MATHEMATICS OF COMPUTATION
VOLUME 52, NUMBER 185
JANUARY 1989, PAGES 161-174

On the Computation of Totally Real Quartic Fields of Small Discriminant*

By Johannes Buchmann and David Ford

Abstract. All totally real quartic fields of discriminant less than 10^6 are computed. The method used to generate the fields is derived from Delone and Faddeev, with corrections and improvements. A new method for deciding field isomorphism is used to eliminate redundant examples. Integral bases and Galois groups are given for each field.

1. Introduction. In [3, pp. 184-200] Delone and Faddeev give a number-geometric method for computing generating equations for all totally real quartic fields of discriminant not exceeding a fixed upper bound $L \in \mathbf{R}^{>0}$. This method is well suited for implementation on a computer. Unfortunately, the original paper contains many mistakes, and the proofs are sometimes hard to understand.

In the present paper we give a corrected version of the Delone-Faddeev algorithm, we describe its implementation, and we give a table of all totally real quartic fields of discriminant less than 1,000,000, including their integral bases and the Galois groups of their normal closures.

A different method for computing totally real quartic fields was given by Godwin [6], and for general algorithms for computing fields of small discriminants, see Martinet [8] and Pohst [9], [10].

2. Computing Finitely Many Generating Equations. Each totally real quartic field F will be given by a generating polynomial

$$f(x) = x^4 - sx^3 + px^2 - qx + n \in \mathbf{Z}[x], \tag{2.1}$$

i.e., a root ρ of the irreducible polynomial f generates F over $\mathbf{Q}$. We will now describe a method for computing finitely many generating polynomials f, among which generating polynomials for all the fields under consideration can be found. This is done by first proving that the rings of integers $\mathcal{O}_F$ of those fields contain "small" irrationalities α. We then show how to compute the characteristic polynomials of all such quartic irrationalities. But since α might also be a quadratic irrationality, we then explain how to compute generating equations for the remaining quadratic extensions of the quadratic fields $\mathbf{Q}(\alpha)$. For this section we fix a totally real quartic field F, we denote by Δ_F its discriminant and by $\mathcal{O}_F$ its ring of integers. Also, for every number ξ in F we denote by $\xi_1, \xi_2, \xi_3, \xi_4$ its conjugates.

Received September 21, 1987; revised January 29, 1988.
1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 11-04, 11R16, 11Y40.
*Research supported in part by the Natural Sciences and Engineering Research Council (Canada) and Fonds pour la Formation de Chercheurs et l'Aide à la Recherche (Quebec).

(a) "*Small*" *irrationalities in* $\mathcal{O}_F$. For each α in $\mathcal{O}_F$ we consider the projection $\varphi(\alpha)$ of its *conjugate vector*

$$\boldsymbol{\alpha} = (\alpha_1, \alpha_2, \alpha_3, \alpha_4)^t$$

onto the trace zero hyperplane

$$H = \{\mathbf{x} = (x_1, x_2, x_3, x_4)^t \in \mathbf{R}^4 \mid x_1 + x_2 + x_3 + x_4 = 0\}$$

parallel to the vector $\mathbf{1}$. Since the vectors

$$\mathbf{x}_1 = \tfrac{1}{2}(1, 1, -1, -1)^t, \quad \mathbf{x}_2 = \tfrac{1}{2}(1, -1, 1, -1)^t, \quad \mathbf{x}_3 = \tfrac{1}{2}(-1, 1, 1, -1)^t$$

form an orthonormal basis of H, this projection is given by the formula

$$\varphi(\alpha) = \sum_{i=1}^{3} (\mathbf{x}_i, \boldsymbol{\alpha})\mathbf{x}_i, \tag{2.2}$$

where (,) denotes the standard inner product on $\mathbf{R}^4$. We put

$$\Lambda = \varphi(\mathcal{O}_F).$$

(2.3) PROPOSITION. *The mapping* $\varphi\colon \mathcal{O}_F \mapsto \mathbf{R}^4$ *is a* $\mathbf{Z}$*-module homomorphism with kernel* $\mathbf{Z}$.

