

# ANNALES DE L'INSTITUT FOURIER

MICHEL OLIVIER

## **Corps sextiques primitifs**

*Annales de l'institut Fourier*, tome 40, n° 4 (1990), p. 757-767

[http://www.numdam.org/item?id=AIF\\_1990\\_\\_40\\_4\\_757\\_0](http://www.numdam.org/item?id=AIF_1990__40_4_757_0)

© Annales de l'institut Fourier, 1990, tous droits réservés.

L'accès aux archives de la revue « Annales de l'institut Fourier » (<http://annalif.ujf-grenoble.fr/>) 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/>

## CORPS SEXTIQUES PRIMITIFS

par Michel OLIVIER

---

### 1. Introduction.

Dans deux articles précédents [1] et [7], nous décrivons dix tables de corps sextiques imprimitifs (quatre tables de corps sextiques contenant un corps quadratique, et six tables de corps sextiques avec un sous-corps cubique). Pour chaque signature, nous donnons le type de la clôture galoisienne : pour chacun des douze types possibles, figure dans nos tables le discriminant minimal. Le calcul de ces corps imprimitifs est basé sur une méthode de géométrie des nombres et l'utilisation de méthodes relatives qui tirent profit de l'existence d'un sous-corps.

Afin d'être exhaustif, nous donnons ici quatre tables étendues de corps sextiques primitifs (une par signature). Les techniques de calculs utilisées sont celles de M. Pohst dans [8] et de F. Diaz y Diaz in [5] ; étant donnée une borne  $M$  (dépendant de la signature) pour la valeur absolue du discriminant  $d_K$  du corps sextique  $K = \mathbb{Q}(\theta)$ , où  $\theta$  est racine du polynôme

$$P(X) = X^6 + a_1X^5 + a_2X^4 + a_3X^3 + a_4X^2 + a_5X + a_6$$

irréductible sur  $\mathbb{Z}[X]$ , leur méthode, basée sur des considérations de géométrie des nombres, permet de majorer la valeur absolue des coefficients  $a_i$ , qu'il suffit de considérer pour trouver tous les corps sextiques dont la valeur absolue du discriminant est inférieure à  $M$ . Ceci permet donc de limiter la recherche à un nombre fini de polynômes  $P(X)$  ; les bornes  $M$  choisies sont respectivement  $10^7$  ( $10^6$ ,  $4 \cdot 10^5$  et  $2 \cdot 10^5$ ) pour la signature  $r_1 = 6(4, 2, 0)$ , où  $r_1$  est le nombre de places réelles de  $K$ .

---

*Mots-clés* : Corps sextiques - Groupe de Galois.

*Classification A.M.S.* : 11R21.

L'algorithme de construction des tables comporte les étapes suivantes :

- (1) Trouver des polynômes de bonne signature susceptibles de définir tous les corps sextiques  $K$  de discriminant  $|d_K| \leq M$  ;
- (2) Tester l'irréductibilité de ces polynômes et éliminer ceux qui définissent des corps imprimitifs ;
- (3) Calculer le discriminant du corps sextique défini par chacun des polynômes précédents ;
- (4) Tester les isomorphismes des corps de même discriminant ;
- (5) Calculer le type de la clôture galoisienne de chacun des corps sextiques.

Le paragraphe 2 fixe les notations utilisées dans la suite ; la recherche des polynômes est l'objet du paragraphe 3 et consiste en un rappel des techniques décrites dans [8] ; les tests d'irréductibilité et d'imprimitivité sont donnés dans le paragraphe 4 ; le paragraphe 5 est consacré au calcul du discriminant et aux tests d'isomorphismes des corps sextiques ; le calcul du type de la clôture galoisienne des corps obtenus est fondé sur une méthode due à Stauduhar (cf. [9]) qui est décrite dans notre cas particulier au paragraphe 6.

Enfin, le dernier paragraphe est consacré à la description des tables obtenues.

