1 - \dots - a_{d-1} \mathfrak{A}^{d-1}(f_1)$$

Comme $f_1 = e_1$, $(e_1, \dots, \mathfrak{A}^{d-1}(e_1))$ est un système libre, et $\mathfrak{A}^d(e_1) + a_{d-1} \mathfrak{A}^{d-1}(e_1) + \dots + a_0 e_1 = 0$ ce qui termine la démonstration.

remarque : on peut calculer le polynôme minimal d'un vecteur v non nul à l'aide de "polymine1". Il suffit pour cela de considérer une base \mathfrak{B}_1 dont v est le premier vecteur, de construire la matrice A représentant \mathfrak{A} dans la base \mathfrak{B}_1 , puis d'exécuter la procédure "polymine1". Le polynôme associé à la matrice compagnon C_1 est alors le polynôme minimal du vecteur v .

Signalons que nous pouvons obtenir aisément comme conséquence du dernier théorème quelques résultats bien connus d'algèbre linéaire, mais démontrés en général d'une toute autre manière, et parfois accompagnés d'hypothèses restrictives sur le corps \mathbb{K} .

Théorème 2: le polynôme minimal d'un vecteur v non nul divise le polynôme caractéristique P_A d'un endomorphisme \mathfrak{A} .

démonstration: considérons une base \mathfrak{B}_1 ayant comme premier vecteur v , et la matrice A représentant \mathfrak{A} dans la base \mathfrak{B}_1 .

P_A est égal au produit des polynômes caractéristiques de C_1 et de B_2 (voir figure 1). Or le polynôme minimal π_v de v est égal au polynôme caractéristique de C_1 (théorème 1 et sa remarque).

Théorème 3 (Cayley - Hamilton) le polynôme minimal Π_A d'un endomorphisme divise le polynôme caractéristique P_A .

démonstration: Si (v_1, \dots, v_n) est une base de \mathbb{K}^n ,
 $\Pi_A = \text{ppcm}(\pi_{v_1}, \dots, \pi_{v_n})$, chaque π_{v_i} divise P_A
 et donc Π_A divise P_A .

II.4 La procédure zéroadroite.

Après avoir utilisé la procédure "polymine1", nous avons une matrice de la forme (1) :

$$\left(\begin{array}{cc|c} C_1 & & B_1 \\ \hline 0 & 0 & \\ \hline 0 & 0 & B_2 \end{array} \right)$$

La suite de l'algorithme consiste à faire apparaître des zéros dans la partie située à droite du bloc C_1 . Malheureusement on ne parviendra pas toujours à remplacer complètement le bloc B_1 par un bloc contenant uniquement des zéros, il restera en général des termes non nuls sur la première ligne du bloc B_1 . C'est la procédure "zéroadroite" qui transformera notre matrice en une matrice de la forme suivante :

$$(2) \quad \left(\begin{array}{cc|ccc} & & * & * & \dots & * \\ & C_1 & 0 & & & 0 \\ & & 0 & & & 0 \\ \hline 0 & 0 & & & & \\ & & & B_3 & & \\ 0 & 0 & & & & \end{array} \right)$$

les $*$ représentant des éléments quelconques de \mathbb{K} .

La stratégie que nous proposons commence par mettre des zéros sur la d ème ligne de B_1 en utilisant le 1 se situant sur la même ligne , colonne $d-1$. Nous utilisons pour cela les transformations élémentaires $C_j, -b_{d,j}, d-1$ avec $d+1 \leq j \leq n$. Puis nous mettons des zéros sur la ligne $d-1$ de B_1 , en utilisant le 1 qui se trouve sur la même ligne , colonne $d-2$. La ligne d de B_1 où nous avons mis des zéros à l'étape précédente , reste inchangée par ces nouvelles transformations . Le processus se poursuit jusqu'à la 2 ème ligne de B_1 .

procedure zéroadroite (B, i_1, i_2) ;

entrées : B une matrice de la forme (1) , i_1 et i_2 deux entiers tels que $0 \leq i_1 < i_2 \leq n$.

effet : transforme la matrice B en une matrice de la forme (2) lorsque $i_1 = 0$ et $i_2 = d$

begin

for $i = i_2$ *step* -1 *until* $i_1 + 2$ *do*

for $j = i_2 + 1$ *to* n *do* $C_j, -b_{i,j}, i-1$;

end ;

Exemple 2 : prenons pour B la matrice de l'exemple 1 .

zéroadroite ($B, 0, 2$) ;

$$\begin{pmatrix} 0 & -5 & \frac{-9}{5} & \frac{8}{5} & \frac{-4}{5} & 0 \\ 1 & 4 & 0 & 0 & 0 & 0 \\ 0 & 0 & \frac{1}{5} & \frac{4}{5} & \frac{2}{5} & 0 \\ 0 & 0 & \frac{-3}{5} & \frac{3}{5} & \frac{9}{5} & 0 \\ 0 & 0 & \frac{-2}{5} & \frac{-8}{5} & \frac{21}{5} & 0 \\ 0 & 0 & \frac{-1}{5} & \frac{-4}{5} & \frac{3}{5} & 3 \end{pmatrix}$$

II. 5. Obtention de la forme de Frobenius.

Après la procédure "zéroadroite", nous obtenons une matrice $B = (b_{i,j})$ de la forme (2), qui représente l'endomorphisme \mathfrak{A} dans une nouvelle base $(f_1, \dots, f_d, g_{d+1}, \dots, g_n)$ dont chaque vecteur est représenté par une colonne de la matrice de passage P .

Deux cas peuvent se présenter :

1) Supposons que $b_{1,j} = 0 \quad \forall j \quad d+1 \leq j \leq n$ alors les sous espaces \mathcal{F} et \mathcal{G} engendrés par (f_1, \dots, f_d) et (g_{d+1}, \dots, g_n) sont stables par \mathfrak{A} , et en somme directe. Le premier bloc F_1 est donc trouvé, l'algorithme se poursuivra en travaillant sur la matrice B_3 de dimension $n - d$.

2) il existe j tel que $b_{1,j} = a \neq 0$ et $d+1 \leq j \leq n$.

Il semble alors difficile de trouver des transformations élémentaires pour annuler les termes $b_{1,j} \quad d+1 \leq j \leq n$, et donc de trouver un sous espace stable par \mathfrak{A} et en somme directe avec \mathcal{F} . C'est le théorème suivant qui va nous permettre de progresser.

Théorème 4.

Le degré du polynôme minimal de g_j est supérieur ou égal à $d+1$.

démonstration : le $\$$ représente un élément quelconque du corps \mathbb{K} , et nous supposons $b_{1,j} = a \neq 0$.

$$\begin{aligned} \mathfrak{A}(g_j) &= a f_1 + \sum_{j=d+1}^n \$ g_j \\ \mathfrak{A}^2(g_j) &= a \mathfrak{A}(f_1) + \sum_{j=d+1}^n \$ \mathfrak{A}(g_j) \\ &= \$ f_1 + a f_2 + \sum_{j=d+1}^n \$ g_j \\ \mathfrak{A}^d(g_j) &= \sum_{i=1}^{d-1} \$ f_i + a f_d + \sum_{j=d+1}^n \$ g_j \end{aligned}$$

ce qui montre que les $d+1$ vecteurs $g_j, \mathfrak{A}(g_j), \mathfrak{A}^2(g_j), \dots, \mathfrak{A}^d(g_j)$ forment une famille libre, et que le degré du polynôme minimal de g_j est supérieur ou égal à $d+1$.

La dimension du sous espace cyclique $\mathfrak{E}_j = (g_j, \mathfrak{A}(g_j), \mathfrak{A}^2(g_j), \dots)$ est alors supérieure ou égale à $d+1$. Puisque le sous espace \mathcal{F} semble être un "mauvais" candidat pour vérifier les propriétés (\mathcal{P}) avec un autre sous espace, nous allons tout simplement permuter les colonnes 1 et j de la matrice, (ainsi que les lignes 1 et j), puis recommencer en appelant la procédure "polymine1".

Nous obtiendrons encore une matrice de la forme (1) avec une matrice compagnon C_2 de dimension supérieure ou égale à $d+1$. En appelant "zéroadroite", nous aurons une matrice de la forme (2), et nous continuerons jusqu'à obtenir deux sous espaces vérifiant les propriétés (\mathcal{P}) . Le procédé s'arrêtera puisque la suite $\{d_i\}$ des dimensions des matrices compagnons obtenues à chaque étape par "polymine1", est strictement croissante et bornée par n .

Exemple 3 : reprenons l'exemple 2. Dans cet exemple, la dimension de la matrice compagnon C_1 est égale à 2. Comme $b_{1,3}$ est non nul, on permute les colonnes 1 et 3, puis les lignes 1 et 3. Puis

polymine1 (B, 1);

$$B = \begin{pmatrix} 0 & 0 & 0 & -5 & \frac{-672}{53} & 0 \\ 1 & 0 & 0 & 14 & \frac{-2023}{106} & 0 \\ 0 & 1 & 0 & -14 & \frac{1271}{106} & 0 \\ 0 & 0 & 1 & 6 & \frac{-279}{106} & 0 \\ 0 & 0 & 0 & 0 & 3 & 0 \\ 0 & 0 & 0 & 0 & 0 & 3 \end{pmatrix}$$

la dimension de la matrice compagnon est maintenant égale à 4.

zéroadroite (B , 0 , 4) ;

$$B = \begin{pmatrix} 0 & 0 & 0 & -5 & \frac{-672}{53} & 0 \\ 1 & 0 & 0 & 14 & 0 & 0 \\ 0 & 1 & 0 & -14 & 0 & 0 \\ 0 & 0 & 1 & 6 & 0 & 0 \\ 0 & 0 & 0 & 0 & 3 & 0 \\ 0 & 0 & 0 & 0 & 0 & 3 \end{pmatrix}$$

Comme $b_{1,5} \neq 0$, on permute les colonnes 1 et 5 , puis les lignes 1 et 5 .

polymine1 (B , 1) ;

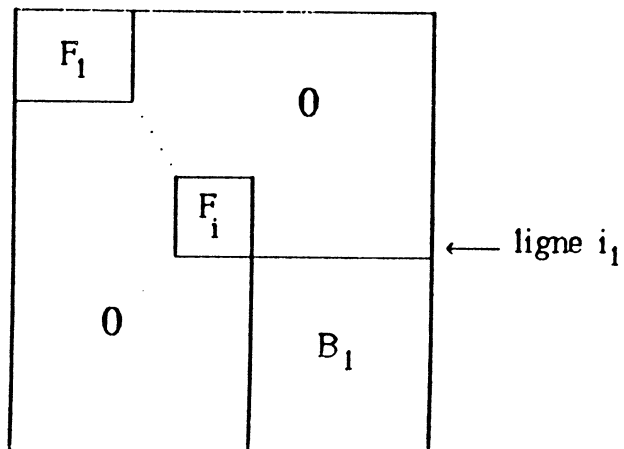
$$B = \begin{pmatrix} 0 & 0 & 0 & 0 & 15 & 0 \\ 1 & 0 & 0 & 0 & -47 & 0 \\ 0 & 1 & 0 & 0 & 56 & 0 \\ 0 & 0 & 1 & 0 & -32 & 0 \\ 0 & 0 & 0 & 1 & 9 & 0 \\ 0 & 0 & 0 & 0 & 0 & 3 \end{pmatrix}$$

La dimension de la matrice compagnon C_1 est égale à 5 .

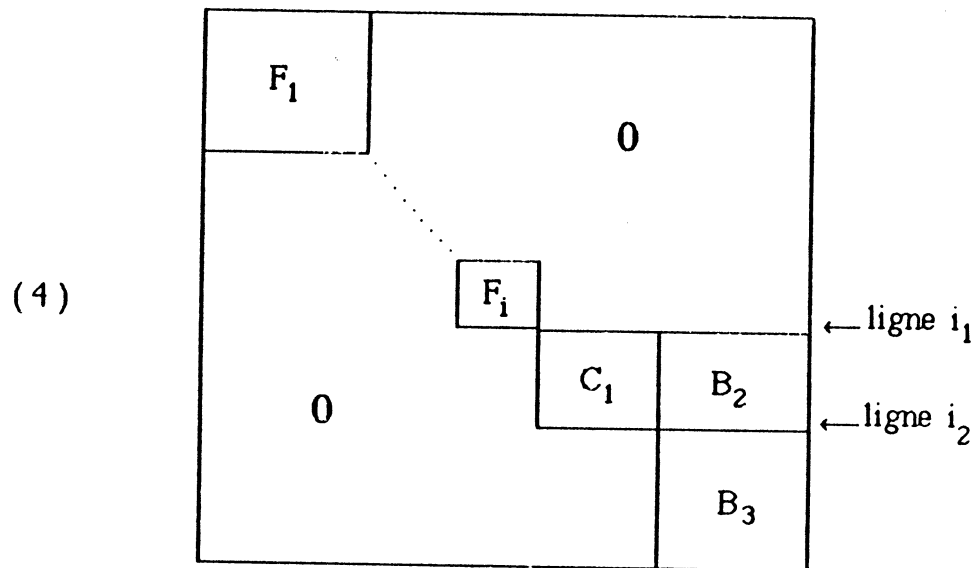
zéroadroite (B , 0 , 5) laisse B inchangée . Comme $b_{1,6} = 0$, le premier bloc F_1 est trouvé .

Pour former les autres blocs F_2, \dots, F_k nous utilisons exactement la même technique . Si B est de la forme

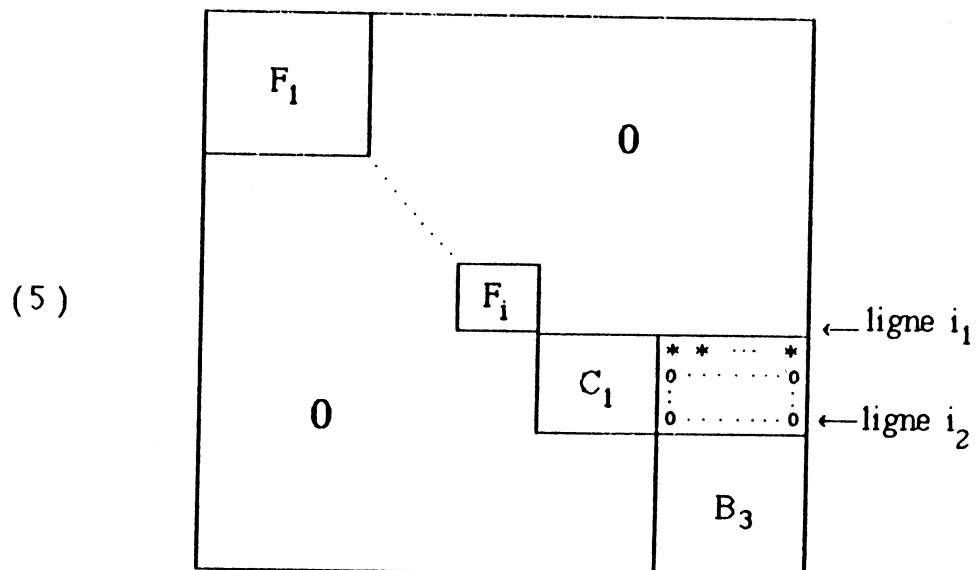
(3)



les F_i étant des matrices compagnons et B_1 une matrice quelconque, la procédure "polyminel ($B, i_1 + 1$)" transforme B en une matrice de la forme :



puis zéroadroite (B, i_1, i_2) donnera une matrice



* si tous les éléments $b_{i,j}$ avec $i = i_1 + 1$ et $i_2 < j \leq n$ sont nuls, un nouveau bloc $F_{i+1} = C_1$ est trouvé.

* s'il existe $b_{i,j} \neq 0$ avec $i = i_1 + 1$ et $i_2 < j \leq n$, on permutera les colonnes $i_1 + 1$ et j ainsi que les lignes de mêmes indices, et on continuera en appelant alternativement les procédures "polymine1" et "zéroadroite" jusqu'à obtenir un nouveau bloc F_{i+1} .

Pour former ce nouveau bloc, nous utilisons les procédures "chercheco" et "unbloc".

$\text{chercheco}(B, i, j_1)$ recherche dans la $i^{\text{ème}}$ ligne de B un terme non nul $b_{i,j}$ tel que $j_1 \leq j$. Si tous les $b_{i,j}$ $j_1 \leq j \leq n$ sont nuls, "chercheco" retourne $n+1$.

procedure **chercheco** (B, i, j_1);

entrées : B une matrice de dimension $n \times n$ (ou $2n \times n$), i et j_1 deux entiers tels que $1 \leq i, j_1 \leq n$.

sorties : un entier j tel que $b_{i,j} \neq 0$ et $j_1 \leq j$.

begin

$j = j_1$;

while ($j \leq n$ and $b_{i,j} = 0$) *do* $j = j + 1$;

return j ;

end;

procedure **unbloc** (B , i_1) ;

entrées : B une matrice de dimension $n \times n$ (ou $2n \times n$) de la forme (3)
et i_1 un entier $1 \leq i_1 \leq n$.

sortie : transforme la matrice B en une matrice de la forme (3)
mais avec un bloc F_{i+1} supplémentaire . Retourne l'entier
 $i_2 = i_1 + \dim (F_{i+1})$.

begin

repeat

begin

$i_2 := \text{polymine1} (B , i_1 + 1) ;$

$\text{zéroadroite} (B , i_1 , i_2) ;$

$j := \text{chercheco} (B , i_1 + 1 , i_2 + 1) ;$

if $j \leq n$ *then* $P_{i_1+1,j} ;$

end

until $j > n ;$

return $i_2 ;$

end ;

Enfin , c'est la procédure "frobenius" qui nous permettra de déterminer une forme faible de Frobenius $F = \text{diag} (F_1 , \dots , F_k)$ d'une matrice A , avec si on le désire, une matrice de passage P .

procedure frobenius (A)

entrée : A une matrice de dimension $n \times n$ (ou $2n \times n$ si l'on souhaite une matrice de passage) .

effet : transforme A en une matrice $F = \text{diag} (F_1 , \dots , F_k)$. (dans le cas où l'on a demandé une matrice de passage , on aura une matrice de dimension $2n \times n$ de la forme :

$$\begin{bmatrix} F \\ P \end{bmatrix}$$

avec $F = \text{diag} (F_1 , \dots , F_k)$ et P telle que $AP = PF$.

begin

$i_1 = 0$;

repeat

begin

$i_2 = \text{unbloc} (A , i_1)$;

$i_1 = i_2$;

end ;

until $i_2 = n$;

end ;

Complexité :

Supposons que l'on désire connaître seulement la forme de Frobenius (on travaille alors avec une matrice de dimension $n \times n$) .

Pour construire la matrice C_1 (figure 4) de dimension $d \times d$ ($d = i_2 - i_1$) avec "polymine1" , nous effectuons :

$d-1$ calculs d'inverses

$n \times (d-1)$ transformations élémentaires de type $L_{i,a,j}$ ou $M_{i,a}$.

on peut majorer le nombre d'opérations par :

$d-1$ calculs d'inverses

$n \times (d-1) \times 2 \times n$ additions et multiplications.

La procédure "zéroadroite" qui transformera notre matrice en une matrice de la forme (5) demandera $(i_2 - i_1 - 1) * (n - i_2 - 1)$ transformations élémentaires soit au plus :

$(d - 1) * n * 2 * n$ additions et multiplications.

Le cas le plus défavorable est le cas où les procédures "polyminel" et "zéroadroite" sont appelées alternativement n fois pour former le premier (et unique) bloc F_1 . La procédure "unbloc" est alors appelée une seule fois, et la $d^{\text{ième}}$ itération de la boucle de "unbloc" demande au plus $4 n^2 * (d-1)$ additions et multiplications, soit au total pour "unbloc" : $4 n^2 * (0 + 1 + 2 + \dots + n-1)$.

Conclusion:

Le nombre d'opérations arithmétiques nécessaires pour calculer une forme faible de Frobenius à l'aide de cet algorithme peut être majoré par :

$n^2 / 2$ calculs d'inverses.

$2 n^4$ additions et multiplications .

Remarques :

1) Si l'on travaille avec une matrice de dimension $2n \times n$ pour avoir une matrice de passage, le résultat est :

$n^2 / 2$ calculs d'inverses.

$3 n^4$ additions et multiplications .

2) Si le polynôme caractéristique de la matrice est irréductible, l'algorithme se réduit à un seul appel à "polyminel", et nous effectuerons seulement :

$n - 1$ calculs d'inverses.

$2 n^3$ additions et multiplications .

II . 6 Résultats lorsque $K = F_p$ et $K = \mathbb{Q}$.

Nous présentons dans cette partie, les résultats obtenus en programmant l'algorithme tel qu'il a été décrit dans les précédents paragraphes . Les calculs ont été effectués sur une machine DPS8/70M , système Multics . Les programmes ont été écrits en Maclisp , et aussi en Reduce (version 3.0) afin d'établir quelques comparaisons. Nous verrons à cette occasion, que si le langage Reduce offre comme intérêt évident pour l'utilisateur une grande facilité pour écrire les programmes, il reste certain qu'un programme écrit en Maclisp demeure beaucoup moins coûteux lors de l'exécution, et permet donc d'envisager le traitement d'une plus large classe d'exemples.

II . 6 . a Quelques commentaires au sujet du cas $K = F_p$.

F_p désigne ici un corps fini à p éléments, p étant un nombre premier. Signalons le livre de Lipson [Lipson , 1981] pour une introduction à l'arithmétique dans ces corps , et la thèse [Howell , 1971] .

Le cas où le corps de base est un corps fini F_p est d'un intérêt particulier . En effet, en représentant tous les éléments de F_p par des entiers compris entre 0 et $p-1$, on évitera tous les problèmes d'éclatement des coefficients qui peuvent se produire lorsqu'on travaille dans \mathbb{Q} . De plus si le nombre premier p est un "petit" entier (c'est à dire si p^2 est inférieur à l'entier maxint de multics , soit $p \leq 185363$) on utilisera pour écrire les opérations arithmétiques de F_p , les fonctions spéciales qu'offre Maclisp pour travailler avec les petits entiers.

Ces fonctions spéciales sont :

$+$ et $*$	pour la somme et les produit de deux petits entiers .
$-$	pour l'opposé d'un petit entier .
$//$ et \backslash	pour le quotient et le reste de la division euclidienne .
$>$, $<$, $=$	pour comparer deux petits entiers .

Nous donnons à la fin de ce chapitre , l'ensemble des procédures que nous avons écrites pour effectuer les opérations arithmétiques de F_p . On trouvera les procédures "plusfp" et "timesfp" pour la somme et le produit de deux éléments de F_p , "minusfp" et "invfp" pour le calcul de l'opposé et de l'inverse d'un élément de F_p .

Pour obtenir les résultats présentés à la fin de cette partie, nous avons choisi comme nombre premier $p = 185363$.

Si l'on choisit un nombre premier $p < 185363$, les temps de calcul seraient comparables à ceux que nous avons obtenus puisque nous travaillons avec des petits entiers.

Si l'on choisit un nombre premier $p > 185363$ il faut utiliser les fonctions plus, times, minus ... destinées à travailler avec des entiers de taille quelconque. Le temps de calcul sera alors beaucoup plus long.

II.6.b Commentaires au sujet du cas $K = \mathbb{Q}$.

Nous avons fait l'essai d'écrire les programmes directement en langage Reduce. Le temps d'exécution est malheureusement bien supérieur à ce que l'on peut obtenir en écrivant les programmes en Maclisp.

Les rationnels n'étant pas connus au niveau Maclisp, nous avons écrit l'ensemble des procédures permettant d'effectuer les opérations arithmétiques dans \mathbb{Q} . Ces procédures se trouvent à la fin de ce chapitre.

II.6.c Tableau des résultats.

Nous avons travaillé avec les matrices mat-4, mat-6, mat-10, mat-20, mat1-20, décrites en annexe. (rappelons que mat-n est une matrice de taille n).

Les colonnes correspondent aux expériences suivantes :

- (1) $K = F_p$ avec $p = 185363$. Calcul d'une forme faible de Frobenius. Programmes Maclisp.
- (2) $K = F_p$ avec $p = 185363$. Calcul d'une forme faible de Frobenius et d'une matrice de passage. Programmes Maclisp.
- (3) $K = \mathbb{Q}$. Calcul d'une forme faible de Frobenius. Programmes Maclisp.
- (4) $K = \mathbb{Q}$. Calcul d'une forme faible de Frobenius et d'une matrice de passage. Programmes Maclisp.
- (5) $K = \mathbb{Q}$. Calcul d'une forme faible de Frobenius et d'une matrice de passage. Programmes Reduce.

Dans chaque colonne les temps d'exécution sont exprimés en secondes. Les formes de Frobenius ($\mathbb{K} = \mathbb{Q}$) et leurs matrices de passage sont données à la fin de ce chapitre.

nom de la matrice	(1)	(2)	(3)	(4)	(5)
mat - 4	0 , 0 12	0 , 017	0 , 044	0 , 071	1 , 986
mat - 6	0 , 071	0 , 107	0 , 241	0 , 555	9 , 970
mat - 10	0 , 408	0 , 651	1 , 648	2 , 635	
mat - 20	2 , 500	4 , 174	11 , 838	20 , 037	
mat 1 - 20	1 , 944	2 , 887	39 , 879	81 , 219	

Dans le paragraphe II . 4 . nous avons montré que le rapport entre le nombre d'opérations (multiplications et additions) nécessaires pour le calcul, d'une part de la forme de Frobenius et d'une matrice de passage, d'autre part de la seule forme de Frobenius était égal à 1,5.

Il est intéressant de constater, en comparant les colonnes (1) et (2) ($K = F_p$) du tableau des résultats , qu'on retrouve la quantité 1,5 lorsqu'on fait le rapport des temps de calculs.

En comparant les colonnes (3) et (4) ($K = \mathbb{Q}$) , se rapport varie suivant les exemples, et peut être supérieur à 2 . Ce qui montre que les opérations effectuées avec les éléments de la matrice de passage, sont souvent plus coûteuses que les opérations effectuées pour rechercher la seule forme de Frobenius. Ce surcoût étant dû lui-même à la présence de "trop grands" entiers dans la matrice de passage.

L'influence des grands entiers peut aussi être mise en évidence en comparant les colonnes (4) ($K = \mathbb{Q}$) et (2) ($K = F_p$) . Le rapport varie entre 4,2 pour la matrice mat-4 , à 28 pour la matrice mat1-20 .

C'est ce phénomène qui a motivé la recherche d'un deuxième algorithme, présenté dans le chapitre suivant.

Mais avant, nous étudions ce que peut apporter un algorithme modulaire.

II . 7 Un algorithme modulaire pour le cas $K = \mathbb{Q}$.

Nous supposons dans cette partie que A est une matrice à coefficients entiers. La forme de Frobenius F de A est aussi une matrice à coefficients entiers. Nous donnons dans la proposition suivante , une borne des coefficients de F en fonction des coefficients et de la dimension de A .

proposition 1 :

Soit A une matrice à coefficients entiers d'ordre n .

Notons $M_A = \max |a_{i,j}|$ et F sa forme de Frobenius .

