REVUE FRANÇAISE D'INFORMATIQUE ET DE RECHERCHE OPÉRATIONNELLE. SÉRIE ROUGE

JEAN-PIERRE DUPORT
RENÉ DUSSAUD

Introduction à la classification automatique des corps de nombres algébriques

Revue française d'informatique et de recherche opérationnelle. Série rouge, tome 3, n° R3 (1969), p. 71-84

<http://www.numdam.org/item?id=M2AN_1969__3_3_71_0>

© AFCET, 1969, tous droits réservés.

L'accès aux archives de la revue « Revue française d'informatique et de recherche opérationnelle. Série rouge » implique l'accord avec les conditions générales d'utilisation (http://www.numdam.org/conditions). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM
Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
http://www.numdam.org/

R.I.R.O.
(3e année, No R-3, 1969, p. 71-84)

INTRODUCTION A LA CLASSIFICATION AUTOMATIQUE DES CORPS DE NOMBRES ALGEBRIQUES

par Jean-Pierre DUPORT et René DUSSAUD (1)

Résumé. — *On énumère dans le présent article quelques théorèmes issus du théorème fondamental de la théorie de Galois et axés généralement sur l'emploi de résolvantes non normales. Les conditions énoncées ne font intervenir en général que le corps de base : appliquées à Q elles permettent la détermination en calcul automatique du groupe de Galois de l'équation considérée. On montre ensuite que les méthodes générales se simplifient dans le cas où le degré n de l'équation n'est pas trop élevé. A titre d'exemple on indique la procédure pour* $n = 4$.

Si l'étude des extensions abéliennes semble avoir acquis une forme quasi définitive depuis les travaux qui ont conduit à l'élaboration de la théorie du corps de classes, des difficultés apparaissent déjà dans l'approche des problèmes soulevés par les extensions galoisiennes de degré non premier et semblent encore croître dès que l'ordre du groupe de l'équation est supérieur au degré du corps. On a pu obtenir récemment une classification des équations du troisième degré : cela suffit à montrer que les progrès restent lents avec les méthodes actuelles qui utilisent non seulement le corps factorisant de l'équation mais aussi des irrationnelles accessoires. Les théorèmes énoncés ci-dessous opèrent au contraire et généralement sur le corps de base : nous avons pu en tester quelques-uns, nous essaierons ultérieurement de distinguer ceux d'entre eux qui conduisent à la programmation la plus rationnelle. Nous indiquons ensuite quelques applications simples aux corps du 3e et du 4e degré; une variante des méthodes générales est employée enfin pour obtenir une classification des corps de degré quatre.

(1) Collège Scientifique Universitaire de Chambéry.

I. RAPPELS

Soient les polynômes $f(x)$ et $g(x)$ éléments de $K[x]$; K corps commutatif :

$$(1)\quad f(x) = \sum_{i=0}^{i=n} a_i x^{n-i}; \qquad (2)\quad g(x) = x^p - \sum_{i=1}^{i=p} b_i x^{p-i}$$

Nous avons désigné par « division *euclidienne* généralisée de longueur k » de $f(x)$ par $g(x)$ [3 p 15] l'opération définie par :

$$f(x) = g(x)[A_0^0 x^{n-p} + A_1^0 x^{n-p-1} + \dots + A_{k-1}^0 x^{n-p-k+1}]$$
$$+ A_k^0 x^{n-k} + A_{k+1}^1 x^{n-k-1} + \dots + A_{k+p-1}^{p-1} x^{n-p-k+1} + a_{k+p} x^{n-p-k} + \dots + a_n$$

En comparant à la division euclidienne généralisée de longueur $k+1$ on obtient dans l'espace K^p :

$$(3)\quad \begin{Vmatrix} A_{k+1}^0 \\ \cdot \\ \cdot \\ \cdot \\ \cdot \\ A_{k+m+1}^m \\ \cdot \\ \cdot \\ \cdot \\ \cdot \\ A_{k+p}^{p-1} \end{Vmatrix} = \begin{Vmatrix} b_1 & 1 \dots 0 \\ b_2 & 0 \dots 0 \\ \dots & \dots \\ \dots & \dots \\ b_{p-1} & 0 \dots 1 \\ b_p & 0 \dots 0 \end{Vmatrix} \times \begin{Vmatrix} A_k^0 \\ \cdot \\ \cdot \\ \cdot \\ \cdot \\ A_{k+m}^m \\ \cdot \\ \cdot \\ \cdot \\ \cdot \\ A_{k+p-1}^{p-1} \end{Vmatrix} + \begin{Vmatrix} 0 \\ \cdot \\ \cdot \\ \cdot \\ \cdot \\ 0 \\ \cdot \\ \cdot \\ \cdot \\ 0 \\ a_{k+p} \end{Vmatrix}$$