*Remerciements.* Cet article doit beaucoup aux conseils avisés et à l'expérience de F. Diaz y Diaz dans le calcul des corps de nombres de petits discriminants. En outre, de nombreux préalables dus à la nécessité de calculer avec des entiers de grande taille sont levés grâce à l'utilisation intensive du système PARI développé à l'Université de Bordeaux I sous la supervision de H. Cohen par C. Batut, D. Bernardi et l'auteur ; ce système contient la plupart des algorithmes de calcul dans les corps de nombres, ce qui a réduit considérablement la programmation. Ce système est implanté sur des stations SUN dont l'installation et la maintenance sont partiellement financées par le « P.R.C. mathématiques-informatique ».

## 2. Notations.

Le corps sextique est noté  $K$ , son discriminant  $d_K$  ; il est défini par un élément primitif  $\theta$  de polynôme minimal

$$P(X) = X^6 + a_1X^5 + a_2X^4 + a_3X^3 + a_4X^2 + a_5X + a_6$$

irréductible sur  $\mathbb{Z}[X]$ . Nous noterons  $(\theta_1, \theta_2, \theta_3, \theta_4, \theta_5, \theta_6)$  les racines de  $P$  dans une clôture algébrique de  $\mathbb{Q}$ ;  $M$  est la borne choisie pour les discriminants  $|d_K|$ , et  $d_P$  est le discriminant du polynôme  $P$ .

Suivant M. Pohst, nous utiliserons dans la suite les quantités :

$$S_m(\theta) = \sum_{i=1}^6 \theta_i^m, \quad T_m(\theta) = \sum_{i=1}^6 |\theta_i|^m, \quad \text{pour } m \in \mathbb{Z}.$$

### 3. Recherche des polynômes.

Nous donnons ici le détail des calculs pour le cas des corps sextiques totalement réels; dans cette situation, nous disposons d'un grand nombre d'inégalités qui limitent le nombre de polynômes à tester par la suite.

En effet, la forme bilinéaire symétrique  $(x, y) \mapsto \text{Trace}(xy)$  est définie positive sur  $\mathbb{Z}[\theta]$ , si bien que ses restrictions à tout sous-module le sont aussi. On obtient ainsi les inégalités suivantes qui servent — si elles ne sont pas satisfaites par  $P$  — à éliminer ce polynôme :

$$12a_4a_6 < 5a_5^2, \quad 15a_3a_5 < 8a_4^2, \quad 16a_2a_4 < 9a_3^2,$$

$$15a_1a_3 < 8a_2^2, \quad 12a_2 < 5a_1^2$$

$$5(-5a_1^3 + 18a_1a_2 - 27a_3)^3 < (5a_1^2 - 12a_2)^3,$$

$$S_2(\theta) > 0, \quad S_4(\theta) > 0, \quad S_6(\theta) > 0, \quad S_2(\theta)^2 < 6S_4(\theta),$$

$$S_3(\theta)^2 < 6S_6(\theta), \quad S_3(\theta)^2 < S_2(\theta)S_4(\theta), \quad S_4(\theta)^2 < S_2(\theta)S_6(\theta),$$

$$S_5(\theta)^2 < S_4(\theta)S_6(\theta),$$

$$6S_2(\theta)S_4(\theta) + 2S_1(\theta)S_2(\theta)S_3(\theta) - S_2(\theta)^3 - S_1(\theta)^2S_4(\theta) - 6S_3(\theta)^2 > 0,$$

$$6S_2(\theta)S_6(\theta) + 2S_1(\theta)S_3(\theta)S_4(\theta) - S_2(\theta)S_3(\theta)^2 - 6S_4(\theta) - S_1(\theta)^2S_6(\theta) > 0,$$

$$6S_4(\theta)S_6(\theta) + 2S_2(\theta)S_3(\theta)S_5(\theta) - S_3(\theta)^2S_4(\theta) - S_2(\theta)^2S_6(\theta) - 6S_5(\theta)^2 > 0,$$

$$S_2(\theta)S_4(\theta)S_6(\theta) + 2S_3(\theta)S_4(\theta)S_5(\theta) - S_4(\theta)^3 - S_2(\theta)S_5(\theta)^2 - S_3(\theta)^2S_6(\theta) > 0.$$

• Il n'y a que 4 valeurs de  $a_1$  à considérer : changer  $a_1$  en  $a_1 + n$  ( $n \bmod 6$ ), puis  $a_1$  en  $-a_1$ . On choisit donc  $a_1$  parmi l'ensemble  $\{0, -1, -2, -3\}$ .

