SÉMINAIRE DE THÉORIE DES NOMBRES DE GRENOBLE

ELISABETH GALLOU

Discriminants minimaux successifs pour les corps de nombres algébriques totalement réels de degré n

Séminaire de théorie des nombres de Grenoble, tome 5 (1975-1977), exp. nº 5, p. 1-29
<http://www.numdam.org/item?id=STNG_1975-1977__5__A5_0>

© Institut Fourier – Université de Grenoble, 1975-1977, tous droits réservés.

L'accès aux archives du séminaire de théorie des nombres de Grenoble 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/

Séminaire de Théorie des Nombres
25 novembre et 2 décembre 1976
Grenoble

DISCRIMINANTS MINIMAUX SUCCESSIFS POUR LES CORPS DE NOMBRES ALGEBRIQUES TOTALEMENT REELS DE DEGRE n

par

Elisabeth GALLOU

Le problème est de calculer les discriminants minimaux successifs parmi les discriminants de corps de nombres algébriques totalement réels de degré n donné sur Q .

Les résultats connus sont les suivants :

n	nombre de racines réelles de l'extension F sur Q	valeur minimale de $\lvert D \rvert$ D discriminant de F
2	0 2	3 5
3	1 3	23 49
4	0 2 4	117 275 725
5	1 3 5	1609 4511 14641
6	0 6	9747 300125
7	7	20134393

le cas $n = 3$ a été résolu par Furtwangler en 1896, $n = 4$ par Mayer en 1929, $n = 5$ par Hunter en 1956 [7], $n = 6$ par Kaur en 1970 [8] pour le cas totalement réel et par Liang et Zassenhaus en 1973 [9] pour le cas totalement complexe, $n = 7$ par Pohst pour le cas totalement réel [11]. Siegel a conjecturé que pour les corps totalement réels de degré n le discriminant minimum $a(n)$ est tel que $a(n) = (2n+1)^{n-1}$ si $2n+1$ est premier ; c'est exact pour $n = 2,3,5$. Cohn en 1952, [3] a montré que si $n+1$ et $2n+1$ sont premiers $a(n) < (2n+1)^{n-1}$. On constate que c'est exact pour $n = 6$. Pour $n = 8,9,11$, $2n+1$ est premier et $n+1$ ne l'est pas. On peut se demander si la conjecture de Siegel est exacte dans ces 3 cas.

- I -

A) Dans cette partie n sera un entier naturel supérieur ou égal à 3 quelconque. Soit $F_1 = Q(\theta)$ un corps de nombres algébriques de degré n sur Q. Les F_i, $i = 1,2,\dots,n$ sont les corps conjugués de F_1. Pour ρ_1 entier de F_1 nous appelons ρ_i, $1 \le i \le n$, les conjugués de ρ_1. Posons $\sum_{i=1}^{n} \rho_i = S(\rho_1)$, $\sum_{i=1}^{n} |\rho_i| = S(|\rho_1|)$, $\sum_{i=1}^{n} \rho_i^2 = S(\rho_1^2)$ et $\sum_{i=1}^{n} |\rho_i|^2 = S(|\rho_1|^2)$, (x) est le n-uplet $(x_1,\dots,x_n)$.

THEOREME 1. - <u>Si</u> F_1 <u>est de degré</u> n <u>sur</u> Q <u>et de discriminant</u> D, <u>il existe</u> ρ_1 <u>entier algébrique de</u> F_1 <u>tel que</u> ρ_1 <u>ne soit pas un rationnel et</u>

$$|S(\rho_1)| < [n/2]$$

$$n^{n-1} \le (S|\rho_1|^2)^{n-1} \le \frac{\gamma_n^n}{n} |D| .$$

$\gamma_n = \left(\dfrac{2^n p(1+\frac{n}{2})}{(p(\frac{1}{2}))^n}\right)^{2/n}$. Les valeurs connues de γ_n sont $\gamma_2 = \sqrt{4/3}$, $\gamma_3 = \sqrt[3]{2}$, $\gamma_4 = \sqrt[4]{4}$, $\gamma_5 = \sqrt[5]{8}$, $\gamma_6 = \sqrt[6]{64/3}$, $\gamma_7 = \sqrt[7]{64}$, $\gamma_8 = 2$. Pour les valeurs suivantes nous utiliserons l'inégalité $\gamma_n \le \gamma_{n-1}^{\frac{n-1}{n-2}}$.

COROLLAIRE DU THEOREME 1. - Si F_1 est un corps de nombres algébriques totalement réel de degré n sur Q, de discriminant D il existe ρ_1 entier algébrique de F_1 tel que ρ_1 ne soit pas rationnel et

$$[\tfrac{n}{2}] \leq S(\rho_1) \leq 0$$

$$n+1 \leq S(\rho_1^2) \leq (\frac{\gamma_n^n}{n}|D|)^{\frac{1}{n-1}} .$$

En effet si F_1 est totalement réel les ρ_i sont tous réels donc $\rho_i^2 = |\rho_i|^2$. En remplaçant éventuellement ρ_1 par $-\rho_1$ nous pouvons supposer que $S(\rho_1)$ est négatif. Supposons $S(\rho_1^2) = n$. $|\prod_{i=1}^{n} \rho_i|$ est un entier puisque c'est la valeur absolue de la norme de ρ_1 et cet entier est non nul. Par suite

$$|\prod_{i=1}^{n} \rho_i| \geq 1$$

$S(\rho_1^2) = n$ avec $\prod_{i=1}^{n} \rho_i^2 \geq 1$ entraîne $\rho_i^2 = 1$ pour tout i. Ceci est en contradiction avec le fait que ρ_1 n'est pas rationnel donc $n+1 \leq S(\rho_1^2)$.

Démonstration du théorème 1 : Soit $\omega_1 = (1, \rho_{11}, \rho_{12}, \ldots, \rho_{1n-1})$ une base entière de F_1 ; $\omega_i = (1, \rho_{i1}, \ldots, \rho_{in-1})$ où ρ_{ij} est conjugué de ρ_{1j} est une base entière de F_i. Soit D le discriminant de F_1, $D = \det \omega_1^2$. Soit $X_i = x_1 + \rho_{i1}x_2 + \ldots + \rho_{in-1}x_n$;

$$f((x)) = \sum_{i=1}^{n} |X_i|^2$$

$\prod_{i=1}^{n} |X_i|$ est la valeur absolue de la norme d'un entier algébrique non nul donc $\prod_{i=1}^{n} |X_i| \geq 1$. En appliquant l'inégalité entre moyenne arithmétique et moyenne géométrique nous trouvons

$$\sum_{i=1}^{n} |X_i|^2 \geq n$$

f est une forme quadratique définie positive à coefficients dans $\mathbb{Z}$ de déterminant $|D|$. f a pour minimum n, ce minimum étant atteint en

$(x_1) = (1,0,\dots,0)$. m_2 est le minimum de f sur l'ensemble des entiers (x) non proportionnels à (x_1) . m_2 est atteint en (x_2) . m_3 est le minimum de f sur l'ensemble des (x) entiers qui ne sont pas des combinaisons linéaires de (x_1) et (x_2) . m_3 est atteint en (x_3) et ainsi de suite nous définissons $m_4,\dots,m_n$

$$n \le m_2 \le m_3 \le \dots \le m_n$$

D'après [4] , $m_1 m_2 \dots m_n \le \gamma_n^n |D|$

$$n m_2^{n-1} \le \gamma_n^n |D| \ . \qquad (1)$$

Nous écrivons

$$f((x)) = nx_1^2 + 2 \sum_{\substack{i=1\,j=1 \\ i\neq j}}^{i=n\,j=n} b_{ij} x_i x_j + \sum_{k=2}^{k=n} b_{kk} x_k 2$$

$$f((x)) = n(x_1 + \frac{1}{n} \sum_{k=2}^{n} b_{1k} x_k)^2 + g(x_2,\dots,x_n) \ .$$

Soit $x_2,\dots,x_n$ des entiers donnés non tous nuls , il existe x_1 entier tel que $x_1 + \sum_{k=2}^{n} b_{1k} x_k = 0$ donc $g(nx_2,\dots,nx_n) > 0$ et $g(x_2,\dots,x_n) > 0$. g est une forme quadratique définie positive à $n-1$ variables . $m_2 = f((x_2))$ posons $(x_2) = (\alpha_1,\dots,\alpha_n)$ (x_2) n'étant pas proportionnel à (x_1) les α_i pour i supérieur ou égal à 2 ne sont pas tous nuls . Posons

$$\delta = \text{pgcd}\{\alpha_2,\dots,\alpha_n\} \ .$$

Nous allons montrer que $\delta = 1$.

Supposons $\delta \ge 2$, $\alpha_i = \delta\beta_i$, $2 \le i \le n$,

$$m_2 = f((x_2)) = n(\alpha_1 + \frac{1}{n} \sum_{k=2}^{n} b_{1k} \alpha_k)^2 + \delta^2 g(\beta_1,\dots,\beta_n) \ .$$

Il existe γ tel que

$$|\gamma + \frac{1}{n} \sum_{k=2}^{n} b_{1k} \beta_k| \le \frac{1}{2} \ .$$

Appelons μ_2 le minimum de f pour les (x) entiers tels que $x_i = \beta_i$ pour $i \ge 2$

$$\mu_2 \le \frac{n}{4} + g(\beta_2,\dots,\beta_n) \ .$$

$$\delta^2 g(\beta_2,\dots,\beta_n) \le m_2 = n\,\alpha_1 + \frac{1}{n}\sum_{k=2}^{n} b_{1k}\alpha_k{}^2 + \delta^2 g(\beta_2,\dots,\beta_n) \le \mu_2 \le \frac{n}{4} + g(\beta_2,\dots,\beta_n)$$

donc

$$(\delta^2-1)\,g(\beta_2,\dots,\beta_n) \le \frac{n}{4}$$

$$g(\beta_2,\dots,\beta_n) \le \frac{n}{12}\ .$$

Par suite, $m_2 \le \frac{n}{4} + \frac{n}{12} < n$. Il y a contradiction car $m_2 \ge n$. Nous avons bien montré que $\delta = 1$.