On a notamment pour les p divisions euclidiennes de $f(x)$, $xf(x)$; ...; $x^{p-1}f(x)$, par $g(x)$:

$$(4)\quad \begin{cases} f(x) = g(x) \cdot q(x) + A_{n-p+1}^0 x^{p-1} + \dots + A_n^{p-1} \\ x \cdot f(x) = g(x) \cdot q_1(x) + A_{n-p+2}^0 x^{p-1} + \dots + A_{n+1}^{p-1} \\ \dots\dots\dots\dots\dots\dots\dots\dots \\ x^{p-1} \cdot f(x) = g(x) \cdot q_{p-1}(x) + A_n^0 x^{p-1} + \dots + A_{n+p-1}^{p-1} \end{cases}$$

Soit la matrice M_f à éléments dans K :

$$(5)\quad M_f = \begin{Vmatrix} A_{n-p+1}^0 & A_{n-p+2}^1 \dots A_n^{p-1} \\ A_{n-p+2}^0 & A_{n-p+3}^1 \dots A_{n+1}^{p-1} \\ \dots\dots\dots & \dots\dots\dots \\ A_n^0 & A_{n+1}^0 \quad \dots A_{n-1+p}^{p-1} \end{Vmatrix}$$

et la matrice $M_f^{-\frac{\pi}{2}}$ déduite de M_f par rotation de $\frac{-\pi}{2}$ autour de son centre.

On a :

(6) $M_f^{-\frac{\pi}{2}} = f(m)$ $\quad m = \begin{Vmatrix} b_1 & 1 & . & 0 \\ b_2 & 0 & . & 0 \\ \cdots & \cdots & \cdots & \cdots \\ . & . & . & . \\ . & . & . & . \\ b_{p-1} & 0 & . & 1 \\ b_p & 0 & . & 0 \end{Vmatrix}$

m matrice de Frobenius relative à $g(x)$

En utilisant la chaîne des mineurs principaux de M_f :

(7) $d_0 = 1\ d_1 = A^0_{n-p+1} \ldots d_k = \begin{vmatrix} A^0_{n-p+1} \ldots A^{k-1}_{n-p+k} \\ \cdots \\ A^0_{n-p+k} \ldots A^{k-1}_{n-p+2k-1} \end{vmatrix} \ldots d_p = \text{det. } M_f$

On démontre que :

a) d_p est le résultant de $f(x)$ et $g(x)$,

b) si $f(x)$ et $g(x)$ admettent comme p.g.c.d. $D(x)$ de degré $p - c$ on a :

(8) $D(x) = \begin{vmatrix} A^0_{n-p+1} \ldots A^{c-2}_{n-p+c-1} & , & A^{c-1}_{n-p+c} & x^{p-c} + \ldots + A^{p-1}_n \\ \cdots & & & \cdots \\ A^0_{n-p+c} \ldots A^{c-2}_{n-p+2c-2} & , & A^{c-1}_{n-p+2c-1} x^{p-c} + \ldots & A^{p-1}_{n+c-1} \end{vmatrix}$

avec $d_c \neq 0$; $d_{c+1} = d_{c+2} = \ldots = d_p = 0$.

c) que l'on peut symétriser M_f sous la forme :

(9) $M_f \cdot S = \begin{Vmatrix} A^0_{n-p+1} & A^0_{n-p+2} \ldots A^0_n \\ \cdots & \cdots \\ A^0_n & A^0_{n+1} \ldots A^0_{n+p-1} \end{Vmatrix} = L$

La matrice L a comme éléments les coefficients directeurs des restes des divisions de $f(x)$, $xf(x) \ldots x^{2p-2}f(x)$ par $g(x)$ et la matrice S a pour éléments de sa première ligne les coefficients directeurs des restes de la division de x^{p-1}, $x^p \ldots x^{2p-2}$ par $g(x)$, pour les autres lignes on décale les éléments de la ligne précédente de un rang vers la droite et on complète par des zéros :

(10) $S = \begin{Vmatrix} 1 & b_1 & \alpha_2 & \ldots & \alpha_{p-1} \\ 0 & 1 & b_1 & \ldots & \alpha_{p-2} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & \ldots & 1 \end{Vmatrix}$

d) que la matrice M_q relative au quotient $q(x)$ de la division euclidienne ordinaire de $f(x)$ par $g(x)$ est :

$$M_q = \left\| \begin{matrix} \dfrac{\delta A^0_{n-p+1}}{\delta b_p} & \cdots & \dfrac{\delta A^{p-1}_n}{\delta b_p} \\ \cdots\cdots & & \cdots\cdots \\ \dfrac{\delta A^0_{n-p+1}}{\delta b_1} & \cdots & \dfrac{\delta A^{p-1}_n}{\delta b_1} \end{matrix} \right\| \tag{11}$$

e) que les coefficients $A^0_{n-p+1} \ldots A^{p-1}_n$ satisfont aux « conditions d'analycité » :

$$\frac{\delta \vec{R}_n}{\delta b_1} = m \frac{\delta \vec{R}_n}{\delta b_2} = \ldots = m^{p-1} \frac{\delta \vec{R}_n}{\delta b_p} ; \vec{R}_n : \left| \begin{matrix} A^0_{n-p+1} \\ A^1_{n-p+1} \\ \cdots\cdots \\ A^{p-1}_n \end{matrix} \right. \tag{12}$$