• Pour limiter le choix de  $a_2$ , nous utilisons l'inégalité (cf. J. Martinet, [6], Théorème 2.8), qui s'écrit dans notre cas particulier :

$$S_2(\theta) \leq \frac{a_1^2}{6} + \left(\frac{4M}{3}\right)^{1/5}.$$

Remarquons que  $S_2$  est  $\geq 7$ ; en effet,  $a_6^2 = \prod_{1 \leq i \leq 6} |\theta_i|^2 \leq (S_2(\theta)/6)^6$

(inégalité entre moyenne arithmétique et moyenne géométrique); comme  $a_6 \neq 0$ , on a  $1 \leq a_6^2 \leq (S_2(\theta)/6)^6$ , ce qui donne  $S_2(\theta) \geq 6$ ; si  $S_2(\theta) = 6$ , il y a égalité entre moyenne arithmétique et moyenne géométrique, et les racines de  $P$  sont égales, ce qui ne peut être.

Posons  $c_1 = (4M/3)^{1/5}$ ; les deux inégalités précédentes et l'égalité  $S_2(\theta) = a_1^2 - 2a_2$  entraînent :

$$\frac{5}{12} a_1^2 - \frac{1}{2} c_1 \leq a_2 \leq \frac{1}{2} a_1^2 - \frac{7}{2}.$$

- On vient de voir ci-avant que  $a_6 \neq 0$  et  $|a_6| \leq (S_2(\theta)/6)^3$ .
- Connaissant  $a_1$ ,  $a_2$  et  $a_6$ , il s'agit maintenant de limiter la recherche de  $a_3$ . On utilise la méthode de Pohst ([8], Théorème 4) :

- (1) Pour  $t = 1, 2, 3, 4, 5$ , on calcule la plus petite racine  $\alpha_t$  de l'équation

$$t \left( \frac{|a_6|}{x^{6-t}} \right)^2 + (6-t)x^2 = S_2(\theta);$$

- (2) Puis, pour  $m = -1, 1, 3, 4, 5$ , on évalue

$$T_m = \max_{1 \leq t \leq 5} \left( t \left( \frac{|a_6|}{\alpha_t^{6-t}} \right)^m + (6-t)\alpha_t^m \right).$$

On sait qu'alors pour  $m = -1, 1, 3, 4, 5$  on a  $|S_m(\theta)| \leq T_m$ . Ceci nous permet de borner  $S_3(\theta)$  d'où  $a_3$ , puisque  $a_3 = -(S_3(\theta) + a_1 S_2(\theta) + a_2 S_1(\theta))/3$ .

- Au lieu de borner directement  $a_4$  et  $a_5$ , on cherche des inégalités sur  $P(1)$  et  $P(-1)$ ; on a

$$a_4 = \frac{P(1) + P(-1)}{2} - (1 + a_2 + a_6),$$

$$a_5 = \frac{P(1) - P(-1)}{2} - (a_1 + a_3).$$

Il suffit alors d'écrire :

$$|P(1)|^2 = \prod_{i=1}^6 (1 - 2\theta_i + \theta_i^2) \leq \left( \frac{1}{6} (6 - 2S_1(\theta) + S_2(\theta)) \right)^6$$

$$|P(-1)|^2 = \prod_{i=1}^6 (1 + 2\theta_i + \theta_i^2) \leq \left( \frac{1}{6} (6 + 2S_1(\theta) + S_2(\theta)) \right)^6.$$

Ceci, ajouté à la congruence  $P(1) + P(-1) \equiv 0 \pmod{2}$ , permet de borner  $a_4$  et  $a_5$ ; notons que l'on doit avoir aussi  $|a_5| \leq |a_6| T_{-1}$ , ce qui élimine quelques polynômes.

• On vérifie enfin à l'aide de l'algorithme de Sturm, que le polynôme obtenu est bien totalement réel et que son discriminant  $d_p$  n'est pas nul.

Avec la borne  $M = 10^7$  choisie pour cette signature, on obtient une table d'environ 600 000 polynômes.