Nous trouvons une matrice entière $n-1 \times n-1$ de déterminant 1 :

$$\begin{pmatrix} \alpha_2 & \lambda_{22} & \cdots & \lambda_{2n-1} \\ \alpha_3 & \lambda_{32} & & \\ \vdots & & & \\ \alpha_n & \lambda_{n2} & \cdots & \lambda_{nn-1} \end{pmatrix}$$

les α_i sont toujours définis par $(x_2) = (\alpha_1,\alpha_2,\dots,\alpha_n)$. Posons

$$x_1 = x'_1 + \alpha_1 x'_2$$

$$x_i = \alpha_i x'_2 + \lambda_{i2}x'_3 + \dots + \lambda_{in-1}x'_n\ .$$

Il s'agit d'une substitution unimodulaire entière. Appliquons-la à $f((x))$

$$f((x)) = \sum_{i=1}^{n} |x'_1 + p_{i1}x'_2 + p_{i2}x'^3 + \dots + p_{i\,n-1}x'_n|^2$$

avec $p_{i1} = \alpha_1 + \rho_{i1}\alpha_2 + \dots + \rho_{i\,n-1}\alpha_n$ et $p_{ij} = \lambda_{2j}\rho_{ij} + \lambda_{3j}\rho_{i2} + \dots + \lambda_{nj}\rho_{i\,n-1}$ pour $j \ge 2$. La substitution étant entière et unimodulaire $(1,p_{11},\dots,p_{1\,n-1})$ est une base entière de F_1 et $(1,p_{i1},\dots,p_{i\,n-1})$ en est une de F_i . Posons $\rho_1 = p_{11}$ et montrons qu'il vérifie les conclusions du théorème 1.

$$f((x)) = \sum_{i=1,j=1}^{i=n,j=n} b_{ij}x'_i x'_j$$

avec $b_{11} = n$, $b_{22} = S(|\rho_1|^2)$ et $2b_{12} = S(\rho_1+\bar{\rho}_1) = 2S(\rho_1)$, $(x_2) = (\alpha_1,\dots,\alpha_n)$ se transforme en $(x'_2) = (0,1,0,\dots,0)$ dans la substitution entière unimodulaire considérée, donc $m_2 = f((x_2)) = b_{22} = S(|\rho_1|^2)$. Par suite, en utilisant (1) nous obtenons

$$n(S(|\rho_1|^2))^{n-1} \leq \gamma_n^n |D| \ .$$

Il reste à montrer que $|S(\rho_1)| \leq [n/2]$ pour terminer la démonstration du théorème 1.

Dans la transformation entière unimodulaire considérée $(x) = (x_1,\ldots,x_n)$ est tel que pour tout i supérieur ou égal à 2, $x_i = 0$, si et seulement si son image $(x') = (x'_1,\ldots,x'_n)$ possède cette propriété. Par suite (x') égal à $(1,1,0,\ldots,0)$ ou à $(1,-1,0,\ldots,0)$ est l'image d'un (x) non proportionnel à $(1,0,0,\ldots,0)$ et donc tel que $f((x)) \geq m_2$. m_2 est égal à b_{22}, nous obtenons par conséquent :

$$b_{11} + 2b_{12} + b_{22} \geq b_{22}$$

et

$$b_{11} - 2b_{12} + b_{22} \geq b_{22}$$

donc

$$|b_{12}| \leq \frac{1}{2} b_{11} \ .$$

Comme $|b_{12}| = |S(\rho_1)|$ et $b_{11} = n$ nous avons montré que $|S(\rho_1)| \leq \frac{n}{2}$ $|S(\rho_1)|$ est un entier. Il est donc inférieur ou égal à la partie entière de $n/2$. Le théorème 1 est démontré.

B) Soit F_1 un corps de nombres algébriques totalement réel, de degré n sur $\mathbb{Q}$, de discriminant D. D'après le corollaire du théorème 1, il existe ρ_1 entier algébrique de F_1 non rationnel tel que

$$-[n/2] \leq S(\rho_1) \leq 0 \qquad (2)$$

et

$$n+1 \leq S(\rho_1^2) \leq \left(\frac{\gamma_n^n}{n} |D|\right)^{\frac{1}{n-1}} \qquad (3)$$

ρ_1 engendre un sous-corps de degré d de F_1 sur $\mathbb{Q}$ où d est un diviseur de n avec éventuellement $d = n$. Il existe donc un polynôme $g(X)$ de $Z[X]$, irréductible dans $Q[X]$, de degré d, ayant d racines réelles distinctes et admettant ρ_1 pour une de ses racines. Le terme de plus haut degré de ce polynôme est x^d.

Notons $g(X) = \sum_{i=0}^{d} a_i X^{d-i}$. Les a_i sont des entiers relatifs,

$a_o = 1$ et les inégalités (2) et (3) nous donnent une majoration et une minoration de a_1 et a_2 en fonction de d et D. Nous allons montrer que les conditions sur $g(X)$ nous permettent de calculer pour chaque a_i une majoration et une minoration en fonction de d et de D. Nous établissons d'abord un théorème valable pour un polynôme de degré d à coefficients entiers.

THEOREME 2. - $g(X)$ <u>polynôme de</u> $Z[X]$ <u>de degré</u> d <u>a</u> d <u>racines réelles distinctes si et seulement si</u> Mg <u>est la matrice d'une forme quadratique définie positive</u>

$$g(X) = \sum_{i=0}^{d} a_i x^{d-i} .$$

Mg <u>est la matrice carrée d'ordre</u> $d-1$ <u>et de coefficients</u> :

$$Mg = (m_{ij})_{\substack{1\le i\le d-1 \\ 1\le j\le d-1}}$$

$$m_{ij} = i(d-j)a_i a_j + \sum_{t=1}^{t=i} d(i-j-2t)a_{j+t}\, a_{i-t} \quad \underline{\text{si}} \quad i+j \le d$$

$$m_{ij} = i(d-j)a_i a_j + \sum_{t=1}^{t=d-j} d(i-j-2t)a_{j+t}\, a_{i-t} \quad \underline{\text{si}} \quad j+i > d .$$

<u>Démonstration du théorème 2</u> : D'après [5], p. 199, $g(X)$ a d racines réelles distinctes si et seulement si les déterminants s_o, $\begin{vmatrix} s_o & s_1 \\ s_1 & s_2 \end{vmatrix}, \ldots, \begin{vmatrix} s_o & s_1 \cdots s_{d-1} \\ \vdots & \\ s_{d-1} & s_d \cdots s_{2d-2} \end{vmatrix}$ sont tous strictement positifs. $s_p = \sum_{i=1}^{d} \alpha_i^p$, $\alpha_1, \alpha_2, \ldots, \alpha_d$ étant les racines de $g(X)$. Posons

$$S_d((x)) = \sum_{i=0,k=0}^{i=d-1,k=d-1} s_{i+k} x_i x_k = \sum_{j=1}^{j=d} (x_o + \alpha_j x_1 + \ldots + \alpha_j^{d-1} x_{d-1})^2 .$$

S_d est une forme quadratique à d variables. S_d est définie positive si et seulement si les déterminants s_o, $\begin{vmatrix} s_o & s_1 \\ s_1 & s_2 \end{vmatrix}, \ldots, \begin{vmatrix} s_o & s_1 \cdots s_{d-1} \\ \vdots & \\ s_{d-1} & s_d \cdots s_{2d-2} \end{vmatrix}$ sont strictement positifs.

$$d\, S_d((x)) = (dx_o + s_1 x_1 + \ldots + s_{d-1} x_{d-1})^2 + h(x_1, \ldots, x_{d-1}) .$$

S_d est une forme quadratique définie positive si et seulement si la forme quadratique à $d-1$ variables h est définie positive. En effet, soit $x_1,\dots,x_{d-1}$ non tous nuls, il existe x_o tel que $x_o+s_1x_1+\dots+s_{d-1}x_{d-1} = 0$. Alors $d\,S_d(x_o,dx_1,\dots,dx_{d-1}) = d^2h(x_1,\dots,x_{d-1})$ ce qui entraîne $h(x_1,\dots,x_{d-1}) > 0$.

Soit A la matrice entière de déterminant 1 suivante :

$$A = \begin{pmatrix} 1 & a_1 & a_2 & \cdots & a_{d-2} \\ & \ddots & \ddots & \ddots & \vdots \\ & & \ddots & \ddots & a_2 \\ & & & \ddots & a_1 \\ 0 & & & & 1 \end{pmatrix}$$

les a_i sont définis par $g(X) = \sum_{i=0}^{d} a_i X^{d-i}$. Considérons la substitution entière unimodulaire qui à $(x_1,\dots,x_{d-1})$ associe $(\zeta_1,\dots,\zeta_{d-1})$ tel que $\begin{pmatrix} x_1 \\ \vdots \\ x_{d-1} \end{pmatrix} = A \begin{pmatrix} \zeta_1 \\ \vdots \\ \zeta_{d-1} \end{pmatrix}$. Nous définissons une nouvelle forme quadratique à $d-1$ variables h' par $h'(\zeta_1,\dots,\zeta_{d-1}) = h(x_1,\dots,x_{d-1})$. La forme quadratique à $d-1$ variables h est définie positive si et seulement si h' est une forme quadratique définie positive. Appelons M_g la matrice de la forme quadratique h' . Nous avons montré que $g(X)$ a d racines réelles distinctes si et seulement si M_g est la matrice d'une forme quadratique définie positive.