Proof. Formula (2.2) shows that φ is in fact additive and $\mathbf{Z}$-linear, and since 1 can always be taken as the first element of a $\mathbf{Z}$-module basis of $\mathcal{O}_F$, only the rational integers are projected by φ onto $\mathbf{0}$. □

(2.4) COROLLARY. *The set* $\Lambda = \varphi(\mathcal{O}_F)$ *is a three-dimensional lattice in* $\mathbf{R}^4$ *of determinant* $d(\Lambda) = \frac{1}{2}\sqrt{\Delta_F}$.

Proof. Clearly, by (2.3), Λ is isomorphic to the three-dimensional $\mathbf{Z}$-module $\mathcal{O}_F/\mathbf{Z}$, hence Λ is a lattice of dimension 3. Now let $1, \theta_1, \theta_2, \theta_3$ be an integral basis of $\mathcal{O}_F$. Then the parallelotope which is spanned by the vectors $\mathbf{1}, \boldsymbol{\theta}_1, \boldsymbol{\theta}_2, \boldsymbol{\theta}_3$ is of the same volume as the parallelotope spanned by the vectors $\mathbf{1}, \varphi(\theta_1), \varphi(\theta_2), \varphi(\theta_3)$, namely $\sqrt{\Delta_F}$. But since $\mathbf{1}$ is orthogonal to $\varphi(\theta_i)$ for $1 \le i \le 3$ and because the vectors $\varphi(\theta_1), \varphi(\theta_2), \varphi(\theta_3)$ form a basis of Λ, we have

$$\sqrt{\Delta_F} = \|\mathbf{1}\| \cdot d(\Lambda) = 2d(\Lambda). \quad \square$$

(2.5) PROPOSITION. *The ring* $\mathcal{O}_F$ *contains an irrationality* $\alpha \in \mathcal{O}_F \backslash \mathbf{Z}$ *with* $\operatorname{Tr}(\alpha) \in \{0, 1, 2\}$ *and* $\|\varphi(\alpha)\|^2 \le \sqrt[3]{(\Delta_F/2)}$.

Proof. It is known from Cassels [2, Chapter II, Theorem III] that Λ contains a vector $\mathbf{v} = \varphi(\alpha)$, $\mathbf{v} \ne \mathbf{0}$, with

$$\|\mathbf{v}\|^2 \le (2d(\Lambda)^2)^{1/3}.$$

Now we have by Corollary (2.4)

$$(2d(\Lambda)^2)^{1/3} \le (\Delta_F/2)^{1/3}.$$

By substituting $\pm\alpha + k$ for α with a suitable $k \in \mathbf{Z}$ we can make $\operatorname{Tr}(\alpha) \in \{0, 1, 2\}$. By Proposition (2.3) this substitution does not affect the value of $\|\varphi(\alpha)\|^2$. □

(b) *Case* I: *The "small α" generates F*. We assume in this subsection that $\mathcal{O}_F$ contains a quartic irrationality α which satisfies the conditions of Proposition (2.5), and we let (2.1) be the characteristic polynomial of α, i.e., we assume

$$s \in \{0,1,2\} \quad \text{and} \quad \|\varphi(\alpha)\|^2 \leq \sqrt[3]{(\Delta_F/2)}. \tag{2.6}$$

In order to use (2.6) for deriving bounds on the coefficients p, q, n, we need

(2.7) LEMMA. *The coefficients s and p satisfy $\|\varphi(\alpha)\|^2 = \frac{3}{4}s^2 - 2p$.*