Dans le cas des autres signatures, il faut essentiellement remplacer les  $S_m(\theta)$  par les  $T_m(\theta)$ . Nous obtenons pour  $r_1 = 4$  (resp. 2 et 0) et  $M = 10^6$  (resp.  $4 \cdot 10^5$  et  $2 \cdot 10^5$ ) une table de 1 500 000 (resp. 2 000 000 et 200 000) polynômes. Les temps d'exécution des programmes sont très divers (de quelques heures à quelques jours!).

#### 4. Irréductibilité et imprimitivité.

• On teste d'abord en les comparant avec chacun des 9 polynômes irréductibles de degré 6 modulo 2 si  $P$  est irréductible modulo 2; s'il ne l'est pas, on calcule une approximation des racines et on teste si l'une des racines est entière, puis si besoin, la divisibilité de  $P$  par les différents facteurs possibles de degré 2 et 3 (dépendant de la signature). Dans le cas le plus favorable ( $r_1=6$ ), il y a au plus 6 essais pour les facteurs de degré 1, 15 pour les facteurs de degré 2 et 20 pour les facteurs de degré 3. Le cas le plus favorable est  $r_1 = 0$ , où il n'y a au plus que 3 essais à faire (facteurs de degré 2).

• L'existence d'un sous-corps quadratique (resp. cubique) est testé de la façon suivante: si  $d_p$  n'est divisible par aucun cube (resp. carré) de discriminant de corps quadratique (resp. cubique) inférieur à  $d_p^{1/3}$  (resp.  $d_p^{1/2}$ ), alors  $K$  est primitif.

Sinon, on utilise une approximation des racines de  $P$  et les remarques suivantes.

Il existe un sous-corps quadratique  $k_2$  si et seulement si on peut trouver une partition de l'ensemble des 6 racines de la forme  $\{\theta_1, \theta_i, \theta_j\}$ ,  $\{\theta_k, \theta_l, \theta_m\}$  telle que: si  $\{s_1, s_2, s_3\}$  sont les fonctions symétriques élémentaires de  $\theta_1, \theta_i, \theta_j$  et  $\{t_1, t_2, t_3\}$  celles de  $\theta_k, \theta_l, \theta_m$ , alors, les  $s_i$  sont des entiers de  $k_2$  de conjugués les  $t_i$ , et  $k_2 = \mathbb{Q}(s_1, s_2, s_3)$  si les  $s_3$  ne sont pas tous dans  $\mathbb{Z}$ ; dans le cas contraire, on démontre qu'il y a un sous-corps cubique  $k_3$  de discriminant  $d_{k_3}$  et  $k_2 = \mathbb{Q}(\sqrt{d_{k_3}})$ .

Il existe un sous-corps cubique  $k_3$  si et seulement si on peut trouver une partition des racines de la forme  $\{\theta_1, \theta_i\}$ ,  $\{\theta_j, \theta_k\}$ ,  $\{\theta_l, \theta_m\}$  telle que les fonctions symétriques élémentaires  $s_1, s_2$  de  $\theta_1, \theta_i$  soient des entiers de  $k_3$  dont les conjugués sont les fonctions symétriques  $t_1, t_2, u_1, u_2$  des autres ensembles de la partition.

On élimine ainsi environ 10 % des polynômes trouvés dans les tables précédentes.

### 5. Calcul du discriminant et tests d'isomorphismes.

• *Discriminant.* Le calcul du discriminant repose sur le test suivant (Dedekind) : soit  $f$  tel que  $d_p = f^2 d_K$  et  $p$  un nombre premier tel que  $p^2$  divise  $d_p$  ; dans  $\mathbb{F}_p[X]$ , soit

$$\bar{P}(X) = \prod_{i=1}^t \bar{P}_i(X)^{k_i}$$

la décomposition de  $P$  en facteurs premiers. Posons

$$\bar{A}(X) = \prod_{i=1}^t \bar{P}_i(X),$$

$$\bar{B}(X) = \prod_{i=1}^t \bar{P}_i(X)^{k_i-1},$$

$$\bar{C}(X) = (\bar{A}(X), \bar{B}(X)),$$

$$\bar{D}(X) = -\frac{1}{p}(A(X)B(X) - P(X)),$$

où  $A$  (resp.  $B$ ) relève  $\bar{A}$  (resp.  $\bar{B}$ ) dans  $\mathbb{Z}[X]$ .