<u>Calcul de</u> M_g . Notons H la matrice de la forme quadratique h ,

$$H = (h_{ij})_{\substack{1\le i\le d-1 \\ 1\le j\le d-1}}$$

$$h_{ij} = ds_{i+j} - s_i s_j \ .$$

Posons

$$M_g = (m_{ij})_{\substack{1\le i\le d-1 \\ 1\le j\le d-1}}$$

$$M_g = {}^tA\,H\,A \ .$$

Donc

$$m_{ij} = \sum_{t=1}^{t=i} \sum_{k=1}^{k=j} (ds_{t+k}\, a_{i-t}\, a_{j-k} - s_t s_k a_{i-t} a_{j-k}) \ .$$

Nous utilisons les formules de Newton

$$\begin{aligned} s_p &= -a_1 s_{p-1} \dots -pa_p \quad \text{si} \quad p > d \\ s_p &= -a_1 s_{p-1} \dots -a_d s_{p-d} \quad \text{si} \quad p \leq d \end{aligned} \quad . \qquad (4)$$

Posons

$$B = \sum_{t=1}^{t=i} \sum_{k=1}^{k=j} s_t s_k a_{i-t} a_{j-k}$$

$$B = \sum_{t=1}^{t=i} s_t a_{i-t} \sum_{k=1}^{k=j} s_k a_{j-k}$$

$$B = ij\, a_i a_j \ .$$

Posons

$$C = \sum_{t=1}^{t=i} \sum_{k=1}^{k=j} s_{t+k}\, a_{i-t}\, a_{j-k} \ .$$

<u>Supposons $i+j \leq d$</u> :

Posons

$$C_t = \sum_{k=1}^{k=j} s_{t+k}\, a_{j-k}$$

$$C = \sum_{t=1}^{t=i} C_t\, a_{i-t} \ .$$

$$\begin{aligned} C = & -a_j(a_{i-1}s_1 + a_{i-2}s_2 + \dots + s_i) \\ & -a_{j+1}(a_{i-2}s_1 + a_{i-3}s_2 + \dots + s_i - 1) \\ & \dots\dots\dots\dots\dots\dots\dots\dots \\ & -a_{j+i-1}\, a_o s_1 \\ & -a_{i-1}(j+1)a_{j+1} - a_{i-2}(j+2)a_{j+2} \dots - a_o(j+i)a_{j+i} \ . \end{aligned}$$

$$C = \sum_{t=1}^{t=i} (i-t+1)a_{j+t-1}\, a_{i-t+1} - \sum_{t=1}^{t=i} a_{i-t}(j+t)a_{j+t}$$

$$C = \sum_{t=1}^{t=i-1} (i-j-2t)a_{j+t}\, a_{i-t} + ia_i a_j - (j+i)a_{j+i}\, a_o \ .$$

$m_{ij} = dC - B$ ce qui donne l'expression de m_{ij} écrite dans l'énoncé du théorème 2 .

<u>Supposons $i+j > d$</u> :

Nous posons $C'_t = -a_j s_t \dots - a_d s_{t+j} - d$ et nous effectuons les calculs de façon analogue. Le théorème 2 est démontré.

THEOREME 3. - Soit $g(X)$ un polynôme de degré d, de $Z[X]$ avec $d \geq 3$. $g(X)$ est unitaire, a d racines réelles distinctes et

$$g(X) = \sum_{i=0}^{i=d} a_i x^{d-i} \quad \text{avec} \begin{cases} A_2 \leq a_1 \leq A_1 \\ B_2 \leq a_2 \leq B_1 \end{cases},$$

A_1, A_2, B_1, B_2 étant des entiers relatifs donnés. Alors

$$\forall p \ , \ 3 \leq p \leq d \ , \ \exists (L_{1p}, L_{2p}) \ , \ (L_{1p}, L_{2p}) \in \mathbb{Z}^2 \ , \ L_{2p} < a_p < L_{1p} \ .$$

Démonstration du théorème 3 : Soit p un entier compris entre 2 et d. Appelons $\mathcal{P}(p)$ la propriété suivante :

$$\forall i \ , \ 1 \leq i \leq p \ , \ \exists (L_{1i}, L_{2i}) \ , \ (L_{1i}, L_{2i}) \in \mathbb{Z}^2 \ , \ L_{2i} < a_i < L_{1i} \ .$$

$\mathcal{P}(2)$ est vraie par hypothèse.

Montrons que $\mathcal{P}(p)$ entraîne $\mathcal{P}(p+1)$ si $p+1 \leq d$. Supposons $\mathcal{P}(p)$ vraie et $p+1 \leq d$. Notons $g_{p+1}(x)$ la dérivée d'ordre $d-p-1$ de $g(x)$. $g_{p+1}(x)$ est un polynôme de $Z[X]$, de degré $p+1$ ayant $p+1$ racines réelles distinctes. Appliquons le théorème 2

$$g_{p+1}(x) = \sum_{i=0}^{i=p+1} a'_i x^{p+1-i}$$

avec $a'_i = (d-i) \ldots (p+2-i) a_i$ en particulier $a'_{p+1} = (d-p-1)!\, a_{p+1}$

$$Mg_{p+1} = (m_{ij})_{\substack{1 \leq i \leq p \\ 1 \leq j \leq p}}$$

si $i+j \leq p+1$, $m_{ij} = i(p+1-j) a'_i a'_j + \sum_{t=1}^{t=i} (p+1)(i-j-2t) a'_{j+t} a'_{i-t}$

si $i+j > p+1$, $m_{ij} = i(p+1-j) a'_i a'_j + \sum_{t=1}^{t=p+1-j} (p+1)(i-j-2t) a'_{j+t} a'_{i-t}$.

Alors, Mg_{p+1} est la matrice d'une forme quadratique définie positive.

1) Supposons p pair :

Posons

$$\Delta_{p+1} = \begin{vmatrix} m_{\frac{p}{2}\frac{p}{2}} & m_{\frac{p}{2}\frac{p}{2}+1} \\ m_{\frac{p}{2}\frac{p}{2}+1} & m_{\frac{p}{2}+1\ \frac{p}{2}+1} \end{vmatrix}$$

Δ_{p+1} est strictement positif

$$m_{\frac{p}{2}\frac{p}{2}} = \frac{p}{2}\left(\frac{p}{2}+1\right)a'^{2}_{\frac{p}{2}} - 2(p+1)a'_{\frac{p}{2}+1}\ a'_{\frac{p}{2}-1} \ldots - (p+1)pa'_p a'_o$$

$$m_{\frac{p}{2}\frac{p}{2}+1} = \left(\frac{p}{2}\right)^2 a'_{\frac{p}{2}}\ a'_{\frac{p}{2}+1} - 3(p+1)a'_{\frac{p}{2}+2}\ a'_{\frac{p}{2}-1} \ldots - (p+1)^2 a'_{p+1} a'_o$$

$$m_{\frac{p}{2}+1\frac{p}{2}+1} = \left(\frac{p}{2}+1\right)\frac{p}{2}a'^{2}_{\frac{p}{2}+1} - 2(p+1)\ a'_{\frac{p}{2}+2}\ a'_{\frac{p}{2}} \ldots - (p+1)pa'_{p+1}a'_1$$

Δ_{p+1} est un polynôme du second degré en a'_{p+1} tel que le coefficient de a'^{2}_{p+1} soit $-(p+1)^4 a'^{2}_o$ et tel que le coefficient de a'_{p+1} et le terme constant soient des polynômes en $(a'_o, a'_1, \ldots, a'_p)$ à coefficients entiers. Pour que Δ_{p+1} soit strictement positif, il faut et il suffit qu'il ait 2 racines réelles et que a'_{p+1} soit compris strictement entre ces racines. Si les racines ne sont pas réelles, il n'existe pas de valeur possible de $\mathbb{Z}$ pour a'_{p+1}. Nous posons $L_{1\,p+1} = L_{2\,p+1} = 0$. Si les racines sont des réels x_1 et x_2 avec $x_2 \leq x_1$ nous avons $L_{2\,p+1} < a_{p+1} < L_{1\,p+1}$ avec

$$L_{1\,p+1} = E\left(\frac{x_1}{(d-p-1)!}\right)+1 \quad \text{si} \quad \frac{x_1}{(d-p-1)!} \notin \mathbb{Z}$$

$$L_{1\,p+1} = \frac{x_1}{(d-p-1)!} \quad \text{si} \quad \frac{x_1}{(d-p-1)!} \in \mathbb{Z}$$

$$L_{2\,p+1} = E\left(\frac{x_2}{(d-p-1)!}\right) .$$

2) <u>Supposons p impair</u> :

$$\Delta'_{p+1} = \begin{vmatrix} m_{\frac{p+1}{2}\frac{p+1}{2}} & m_{\frac{p+1}{2}\frac{p+3}{2}} \\ m_{\frac{p+1}{2}\frac{p+3}{2}} & m_{\frac{p+3}{2}\frac{p+3}{2}} \end{vmatrix} \quad \text{doit être strictement positif}$$

$$m_{\frac{p+1}{2}\frac{p+1}{2}} = \left(\frac{p+1}{2}\right)^2 a'^{2}_{\frac{p+1}{2}} - 2(p+1)a'_{\frac{p+3}{2}}\ a'_{\frac{p-1}{2}} \ldots - (p+1)^2 a'_{p+1}a'_o$$

$$m_{\frac{p+1}{2}\frac{p+3}{2}} = \left(\frac{p+1}{2}\right)\left(\frac{p-1}{2}\right)a'_{\frac{p+1}{2}}\ a'_{\frac{p+3}{2}} - 3(p+1)a'_{\frac{p+5}{2}}\ a'_{\frac{p-1}{2}} \ldots - p(p+1)a'_{p+1}a'_1$$

$$m_{\frac{p+3}{2}\ \frac{p+3}{2}} = (\frac{p+3}{2})(\frac{p-1}{2})a'_{\frac{p+3}{2}} - 2(p+1)a'_{\frac{p+5}{2}}\,a'_{\frac{p+1}{2}} - \ldots - (p-1)(p+1)a'_{p+1}a'_2$$

Δ'_{p+1} est un polynôme du second degré en a'_{p+1} tel que le coefficient de a'_{p+1} soit $(p-1)(p+1)^3a'_2a'_o - p^2(p+1)^2a'^2_1$ et tel que le coefficient de a'_{p+1} et le terme constant soient des polynômes en $(a'_o, a'_1, \ldots, a'_p)$ à coefficients entiers. Le coefficient m_{11} de Mg_{p+1} est strictement positif. Or $m_{11} = p\,a'^2_1 - 2(p+1)a'_2\,a'_o$. A fortiori $p^2a'^2_1 - (p-1)(p+1)a'_2\,a'_o$ est strictement positif donc le coefficient de a'_{p+1} dans Δ'_p est strictement positif. La fin de la démonstration est analogue à celle du cas p pair.