Alors $M_F = \max |f_{i,j}| \leq 2^{n-1} (n M_A)^n$.

démonstration :

F est une matrice bloc-diagonale , chaque bloc étant une matrice compagnon. Les polynômes associés à ces blocs sont des diviseurs du polynôme caractéristique P_F de F .

Définissons la norme matricielle $\| A \| = \max_i \sum_j | a_{ij} |$.

Nous avons $\| A \| \leq n M_A$ et si λ est une valeur propre de A $|\lambda| \leq \| A \|$.

Si $Q = X^d + b_1 X^{d-1} + \dots + b_n$ est un polynôme divisant le polynôme caractéristique de A , on peut le factoriser sur le corps des nombres complexes :

$$Q = \prod (X - \lambda_i) \quad \text{les } \lambda_i \text{ appartenant au spectre de } A.$$

Nous avons alors les inégalités $|b_j| \leq C_n \| A \|^j$.

Comme pour tout $j \leq n$ $C_n \leq 2^{n-1}$

on en déduit que $|b_j| \leq 2^{n-1} \| A \|^n \leq 2^{n-1} (n M_A)^n$.

Dans la suite nous noterons $B = 2^{n-1} (n M_A)^n$ la borne donnée par la proposition 1. Choisissons maintenant k nombres premiers p_1, \dots, p_k tels que $p = p_1 \cdot \dots \cdot p_k \leq 2B$; et cherchons une forme faible de Frobenius de A en utilisant l'algorithme précédent et en travaillant dans l'anneau

$$F_{p_1} \cdot \dots \cdot F_{p_k}$$

Si tous les calculs d'inverses sont possibles , il suffit à la fin de l'algorithme de "remonter" les coefficients de F en utilisant le théorème des restes chinois. Si un calcul d'inverse s'avère impossible au cours de l'algorithme , il faut choisir une autre famille de nombres premiers et relancer l'algorithme.

Nous n'avons pas envisagé le calcul d'une matrice de passage avec cette méthode car cela semble plus difficile. En effet , même si A est une matrice à coefficients entiers , l'algorithme peut produire une matrice de passage contenant des coefficients rationnels et non entiers . De plus nous n'avons pu trouver une borne "raisonnable" pour majorer les numérateurs et dénominateurs figurant dans la matrice de passage. C'est pour cette raison que nous ne donnons que les

résultats concernant l'obtention d'une forme faible de Frobenius , ainsi qu'un rappel des résultats obtenus lorsque $\mathbb{K} = \mathbb{Q}$.

nom de la matrice	(3)	(6)	k
mat-4	0,044	0,041	2
mat-6	0,241	0,231	3
mat-10	1,648	2,807	6
mat-20	11,838	42,609	14
mat1-20	39,879	29,216	14

(3) $\mathbb{K} = \mathbb{Q}$. Calcul d'une forme faible de Frobenius.
Programmes Maclisp.

(6) algorithme modulaire . Programmes Maclisp.

Nous avons porté dans la dernière colonne le nombre k d'entiers premiers utilisés dans l'algorithme modulaire.

Conclusion :

Il est difficile , au vu de ces résultats de déclarer que l'un des deux algorithmes est meilleur que l'autre. Dans les cas où de grands entiers apparaissent lors de l'exécution de l'algorithme non modulaire , l'algorithme modulaire est plus performant (mat1-20) . Dans les autres cas , l'algorithme modulaire peut être nettement plus coûteux (mat-10 , mat-20) .

Le fait que l'algorithme modulaire ne nous permet pas d'obtenir la matrice de passage semble à notre avis le plus gros inconvénient .

forme de Frobenius de mat-4 et matrice de passage.

0	0	-75	0
1	0	-55	0
0	1	19	0
0	0	0	5
1	6	69	1/8
0	4	56	-1/2
0	4	56	1/2
0	1	44	-1/8

~~~~~

forme de Frobenius de mat-6 , et matrice de passage.

|           |           |            |            |            |   |
|-----------|-----------|------------|------------|------------|---|
| 0         | 0         | 0          | 0          | 15         | 0 |
| 1         | 0         | 0          | 0          | -47        | 0 |
| 0         | 1         | 0          | 0          | 56         | 0 |
| 0         | 0         | 1          | 0          | -32        | 0 |
| 0         | 0         | 0          | 1          | 9          | 0 |
| 0         | 0         | 0          | 0          | 0          | 3 |
| 2175/53   | 37329/265 | 120051/265 | 308409/265 | 644331/265 | 0 |
| 2511/53   | 7533/53   | 22599/53   | 55701/53   | 111999/53  | 0 |
| 11211/265 | 30273/265 | 90147/265  | 224073/265 | 456507/265 | 0 |
| 7347/265  | 22041/265 | 68139/265  | 172161/265 | 357219/265 | 0 |
| 5163/265  | 15489/265 | 47811/265  | 121929/265 | 259611/265 | 0 |
| 2449/265  | 7347/265  | 22713/265  | 57387/265  | 119073/265 | 1 |

forme de Frobenius de  $\text{mat-10}$  , et matrice de passage.

|   |   |   |   |   |      |   |   |   |     |
|---|---|---|---|---|------|---|---|---|-----|
| 0 | 0 | 0 | 0 | 0 | -72  | 0 | 0 | 0 | 0   |
| 1 | 0 | 0 | 0 | 0 | 228  | 0 | 0 | 0 | 0   |
| 0 | 1 | 0 | 0 | 0 | -290 | 0 | 0 | 0 | 0   |
| 0 | 0 | 1 | 0 | 0 | 191  | 0 | 0 | 0 | 0   |
| 0 | 0 | 0 | 1 | 0 | -69  | 0 | 0 | 0 | 0   |
| 0 | 0 | 0 | 0 | 1 | 13   | 0 | 0 | 0 | 0   |
| 0 | 0 | 0 | 0 | 0 | 0    | 0 | 0 | 0 | -36 |
| 0 | 0 | 0 | 0 | 0 | 0    | 1 | 0 | 0 | 60  |
| 0 | 0 | 0 | 0 | 0 | 0    | 0 | 1 | 0 | -37 |
| 0 | 0 | 0 | 0 | 0 | 0    | 0 | 0 | 1 | 10  |

|    |    |     |     |     |      |     |      |      |       |
|----|----|-----|-----|-----|------|-----|------|------|-------|
| 36 | 52 | 68  | 72  | 32  | -124 | 2   | 2    | 0    | -8    |
| 0  | 0  | 0   | 0   | 0   | 8    | 0   | 0    | 0    | 0     |
| 4  | 20 | 60  | 152 | 352 | 780  | 2   | 6    | 16   | 40    |
| 0  | 24 | 88  | 240 | 576 | 1296 | 4   | 12   | 32   | 80    |
| 8  | 36 | 100 | 232 | 480 | 916  | 6   | 16   | 40   | 96    |
| 0  | 16 | 48  | 96  | 128 | 24   | 6   | 16   | 40   | 96    |
| 0  | 20 | 68  | 176 | 424 | 1076 | 7/2 | 19/2 | 47/2 | 111/2 |
| 0  | 24 | 88  | 256 | 720 | 2128 | 2   | 6    | 16   | 42    |
| 1  | 29 | 105 | 309 | 881 | 2613 | 3   | 9    | 25   | 69    |
| 0  | 28 | 104 | 308 | 880 | 2612 | 3   | 9    | 25   | 69    |

forme de Frobenius de mat-20.

|   |   |   |   |   |   |      |   |   |   |   |   |   |   |       |   |   |   |     |   |
|---|---|---|---|---|---|------|---|---|---|---|---|---|---|-------|---|---|---|-----|---|
| 0 | 0 | 0 | 0 | 0 | 0 | 72   | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0     | 0 | 0 | 0 | 0   | 0 |
| 1 | 0 | 0 | 0 | 0 | 0 | -300 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0     | 0 | 0 | 0 | 0   | 0 |
| 0 | 1 | 0 | 0 | 0 | 0 | 518  | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0     | 0 | 0 | 0 | 0   | 0 |
| 0 | 0 | 1 | 0 | 0 | 0 | -481 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0     | 0 | 0 | 0 | 0   | 0 |
| 0 | 0 | 0 | 1 | 0 | 0 | 260  | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0     | 0 | 0 | 0 | 0   | 0 |
| 0 | 0 | 0 | 0 | 1 | 0 | -82  | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0     | 0 | 0 | 0 | 0   | 0 |
| 0 | 0 | 0 | 0 | 0 | 1 | 14   | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0     | 0 | 0 | 0 | 0   | 0 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0    | 0 | 0 | 0 | 0 | 0 | 0 | 0 | -144  | 0 | 0 | 0 | 0   | 0 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0    | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 672   | 0 | 0 | 0 | 0   | 0 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0    | 0 | 1 | 0 | 0 | 0 | 0 | 0 | -1336 | 0 | 0 | 0 | 0   | 0 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0    | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 1480  | 0 | 0 | 0 | 0   | 0 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0    | 0 | 0 | 0 | 1 | 0 | 0 | 0 | -1001 | 0 | 0 | 0 | 0   | 0 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0    | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 424   | 0 | 0 | 0 | 0   | 0 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0    | 0 | 0 | 0 | 0 | 0 | 1 | 0 | -110  | 0 | 0 | 0 | 0   | 0 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0    | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 16    | 0 | 0 | 0 | 0   | 0 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0    | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0     | 0 | 0 | 0 | -4  | 0 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0    | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0     | 1 | 0 | 0 | 12  | 0 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0    | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0     | 0 | 1 | 0 | -13 | 0 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0    | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0     | 0 | 0 | 1 | 6   | 0 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0    | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0     | 0 | 0 | 0 | 0   | 1 |

Il nous semble sans interet de donner tous les coefficients de la matrice de passage. Signalons toutefois que la plupart d'entre eux sont entiers, et que les denominateurs des rationnels sont tous bornes par 125, les numerateurs etant bornes par 50000. Profitons de cet exemple pour dire une nouvelle fois, que nous commettons un abus en appelant cette matrice "forme de Frobenius". Les tailles des blocs  $F_i$  de cette matrice sont respectivement egales a 7,8,4,1. Donc les polynomes  $P_1$  et  $P_2$  associes aux blocs  $F_1$  et  $F_2$  ne verifient pas la relation " $P_2$  divise  $P_1$ ". Il s'agit donc d'une forme faible de Frobenius .

forme de Frobenius de mat1-20.

|   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |        |   |   |   |     |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|--------|---|---|---|-----|
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0      | 0 | 0 | 0 | 0   |
| 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0      | 0 | 0 | 0 | 0   |
| 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0      | 0 | 0 | 0 | 0   |
| 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 62500  | 0 | 0 | 0 | 0   |
| 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | -20000 | 0 | 0 | 0 | 0   |
| 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 2500   | 0 | 0 | 0 | 0   |
| 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | -62500 | 0 | 0 | 0 | 0   |
| 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 19900  | 0 | 0 | 0 | 0   |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | -2468  | 0 | 0 | 0 | 0   |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | 15621  | 0 | 0 | 0 | 0   |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | -4900  | 0 | 0 | 0 | 0   |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | 593    | 0 | 0 | 0 | 0   |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 4      | 0 | 0 | 0 | 0   |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | -25    | 0 | 0 | 0 | 0   |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 8      | 0 | 0 | 0 | 0   |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0      | 0 | 0 | 0 | 0   |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0      | 1 | 0 | 0 | 0   |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0      | 0 | 1 | 0 | -25 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0      | 0 | 0 | 1 | 8   |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0      | 0 | 0 | 0 | 0   |

Comme dans l'exemple precedent, nous ne donnerons pas tous les coefficients de la matrice de passage. Mais cette fois, la plupart des coefficients sont des nombres rationnels et il faut pour beaucoup d'entre eux environ 80 chiffres pour les représenter en base 10.

Arithmétique dans un corps  $F_p$  a  $p$  éléments, où  $p$  est un nombre premier.  
Tous les paramètres des procédures doivent être des petits entiers.

$!p$  est un petit entier inférieur ou égal à 185363.

```
(defun fp_fp (q)
  (prog (c)
    (setq c (\ q !p))
    (cond ((< c 0) (return (+ c !p)))
          (t (return c)))))
```

;; q un petit entier. Retourne q modulo  $!p$ .

~~~~~

```
(defun minusfp (q)
  (cond ((= q 0) 0)
        (t (- !p q))))
```

Calcule l'opposé de q modulo $!p$.

~~~~~

```
(defun plusfp (a b) (\ (+ a b) !p))
```

Calcule la somme de a et de b modulo  $!p$ .

~~~~~

```
(defun timesfp (a b) (\ (* a b) !p))
```

Calcule le produit de a et de b modulo $!p$.

~~~~~

```
(defun invfp (a)
  (prog (u1 u3 v1 v3 t1 t3 q)
    (setq u1 a u3 1 v1 !p v3 0 t1 0)
    (cond ((= a 0) (return nil)))
    e1
    (cond ((= t1 1) (return (fp_fp t3))))
    (setq q (/ u1 v1))
    (setq t3 (- u3 (* q v3)))
    (setq t1 (\ u1 v1))
    (setq u1 v1 u3 v3 v1 t1 v3 t3)
    (go e1)))
```

Calcule l'inverse de a modulo  $!p$ .

## Arithmetique dans le corps des rationnels .

Les nombres rationnels sont representes par des listes de deux entiers (p . q) ou p et q designe respectivement le numerateur et le denominateur. De plus , q sera un entier strictement positif.

```
(defun q_q (q)
  (cond ((numberp q) (cons q 1))
        (t q)))
```

Transforme un entier q en une liste ( q . 1 ) , et laisse invariant un rationnel represente par une liste ( a . b ) .

```
~~~~~
(defun nq (a)
 (prog (c1 c2 c3)
 (cond ((eq (car a) 0) (return (cons 0 1))))
 (setq c1 (gcd (car a) (cdr a)))
 (setq c2 (quotient (car a) c1))
 (setq c3 (quotient (cdr a) c1))
 (cond ((plusp c3) (return (cons c2 c3))))
 (return (cons (minus c2) (minus c3)))))
```

Si a = ( p . q ) represente un rationnel , nq(a) retourne une liste (p' . q') representant aussi a mais avec p' et q' premiers entre eux, et q' > 0 .

```
~~~~~
(defun minusq (a) (cons (minus (car a)) (cdr a)))
```

Calcule l'oppose d'un nombre rationnel.

```
~~~~~
(defun plusq (a b)
 (nq (cons (plus (times (car a) (cdr b)) (times (cdr a) (car b)))
 (times (cdr a) (cdr b)))))
```

Calcule la somme de deux rationnels.

```
~~~~~
(defun timesq (a b)
  (nq (cons (times (car a) (car b)) (times (cdr a) (cdr b)))))
```

Calcule le produit de deux rationnels.

```
~~~~~
(defun invq (a)
 (cond ((eq (car a) 0) nil)
 ((plusp (car a)) (cons (cdr a) (car a)))
 (t (cons (minus (cdr a)) (minus (car a))))))
```

Calcule l'inverse d'un nombre rationnel.





## **Chapitre III**

Deuxième algorithme pour le calcul de la forme de  
Frobenius d'une matrice .

### III.1. Introduction

Nous avons remarqué dans le chapitre II, que le premier algorithme pouvait produire dans le cas  $K = \mathbb{Q}$ , une matrice de passage ayant des coefficients rationnels formés par des entiers "très grands" (voir les exemples mat-6 et mat1-20).

La matrice de passage n'étant pas unique, on peut essayer de rechercher une matrice dont les coefficients sont "les plus petits possible". Nous ne sommes pas parvenu à trouver un algorithme qui fournisse chaque fois une matrice de passage "idéale". Cependant, nous pensons que le nouvel algorithme que nous présentons dans ce chapitre constitue un progrès par rapport au précédent.

Nous donnerons d'ailleurs une borne pour majorer tous les entiers intervenant en cours de calcul, et ce résultat nous permettra de conclure que cet algorithme est polynomial en  $O(n^8 \log^2 \|A\|)$ .

De plus on peut rappeler une nouvelle fois, que le premier algorithme ne donne pas toujours la forme de Frobenius de  $A$  mais une forme faible de Frobenius, c'est à dire une matrice bloc-diagonale  $F = \text{diag}(F_1, \dots, F_k)$  où les  $F_i$  sont des matrices compagnons, mais dont les polynômes associés  $P_1, \dots, P_k$  ne vérifient pas forcément la relation de divisibilité  $P_k \mid \dots \mid P_2 \mid P_1$ . Le deuxième algorithme fournira exactement la forme de Frobenius.

Si le premier algorithme consiste à exécuter une suite de transformations élémentaires pour parvenir à une forme de Frobenius, le deuxième algorithme trouve une explication plus géométrique.

En effet, supposons connue une matrice de passage  $P$ . Notons  $d_i$  la dimension de  $F_i$ ;  $s_i = d_1 + \dots + d_i$  et  $s_0 = 0$ ;  $f_i$  le vecteur représenté par la  $(s_{i-1} + 1)$ ème colonne de  $P$ . Notons enfin  $\mathcal{V}_i = (f_1, \dots, f_i)_A$  le sous espace vectoriel engendré par les vecteurs  $f_i$  (au sens des modules),  $\mathcal{V}_0 = \{0\}$ . Les sous espaces vectoriels  $\mathcal{V}_i$  sont stables par  $A$ , et on appelle  $A_i$  l'endomorphisme de l'espace quotient  $\mathcal{V}_i / \mathcal{V}_{i-1}$  induit par  $A$  (cette notion sera développée dans III.5.c et III.5.d).

Si  $F = \text{diag}(F_1, \dots, F_k)$  est la forme de Frobenius de  $A$ , alors les vecteurs  $f_i$  vérifient la propriété suivante :

$$(\mathcal{P}) \quad \left\{ \begin{array}{l} \pi_{f_i} = \pi_{A_{i-1}} \quad \text{pour tout } i \in \{1, \dots, k\} \\ \text{où } \pi_{f_i} \text{ est le polynôme minimal de } f_i \text{ modulo } \mathcal{V}_{i-1} \\ \text{et } \pi_{A_{i-1}} \text{ le polynôme minimal de } A_{i-1} \end{array} \right.$$

Compte tenu de cette remarque , nous avons construit un algorithme qui comporte deux étapes :

1) (procédure "forminterm" )

Rechercher des vecteurs  $f_1, \dots, f_k$  vérifiant la propriété (  $\mathfrak{P}$  ). Ces vecteurs seront donnés par la procédure "veminimax" ( III.4.b ).

Si nous considérons la matrice  $P_1$  dont les colonnes sont formées par les composantes des vecteurs

$$(f_1, \dots, A^{d_1-1}(f_1), f_2, \dots, f_k, \dots, A^{d_k-1}(f_k))$$

alors la matrice  $H = P_1^{-1} A P_1$  , appelée forme intermédiaire , est de la forme ci-dessous :

Diagram illustrating a block upper triangular matrix structure  $H$ . The matrix is partitioned into blocks along its main diagonal. The diagonal blocks are labeled  $H_1$ ,  $H_2$ , ...,  $H_k$ . The blocks above the diagonal are labeled 0. The matrix is shown as a large square with a smaller square block  $H_1$  in the top-left, a smaller square block  $H_2$  in the middle-right, and a small square block  $H_k$  in the bottom-right. The blocks are connected by dotted lines, indicating a sequence of blocks. The matrix is labeled  $H =$  on the left.

Les blocs  $H_i$  sont des matrices compagnons et les  $*$  situées dans les colonnes  $d_1 + d_2$ ,  $d_1 + d_2 + d_3$ , ...,  $d_1 + \dots + d_k$  représentent des éléments quelconques du corps  $\mathbb{K}$ .

2) ( procédure "zeroadroites" )

Annuler les termes situés dans la partie supérieure de la matrice  $H$  en utilisant  $k - 1$  fois la procédure "zeroadroite" ( II.4 ) ; les blocs  $H_i$  étant conservés . Nous obtiendrons alors une matrice  $P_2$  inversible telle que :

$$H P_2 = P_2 H_d \quad \text{avec} \quad H_d = \text{diag} (H_1, \dots, H_k) .$$

La matrice  $H_d$  est à priori une forme faible de Frobenius .

Le théorème 1 , que nous démontrerons dans le paragraphe III . 5 . , montre l'intérêt de cette construction .

*Théorème 1 :* *la matrice  $H_d$  est la forme de Frobenius de  $A$  .*

Les prochains paragraphes présentent les outils nécessaires pour construire la forme intermédiaire  $H$  .

- calcul du polynôme minimal d'un vecteur ( III.2. ) .
- calcul du polynôme minimal d'un endomorphisme ( III.3. ) .
- recherche d'un vecteur dont le degré du polynôme minimal est maximal . ( III.4. ) .

### III . 2 Polynôme minimal d'un vecteur.

Nous avons étudié dans le paragraphe II.3. la procédure "polymine1" qui donne , entre autre , le polynôme minimal du vecteur  $e_1$  .

Une légère modification nous permet de calculer le polynôme minimal d'un vecteur  $e = b_r e_r + \dots + b_n e_n$  . Il suffit pour cela , avant d'appeler la procédure "polymine1" , de faire les transformations suivantes:

- 1)  $P_{1,r}$
- 2)  $M_{1, \frac{1}{b_r}}$
- 3)  $C_{1, b_j, j}$  pour  $j = r + 1$  à  $n$

Les notations sont celles du II.2. Ainsi on trouve dans la première colonne de la matrice de passage  $P$  les composantes du vecteur  $e$  . Nous avons appelé cette procédure "polymine" . La matrice est transformée , comme le fait "polymine1" , en une matrice de la forme:

$$(1) \quad \begin{pmatrix} & C_1 & & B_1 \\ & & & \\ 0 & & 0 & \\ & & & B_2 \\ 0 & & 0 & \end{pmatrix}$$

Avant d'écrire la procédure "polymine" , nous donnons la procédure "polyassbloc" , utilisée pour obtenir le polynôme  $P$  associé à un bloc compagnon .

*procedure polyassbloc* (  $B, k, j$  ) ;

entrées :  $B$  une matrice contenant un bloc compagnon , les  
coefficients de  $P$  se trouvant colonne  $j$  , lignes  $k$  à  $j$  .  
sortie : le polynôme  $P$  .

*begin*

$P := X^{(j-k+1)}$  ;  
*for*  $i = k$  *to*  $j$  *do*  $P := P - b(i, j) * X^{(i-k)}$  ;  
*return*  $P$  ;

*end* ;

*procedure polymine* (  $B, e$  ) ;

entrées :  $B$  une matrice d'ordre  $n$  , et  $e$  un vecteur  
 $e = b_r e_r + \dots + b_n e_n$  avec  $b_r \neq 0$  .  
sortie : le polynôme minimal  $\pi_e$  de  $e$  .  
effet : transforme la matrice  $B$  en une matrice de la forme ( 1 )

*begin*

*if*  $r \neq 1$  *then*  $P_{1,r}$  ;

$M_{1, \frac{1}{b_r}}$  ;

*for*  $j = r + 1$  *to*  $n$  *do*  $C_{1, b_j, j}$  ;

$d = \text{polymine1}(B, 1)$  ;

*return*  $\text{polyassbloc}(B, 1, d)$  ;

*end* ;

### Exemple 1 :

Prenons comme matrice  $B$  la matrice  $\text{mat-10}$ , et comme vecteur  $e$  le vecteur  $e_1 + e_4 + e_{10}$ . Nous donnons à la fin de ce chapitre, la matrice transformée par "polymine" ainsi que la matrice de passage. Remarquons que la dimension du bloc  $C_1$  est égal à 6.

## III.3 Polynôme minimal d'un ensemble de vecteurs.

### III.3.a Polynôme minimal d'un s.e.v. $\mathcal{V} \neq \{0\}$ .

C'est le polynôme unitaire  $\pi_{\mathcal{V}}$  de plus bas degré tel que  $\pi_{\mathcal{V}}(g) = 0 \quad \forall g \in \mathcal{V}$ .

Autrement dit, si l'on considère l'ensemble  $\mathcal{J}$ , des polynômes  $\pi$  tels que  $\pi(g) = 0 \quad \forall g \in \mathcal{V}$ ,  $\mathcal{J}$  est un idéal de  $\mathbb{K}[X]$ . Comme  $\mathbb{K}[X]$  est un anneau principal,  $\mathcal{J}$  est un idéal principal et  $\pi_{\mathcal{V}}$  est le polynôme unitaire engendrant  $\mathcal{J}$ .

Remarque : il existe  $(g_1, \dots, g_r)$  une partie génératrice de  $\mathcal{V}$ , et si  $\pi = \text{ppcm}(\pi_{g_1}, \dots, \pi_{g_r})$  alors  $\pi(g) = 0 \quad \forall g \in \mathcal{V}$ ; donc  $\pi \in \mathcal{J}$  et  $\pi_{\mathcal{V}}$  est un diviseur de  $\pi$ . En fait  $\pi = \pi_{\mathcal{V}}$ , car  $\pi_{\mathcal{V}}(g_i) = 0$  donc  $\pi_{\mathcal{V}}$  est un multiple de  $\pi_{g_i}$  et par suite un multiple de  $\pi$ .

### III.3.b Cas où $\mathcal{E} = \mathcal{V}$

Dans le cas où  $\mathcal{V} = \mathcal{E}$  l'espace tout entier, le polynôme minimal  $\Pi_{\mathcal{E}}$  est encore appelé polynôme minimal de l'endomorphisme  $A$ , et noté  $\Pi_A$ .

Nous cherchons un algorithme pour trouver le polynôme minimal de  $\mathcal{E}$ . Puisque  $(e_1, \dots, e_n)$  engendre  $\mathcal{E}$ , on peut penser à l'algorithme suivant :

$$(1) \quad \begin{array}{ll} B_1 & \text{pour } i=1 \text{ à } n \quad \text{calculer } \pi_{e_i} \\ B_2 & \Pi_{\mathcal{E}} = \text{ppcm}(\pi_{e_i}) \\ & i=1, \dots, n \end{array}$$

Mais on peut en général éviter de calculer tous les  $\pi_{e_i}$ , en utilisant les deux théorèmes suivants:

**Théorème 1 :**

*Le degré du polynôme minimal d'un vecteur est inférieur ou égal à  $n$ .*

Par conséquent, dans la boucle  $B_1$  on peut s'arrêter si  $\deg \pi_{e_i} = n$ , et en déduire immédiatement  $\Pi_{\mathfrak{z}} = \pi_{e_i}$ .