Proof. According to (2.2) we have

$$\|\varphi(\alpha)\|^2 = (\mathbf{x}_1, \boldsymbol{\alpha})^2 + (\mathbf{x}_2, \boldsymbol{\alpha})^2 + (\mathbf{x}_3, \boldsymbol{\alpha})^2,$$

because the vectors $\mathbf{x}_1, \mathbf{x}_2, \mathbf{x}_3$ are pairwise orthogonal. Furthermore, we have

$$\begin{aligned} &4((\mathbf{x}_1, \boldsymbol{\alpha})^2 + (\mathbf{x}_2, \boldsymbol{\alpha})^2 + (\mathbf{x}_3, \boldsymbol{\alpha})^2) \\ &\quad = 3(\alpha_1^2 + \alpha_2^2 + \alpha_3^2 + \alpha_4^2) - 2(\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_1\alpha_4 + \alpha_2\alpha_4 + \alpha_2\alpha_3) \\ &\quad = 3s^2 - 8p. \quad \square \end{aligned}$$

The nice property of this formula is that the coefficients s and p are separated.

(2.8) PROPOSITION. *The coefficients s and p satisfy $-\sqrt[3]{(\Delta_F/16)} \leq p - \frac{3}{8}s^2 < 0$.*

Proof. In view of Lemma (2.7), the second inequality follows immediately from the fact that the length of $\varphi(\alpha)$ is always positive. The first inequality is a direct consequence of condition (2.6). □

(2.9) LEMMA. *The coefficients s, p and q satisfy $(\mathbf{x}_1, \boldsymbol{\alpha}) \cdot (\mathbf{x}_2, \boldsymbol{\alpha}) \cdot (\mathbf{x}_3, \boldsymbol{\alpha}) = \frac{1}{8}(-s^3 + 4sp) - q$.*

Proof. This follows easily by a straightforward application of symmetric functions. □

(2.10) PROPOSITION. *The coefficients s, p and q satisfy $|\frac{1}{8}(-s^3 + 4sp) - q| < \frac{1}{\sqrt{27}}\|\varphi(\alpha)\|^3$.*

Proof. By the inequality between the arithmetic and geometric means we have

$$((\mathbf{x}_1, \boldsymbol{\alpha})^2 (\mathbf{x}_2, \boldsymbol{\alpha})^2 (\mathbf{x}_3, \boldsymbol{\alpha})^2)^{1/3} \leq \frac{1}{3}\|\varphi(\alpha)\|^2,$$

hence, by Lemma (2.9), the result follows. □

In order finally to get bounds on n we need

(2.11) PROPOSITION. *The coefficients s, p, q and n satisfy*
(i) $p^2 - s^2p + \frac{3}{16}s^4 + sq - 4n > 0$;
(ii) $4(p^2 - 3sq + 12n)^3 - (2p^3 - 72pn + 27s^2n - 9sqp + 27q^2)^2 > 0$.

Remark. The left-hand side of (ii) is the polynomial discriminant of f multiplied by 27.

Proof. By [3, p. 184], these conditions are necessary for α to be totally real. □

A further bound is given in

(2.12) PROPOSITION. *The coefficients s, p, q and n satisfy $|n| \leq \frac{1}{16}(s^2 - 2p)^2$.*

Proof. First, we notice that

$$\boldsymbol{\alpha} = \varphi(\alpha) + \frac{s}{4}\mathbf{1}$$

and thus

$$\|\boldsymbol{\alpha}\|^2 = \|\varphi(\alpha)\|^2 + \frac{s^2}{4}.$$

Now we get from the inequality between the geometric and arithmetic means

$$|n|^{1/2} = \left(\prod_{i=1}^{4} |\alpha_i|\right)^{1/4} \leq \|\varphi(\alpha)\|^2 + \frac{s^2}{4}.$$

So it follows from Lemma (2.7) that

$$|n|^{1/2} \leq \frac{1}{4}(s^2 - 2p). \quad \square$$

Using (2.6) and Propositions (2.8), (2.10), (2.11), and (2.12), we can compute a finite number of polynomials (2.1) among which there are generating equations for all those totally real quartic fields which possess a generating integer satisfying (2.6). Notice that the bounds on each coefficient depend on the previous coefficients.

(c) *Case* II: *The "small α" generates a quadratic subfield of F.* We now assume that F does not contain a generating integer satisfying (2.6).