II. THEOREMES GENERAUX

Nous désignons par « division euclidienne généralisée » la suite d'algorithmes qui conduisent à la formation de M_f, du résultant de $f(x)$ et de $g(x)$ et du p.g.c.d. de $f(x)$ et $g(x)$. Le polynôme $g(x)$ est unitaire et caractéristique de l'extension $K(\theta)$, les racines de $g(x) = 0$ sont : $\theta = x_0$; $x_1 \ldots x_{p-1}$.

Théorème I (*p premier*). *Par division euclidienne généralisée de :*

$$f(x, A_0, \ldots, A_{p-1}, y) = \sum_{i=0}^{i=p-1} A_i x^{p-1-i} - y \tag{13}$$

par $g(x)$ on obtient $R(y)$ déterminant de M_f tel que $R(y)$ soit identique à $g(y)$ pour des systèmes rationnels $(A_0, A_1 \ldots A_{p-1})$ autres que (0, 0, ... 0, 1, 0) *si et seulement si l'extension $K(\theta)$ est cyclique.*

En utilisant les mêmes notations on obtient :

Théorème II (*p non premier*)

$R(y)$ est identique à $g(y)$ pour des systèmes rationnels autres que (0, 0, ..., 0, 1, 0) *si et seulement si l'extension $K(\theta)$ est galoisienne.*

En effet si $K(\theta)$ est galoisienne par rapport à K le théorème fondamental de la théorie classique de Galois nous indique que tout automorphisme T de $K(\theta)$ par rapport à K est tel que $T(\theta) = x_i$; $x_1, x_2 \ldots x_{p-1}$ sont donc des fonctions rationnelles de θ de la forme : $\sum_{i=0}^{i=p-1} A_i x^{p-1-i}$; les théorèmes I et II traduisent simplement la propriété d'invariance d'une équation algébrique par

les p isomorphismes qui permutent les racines et tiennent compte en même temps du fait que pour tout corps galoisien ces isomorphismes constituent tous les automorphismes de $K(\theta)$ par rapport à K. Notons enfin que l'emploi de la division euclidienne généralisée et des méthodes d'élimination qui en découlent évite l'introduction de solutions étrangères; le nombre de systèmes rationnels prévu par les théorèmes précédents coïncide avec le nombre p d'automorphismes du corps.

Pour p non premier les groupes des corps galoisiens de degré p n'étant pas tous isomorphes le théorème II est insuffisant pour les caractériser. Cependant les p automorphismes de $K(\theta)$ par rapport à : $K : T_0, T_1, \ldots T_{p-1}$ transforment θ suivant : $T_0(\theta) = \theta$, $T_1(\theta) = x_1 \ldots T_{p-1}(\theta) = x_{p-1}$, d'où :

Théorème III : *Pour toute extension galoisienne $K(\theta)$ de degré p par rapport à K les p automorphismes de $K(\theta)$ par rapport à K transforment :*

$$x_1 = \sum_{i=0}^{i=p-1} A_i x_0^{p-1-i} \tag{14}$$

en p équations de la forme :

$$T_j(x_1) = \sum_{i=0}^{i=p-1} A_i T_j(x_0^{p-1-i}) \Leftrightarrow x_k = \sum_{i=0}^{i=p-1} A_i x_j^{p-1-i}$$

On obtient ainsi un système (S) de p équations à p inconnues $A_0 A_1 \ldots A_{p-1}$ qui admet une solution rationnelle.

EXEMPLE : Extensions galoisiennes du 4e degré.

a) *Cas cyclique.* On a le système :

$$x_1 = A_0 x_0^3 + A_1 x_0^2 + A_2 x_0 + A_3 \quad , \quad x_2 = A_0 x_1^3 + A_1 x_1^2 + A_2 x_1 + A_3$$

$$x_3 = A_0 x_2^3 + A_1 x_2^2 + A_2 x_2 + A_3 \quad , \quad x_0 = A_0 x_3^3 + A_1 x_3^2 + A_2 x_3 + A_3$$

b) *Groupe de type* (2, 2) : $(x_0)(x_1)(x_2)(x_3)$; $(x_0, x_1)(x_2, x_3)$; $(x_0, x_2)(x_1, x_3)$; $(x_0, x_3)(x_1, x_2)$.