On a alors :  $p$  divise  $f$  si et seulement si  $(\bar{C}(X), \bar{D}(X)) \neq 1$  dans  $\mathbb{F}_p[X]$ .

Si  $d_p = (q_1 \dots q_k)(p_1^{m_1} \dots p_l^{m_l})^2$  est la décomposition de  $d_p$  en facteurs premiers (les  $q_i$  ne sont pas forcément différents des  $p_j$ ), posons  $d = q_1 \dots q_k$  ; pour  $i = 1$  à  $l$ , tester si  $p_i | f$  : si  $p_i \nmid f$ , changer  $d$  en  $d p_i^{2m_i}$  ; si  $d > M$ , éliminer  $P$  de la table ; sinon tester  $p_{i+1}$ .

Ce test élimine 95 % des corps sextiques pour cause de discriminant trop grand. Parmi les 5 % restant seuls 20 % des discriminants de  $K$  sont effectivement calculés par l'algorithme de Dedekind.

Pour les autres corps, on met en œuvre l'algorithme « ROUND TWO » de Zassenhaus dans une version due à D. Ford, implantée sur le système PARI.

• *Isomorphismes.* Il s'agit de tester si deux corps sextiques primitifs de même discriminant sont  $\mathbb{Q}$ -isomorphes ou non. La méthode utilisée est expliquée dans [1], § 5. On trouve environ dix polynômes pour un corps sextique dans chaque table. On choisit un polynôme donnant le plus petit indice de  $\mathbb{Z}[\theta]$  dans l'anneau des entiers de  $K$ .

### 6. Clôture galoisienne.

On peut faire correspondre à tout corps sextique un groupe transitif de degré 6. Il y a 16 groupes en degré 6, dont une classification a été donnée par G. Butler et J. McKay dans [4]. Pour les corps sextiques primitifs, seuls 4 des 16 groupes sont possibles. On trouvera ci-après la liste de ces cas selon la signature.

$$\begin{aligned} A_5: r_1 &= 6, 2 \\ S_5: r_1 &= 6, 2, 0 \\ A_6: r_1 &= 6, 2 \\ S_6: r_1 &= 6, 4, 2, 0, \end{aligned}$$

où  $S_n$  (resp.  $A_n$ ) désigne le groupe symétrique (resp. alterné) sur  $n$  lettres.

Pour reconnaître le type de la clôture galoisienne, on utilise un algorithme décrit par R. P. Stauduhar dans [9] : on considère le polynôme résolvant

$$\begin{aligned} F(X_1, X_2, X_3, X_4, X_5, X_6) &= (X_1 X_2 + X_3 X_5 + X_4 X_6)(X_1 X_3 + X_4 X_5 + X_2 X_6) \\ &\quad (X_3 X_4 + X_1 X_6 + X_2 X_5)(X_1 X_5 + X_2 X_4 + X_3 X_6) \\ &\quad (X_1 X_4 + X_2 X_3 + X_5 X_6). \end{aligned}$$

S'il existe une permutation  $\sigma \in S_6$  telle que  $F(\theta_{\sigma(1)}, \theta_{\sigma(2)}, \theta_{\sigma(3)}, \theta_{\sigma(4)}, \theta_{\sigma(5)}, \theta_{\sigma(6)})$  soit dans  $\mathbb{Z}$ , alors le type est  $A_5$  ou  $S_5$  selon que  $d_K$  est un carré ou non. Dans le cas contraire, le type est  $A_6$  ou  $S_6$  selon que  $d_K$  est un carré ou non.

### 7. Description des tables et commentaires.

Voici le nombre de corps sextiques primitifs figurant dans les tables, suivant la signature et le type :

sign.	$ d_K $ max.	$A_5$	$A_6$	$S_5$	$S_6$
6	9979841	0	0	0	177
4	994787	×	×	×	312
2	399925	2	1	0	934
0	199664	×	×	0	220

(« × » signifie « impossible »).