(2.13) PROPOSITION. *The field F contains a quadratic subfield of discriminant $d < \sqrt[3]{(\Delta_F/2)}$.*

Proof. By Proposition (2.5) and by our assumption, F contains a quadratic irrationality α satsifying (2.6). Let d be the discriminant of the quadratic subfield generated by α. Then the area of the lattice generated by $\mathbf{1}$ and $\boldsymbol{\alpha}$ exceeds $2\sqrt{d}$. In fact, this is true, because of the length of $\mathbf{1}$ and $\boldsymbol{\alpha}$ is twice the length of the corresponding quadratic conjugate vector, so the area of our parallelotope is twice the area of the two-dimensional parallelotope. But the area of the parallelotope spanned by $\mathbf{1}$ and $\boldsymbol{\alpha}$ is $\|\varphi(\alpha)\| \cdot 2$, and this proves our assertion. $\square$

We now fix a quadratic subfield K of F, $K = \mathbb{Q}(\sqrt{d})$ with discriminant d and

$$d \leq \sqrt[3]{(\Delta_F/2)}. \tag{2.14}$$

We also let

$$\omega = \begin{cases} \dfrac{\sqrt{d}}{2} & \text{if } d \equiv 0 \bmod 4, \\ \dfrac{1+\sqrt{d}}{2} & \text{if } d \equiv 1 \bmod 4, \end{cases}$$

so 1, ω is an integral basis of K. Since F contains a quadratic subfield, K, there is an automorphism σ of order 2 of F which fixes K. We assume that

$$\sigma(\alpha_1) = \alpha_2 \quad \text{and} \quad \sigma(\alpha_3) = \alpha_4 \tag{2.15}$$

for every α in F. F is generated by a root ρ of a polynomial

$$g(x) = x^2 - \alpha x + \beta \in \mathcal{O}_K[x]. \tag{2.16}$$

Here $\mathscr{O}_K$ denotes the ring of integers of K. Notice that

$$\begin{aligned} \alpha &= \rho_1 + \rho_2, & \beta &= \rho_1 \cdot \rho_2, \\ \alpha' &= \rho_3 + \rho_4, & \beta' &= \rho_3 \cdot \rho_4, \end{aligned} \tag{2.17}$$

where prime denotes conjugation in K. We write

$$\alpha = a_1 + a_2\omega, \qquad \beta = b_1 + b_2\omega$$

with $a_i, b_i \in \mathbb{Z}$, and we want to compute bounds on a_i and b_i such that among the corresponding equations (2.16) a generating equation for F can always be found. For this purpose we consider the projection

$$\begin{aligned} &\lambda\colon \mathscr{O}_F \mapsto \mathbb{R}^4, \\ &\gamma \mapsto \lambda(\gamma) = (\gamma, \mathbf{y}_1)\mathbf{y}_1 + (\gamma, \mathbf{y}_2)\mathbf{y}_2, \end{aligned} \tag{2.18}$$

with

$$\mathbf{y}_1 = \frac{1}{\sqrt{2}}(1, -1, 0, 0)^t, \qquad \mathbf{y}_2 = \frac{1}{\sqrt{2}}(0, 0, 1, -1)^t.$$

Notice that $\mathbf{y}_1$ and $\mathbf{y}_2$ are orthogonal and both of length 1. We also put

$$\Gamma = \lambda(\mathscr{O}_F).$$

(2.19) PROPOSITION. *The projection λ is a $\mathbb{Z}$-module homomorphism with kernel $\mathscr{O}_K$.*

Proof. Again, it is clear from (2.18) that λ is additive and $\mathbb{Z}$-linear. Furthermore, each element γ of the kernel of λ has the property $\gamma_1 = \gamma_2$ and $\gamma_3 = \gamma_4$, which means that γ is an integer in the fixed field K of σ. □

(2.20) PROPOSITION. *The set $\Gamma = \lambda(\mathscr{O}_F)$ is a two-dimensional lattice in $\mathbb{R}^4$ of determinant $d(\Gamma) = \frac{1}{2}\sqrt{(\Delta_F/d)}$.*