C)

1) Nous cherchons maintenant les corps de nombres algébriques totalement réel, de degré n sur Q de discriminant D inférieur à un nombre K donné. Soit F_1 un de ces corps de nombres algébriques. D'après le théorème 1, il existe ρ_1 entier algébrique de F_1 , ρ_1 n'étant pas un rationnel, tel que :

$$-[n/2] \leq S(\rho_1) \leq 0 \qquad (2)$$

et

$$n+1 \leq S(\rho_1^2) \leq (\frac{\gamma_n^n}{n}|D|)^{\frac{1}{n-1}} \qquad (3)$$

ρ_1 engendre un sous-corps de degré d de F_1 sur Q . Il existe un polynôme $g(X)$ de $Z[X]$ de degré d unitaire, irréductible dans $Q(X)$, admettant d racines réelles distinctes dont l'une est ρ_1 . Nous notons $g(X) = \sum_{i=0}^{i=d} a_iX^{d-i}$ avec $a_o = 1$. Soit $s'_1, \ldots, s'_d$ les homomorphismes de $Q(\rho_1)$ dans $\mathbb{C}$. Notons $\rho'_i = s'_i(\rho_1)$. Il y a n homomorphismes de F_1 dans $\mathbb{C}$ et leurs restrictions à $Q(\rho_1)$ sont $s'_1, \ldots, s'_d$. Chaque s'_i se prolonge en n/d homomorphismes de F_1 dans $\mathbb{C}$. Par suite

$$S(\rho_1) = \frac{n}{d}(\rho'_1 + \ldots + \rho'_d) \ , \quad S(\rho_1^2) = \frac{n}{d}(\rho'^2_1 + \ldots + \rho'^2_d)$$

comme $a_1 = -(\rho'_1 + \ldots + \rho'_d)$ et $a_2 = \dfrac{a_1^2 - (\rho'^2_1 + \ldots + \rho'^2_d)}{2}$. Nous déduisons de cela

$$0 \leq a_1 \leq [\frac{d}{2}]$$

et

$$-\frac{1}{2}[\frac{d}{n}(\frac{\gamma_n^n}{n}K)^{\frac{1}{n-1}} - a_1^2] \leq a_2 \leq -\frac{1}{2}[(n+1)\frac{d}{n} - a_1^2] \quad . \tag{4}$$

Utilisons maintenant le théorème 3 : pour chaque a_i nous calculons un majorant et un minorant qui sont exprimés en fonction de d, n, K, $a_o,\ldots,a_{i-1}$. Tout corps de nombres algébriques F totalement réel de degré n sur Q de discriminant inférieur ou égal à K est tel qu'il existe d divisant n , tel que F contienne un sous corps engendré sur $\mathbb{Q}$ par une racine d'un polynôme unitaire $g(X)$ de $Z[X]$ de degré d , irréductible dans $Q[X]$, ayant d racines réelles distinctes et dont les coefficients sont compris entre les bornes calculées à partir de (4) par la méthode indiquée dans le théorème 3.

2) Nous supposons pour cette partie que n est un nombre premier. Alors tout corps de nombres algébriques F de degré n sur Q de discriminant inférieur ou égal à K est engendré par une racine d'un polynôme unitaire de $Z[X]$, de degré n , ayant n racines réelles distinctes, et dont les coefficients sont compris entre les bornes calculées à partir de (4) par la méthode indiquée dans le théorème 3. Soit un polynôme $g(X) = \sum_{i=0}^{i=n} a_i X^{n-i}$ avec $a_o = 1$.

Supposons que les a_i soient des entiers compris entre les bornes calculées à partir de (4) pour les corps de nombres algébriques totalement réels de degré n de discriminant inférieur ou égal à K .

Nous indiquons comment nous vérifions si une racine de $g(X)$ définit une extension de degré n , totalement réelle, de Q de discriminant inférieur ou égal à K : nous cherchons si $g(X)$ est irréductible dans $Q[X]$. S'il l'est nous formons M_g dont l'expression en fonction des a_i est donnée dans l'énoncé du théorème 2 . Nous vérifions que tous les mineurs principaux ont des déterminants strictement positifs. Notons Δ le déterminant de M_g . Nécessairement Δ doit être strictement positif. Si $g(X)$ n'a été éliminé par aucune des vérifications précédentes une racine ρ de $g(X)$ définit une extension totalement réelle de degré n sur Q

de discriminant D . $\frac{\Delta}{n-2} = D_\rho$ et $D_\rho = d^2 D$ avec $d \in \mathbb{Z}$. Il reste à vérifier si on a effectivement $D \leq K$. D est supérieur à la minoration de Minkowski pour les extensions totalement réelles de degré n sur Q que nous notons D_o donc

$$\frac{D_\rho}{K} \leq d^2 \leq \frac{D_\rho}{D_o} \quad \text{si} \quad D \leq K$$

Si p est un nombre premier tel que pour un k , $\frac{D_\rho}{K} \leq (pk)^2 \leq \frac{D_\rho}{D_o}$, et si p^2 divise D_ρ nous cherchons la décomposition de l'idéal (p) dans $Q(\rho)$ par la méthode de Berwick [1] et nous appliquons ensuite le lemme suivant

LEMME. - <u>Soit</u> p <u>un nombre premier de</u> $\mathbb{Z}$, $p = p_1^{e_1} \dots p_s^{e_s}$ <u>dans un corps</u> F <u>sur</u> Q , <u>les</u> p_i <u>étant des idéaux premiers distincts de</u> F , <u>alors la puissance</u> D_p <u>de</u> p <u>contenue dans le discriminant de</u> K <u>sur</u> $\mathbb{Q}$ <u>est</u>

$$D_p = \prod_{i=1}^{i=s} p^{f_i(\bar{e}_i - 1)}$$

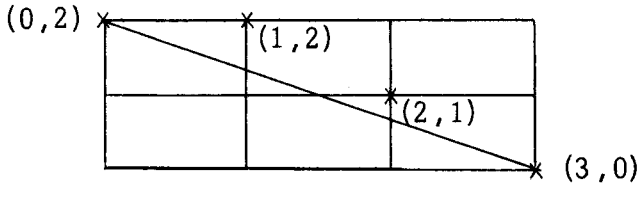
<u>avec</u> $\bar{e}_i = e_i$ <u>si</u> $p \nmid e_i$, $e_i + 1 \leq \bar{e}_i \leq (\Omega_i + 1)e_i$ <u>si</u> p/e_i <u>et</u> p^{Ω_i} <u>est la puissance maximum de</u> p <u>contenu dans</u> e_i

Prenons par exemple $n = 3$ et $K = 150$. Considérons le polynôme $g(X) = X^3 + X^2 - 5X - 1$. Il est bien irréductible dans $Q[X]$ et M_g est la matrice d'une forme quadratique définie positive. Appelons ρ une racine de $g(X)$

$$D_\rho = \frac{\Delta}{3} = 592 = d^2 D \quad , \quad D \text{ discriminant de } Q(\rho) .$$

Nous avons a priori comme possibilité $d = 1$ ou $d = 2$ donc $D = 592$ ou $D = 148$. Cherchons la décomposition de l'idéal (2)

$$g(X) = (X+1)^3 - 2[(X+1)^2] - 4[(X+1)-1] \mod .8$$



donc $(2) = p_1^3$; en utilisant le lemme nous trouvons <u>$D = 148$</u> .

3) Recherche des discriminants minimaux successifs pour les extensions totalement réelles de degré 3 sur $\mathbb{Q}$

a) Le discriminant minimum pour les extensions totalement réelles de degré 3 sur $\mathbb{Q}$ est 49 . Nous allons chercher le plus petit parmi les discriminants suivants , ensuite nous chercherons le plus petit parmi les discriminants supérieurs aux deux premiers et nous continuerons ainsi.

Une extension totalement réelle de degré 3 sur $\mathbb{Q}$ de discriminant inférieur ou égal à K est engendrée par une racine d'un polynôme $g(X)$ tel que

$$g(X) = X^3 + a_1X^2 + a_2X + a_3 \quad , \quad (a_1,a_2,a_3) \in \mathbb{Z}^3$$

$$\begin{aligned} 0 \le a_1 &\le 1 \\ -\frac{1}{2}\left[\left(\frac{\sqrt[3]{3}}{3}K\right)^{1/2} - a_1^2\right] \le a_2 &\le -\frac{1}{2}[4-a_1^2] \\ -27a_3^2 + a_3(18a_1a_2 - 4a_1^3) + a_1^2a_2^2 - 4a_2^3 &> 0 \end{aligned} \qquad (5)$$

De plus si ces 3 conditions sont vérifiées, nous appelons ρ une racine de $g(X)$, D le discriminant de $\mathbb{Q}(\rho)$. Alors

$$D = \frac{\Delta}{3d^2} \quad \text{avec} \quad d \in \mathbb{Z}$$

et

$$\Delta = -27a_3^2 + a_3(18a_1a_2 - 4a_1^3) + a_1^2a_2^2 - 4a_2^3 \ .$$

Pour $a_1 = 0$, (5) devient $-\frac{1}{2}\left(\frac{2K}{3}\right)^{1/2} \le a_2 \le -2$ et $\Delta = -27\,a_3^2 - 4a_2^3$.