Remarquons que l'indice  $\mathbb{Z}[\theta]$  dans l'anneau des entiers de  $K$  est presque toujours égal à 1 dans les tables (on a systématiquement choisi, parmi tous les polynômes trouvés qui définissent le même corps sextique, celui qui donne le plus petit indice); il y a pour  $r_1 = 6$  (resp. 4, 2, 0) 3 (resp. 4, 37, 1) exceptions.

Nous donnons maintenant le tableau des discriminants minimaux des corps sextiques primitifs pour les différents types dans chaque signature: ceux qui n'ont pas été trouvés dépassent largement les possibilités effectives de nos algorithmes et de nos ordinateurs, et les tables existantes en degré 5 ne permettent pas de trouver les discriminants minimaux pour les types  $A_5$  et  $S_5$ .

sign.	(6,0)	(4,1)	(2,2)	(0,3)
type $A_5$	?	×	287296	×
type $A_6$	?	×	287296	×
type $S_5$	?	×	?	?
type $S_6$	592661	-92779	29077	-14731

(« × » signifie « impossible »; « ? » signifie « non trouvé »).

Noter l'égalité en signature (2,2) des minima pour les types  $A_5$  et  $A_6$  (voir ci-après).

Signalons qu'il n'y a coïncidences de discriminants que dans la table en signature (2,2) dans laquelle figurent 9 doublons parmi lesquels les deux corps suivants de discriminant  $287296 = (2^3 \cdot 67)^2$ , l'un de type  $A_5$

défini par le polynôme

$$x^6 + 2x^5 + x^4 + 4x^3 + 2x^2 - 4x + 1,$$

l'autre de type  $A_6$  défini par  $x^6 + 2x^5 - x^4 + 2x^2 - 1$  (les indices sont égaux à 1).

Soit  $f(x)$  le premier de ces polynômes; son polynôme résolvant s'écrit  $f_1(x) = (x-580)f_2(x)$ , où

$$f_2(x) = x^5 - 436x^4 - 50552x^3 - 2486048x^2 - 58353392x - 612934720$$

est de groupe de Galois  $A_5$  et de discriminant  $(2^3 \cdot 67)^2 \cdot a^2$ , avec  $a = (2^{13} \cdot 67^2 \cdot 257 \cdot 4438639)^2$ . En appliquant à  $f_2$  l'algorithme « POLRED » (dû à H. Cohen et F. Diaz y Diaz) implanté dans PARI, on obtient le polynôme  $f_3(x) = x^5 + 2x^3 - 4x^2 + 6x - 4$ , de discriminant  $(2^3 \cdot 67)^2 \cdot 2^2$  (le corps quintique défini par  $f_3$  a pour discriminant  $(2^3 \cdot 67)^2$ , comme le corps sextique de départ).

Revenons au polynôme  $f$ : l'application à  $f$  de l'algorithme « POLRED » donne entre autres le polynôme

$$g(x) = x^6 + 2x^5 + x^4 - 2x^3 + 2x^2 - 4x + 1;$$

comme l'a remarqué Brumer,  $f$  et  $g$  possèdent une interprétation modulaire (cf. [3]). La jacobienne  $J(67)$  de la courbe  $X(67)$  est canoniquement isogène à un produit  $J^+(67) \times J^-(67)$  de deux variétés abéliennes. On sait (cf. [2], table 5, p. 137) que  $J^+(67)$  est irréductible et que  $J^-(67)$  est isogène à un produit  $J_1^-(67) \times J_2^-(67)$ , où  $J_1^-$  est la courbe elliptique décrite dans [2], table 1, p. 89, et  $J_2^-$  est irréductible. Les variétés abéliennes  $J^+(67)$  et  $J_2^-(67)$  sont à multiplications réelles

(par  $\mathcal{O} = \mathbb{Z} \left[ \frac{1 + \sqrt{5}}{2} \right]$ , d'où le groupe de Galois par l'isomorphisme

$A_5 \simeq Gl(\mathcal{O}/2\mathcal{O})$ ), et sont des jacobiniennes de courbes de genre 2. Or, Brumer donne dans [3] la famille suivante à trois paramètres  $b, c, d$  décrivant les courbes de genre 2 dont les jacobiniennes sont à multiplications réelles :

$$\begin{aligned} y^2 = & x^6 + 2cx^5 + (c^2 + 2c + 2 - bd)x^4 \\ & + (2c^2 + 2c + 2 + b - 2bd - 4d)x^3 \\ & + (c^2 + 4c + 5 + 3b - bd)x^2 + (2c + 6 + 3b)x + (b + 1). \end{aligned}$$

On obtient l'équation  $y^2 = g(-x)$  (resp.  $y^2 = f(-x)$ ) en donnant aux paramètres les valeurs  $(0, -1, 0)$  (resp.  $(0, -1, 3/2)$ ). La première correspond à  $J^+(67)$  et la seconde à  $J_2^-(67)$ .