Proof. By (2.19) we know that $\Gamma \simeq \mathscr{O}_F/\mathscr{O}_K$, so Γ is a two-dimensional lattice in $\mathbb{R}^4$. Now let $1, \omega, \gamma_1, \gamma_2$ be an integral basis of F. Then the volume of the parallelotope spanned by the vectors $\mathbf{1}, \omega, \gamma_1, \gamma_2$ is the same as the volume of the parallelotope spanned by $\mathbf{1}, \omega, \lambda(\gamma_1), \lambda(\gamma_2)$, namely $\sqrt{\Delta_F}$. On the other hand, for orthogonality reasons we have $\sqrt{\Delta_F} = 2\sqrt{d} \cdot d(\Gamma)$. □

(2.21) PROPOSITION. *There is a generating element $\rho \in \mathscr{O}_F$ with relative trace*

$$\mathrm{Tr}_{F/K}(\rho) \in \{0, 1, \omega, 1+\omega, 2\omega, 1+2\omega, 3\omega, 1+3\omega\} \quad \textit{and} \quad \|\lambda(\rho)\|^4 \le \Delta_F/3d.$$

Proof. We know from Cassels [2, Chapter II, Theorem II] that the lattice Γ contains a vector $\mathbf{v} = \lambda(\rho)$ with $\|\mathbf{v}\|^2 \le 2d(\Gamma)/\sqrt{3}$. Hence, by Proposition (2.20), we have

$$\|\mathbf{v}\|^4 \le 4\Delta_F/4 \cdot 3d = \Delta_F/3d.$$

We now replace ρ by $\rho + k_1 + k_2\omega$ with suitable $k_1, k_2 \in \mathbb{Z}$ so that

$$\mathrm{Tr}_{F/K}(\rho) \in \{0, 1, \omega, 1+\omega\}.$$

This substitution does not affect the value of $\lambda(\rho)$. Since $1, \omega, \rho, \omega\rho$ are independent over $\mathbb{Q}$, either ρ or $\rho + \omega$ must be a quartic irrationality. If ρ is not, then we make the further replacement of ρ by $\rho + \omega$, so that ρ is a generating element of F and

$$\mathrm{Tr}_{F/K}(\rho) \in \{0, 1, \omega, 1+\omega, 2\omega, 1+2\omega, 3\omega, 1+3\omega\}. \quad \square$$

We now let ρ be a generating element of F satisfying the conditions of Proposition (2.21) and we let (2.16) be the corresponding relative quadratic equation, i.e.,

$$\alpha \in \{0, 1, \omega, 1+\omega, 2\omega, 1+2\omega, 3\omega, 1+3\omega\} \quad \text{and} \quad \|\lambda(\rho)\|^4 \leq \Delta_F/3d. \tag{2.22}$$

(2.23) LEMMA. *The elements α, α', β and β' satisfy*

$$\|\lambda(\rho)\|^2 = \frac{1}{2}(\alpha^2 + \alpha'^2) - 2(\beta + \beta'),$$

and

$$(\mathbf{y}_1, \boldsymbol{\rho})^2 - (\mathbf{y}_2, \boldsymbol{\rho})^2 = \frac{1}{2}(\alpha^2 - \alpha'^2) - 2(\beta - \beta').$$

Proof. Since $\mathbf{y}_1$ and $\mathbf{y}_2$ are orthogonal, we see from formula (2.18) that

$$\begin{aligned}\|\lambda(\rho)\|^2 &= (\mathbf{y}_1, \boldsymbol{\rho})^2 + (\mathbf{y}_2, \boldsymbol{\rho})^2 \\ &= \frac{1}{2}[(\rho_1 - \rho_2)^2 + (\rho_3 - \rho_4)^2] \\ &= \frac{1}{2}(\alpha^2 + \alpha'^2) - 2(\beta + \beta').\end{aligned}$$