$$x_1 = A_0 x_0^3 + A_1 x_0^2 + A_2 x_0 + A_3 \qquad x_0 = A_0 x_1^3 + A_1 x_1^2 + A_2 x_1 + A_3 ;$$

$$\overline{x_3 = A_0 x_2^3 + A_1 x_2^2 + A_2 x_2 + A_3} \quad , \quad \overline{x_2 = A_0 x_3^3 + A_1 x_3^2 + A_2 x_3 + A_3}$$

On peut étendre les résultats précédents à l'étude de toute équation quel que soit l'ordre de son groupe. Par exemple une équation métacyclique (p premier) peut s'étudier à partir de :

$$y = \sum_{i=0}^{i=p-1} x_0^{p-1-i} \sum_{j=0}^{j=p-2} A_{ij} x_1^{p-2-j} \tag{15}$$

En effet en utilisant :

$$g(x_0) = 0 \tag{16}$$

$$\left[\frac{g(x)}{x - x_0}\right]_{x=x_1} = 0 \tag{17}$$

et par élimination de x_0 et x_1 entre (15), (16) et (17) on voit que le résultant $R(A_{00}, \ldots A_{(p-1)(p-2)}, y)$ est divisible par $g(y)$ pour des systèmes rationnels A_{ij} autres que celui qui correspond à l'automorphisme identique.

Les théorèmes qui viennent d'être énoncés présentent l'avantage d'opérer uniquement sur le corps de base; leur programmation en entiers est donc possible. Il est facile cependant d'obtenir des méthodes applicables sur des corps intermédiaires $K(\alpha)$ $K \subset K(\alpha) \subset K(\theta)$. Par exemple pour p premier, $K(j)$ étant le corps d'adjonction obtenu à partir de la racine primitive $p^{\text{ième}}$ j de l'unité on a :

Théorème IV. *Par division euclidienne généralisée de :*

$$U^{p-1} - xU^{p-2} + \alpha_2 U^{p-3} + \ldots + \alpha_{p-2}U + \alpha_{p-1} \tag{18}$$

par $U^p - z$ *on obtient l'équation* $F(x, z, \alpha_2, \ldots \alpha_{p-1}) = 0$. *Les polynômes* $F(x)$ et $g(x)$ *sont identiques pour* $z, \alpha_2 \ldots \alpha_{p-1}$ *éléments de* $K(j)$ *si et seulement si* $K(\theta)$ *est une extension cyclique.*

Citons enfin une conséquence importante des théorèmes I et III relative à la norme de certains éléments des modules incomplets du corps $K(\theta)$:

Théorème V. Appliquons à :

$$\lambda_1 = x_1 - x_2 = \sum_{i=0}^{i=p-1} A_i x_0^{p-1-i} - \sum_{i=0}^{i=p-1} A_i x_1^{p-1-i} \quad , \quad p \text{ premier} \; ; \; g(x) \in Z[x]$$

les p automorphismes du groupe cyclique $K(\theta)$:

$$T_0(\lambda_1) = \lambda_1, \; T_1(\lambda_1) = \lambda_2; \ldots; \; T_{p-1}(\lambda_1) = \lambda_p$$

On a :

$$F(A_0 \; ; \; A_1 \; ; \; \ldots \; ; \; A_{p-2}) = \frac{\lambda_1 \lambda_2 \ldots \lambda_{p-1} \lambda_p}{(x_1 - x_2) \ldots (x_{p-1} - x_0)(x_0 - x_1)} = 1 \tag{19}$$

Les solutions entières du système (S) *formé à partir de* (14) *si elles existent, fournissent des solutions entières pour* (19).

REMARQUES : *a*) Il est possible à partir d'une solution entière de (19) d'obtenir des unités de modules complets de $K(\theta)$.

b) $F(A_0, A_1 \ldots, A_{p-2})$ est rationnellement indécomposable.

c) Si p n'est pas premier on peut énoncer un théorème analogue pour les extensions — abéliennes ou non — à condition qu'elles soient galoisiennes, mais $F(A_0, A_1 \ldots A_{p-2})$ peut être rationnellement décomposable.

III. APPLICATIONS

Nous allons étudier à titre d'exemples des applications aux corps algébriques de degré trois et de degré quatre.

A) *Corps du 3e degré :* Équation réduite $x^3 + px + q = 0$; $[p, q \in Q]$.

a) Cas cyclique : La résolution du système S (th. 3) $A_2 = A$, $A_1 = B$, $A_0 = C$ conduit à :

$$q = -\frac{(2B+1)[3+(2B+1)^2]}{4C^3}; \qquad p = -\frac{3[3+(2B+1)^2]}{4C^2}$$

Si u et v sont deux entiers naturels premiers entre eux on voit qu'il existe dans toute extension cyclique de degré 3 au moins un polynôme caractéristique de la forme :

$$x^3 - 3(u^2 - uv + v^2)X - (2u - v)(u^2 - uv + v^2)$$

On peut ensuite distinguer les extensions cycliques grâce au critère suivant :