Enfin, nous donnons pour chaque signature les dix premiers corps figurant dans les tables. Des tables plus étendues seront publiées dans la revue « Séminaire de Théorie des Nombres de Bordeaux » ; elles sont disponibles auprès de l'auteur, soit sur papier, soit sur support magnétique (fichier source TEX).

Les colonnes contiennent (de gauche à droite) le discriminant  $d_K$  de  $K$ , la factorisation de  $d_K$ , le type de la clôture galoisienne, l'indice et un polynôme définissant  $K$ .

## signature (6,0)

592661	592661	S6	1	$x^6 + 2x^5 - 5x^4 - 4x^3 + 5x^2 + x - 1$
1134389	1134389	S6	1	$x^6 + x^5 - 6x^4 - 7x^3 + 5x^2 + 6x + 1$
1202933	$79 \times 15227$	S6	1	$x^6 - 9x^4 - 9x^3 + 4x^2 + 5x + 1$
1541581	1541581	S6	1	$x^6 - 8x^4 + 18x^2 + x - 11$
1868969	$107 \times 17467$	S6	1	$x^6 - 10x^4 + 3x^3 + 9x^2 - 6x + 1$
2286997	$349 \times 6553$	S6	1	$x^6 - 10x^4 - 6x^3 + 22x^2 + 17x - 5$
2323397	2323397	S6	1	$x^6 + 3x^5 - 9x^4 - 42x^3 - 45x^2 - 10x + 1$
2460365	$5 \times 263 \times 1871$	S6	1	$x^6 + x^5 - 8x^4 - 4x^3 + 17x^2 - x - 1$
2495261	$199 \times 12539$	S6	1	$x^6 + x^5 - 6x^4 - 6x^3 + 6x^2 + 6x + 1$
2501557	$769 \times 3253$	S6	1	$x^6 + 2x^5 - 9x^4 - 8x^3 + 23x^2 + 7x - 17$

## signature (4,1)

-92779	-92779	S6	1	$x^6 - 6x^4 - 11x^3 - 4x^2 + 2x + 1$
-94363	$-197 \times 479$	S6	1	$x^6 - 2x^4 + 2x^3 - 3x + 1$
-104483	$-163 \times 641$	S6	1	$x^6 + x^5 - 2x^4 - 2x^3 - x^2 + x + 1$
-118987	$-11 \times 29 \times 373$	S6	1	$x^6 + 2x^5 - 3x^4 - 7x^3 - 2x^2 - x - 1$
-133787	$-353 \times 379$	S6	1	$x^6 - 4x^4 - 2x^3 + 2x^2 + 3x + 1$
-161939	$-67 \times 2417$	S6	1	$x^6 + 2x^5 - 2x^4 - 7x^3 + 6x + 1$
-195379	$-47 \times 4157$	S6	1	$x^6 + 3x^5 - 2x^4 + x^3 + 9x^2 + 6x + 1$
-209107	$-67 \times 3121$	S6	1	$x^6 + 3x^5 + 4x^2 - 10x + 1$
-214747	$-13 \times 16519$	S6	1	$x^6 + x^5 - 3x^4 + 2x^3 + 5x^2 - 6x + 1$
-215811	$-3^3 \times 7993$	S6	1	$x^6 + x^5 - 2x^4 + 2x^3 + x^2 - 3x + 1$