**Théorème 2 :** si  $(f_1, \dots, f_r)_A = \mathfrak{y}$  alors  $\pi_{\mathfrak{y}} = \text{ppcm}(\pi_{f_i})_{i=1, \dots, r}$

Dans ce théorème  $\mathfrak{y}$  est le sous espace engendré par  $f_1, \dots, f_r$  au sens des modules, c'est à dire  $\mathfrak{y} = \{ \alpha_1 f_1 + \dots + \alpha_r f_r \text{ avec } \alpha_i \in K[X] \}$ .

démonstration: Par définition on a  $\pi_{\mathfrak{y}}(f_i) = 0 \quad \forall i = 1, \dots, r$   
 donc  $\pi_{\mathfrak{y}}$  est un multiple de  $\pi_{f_i} \quad \forall i = 1, \dots, r$   
 et  $\pi_{\mathfrak{y}}$  est un multiple de  $\pi = \text{ppcm}(\pi_{f_i})_{i=1, \dots, r}$

D'autre part si  $\pi = \text{ppcm}(\pi_{f_i})_{i=1, \dots, r}$  et  $f \in \mathfrak{y}$  alors

$$f = \alpha_1 f_1 + \dots + \alpha_r f_r \quad \text{avec} \quad \alpha_i \in K[X].$$

$$\pi(f) = \sum_{i=1}^r \pi(\alpha_i f_i) = \sum_{i=1}^r (\pi \alpha_i)(f_i) = \sum_{i=1}^r \alpha_i (\pi(f_i)) = 0$$

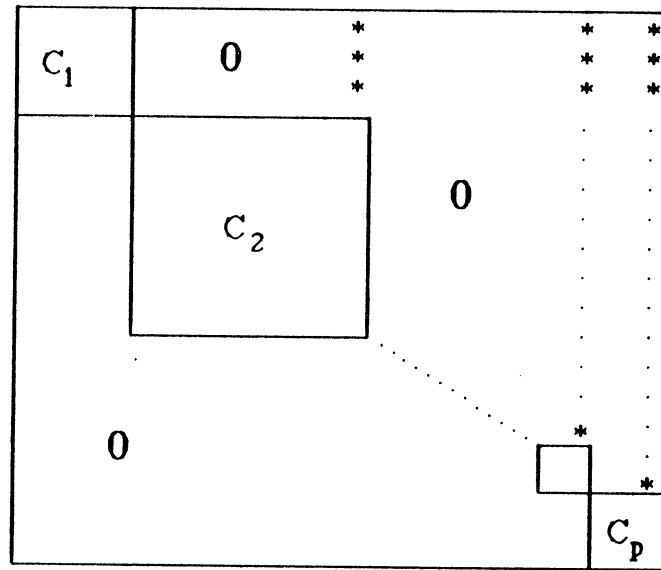
c.q.f.d.

Nous voyons maintenant, que dans l'algorithme (1), il est souvent inutile de calculer les polynômes minimaux de tous les vecteurs  $e_i \quad i=1, \dots, n$  et qu'il suffit de calculer les polynômes minimaux des éléments d'une sous famille  $f_i \quad i=1, \dots, r$  telle que  $(f_1, \dots, f_r)_A = \mathfrak{z}$ .

Mais comment extraire de l'ensemble  $\{e_1, \dots, e_n\}$  un sous ensemble  $\{f_1, \dots, f_r\}$  tel que  $(f_1, \dots, f_r)_A = \mathfrak{z}$  ?

On peut y parvenir en utilisant la procédure "extgen" décrite ci-dessous. La matrice sera transformée en une matrice  $B$  de la forme:





les matrices  $C_i$  étant des matrices compagnons de taille  $t_i$ .

Les colonnes de la matrice de passage sont formées par les composantes des vecteurs  $f_1, A(f_1), \dots, A^{t_1-1}(f_1), f_2, \dots, A^{t_p-1}(f_p)$  où les  $f_i \in \{e_1, \dots, e_n\}$ .

Remarque :

Puisque les  $f_i$  sont choisis parmi les éléments de la base canonique  $\{e_1, \dots, e_n\}$ , il est inutile de calculer la matrice de passage, il suffit de repérer les permutations effectuées sur les colonnes et la taille de chaque bloc  $C_i$  pour connaître tous les  $f_i$ . Pour cela, on modifie légèrement la procédure "polymine1". On initialise un tableau "pas" de dimension  $n$ ,  $\text{pas}(i) = i$  pour  $i = 1$  à  $n$ , puis on effectue sur "pas" les mêmes permutations que sur les colonnes de la matrice elle-même.

*procedure* **polymine1** ( B , j , pas ) ;

entrées : une matrice B d'ordre n , j un entier  $j \leq n$  et "pas"  
un tableau de dimension n , avec  $\text{pas}(i) = i$   $i = 1$  à n.  
sortie : l'entier d ( égal à l'ordre de la matrice compagne  $C_1$  )  
effet : transforme la matrice B en une matrice de la forme (1) .

*begin*

k := **chercheli** ( B , j ) ;

*while*  $k \leq n$  *do*

*begin*

*if*  $k \neq j+1$  *then*

*begin*

$P_{k,j+1}$  ;

pe := **pas**( j+1 ) ; **pas** ( j+1 ) := **pas**(k) ;

**pas**(k) := pe ;

*end;*

$M_{j+1, \frac{1}{b_{j+1,j}}}$  ; ( ainsi  $b_{j+1,j} = 1$  )

*for*  $i=1$  *to* n *do*

*if*  $i \neq j+1$  *then*  $L_{i,-b_{i,j},j+1}$  ( ainsi  $b_{i,j} = 0$  si  $i \neq j+1$  )

j = j+1 ;

k = **chercheli** ( B , j ) ;

*end;*

d := j

*return* d ;

*end;*

*Procedure extgen* ( B , pasb )

entrées : B une matrice d'ordre  $n$  , et pasb un tableau de dimension  $n$  avec  $\text{pasb}(i) = i$  .

effet : transforme B en une matrice de la forme décrite ci-dessus.  
Deux tableaux de dimension  $n$  , "tbl" et "famgen" sont utilisés pour avoir des renseignements complémentaires sur les blocs  $C_i$  .  $\text{tbl}(i)$  est l'indice de la dernière colonne du bloc  $C_i$  ;  $\text{famgen}(i)$  est l'indice  $k_i$  du vecteur  $e_k$  représenté dans la matrice de passage , par la première colonne du bloc  $C_i$  . On en déduit ainsi une famille  $(e_{k_1}, \dots, e_{k_p})$  telle que  $(e_{k_1}, \dots, e_{k_p})_{\Lambda} = \mathbb{I}$  .  
 $\text{famgen}(0) = p$  le nombre de blocs  $C_i$  .

*begin*

$k := 1$  ;  $h := 1$  ;  $\text{famgen}(1) := 1$  ;

*while*  $k \leq n$  *do*

*begin*

$d := \text{polymine1}(B, k, \text{pasb})$  ;

$\text{tbl}(h) := d$  ;

$k := d + 1$  ;  $h := h + 1$  ;

*end* ;

*for*  $i = 2$  *to*  $h - 1$  *do*  $\text{famgen}(i) = \text{pasb}(\text{tbl}(i - 1) + 1)$  ;

$\text{famgen}(0) = h - 1$  ;

*end* ;

### Exemple 2 :

Prenons à nouveau pour  $B$  la matrice  $\text{mat-10}$ . Nous donnons à la fin de ce chapitre, la transformée de la matrice  $B$  par "extgen" ainsi que la matrice de passage. Nous avons aussi  $\text{pasb}(i) = i$  pour  $i = 1$  à  $10$ , et  $\text{famgen}(0) = 6$ .

Les tableaux "tbl" et "famgen" contiennent les valeurs suivantes :

|                      |    |                         |
|----------------------|----|-------------------------|
| $\text{tbl}(1) = 2$  | et | $\text{famgen}(1) = 1$  |
| $\text{tbl}(2) = 3$  | et | $\text{famgen}(2) = 3$  |
| $\text{tbl}(3) = 5$  | et | $\text{famgen}(3) = 4$  |
| $\text{tbl}(4) = 7$  | et | $\text{famgen}(4) = 6$  |
| $\text{tbl}(5) = 9$  | et | $\text{famgen}(5) = 8$  |
| $\text{tbl}(6) = 10$ | et | $\text{famgen}(6) = 10$ |

Nous pouvons aussi en déduire le polynôme minimal

$$\pi_{e_1} = X^2 - 4X + 4$$

De plus, nous avons les égalités suivantes :

$$\begin{aligned} \dim(e_1, e_3)_A &= 3 ; \dim(e_1, e_3, e_4)_A = 5 ; \dim(e_1, e_3, e_4, e_6)_A = 7 \\ \dim(e_1, e_3, e_4, e_6, e_8)_A &= 9 \quad \text{et} \quad \dim(e_1, e_3, e_4, e_6, e_8, e_{10})_A = 10. \end{aligned}$$

### Complexité :

Si on suppose que la matrice transformée par "extgen" contient  $p$  blocs, il faut au plus  $n - p$  transformations du type  $M_{i,a}$ , et au plus  $(n - 1)(n - p)$  transformations du type  $L_{i,a,j}$ ; ce qui donne :

- $n - p$  calculs d'inverses.
- $2n(n - 1)(n - p)$  multiplications et additions.

Terminons ce paragraphe sur le calcul de polynômes minimaux , en donnant la procédure "polymina" qui calcule le polynôme minimal d'une matrice  $A$  . Cette procédure retourne le polynôme "pp" égal à  $\Pi_A$  . Mais elle donne également des renseignements complémentaires qui nous seront utiles par la suite .

On appelle d'abord "extgen" pour obtenir la famille  $(e_{k_1}, \dots, e_{k_p})$  telle que  $(e_{k_1}, \dots, e_{k_p})_A = \mathfrak{z}$ . Le polynôme  $\pi_{e_{k_1}}$  est donné directement par "extgen" , puis on calcule les polynômes  $\pi_{e_{k_i}}$  dans l'ordre décroissant de  $i = p$  à 2.

On en déduit alors une sous-famille  $(e_{h_1}, \dots, e_{h_s})$  telle que  $\text{ppcm}(e_{h_1}, \dots, e_{h_s}) = \Pi_A$  , ainsi que la suite des polynômes

$$\pi_{e_{h_1}} ; \quad \text{ppcm}(\pi_{e_{h_1}}, \pi_{e_{h_2}}) ; \quad \dots ; \quad \text{ppcm}(\pi_{e_{h_1}}, \dots, \pi_{e_{h_s}})$$

dont les degrés sont strictement croissants .

Les entiers  $h_i$  sont stockés dans le tableau "fam" ( $\text{fam}(i) = h_i$ ) et les polynômes dans le tableau "poly" ( $\text{poly}(i) = \text{ppcm}(\pi_{e_{h_1}}, \dots, \pi_{e_{h_i}})$ ) .

La variable "nbpo" est le nombre de polynômes minimaux restant à calculer, et "dim" est la dimension de l'espace vectoriel  $(e_{k_1}, \dots, e_{k_i})_A$  , connue par "extgen" ( voir exemple 2 , paragraphe III. 3.b ) . Elle est utilisée dans un test d'arrêt car si le degré de  $\pi_{e_{k_i}}$  est égal à "dim" il est inutile de poursuivre les calculs .

Avant d'appeler "polymina" , on déclare un tableau  $B$  de dimension  $n \times n$  , et des tableaux "pasb" , "tbl" , "famgen" , "fam" , "poly" de dimension  $n$  . Le tableau "pasb" doit être initialisé :  $\text{pasb}(i) = i$  pour  $i = 1$  à  $n$  .

*procedure* **polymina** ( A ) ;

entrées : une matrice A d'ordre n .  
effets : voir commentaires précédents .  
sortie : le polynôme minimal de A .

*begin*

copymat ( A , B ) ;

extgen ( B , pasb ) ; nbpo := famgen ( 0 ) ;

pp := polyassbloc ( B , 1 , tbl ( 1 ) ) ;

s := 1 ; poly ( 1 ) := pp ; fam ( 1 ) := famgen ( 1 ) ;

p := pp ; dim := n ;

*while* ( nbpo > 1 and deg ( pp ) < n and deg ( p ) < dim )

*begin*

copymat ( A , B ) ;

k := famgen ( nbpo ) ;

p := polymine ( B , e<sub>k</sub> ) ;

g := pgcd ( p , pp ) ;

*if* deg ( g ) < deg ( pp ) *then*

*begin*

pp := pp \* ( p / g ) ;

s := s + 1 ; fam ( s ) := k ; poly ( s ) := pp ;

*end;*

dim :=tbl ( nbpo ) ; nbpo = nbpo - 1 ;

*end;*

fam ( 0 ) := s ; *return* pp ;

*end;*

Afin de mieux comprendre cette procédure , nous donnons la trace du calcul lorsque la matrice  $A$  est la matrice mat-10 .

```

copymat (A , B) % les calculs se font sur B afin de sauvegarder A %
extgen (B , pasb) % déjà expliquée page 64 %
nbpo = 6
pp = X2 - 4 X + 4 % c'est le polynôme minimal de e1 , πe1 %
p = pp ; dim = 10

```

% on entre dans la boucle %

```

k = 10
p = X3 - 7 X2 + 15 X - 9 % p = πe10 %
g = 1
% la condition deg (g) < deg (p) est satisfaite . %

```

```

pp = X5 - 11 X4 + 47 X3 - 97 X2 + 96 X - 36
s = 2 ; fam (2) = 10 ; poly (2) = pp ;
dim = 10 ; nbpo = 5

```

% nouvelle itération %

```

k = 8
p = X2 - 6 X + 9 % p = πe8 %
g = X2 - 6 X + 9
% la condition deg (g) < deg (p) n'est pas satisfaite . %
dim = 9 ; nbpo = 4

```

% nouvelle itération %

```

k = 6
p = X4 - 10 X3 + 37 X2 - 60 X + 36 % p = πe6 %
g = X4 - 10 X3 + 37 X2 - 60 X + 36
% la condition deg (g) < deg (p) n'est pas satisfaite . %
dim = 7 ; nbpo = 3

```

% nouvelle itération %

```

k = 4
p = X3 - 6 X2 + 12 X - 8 % p = πe4 %
g = X2 - 4 X + 4

```

% la condition  $\deg(g) < \deg(p)$  est satisfaite . %

$$pp = X^6 - 13 X^5 + 69 X^4 - 191 X^3 + 290 X^2 - 228 X + 72$$

$$s = 3 ; \text{fam}(s) = 4 ; \text{poly}(s) = pp$$

$$\text{dim} = 5 ; \text{nbpo} = 2$$

% nouvelle itération %

$$k = 3$$

$$p = X^3 - 6 X^2 + 12 X - 8$$

$$\% p = \pi_{e_3} \%$$

$$g = X^3 - 6 X^2 + 12 X - 8$$

% la condition  $\deg(g) < \deg(p)$  n'est pas satisfaite . %

$$\text{dim} = 3 ; \text{nbpo} = 1$$

% fin de la boucle %

$$\text{fam}(0) = 3$$

Nous obtenons alors deux résultats importants :

$$- \Pi_A = X^6 - 13 X^5 + 69 X^4 - 191 X^3 + 290 X^2 - 228 X + 72$$

$$- \Pi_A = \text{ppcm}(\pi_{e_1}, \pi_{e_{10}}, \pi_{e_4}).$$

### Complexité:

Supposons que le degré du polynôme minimal de  $A$  soit égal à  $d$  ; les degrés des polynômes rencontrés dans cette procédure sont inférieurs ou égaux à  $d$ . On suppose de plus que la procédure "extgen" donne  $k$  blocs .

La procédure "extgen" coûte au plus :

$$n - k \quad \text{calculs d'inverses}$$

$$2n^2(n - k) \quad \text{multiplications et additions}$$

Nous effectuons ensuite au plus  $k - 1$  itérations , chacune d'elles demandent:

pour "polymine" :

$$d - 1 \quad \text{calculs d'inverses}$$

$$2n^2(d - 1) \quad \text{multiplications et additions}$$



pour le calcul  $\text{pgcd}(g, p)$  ;

$2d$  calculs d'inverses

$d(d+1)$  multiplications et additions

pour le calcul de  $pp * (p/g)$  :

$d+1$  calculs d'inverses

$2d(d+1)$  multiplications et additions

### Conclusion :

L'algorithme que nous utilisons pour calculer le polynôme minimal d'une matrice demande :

$4nd$  calculs d'inverses

$2n^3d$  multiplications et additions

## III.4 Recherche d'un vecteur dont le degré du polynôme minimal est maximal.

### III.4.a Présentation du problème et théorème.

Nous nous intéressons au problème suivant :

Etant donné  $\gamma$  un s.e.v. de  $\mathfrak{z}$  ; existe-t-il un vecteur  $E$  tel que  $\pi_E = \pi_\gamma$  ; si oui , déterminer une méthode pour trouver un tel vecteur.

On trouvera une démonstration de l'existence ainsi qu'une méthode pour déterminer un tel vecteur  $E$  dans [ Jacobson , 1953 ] . Toutefois , nous exposons dans cette partie , un autre algorithme qui aura l'avantage de donner un vecteur  $E$  dont toutes les composantes seront majorées par l'entier  $n$  , égal à la dimension de  $\mathfrak{z}$  .

Nous commençons par étudier le cas où  $\gamma = (e, f)_A$  .

Soit  $\mathcal{V} \neq \{0\}$  un s.e.v., on peut factoriser  $\pi_{\mathcal{V}}$  de la façon suivante:

$$\pi_{\mathcal{V}} = R_1^{d_1} \cdot \dots \cdot R_k^{d_k} \quad \text{où les } R_i \text{ sont irréductibles et premiers entre eux.}$$

Notons alors pour  $i = 1$  à  $k$

$$V_i = \text{Ker} \left( \frac{\pi_{\mathcal{V}}}{R_i} \right)$$

$\frac{\pi_{\mathcal{V}}}{R_i}$  est un polynôme où l'on a remplacé la variable  $X$  par l'endomorphisme  $A$ .

**Théorème** : Si  $\mathfrak{d}$  est une droite affine de  $\mathcal{V}$ , alors deux possibilités:

- il existe  $i \in \{1, \dots, k\}$  tel que  $\mathfrak{d} \subset V_i$
- $\mathfrak{d} \cap (\cup V_i)$  est un ensemble fini de points dont le cardinal est inférieur ou égal à  $k$ .

**démonstration** :  $\mathfrak{d} \cap (\cup V_i) = \cup (\mathfrak{d} \cap V_i)$

or  $\mathfrak{d} \cap V_i$  est soit  $\mathfrak{d}$  si  $\mathfrak{d} \subset V_i$ , soit un point  $a_i$ , soit l'ensemble vide.

finalement soit  $\exists i \in \{1, \dots, k\}$  tel que  $\mathfrak{d} \subset V_i$

soit  $\forall i$   $\mathfrak{d} \cap V_i$  contient au plus un point. c.q.f.d.

**Corollaire.** Soient  $e$  et  $f$  deux vecteurs non nuls,  $\pi_e$  et  $\pi_f$  leurs polynômes minimaux, et supposons de plus que la caractéristique de  $\mathbb{K}$  soit supérieure strictement à  $k$ , alors il existe  $j \in \{1, \dots, k\}$  tel que le polynôme minimal de  $e + jf$  soit égal au ppcm  $(\pi_e, \pi_f)$ .

**démonstration** :

Appelons  $\mathfrak{d}$  la droite affine  $e + \lambda f$ ,  $\lambda \in \mathbb{K}$ ; et  $\mathcal{V} = (e, f)_A$ .

Nous avons  $\forall i \in \{1, \dots, k\}$   $V_i \not\subset \mathcal{V}$  car le polynôme minimal de  $V_i$  divise strictement celui de  $\mathcal{V}$ .

Montrons par l'absurde que la droite affine  $\mathfrak{d}$  n'est incluse dans aucun  $V_i$ .

Supposons  $\mathfrak{d} \subset V_i$  alors  $e \in V_i$  ( $\lambda = 0$ )

$$e + f \in V_i \quad (\lambda = 1)$$

et donc  $f \in V_i$

Les  $V_i$  étant des sous espaces stables par  $A$  on a  $\mathcal{V} = (e, f)_A \subseteq V_i$  ce qui est en contradiction avec  $V_i \not\subseteq \mathcal{V}$ .

Comme  $\mathcal{D}$  n'est incluse dans aucun des  $V_i$ , le cardinal de  $\mathcal{D} \cap (\cup V_i)$  est inférieur ou égal à  $k$  (théorème ci-dessus). Or si  $\pi_{e+jf}$  est différent de  $\pi_{\mathcal{V}}$  alors c'est un diviseur strict de  $\pi_{\mathcal{V}}$  et  $e + j f$  appartient à l'un des  $V_i$ . Par ailleurs, l'ensemble des points  $\{e + j f ; j = 0, \dots, k\}$  a  $k + 1$  éléments distincts (car nous avons fait l'hypothèse: caractéristique  $\mathbb{K} > k$ ) et ne peut être inclus dans l'ensemble  $\mathcal{D} \cap (\cup V_i)$  qui a  $k$  éléments au plus.

### III.4.b Les procédures veminimax.

Les procédures "veminimax2" et "veminimax" décrites ci-dessous, calculent un vecteur  $E$  de  $\mathcal{V}$  tel que  $\pi_E = \pi_{\mathcal{V}}$ , et dont les composantes sont des entiers compris entre 0 et  $n$ . "veminimax2" traite le cas  $\mathcal{V} = (e, f)_A$ , et "veminimax" le cas général.

*Procedure veminimax2* ( $A, e, f, \pi$ );

entrées :  $A$  une matrice d'ordre  $n$ ,  $e$  et  $f$  deux vecteurs  
et  $\pi = \text{ppcm}(\pi_e, \pi_f)$ . Nous supposons de plus que  
 $\pi_e$  divise strictement  $\pi$ .

sortie : un vecteur de la forme  $e + k f$  tel que  $\pi_{e+kf} = \pi$ .

*begin*

-  $k = 0$

- *repeat*

*begin*

-  $k = k + 1$ ;

- *copymat* ( $A, B$ );

-  $\pi_{e+kf} = \text{polymine}(B, e + k f)$ ;

*end*

*until*  $\pi_{e+kf} = \pi$ ;

- *return*  $e + k f$ ;

*end*;

complexité :

Le nombre d'itérations est borné par  $\deg(\pi) - \deg(\pi_e) + 1$ .

En effet  $\pi_r = R_1^{d_1} \cdot \dots \cdot R_k^{d_k}$  ;  $\pi_e = R_1^{e_1} \cdot \dots \cdot R_k^{e_k}$

Notons  $A_e = \{ j / e_j < d_j \}$  et  $n_e$  le cardinal de  $A_e$ .

Si  $j \in A_e$  alors  $e \in V_j$ , donc  $\Phi \cap (\cup V_i)$  a au plus  $k - n_e + 1$  éléments, et  $k - n_e \leq \deg(\pi) - \deg(\pi_e)$ .

conclusion :

la procédure "veminimax2" demande au plus :

$2n^2 (d - 1) * (\deg(\pi) - \deg(\pi_e) + 1)$  additions et multiplications.

La procédure "polymina" nous donne une liste de vecteurs  $e_{h_1}, \dots, e_{h_s}$  tels que  $\text{ppcm}(e_{h_1}, \dots, e_{h_s}) = \Pi_A$ . Nous allons chercher un vecteur  $E$  tel que  $\pi_E = \pi_A$ , parmi les vecteurs de la forme  $E = e_{h_1} + j_2 e_{h_2} + \dots + j_s e_{h_s}$ .

*Procedure* **veminimax** ( A , s ) ;

entrées : une matrice A d'ordre n , et s un entier .

On suppose que l'on a déjà appelé "polymina" ,

et donc que la famille  $e_{h_1}, \dots, e_{h_s}$  est connue , et que

$\pi_A$  est stocké dans poly ( s ) .

sortie : un vecteur de la forme  $E = e_{h_1} + j_2 e_{h_2} + \dots + j_s e_{h_s}$

tel que  $\pi_E = \pi_A$  .

*begin*

- if s = 1 then return  $e_{h_1}$  ;

- if s = 2 then return veminimax2 ( A ,  $e_{h_1}$  ,  $e_{h_2}$  , poly ( 2 ) ) ;

- copymat ( A , B ) ;

-  $\pi = \text{polymine} ( B , e_{h_1} + e_{h_2} + \dots + e_{h_s} )$  ;

- if  $\pi = \text{poly} ( s )$  then return  $e_{h_1} + e_{h_2} + \dots + e_{h_s}$  ;

-  $\pi = \text{veminimax} ( A , s - 1 )$  ;

- veminimax2 ( A ,  $\pi$  ,  $e_{h_s}$  , poly ( s ) ) ;

*end* ;

Si  $k \geq 3$  on commence par tester si le polynôme minimal  $\pi$  de  $e_{h_1} + e_{h_2} + \dots + e_{h_s}$  est égal à  $\pi_A$  . Si oui ,  $E = e_{h_1} + e_{h_2} + \dots + e_{h_s}$  convient , ce qui est presque toujours le cas en pratique .

Sinon on appelle "veminimax " après avoir décrémenté s , ce qui nous donne un vecteur  $E' = e_{h_1} + j_2 e_{h_2} + \dots + j_{s-1} e_{h_{s-1}}$  tel que  $\pi_{E'} = \text{poly} ( s-1 )$  .

Pour terminer , on appelle veminimax2 ( A ,  $E'$  ,  $e_{h_s}$  ,  $\pi_A$  ) qui nous donne un vecteur  $E = E' + j_s e_{h_s}$  vérifiant  $\pi_E = \pi_A$  .

### Complexité.

Notons  $d$  le degré de  $\pi_A$ . Nous avons vu que  $\text{veminimax2} (A, e, f, \pi)$  demande  $(\deg(\pi) - \deg(\pi_c) + 1) * 2n^2 * (d - 1)$  additions et multiplications.

Afin d'alléger les notations, notons  $\Pi_i$  le ppcm  $(\pi_{e_{h_1}}, \dots, \pi_{e_{h_i}})$ .

Dans le cas le plus défavorable, la procédure "veminimax" appelle  $s$  fois "veminimax2" et  $s - 1$  fois "polymine".

Le nombre d'additions et multiplications est donc borné par :

$$2n^2 * (d - 1) (s - 1 + \deg(\Pi_2) - \deg(\Pi_1) + 1 + \deg(\Pi_3) - \deg(\Pi_2) + 1 + \dots + \deg(\Pi_s) - \deg(\Pi_{s-1}) + 1)$$

$$\text{soit } 2n^2 * (d - 1) (2s - 2 + \deg(\Pi_s) - \deg(\Pi_1))$$

en majorant  $s$  et  $\deg(\Pi_s)$  par  $n$  on obtient le résultat suivant :

Proposition : le nombre d'additions et multiplications demandé par "veminimax" est borné par  $6n^3 * d$ .

Rappelons qu'en pratique le vecteur  $E = e_{h_1} + e_{h_2} + \dots + e_{h_s}$  est solution du problème, la coût de la procédure "veminimax" est alors réduit à  $2n^2 * d$ .

## III.5. Forme de Frobenius.

### III.5.a Introduction.

Nous allons maintenant introduire une notion supplémentaire. Si  $\mathfrak{r}$  est un s.e.v. de  $\mathfrak{E}$ , stable par l'endomorphisme  $A$ , alors l'espace quotient  $\mathfrak{E}/\mathfrak{r}$  a une structure d'espace vectoriel et nous pouvons définir un endomorphisme

$$A_{\mathfrak{r}} : \mathfrak{E}/\mathfrak{r} \rightarrow \mathfrak{E}/\mathfrak{r} \text{ induit par } A.$$

Si  $f$  est un élément de  $\mathcal{E}/\mathfrak{r}$  on peut définir la notion de polynôme minimal de  $f$  pour l'endomorphisme  $A_{\mathfrak{r}}$  ; c'est le polynôme  $\pi_{\mathfrak{r},f}$  de degré minimal tel que  $\pi_{\mathfrak{r},f}(f) \equiv 0 \pmod{\mathfrak{r}}$  ; c'est à dire  $\pi_{\mathfrak{r},f}(f) \in \mathfrak{r}$ .