Théorème VI

Une condition nécessaire et suffisante pour que les équations :

$Z^3 + PZ + Q = 0$, $H = \sqrt{\Delta} = \sqrt{-4P^3 - 27Q^2}$; H, P, Q, rationnels

$T^3 + P_1T + Q_1 = 0$, $H_1 = \sqrt{\Delta_1} = \sqrt{-4P_1^3 - 27Q_1^3}$; H_1, P_1, Q_1 rationnels

définissent la même extension cyclique est que l'une des équations :

$$(21) \qquad S^3 - PP_1S + \tfrac{1}{2}[Q_1H + \varepsilon QH_1] = 0 \qquad \varepsilon = \pm 1$$

admette une solution rationnelle.

Le groupe de Galois de chacune des équations (21) est d'ordre trois; si l'une d'elles admet une racine rationnelle elle se décompose entièrement.

b) Parallèlement au cas abélien on montre que lorsque le groupe de Galois d'une équation du 3e degré est d'ordre six, il existe au moins un polynôme caractéristique de la forme :

$$(22) \qquad X^3 - \frac{hm^2 + 27n^2}{4} \cdot X + n\frac{hm^2 + 27n^2}{4} = 0$$

m et n étant des entiers naturels, h un entier relatif dont la décomposition en facteurs premiers ne contient que des exposants égaux à l'unité.

On a enfin le critère :

Théorème VII. *Une condition nécessaire et suffisante pour que les équations non abéliennes :*

$$Z^3 + PZ + Q = 0; \qquad P, Q \text{ nombres rationnels}$$
$$T^3 + P_1T + Q_1 = 0; \qquad P_1, Q_1 \text{ nombres rationnels}$$

définissent la même extension est que l'une des équations :

(23)
$$\gamma^3 + \frac{PP_1\gamma}{4P^3 + 27Q^2} + \frac{Q_1}{4P^3 + 27Q^2} + \frac{\varepsilon Q}{2(4P^3 + 27Q^2)}\sqrt{\frac{4P_1^3 + 27Q_1^3}{4P^3 + 27Q^2}} = 0$$

admette une solution rationnelle.

On en déduit immédiatement que h (équation 22) est un invariant du corps et l'étude peut se poursuivre comme dans les méthodes classiques.

Dans le cas abélien par exemple, on obtient rapidement les résultats essentiels sur le discriminant du corps et les idéaux de l'extension [1], [4, chap. 21].

B) *Corps du 4e degré :* Par décomposition de l'équation générale du 4e degré en facteurs quadratiques [2] on obtient à partir de l'équation réduite :

(24) $$f(x) = x^4 + a_2x^2 + a_3x + a_4 = 0$$

les résultats suivants.

La division de $f(x)$ par $x^2 - ux - v$ à coefficients indéterminés conduit à :

$$f(x) = (x^2 - ux - v)q(x) + x[2uv + u^3 + a_2u + a_3] + v^2 + v(u^2 + a_2) + a_4$$

avec :

$$A_3^0 = 2uv + u^3 + a_2u + a_3; \qquad A_4^1 = v^2 + v(u^2 + a_2) + a_4$$

On élimine v entre les équations $A_3^0 = 0$ et $A_4^1 = 0$:

(25) $$u^6 + 2a_2u^4 + (a_2^2 - 4a_4)u^2 - a_3^2 = 0$$

et par $z = u^2$ on obtient :

(26) $$z^3 + 2a_2z^2 + (a_2^2 - 4a_4)z - a_3^2 = 0$$

Soit z_0 une solution de l'équation (26) et u_0 et u_1 les racines carrées de z_0 : $u_1 = -u_0$. On a :

$$V_0 = -\frac{u_0^3 + a_2u_0 + a_3}{2u_0} \qquad V_1 = -\frac{-u_0^3 - a_2u_0 + a_3}{2u_0}$$

et

(27) $$f(x) = (x^2 - u_0x - V_0)(x^2 - u_1x - V_1)$$

Étudions le groupe de Galois de l'équation (24).

1° L'équation (26) définit une extension non galoisienne du 3e degré; le groupe de (24) est d'ordre 24.

2° L'équation (26) définit une extension galoisienne du 3e degré; le groupe de (24) est d'ordre 12.

3° L'équation (26) admet une racine rationnelle et une seule ; le groupe de (24) est d'ordre 8.

4° L'équation (26) admet trois racines rationnelles; le groupe de (24) est d'ordre 4.