## signature (2,2)

29077	29077	S6	1	$x^6 + 2x^5 - x^4 - x^2 - x + 1$
29189	$17^2 \times 101$	S6	1	$x^6 - 4x^4 + 4x^2 + x - 1$
31133	$163 \times 191$	S6	1	$x^6 + x^5 + 2x^4 - x^3 - 3x^2 + 1$
31709	$37 \times 857$	S6	1	$x^6 - 6x^4 - 4x^3 + 4x^2 + 3x + 1$
37253	37253	S6	1	$x^6 + x^5 - 4x^4 - 4x^3 + 3x^2 + 3x + 1$
37568	$2^6 \times 587$	S6	1	$x^6 + 2x^5 + x^4 - 4x^3 - 6x^2 - 4x - 1$
39269	$107 \times 367$	S6	1	$x^6 + 2x^5 - 2x^4 - 5x^3 + 2x^2 + 4x - 1$
40277	40277	S6	1	$x^6 + 2x^5 - 5x^4 - 3x^3 + 4x^2 + x - 1$
41069	$7 \times 5867$	S6	1	$x^6 - 2x^4 + 2x^2 - x - 1$
45301	$89 \times 509$	S6	1	$x^6 + x^5 - x^2 - x - 1$

signature (0,3)

-14731	-14731	S6	1	$x^6 + 3x^5 + 5x^4 + 4x^3 + 3x^2 + 2x + 1$
-20627	-20627	S6	1	$x^6 + x^5 + 5x^4 + 8x^3 + 7x^2 + 4x + 1$
-22291	-22291	S6	1	$x^6 + x^5 - 5x^4 - 2x^3 + 7x^2 - 2x + 1$
-25747	-25747	S6	1	$x^6 + 3x^4 - 4x^3 + 5x^2 - 7x + 3$
-27971	$-83 \times 337$	S6	1	$x^6 + 3x^5 + 8x^4 + 10x^3 + 8x^2 + 4x + 1$
-30808	$-2^3 \times 3851$	S6	1	$x^6 - x^4 - x^3 + x^2 + x + 1$
-31223	-31223	S6	1	$x^6 + 3x^5 + 7x^4 + 6x^3 + 6x^2 + 2x + 1$
-32171	$-53 \times 607$	S6	1	$x^6 + 3x^5 + 9x^4 + 14x^3 + 20x^2 + 15x + 11$
-32911	-32911	S6	1	$x^6 + 3x^5 + 3x^4 - x^3 - 2x^2 + 1$
-33791	-33791	S6	1	$x^6 + 3x^5 + 7x^4 + 10x^3 + 11x^2 + 7x + 2$

## BIBLIOGRAPHIE

- [1] A.-M. BERGÉ, J. MARTINET et M. OLIVIER, The computation of sextic fields with a quadratic subfield, *Math. Comp.*, 54 (1990), 869-884.
- [2] B. J. BIRCH et W. KUYK, éd., *Modular Functions of One Variable IV*, dit « Anvers IV », *Lectures Notes 476* (1975), Springer-Verlag, Heidelberg.
- [3] A. BRUMER, Exercices diédraux et courbes à multiplications réelles, *Actes du Séminaire de théorie des nombres de Paris (1989/1990)*, Birkhäuser, Boston, à paraître.
- [4] G. BUTLER and J. MCKAY, , The transitive groups of degree up to eleven, *Comm. Alg.*, 11 (1983), 863-911.
- [5] F. DIAZ Y DIAZ, Discriminant minimal et petits discriminants des corps de nombres de degré 7 avec 5 places réelles, *J. London Math. Soc.*, 38 (1988), 33-46.
- [6] J. MARTINET, Méthodes géométriques dans la recherche des petits discriminants, *Progress in Mathematics*, 59 (1985), 147-179, Birkhäuser.
- [7] M. OLIVIER, The computation of sextic fields with a cubic subfield and no quadratic subfield, *Math. Comp.* (à paraître).
- [8] M. POHST, On the computation of number fields of small discriminants including the minimum discriminants of sixth degree fields, *J. Number Theory*, 14 (1982), 99-117.
- [9] R. P. STAUDUJAR, The determination of Galois groups, *Math. Comp.*, 27 (1973), 981-996.

Manuscrit reçu le 30 juillet 1990.

Michel OLIVIER,  
Centre de Recherche  
en Mathématique de Bordeaux  
351, cours de la Libération  
F-33405 Talence Cedex.