Dans le cas particulier où  $\mathfrak{r} = \mathfrak{r}_{i-1} = (f_1, \dots, f_{i-1})_A$ , nous avons trois propositions équivalentes :

- 1)  $\pi_{\mathfrak{r},f}(f) \equiv 0 \pmod{\mathfrak{r}}$
- 2)  $\pi_{\mathfrak{r},f}(f) \in \mathfrak{r}$
- 3) il existe des polynômes  $Q_{i,j}$   $1 \leq j \leq i-1$  tels que
 
$$\pi_{\mathfrak{r},f}(f) = Q_{i,1}(f_1) + \dots + Q_{i,i-1}(f_{i-1})$$

Comme nous l'avons déjà dit dans l'introduction de ce troisième chapitre, avant de calculer la forme de Frobenius d'une matrice, nous allons chercher un ensemble de vecteurs  $(f_1, \dots, f_k)$  vérifiant les propriétés  $(\mathcal{P})$  que nous rappelons :

$$(\mathcal{P}) \quad \left\{ \begin{array}{l} \pi_{f_i} = \pi_{A_{i-1}} \text{ pour tout } i \in \{1, \dots, k\} \\ \text{où } \pi_{f_i} \text{ est le polynôme minimal de } f_i \text{ modulo } \mathfrak{r}_{i-1} \\ \text{et } \pi_{A_{i-1}} \text{ le polynôme minimal de } A_{i-1} \end{array} \right.$$

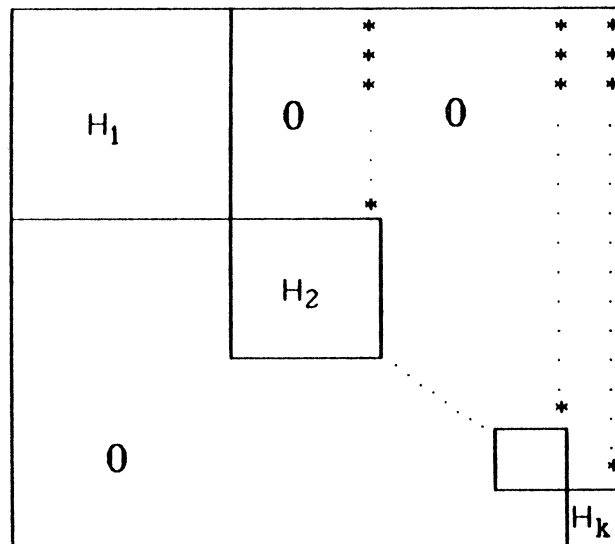
Considérons la matrice  $P$  dont les colonnes sont formées par les composantes des vecteurs

$$(f_1, \dots, A^{d_1-1}(f_1), f_2, \dots, f_k, \dots, A^{d_k-1}(f_k))$$

$$\text{Comme } \pi_{\mathfrak{r}_{i-1},f_i}(f_i) = Q_{i,1}(f_1) + \dots + Q_{i,i-1}(f_{i-1})$$

la forme intermédiaire  $H = P^{-1} A P$  est de la forme :

(2)



Si on note  $s_i$  les indices des dernières colonnes des blocs  $H_i$ , nous avons les relations suivantes :

$$s_1 = d_1 ; \quad s_2 = d_1 + d_2 ; \quad \dots ; \quad s_i = d_1 + \dots + d_i .$$

et si  $P_i$  désigne le polynôme associé au bloc  $H_i$ , alors

$$P_i = \pi_{r_{i-1}, f_i}$$

et les coefficients des polynômes  $Q_{i,k}$  sont les éléments de la matrice  $H$ , colonne  $s_i$ , lignes 1 à  $s_1$  pour  $Q_{i,1}$ , lignes  $s_1 + 1$  à  $s_2$  pour  $Q_{i,2}$  ...

Nous voyons qu'il suffit de généraliser les algorithmes présentés (calcul du polynôme minimal d'un vecteur, d'un endomorphisme, ..... ) au cas où l'espace vectoriel est un espace vectoriel quotient .



### III.5.b Polynôme minimal dans une structure quotient.

Pour commencer , plaçons nous dans le cas où  $\mathfrak{r} = (f_1)_A$  ,  $f_1$  étant un vecteur dont le degré du polynôme minimal est maximal , et revoyons l'exemple 1 pour lequel  $f_1 = e_1 + e_4 + e_{10}$  .

Dans cet exemple  $\dim \mathfrak{r} = 6$ . La 7<sup>ieme</sup> colonne de  $P$  représente le vecteur  $e_7$  et il est facile de connaître son polynôme minimal modulo  $\mathfrak{r}$  . Il suffit pour cela, d'appeler la procédure `polymine1 ( B , 7 , pas )` . Elle aura pour effet de faire apparaître dans la 7<sup>ieme</sup> colonne de  $B$  un 1 à la 8<sup>ieme</sup> ligne et des zéros ailleurs .

Puis on continue avec les colonnes suivantes jusqu'à obtenir une nouvelle matrice compagnon .

#### Exemple 3 .

Nous montrons à la fin de ce chapitre , l'effet de `polymine1 ( B , 7 , pas )` , qui calcule le polynôme minimal de  $e_7$  modulo  $\mathfrak{r} = (e_1 + e_4 + e_{10})_A$  .

Les résultat est  $\pi_{e_7} = X^2 - 6X + 9$  modulo  $\mathfrak{r}$  .

### III.5.c Obtention de la forme intermédiaire.

Dans le cas le plus général que nous envisagerons  $\mathfrak{r} = (f_1, \dots, f_h)_A$ . Supposons que  $B$  soit de la forme suivante:

(4)

|          |                                                          |                                                               |          |
|----------|----------------------------------------------------------|---------------------------------------------------------------|----------|
| $H_1$    | $\begin{matrix} * \\ * \\ 0 \\ \vdots \\ * \end{matrix}$ | $\begin{matrix} * \\ * \\ \vdots \\ \vdots \\ * \end{matrix}$ | $\vdots$ |
| $\vdots$ | $\vdots$                                                 | $0$                                                           | $\vdots$ |
| $\vdots$ | $H_2$                                                    | $\vdots$                                                      | $\vdots$ |
| $\vdots$ | $\vdots$                                                 | $\vdots$                                                      | $\vdots$ |
| $0$      | $\vdots$                                                 | $\vdots$                                                      | $\vdots$ |
| $\vdots$ | $\vdots$                                                 | $\vdots$                                                      | $\vdots$ |
| $\vdots$ | $\vdots$                                                 | $\vdots$                                                      | $\vdots$ |
| $\vdots$ | $\vdots$                                                 | $\vdots$                                                      | $\vdots$ |
| $\vdots$ | $\vdots$                                                 | $\vdots$                                                      | $\vdots$ |
| $\vdots$ | $\vdots$                                                 | $\vdots$                                                      | $\vdots$ |
| $\vdots$ | $\vdots$                                                 | $\vdots$                                                      | $\vdots$ |
| $\vdots$ | $\vdots$                                                 | $\vdots$                                                      | $\vdots$ |
| $\vdots$ | $\vdots$                                                 | $\vdots$                                                      | $\vdots$ |
| $\vdots$ | $\vdots$                                                 | $\vdots$                                                      | $\vdots$ |
| $\vdots$ | $\vdots$                                                 | $\vdots$                                                      | $\vdots$ |
| $\vdots$ | $\vdots$                                                 | $\vdots$                                                      | $\vdots$ |
| $\vdots$ | $\vdots$                                                 | $\vdots$                                                      | $\vdots$ |
| $\vdots$ | $\vdots$                                                 | $\vdots$                                                      | $\vdots$ |
| $\vdots$ | $\vdots$                                                 | $\vdots$                                                      | $\vdots$ |
| $\vdots$ | $\vdots$                                                 | $\vdots$                                                      | $\vdots$ |
| $\vdots$ | $\vdots$                                                 | $\vdots$                                                      | $\vdots$ |
| $\vdots$ | $\vdots$                                                 | $\vdots$                                                      | $\vdots$ |
| $\vdots$ | $\vdots$                                                 | $\vdots$                                                      | $\vdots$ |
| $\vdots$ | $\vdots$                                                 | $\vdots$                                                      | $\vdots$ |
| $\vdots$ | $\vdots$                                                 | $\vdots$                                                      | $\vdots$ |
| $\vdots$ | $\vdots$                                                 | $\vdots$                                                      | $\vdots$ |
| $\vdots$ | $\vdots$                                                 | $\vdots$                                                      | $\vdots$ |
| $\vdots$ | $\vdots$                                                 | $\vdots$                                                      | $\vdots$ |
| $\vdots$ | $\vdots$                                                 | $\vdots$                                                      | $\vdots$ |
| $\vdots$ | $\vdots$                                                 | $\vdots$                                                      | $\vdots$ |
| $\vdots$ | $\vdots$                                                 | $\vdots$                                                      | $\vdots$ |
| $\vdots$ | $\vdots$                                                 | $\vdots$                                                      | $\vdots$ |
| $\vdots$ | $\vdots$                                                 | $\vdots$                                                      | $\vdots$ |
| $\vdots$ | $\vdots$                                                 | $\vdots$                                                      | $\vdots$ |
| $\vdots$ | $\vdots$                                                 | $\vdots$                                                      | $\vdots$ |
| $\vdots$ | $\vdots$                                                 | $\vdots$                                                      | $\vdots$ |
| $\vdots$ | $\vdots$                                                 | $\vdots$                                                      | $\vdots$ |
| $\vdots$ | $\vdots$                                                 | $\vdots$                                                      | $\vdots$ |
| $\vdots$ | $\vdots$                                                 | $\vdots$                                                      | $\vdots$ |
| $\vdots$ | $\vdots$                                                 | $\vdots$                                                      | $\vdots$ |
| $\vdots$ | $\vdots$                                                 | $\vdots$                                                      | $\vdots$ |
| $\vdots$ | $\vdots$                                                 | $\vdots$                                                      | $\vdots$ |
| $\vdots$ | $\vdots$                                                 | $\vdots$                                                      | $\vdots$ |
| $\vdots$ | $\vdots$                                                 | $\vdots$                                                      | $\vdots$ |
| $\vdots$ | $\vdots$                                                 | $\vdots$                                                      | $\vdots$ |
| $\vdots$ | $\vdots$                                                 | $\vdots$                                                      | $\vdots$ |
| $\vdots$ | $\vdots$                                                 | $\vdots$                                                      | $\vdots$ |
| $\vdots$ | $\vdots$                                                 | $\vdots$                                                      | $\vdots$ |
| $\vdots$ | $\vdots$                                                 | $\vdots$                                                      | $\vdots$ |
| $\vdots$ | $\vdots$                                                 | $\vdots$                                                      | $\vdots$ |
| $\vdots$ | $\vdots$                                                 | $\vdots$                                                      | $\vdots$ |
| $\vdots$ | $\vdots$                                                 | $\vdots$                                                      | $\vdots$ |
| $\vdots$ | $\vdots$                                                 | $\vdots$                                                      | $\vdots$ |
| $\vdots$ | $\vdots$                                                 | $\vdots$                                                      | $\vdots$ |
| $\vdots$ | $\vdots$                                                 | $\vdots$                                                      | $\vdots$ |
| $\vdots$ | $\vdots$                                                 | $\vdots$                                                      | $\vdots$ |
| $\vdots$ | $\vdots$                                                 | $\vdots$                                                      | $\vdots$ |
| $\vdots$ | $\vdots$                                                 | $\vdots$                                                      | $\vdots$ |
| $\vdots$ | $\vdots$                                                 | $\vdots$                                                      | $\vdots$ |
| $\vdots$ | $\vdots$                                                 | $\vdots$                                                      | $\vdots$ |
| $\vdots$ | $\vdots$                                                 | $\vdots$                                                      | $\vdots$ |
| $\vdots$ | $\vdots$                                                 | $\vdots$                                                      | $\vdots$ |
| $\vdots$ | $\vdots$                                                 | $\vdots$                                                      | $\vdots$ |
| $\vdots$ | $\vdots$                                                 | $\vdots$                                                      | $\vdots$ |
| $\vdots$ | $\vdots$                                                 | $\vdots$                                                      | $\vdots$ |
| $\vdots$ | $\vdots$                                                 | $\vdots$                                                      | $\vdots$ |
| $\vdots$ | $\vdots$                                                 | $\vdots$                                                      | $\vdots$ |
| $\vdots$ | $\vdots$                                                 | $\vdots$                                                      | $\vdots$ |
| $\vdots$ | $\vdots$                                                 | $\vdots$                                                      | $\vdots$ |
| $\vdots$ | $\vdots$                                                 | $\vdots$                                                      | $\vdots$ |
| $\vdots$ | $\vdots$                                                 | $\vdots$                                                      | $\vdots$ |
| $\vdots$ | $\vdots$                                                 | $\vdots$                                                      | $\vdots$ |
| $\vdots$ | $\vdots$                                                 | $\vdots$                                                      | $\vdots$ |
| $\vdots$ | $\vdots$                                                 | $\vdots$                                                      | $\vdots$ |
| $\vdots$ | $\vdots$                                                 | $\vdots$                                                      | $\vdots$ |
| $\vdots$ | $\vdots$                                                 | $\vdots$                                                      | $\vdots$ |
| $\vdots$ | $\vdots$                                                 | $\vdots$                                                      | $\vdots$ |
| $\vdots$ | $\vdots$                                                 | $\vdots$                                                      | $\vdots$ |
| $\vdots$ | $\vdots$                                                 | $\vdots$                                                      | $\vdots$ |
| $\vdots$ | $\vdots$                                                 | $\vdots$                                                      | $\vdots$ |
| $\vdots$ | $\vdots$                                                 | $\vdots$                                                      | $\vdots$ |
| $\vdots$ | $\vdots$                                                 | $\vdots$                                                      | $\vdots$ |
| $\vdots$ | $\vdots$                                                 | $\vdots$                                                      | $\vdots$ |
| $\vdots$ | $\vdots$                                                 | $\vdots$                                                      | $\vdots$ |
| $\vdots$ | $\vdots$                                                 | $\vdots$                                                      | $\vdots$ |
| $\vdots$ | $\vdots$                                                 | $\vdots$                                                      | $\vdots$ |
| $\vdots$ | $\vdots$                                                 | $\vdots$                                                      | $\vdots$ |
| $\vdots$ | $\vdots$                                                 | $\vdots$                                                      | $\vdots$ |
| $\vdots$ | $\vdots$                                                 | $\vdots$                                                      | $\vdots$ |
| $\vdots$ | $\vdots$                                                 | $\vdots$                                                      | $\vdots$ |
| $\vdots$ | $\vdots$                                                 | $\vdots$                                                      | $\vdots$ |
| $\vdots$ | $\vdots$                                                 | $\vdots$                                                      | $\vdots$ |
| $\vdots$ | $\vdots$                                                 | $\vdots$                                                      | $\vdots$ |
| $\vdots$ | $\vdots$                                                 | $\vdots$                                                      | $\vdots$ |
| $\vdots$ | $\vdots$                                                 | $\vdots$                                                      | $\vdots$ |
| $\vdots$ | $\vdots$                                                 | $\vdots$                                                      | $\vdots$ |
| $\vdots$ | $\vdots$                                                 | $\vdots$                                                      | $\vdots$ |
| $\vdots$ | $\vdots$                                                 | $\vdots$                                                      | $\vdots$ |
| $\vdots$ | $\vdots$                                                 | $\vdots$                                                      | $\vdots$ |
| $\vdots$ | $\vdots$                                                 | $\vdots$                                                      | $\vdots$ |
| $\vdots$ | $\vdots$                                                 | $\vdots$                                                      | $\vdots$ |
| $\vdots$ | $\vdots$                                                 | $\vdots$                                                      | $\vdots$ |
| $\vdots$ | $\vdots$                                                 | $\vdots$                                                      | $\vdots$ |
| $\vdots$ | $\vdots$                                                 | $\vdots$                                                      | $\vdots$ |
| $\vdots$ | $\vdots$                                                 | $\vdots$                                                      | $\vdots$ |
| $\vdots$ | $\vdots$                                                 | $\vdots$                                                      | $\vdots$ |
| $\vdots$ | $\vdots$                                                 | $\vdots$                                                      | $\vdots$ |
| $\vdots$ | $\vdots$                                                 | $\vdots$                                                      | $\vdots$ |
| $\vdots$ | $\vdots$                                                 | $\vdots$                                                      | $\vdots$ |
| $\vdots$ | $\vdots$                                                 | $\vdots$                                                      | $\vdots$ |
| $\vdots$ | $\vdots$                                                 | $\vdots$                                                      | $\vdots$ |

Les colonnes de  $P$  étant  $(f_1, A(f_1), \dots, f_h, \dots, A^{d_h-1}(f_h), g_1, \dots, g_s)$  ;  
 les vecteurs  $g_i$  appartenant à l'ensemble  $\{e_1, \dots, e_n\}$  et  $s$  est égal au  
 nombre de colonnes de  $B_h$  .

Si on désire calculer le polynôme minimal d'un vecteur  $G = \alpha_1 g_1 + \dots + \alpha_s g_s$   
 on effectuera les transformations élémentaires nécessaires pour faire apparaître le  
 vecteur  $G$  dans la colonne  $s_h + 1$  de  $P$  , puis les vecteurs  $A(G)$  ,  $A^2(G)$  , ..... dans  
 les colonnes suivantes jusqu'à ce qu'on obtienne dans  $B$  une nouvelle matrice  
 compagnon , qui nous donnera une relation du type

$$P(G) = Q_1(f_1) + \dots + Q_h(f_h) .$$

On en déduira que  $P$  est le polynôme minimal de  $G$  modulo  $(f_1, \dots, f_h)_A$  .

Dans le paragraphe III . 3 .b nous avons décrit une procédure "extgen" qui  
 recherchait un ensemble de vecteurs  $\{f_1, \dots, f_r\}$  inclus dans  $\{e_1, \dots, e_n\}$  tel que  
 $(f_1, \dots, f_r)_A = \mathfrak{z}$ . Maintenant nous recherchons un ensemble  $\{h_1, \dots, h_t\}$  inclus  
 dans  $\{g_1, \dots, g_s\}$  tel que  $(h_1, \dots, h_t)_{A_f} = \mathfrak{z}/\mathfrak{f}$ .

Il suffit d'utiliser la procédure "extgen" avec la matrice  $B$  ; mais en partant  
 de la  $(s_h + 1)$  ième colonne au lieu de la première . On utilise donc "extgen" avec  
 les paramètres  $B$  ,  $j = s_h + 1$  , et un tableau "pasb".

De plus , après le premier appel de "polyminel" , on sauvegarde les tableaux  
 $B$  et pasb dans les tableaux  $\tilde{C}$  et pasc , car on aura parfois besoin de connaître la  
 matrice représentée par  $\tilde{C}$  lors du calcul de la forme intermédiaire .

*Procedure* extgen ( B , j , pasb )

*begin*

k := j ; h := 1 ; famgen (1) := j ;

d := polymine1 ( B , k , pasb ) ;

copymat ( B , C ) ;

*for* i = 1 *to* n *do* pasc ( i ) := pasb ( i ) ;

tbl ( h ) := d ; k := d + 1 ; h := h + 1 ;

*while* k ≤ n *do*

*begin*

d := polymine1 ( B , k , pasb ) ;

tbl ( h ) := d ;

k := d + 1 ; h := h + 1 ;

*end* ;

*for* i = 2 *to* h - 1 *do* fangen ( i ) := pasb ( tbl ( i - 1 ) + 1 ) ;

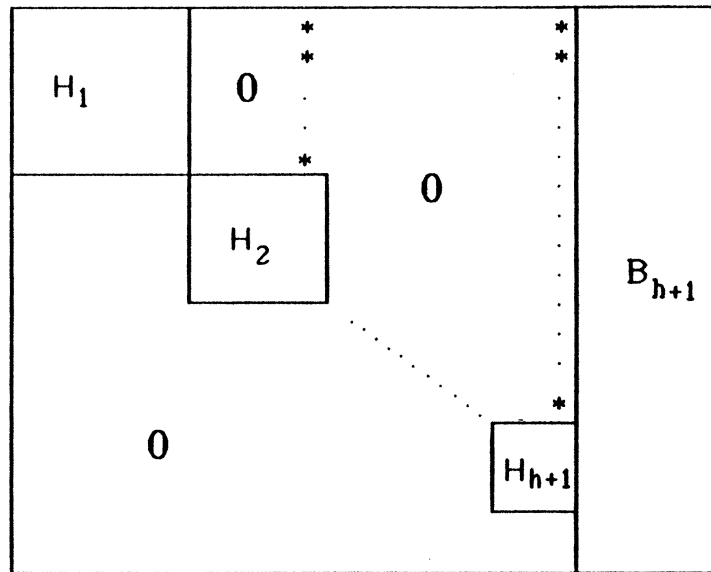
famgen ( 0 ) := h - 1 ;

*end* ;

Exemple 4 .

Si B est la matrice de l'exemple 1 ,  $\mathfrak{r} = (f_1)_A$  et  $f_1 = e_1 + e_4 + e_{10}$  alors extgen ( B , 7 , pas ) nous montre que  $(e_5, e_7)_{\Lambda_{\mathfrak{r}}} = \mathfrak{z}/\mathfrak{r}$  .

On calculera le polynôme minimal  $\pi_{A_{\mathfrak{r}}}$  comme pour  $\pi_A$  , mais les calculs des  $\pi_{h_i}$  se feront modulo  $\mathfrak{r}$  . On cherchera ensuite un vecteur  $f_{h+1}$  dont le polynôme minimal est égal à  $\pi_{A_{\mathfrak{r}}}$  , en utilisant la procédure veminimax , les calculs de polynômes minimaux se faisant aussi modulo  $\mathfrak{r}$  . On obtiendra alors un nouveau bloc  $H_{h+1}$  :



Exemple 5 .

$$\pi_{e_7} = X^2 - 6X + 9 \quad \text{modulo } (e_1 + e_4 + e_{10})_A$$

$$\pi_{e_5} = X^2 - 4X + 4 \quad \text{modulo } (e_1 + e_4 + e_{10})_A$$

"veminimax" nous donne  $e_5 + e_7$  comme vecteur ayant un polynôme minimal égal à  $\pi_{\Lambda_f}$  modulo  $(e_1 + e_4 + e_{10})_A$ .

Nous donnons maintenant la procédure "forminterm" qui calcule d'une part la forme intermédiaire  $H$  d'une matrice, et d'autre part la matrice de passage  $P$ . Nous utiliserons un tableau  $F$  de dimension  $2n \times n$ , dans laquelle nous affecterons la matrice  $H$  dans les  $n$  premières lignes de  $F$ , et la matrice  $P$  dans les  $n$  dernières lignes.

Nous savons que la matrice de passage est de la forme :

$$P = (f_1, A(f_1), \dots, A^{d_1-1}(f_1), f_2, \dots, f_k, \dots, A^{d_k-1}(f_k))$$

Les vecteurs  $f_i$  étant donnés par "veminimax", nous calculons les vecteurs  $A^h(f_i)$  en utilisant la procédure "constpas".

*Procédure constpas* ( A , F , j , d ) ;

entrées : A une matrice d'ordre n , et F un tableau de dimension  $2n \times n$  . j est l'indice de la colonne contenant le vecteur  $f_i$  ,

et d l'indice de la colonne de  $A^{d_i-1}(f_i)$  .

effet : calcule les vecteurs  $A^h(f_i)$  , et les affecte dans les n dernières lignes de F .

*begin*

*for* k = j + 1 *to* d *do*

*for* i = n + 1 *to* 2 n *do*

*for* h = 1 *to* n *do*

$F(i, k) := F(i, k) + A(n - i, h) * F(n + h, k - 1)$  ;

*end* ;

Remarque :

Cette procédure recherche la forme intermédiaire  $H$  d'une matrice A d'ordre n . Nous utilisons pour les calculs un tableau F de dimension  $2n \times n$  , et deux tableaux B et C de dimension  $n \times n$  . Nous utilisons aussi les tableaux "pasa", "pasb", "pasc" de dimension n pour repérer les permutations effectuées sur les colonnes . Cette astuce nous évite de toujours travailler avec une matrice de dimension  $2n \times n$  pour connaître la matrice de passage . La matrice de passage se calcule au fur et à mesure que l'on connaît les vecteurs  $f_i$  en utilisant la procédure "constpas" . Les composantes des vecteurs  $f_i$  , données par "veminimax", sont stockées dans le tableau "vect" . Les indices des dernières colonnes des blocs  $H_i$  de la forme intermédiaire sont stockés dans le tableau "ta" . De plus ta ( 0 ) contient le nombre de blocs  $H_i$  . Enfin , la forme intermédiaire  $H$  sera stockée dans les n premières lignes de F , et la matrice de passage P dans les n dernières lignes .

*procedure forminterm ( A , F ) ;*

*begin*

copymat ( A , F ) ; d := 0 ; nbl := 0 ;

*for* i = 1 *to* n *do* pasa ( i ) := i ;

*while* d < n *do*

*begin*

j := d + 1 ; polymina ( F , j ) ;

r := fam ( 0 ) ;

*if* r = 1 *then begin*

copymat ( C , F ) ;

*for* i = 1 *to* n past ( i ) := pasa ( pasc ( i )) ;  
*end* ;

*else begin*

veminimax ( F , j ) ;

copymat ( B , F ) ;

*for* i = 1 *to* n past ( i ) := pasa ( pasb ( i )) ;

*end* ;

d = d + deg ( poly ( r ) ) ; nbl := nbl + 1 ; ta ( nbl ) = d ;

*for* i = 1 *to* n *do* pasa ( i ) = past ( i ) ;

*for* i = 1 *to* n *do* F ( n + pasa ( i ) , j ) = vect ( i ) ;

constpas ( A , F , j , d ) ;

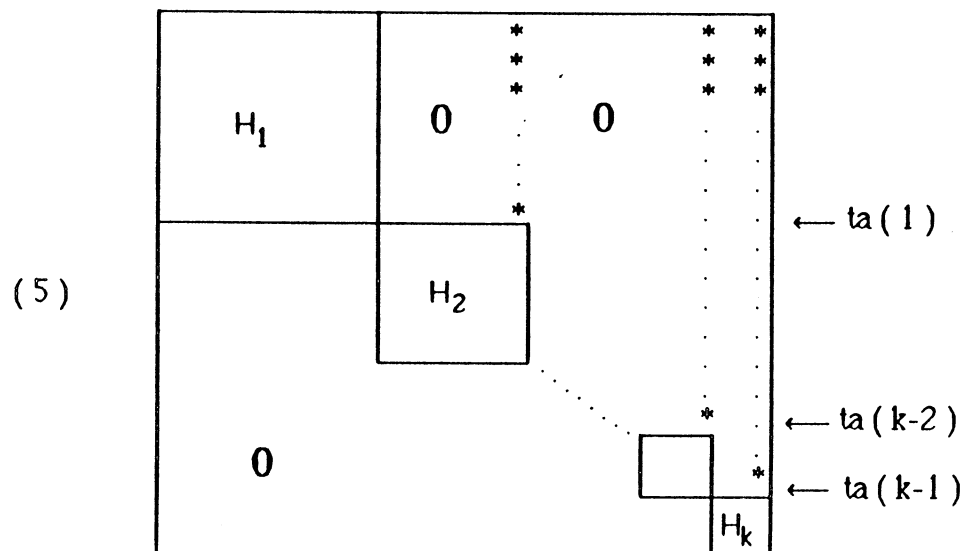
*end* ;

ta ( 0 ) = nbl ;

*end* ;

### III.5.d Obtention de la forme normale.

Supposons maintenant connue la forme intermédiaire  $H$  ainsi qu'une matrice de passage  $P$ , toutes deux étant stockées dans le tableau  $F$  de dimension  $2n \times n$ . Si l'on regarde la figure ( 5 ) qui représente la matrice  $H$ , on s'aperçoit qu'il suffit de faire apparaître des zéros dans la partie supérieure de  $H$  pour obtenir la forme de Frobenius. Nous allons employer, comme dans le chapitre II la procédure zéroadroite.