The other formula is proved analogously. □

(2.24) PROPOSITION. *The elements α, α', β and β' satisfy*

$$0 < \frac{1}{4}(\alpha^2 + \alpha'^2) - (\beta + \beta') \leq \frac{1}{2}\sqrt{(\Delta_F/3d)};$$

$$\left|\frac{1}{4}(\alpha^2 - \alpha'^2) - (\beta - \beta')\right| \leq \frac{1}{2}\sqrt{(\Delta_F/3d)}.$$

Proof. The first two inequalities are an immediate consequence of condition (2.22) and Lemma (2.23), and the third follows from the same argument together with the fact that for any two real numbers x_1, x_2 it always holds that $|x_1^2 - x_2^2| \leq |x_1^2 + x_2^2|$. □

(2.25) PROPOSITION. (i) *If $d \equiv 0 \bmod 4$, then*

$$0 < \frac{1}{16}(4a_1^2 + a_2^2 d) - b_1 \leq \frac{1}{4}\sqrt{(\Delta_F/3d)}$$

and

$$\left|\frac{1}{2}a_1 a_2 - b_2\right| \leq \frac{1}{2}\sqrt{(\Delta_F/3d^2)}.$$

(ii) *If $d \equiv 1 \bmod 4$, then*

$$0 < \frac{1}{8}(4a_1^2 + a_2^2(1+d) + 4a_1 a_2) - 2b_1 - b_2 \leq \frac{1}{2}\sqrt{(\Delta_F/3d)}$$

and

$$\left|\frac{1}{4}(2a_1 a_2 + a_2^2) - b_2\right| \leq \frac{1}{2}\sqrt{(\Delta_F/3d^2)}.$$

Proof. (i) In this case we have $\omega = \sqrt{d}/2$ and so

$$\alpha^2 = \left(a_1 + \frac{1}{2}a_2\sqrt{d}\right)^2 = a_1^2 + \frac{1}{4}a_2^2 d + a_1 a_2\sqrt{d},$$

$$\alpha'^2 = \left(a_1 - \frac{1}{2}a_2\sqrt{d}\right)^2 = a_1^2 + \frac{1}{4}a_2^2 d - a_1 a_2\sqrt{d}.$$

Consequently, $\alpha^2+\alpha'^2 = 2a_1^2+\frac{1}{2}a_2^2d$. However, $\beta+\beta' = b_1+\frac{1}{2}b_2\sqrt{d}+b_1-\frac{1}{2}b_2\sqrt{d} = 2b_1$. Hence, by Proposition (2.24),

$$0 < \frac{1}{4}\left(2a_1^2+\frac{1}{2}a_2^2 d\right) - 2b_1 \le \frac{1}{2}\sqrt{(\Delta_F/3d)}$$

and

$$\left|\frac{1}{2}a_1a_2\sqrt{d} - b_2\sqrt{d}\right| \le \frac{1}{2}\sqrt{(\Delta_F/3d)}$$

or

$$0 < \frac{1}{16}(4a_1^2 + a_2^2d) - b_1 \le \frac{1}{4}\sqrt{(\Delta_F/3d)},$$

and

$$\left|\frac{1}{2}a_1a_2 - b_2\right| \le \frac{1}{2}\sqrt{(\Delta_F/3d^2)}.$$

(ii) In this case we have $\omega = (1+\sqrt{d})/2$ and so

$$\begin{aligned}
\alpha^2 &= \left(a_1 + \frac{1}{2}a_2 + \frac{1}{2}a_2\sqrt{d}\right)^2 \\
&= a_1^2 + \frac{1}{4}a_2^2 + \frac{1}{4}a_2^2d + a_1a_2 + a_1a_2\sqrt{d} + \frac{1}{2}a_2^2\sqrt{d}, \\
\alpha'^2 &= a_1^2 + \frac{1}{4}a_2^2 + \frac{1}{4}a_2^2d + a_1a_2 - a_1a_2\sqrt{d} - \frac{1}{2}a_2^2\sqrt{d}, \\
\alpha^2 + \alpha'^2 &= 2a_1^2 + \frac{1}{2}a_2^2(1+d) + 2a_1a_2, \\
\beta + \beta' &= 2b_1 + b_2,
\end{aligned}$$