Pour $a_1 = 1$, (5) devient $-\frac{1}{2}\left(\left(\frac{2K}{3}\right)^{1/2} - 1\right) \le a_2 \le -2$ et

$$\Delta = -27a_3^2 + a_3(18a_2 - 4) + a_2^2 - 4a_2^3 \ .$$

Considérons $g(X) = X^3 - 3X + 1$. $g(X)$ est irréductible, a 3 racines réelles distinctes et $\Delta/3 = 81$. Une racine ρ de $g(X)$ définit une extension de degré 3 totalement réelle de $\mathbb{Q}$ de discriminant D tel que

$$D = \frac{81}{d^2} \ , \ d \in \mathbb{Z}$$

comme nécessairement $D \geq 49$, cela entraîne $d = 1$ et $D = 81$.

b) <u>Cherchons les extensions totalement réelles de degré</u> 3 <u>sur</u> Q <u>de discriminant inférieur à</u> 81 . Une telle extension est engendrée par une racine ρ d'un polynôme $g(X) = X^3 + a_1X^2 + a_2X + a_3$, $(a_1, a_2, a_3) \in \mathbb{Z}^3$

$$\begin{cases} a_1 = 0 \\ -3 \leq a_2 \leq -2 \\ 0 \leq a_3 \leq 2\sqrt{-a_2^3/27} \end{cases} \quad \text{ou} \quad \begin{cases} a_1 = 1 \\ -3 \leq a_2 \leq -2 \\ -27a_3^2 + a_3(18a_2 - 4) + a_2^2 - 4a_2^3 > 0 \end{cases}$$

nous étudions tous les polynômes $g(X)$ possibles. D désignera le discriminant de $Q(\rho)$ quand $g(X)$ vérifie les conditions imposées et est irréductible dans $Q(X)$.

<u>$a_1 = 0$, $a_2 = -2$</u> . Alors $0 \leq a_3 \leq 1$, $X^3 - 2X$ et $X^3 - 2X + 1$ ne sont pas irréductibles dans $Q(X)$ ayant comme racines évidentes respectivement 0 et 1 .

<u>$a_1 = 0$, $a_2 = -3$</u> . Alors $0 \leq a_3 \leq 2$, $X^3 - 3X$ et $X^3 - 3X + 2$ ne sont pas irréductibles dans $Q(X)$ ayant comme racines évidentes respectivement 0 et 1 . $X^3 - 3X + 1$ définit l'extension cyclique de $\mathbb{Q}$ non ramifiée en dehors de 3 , de degré 3 . C'est une extension totalement réelle de degré 3 de Q , de discriminant 81 ainsi que nous l'avons calculé à la fin du a) .

<u>$a_1 = 1$, $a_2 = -2$</u> . $-27a_3^2 - 40a_3 + 36 > 0$ entraîne $-2 \leq a_3 \leq 0$, $X^3 + X^2 - 2X$ et $X^3 + X^2 - 2X - 2$ ne sont pas irréductibles dans $Q[X]$. Etudions $g(X) = X^3 + X^2 - 2X - 1$, $\Delta/3 = D = 49$. Une racine de ce polynôme engendre l'extension de degré 3 sur Q totalement réelle de discriminant minimum.

<u>$a_1 = 1$, $a_2 = -3$</u> . Alors $-3 \leq a_3 \leq 1$. $X^3 + X^2 - 3X + 1$, $X^3 + X^2 - 3X$, $X^3 + X^2 - 3X - 2$, $X^3 + X^2 - 3X - 3$ ne sont pas irréductibles dans $Q[X]$, $g(X) = X^3 + X^2 - 3X - 1$, $g(X)$ est bien irréductible dans $Q[X]$, $\Delta/3 = 148$ donc $D = 148/d^2$ nécessairement $D \geq 49$; donc $d = 1$ et $D = 148$.

Il n'y a pas d'extension totalement réelle de degré 3 sur Q dont le discriminant soit compris strictement entre 49 et 81 . Il existe une extension de degré 3 sur Q totalement réelle de discriminant 49 et une extension de degré 3 sur Q totalement réelle de discriminant 81 . Ce sont toutes deux des extensions cycliques de Q .

c) Nous allons chercher maintenant le discriminant minimum parmi les discriminants d'extensions totalement réelles de degré 3 sur Q non cycliques ainsi que le discriminant minimum pour les extensions totalement réelles de degré 3 sur Q de discriminant strictement supérieur à 81 . Dans l'étude précédente nous avons rencontré le polynôme X^3+X^2-3X-1 . Une racine de ce polynôme engendre une extension totalement réelle de degré 3 sur Q de discriminant $148 = 37\times 2^2$.

Une extension F de degré 3 sur Q non cyclique a pour clôture galoisienne N une extension de Q dont le groupe de Galois est S_3 . N a 3 sous-extensions de degré 3 sur Q conjuguées et une seule sous-extension quadratique k de discriminant d . Notons D le discriminant de F . Alors $D = df^2$ avec $f \in \mathbb{Z}$ (voir [10]) . Une racine de X^3+X^2-3X-1 engendre une extension de degré 3 sur Q totalement réelle non cyclique dont la clôture galoisienne N est l'extension de degré 3 de $Q(\sqrt{37})$ non ramifiée en dehors de 2 . Il y a 3 extensions de degré 3 de Q conjuguées totalement réelles de discriminant 148 .

Nous allons montrer que 148 est le discriminant minimum pour les extensions totalement réelles de degré 3 sur Q non cycliques et que c'est le discriminant minimum pour les extensions totalement réelles de degré 3 sur Q de discriminant strictement supérieur à 81 .

<u>Recherche des extensions totalement réelles de degré</u> 3 <u>sur</u> Q <u>de discriminant supérieur à</u> 81 <u>et inférieur à</u> 148 . Elles sont engendrées par une racine ρ d'un polynôme $g(X) = X^3+a_1X^2+a_2X+a_3$, $(a_1,a_2,a_3)\in\mathbb{Z}^3$ avec $\begin{pmatrix} a_1 = 0 \\ -4 \le a_2 \le -2 \\ -27a_3^2-4a_2^3 > 0 \end{pmatrix}$ ou $\begin{pmatrix} a_1 = 1 \\ -4 \le a_2 \le -2 \\ -27a_3^2+a_3(18a_2-4)+a_2^2-4a_2^3 > 0 \end{pmatrix}$. Les

cas $(a_1 = 0$ et $-3 \leq a_2 \leq -2)$ et $(a_1 = 1$ et $-3 \leq a_2 \leq -2)$ ont été étudiés pendant la recherche des extensions de discriminant inférieur à 81 .

$\underline{a_1 = 0 \ , \ a_2 = -4}$; alors $0 \leq a_3 \leq 3$. $X^3 - 4X$ et $X^3 - 4X + 3$ ne sont pas irréductibles dans $Q[X]$, $g(X) = X^3 - 4X + 1$ est irréductible dans $Q[X]$ $\Delta/3 = d^2 D = 229$. 229 est premier donc $a = 1$ et $D = 229$.
$g(X) = X^3 - 4X + 2$, $\Delta/3 = 148$. Une racine de $g(X)$ engendre une des 3 extensions conjuguées de degré 3 totalement réelles sur Q sous-extensions de l'extension de degré 3 de $Q(\sqrt{37})$ non ramifiée en dehors de 2 . Ces sous-extensions sont de discriminant 148 .

$\underline{a_1 = 1 \ , \ a_2 = -4}$; alors $-3 \leq a_3 \leq 2$. $X^3 + X^2 - 4X + 2$, $X^3 + X^2 - 4X$ ne sont pas irréductibles dans $Q[X]$. $g(X) = X^3 + X^2 - 4X + 1$ donne une extension cyclique de degré 3 sur Q totalement réelle de discriminant $169 = 13^2$. $g(X) = X^3 + X^2 - 4X - 1$ donne des extensions de degré 3 sur Q totalement réelles non cycliques de discriminant 321. $g(X) = X^3 + X^2 - 4X - 2$ donne des extensions de degré 3 sur Q totalement réelles non cycliques de discriminant 4×79 . $g(X) = X^3 + X^2 - 4X - 3$ donne des extensions de degré 3 sur Q totalement réelles non cycliques de discriminant 257 .

Nous avons montré qu'il n'existe pas d'extension totalement réelle de degré 3 sur Q dont le discriminant soit strictement compris entre 81 et 148 .

- II -

Dans cette partie, nous allons chercher les discriminants minimaux successifs pour les extensions totalement réelles de degré n sur Q où n n'est pas un nombre premier. Nous allons étudier particulièrement les cas $n = 4$ et $n = 9$. Nous utiliserons les théorèmes 1, 2, 3 de la partie I et le théorème suivant du à Godwin [6] que j'énonce, dans le cas totalement réel sous le nom de théorème 4.

THEOREME 4. - Soit K un corps totalement réel de degré $N = n\nu$ sur Q de discriminant D ayant un sous-corps k de degré n sur Q de discriminant d. Alors K est engendré sur k par une racine d'un polynôme $\Phi_1(X)$ tel que :

$$\Phi_1(X) = X^{\nu} + \lambda_{11}X^{\nu-1} + \ldots + \lambda_{1\nu} \ , \ \lambda_{1i} \text{ entier de } k \ .$$

Notons $\alpha_{11},\ldots,\alpha_{1\nu}$ les racines de Φ_1. Elles sont nécessairement réelles. Notons $\Phi_1 \ldots \Phi_n$ les conjugués de Φ_1 pour les homomorphismes de k dans $\mathbb{C}$ et $\alpha_{j1},\ldots,\alpha_{j\nu}$ les racines de Φ_j.

$$0 < \sum_{j=1}^{j=n} \left\{ \sum_{i=1}^{i=\nu} \alpha_{ji}^2 - \left(\sum_{i=1}^{i=\nu} \alpha_{ji} \right)^2 \Big/ \nu \right\} \leq \gamma_{N-n} \left\{ \frac{|D|^{1/2}}{|d|^{1/2}\,\nu^{n/2}} \right\}^{\frac{2}{N-n}} . \qquad (6)$$

γ_ℓ pour ℓ entier est la constante de Minkowski dont la définition est donnée dans le théorème 1.