**Procédure zéroadroites ( F ) ;**

entrées : le tableau F donné par "forminterm" de dimension  $2n \times n$ .

effet : transforme F à l'aide des transformations élémentaires, afin d'obtenir la forme de Frobenius de A dans les n premières lignes de F, et une matrice de passage P dans les n dernières lignes.

**begin**

$k = \text{ta}(0)$  ;  $\text{ta}(0) = 0$  ;

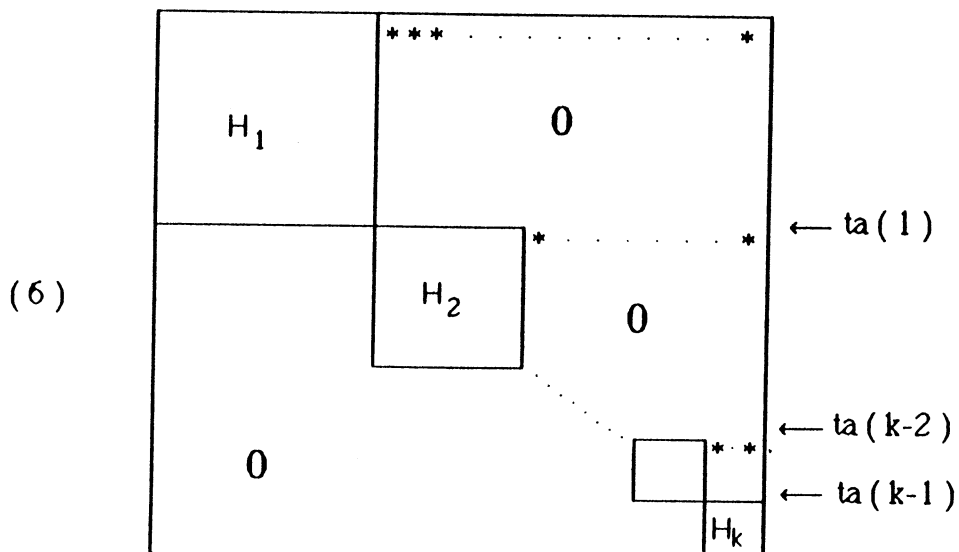
**for**  $h = k - 1$  **step** -1 **to** 1 **do**

    zéroadroite ( F,  $\text{ta}(h - 1)$ ,  $\text{ta}(h)$  ) ;

$\text{ta}(0) = k$  ;

**end;**

A priori, la procédure "zéroadroites" transforme les n premières lignes de la matrice H en une matrice de la forme (6). ( les \* représentant des éléments quelconques du corps  $\mathbb{K}$  ).





Toutefois , si on se reporte au théorème démontré au paragraphe II .4 , on s'aperçoit que tous les éléments notés \* dans la partie supérieure de la matrice ( 6 ) sont nuls . En effet , supposons par exemple qu'un des éléments de la première ligne  $F_{1,j}$  avec  $1 \leq j \leq n$  soit non nul . Alors le degré du polynôme minimal du vecteur  $g_j$  représenté par la  $j^{\text{ième}}$  colonne de  $P$  est strictement supérieur à celui de  $f_1$  . Ce qui est une contradiction avec le fait que le degré de  $\pi_{f_1}$  est maximal . Un raisonnement analogue pour les autres lignes permet de conclure que tous les éléments notés \* sont nuls .

La matrice  $H_d$  , obtenue après "zerodroites" , est donc bloc-diagonale  
 $H_d = \text{diag} ( H_1 , \dots , H_k )$  , les blocs  $H_i$  étant les mêmes que dans la forme intermédiaire .

Démontrons maintenant , le théorème 1 énoncé dans l'introduction de ce chapitre ( III . 1 . ) :

*Théorème 1 :*      *la matrice  $H_d$  est la forme de Frobenius de  $A$  .*

démonstration :

lemme 1 : Soient  $\{ f_1 , \dots , f_k \}$   $k$  vecteurs vérifiant la propriété (  $\mathfrak{P}$  ) .

alors pour tout  $i \in \{ 1 , \dots , k - 1 \}$        $\pi_{f_{i+1}}$  divise  $\pi_{f_i}$

démonstration du lemme : Reprenons les notations habituelles .

Soit  $i \in \{ 1 , \dots , k - 1 \}$  alors  $\mathcal{V}_i \supset \mathcal{V}_{i-1}$  car  $\mathcal{V}_i = ( \mathcal{V}_{i-1} , f_i )_A$

donc  $\pi_{A_i}$  divise  $\pi_{A_{i-1}}$

par hypothèse , nous avons  $\pi_{A_i} = \pi_{f_{i+1}}$  et  $\pi_{A_{i-1}} = \pi_{f_i}$

donc  $\pi_{f_{i+1}}$  divise  $\pi_{f_i}$

fin de la démonstration du lemme .

Si l'on désigne par  $P_i$  le polynôme associé au bloc  $H_i$  de la forme intermédiaire , on a :

$P_i = \pi_{i_j}$  et donc, d'après le lemme  $P_{i+1}$  divise  $P_i$  pour tout  $i \in \{1, \dots, k-1\}$ .

La matrice  $H_d$  obtenue après "zeroadroites" est une forme faible de Frobenius, et  $P_{i+1}$  divise  $P_i$ . De l'unicité de la forme normale de Frobenius, on déduit que pour tout  $i \in \{1, \dots, k\}$   $F_i = H_i$ .

fin de la démonstration du théorème.

*procedure* **frobenius** ( A , F ) ;

entrées : A une matrice d'ordre n , et F un tableau de dimension  $n \times n$ .

effet : calcule la forme de Frobenius de A ainsi qu'une matrice de passage P. On trouve la forme de Frobenius dans les n premières lignes du tableau F, et la matrice de passage dans les n dernières lignes de F.

*begin*

forminterm ( A , F ) ;

zeroadroites ( F ) ;

*end* ;

Complexité :

a) la procédure "forminterm".

Si la  $i^{\text{ème}}$  itération donne un bloc  $H_i$  de dimension  $d_i$ , le coût de chaque procédures est :

- polymina :  $2 n^3 d_i$  additions et multiplications.

- veminimax :  $6 n^3 d_i$  additions et multiplications.

- constpas :  $n^2 d_i$  additions et multiplications.

ce qui donne pour "forminterm" :

$8 n^4 + n^3$  additions et multiplications.

b) la procédure "zéroadroites" :

le nombre de transformations élémentaires nécessaires est inférieure à  $n(n-1)/2$ . Chacunes d'elles demandent au plus  $2n$  additions et multiplications.

ce qui donne pour "zéroadroites" :

$n^3$  additions et multiplications.

Nous pouvons en conclusion énoncer le théorème suivant :

Théorème :

*Le nombre d'additions et multiplications nécessaires pour le calcul de la forme de Frobenius d'une matrice d'ordre  $n$ , et d'une matrice de passage est borné par  $8n^4 + 2n^3$ .*

### III.6 Le cas particulier $K = \mathbb{Q}$ , complexité polynomiale de l'algorithme.

#### III.6.a Taille des coefficients.

Nous donnons dans ce paragraphe une majoration de la taille des coefficients qui interviennent dans les calculs. En utilisant le dernier théorème du III.5., on déduira que la complexité de l'algorithme est polynomiale.

Nous supposons que les coefficients de la matrice  $A$  sont des entiers. Reprenons les notations du paragraphe II.6.

$$- M_A = \max_{i,j} |a_{i,j}|$$

$$- \|A\| = \max_i \sum_{j=1}^n |a_{i,j}| \quad \text{on a} \quad \|A\| \leq n M_A$$

- Si  $Q$  est un diviseur du polynôme caractéristique  $P_A$

$$Q = X^r + b_{r-1}X^{r-1} + \dots + b_0$$

$$\text{et on note } K_A = \max_{i,Q} |b_i| \quad \text{où } Q \text{ est un diviseur de } P_A$$

Théorème :  $K_A \leq 2^{n-1} \|A\|^n$

la démonstration est donnée dans le paragraphe II . 6 .

Pour le calcul de la forme intermédiaire  $H$  , on peut rappeler une nouvelle fois , que pendant et après chaque procédure, on peut écrire la matrice de passage colonne par colonne à l'aide de  $r$  vecteurs  $(f_1, \dots, f_r)$  , les autres colonnes étant formées par des vecteurs de la forme  $A^k(f_i)$  . Les vecteurs  $f_i$  , donnés par la procédure "veminimax" , s'expriment comme une combinaison linéaire des vecteurs  $e_j$  de la base canonique :

$$f_i = j_1 e_1 + \dots + j_n e_n \quad \text{avec} \quad |j_i| \leq n.$$

A chaque pas les coefficients de la matrice de passage  $P$  sont entiers et on a :

$$M_P \leq n \|A\|^{n-1} \quad \text{et} \quad \|P\| \leq n^2 \|A\|^{n-1}$$

$$\text{donc} \quad |\det P| \leq n^n (n \|A\|^{n-1})^n = n^{2n} \|A\|^{n(n-1)}$$

La matrice  $P^{-1}$  est une matrice à coefficients rationnels , et on a :

$$P^{-1} = \frac{1}{\det P} P'$$

les coefficients de  $P'$  étant des déterminants de sous matrices de  $P$  , nous avons les inégalités suivantes :

$$M_{P'} \leq n^{2n} \|A\|^{n(n-1)} \quad \text{et} \quad \|P'\| \leq n^{2n+1} \|A\|^{n(n-1)}.$$

$$\text{Soit } B \text{ telle que } B = P^{-1} A P = \frac{1}{\det P} P' A P.$$

Les coefficients de  $B$  sont des rationnels dont les numérateurs sont majorés par :

$$\|P'\| \|A\| \|P\| \leq n^{2n+3} \|A\|^{n^2}$$

$$\text{et les dénominateurs par } |\det P| \leq n^{2n} \|A\|^{n^2-n}.$$

Etudions ce qui se passe dans la dernière partie de l'algorithme lors de l'appel de la procédure "zéroadroites", avec comme paramètre le tableau  $F$  décrit en ( 6 ) .

Les coefficients des blocs  $F_i$  sont des entiers majorés par  $K_A$ . Notons  $D$  le ppcm des dénominateurs des éléments de la forme intermédiaire, et  $M_F$  le maximum des numérateurs.

Supposons, dans un premier temps, que la forme intermédiaire  $H$  ne contienne que deux blocs  $F_1$  et  $F_2$ , de dimension  $d_1$  et  $d_2$ .

Il suffit alors d'appeler zéroadroite (  $F, 0, d_1$  ).

Notons  $S_i$  l'étape qui consiste à annuler les termes de la  $i$ ème ligne de  $F$ ,  $f_{i,j}$  avec  $d_1 + 1 \leq j \leq n$ , avec les transformations élémentaires  $C_{j, -f_{i,j}, i-1}$ ; et  $Q_i$  la matrice de passage correspondant à l'étape  $S_i$ .

$$Q_i = \begin{array}{|c|} \hline \begin{array}{ccccccc} 1 & & & & & & \\ & 1 & & & & & \\ & & \ddots & & & & \\ & & & 1 & 0 & * & \dots & * \\ & & & & \ddots & & & \\ & & & & & 0 & & \\ & & & & & & \ddots & \\ & & & & & & & 1 \end{array} \\ \hline \end{array}$$

← ligne  $i-1$   
les \* représentent  
les éléments  $-f_{i,j}$

La procédure zéroadroite est la suite des étapes  $S_i$  pour  $i = d_1$  à 2.

Après l'étape  $S_{d_1}$ , les éléments de la ligne  $d_1-1$  de  $F$  ont un dénominateur majoré par  $D$  et un numérateur majoré par  $d_2 K_A M_F$ . Ces éléments figureront sur la ligne  $d_1 - 2$  de la prochaine matrice de passage  $Q_i$  avec  $i = d_1 - 1$ .

Lorsqu'on poursuit les étapes  $S_i$  jusqu'à  $S_2$ , les dénominateurs du tableau  $F$  restent majorés par  $D$ , et les numérateurs par  $(d_2 K_A)^{d_1-1} M_F$ .

La matrice de passage  $Q$  entre la forme intermédiaire et la forme normale de Frobenius est égale au produit des matrices  $Q_i$ , c'est une matrice triangulaire supérieure, où les numérateurs sont majorés par :

$$(d_2 K_A)^{l_1-1} M_F$$

et les dénominateurs par  $D$ .

Dans le cas où il y a plus de deux blocs dans la forme intermédiaire, un raisonnement similaire nous montre que les rationnels que l'on rencontre dans la procédure "zéroadroites" ont un dénominateur majoré par  $D$ , et un numérateur majoré par :

$$(n K_A)^{d-1} M_F \text{ avec } d = \max(d_i) \text{ et } d_i \text{ égal à la dimension du bloc } F_i.$$

Si  $P$  est la matrice de passage entre  $A$  et la forme intermédiaire  $H$ , et  $Q$  la matrice de passage entre  $H$  et la forme normale de Frobenius  $F_1$ , alors  $AP = PH$  et  $HQ = QF_1$  donc  $APQ = PQF_1$ . Les dénominateurs de  $PQ$  sont majorés par  $D$  et les numérateurs par :

$$n M_P M_Q \leq n (n \|A\|^{n-1}) (n K_A)^n M_F.$$

En tenant compte des différentes majorations, on peut conclure en disant que les entiers qui apparaissent dans cet algorithme sont tous majorés par :

$$n^{3n+5} 2^{n^2} \|A\|^{2n^2+n-1}.$$

### Conclusion :

*Si on appelle taille d'un entier  $M$ , le nombre de bits nécessaire pour représenter  $M$ , nous avons les résultats suivants :*

- Avec cet algorithme, la taille des entiers est bornée par  $O(n^2 \log(\|A\|))$ .
- Le temps nécessaire pour effectuer une opération arithmétique sur ces entiers sera majoré par  $O(n^4 \log^2(\|A\|))$ , et pour avoir la forme de Frobenius de  $A$  ainsi qu'une matrice de passage :

$$O(n^8 \log^2(\|A\|)).$$

### III. 6. b Résultats.

Nous rappelons dans les deux premières colonnes du tableau , les résultats concernant le premier algorithme ( exposé du chapitre II ) , afin d'établir quelques comparaisons . Dans tous les cas nous avons calculé la forme de Frobenius et une matrice de passage , et nous avons porté dans ce tableau les temps de calcul exprimés en seconde .

| nom de la matrice | ( 2 )   | ( 4 )    | ( 7 )    | ( 8 )     |
|-------------------|---------|----------|----------|-----------|
| mat - 4           | 0 , 017 | 0 , 071  | 0 , 085  | 0 , 158   |
| mat - 6           | 0 , 107 | 0 , 555  | 0 , 296  | 0 , 911   |
| mat - 10          | 0 , 651 | 2 , 635  | 1 , 232  | 3 , 604   |
| mat - 20          | 4 , 174 | 20 , 037 | 10 , 159 | 30 , 260  |
| mat1 - 20         | 2 , 887 | 81 , 219 | 8 , 970  | 211 , 832 |

Les colonnes correspondent aux expériences suivantes :

( 2 )  $\mathbb{K} = \mathbb{F}_p$  avec  $p = 185363$  . Premier algorithme .

( 4 )  $\mathbb{K} = \mathbb{Q}$  . Premier algorithme .

( 7 )  $\mathbb{K} = \mathbb{F}_p$  avec  $p = 185363$  . Deuxième algorithme .

( 8 )  $\mathbb{K} = \mathbb{Q}$  . Deuxième algorithme .

En comparant les résultats des expériences ( 2 ) et ( 7 ) d'une part , et ( 4 ) et ( 8 ) d'autre part , nous voyons sur ces cinq exemples que le deuxième algorithme demande plus d'opérations que le premier .

Le deuxième algorithme semble donc plus coûteux , mais on obtient en général des matrices de passage "plus simples" qu'avec le premier algorithme . Nous donnons à la fin de ce chapitre , les matrices de passage des exemples traités afin d'établir une comparaison avec celles obtenues par le premier algorithme .

Nous proposons dans le prochain paragraphe , une modification du deuxième algorithme afin de le rendre moins coûteux .



### III. 7 Une modification lorsque $K = \mathbb{Q}$ .

#### III. 7. a Nouvelle programmation de "polymine1".

Jusqu'à maintenant , nous avons travaillé avec des matrices où tous les éléments étaient considérés comme des rationnels , et étaient représentés par des listes ( a . b ) .

De plus , après chaque addition et multiplication de deux rationnels , on effectuait un calcul de pgcd et deux quotients afin de représenter les éléments de la matrice par des fractions rationnelles irréductibles .

Dans le but d'éviter ces nombreux calculs de pgcd et de quotients , nous avons envisagé de représenter une matrice  $B$  à coefficients rationnels , par un entier "denb" et une matrice  $B'$  à coefficients entiers ; "denb" étant un multiple du ppcm des dénominateurs de  $B$  , et

$$B = \frac{1}{\text{denb}} B'$$

Nous allons montrer comment écrire "polymine1" , la procédure fondamentale de l'algorithme , lorsqu'on travaille avec une matrice  $B$  représentée par "denb" et  $B'$  .

Nous supposons pour simplifier , qu'au départ  $\text{denb} = 1$  , c'est à dire que les éléments de  $B$  sont entiers ( le cas où "denb" est un entier quelconque sera étudié à la fin de ce paragraphe ) , et revoyons la procédure "polymine1" décrite dans le paragraphe III . 3 . Cette procédure est une boucle , qui transforme à chaque itération la matrice  $B$  en  $B_1$  , puis  $B_2$  , ... , et  $B_{d-1}$  ,  $d$  étant le degré du polynôme minimal de  $e_1$  . Les matrices de passage  $P_1, P_2, \dots, P_{d-1}$  , que l'on ne calcule pas , peuvent se décrire colonne par colonne de la façon suivante :

$$P_k = ( e_1 , A(e_1) , \dots , A^{k-1}(e_1) , \dots , g_i , \dots )$$

les  $g_i$  étant des vecteurs appartenant à l'ensemble  $\{e_1, \dots, e_n\}$  .

Le problème est de savoir comment calculer un entier  $\Delta_k$  , multiple des dénominateurs des éléments de  $B_k$  .

$$\text{Nous avons : } B P_k = P_k B_k$$

$$\text{donc } B_k = P_k^{-1} B P_k$$

$$\text{et } B_k = \left( \frac{1}{\det P_k} \right) (P_k^{-1})' B P_k$$

$(P_k^{-1})'$  étant égale à la transposée de la matrice des cofacteurs de  $P_k$ .

$B$  et  $P_k$  étant des matrices à coefficients entiers, le produit  $(P_k^{-1})' B P_k$  est une matrice à coefficients entiers. On peut donc choisir pour  $\Delta_k$  le déterminant de  $P_k$ .

Mais même si l'on ne calcule pas la matrice de passage  $P_k$ , on peut connaître exactement son déterminant. En effet, la procédure "polymine1" effectuée sur  $B$  est une suite de transformations élémentaires. Or, à une transformation élémentaire du type  $P_{i,j}$  sur  $B$  correspond la permutation des colonnes  $i$  et  $j$  de la matrice de passage  $P$ , qui est une transformation de déterminant  $-1$ .

À une transformation de type  $M_{i,a}$  sur  $B$  correspond la multiplication de la  $i^{\text{ème}}$  colonne de  $P$  par  $1/a$ , qui est une transformation de déterminant  $1/a$ .

Enfin, à une transformation de type  $L_{i,a,j}$  ou  $C_{i,a,j}$  sur  $B$  correspond une transformation sur  $P$  de déterminant  $1$ .

Nous avons donc l'important résultat :

L'entier  $\Delta_k$  est égal au produit des déterminants des transformations élémentaires de type  $P_{i,j}$  ou  $M_{i,a}$  que l'on exécute lors de la procédure "polymine1".

Maintenant nous allons détailler les différentes étapes de la procédure "polymine1" pour montrer comment nous pouvons utiliser le résultat ci-dessus.

Soit  $B$  est une matrice à coefficients entiers :

$$B = \begin{array}{|l|} \hline a \quad \dots\dots \\ b \quad \dots\dots \\ c \quad \dots\dots \\ \vdots \\ \vdots \\ \vdots \\ \vdots \\ \vdots \\ \hline \end{array}$$

si  $b \neq 0$ , la première transformation effectuée par "polymine1" est  $M_{2,1/b}$ . Le déterminant  $\Delta_1$  de  $P_1$  est donc égal à  $b$ .

Après  $k$  itérations de la boucle de "polymine1", nous avons obtenu une matrice  $B_k$  de la forme :

$$B_k = \begin{bmatrix} 0 & \dots & 0 & \frac{a}{\Delta_k} & \dots & \dots & \frac{*}{\Delta_k} \\ 1 & & & & & & \vdots \\ & 0 & & & & & \vdots \\ 0 & & 1 & \frac{f}{\Delta_k} & \dots & \dots & \frac{*}{\Delta_k} \\ 0 & \dots & 0 & \frac{g}{\Delta_k} & \dots & \dots & \frac{*}{\Delta_k} \\ 0 & \dots & 0 & \frac{h}{\Delta_k} & \dots & \dots & \frac{*}{\Delta_k} \\ 0 & \dots & 0 & \frac{*}{\Delta_k} & \dots & \dots & \frac{*}{\Delta_k} \end{bmatrix} = \frac{1}{\Delta_k} B'_k$$

La prochaine transformation effectuée par "polymine1" est :

$$M_{k+2, \frac{\Delta_k}{g}}$$

Le déterminant  $\Delta_{k+1}$  de  $P_{k+1}$  est donc égal à :

$$\Delta_{k+1} = \Delta_k \frac{g}{\Delta_k} = g$$

Avant de décrire en détail la procédure "polymine1", montrons comment se calcule la matrice  $B_{k+1}$ .

$$B_{k+1} = (P_{k+1})^{-1} B_k P_{k+1}.$$

$$P_{k+1} =$$

$$\begin{array}{ccc} 1 & \frac{a}{\Delta_k} & \\ & \vdots & \\ & \frac{f}{\Delta_k} & 0 \\ & \frac{g}{\Delta_k} & \\ & \frac{h}{\Delta_k} & 1 \\ & \vdots & \\ 0 & & 1 \end{array}$$

$$P_{k+1}^{-1} =$$

$$\begin{array}{ccc} 1 & -\frac{a}{g} & \\ & \vdots & \\ & -\frac{f}{g} & 0 \\ & \frac{\Delta_k}{g} & \\ & -\frac{h}{g} & 1 \\ & \vdots & \\ 0 & & 1 \end{array}$$

Nous avons de plus :

$$P_{k+1} = \underbrace{\begin{array}{ccc} 1 & & a \\ & \ddots & f \\ & & 0 \\ & & g \\ & & h \\ & & \vdots \end{array}}_{Q_1} * \underbrace{\begin{array}{ccc} 1 & & 0 \\ & \ddots & \\ & & \frac{1}{\Delta_k} \\ & & 1 \\ & & \ddots \end{array}}_{Q_2}$$

et :

$$P_{k+1}^{-1} = \frac{1}{g} \underbrace{\begin{array}{ccc} 1 & & 0 \\ & \ddots & \\ & & \Delta_k \\ & & 1 \\ & & \ddots \end{array}}_{Q_3} \underbrace{\begin{array}{ccc} g & & -a \\ & \ddots & -f \\ & & 1 \\ & & -h \\ & & g \\ & & \vdots \end{array}}_{Q_4}$$

$$B_{k+1} = \frac{1}{g} Q_3 Q_4 B_k Q_1 Q_2$$

$$B_{k+1} = \frac{1}{g} Q_3 Q_4 \frac{1}{\Delta_k} B_k Q_1 Q_2$$

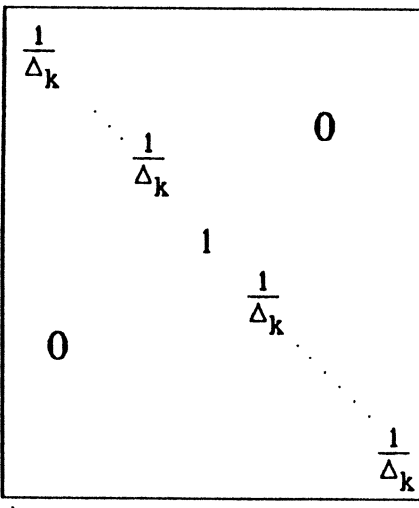
comme

$$B_{k+1} = \frac{1}{g} B_{k+1}$$

nous avons :

$$B_{k+1} = \frac{1}{\Delta_k} Q_3 Q_4 B_k Q_1 Q_2$$

et  $\frac{1}{\Delta_k} Q_3 =$



$R_3$

$$B_{k+1} = R_3 (Q_4 B_k Q_1) Q_2$$

Il est intéressant de remarquer que  $R_3$  et  $Q_2$  ne sont pas des matrices à coefficients entiers . Les éléments de la matrice  $C_{k+1} = Q_4 B_k Q_1$  sont des entiers , et les divisions par  $\Delta_k$  lors du calcul de  $R_3 C_{k+1} Q_2$  seront toujours possibles . Ce résultat ne serait pas trivial , si l'on n'avait démontré auparavant que les éléments de la matrice  $R_3 C_{k+1} Q_2 = (B_{k+1})' = g B_{k+1}$  étaient des entiers .

*procedure* **polymine1** ( B ,  $\Delta$  , j ) ;

entrées : B une matrice à coefficients entiers ,  $\Delta$  et j deux entiers .  
effets : voir § III . 3 .