and thus

$$\begin{aligned}
\frac{1}{4}(\alpha^2+\alpha'^2) - (\beta+\beta') &= \frac{1}{8}(4a_1^2 + a_2^2(1+d) + 4a_1a_2) - 2b_1 - b_2, \\
\frac{1}{4}(\alpha^2-\alpha'^2) - (\beta-\beta') &= \frac{1}{4}(2a_1a_2 + a_2^2)\sqrt{d} - b_2\sqrt{d}. \quad \square
\end{aligned}$$

Clearly, by condition (2.22) and Proposition (2.25), we get bounds on the coefficients a_i and b_i. In order to compute the generating polynomial from the polynomial (2.16), we apply the following

(2.26) LEMMA. *If* $d \equiv 0 \bmod 4$, *let* $\sigma = 0$, $\pi = -d/4$, *and if* $d \equiv 1 \bmod 4$, *let* $\sigma = 1$, $\pi = (1-d)/4$. *Then* ρ *is a root of the irreducible quartic polynomial*

$$f(x) = x^4 - sx^3 + px^2 - qx + n \in \mathbb{Z}[x],$$

with

$$\begin{aligned}
s &= 2a_1 + a_2\sigma, \\
p &= a_1^2 + 2b_1 + (a_1a_2 + b_2)\sigma + a_2^2\pi, \\
q &= 2a_1b_1 + (a_1b_2 + a_2b_1)\sigma + 2a_2b_2\pi, \\
n &= b_1^2 + b_1b_2\sigma + b_2^2\pi.
\end{aligned}$$

Proof. In each case, we have $\sigma = \omega + \omega'$ and $\pi = \omega \cdot \omega'$. The values given for s, p, q, n follow immediately when we define

$$f(x) = (x^2 - \alpha x + \beta)(x^2 - \alpha' x + \beta'),$$

which is obviously satisfied by ρ. □

3. The Computation. Our search proceeds in three phases. In each phase, the programs are written in PASCAL whenever possible. When large integer values are unavoidable, we use the ALGEB language. This occurs in two situations: when the discriminant of a polynomial must be computed exactly; and when testing whether two fields are isomorphic.

MAXINT $= 2^{31} - 1 = 2,147,483,647$ is the maximum value of an integer variable in VAX PASCAL.

$\Delta_{\min}$ and $\Delta_{\max}$ are lower and upper bounds for the field discriminant.

D_f is the discriminant of the polynomial f.

(a) *Phase* I—*Generation of Totally Real Quartic Fields.*

3.1: PSRCH3 and QSRCH3 (PASCAL). We apply the method of Section 2 to generate example polynomials $f(x)$ with coefficients s, p, q, and n as in (2.1). Among the examples is at least one for each totally real quartic field F with $\Delta_F \leq \Delta_{\max}$.

PSRCH3 generates characteristic polynomials of "small" quartic irrationalities.

By Proposition (2.5), we may take $s \in \{0, 1, 2\}$. For each value of s, Proposition (2.8), with $\Delta_F = \Delta_{\max}$, gives bounds for p. Given s and p, Proposition (2.10) and Lemma (2.7) give bounds for q. Finally, given s, p, and q, Propositions (2.11) and (2.12) produce bounds for n.

QSRCH3 generates quadratic extension fields of quadratic fields.

By condition (2.14), the quadratic subfield discriminant d is bounded by $\sqrt[3]{(\Delta_F/2)}$. We therefore consider every square-free m with $2 \leq m \leq \sqrt[3]{(\Delta_{\max}/2)}$. If $m \equiv 1 \bmod 4$ we take $d = m$; otherwise we take $d = 4m$. Applying condition (2.22), we choose $a_1 \in \{0, 1\}$ and $a_2 \in \{0, 1, 2, 3\}$. For each choice of a_1, a_2, and d, Proposition (2.25) gives bounds for b_1 and b_2. Then s, p, q, and n are computed according to Lemma (2.26).