A) Supposons que F_1 soit une extension totalement réelle de degré n sur Q de discriminant D inférieur ou égal à K. D'après le théorème 1 il existe ρ_1 entier algébrique de F_1, ρ_1 n'étant pas un rationnel tel que

$$|S(\rho_1)| \leq [n/2]$$

et

$$(n+1)^{n-1} \leq (S(|\rho_1|^2))^{n-1} \leq \frac{\gamma_n^n}{n}|D|$$

$Q(\rho_1)$ est une extension de degré d sur Q avec d diviseur de n. Nous avons démontré dans la partie I que $Q(\rho_1)$ est engendrée par une racine d'un polynôme unitaire $g(X)$ de $Z[X]$, de degré d, ayant d racines réelles distinctes, irréductible dans $Q[X]$ et tel que

$$g(X) = \sum_{i=0}^{i=d} a_i X^{d-i} \quad \text{avec} \quad 0 \leq a_1 \leq [d/2]$$

et

$$-\frac{1}{2}\left[\frac{d}{n}\left(\frac{\gamma_n^n}{n}K\right)^{\frac{1}{n-1}} - a_1^2\right] \leq a_2 \leq -\frac{1}{2}\left[\frac{(n+1)d}{n} - a_1^2\right]$$

d'après le théorème 3 ceci entraîne que pour tout i compris entre 1 et d il existe un couple d'entier (L_{1i}, L_{2i}) tels que $L_{2i} < a_i < L_{1i}$. Supposons que d est un diviseur strict de n, d'après le théorème 4, F_1 est

engendré sur $Q(\rho_1)$ par une racine θ_1 d'un polynôme $\Phi_1(X)$ tel que :

$$\Phi_1(X) = X^{\frac{n}{d}} + \lambda_{11} X^{\frac{n}{d}-1} + \ldots + \lambda_{1\nu} \ , \ \lambda_{1i} \text{ entier de } Q(\rho_1) \ .$$

Si $\Phi_1, \ldots, \Phi_d$ sont les conjugués de Φ_1 , notons $\alpha_{j1}, \ldots, \alpha_{j\frac{n}{d}}$ les racines de Φ_j . Alors

$$0 < \sum_{j=1}^{j=n} \left\{ \sum_{i=1}^{i=\frac{n}{d}} \alpha_{ji}^2 - \left(\sum_{i=1}^{i=\frac{n}{d}} \alpha_{ji} \right)^2 \Big/ \frac{n}{d} \right\} \leq \gamma_{n-d} \left(\frac{|D|^{\frac{1}{2}}}{|\delta|^{\frac{1}{2}} \left(\frac{n}{d}\right)^{\frac{n}{2}}} \right)^{\frac{2}{n-d}} \qquad (7)$$

avec D discriminant de F_1 , δ discriminant de $Q(\rho_1)$.
$\psi(X) = \Phi_1(X)\Phi_2(X)\ldots\Phi_{\frac{n}{d}}(X)$ est le polynôme minimal de θ_1 sur Q si $Q(\theta_1) = F_1$. Alors $\psi(X)$ a nécessairement n racines réelles distinctes, est de degré n , est à coefficients dans $\mathbb{Z}$, est unitaire et irréductible dans $Q(X)$. Montrons qu'il existe une majoration et une minoration en fonction de K , n et d des coefficients de X^{n-1} et de X^{n-2} . Le coefficient de X^{n-1} est $\mathrm{Tr}\, Q(\rho_1)/Q(\lambda_{11}) = a'_1$. Le coefficient de X^{n-2} est

$$\mathrm{Tr}\, Q(\rho_1)/Q(\lambda_{12}) + \frac{1}{2}(\mathrm{Tr}\, Q(\rho_1)/Q(\lambda_{11}))^2 - \frac{1}{2}\mathrm{Tr}\, Q(\rho_1)/Q(\lambda_{11}^2) = a'_2$$

(7) donne

$$0 < (1 - \frac{d}{n})\mathrm{Tr}\, Q(\rho_1)/Q(\lambda_{11}^2) - 2\,\mathrm{Tr}\, Q(\rho_1)/Q(\lambda_{12}) < \gamma_{n-d} \left(\frac{D^{\frac{1}{2}}}{\delta^{\frac{1}{2}} \left(\frac{n}{d}\right)^{\frac{n}{2}}} \right)^{\frac{2}{n-d}} \ . \qquad (8)$$

$D \leq K$ par hypothèse et δ est minoré par le discriminant minimum pour les extensions totalement réelles de degré d sur Q que nous notons k donc (8) donne

$$0 < (1 - \frac{d}{n})\mathrm{Tr}\, Q(\rho_1)/Q(\lambda_{11}^2) - 2\,\mathrm{Tr}\, Q(\rho_1)/Q(\lambda_{12}) < \gamma_{n-d} \left(\frac{K^{\frac{1}{2}}}{k^{\frac{1}{2}} \left(\frac{n}{d}\right)^{\frac{n}{2}}} \right)^{\frac{2}{n-d}} \ . \qquad (9)$$

Si on ajoute à θ_1 un entier relatif (9) ne change pas. Par suite, en remplaçant éventuellement θ_1 par sa somme avec un entier, on peut supposer

$$\lambda_{11} = \alpha_o + \alpha_1\rho_1 + \ldots + \alpha_{d-1}\rho_1^{d-1}$$

avec les α_i éléments de Q , $-[\frac{n}{2d}] < \alpha_i \leq [\frac{n}{2d}]$ pour $i \geq 1$ et α_o tel que $-d[\frac{n}{2d}] < \mathrm{Tr}\, Q(\rho_1)/Q(\lambda_{11}) \leq d[\frac{n}{2d}]$. Si on change θ_1 en $-\theta_1$ (9) ne change pas donc nous pouvons supposer

$$\lambda_{11} = \alpha_o + \alpha_1\rho_1 + \ldots + \alpha_{d-1}\rho_1^{d-1} \quad , \quad \alpha_i \in \mathbb{Q}$$

$$\forall i \geq 1 \quad , \quad -[\frac{n}{2d}] < \alpha_i \leq [\frac{n}{2d}) \quad \text{et} \quad 0 \leq \mathrm{Tr}\, Q(\rho_1)/Q(\lambda_{11}) \leq [\frac{n}{2}] \ .$$

Pour un entier j donné $\mathrm{Tr}\, Q(\rho_1)/Q(\rho_1^j)$ s'exprime en fonction des a_i coefficients de $g(X)$. Les a_i étant tous majorés et minorés en fonction de n , d et K . $\mathrm{Tr}\, Q(\rho_1)/Q(\lambda_{11}^2)$ est par suite majoré en fonction de n , d et K . Cette majoration et (9) entraînent que a'_1 et a'_2 sont majorés et minorés en fonction de n , d et K .

Pour démontrer cela, nous avons dû supposer $F_1 = Q(\theta_1)$. Si $n = pq$ où p et q sont deux nombres premiers non nécessairement distincts et si nous sommes dans le cas $Q(\rho_1) \neq F_1$ alors nécessairement $F_1 = Q(\theta_1)$ ou F_1 est une extension composée d'une extension de degré p sur Q et d'une extension de degré q sur Q . La recherche des extensions totalement réelles de degré $n = pq$ sur Q , avec p et q premiers non nécessairement distincts, de discriminant inférieur ou égal à K consiste d'une part à chercher les extensions composées d'une extension totalement réelle de degré p sur Q et d'une extension totalement réelle de degré q sur Q et d'autre part à calculer pour $d = p$, pour $d = q$ les majorations et minorations de a'_1 et a'_2 et ensuite à chercher les polynômes qui vont convenir parmi les polynômes unitaires de degré n de $Z[X]$, ayant n racines réelles distinctes, irréductibles dans $Q[X]$ et tels que les coefficients de X^{n-1} et X^{n-2} soient majorés et minorés. Cette dernière partie se fait par la méthode indiquée dans I pour le cas n premier.

B) <u>Recherche des discriminants minimaux successifs pour les extensions totalement réelles de degré</u> 4 <u>sur</u> Q .

Nous savons que le discriminant minimum pour de telles extensions est 725 et que l'extension correspondante est cyclique. Le discriminant mi-

nimum pour les extensions totalement réelles de degré 4 sur Q qui sont composées de 2 extensions quadratique est $(5 \times 8)^2 = 1600$ qui est le discriminant de $\mathbb{Q}(\sqrt{5},\sqrt{2})$. Une extension de degré 4 sur Q galoisienne est soit cyclique, soit la composée de 2 extensions quadratiques. Nous chercherons le discriminant minimum pour les extensions totalement réelles de degré 4 sur Q non galoisiennes.

D'après le théorème 1 pour une extension F_1 de degré 4 sur Q de discriminant inférieur ou égal à 5000 il existe ρ_1 tel que ρ_1 ne soit pas rationnel et $0 \leq -S(\rho_1) \leq 2$ avec $5 \leq S(\rho_1^2) \leq (\frac{\gamma_4^4}{4}\ 5000)^{1/3}$ donc $5 \leq S(\rho_1^2) \leq 17$.

1) <u>Si $F_1 = Q(\rho_1)$</u> . ρ_1 a pour polynôme minimal

$$g(X) = X^4 + a_1X^3 + a_2X^2 + a_3X + a_4 \quad , \quad a_i \in \mathbb{Z}$$

g irréductible dans $Q[X]$, ayant 4 racines réelles distinctes et

$$\begin{pmatrix} a_1 = 0 \\ -8 \leq a_2 \leq -3 \end{pmatrix} \text{ ou } \begin{pmatrix} a_1 = 1 \\ -8 \leq a_2 \leq -3 \end{pmatrix} \text{ ou } \begin{pmatrix} a_1 = 2 \\ -6 \leq a_2 \leq -1 \end{pmatrix} .$$

2) <u>Si</u> $Q(\rho_1)$ <u>est une extension de degré</u> 2 <u>de</u> Q . ρ_1 a pour polynôme minimal

$$g(X) = X^2 + a_1X + a_2 \quad , \quad a_i \in \mathbb{Z}$$

avec $a_1^2 - 4a_2 > 0$, $a_1^2 - 4a_2$ n'étant pas un carré de $\mathbb{Z}$, $0 \leq a_1 \leq 1$ et $\frac{a_1^2 - 17/2}{2} \leq a_2 \leq \frac{a_1^2 - 5/2}{2}$. Ces 2 dernières conditions donnent $(a_1 = 0$ et $-4 \leq a_2 \leq -2)$ ou $(a_1 = 1$ et $-3 \leq a_2 \leq -1)$. $Q(\rho_1)$ est par suite engendré par une racine ρ_1 de l'un des polynômes suivants : $X^2 - 2$, $X^2 - 3$, $X^2 + X - 1$, $X^2 + X - 3$. $Q(\rho_1)$ est donc l'une des extensions quadratiques de $\mathbb{Q}$ suivantes : $Q\sqrt{2}$, $Q\sqrt{3}$, $Q\sqrt{5}$, $Q\sqrt{13}$.