*begin*

$j_1 = j + 1$  ;

k := **chercheli** ( B , j ) ;

*while*  $k \leq n$  *do*

*begin*

*if*  $k \neq j_1$  *then*  $P_{i,j_1}$  ;

$g := B(j_1, j)$  ;

*for*  $i = 1$  *to* n *do*

*begin*

$c := 0$

*for*  $k = 1$  *to* n *do*  $c := c + B(k, j) * B(i, k)$  ;

$B(i, j_1) := c$  ;

*end* ;

%  $B \leftarrow B Q_1$  %

*for*  $i = 1$  *to* n *do* *if*  $i \neq j_1$  *then*

*begin*

$q := B(i, j)$  ;

*for*  $k = 1$  *to* n *do*

$B(i, k) = g * B(i, k) - q * B(j_1, k)$  ;

*end* ;

%  $B \leftarrow Q_4 B$  %

*for*  $i = 1$  *to* n *do*  $B(i, j_1) = B(i, j_1) / \Delta$  ;

%  $B \leftarrow B Q_2$  %

*for*  $i = 1$  *to* n *do*

*if*  $i \neq j_1$  *then*

*for*  $k = 1$  *to* n *do*  $B(i, k) = B(i, k) / \Delta$  ;

%  $B \leftarrow R_3 B$  %

$\Delta := g$  ;  $j = j_1$  ;  $j_1 = j + 1$  ;

k := **chercheli** ( B , j ) ;

*end* ;

*return* j ;

*end* ;

Toujours dans le cas où l'on souhaite travailler uniquement avec des matrices à coefficients entiers, nous pouvons, comme nous l'avons fait pour "polymine1", réécrire les procédures "zéroadroites" et "zeroadroite" de telle sorte que les éléments de la matrice de passage restent entiers. Les autres procédures appellent essentiellement "polymine1", et peuvent donc être encore utilisées sans modification.

Nous faisons quelques rappels avant d'écrire les nouvelles procédures "zéroadroites" et "zéroadroite".

F désigne la matrice de dimension  $2n * n$

$$F = \begin{bmatrix} H' \\ P' \end{bmatrix}$$

avec  $H' = \Delta H$ , H la forme intermédiaire de A et  $\Delta$  un entier, et P' une matrice à coefficients entiers telle que  $AP' = P'H$ .

"ta" est le tableau de dimension n donné par la procédure "forminterm". Nous avons  $ta(0) = k$  le nombre de blocs  $H_i$  dans la forme intermédiaire H, et  $ta(i)$  est l'indice de la dernière colonne du bloc  $H_i$ .

*Procedure zeroadroite (F, h);*

*begin*

```

 t1 = ta(h - 1) ; t2 = ta(h) ;
 for i = n + 1 to 2n do
 for j = 1 + t2 to ta(h + 1) do a(i, j) = Δ a(i, j) ;
 for i = t2 step -1 to t1 + 2 do
 for j = 1 + t2 to n do Cj, -a(i, j), i - 1

```

*end;*



*Procedure* **zeroadroites** ( F , Δ ) ;

*begin*

$k := ta(0) ; ta(0) := 0 ;$

*for*  $h = 1$  *to*  $k$  *do*

$a(1 + ta(h-1), ta(h)) := a(1 + ta(h-1), ta(h)) /_{\Delta} ;$

*for*  $i = 2 + ta(h-1)$  *to*  $ta(h)$  *do*

*begin*

$a(i, i-1) := 1 ;$

$a(i, ta(h)) := a(i, ta(h)) /_{\Delta} ;$

*end;*

*for*  $h = k-1$  *step*  $-1$  *to*  $1$  *do*

**zeroadroite** ( F , h ) ;

$ta(0) := k ;$

*end;*

Il nous reste à étudier le cas où les éléments de la matrice **B** de départ sont rationnels . Après avoir calculé "denb" le ppcm des dénominateurs , nous avons :

$$B = \frac{1}{denb} B' \quad B' \text{ à coefficients entiers .}$$

L'algorithme modifié nous donne **F'** la forme de Frobenius de **B'** , et **P'** une matrice de passage . On en déduit que **B** est semblable à :

$$F'' = \frac{1}{denb} F'$$

C'est le théorème suivant que nous permettra de déterminer la forme de Frobenius de **F''** .

*Théorème :*

$$\text{si } C = \begin{pmatrix} 0 & . & . & . & . & 0 & -a_0 \\ 1 & . & . & . & . & . & -a_1 \\ 0 & . & . & . & . & . & . \\ . & . & . & . & . & . & . \\ . & . & . & . & . & . & . \\ . & . & . & . & . & 0 & -a_{n-2} \\ 0 & . & . & . & . & 0 & 1 & -a_{n-1} \end{pmatrix}$$

$$\text{alors } \frac{1}{\Delta} C \text{ est semblable à } F = \begin{pmatrix} 0 & . & . & . & . & 0 & -\frac{a_0}{\Delta^n} \\ 1 & . & . & . & . & . & -\frac{a_1}{\Delta^{n-1}} \\ 0 & . & . & . & . & . & . \\ . & . & . & . & . & . & . \\ . & . & . & . & . & . & . \\ . & . & . & . & . & 0 & -\frac{a_{n-2}}{\Delta^2} \\ 0 & . & . & . & . & 0 & 1 & -\frac{a_{n-1}}{\Delta} \end{pmatrix}$$

$$\text{et } P = \begin{pmatrix} \Delta^{n-1} & 0 \\ 0 & \Delta \\ & 1 \end{pmatrix} \text{ est une matrice de passage } \left( \frac{1}{\Delta} C \right) P = P F$$

### III. 7. b Résultats et conclusion.

Les résultats obtenus en utilisant la nouvelle procédure "polymine1" figurent dans la colonne ( 9 ) , et les temps de calcul sont exprimés en seconde .

| nom de la matrice | ( 4 )    | ( 8 )     | ( 9 )     |
|-------------------|----------|-----------|-----------|
| mat - 4           | 0 , 071  | 0 , 158   | 0 , 102   |
| mat - 6           | 0 , 555  | 0 , 911   | 0 , 421   |
| mat - 10          | 2 , 635  | 3 , 604   | 2 , 139   |
| mat - 20          | 20 , 037 | 30 , 260  | 21 , 306  |
| mat1 - 20         | 81 , 219 | 211 , 832 | 30 , 743  |
| mat - 40          |          |           | 679 , 160 |

( 4 )  $\mathbb{K} = \mathbb{Q}$  . Premier algorithme .

( 8 )  $\mathbb{K} = \mathbb{Q}$  . Deuxième algorithme .

( 9 )  $\mathbb{K} = \mathbb{Q}$  . Deuxième algorithme modifié .

### Conclusion.

Bien qu'il soit un peu moins facile à programmer , le deuxième algorithme modifié , c'est à dire utilisant les nouvelles procédures "polymine1" , "zeroadroites" et "zeroadroite" , est très avantageux .

De nombreux calculs de pgcd et de quotient sont évités , et l'espace mémoire utilisé est moins grand puisque les éléments des matrices sont toujours des entiers et non des rationnels .

De plus , la matrice de passage obtenue est aussi une matrice à coefficients entiers .

polymine ( B , e1 + e4 + e10 )

|   |     |      |      |       |       |      |       |       |         |
|---|-----|------|------|-------|-------|------|-------|-------|---------|
| 0 | 0   | 0    | 0    | 0     | -72   | 256  | -140  | 360   | -186    |
| 1 | 0   | 0    | 0    | 0     | 228   | -720 | 394   | -1012 | 523     |
| 0 | 1   | 0    | 0    | 0     | -290  | 776  | -425  | 1090  | -1127/2 |
| 0 | 0   | 1    | 0    | 0     | 191   | -404 | 443/2 | -567  | 1173/4  |
| 0 | 0   | 0    | 1    | 0     | -69   | 102  | -56   | 143   | -74     |
| 0 | 0   | 0    | 0    | 1     | 13    | -10  | 11/2  | -14   | 29/4    |
| 0 | 0   | 0    | 0    | 0     | 0     | 1    | 1     | -5    | 2       |
| 0 | 0   | 0    | 0    | 0     | 0     | -4   | 5     | -6    | 3       |
| 0 | 0   | 0    | 0    | 0     | 0     | 0    | 0     | 0     | 1       |
| 0 | 0   | 0    | 0    | 0     | 0     | 0    | 0     | -4    | 4       |
|   |     |      |      |       |       |      |       |       |         |
| 1 | -4  | -23  | -87  | -292  | -935  | 0    | 0     | 0     | 0       |
| 0 | -11 | -49  | -172 | -560  | -1774 | 0    | 0     | 0     | 0       |
| 0 | -15 | -67  | -237 | -780  | -2501 | 0    | 0     | 0     | 0       |
| 1 | -17 | -81  | -294 | -984  | -3196 | 0    | 0     | 0     | 0       |
| 0 | -22 | -99  | -355 | -1188 | -3875 | 0    | 0     | 1     | 0       |
| 0 | -25 | -113 | -408 | -1376 | -4522 | 0    | 0     | 0     | 1       |
| 0 | -28 | -127 | -461 | -1564 | -5169 | 1    | 0     | 0     | 0       |
| 0 | -31 | -141 | -514 | -1752 | -5816 | 0    | 1     | 0     | 0       |
| 0 | -33 | -149 | -540 | -1832 | -6058 | 0    | 0     | 0     | 0       |
| 1 | -32 | -148 | -539 | -1831 | -6057 | 0    | 0     | 0     | 0       |

~~~~~

extgen ( B , pasb )

|   |    |    |   |    |   |      |   |     |      |
|---|----|----|---|----|---|------|---|-----|------|
| 0 | -4 | 4  | 0 | -2 | 0 | 0    | 0 | 0   | -15  |
| 1 | 4  | -3 | 0 | 1  | 0 | 0    | 0 | 0   | 10   |
| 0 | 0  | 2  | 0 | 0  | 0 | 1/2  | 0 | 0   | -7/2 |
| 0 | 0  | 0  | 0 | -4 | 0 | 2    | 0 | 0   | -4   |
| 0 | 0  | 0  | 1 | 4  | 0 | -1/2 | 0 | 0   | -3/2 |
| 0 | 0  | 0  | 0 | 0  | 0 | -9   | 0 | 0   | 25   |
| 0 | 0  | 0  | 0 | 0  | 1 | 6    | 0 | 0   | -9   |
| 0 | 0  | 0  | 0 | 0  | 0 | 0    | 0 | -9  | -13  |
| 0 | 0  | 0  | 0 | 0  | 0 | 0    | 1 | 6   | 5    |
| 0 | 0  | 0  | 0 | 0  | 0 | 0    | 0 | 0   | 1    |
|   |    |    |   |    |   |      |   |     |      |
| 1 | 1  | 0  | 0 | -2 | 0 | -1   | 0 | -2  | 0    |
| 0 | -1 | 0  | 0 | -4 | 0 | -2   | 0 | -4  | 0    |
| 0 | -1 | 1  | 0 | -5 | 0 | -3   | 0 | -6  | 0    |
| 0 | -1 | 0  | 1 | -4 | 0 | -4   | 0 | -8  | 0    |
| 0 | -1 | 0  | 0 | -6 | 0 | -4   | 0 | -10 | 0    |
| 0 | -1 | 0  | 0 | -6 | 1 | -2   | 0 | -12 | 0    |
| 0 | -1 | 0  | 0 | -6 | 0 | -5   | 0 | -13 | 0    |
| 0 | -1 | 0  | 0 | -6 | 0 | -5   | 1 | -11 | 0    |
| 0 | -1 | 0  | 0 | -6 | 0 | -5   | 0 | -14 | 0    |
| 0 | -1 | 0  | 0 | -6 | 0 | -5   | 0 | -14 | 1    |

polynome minimal de  $e_7$  modulo  $(e_1 + e_4 + e_{10})$

|   |   |   |   |   |      |   |    |         |         |
|---|---|---|---|---|------|---|----|---------|---------|
| 0 | 0 | 0 | 0 | 0 | -72  | 0 | 0  | -24     | 6       |
| 1 | 0 | 0 | 0 | 0 | 228  | 0 | 0  | 68      | -17     |
| 0 | 1 | 0 | 0 | 0 | -290 | 0 | 0  | -74     | $37/2$  |
| 0 | 0 | 1 | 0 | 0 | 191  | 0 | 0  | 39      | $-39/4$ |
| 0 | 0 | 0 | 1 | 0 | -69  | 0 | 0  | -10     | $5/2$   |
| 0 | 0 | 0 | 0 | 1 | 13   | 0 | 0  | 1       | $-1/4$  |
| 0 | 0 | 0 | 0 | 0 | 0    | 0 | -9 | $-13/2$ | $11/4$  |
| 0 | 0 | 0 | 0 | 0 | 0    | 1 | 6  | $3/2$   | $-3/4$  |
| 0 | 0 | 0 | 0 | 0 | 0    | 0 | 0  | 0       | 1       |
| 0 | 0 | 0 | 0 | 0 | 0    | 0 | 0  | -4      | 4       |

|   |     |      |      |       |       |   |    |   |   |
|---|-----|------|------|-------|-------|---|----|---|---|
| 1 | -4  | -23  | -87  | -292  | -935  | 0 | 2  | 0 | 0 |
| 0 | -11 | -49  | -172 | -560  | -1774 | 0 | 4  | 0 | 0 |
| 0 | -15 | -67  | -237 | -780  | -2501 | 0 | 6  | 0 | 0 |
| 1 | -17 | -81  | -294 | -984  | -3196 | 0 | 8  | 0 | 0 |
| 0 | -22 | -99  | -355 | -1188 | -3875 | 0 | 10 | 1 | 0 |
| 0 | -25 | -113 | -408 | -1376 | -4522 | 0 | 12 | 0 | 1 |
| 0 | -28 | -127 | -461 | -1564 | -5169 | 1 | 15 | 0 | 0 |
| 0 | -31 | -141 | -514 | -1752 | -5816 | 0 | 12 | 0 | 0 |
| 0 | -33 | -149 | -540 | -1832 | -6058 | 0 | 12 | 0 | 0 |
| 1 | -32 | -148 | -539 | -1831 | -6057 | 0 | 12 | 0 | 0 |

forme de Frobenius de mat-4 et matrice de passage.

Le deuxieme algorithme donne les memes matrices que le premier algorithme.

~~~~~

forme de Frobenius de mat-6 et matrice de passage.

|   |   |   |   |     |   |
|---|---|---|---|-----|---|
| 0 | 0 | 0 | 0 | 15  | 0 |
| 1 | 0 | 0 | 0 | -47 | 0 |
| 0 | 1 | 0 | 0 | 56  | 0 |
| 0 | 0 | 1 | 0 | -32 | 0 |
| 0 | 0 | 0 | 1 | 9   | 0 |
| 0 | 0 | 0 | 0 | 0   | 3 |

|   |    |     |     |     |   |
|---|----|-----|-----|-----|---|
| 1 | -7 | -25 | -53 | -47 | 0 |
| 0 | -8 | -24 | -44 | -16 | 0 |
| 0 | -6 | -16 | -22 | 32  | 0 |
| 0 | -3 | -6  | 3   | 84  | 0 |
| 1 | 1  | 5   | 29  | 137 | 0 |
| 1 | 2  | 7   | 28  | 109 | 1 |

On pourra comparer cette matrice de passage avec celle obtenue en travaillant avec le premier algorithme. Sur cet exemple , l'amelioration qu'apporte le deuxieme algorithme est assez frappante .

forme de Frobenius de mat-10 et matrice de passage.

|   |   |   |   |   |      |   |   |   |     |
|---|---|---|---|---|------|---|---|---|-----|
| 0 | 0 | 0 | 0 | 0 | -72  | 0 | 0 | 0 | 0   |
| 1 | 0 | 0 | 0 | 0 | 228  | 0 | 0 | 0 | 0   |
| 0 | 1 | 0 | 0 | 0 | -290 | 0 | 0 | 0 | 0   |
| 0 | 0 | 1 | 0 | 0 | 191  | 0 | 0 | 0 | 0   |
| 0 | 0 | 0 | 1 | 0 | -69  | 0 | 0 | 0 | 0   |
| 0 | 0 | 0 | 0 | 1 | 13   | 0 | 0 | 0 | 0   |
| 0 | 0 | 0 | 0 | 0 | 0    | 0 | 0 | 0 | -36 |
| 0 | 0 | 0 | 0 | 0 | 0    | 1 | 0 | 0 | 60  |
| 0 | 0 | 0 | 0 | 0 | 0    | 0 | 1 | 0 | -37 |
| 0 | 0 | 0 | 0 | 0 | 0    | 0 | 0 | 1 | 10  |

|   |     |      |      |       |       |   |    |    |     |
|---|-----|------|------|-------|-------|---|----|----|-----|
| 1 | -4  | -23  | -87  | -292  | -935  | 0 | 3  | 15 | 59  |
| 0 | -11 | -49  | -172 | -560  | -1774 | 0 | 6  | 30 | 118 |
| 0 | -15 | -67  | -237 | -780  | -2501 | 0 | 9  | 45 | 177 |
| 1 | -17 | -81  | -294 | -984  | -3196 | 0 | 12 | 60 | 236 |
| 0 | -22 | -99  | -355 | -1188 | -3875 | 1 | 15 | 71 | 279 |
| 0 | -25 | -113 | -408 | -1376 | -4522 | 0 | 14 | 74 | 306 |
| 0 | -28 | -127 | -461 | -1564 | -5169 | 1 | 17 | 83 | 333 |
| 0 | -31 | -141 | -514 | -1752 | -5816 | 0 | 14 | 74 | 306 |
| 0 | -33 | -149 | -540 | -1832 | -6058 | 0 | 14 | 74 | 306 |
| 1 | -32 | -148 | -539 | -1831 | -6057 | 0 | 14 | 74 | 306 |



forme de Frobenius de mat-20 .

|   |   |   |   |   |   |   |   |       |   |   |   |   |   |      |   |   |   |     |   |
|---|---|---|---|---|---|---|---|-------|---|---|---|---|---|------|---|---|---|-----|---|
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | -144  | 0 | 0 | 0 | 0 | 0 | 0    | 0 | 0 | 0 | 0   | 0 |
| 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 672   | 0 | 0 | 0 | 0 | 0 | 0    | 0 | 0 | 0 | 0   | 0 |
| 0 | 1 | 0 | 0 | 0 | 0 | 0 | 0 | -1336 | 0 | 0 | 0 | 0 | 0 | 0    | 0 | 0 | 0 | 0   | 0 |
| 0 | 0 | 1 | 0 | 0 | 0 | 0 | 0 | 1480  | 0 | 0 | 0 | 0 | 0 | 0    | 0 | 0 | 0 | 0   | 0 |
| 0 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | -1001 | 0 | 0 | 0 | 0 | 0 | 0    | 0 | 0 | 0 | 0   | 0 |
| 0 | 0 | 0 | 0 | 1 | 0 | 0 | 0 | 424   | 0 | 0 | 0 | 0 | 0 | 0    | 0 | 0 | 0 | 0   | 0 |
| 0 | 0 | 0 | 0 | 0 | 1 | 0 | 0 | -110  | 0 | 0 | 0 | 0 | 0 | 0    | 0 | 0 | 0 | 0   | 0 |
| 0 | 0 | 0 | 0 | 0 | 0 | 1 | 0 | 16    | 0 | 0 | 0 | 0 | 0 | 0    | 0 | 0 | 0 | 0   | 0 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0     | 0 | 0 | 0 | 0 | 0 | 72   | 0 | 0 | 0 | 0   | 0 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0     | 1 | 0 | 0 | 0 | 0 | -300 | 0 | 0 | 0 | 0   | 0 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0     | 0 | 1 | 0 | 0 | 0 | 518  | 0 | 0 | 0 | 0   | 0 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0     | 0 | 0 | 1 | 0 | 0 | -481 | 0 | 0 | 0 | 0   | 0 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0     | 0 | 0 | 0 | 1 | 0 | 260  | 0 | 0 | 0 | 0   | 0 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0     | 0 | 0 | 0 | 0 | 1 | -82  | 0 | 0 | 0 | 0   | 0 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0     | 0 | 0 | 0 | 0 | 0 | 14   | 0 | 0 | 0 | 0   | 0 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0     | 0 | 0 | 0 | 0 | 0 | 0    | 0 | 0 | 0 | -4  | 0 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0     | 0 | 0 | 0 | 0 | 0 | 0    | 1 | 0 | 0 | 12  | 0 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0     | 0 | 0 | 0 | 0 | 0 | 0    | 0 | 1 | 0 | -13 | 0 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0     | 0 | 0 | 0 | 0 | 0 | 0    | 0 | 0 | 1 | 6   | 0 |
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0     | 0 | 0 | 0 | 0 | 0 | 0    | 0 | 0 | 0 | 0   | 1 |

Cette matrice est une matrice bloc-diagonale  $F = (F_1, F_2, F_3, F_4)$ , les blocs  $F_i$  étant d'ordre 8, 7, 4 et 1. Les polynomes associés à ces blocs, vérifient la relation de divisibilité  $P_4 \mid P_3 \mid P_2 \mid P_1$ , alors que le premier algorithme donnait une matrice bloc-diagonale, dont les blocs étaient respectivement d'ordre 7, 8, 4, 1 et les polynomes associés aux blocs ne vérifiaient pas la relation de divisibilité.

La matrice de passage est une matrice dont les coefficients sont entiers et majores par 128626.

## **Chapitre IV .**

**Calcul de la forme de Frobenius et de la forme de Jordan  
d'une matrice dont les coefficients sont  
des nombres algébriques .**

#### IV 1 Présentation du système D5.

Nous nous intéressons dans ce chapitre au cas des matrices dont les coefficients appartiennent au corps  $\mathbb{Q}_{\text{alg}}$  des nombres algébriques sur  $\mathbb{Q}$ .

Nous donnerons dans le second paragraphe des résultats concernant le calcul de la forme de Frobenius d'une matrice à coefficients dans  $\mathbb{Q}_{\text{alg}}$  en utilisant l'algorithme présenté dans le chapitre II. Enfin dans le troisième paragraphe on s'intéressera à la forme de Jordan d'une matrice. On peut à ce sujet rappeler, que même si les coefficients d'une matrice  $A$  sont des nombres rationnels, les coefficients de la matrice de Jordan  $J$  de  $A$  sont des nombres algébriques en général non rationnels.

Mais qu'est ce qu'un nombre algébrique, et comment le représenter ?

Un nombre algébrique est une racine d'un polynôme à coefficients dans  $\mathbb{Q}$ .

Pour représenter un nombre algébrique, on peut parfois utiliser le signe  $\sqrt{\phantom{x}}$ , comme dans l'exemple suivant :

$$P_1 = X^2 - X - 1 \quad \text{a deux racines} \quad X_1 = \frac{1}{2}(1 + \sqrt{5}) \quad \text{et} \quad X_2 = \frac{1}{2}(1 - \sqrt{5})$$

Si l'utilisation du signe  $\sqrt{\phantom{x}}$  semble satisfaisante pour les racines des polynômes de degré 2, elle devient plus difficile pour des polynômes de degré 3 ou 4, et souvent impossible pour des polynômes de degré supérieur ou égal à 5.

Une autre solution consiste à représenter un nombre algébrique par un polynôme  $P$  à coefficient dans  $\mathbb{Q}$  dont il est racine. Cette représentation pose plusieurs problèmes :

Pb1 la non unicité de  $P$  : elle peut être évitée si on impose à  $P$  d'être un polynôme irréductible.

Pb2 la non unicité des racines de  $P$ .

Pb3 la difficulté de trouver le polynôme  $P$ . Pour s'en convaincre on peut considérer l'exemple suivant :

$$X_1 \text{ une racine de } X_1^2 - X_1 - 1 \quad \text{et} \quad X_2 \text{ une racine de } X_2^2 + 3X_2 + 7$$

comment représenter  $X_1 + X_2$  ?

La solution que nous avons retenue est la méthode D5 proposée dans [ Della Dora , Di Crescenzo , Duval , 1985 ] . Un nombre algébrique  $a$  est représenté par un polynôme  $P_a$  de  $\mathbb{Q} [ X_1 , \dots , X_n ]$

Les  $X_i$  sont définis par des équations du type :

$$\begin{aligned} P_1 ( X_1 ) &= 0 \\ P_2 ( X_1 , X_2 ) &= 0 \\ &\dots\dots\dots \\ P_{n-1} ( X_1 , \dots , X_{n-1} ) &= 0 \\ P_n ( X_1 , \dots , X_n ) &= 0 \end{aligned}$$

où les  $P_i ( X_1 , \dots , X_{i-1} , X_i )$  sont des polynômes en  $X_i$  , à coefficients dans  $\mathbb{Q} [ X_1 , \dots , X_{i-1} ]$  , unitaires et de degré  $d_i > 0$  .  $X_i$  désigne donc une racine quelconque de  $P_i$  .

On dit alors qu'on travaille dans l'extension  $( P_1 , P_2 , \dots , P_n )$  de niveau  $n$  . Il faut ajouter que si  $a$  est représenté par un polynôme  $P_a$  ,  $P_a$  représente un ensemble fini de nombres algébriques .

De cette façon , le principal problème Pb3 est évité .

Le problème Pb1 demeure , car on n'impose pas aux polynômes  $P_i$  d'être irréductibles , la factorisation de ces polynômes pouvant s'avérer très coûteuse .

$\mathbb{Q} [ X_1 , \dots , X_n ]$  n'est donc pas toujours un corps ( on désigne cette structure par anneau de Lazard ) , ce qui n'est pas gênant lorsqu'on souhaite additionner , multiplier ou prendre l'opposé d'un nombre algébrique . En effet, supposons qu'on travaille dans une extension de niveau  $n$  . Nous avons donc des relations du type  $P_i ( X_1 , \dots , X_i ) = 0$  , où  $P_i$  est un polynôme de degré  $d_i > 0$  en  $X_i$  .

Si  $a$  et  $b$  sont des nombres algébriques représentés par  $P_a$  et  $P_b$  deux éléments de  $\mathbb{Q} [ X_1 , \dots , X_n ]$  de degré en  $X_i$  strictement inférieur à  $d_i$  , alors  $a + b$  et  $-a$  sont représentés par  $P_a + P_b$  et  $-P_a$  ; et le produit  $a * b$  est représenté par  $P_a * P_b$  polynôme dans lequel on pourra remplacer les termes

$X_i^{d_i} , \dots , X_i^{2d_i - 2}$  par des polynômes de degré inférieur à  $d_i$  .

Supposons maintenant que l'on souhaite tester si un nombre algébrique  $a$  est nul ( le test  $a = b$  se ramènera au test  $a - b = 0$  ), et pour simplifier, que l'on travaille dans une extension de niveau 1, avec  $P_1(X) = 0$ ,  $P_1$  sans facteurs carrés.

( si  $P_1$  à des facteurs carrés, on considèrera  $\frac{P_1}{\text{pgcd}(P_1, P_1')}$  )

Calculons  $G = \text{PGCD}(P_a, P_1)$ , où  $P_a$  est un polynôme qui représente  $a$ , avec  $\deg P_a < \deg P_1$ .

Si le degré de  $G$  est égal à 0 alors  $P_a(X)$  est non nul pour toutes les racines  $X$  de  $P_1$  et donc  $a$  est non nul.

Sinon, nous obtenons une factorisation non triviale  $P_1 = G(X) \cdot F(X)$  et nous pouvons dire que si  $X$  est une racine de  $G$  alors  $a = 0$ , sinon  $X$  est une racine de  $F$ , et  $a$  est non nul.