Nous pouvons en effet supposer que :

$$z_0 = -(x_0 + x_1)^2 \qquad \text{(par numérotation convenable des racines)}$$

et que $z_1 = -(x_0 + x_2)^2$, $z_2 = -(x_0 + x_3)^2$; $x_0 + x_1 = -(x_2 + x_3)$; les substitutions du groupe symétrique de degré 4 induisent sur l'ensemble $(z_0 z_1 z_2)$ les six substitutions du groupe symétrique de degré 3, les substitutions du groupe alterné de degré 4 induisent sur l'ensemble $(z_0 z_1 z_2)$ les trois permutations du groupe alterné de degré 3; les substitutions du groupe P d'ordre 8 : $(x_0)(x_1)(x_2)(x_3)$; (x_0, x_2); (x_1, x_3); $(x_0, x_2)(x_1, x_3)$; $(x_0, x_1)(x_2, x_3)$; $(x_0, x_3)(x_1, x_2)$; (x_0, x_3, x_2, x_1); (x_0, x_1, x_2, x_3) conservent z_1 et permutent z_0 et z_2.

Enfin les substitutions du groupe d'ordre 4 de type (2, 2) : $(x_0)(x_1)(x_2)(x_3)$; $(x_0, x_1)(x_2, x_3)(x_0, x_2)(x_1, x_3)$, $(x_0, x_3)(x_1, x_2)$ laissent invariants z_0, z_1 et z_2; or la classification précédente ne fait apparaître nulle part les groupes cycliques d'ordre 4. Utilisons la fonction de Lagrange :

$$\begin{aligned}(x_0 + ix_1 - x_2 - ix_3)^4 &= (x_0 - x_2)^4 + (x_1 - x_3)^4 - 6(x_0 - x_2)^2(x_1 - x_3)^2 \\ &\quad + 4i(x_0 - x_2)(x_1 - x_3)[(x_0 - x_2)^2 - (x_1 - x_3)^2] = A + iB\end{aligned}$$

On voit que A appartient au groupe P; B caractérise donc le groupe cyclique; la racine z_1 doit être rationnelle ainsi que B. On a :

$$\begin{aligned} x_0 + x_2 &= \sqrt{z_1} & x_0 + x_1 &= \sqrt{z_0} & x_0 + x_3 &= \sqrt{z_2} \\ x_1 + x_3 &= -\sqrt{z_1} & x_2 + x_3 &= -\sqrt{z_0} & x_1 + x_2 &= -\sqrt{z_2} \end{aligned}$$

d'où :

$$x_0 - x_2 = \sqrt{z_2} + \sqrt{z_0} \qquad x_1 - x_3 = \sqrt{z_0} - \sqrt{z_2};$$

$$B = 16(z_0 - z_2)\sqrt{z_0 z_2}; \qquad \left(\frac{B}{16}\right)^2 = (z_0 - z_2)^2 z_0 z_2$$

D'autre part z_0 et z_2 vérifient l'équation :

$$\frac{z^3 + 2a_2z^2 + (a_2^2 - 4a_4)z - a_3^2}{z - z_1}$$

$$= z^2 + (2a_2 + z_1)z + z_1^2 + 2a_2z_1 + a_2^2 - 4a_4 = 0$$

d'où :

$$(z_0 - z_2)^2 = -3z_1^2 - 4a_2z_1 + 16a_4;$$

$$z_0z_2 = \frac{a_3^2}{z_1}; \qquad a_4 = \frac{z_1^3 + 2a_2z_1^2 + a_2^2z - a_3^2}{4z_1}$$

$$(z_0 - z_2)^2 = \frac{z_1^3 + 4a_2z_1^2 + 4a_2^2z - 4a_3^2}{4z_1}$$

Finalement on voit que si le groupe de Galois de l'équation (24) est cyclique une racine z_1 est rationnelle et l'expression :

$$z_1^3 + 4a_2z_1^2 + 4a_2^2z_1 - 4a_3^2$$

est le carré d'un nombre rationnel.

On a donc les résultats généraux ci-dessous concernant l'équation du 4e degré :

Théorème VIII : *Soit l'équation irréductible du 4e degré :*

$$(E) f(x) = x^4 + a_2x^2 + a_3x + a_4 = 0; \qquad f(x_i) = 0 \qquad i = 0, 1, 2, 3$$

et sa résolvante du 3e degré :

$$(R) : z^3 + 2a_2z^2 + (a_2^2 - 4a_4)z - a_3^2 = 0$$

Le groupe de Galois de (E) est :

a) *d'ordre* 24 *si et seulement si (R) est une équation non cyclique du* 3e *degré,*

b) *d'ordre* 12 *si et seulement si (R) est une équation cyclique du* 3e *degré,*

c) *d'ordre* 8 *si et seulement si (R) admet une racine rationnelle et une seule,*

d) *d'ordre* 4 *et de type* (2, 2) *si et seulement si (R) admet trois racines rationnelles,*

e) *d'ordre* 4 *et cyclique si et seulement si (R) admet une racine rationnelle et une seule* z_1 *telle que :* $z_1^3 + 4a_2z_1^2 + 4a_2^2z_1 - 4a_3^2$ *soit le carré d'un nombre rationnel.*

Remarques :

a) Les invariants signalés dans les exemples du paragraphe II conduisent à une classification analogue.

b) Si le groupe de l'équation est d'ordre 24, l'adjonction d'une racine z_0 au corps de base fournit une extension non galoisienne $K(z_0)$; en utilisant les

résultats relatifs aux équations cycliques, on voit la possibilité d'opérer par extensions non galoisiennes.

c) Nous étudierons ultérieurement les problèmes arithmétiques liés aux corps de degré quatre. Notons cependant que les fonctions résolvantes de Lagrange et les idéaux essentiels ne semblent pas fournir la solution la plus directe pour les corps cycliques de degré non premier.