Appliquons maintenant le théorème 4 . F_1 est engendré sur $Q(\rho_1)$ par θ_1 racine de $\Phi_1(X) = X^2 + \lambda_{11}X + \lambda_{12}$ avec λ_{11} et λ_{12} entiers de

$Q(\rho_1)$ et $0 < \frac{1}{2}\mathrm{Tr}\, Q(\rho_1)/Q(\lambda_{11}^2) - 2\,\mathrm{Tr}\, Q(\rho_1)/Q(\lambda_{12}) \leq 9$ (10)

a) <u>Supposons</u> $Q(\theta_1)$ <u>extension quadratique de</u> $\mathbb{Q}$. Alors λ_{11} et λ_{12} sont des éléments de $\mathbb{Z}$. (10) ne change pas si on ajoute à θ un entier. Nous pouvons donc supposer $0 \leq \lambda_{11} \leq 1$ on a $0 < \lambda_{11}^2 - 4\lambda_{12} \leq 9$ donc $(\lambda_{11} = 0$ et $-2 \leq \lambda_{12} \leq -1)$ ou $(\lambda_{11} = 1$ et $-2 \leq \lambda_{12} \leq -1)$. $\Phi_1(X)$ est par suite l'un des polynômes suivants $X^2 - 1$, $X^2 - 2$, $X^2 + X - 1$, $X^2 + X - 2$. $X^2 - 1$ et $X^2 + X - 2$ ont des racines entières et ne définissent donc pas d'extension quadratique de $\mathbb{Q}$. Par suite $\Phi_1(X)$ est $X^2 - 2$ ou $X^2 + X - 1$ et $Q(\theta_1)$ est $Q(\sqrt{2})$ ou $Q(\sqrt{5})$. Nous obtenons ainsi les extensions totalement réelles de degré 4 sur Q de discriminant inférieur ou égal à 5000 suivantes : $Q(\sqrt{2},\sqrt{5})$ de discriminant 1600 , $(Q\sqrt{3},\sqrt{5})$ de discriminant 3600 , $Q(\sqrt{13},\sqrt{5})$ de discriminant 4225 .

b) <u>Supposons</u> $Q(\theta_1)$ <u>extension de degré</u> 4 <u>sur</u> Q . Le polynôme minimal de θ_1 sur Q est $\psi(X)$ tel que

$$\psi(X) = (X^2 + \lambda_{11}X + \lambda_{12})(X^2 + \bar{\lambda}_{11}X + \bar{\lambda}_{12}) .$$

Pour un élément λ de $Q(\rho_1)$, $\bar{\lambda}$ désigne son conjugué.

$$\psi(X) = X^4 + a_1'X^3 + a_2'X^2 + a_3'X + a_4' .$$

Pour tout i , a_i' est un élément de $\mathbb{Z}$

$$a_1' = \mathrm{Tr}(Q(\rho_1)/Q)(\lambda_{11})$$

$$a_2' = \mathrm{Tr}(Q(\rho_1)/Q)(\lambda_{12}) + \frac{1}{2}(\mathrm{Tr}(Q(\rho_1)/Q)(\lambda_{11}))^2 - \frac{1}{2}\mathrm{Tr}(Q(\rho_1)/Q)(\lambda_{11}^2) .$$

Nous continuons la démonstration par la méthode indiquée dans la partie A de II .

$\lambda_{11} = \alpha_o + \alpha_1\rho_1$ avec (α_o, α_1) élément de $\mathbb{Q}^2$, $-1 \leq \alpha_1 \leq 1$ et $0 \leq \mathrm{Tr}\, Q(\rho_1)/Q\,(\lambda_{11}) \leq 2$. $\mathrm{Tr}\, Q(\rho_1)/Q\,(\lambda_{11})$ est un élément de $\mathbb{Z}$ égal à $2\alpha_o + \alpha_1\, \mathrm{Tr}\, Q(\rho_1)/Q\,(\rho_1)$.

<u>Si $Q(\rho_1) = Q\sqrt{2}$. $\mathrm{Tr}(Q(\rho_1)/Q)\,(\rho_1) = 0$ et $\mathrm{Tr}\, Q(\rho_1)/Q\,(\rho_1^2) = 4$ donc</u>
$0 \leq \alpha_o \leq 1$ et $\mathrm{Tr}(Q(\rho_1)/Q)\,(\lambda_{11}^2) \leq 6$.

<u>Si $Q(\rho_1) = Q\sqrt{3}$</u> . $\mathrm{Tr}\, Q((\rho_1)/Q)\,(\rho_1) = 0$ et $\mathrm{Tr}\, Q(\rho_1)/Q\,(\rho_1^2) = 6$ donc $0 \leq \alpha_o \leq 1$ et $\mathrm{Tr}\, Q(\rho_1)/Q\,(\lambda_{11}^2) \leq 8$.

<u>Si $Q(\rho_1) = Q\sqrt{5}$</u> . $\mathrm{Tr}\, Q(\rho_1)/Q)\,(\rho_1) = -1$ et $\mathrm{Tr}\, Q(\rho_1)/Q\,(\rho_1^2) = 3$ donc $-\frac{1}{2} \leq \alpha_o \leq \frac{3}{2}$ et $\mathrm{Tr}\, Q(\rho_1)/Q\,(\lambda_{11}^2) \leq \frac{15}{2}$.

<u>Si $Q(\rho_1) = Q\sqrt{13}$</u> . $\mathrm{Tr}\, Q(\rho_1)/Q\,(\rho_1) = -1$ et $\mathrm{Tr}\, Q(\rho_1)/Q\,(\rho_1^2) = 7$ donc $-\frac{1}{2} \leq \alpha_o \leq \frac{3}{2}$ et $\mathrm{Tr}\, Q(\rho_1)/Q\,(\lambda_{11}^2) \leq \frac{23}{2}$.

Nous obtenons $0 \leq a'_1 \leq 2$ et $a'_2 \geq -\frac{9}{2} - \frac{23}{4} + \frac{a_1'^2}{2}$. Par ailleurs, $\psi(X)$ devant avoir 4 racines réelles distinctes, $a_1'^2 - 8a'_2 > 0$ car c'est le premier coefficient de la matrice $M_{\psi(X)}$ définie dans l'énoncé du théorème 2 .

Donc F_1 est engendré sur $\mathbb{Q}$ par une racine d'un polynôme unitaire $\psi(X)$ de $Z[X]$, irréductible dans $Q[X]$, ayant 4 racines réelles distinctes et tel que $\psi(X) = X^4 + a'_1X^3 + a'_2X^2 + a'_3X + a'_4$ avec $(a'_1 = 0$ et $-10 \leq a'_2 \leq -1)$ ou $(a'_1 = 1$ et $-10 \leq a'_2 \leq 0)$ ou $(a'_1 = 2$ et $-9 \leq a'_2 \leq 0)$.

THEOREME 5.- <u>Une extension</u> F_1 <u>totalement réelle de degré</u> 4 <u>sur</u> Q <u>de discriminant inférieur à</u> 5000 <u>est soit</u> $Q(\sqrt{5},\sqrt{2})$, $Q(\sqrt{5},\sqrt{3})$, $Q(\sqrt{5},\sqrt{13})$, <u>soit engendrée par une racine d'un polynôme de</u> $Z[X]$, $g(X) = X^4 + a'_1X^3 + a'_2X^2 + a'_3X + a'_4$, <u>irréductible dans</u> $\mathbb{Q}[X]$, <u>ayant</u> 4 <u>racines réelles distinctes et tel que</u> $(a'_1 = 0$, $-10 \leq a'_2 \leq -1)$ <u>ou</u> $(a'_1 = 1$, $-10 \leq a'_2 \leq 0)$ <u>ou</u> $(a'_1 = 2$, $-9 \leq a'_2 \leq 0)$.

Parmi les polynômes tels que $a'_1 = 0$, nous remarquons : $X^4 - 4X^2 + 2$ qui donne l'extension $F_1 = Q(\sqrt{2+\sqrt{2}})$, extension cyclique de degré 4 sur $\mathbb{Q}$, totalement réelle, non ramifiée en dehors de 2 qui a pour discriminant 2048 ; $X^4 - 5X^2 + 5$ qui donne une extension cyclique de degré 4 sur $\mathbb{Q}$, $F_1 = Q\left(\sqrt{\frac{5+\sqrt{5}}{2}}\right)$, de discriminant 2000 ; $X^4 - 7X^2 + X + 9$ qui donne des extensions de degré 4 sur $\mathbb{Q}$ totalement réelles non galoisiennes de discriminant 4705 .

C) Nous cherchons le discriminant minimum pour les extensions de degré 9 totalement réelles sur Q . Nous connaissons l'extension $Q(\cos\frac{2\pi}{19})$ de discriminant 19^8 . Nous allons donc chercher les corps F_1 dont le discriminant est inférieur à 19^8 , F_1 étant une extension totalement réelle de degré 9 sur Q .

Appliquons le théorème 1 : il existe ρ_1 entier de F_1 , ρ_1 n'appartenant pas à Q tel que

$$0 \leq S(\rho_1) \leq 4$$

et

$$10 \leq S(\rho_1^2) \leq \left(\frac{\gamma^9}{9}\right)^{1/8} \times 19 .$$

Il y a 2 cas possibles : ρ_1 engendre F_1 ou ρ_1 engendre une sous-extension de degré 3 de F_1 .

1) ρ_1 <u>engendre</u> F_1 . Soit $g(X)$ le polynôme minimal de ρ_1 . $g(X)$ est de degré 9 , est unitaire, a ses coefficients dans $\mathbb{Z}$ est irréductible dans $Q(X)$, a 9 racines réelles distinctes et

soit $\begin{cases} a_1 = 0 \\ -17 \leq a_2 \leq -5 \end{cases}$, soit $\begin{cases} a_1 = 1 \\ -17 \leq a_2 \leq -5 \end{cases}$, soit $\begin{cases} a_1 = 2 \\ -15 \leq a_2 \leq -3 \end{cases}$, soit $\begin{cases} a_1 = 3 \\ -13 \leq a_2 \leq -1 \end{cases}$

soit $\begin{cases} a_1 = 4 \\ -9 \leq a_2 \leq 3 \end{cases}$.