Exemple 1 :  $P_1 = X^6 + 1$  ;  $P_a = X^4 - 1$

$$G = \text{PGCD}(P_a, P_1) = X^2 + 1$$

On en déduit alors une factorisation ( ou scindage ) de  $P_1$

$$P_1 = (X^2 + 1) \cdot (X^4 - X^2 + 1)$$

et nous avons :

$$a = 0 \quad \text{si} \quad X^2 + 1 = 0$$

$$a \neq 0 \quad \text{si} \quad X^4 - X^2 + 1 = 0$$

Pour calculer l'inverse d'un nombre algébrique  $a$ , il faut commencer par tester la non nullité de  $a$ , test qui peut nous conduire à envisager plusieurs extensions. En se plaçant dans une extension  $P_1$  où  $a$  est non nul, on détermine les polynômes  $U$  et  $V$  de l'égalité de Bezout  $U \cdot P_a + V \cdot P_1 = 1$  en utilisant l'algorithme d'Euclide. On en déduit alors  $U \cdot P_a = 1$  dans l'extension  $P_1$ , et  $1/a$  peut être représenté par  $U$ . Nous donnons maintenant un exemple de calcul d'inverse lorsqu'on travaille dans une extension de niveau 2, définie par les polynômes  $P_1$  et  $P_2$  ci-dessous.

$$p1 := x^6 + 1$$

$$p2 := x^2 y^2 - x^3 + y^3 + 3xy$$

$$a := y^2 + y^3 x + y^4 x^2 - x^4 - 2x^2$$

inva();

a est nul dans l'extension :

$$\text{RELATION 2 en y : } 0 = y^2 - x$$

$$\text{RELATION 1 en x : } 0 = x^2 + 1$$

~~~~~

$$1/a \text{ est egal a : } (-y^3 x + 2)/2$$

dans l'extension :

$$\text{RELATION 2 en y : } 0 = y^2 + 2y^3 x + 1$$

$$\text{RELATION 1 en x : } 0 = x^2 + 1$$

~~~~~

$$1/a \text{ est egal a : } (22y^2 x^2 - 2y^3 + 32y^3 x^3 - 13y^3 x + 115x^2 - 71)/222$$

dans l'extension :

$$\text{RELATION 2 en y : } 0 = y^3 + y^2 x + 3y - x$$

$$\text{RELATION 1 en x : } 0 = x^4 - x^2 + 1$$

Le problème Pb2 lui non plus n'est pas résolu. On peut adjoindre à la représentation d'un nombre  $a$  une approximation complexe de  $a$  suffisante pour séparer tous les nombres algébriques représentés par  $P_a$  dans une extension  $(P_1, \dots, P_n)$ . Cette solution peut en général être évitée, car tout calcul algébrique dans une extension est valable pour tous les nombres algébriques représentés par  $P_a$ .

On peut aussi dans certains cas, séparer les racines d'un polynôme en rajoutant des relations. On rencontrera ce problème dans le dernier paragraphe de ce chapitre, lorsqu'on s'intéressera à la forme de Jordan d'une matrice.

### Conclusion :

La particularité du système D5 est de pouvoir effectuer toutes les opérations  $+$ ,  $-$ ,  $*$ ,  $/$ , et les tests d'égalité sans jamais factoriser de polynômes. En contrepartie, chaque test d'égalité nécessite un calcul de PGCD, et il faut s'attendre à un scindage qui, s'il a lieu, nous conduira à travailler successivement dans chaque extension.

## IV.2 Forme de Frobenius d'une matrice dont les coefficients sont des nombres algébriques.

Nous avons choisi pour traiter ce cas, d'utiliser le premier algorithme (présenté dans le chapitre II), plus facile à programmer.

Quelles modifications doit-on apporter par rapport aux procédures décrites dans le chapitre II ? Souvenons nous que cet algorithme exécute une suite de transformations élémentaires de type semblable  $P_{i,j}$ ,  $M_{i,a}$  avec  $a \neq 0$ ,  $L_{i,q,j}$  et  $C_{i,q,j}$ . Toutes ces transformations réalisent des permutations (de lignes ou de colonnes), des additions, multiplications, calculs d'inverses, et on ne rencontre aucun problème de scindage lorsqu'on travaille dans une extension  $(P_1, \dots, P_n)$ .

Toutefois, la stratégie qui détermine le choix et l'ordre des transformations à exécuter, est fixée par deux procédures "chercheli" et "chercheco", décrites dans les paragraphes II.3 et II.5, qui recherchent des éléments non nuls d'une colonne pour "chercheli", ou d'une ligne pour "chercheco". Ces deux procédures peuvent donner lieu à des scindages.

Nous détaillons seulement le cas de la procédure "chercheli", pour montrer les modifications que l'on doit apporter pour travailler avec les nombres algébriques.

Lorsque  $\mathbb{K} = \mathbb{Q}$ , nous avons écrit "chercheli" de la façon suivante:

```
procedure chercheli (B , j) ;

begin
 k = j+1 ;
 while Bk,j ≠ 0 do k = k + 1 ;
 return k ;
end ;
```

Malheureusement, lorsque les coefficients de  $B$  sont des nombres algébriques, l'usage des boucles est à proscrire lorsqu'on trouve à l'intérieur un test pouvant donner lieu à un scindage (c'est le cas du test  $B_{k,j} \neq 0$ ). Il faut d'abord transformer le programme en un programme récursif.

```
procedure chercheli (B , j , i) ;
```

entrée :  $B$  une matrice d'ordre  $n$ ,  $j$  et  $i$  deux entiers, avec  $i = j + 1$  au départ.

sortie : un entier  $k$  tel que  $i \leq k \leq n$  si  $B_{k,j} \neq 0$ , ou  $k = n + 1$  si  $B_{h,j} = 0 \quad \forall h \in \{i, \dots, n\}$ .

```
begin
 if i > n then return i
 else
 if Bi,j = 0 then chercheli (B , j , i+1)
 else return i ;
end ;
```

Il faut ensuite faire une deuxième transformation de programme, car  $B_{i,j}$  est un nombre algébrique, et le test  $B_{i,j} = 0$  peut provoquer un scindage.



1

ou  $k_r = n + 1$  si  $B_{k,j} = 0 \quad \forall k \in \{i, \dots, n\}$ .

**end;**

Enfin "solalg" est utilisée pour présenter le résultat sous forme d'une liste  $((k_1, \text{Ext-1}), \dots, (k_s, \text{Ext-s}))$ .

Exemple :

$$P_1 = X^3 - X, \quad B = \text{matalg-3}$$

$$B = \begin{pmatrix} 2X+1 & 0 & X \\ X^2-X & 2X+1 & X+3 \\ 0 & 0 & 2X+1 \end{pmatrix}$$

chercheli ( B , 1 , 2 ) retourne la liste

$$\text{sol} = ((2, X+1), (4, X^2-X))$$

qui s'interprète par :

- 2 si X vérifie la relation  $X+1=0$
- 4 si X vérifie la relation  $X^2-X=0$

Si **chercheli** a donné lieu à un ou plusieurs scindages , on devra ensuite exécuter "**polyminel**" en se plaçant successivement dans chaque extension .

exemple : reprenons l'exemple précédent avec  $B = \text{matalg-3}$  .

"**polyminel**" retourne l'ordre du bloc formé et la matrice transformée.

**polyminel** ( B , 1 ) ;

1) Un bloc d'ordre 2 si X vérifie la relation  $X+1=0$

$$B = \begin{pmatrix} 0 & -1 & 0 \\ 1 & -2 & 1 \\ 0 & 0 & -1 \end{pmatrix}$$

2) Un bloc d'ordre 1 si  $X$  vérifie la relation  $X^2 - X = 0$

$$B = \begin{pmatrix} 2X+1 & 0 & X \\ 0 & 2X+1 & X+3 \\ 0 & 0 & 2X+1 \end{pmatrix}$$

Puis , lorsqu'on se placera dans l'extension  $(X^2 - X)$  pour continuer les calculs , la procédure "chercheco" recherchera un élément non nul dans la première ligne de  $B$  , et testera si  $X = 0$  , ce qui donnera un nouveau scindage .

Ceci explique pourquoi la procédure "frobenius" distingue trois cas , comme le montre le résultat de la page suivante .

```
frobenius(matalg-3,3);
```

```
cpu time : 0,511 s
```

```
cas 1) var : x
```

```
extension:
```

$$x - 1 = 0$$

```
solution:
```

```
0 -9 0
```

```
1 6 0
```

```
0 0 3
```

```
cas 2) var : x
```

```
extension:
```

$$x = 0$$

```
solution:
```

```
1 0 0
```

```
0 0 -1
```

```
0 1 2
```

```
cas 3) var : x
```

```
extension:
```

$$x + 1 = 0$$

```
solution:
```

```
0 0 -1
```

```
1 0 -3
```

```
0 1 -3
```

Terminons ce paragraphe en donnant comme exemples les formes de Frobenius des matrices "matalg-4" et "matialg-4" definies dans l'annexe.

extension:  $x^4 - 3x^2 - 4 = 0$

frobenius(matalg-4,4);

cpu time : 2,072 s

cas 1) var : x

extension:

$x^2 - 4 = 0$

solution:

|   |   |   |     |
|---|---|---|-----|
| 0 | 0 | 0 | -24 |
| 1 | 0 | 0 | 50  |
| 0 | 1 | 0 | -35 |
| 0 | 0 | 1 | 10  |

cas 2) var : x

extension:

$x^2 + 1 = 0$

solution:

|   |   |     |   |
|---|---|-----|---|
| 0 | 0 | 0   | 0 |
| 1 | 0 | -96 | 0 |
| 0 | 1 | 20  | 0 |
| 0 | 0 | 0   | 8 |

extension:  $x_1^4 - 3x_1^2 - 4 = 0$   
 $x_2^2 + 3x_1x_2 + 1 = 0$

frobenius(mat1alg-4,4);  
 cpu time : 13,803 s

cas 1) var :  $x_2 \ x_1$

extension:  
 $x_2^2 + 3x_1x_2 + 1 = 0$   
 $x_1^4 - 3x_1^2 - 4 = 0$

solution:

|       |   |   |                     |
|-------|---|---|---------------------|
| $x_2$ | 0 | 0 | 0                   |
| 0     | 0 | 0 | $-6x_1x_2 - 2$      |
| 0     | 1 | 0 | $(3x_1 - 4)x_2 + 1$ |
| 0     | 0 | 1 | $2x_2 + 2$          |

cas 2) var :  $x_2 \ x_1$

extension:  
 $x_2^2 - x_1 = 0$   
 $x_1^2 - 4 = 0$

solution:

|   |   |   |     |
|---|---|---|-----|
| 0 | 0 | 0 | -24 |
| 1 | 0 | 0 | 50  |
| 0 | 1 | 0 | -35 |
| 0 | 0 | 1 | 10  |

cas 3) var :  $x_2 \ x_1$

extension:  
 $x_2^2 - x_1 = 0$   
 $x_1^2 + 1 = 0$

solution:

|   |   |     |   |
|---|---|-----|---|
| 0 | 0 | 0   | 0 |
| 1 | 0 | -96 | 0 |
| 0 | 1 | 20  | 0 |
| 0 | 0 | 0   | 8 |

### IV . 3 Représentation de la forme de Jordan d'une matrice .

Nous avons montré dans le premier chapitre comment on pouvait déduire la forme de Jordan d'une matrice à partir de sa forme de Frobenius .

Nous voulons soulever dans ce dernier paragraphe , le problème de la représentation de la forme de Jordan , ce problème étant lié à celui abordé au début de ce chapitre : Comment représenter des nombres algébriques ?

Considérons par exemple la matrice

$$F = \begin{pmatrix} 0 & 0 & -1 \\ 1 & 0 & -4 \\ 0 & 1 & 0 \end{pmatrix}$$

le polynôme caractéristique de  $F$  est  $P_F = X^3 + 4X + 1$

Les racines de  $P_F$  étant distinctes ,  $F$  est une matrice diagonalisable , et nous avons vu dans le premier chapitre que la forme de Jordan  $J$  de  $F$  , ainsi que les matrices  $Q$  et  $Q^{-1}$  telles que  $F = Q^{-1} J Q$  , peuvent se représenter de la façon suivante :

$$J = \begin{pmatrix} X_1 & 0 & 0 \\ 0 & X_2 & 0 \\ 0 & 0 & X_3 \end{pmatrix} , \quad Q = \begin{pmatrix} 1 & X_1 & X_1^2 \\ 1 & X_2 & X_2^2 \\ 1 & X_3 & X_3^2 \end{pmatrix}$$

$$Q^{-1} = \frac{1}{283} \begin{pmatrix} 64X_1^2 - 24X_1 + 265 & 64X_2^2 - 24X_2 + 265 & 64X_3^2 - 24X_3 + 265 \\ -9X_1^2 - 32X_1 - 24 & -9X_2^2 - 32X_2 - 24 & -9X_3^2 - 32X_3 - 24 \\ 24X_1^2 - 9X_1 + 64 & 24X_2^2 - 9X_2 + 64 & 24X_3^2 - 9X_3 + 64 \end{pmatrix}$$

$X_1 , X_2 , X_3$  étant les trois racines distinctes de  $P_F$  , prises dans un ordre quelconque .

Mais comment représenter , dans le système D5 les matrices  $J$  ,  $Q$  et  $Q^{-1}$  ?

Nous ne pouvons évidemment pas nous contenter de la seule relation  $X^3 + 4X + 1 = 0$  qui nous imposerait de représenter la forme de Jordan  $J$  par :

$$J = \begin{pmatrix} X & 0 & 0 \\ 0 & X & 0 \\ 0 & 0 & X \end{pmatrix}$$

Nous ne pouvons pas non plus définir les nombres  $X_1, X_2, X_3$  par les trois relations :

$$X_1^3 + 4X_1 + 1 = 0$$

$$X_2^3 + 4X_2 + 1 = 0$$

$$X_3^3 + 4X_3 + 1 = 0$$

car elles ne font pas intervenir le fait que les  $X_i$  soient distincts.

Pour déclarer que  $X_2$  vérifie  $X_2^3 + 4X_2 + 1 = 0$  et  $X_1 \neq X_2$ , on définit  $X_2$  comme une racine du polynôme

$$P_2 = \frac{P_F(X_2)}{(X_2 - X_1)} = X_2^2 + X_1 X_2 + (X_1^2 + 4)$$

De même, pour déclarer que  $X_3$  vérifie  $X_3^3 + 4X_3 + 1 = 0$  et  $X_3 \neq X_1$  et  $X_3 \neq X_2$ , on définit  $X_3$  comme racine du polynôme

$$P_3 = \frac{P_2(X_3)}{(X_3 - X_2)} = X_3 + X_1 + X_2$$

Cette solution, bien qu'elle permette facilement d'utiliser les matrices  $J, Q$  et  $Q^{-1}$  pour d'autres calculs dans le système D5 (produit de matrices ...), n'est toutefois pas complètement satisfaisante.



En effet, si on revient à un cas plus général où  $J$  est une matrice d'ordre  $n$ , dont les éléments diagonaux  $X_1, \dots, X_n$  sont les racines distinctes d'un polynôme de degré  $n$ , on s'aperçoit que la dernière solution nous impose de travailler avec des éléments de  $\mathbb{Q}[X_1, \dots, X_n]$ , les  $X_i$  étant définies comme des racines de polynôme  $P_i$  de degré  $n - i + 1$ , et à coefficients dans  $\mathbb{Q}[X_1, \dots, X_{i-1}]$ .

Or nous savons maintenant qu'il est possible de faire certains calculs, le calcul de  $Q^{-1}$  par exemple, en se contentant de dire que  $X_1, \dots, X_n$  sont les  $n$  racines distinctes d'un polynôme  $P_n$  de degré  $n$ , et en travaillant dans  $\mathbb{Q}[X]$ .

Finalement pour reprendre l'exemple de ce paragraphe, nous sommes amenés à penser qu'une bonne représentation des matrices  $J$ ,  $Q$  et  $Q^{-1}$  serait la suivante :

$$J = \begin{pmatrix} B(X_1) & 0 & 0 \\ 0 & B(X_2) & 0 \\ 0 & 0 & B(X_3) \end{pmatrix} \quad \text{avec} \quad B(X) = (X)$$

$$Q = \begin{pmatrix} L(X_1) \\ L(X_2) \\ L(X_3) \end{pmatrix} \quad \text{avec} \quad L(X) = (1 \quad X \quad X^2)$$

$$Q^{-1} = (C(X_1) \quad C(X_2) \quad C(X_3)) \quad \text{avec} \quad C(X) = \frac{1}{283} \begin{pmatrix} 64X^2 - 24X + 265 \\ -9X^2 - 32X - 24 \\ 24X^2 - 9X + 64 \end{pmatrix}$$

Pour compléter cette discussion, imaginons que l'on souhaite calculer l'exponentielle de la matrice  $F$ , où  $F$  est la matrice d'ordre 3 définie au début de ce paragraphe.

$$\text{nous avons} \quad e^F = e^{Q^{-1} J Q} = Q^{-1} e^J Q$$

$$\text{et } e^J = \begin{pmatrix} e^{X_1} & 0 & 0 \\ 0 & e^{X_2} & 0 \\ 0 & 0 & e^{X_3} \end{pmatrix}$$

$$e^J Q = \begin{pmatrix} R(X_1) \\ R(X_2) \\ R(X_3) \end{pmatrix} \quad \text{avec} \quad R(X) = ( e^X \quad X e^X \quad X^2 e^X )$$

$$Q^{-1} e^J Q = \frac{1}{283} \begin{pmatrix} \sum P_{11}(X) e^X & \sum P_{12}(X) e^X & \sum P_{13}(X) e^X \\ \sum P_{21}(X) e^X & \sum P_{22}(X) e^X & \sum P_{23}(X) e^X \\ \sum P_{31}(X) e^X & \sum P_{32}(X) e^X & \sum P_{33}(X) e^X \end{pmatrix}$$

$$\sum P(X) e^X \quad \text{signifiant} \quad \sum_{X \in \mathcal{P}(P_F)} P(X) e^X \quad \text{avec} \quad \mathcal{P}(P_F) = \{X_1, X_2, X_3\}.$$

$$\text{avec} \quad \left\{ \begin{array}{l} P_{11}(X) = 64 X^2 - 24 X + 265 \\ P_{12}(X) = -P_{31}(X) = -24 X^2 + 9 X - 64 \\ P_{13}(X) = -P_{21}(X) = -P_{32}(X) = 9 X^2 + 32 X + 24 \\ P_{22}(X) = P_{33}(X) = -32 X^2 + 12 X + 9 \\ P_{23}(X) = 12 X^2 + 137 X + 32 \end{array} \right.$$

ce qui prouve là encore , qu'il est inutile de travailler dans le corps de décomposition  $\mathbb{Q}[X_1, X_2, X_3]$ .

Daniel Lazard donne une généralisation de ce résultat dans [ Lazard ,1985 ], en démontrant le théorème suivant :

### Théorème

Les coefficients de l'exponentielle d'une matrice  $A$  d'ordre  $n$ , sont de la forme :

$$\sum_{X \in \mathcal{r}(P_A)} Q_X(X) e^X$$

les  $Q_X(X)$  étant des polynômes en  $X$ , et  $\mathcal{r}(P_A)$  l'ensemble des racines distinctes du polynôme caractéristique de  $A$ .

On peut énoncer le résultat suivant, un peu plus précis, car on trouve généralement dans cette somme, plusieurs polynômes égaux :

si  $P_A = P_1 P_2^2 \dots P_k^k$  est le polynôme caractéristique de  $A$

les  $P_i$  étant premiers entre eux deux à deux et sans facteurs carrés, alors les coefficients de l'exponentielle de  $A$  sont de la forme

$$\sum_{X \in \mathcal{r}(P_1)} Q_1(X) e^X + \dots + \sum_{X \in \mathcal{r}(P_k)} Q_k(X) e^X$$

les degrés des polynômes  $Q_i$  vérifiant la relation  $\deg(Q_i) < \deg(P_i)$ .

### Remarque :

Il est intéressant de rapprocher la représentation des coefficients de  $e^F$ , de celle que l'on rencontre en intégration formelle lorsqu'on recherche une primitive d'une fraction rationnelle

$$\frac{P(X)}{Q(X)}$$

avec  $P$  et  $Q$  deux polynômes premiers entre eux, tels que  $\deg P < \deg Q$  et  $Q$  sans facteurs carrés. Nous avons alors

$$\int \frac{P(X)}{Q(X)} dx = \sum_{X \in \mathcal{r}(Q)} R(\alpha) \ln(X - \alpha) \quad \text{avec} \quad R(\alpha) = \frac{P(\alpha)}{Q'(\alpha)}$$

$\mathcal{r}(Q)$  étant l'ensemble des racines distinctes de  $Q(X)$ .

## Conclusion

Après avoir rappelé comment déduire la forme de Jordan d'une matrice  $A$ , à partir de la forme de Frobenius, nous donnons explicitement une matrice de passage  $P$  entre ces deux formes normales. Les éléments de  $P$  sont alors des nombres algébriques appartenant au corps de décomposition  $\mathbb{K}[X_1, \dots, X_n]$  du polynôme caractéristique de  $A$ , mais dont chacun d'entre eux peut se représenter comme un élément de  $\mathbb{K}[X]$ ,  $X \in \{X_1, \dots, X_n\}$ . Cette remarque nous permet de donner un algorithme efficace de calcul de l'inverse de  $P$ .

Deux nouveaux algorithmes de calcul de la forme de Frobenius sont présentés dans les chapitres II et III. Nous démontrons que la complexité du second algorithme (chapitre III) est polynomiale, lorsque les éléments de la matrice sont rationnels. Dans ce cas, la représentation d'une matrice  $A$  par un entier "den" et une matrice d'entiers  $A'$  telle que

$$A = \frac{1}{\text{den}} A'$$

est très intéressante en pratique, de nombreux résultats le prouvent.

Une étude particulière est consacrée, dans le chapitre IV, au cas des matrices dont les éléments sont des nombres algébriques sur  $\mathbb{Q}$ .

### Recherches futures :

- Peut-on trouver des algorithmes plus efficaces pour des matrices particulières ( triangulaire, tridiagonale, creuse ) ?
- Peut-on envisager des algorithmes probabilistes ?
- Comment traiter le cas des matrices dépendant d'un ou plusieurs paramètres ?



## **ANNEXE**

Exemples de matrices test .

Nous allons donner dans cette partie les matrices que nous avons utilisées dans les différents exemples . Pour tester les algorithmes présentés , il est nécessaire de disposer d'un ensemble de matrices dont la forme de Frobenius n'est pas triviale. Les noms des matrices sont de la forme " \$ - n " , où \$ est une chaîne de caractères , et n l'ordre de la matrice .

Nous décrirons la forme de Frobenius  $\text{diag} ( C_1 , \dots , C_k )$  d'une matrice , en donnant l'ordre des matrices compagnons  $C_i$  , ainsi que les polynômes  $P_i$  associés aux blocs  $C_i$  .

Pour décrire la forme de Jordan d'une matrice , nous employerons la notation  $J_k ( \lambda )$  pour désigner le bloc d'ordre k associé à une valeur propre  $\lambda$  :

$$J_k ( \lambda ) = \begin{pmatrix} \lambda & 1 & 0 & \dots & 0 \\ 0 & \lambda & 1 & & \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \vdots & & \vdots & \ddots & \vdots \\ \vdots & & & \ddots & 0 \\ \vdots & & & \lambda & 1 \\ 0 & \dots & \dots & 0 & \lambda \end{pmatrix}$$

Les matrices de petites tailles mat-4 , mat -6 , mat - 10 , que nous avons utilisées se trouve dans [ Gregory , Karney , 1969 ] .

#### Matrice mat-4.

$$\text{mat-4} = \begin{pmatrix} 6 & 4 & 4 & 1 \\ 4 & 6 & 1 & 4 \\ 4 & 1 & 6 & 4 \\ 1 & 4 & 4 & 6 \end{pmatrix}$$

Cette matrice est diagonalisable et ses valeurs propres sont : 15 , 5 , 5 , -1 .

Sa forme de Frobenius est  $\text{diag} ( C_1 , C_2 )$  ,  $C_1$  et  $C_2$  étant d'ordre 3 et 1.

$$P_1 = X^3 - 19X^2 + 55X + 75 = (X - 15)(X - 5)(X + 1)$$

$$P_2 = X - 5$$

**Matrice mat-6,**

$$\text{mat-6} = \begin{pmatrix} -9 & 21 & -15 & 4 & 2 & 0 \\ -10 & 21 & -14 & 4 & 2 & 0 \\ -8 & 16 & -11 & 4 & 2 & 0 \\ -6 & 12 & -9 & 3 & 3 & 0 \\ -4 & 8 & -6 & 0 & 5 & 0 \\ -2 & 4 & -3 & 0 & 1 & 3 \end{pmatrix}$$

Les valeurs propres sont : 3, 2 + i, 2 - i, 1.

Sa forme de Jordan est  $\text{diag}(J_2(1), J_1(3), J_1(3), J_1(2+i), J_1(2-i))$ .

La forme de Frobenius de mat-6 et donc  $\text{diag}(C_1, C_2)$ ,  $C_1$  et  $C_2$  étant d'ordre 5 et 1.

$$P_1 = (X - 3)(X - 1)^2(X^2 - 4X + 5)$$

$$P_2 = (X - 3)$$

**Matrice mat-10,**

$$\text{mat-10} = \begin{pmatrix} 1 & 1 & 1 & -2 & 1 & -1 & 2 & -2 & 4 & -3 \\ -1 & 2 & 3 & -4 & 2 & -2 & 4 & -4 & 8 & -6 \\ -1 & 0 & 5 & -5 & 3 & -3 & 6 & -6 & 12 & -9 \\ -1 & 0 & 3 & -4 & 4 & -4 & 8 & -8 & 16 & -12 \\ -1 & 0 & 3 & -6 & 5 & -4 & 10 & -10 & 20 & -15 \\ -1 & 0 & 3 & -6 & 2 & -2 & 12 & -12 & 24 & -18 \\ -1 & 0 & 3 & -6 & 2 & -5 & 15 & -13 & 28 & -21 \\ -1 & 0 & 3 & -6 & 2 & -5 & 12 & -11 & 32 & -24 \\ -1 & 0 & 3 & -6 & 2 & -5 & 12 & -14 & 37 & -26 \\ -1 & 0 & 3 & -6 & 2 & -5 & 12 & -14 & 36 & -25 \end{pmatrix}$$



Les valeurs propres de mat-10 sont : 1, 2 et 3.

La forme de Jordan est :  $\text{diag} (J_3(2), J_2(2), J_2(3), J_2(3), J_1(1))$ .

La forme de Frobenius est :  $\text{diag} (C_1, C_2)$ ,  $C_1$  et  $C_2$  d'ordre 6 et 4.

$$P_1 = (X - 1)(X - 2)^3(X - 3)^2$$

$$P_2 = (X - 2)^2(X - 3)^2$$

### Matrice mat1-20.

Nous avons construit la matrice mat1-20 d'ordre 20, en partant de sa forme de Frobenius, puis en effectuant des transformations élémentaires afin d'obtenir une matrice pleine.