IV. ESSAI DE CLASSIFICATION AUTOMATIQUE

A partir de l'étude qui précède nous allons construire un programme nous permettant de connaître l'ordre du groupe de Galois associé à une équation du type : $X^4 + AX^3 + BX^2 + CX + D = 0$ que nous supposerons ramenée par changement de variable $x = X + \frac{A}{4}$ à l'expression

$$f(x) = x^4 + a_2x^2 + a_3x + a_4 = 0 \qquad \text{avec } a_2, a_3, a_4 \text{ entiers de } Z.$$

Nous nous proposons d'effectuer les opérations suivantes :

1° Par division euclidienne généralisée de $f'(x) = 4x^3 + 2a_2x + a_3$ par $f(x)$ on forme le résultant de $f'(x) = 0$ et $f(x)$ qui n'est autre que le discriminant de $f(x)$.

2° Soit Δ le discriminant obtenu dans l'opération précédente sous forme de tableau à 16 éléments. Nous calculons la valeur du déterminant correspondant.

Ces deux calculs vont s'effectuer à partir d'une fonction de procédure incluant la procédure de calcul d'un déterminant à éléments entiers et la procédure de la division euclidienne généralisée (ces deux procédures ayant été construites dans un travail antérieur).

Dans cette procédure OBELIX (A, C, N, P) nous appellerons A la matrice standard associée au polynôme $f(x)$:

$$A = \begin{Vmatrix} 0 & 1 & 0 & 0 \\ -a_2 & 0 & 1 & 0 \\ -a_3 & 0 & 0 & 1 \\ -a_4 & 0 & 0 & 0 \end{Vmatrix} \quad A \text{ sera de dimension } P$$

C sera la matrice uniligne des coefficients du polynôme $f'(x)$ de dimension N.

```
    entier procédure OBELIX (A, C, N, P); entier tableau A, C; entier N, P;
début entier procédure DET (A, P); entier tableau A; entier P;
    début entier I, J, K, L, Q; Q : = 1;
        pour  K : = 1 pas 1 jusqua P — 1 faire
        début E1 : si A [K, K] = 0 alors allera E2;
              pour I : = K + 1 pas 1 jusqua P faire
              pour J : = E + 1 pas 1 jusqua P faire
              A[I, J] : = (A[I, J]*A[K, K] — A[K, J]*A[I, K])
                ÷ (si K = 1 alors 1 sinon A[K — 1, K — 1]);
              allera E3;
              E2 : début entier M; M : = K + 1;
                        pour L : = M tantque ((A[L, K] = 0) ∧ (L ⩽ P))
                          faire
                        M : = M + 1;
                        si M = P + 1 alors allera E4;
                        pour J : = K pas 1 jusqua P faire
                        début L : = A[K, J];
                              A[K, J] : = A[M, J] :
                              A[M, J] : = L;
                        fin; Q : = — Q; allera E1;
                   fin; E3 :
        fin; DET : = [A[P, P]*Q; allera E5;
        E4 : DET : = 0; E5 :
    fin DET;
    entier I, J, K, M; entier tableau B[1 : P, 1 : P], D[1 : P];
    pour I : = 1 pas 1 jusqua P faire
    pour J : = 1 pas 1 jusqua P faire
    B[I, J] : = C[0]* A[I, J] + si I = J alors C[1] sinon 0;
    pour K : = 2 pas 1 jusqua N faire
    début pour I : = 1 pas 1 jusqua P faire
        début M : = 0; pour J : = 1 pas 1 jusqua P faire
              début M : = M + B[I, J]* A[J, 1];
                    D[J] : = B[I, J];
              fin;
              pour J : = 1 pas 1 jusqua P faire
              B[I, J] : = (si J = 1 alors M sinon D[J — 1])
                        + si I = J alors C[K] sinon 0;
        fin;
    fin;
        OBELIX : = DET (B, P);
fin OBELIX;
```