2) ρ_1 <u>engendre une sous-extension de degré</u> 3 <u>de</u> F_1 . Soit $g(X)$ le polynôme minimal de ρ

$$g(X) = X^3 + a_1X^2 + a_2X + a_3$$

a_1 , a_2 , a_3 éléments de $\mathbb{Z}$. $g(X)$ irréductible dans $Q[X]$, ayant 3 racines réelles distinctes et

$$\begin{cases} a_1 = 0 \\ -5 \leq a_2 \leq -2 \end{cases} \quad \text{ou} \quad \begin{cases} a_1 = 1 \\ -5 \leq a_2 \leq -2 \end{cases} .$$

D'après le théorème 2, $g(X)$ a 3 racines réelles distinctes si et seulement si

$$\Delta = \begin{vmatrix} 2a_1^2 - 6a_2 & a_1a_2 - 9a_3 \\ a_1a_2 - 9a_3 & 2a_2^2 - 6a_3a_1 \end{vmatrix} > 0$$

alors $\Delta/3 = d^2 S$ avec d entier et S discriminant de $Q(\rho_1)$ sur Q

les cas $\begin{matrix} a_1 = 0 \\ -4 \leq a_2 \leq -2 \end{matrix}$ et $\begin{matrix} a_1 = 1 \\ -4 \leq a_2 \leq -2 \end{matrix}$ ont été étudiés dans la partie I .

Les résultats sont contenus dans la liste suivante :

polynôme $g(X)$	discriminant de l'extension $Q(\rho_1)$ engendrée par une racine de g
$X^3 - 3X + 1$	81 cyclique
$X^3 - 4X + 1$	229
$X^3 - X^2 - 2X - 1$	49 cyclique
$X^3 + X^2 - 3X - 1$	$148 = 4 \times 37$
$X^3 - 4X + 2$	$148 = 4 \times 37$
$X^3 + X^2 - 4X + 1$	169 cyclique
$X^3 + X^2 - 4X - 1$	321
$X^3 + X^2 - 4X - 2$	4×79
$X^3 + X^2 - 4X - 3$	257
$X^3 - 5X + 1$	473
$X^3 - 5X + 3$	257
$X^3 + X^2 - 5X + 2$	229
$X^3 + X^2 - 5X + 1$	$404 = 4 \times 101$
$X^3 + X^2 - 5X - 1$	$148 = 4 \times 37$
$X^3 + X^2 - 5X - 3$	4×141
$X^3 + X^2 - 5X - 4$	469

Quand nous n'avons rien indiqué à droite, $Q(\rho_1)$ est non cyclique sur Q . Nous avons indiqué à droite la décomposition en puissances de nombres premiers distincts. Si G_1 est une extension non cyclique de degré 3 sur Q de clôture galoisienne N , si k est le sous-corps quadratique de N , d le discriminant de k , D le discriminant de G_1

$$D = df^2$$

pour les discriminants de la liste ci-dessus, il y a une seule décomposition possible donc un seul k et un seul N .

Par suite, quand dans la liste précédente 2 polynômes nous donnent le même discriminant, il suffit de garder un seul de ces deux polynômes. Si F_1 est tel que $Q(\rho_1)$ soit engendré par une racine d'un polynôme de la liste précédente, d'après le théorème 4, F_1 est engendré par une racine $\hat{e}$ d'un polynôme $\Phi_1(X)$

$$\Phi_1(X) = X^3 + \lambda_{11}X^2 + \lambda_{12}X + \lambda_{13}$$

tel que

$$0 < \frac{2}{3}\,\mathrm{Tr}\,Q(\rho_1)/Q\,(\lambda_{11}^2) - 2\,\mathrm{Tr}\,Q(\rho_1)/Q\,(\lambda_{12}) < \gamma_6\left(\frac{19^4}{3\sqrt{3}\times 7}\right)^{1/3} . \qquad (10)$$

a) <u>Si</u> $Q(\theta)$ <u>est de degré</u> 3 <u>sur</u> Q . Si $Q(\rho_1) = Q(\cos\frac{2\pi}{7})$ nécessairement pour que $Q(\theta,\rho_1)$ soit de degré 9 sur Q le discriminant de $Q(\theta)$ est supérieur ou égal au 2e discriminant minimum pour les extensions de degré 3 totalement réelles, soit 81 . Donc si nous appelons D le discriminant de F_1

$$D \geq (49 \times 81)^3 > 19^8$$

si $Q(\rho_1) \neq Q(\cos\frac{2\pi}{7})$ le discriminant de $Q(\rho_1)$ est supérieur ou égal à 81 . Celui de $Q(\theta)$ est supérieur ou égal à 49 et on a le même résultat.

b) <u>Si</u> $Q(\theta)$ <u>est de degré</u> 9 <u>sur</u> Q .

$$\psi(X) = (X^3+\lambda_{11}X^2+\lambda_{12}X+\lambda_{13})(X^3+\lambda_{21}X^2+\lambda_{22}X+\lambda_{23})(X^3+\lambda_{31}X^2+\lambda_{32}X+\lambda_{33})$$

où λ_{ji} est conjugué de $\lambda_{j'i}$ par un endomorphisme de $Q(\rho_1)$ dans $\mathbb{C}$. $\psi(X)$ est le polynôme minimal de θ . $\psi(X)$ est de degré 9, unitaire, à coefficients dans $\mathbb{Z}$, irréductible dans $Q[X]$, a 9 racines réelles distinctes

$$\psi(X) = X^9 + a'_1X^8 + a'_2X^7 + a'_3X^6 + a'_4X^5 + a'_5X^4 + a'_6X^3 + a'_7X^2 + a'_8X + a'_9$$

$$a'_1 = \mathrm{Tr}\,Q(\rho_1)/Q\,(\lambda_{11})$$

$$a'_2 = \mathrm{Tr}\,Q(\rho_1/Q)(\lambda_{12}) + \frac{1}{2}(\mathrm{Tr}\,Q(\rho_1)/Q\,(\lambda_{11}))^2 - \frac{1}{2}\mathrm{Tr}\,Q(\rho_1)/Q\,(\lambda_{11}^2) .$$

Pour que ψ ait 9 racines réelles distinctes, il faut que $a_1'^2 - 18\,a'_2 > 0$. Nous savons que, en remplaçant éventuellement θ par sa somme avec un entier de $\mathbb{Z}$ et par son opposé, on peut supposer que

$$\lambda_{11} = \alpha_o + \alpha_1 \rho_1 + \alpha_2 \rho_1^2 \quad \text{avec} \quad \alpha_o , \alpha_1 , \alpha_2 \quad \text{élément de} \quad Q$$

$$-\frac{3}{2} < \alpha_1 \leq \frac{3}{2} \quad , \quad -\frac{3}{2} < \alpha_2 \leq \frac{3}{2}$$

et α_o tel que

$$0 \leq \mathrm{Tr}\, Q(\rho_1)/Q(\lambda_{11}) \leq 4 \ .$$

Pour chaque polynôme $g(X)$ de notre liste, dont une racine définit $Q(\rho_1)$ nous calculons une majoration de $\mathrm{Tr}\, Q(\rho_1)/Q(\lambda_{11}^2)$. Avec (10) nous obtenons donc une minoration de a'_2 .

Les résultats sont dans le tableau suivant :

polynôme dont une racine définit $Q(\rho_1)$	discriminant de $Q(\rho_1)$	majoration de $\mathrm{Tr}\, Q(\rho_1)/Q(\lambda_{11}^2)$	minoration de $a'_2 - a'^2_1/2$
$X^3 - 3X + 1$	81	12	-23,95
$X^3 + X^2 - 2X - 1$	49	10	-23,35
$X^3 + X^2 - 3X - 1$	4×37	18	-29,39
$X^3 + X^2 - 4X + 1$	169	36	-46,54
$X^3 + X^2 - 4X - 1$	321	28	-38,04
$X^3 + X^2 - 4X - 2$	4×79	24	-36,20
$X^3 + X^2 - 4X - 3$	257	21	-30,89
$X^3 - 5X + 1$	473	25	-34,44
$X^3 - 4X + 1$	229	18	-28,05
$X^3 + X^2 - 5X + 1$	4×101	47	-56,39
$X^3 + X^2 - 5X - 3$	4×141	32	-43,49
$X^3 + X^2 - 5X - 4$	469	28	-37,44

La majoration de a'_2 est donnée par $a'^2_1 - 18a'_2 > 0$ car $a'^2_1 - 18a'_2$ est le premier coefficient de la matrice M_ψ .

BIBLIOGRAPHIE

[1] BERWICK - Integral Bases. Camb. Tracts on Maths, n° 22.

[2] CASSELS - An introduction to the geometry of numbers.

[3] COHN - Note on fields of small discriminant. Proc. Amer. Math. Soc. 3 (1952), pp. 713-714.

[4] DAVENPORT - The product of n homogeneous linear forms. Indag Math. 8 (1946), pp. 524-541.

[5] GANTMACHER - Théorie des matrices, t.2, Dunod.

[6] GODWIN - The determination of fields of small discriminant with a given subfield. Math. Scand. 6 (1958), pp. 40-46.

[7] HUNTER - The minimum discriminant of quintic fields. Proc. Glasgow Math. Association, vol. III (1957).

[8] KAUR - The minimum discriminant of sixth degree totally real algebric number fields. Journal of the Indian Math. Soc. (1970), pp. 123-134.

[9] LIANG et ZASSENHAUS - The minimum discriminant of sixth degree totally complex algebraic number fields. Journal of number theory, 9 (1977), pp. 16-35.

[10] MARTINET - Sur l'arithmétique des extensions galoisiennes à groupe de Galois diédral d'ordre 2p .

[11] POHST - The minimum discriminant of seventh degree totally real algebraic number fields. Journal of number theory (à paraître).

Laboratoire de Mathématiques Pures - Institut Fourier
dépendant de l'Université Scientifique et Médicale de Grenoble
associé au C.N.R.S.
B.P. 116
38402 ST MARTIN D'HERES (France)