Les valeurs propres sont :

$$0, 5, -5, 5i, -5i, 4 + 3i, 4 - 3i, \sqrt[3]{2}, j\sqrt[3]{2}, j^2\sqrt[3]{2}$$

La forme de Frobenius est  $\text{diag} (C_1, C_2, C_3)$ , les  $C_i$  étant d'ordre 15, 4, 1, avec :

$$P_1 = X^3 (X - 5)(X + 5)(X^2 + 25)(X^2 - 8X + 25)(X^3 - 2)^2$$

$$P_2 = X^2 (X^2 - 8X + 25)$$

$$P_3 = X$$

mat1-20

|     |    |     |     |     |     |     |     |     |     |     |     |    |    |     |     |     |     |     |     |
|-----|----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|----|----|-----|-----|-----|-----|-----|-----|
| -10 | -9 | -51 | 2   | 1   | 14  | 29  | -54 | -16 | -17 | -17 | -53 | 0  | 2  | -8  | 38  | -43 | -1  | -10 | -15 |
| 5   | 0  | 0   | -20 | -22 | -10 | 12  | 0   | 54  | -8  | -5  | -23 | 0  | -2 | -30 | 12  | 22  | -4  | 5   | -2  |
| 3   | 6  | 27  | -38 | -57 | -14 | -1  | 29  | -5  | 4   | 4   | -28 | -1 | 1  | -12 | -7  | -21 | 12  | 3   | 10  |
| 3   | 3  | -25 | 0   | 0   | -5  | -10 | -24 | 46  | 5   | 5   | -24 | 0  | 1  | -40 | -13 | 3   | 0   | 3   | 5   |
| 2   | 0  | 60  | -60 | -30 | 8   | 35  | 60  | -28 | 0   | 1   | 30  | 2  | 0  | 84  | 10  | 2   | -30 | 2   | 0   |
| 3   | 3  | 1   | -6  | -3  | -5  | -9  | 2   | 29  | 5   | 5   | -1  | 0  | -2 | -14 | -12 | 3   | -3  | 3   | 5   |
| 6   | 6  | 0   | 0   | 0   | 0   | -24 | 2   | 0   | 12  | 12  | 3   | 0  | 4  | 0   | -30 | 6   | 1   | 6   | 12  |
| 1   | -2 | 16  | -21 | 27  | 17  | 26  | 15  | 11  | 1   | 1   | 42  | 5  | -1 | 64  | 3   | 26  | -42 | 1   | -5  |
| 3   | 3  | 0   | 0   | 0   | -5  | -10 | 1   | 21  | 5   | 5   | 1   | 0  | 1  | -15 | -13 | 3   | 0   | 3   | 5   |
| -1  | -1 | -25 | -8  | -3  | 1   | 0   | -25 | 37  | -4  | -4  | -28 | -2 | 0  | -25 | 1   | -52 | -7  | -2  | 0   |
| 0   | 0  | 0   | 10  | 4   | -1  | 0   | 0   | -14 | 4   | 4   | 4   | 0  | 0  | 0   | 0   | 50  | 8   | 1   | 0   |
| -4  | -4 | -35 | 60  | 30  | -3  | -25 | -36 | -14 | -5  | -5  | -6  | -4 | -1 | -44 | 4   | -5  | 30  | -4  | -5  |
| 0   | 0  | -4  | 24  | 12  | 0   | -4  | -4  | -20 | 0   | 0   | 8   | 0  | 0  | -4  | -4  | 0   | 12  | 0   | 0   |
| 3   | 3  | 0   | 0   | 0   | -5  | -10 | 1   | 21  | 5   | 5   | 1   | 0  | 1  | -15 | -13 | 3   | 0   | 3   | 5   |
| 3   | 3  | 0   | 0   | 0   | -5  | -10 | 1   | 20  | 5   | 5   | 1   | 0  | 2  | -15 | -13 | 3   | 0   | 3   | 5   |
| 0   | -6 | -8  | -1  | 0   | 0   | 24  | -10 | 25  | -16 | -13 | -11 | 0  | -4 | -8  | 30  | 0   | -5  | 0   | -12 |
| 1   | 0  | 0   | 0   | 0   | 0   | 0   | 0   | 0   | 2   | 2   | 0   | 0  | 0  | 0   | 0   | 9   | 2   | 1   | 0   |
| 4   | 4  | 25  | 0   | 0   | -5  | -10 | 26  | -4  | 5   | 5   | 26  | 2  | 1  | 10  | -14 | 5   | 0   | 4   | 5   |
| 3   | 3  | 51  | -6  | -3  | -4  | -9  | 52  | -23 | 5   | 5   | 49  | 0  | -4 | 39  | -12 | 3   | -3  | 3   | 5   |
| 13  | 1  | 9   | -4  | -1  | 0   | 0   | 9   | 27  | -8  | -2  | 8   | 2  | 0  | 9   | -1  | 14  | -9  | 13  | 0   |

**Matrice mat - 20.**

Nous pouvons construire des matrices d'ordre  $2n$ , à partir de deux matrices d'ordre  $n$ , en utilisant la proposition suivante :

**Proposition 1 :**

Si  $A$  et  $B$  sont deux matrices d'ordre  $n$ , et  $a, b, c, d$  quatre entiers tels que  $ad - bc = 1$ , alors les matrices :

$$F = \begin{array}{|c|c|} \hline A & 0 \\ \hline 0 & B \\ \hline \end{array} \quad \text{et} \quad G = \begin{array}{|c|c|} \hline ad A - bc B & bd (A - B) \\ \hline ac (B - A) & ad B - bc A \\ \hline \end{array}$$

sont semblables .

**démonstration :**

On peut choisir comme matrice de passage la matrice suivante :

$$P = \begin{array}{|c|c|} \hline a I_n & b I_n \\ \hline c I_n & d I_n \\ \hline \end{array}$$

où  $I_n$  représente la matrice identité d'ordre  $n$ .

Nous avons construit mat - 20 en prenant pour A la matrice mat - 10 et pour B la matrice :

$$B = \begin{array}{|c|c|} \hline \begin{array}{c} 2 \ 1 \\ 2 \ 1 \\ 2 \ 1 \\ 2 \end{array} & \begin{array}{c} 0 \\ 0 \\ 0 \\ 0 \end{array} \\ \hline \begin{array}{c} 0 \\ 0 \\ 0 \\ 0 \end{array} & \begin{array}{c} \begin{array}{|c|c|} \hline 1 \ 1 \\ \hline 1 \end{array} \\ \begin{array}{|c|c|} \hline 1 \ 1 \\ \hline 1 \end{array} \\ \begin{array}{|c|c|} \hline 1 \ 1 \\ \hline 1 \end{array} \\ \begin{array}{|c|c|} \hline 1 \ 1 \\ \hline 1 \end{array} \\ \hline \end{array} \end{array}$$

les entiers a , b , c , d étant respectivement égaux à 1 , 1 , 1 , 2 .

Les valeurs propres de mat-20 sont : 1 , 2 , 3 .

La forme de Jordan est :

diag (J<sub>4</sub> ( 2 ) , J<sub>3</sub> ( 2 ) , J<sub>2</sub> ( 2 ) , J<sub>2</sub> ( 3 ) , J<sub>2</sub> ( 3 ) , J<sub>2</sub> ( 1 ) , J<sub>2</sub> ( 1 ) , J<sub>2</sub> ( 1 ) , J<sub>1</sub> ( 1 ) ) .

La forme de Frobenius est diag ( C<sub>1</sub> , C<sub>2</sub> , C<sub>3</sub> , C<sub>4</sub> ) , les matrices C<sub>i</sub> étant d'ordre 8 , 7 , 4 , 1 , avec :

$$P_1 = (X - 1)^2 (X - 2)^4 (X - 3)^2$$

$$P_2 = (X - 1)^2 (X - 2)^3 (X - 3)^2$$

$$P_3 = (X - 1)^2 (X - 2)^2$$

$$P_4 = (X - 1)$$

### Matrice mat-40.

Une autre méthode intéressante de construction de matrice consiste à utiliser le produit de Kronecker de deux matrices .

Si  $A$  et  $B$  sont des matrices respectivement d'ordre  $n$  et  $p$  , avec  $A = (\alpha_{i,j})$  , on appelle produit de Kronecker de  $A$  et  $B$  la matrice :

$$K = A \times B = \begin{pmatrix} \alpha_{11} B & . & . & . & . & \alpha_{1n} B \\ . & & & & & . \\ . & & & & & . \\ . & & & & & . \\ \alpha_{n1} B & . & . & . & . & \alpha_{nn} B \end{pmatrix}$$

### Proposition 2 :

*Si  $J$  est une matrice semblable à  $A$  , alors  $A \times B$  est semblable à  $J \times B$  .*

La matrice mat-40 est le produit de Kronecker  $A \times B$  , où  $B$  désigne la matrice mat-10 , d'ordre 10 , définie dans cette annexe , et  $A$  la matrice d'ordre 4 suivante :

$$A = \begin{pmatrix} -1 & -2 & 4 & -1 \\ 16 & 4 & -2 & 8 \\ 22 & 1 & 1 & 11 \\ 0 & 4 & -8 & 1 \end{pmatrix}$$

dont les valeurs propres sont :  $-1, 1, 2, 3$  .

On déduit de la proposition 2 , les propriétés suivantes de mat-40 :

$$1) \text{ mat-40 est semblable à : } \begin{pmatrix} -B & 0 & 0 & 0 \\ 0 & B & 0 & 0 \\ 0 & 0 & 2B & 0 \\ 0 & 0 & 0 & 3B \end{pmatrix}$$

2) ses valeurs propres sont :  $9, 6, 4, 3, 2, 1, -1, -2, -3$ .

3) sa forme de Jordan :

$$\begin{aligned} \text{diag} ( & J_2(9), J_2(9) , \\ & J_3(6), J_2(6), J_2(6) , J_2(6) , \\ & J_3(4), J_2(4) , \\ & J_2(3), J_2(3), J_1(3) , \\ & J_3(2), J_2(2), J_1(2) , \\ & J_1(1) , \\ & J_1(-1) , \\ & J_3(-2), J_2(-2) , \\ & J_2(-3), J_2(-3) ). \end{aligned}$$

4) sa forme de Frobenius  $\text{diag} (C_1, C_2, C_3, C_4)$ , les matrices  $C_i$  étant d'ordre  $20, 14, 4, 2$ , avec :

$$P_1 = (X-9)^2 (X-6)^3 (X-4)^3 (X-3)^2 (X-2)^3 (X-1)(X+1)(X+2)^3 (X+3)^2$$

$$P_2 = (X-9)^2 (X-6)^2 (X-4)^2 (X-3)^2 (X-2)^2 (X+2)^2 (X+3)^2$$

$$P_3 = (X-6)^2 (X-3) (X-2)$$

$$P_4 = (X-6)^2$$

### Matrice matalg-3.

$$\text{matalg-3} = \begin{pmatrix} 2X+1 & 0 & X \\ X^2-X & 2X+1 & X+3 \\ 0 & 0 & 2X+1 \end{pmatrix}$$

Les coefficients de matalg-3 sont des nombres algébriques, représentés par des polynômes en  $X$ ,  $X$  vérifiant la relation :

$$X^3 - X = 0$$

Matalg-3 possède une seule valeur propre :  $2X + 1$ , mais il faut distinguer au moins deux cas pour décrire sa forme de Jordan  $J$  :

1) Si  $X^2 - X = 0$ ,  $J = \text{diag} (J_2(2X + 1), J_1(2X + 1))$

2) Si  $X + 1 = 0$ ,  $J = J_3(-1)$ .

#### Matrice matalg-4.

Nous pouvons également construire des matrices en utilisant le théorème des restes chinois.

Supposons que  $E$  soit une extension définie par

$$\begin{cases} P_1(X_1) = 0 \\ \dots\dots\dots \\ P_{n-1}(X_1, \dots, X_{n-1}) = 0 \end{cases}$$

nous avons le théorème des restes chinois :

Théorème 1 : Supposons que  $E$  soit un corps, et que  $A_1, A_2, Q_1, Q_2$  soient des polynômes en  $X_n$  à coefficients dans l'extension  $E$ .

Si  $Q_1$  et  $Q_2$  sont premiers entre eux, alors le système

$$\begin{cases} A(X_n) \equiv A_1(X_n) \quad \text{modulo } Q_1(X_n) \\ A(X_n) \equiv A_2(X_n) \quad \text{modulo } Q_2(X_n) \end{cases}$$

admet une unique solution  $A(X_n)$  telle que  $\deg A < \deg Q_1 + \deg Q_2$ .

Ce théorème semble inutilisable en pratique, car l'hypothèse  $E$  est un corps est généralement trop difficile à vérifier. Toutefois, nous pouvons calculer à l'aide de l'algorithme d'Euclide, les polynômes  $K_1$  et  $K_2$  tels que

$$K_1 Q_1 + K_2 Q_2 = 1$$

Si aucun scindage ne se produit lors de ce calcul, nous obtenons la solution du système :

$$A = A_1 + K_1 Q_1 \cdot (A_2 - A_1).$$

Passons maintenant aux cas des matrices .

Théorème 2 :

Soit  $E$  une extension de niveau  $n - 1$  définie par  $P_1, \dots, P_{n-1}$ .

Soient  $Q_1$  et  $Q_2$  deux polynômes en  $X_n$ , à coefficients dans  $E$ , premiers entre eux, et tels que le calcul du PGCD ( $Q_1, Q_2$ ) ne provoque aucun scindage.

Soient  $M_1$  et  $M_2$  deux matrices dont les coefficients appartiennent respectivement aux extensions de niveau  $n$

$$E_1 = (P_1, \dots, P_{n-1}, Q_1) \quad \text{et} \quad E_2 = (P_1, \dots, P_{n-1}, Q_2)$$

Alors il existe une unique matrice  $M$  dont les coefficients appartiennent à l'extension  $E' = (P_1, \dots, P_{n-1}, Q_1 \cdot Q_2)$  de niveau  $n$ , telle que

$$\left\{ \begin{array}{ll} M \equiv M_1 & \text{modulo } Q_1 \\ M \equiv M_2 & \text{modulo } Q_2 \end{array} \right. \\ \text{et } \deg M_{i,j} < \deg Q_1 \cdot \deg Q_2$$

Ainsi, si les formes de Jordan ( ou de Frobenius ) des matrices  $M_1$  et  $M_2$  ont des structures différentes, il y aura au moins un scindage lors du calcul de la forme de Jordan de  $M$ .

La matrice matalg-4 est construite à l'aide de deux matrices  $A$  et  $B$  d'ordre 4, qui se trouvent dans [ Gregory, Karney, 1969 ] :

1)

$$A = \begin{pmatrix} 7 & 3 & 1+2X & -1+2X \\ 3 & 7 & 1-2X & -1-2X \\ 1-2X & 1+2X & 7 & -3 \\ -1-2X & -1+2X & -3 & 7 \end{pmatrix}$$

où  $X$  vérifie la relation  $X^2 + 1 = 0$ .

$A$  est diagonalisable, et ses valeurs propres sont : 0, 8, 8, 12.



2)

$$B = \begin{pmatrix} -2 & 2 & 2 & 2 \\ -3 & 3 & 2 & 2 \\ -2 & 0 & 4 & 2 \\ -1 & 0 & 0 & 5 \end{pmatrix}$$

Les valeurs propres de B sont : 1, 2, 3, 4.

Les coefficients de la matrice matalg-4 appartiennent à l'extension de niveau 1  $E = (P_1)$  avec  $P_1 = X^4 - 3X^2 - 4 = (X^2 + 1) \cdot (X^2 - 4)$  et

$$\begin{cases} \text{matalg-4} \equiv A \text{ modulo } X^2 + 1 \\ \text{matalg-4} \equiv B \text{ modulo } X^2 - 4 \end{cases}$$

### Matrice mat1alg-4.

Elle est construite à l'aide des matrices :

1) matalg-4 définie ci-dessus, considérée comme une matrice à coefficients dans  $E_1 = (P_1, Q_1)$  avec  $P_1(X) = X^4 - 3X^2 - 4$  et  $Q_1(X, Y) = Y^2 - X$ .

2)

$$C = \begin{pmatrix} Y & 0 & 0 & 0 \\ 0 & 2 & -Y & 0 \\ 0 & 0 & Y & 0 \\ 0 & 4Y - Y^2 & -2Y^2 & Y \end{pmatrix}$$

considérée comme une matrice à coefficients dans  $E_2 = (P_1, Q_2)$  avec  $P_1(X) = X^4 - 3X^2 - 4$  et  $Q_2(X, Y) = Y^2 + 3XY + 1$ .

Les valeurs propres de C sont 2 et Y, et sa forme de Jordan est :

$$J = \text{diag} ( J_2(Y), J_1(Y), J_1(2) ).$$

Les coefficients de la matrice  $\text{mat1alg-4}$  appartiennent à l'extension  $E' = (P_1, Q_1, Q_2)$  et

$$\left\{ \begin{array}{ll} \text{mat1alg-4} = \text{matalg-4} & \text{modulo } Q_1(X, Y) = Y^2 - X \\ \text{mat1alg-4} = C & \text{modulo } Q_2(X, Y) = Y^2 + 3XY + 1 \end{array} \right.$$

Nous donnons page suivante l'expression des 4 coefficients de la première ligne de  $\text{mat1alg-4}$ .

a(1,1);

$$\begin{aligned} & (-1500y^3x^3 + 31251y^3x^2 + 6165y^3x^3 - 137379y^2x^3 + 98675y^2x^3 - 4922y^2x^2 \\ & - 437875y^2x^2 + 25738y^2x^2 - 31251y^3x^3 - 1665y^3x^2 + 137379y^2x^3 + \\ & 6000y^3x^3 - 9917y^2x^2 - 25738y^2x^2 + 43738y^2x^2)/84315 \end{aligned}$$

a(1,2);

$$\begin{aligned} & (110y^3x^3 + 16789y^3x^2 + 110y^3x^3 - 52196y^2x^3 + 54680y^2x^3 - 4313y^2x^2 \\ & - 175270y^2x^2 + 18682y^2x^2 - 16789y^3x^3 - 440y^3x^2 + 52196y^2x^3 - 440y^2x^2 \\ & 4313y^3x^3 - 5633y^2x^2 - 18682y^2x^2 + 17362y^2x^2)/84315 \end{aligned}$$

a(1,3);

$$\begin{aligned} & (9308y^3x^3 + 7591y^3x^2 - 36682y^3x^3 - 15404y^2x^3 + 20954y^2x^3 - 31907y^2x^2 \\ & x^2 - 40366y^2x^2 + 129058y^2x^2 - 7591y^3x^3 + 8758y^3x^2 + 15404y^2x^3 - 37232y^2x^2 \\ & - 1819y^3x^3 - 5633y^2x^2 + 5846y^2x^2 + 17362y^2x^2)/84315 \end{aligned}$$

a(1,4);

$$\begin{aligned} & (9308y^3x^3 - 1607y^3x^2 - 36682y^3x^3 + 21388y^2x^3 - 9706y^2x^3 - 28841y^2x^2 \\ & + 82274y^2x^2 + 116794y^2x^2 + 1607y^3x^3 + 8758y^3x^2 - 21388y^2x^3 - 37232y^2x^2 \\ & 4885y^3x^3 - 2567y^2x^2 + 18110y^2x^2 + 5098y^2x^2)/84315 \end{aligned}$$

## sommaire

|                                                                                                                |        |
|----------------------------------------------------------------------------------------------------------------|--------|
| <u>Introduction.</u>                                                                                           | p . 5  |
| <u>Chap I Lien entre forme de Frobenius et forme de Jordan d'une matrice.</u>                                  | p . 9  |
| 1 Rappels.                                                                                                     | p . 10 |
| 2 Description d'une matrice de passage entre la forme de Frobenius et la forme de Jordan , et de son inverse . | p . 15 |
| <u>Chap II Premier algorithme pour le calcul de la forme de Frobenius d'une matrice.</u>                       | p . 27 |
| 1 Introduction                                                                                                 | p . 28 |
| 2 Transformations élémentaires "type semblable" .                                                              | p . 28 |
| 3 La procédure "polymine1".                                                                                    | p . 29 |
| 4 La procédure "zéroadroite".                                                                                  | p . 34 |
| 5 Obtention de la forme de Frobenius.                                                                          | p . 36 |
| 6 Résultats lorsque $\mathbb{K} = \mathbb{F}_p$ et $\mathbb{K} = \mathbb{Q}$ .                                 | p . 44 |
| 7 Un algorithme modulaire pour le cas $\mathbb{K} = \mathbb{Q}$ .                                              | p . 47 |
| <u>Chap III Deuxième algorithme pour le calcul de la forme de Frobenius d'une matrice.</u>                     | p . 57 |
| 1 Introduction                                                                                                 | p . 58 |
| 2 Polynôme minimal d'un vecteur.                                                                               | p . 60 |
| 3 Polynôme minimal d'un ensemble de vecteurs .                                                                 | p . 62 |
| 4 Recherche d'un vecteur dont le degré du polynôme minimal est maximal.                                        | p . 72 |
| 5 Forme de Frobenius .                                                                                         | p . 77 |
| 6 Le cas particulier $\mathbb{K} = \mathbb{Q}$ , complexité polynomiale de l'algorithme .                      | p . 90 |
| 7 Une modification lorsque $\mathbb{K} = \mathbb{Q}$ .                                                         | p . 96 |

|                                                                                                                                           |         |
|-------------------------------------------------------------------------------------------------------------------------------------------|---------|
| <u>Chap IV Calcul de la forme de Frobenius et de la forme de Jordan d'une matrice dont les coefficients sont des nombres algébriques.</u> | p . 113 |
| 1 Présentation du système D5 .                                                                                                            | p . 114 |
| 2 Forme de Frobenius d'une matrice dont les coefficients sont des nombres algébriques.                                                    | p . 118 |
| 3 Représentation de la forme de Jordan d'une matrice .                                                                                    | p . 126 |
| <u>Conclusion.</u>                                                                                                                        | p . 131 |
| <u>Annexe</u> Exemples de matrices test .                                                                                                 | p . 133 |
| <u>Sommaire.</u>                                                                                                                          | p . 147 |
| <u>Références Bibliographiques.</u>                                                                                                       | p . 149 |

### Références bibliographiques

- [Bennett , 1931 ] Bennett A. A. Construction of a rational canonical form for a linear transformation.  
American Mathematical Monthly . p. 377-383 .
- [Browne , 1940 ] Browne E. T. On the reduction of a matrix to a canonical form. American Mathematical Monthly . p. 437-450 .  
( rational canonical form . Jordan canonical form . Jacobson canonical form )
- [Curtis , 1974 ] Curtis Charles W. Linear algebra An introductory approach . Springer-Verlag .
- [ Danilewski , 1937 ] Danilewski A. . O Cislennom Resenii Vekovogo Uravnenija . Mat . Sbornik 2 . p 169 - 171 .
- [ Della Dora , Di Crescenzo , Duval , 1985 ] . Della Dora Jean , Di Crescenzo Claire , Duval Dominique . About a new method for computing in algebraic number fields .  
Proc. Eurocal 1985 p. 289 . Springer-Verlag .
- [ Dickson , 1926 ] Dickson L. E. Modern algebraic theories  
Benj. H. Sanborn & co 1926
- [Di Crescenzo , Duval , 1987 ] Di Crescenzo Claire , Duval Dominique .  
Le système D5 de calcul formel avec des nombres algébriques .
- [ Di Crescenzo , Duval , 1985 ] Di Crescenzo Claire , Duval Dominique .  
Algebraic computations on algebraic numbers .  
Informatique et Calcul . Wiley-Masson 1985 .
- [ Di Crescenzo , Duval , 1985 ] Di Crescenzo Claire , Duval Dominique .  
Calculs algébriques avec des nombres algébriques : exemples .  
CALSYF4 1985 , p. 3-28 . Editeur M. Mignotte , Strasbourg .
- [ Gantmacher , 1966 ] Gantmacher F.R. Théorie des matrices . Tome I .  
Dunod Paris 1966 .
- [ Gastinel , 1966 ] Gastinel Noël . Analyse numérique linéaire .  
Herman .

- [Gregory , Karney , 1969 ] Gregory R. T. and Karney D. L.  
A collection of matrix for testing computational algorithms .  
Wiley - interscience .
- [ Hilton , 1909 ] Hilton Harold . On the canonical form of a linear substitution.  
The messenger of mathematics . p. 24-26 .  
( Jordan canonical form )
- [ Howell , 1971 ] Howell J. A. S. . On the reduction of a matrix to Frobenius  
form using residue arithmetic.  
The university of Texas at Austin , Ph D . Computer science.
- [ Jacobson , 1953 ] Jacobson Nathan . Lectures in Abstract Algebra .  
II Linear algebra . Springer - Verlag .
- [ Kagstrom , Ruhe , 1980 ] Kagstrom Bo , Ruhe Axel  
An algorithm for numerical computation of the Jordan Normal form  
of a complex matrix .  
ACM Transactions on mathematical Software . Vol 6 , n°3 ,  
September 1980 , p. 398 - 419 .
- [ Kannan , Bachem , 1979 ] Kannan Ravindran and Bachem Achim .  
Polynomial algorithms for computing the Smith and Hermite normal  
forms of an integer matrix .  
Siam J. Computing , Vol 8 , n° 4 , November 1979 .
- [ Krishnamoorthy , Saunders , 1985 ] Krishnamoorthy M. Saunders B. D.  
Hermite normal form for matrices of polynomials.
- [ Lazard , 1985 ] Lazard Daniel .  
Maniement des nombres algébriques : Le calcul de l'exponentielle  
d'une matrice est-il exponentiel ?  
Séminaire d'informatique théorique . 10 décembre 1985 .  
L.I.T.P. Université PARIS VI 75252 PARIS .
- [ Lipson , 1981 ] Lipson J. D. Elements of algebra and algebraic computing.  
Addison-Wesley Publishing Compagny .
- [ Mac Duffee , 1956 ] Mac Duffee C. C. The theory of matrices.  
Chelsea Publishing Compagny .
- [ Newman , 1972 ] Newman M. Integral matrices . Academic press
- [ Ozello , 1986 ] Ozello Patrick . Forme de Frobenius d'une matrice .  
RR 578 IMAG , Janvier 1986 .

- [ Ruhe , 1970 ] Ruhe Axel . An algorithm for numerical determination of the structure of a general matrix . BIT 10 , 1970 , p. 196 - 216 .
- [ Schreier , Sperner , 1959 ] Schreier O. , Sperner E.  
Introduction to modern algebra and matrix theory.  
Chelsea Publishing Compagny .
- [ Wilkinson , 1965 ] Wilkinson J.H. The algebraic eigenvalue problem .  
Clarendson Press . Oxford .





AUTORISATION DE SOUTENANCE

DOCTORAT 3ème CYCLE, DOCTORAT-INGENIEUR, DOCTORAT USTMG

Vu les dispositions de l'Arrêté du 16 avril 1974,

Vu les dispositions de l'Arrêté du 5 juillet 1984,

Vu les rapports de M.r..D..LAZARD.....

M.r..E..ROBERT.....

Mr.P..OZELLO..... est autorisé  
à présenter une thèse en vue de l'obtention du grade de Docteur de.....  
l'Université Scientifique Technologique et Médicale de Grenoble  
.....

Grenoble, le 15 JAN. 1987.....

Le Président de l'Université Scientifique  
Technologique et Médicale



  
M. TANCHE