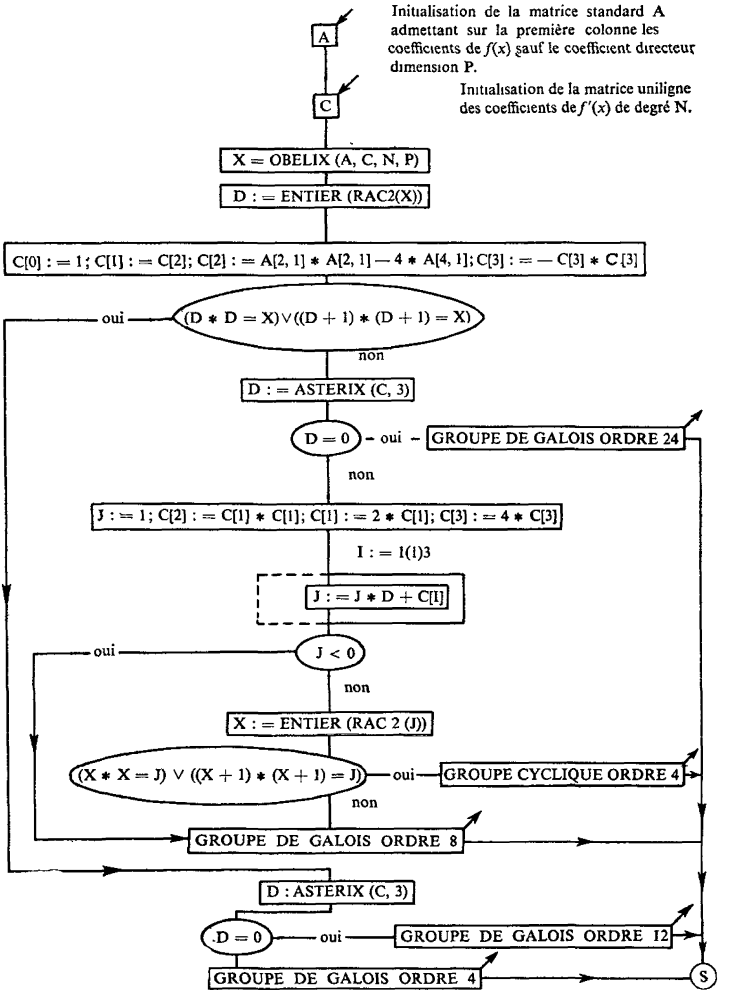
3° On recherche alors si l'équation $V^3 + 2a_2V^2 + (a_2^2 - 4a_4)V - a_3^2 = 0$ admet ou non une racine rationnelle.

A cet effet on construit une fonction de procédure ASTERIX (P, N) où P est un tableau contenant les coefficients du polynôme du degré N. Cette fonction de procédure comprendra une procédure DIV(Q) qui recherche les diviseurs entiers de l'entier Q. En choisissant Q = P[N] c'est-à-dire encore le coefficient constant du polynôme P, on sait que si l'équation donnée (qui est unitaire) admet une racine rationnelle cette racine est un diviseur de son coefficient constant. Dès qu'un diviseur est trouvé, par le schéma de Horner on cherche la valeur du polynôme pour ce diviseur positif et négatif. On sort de la procédure dès que le polynôme s'annule ou que le dernier diviseur essayé est 1.

```
    entier procédure ASTERIX (P, N); entier tableau P; entier N;
début entier procédure DIV(Q); entier Q;
    début entier I, R; I : = — 1;
        E1 : I : = I + 1; si Q — I = 0 alors allera E2;
        R : = Q ÷ (Q — I); si Q — I = 0 alors DIV : = R
                                sinon aller E1;
        E2 : DIV : = 0;
    fin DIV;
    entier I, S, T, X; X : = P[N];
    E1 : X : = DIV(X); si X = 0 alors allera E2;
        S : = T : = P[0];
    pour I : = 1 pas 1 jusqua N faire
    début S : = S * X + P[I] ;
        T : = — T * X + P[I] ;
    fin;
        si (S ≠ 0) ∧ (T ≠ 0) alors allera E1
        sinon si S = 0 alors ASTERIX : = X
            sinon ASTERIX : = — X;
        allera E3; E2 : ASTERIX : = 0; E3 :
fin ASTERIX;
```

4° Il s'agit alors de déterminer par la suite de tests précédemment indiqués l'ordre dans les différents cas du groupe de GALOIS de l'équation. Pour ces opérations nous avons préféré donner un organigramme dans lequel interviennent les fonctions de procédure qui viennent d'être définies.

ORGANIGRAMME



BIBLIOGRAPHIE

1. A. CHATELET, « *Arithmétique des corps abéliens du 3e degré* », *Annales E.N.S. 63*, 1946.
2. R. DUSSAUD, *Décomposition en facteurs de degré quelconque d'un polynôme de degré n* (I.C.N. Toulouse, mai 1963).
3. R. DUSSAUD, *Généralisation des formules de Bairstow et étude des critères de stabilité*, thèse, Toulouse, 1965.
4. D. HILBERT, *Théorie des corps de nombres algébriques.* Traduction de T. Got et A. Levy, Hermann, 1913.