As shown in [3, p. 184], F is totally real precisely if the following three conditions are met:

(i) $3s^2 - 8p > 0$,

(ii) $16(p^2 - s^2 p + sq - 4n) + 3s^4 > 0$,

(iii) $D_f > 0$.

Polynomials satisfying the conditions above are tested for irreducibility over $\mathbf{Q}$. Each divisor of n is tested as a root of f, and if f has no rational roots, it is determined whether f is the product of two quadratics.

The polynomials surviving this test are normalized to satisfy

(1) $|n| = 1 \Rightarrow |s| \leq |q|$,

(2) $s \in \{0, 1, 2\}$,

(3) $s = 0 \Rightarrow q \geq 0$,

and are then sorted to remove duplicates.

3.2: PQMULT (ALGEB). We compute D_f exactly, and exclude f if $D_f \leq \Delta_{\max}$.

A partial factorization $D_f = d_1 d_2 d_3$, with each of d_1, d_2, d_3 not exceeding MAXINT, is then performed. (This enables the subsequent PASCAL program to factorize D_f completely.)

If this factorization reveals that the square-free part of D_f has a prime factor exceeding MAXINT (as occasionally happens), then f is excluded.

3.3: PQFACT (PASCAL). The complete factorization of D_f is performed.

If the square-free part of D_f exceeds $\Delta_{\max}$, then f is rejected.

3.4: PQDISC (PASCAL). For each polynomial f surviving the previous test, we compute the field discriminant Δ_F. The method used is the "Round 2" Maximal Order algorithm of Zassenhaus [13], [14], as implemented by Ford [4], suitably modified to avoid large integer values.

Polynomials for which $\Delta_F \le \Delta_{\min}$ or $\Delta_F > \Delta_{\max}$ are eliminated.

The remaining polynomials are then sorted in order of Δ_F, so that fields with equal discriminants appear consecutively.

(b) *Phase* II—*Elimination of Redundant Fields.*

3.5: IFTEST (ALGEB). Polynomials with equal field discriminants are tested to see if the fields generated by their roots are isomorphic.

The method used is given in Buchmann and Ford [1], with one deviation. In place of the complete LLL algorithm [7], we use the following procedure. Although it is weaker than LLL, we found it produces short vectors about four times as fast. No doubt, this is largely due to the inefficiency of representing the rational values in LLL entirely with integers.

Our lattice has basis $\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3, \mathbf{v}_4, \mathbf{v}_5$ over $\mathbf{Z}^5$.

The following steps are performed alternately until neither produces a change in the lattice basis:

```
1) Repeat 10 times:
     For $1 \le i, j \le 5$, with $i \ne j$:
       $k \leftarrow$ nearest integer to $(\mathbf{v}_i, \mathbf{v}_j)/(\mathbf{v}_j, \mathbf{v}_j)$;
       Replace: $\mathbf{v}_i \leftarrow \mathbf{v}_i - k\mathbf{v}_j$.
2) For $1 \le h \le 5$:
     Solve the $4 \times 4$ system of equations determined by:
       $\left(\mathbf{v}_h - \sum_{j \ne h} x_j \mathbf{v}_j\right) \perp \mathbf{v}_i$, for $i \ne h$;
     For $j \ne h$:
       $r_j \leftarrow$ nearest integer to $x_j$;
     Replace:
       $\mathbf{w} \leftarrow \sum_{j \ne h} r_j \mathbf{v}_j$;
       $k \leftarrow$ nearest integer to $(\mathbf{v}_n, \mathbf{w})/(\mathbf{w}, \mathbf{w})$;
       $\mathbf{v}_h \leftarrow \mathbf{v}_h - k\mathbf{w}$.
```

While either step 1) or step 2) alone produces short vectors eventually, neither of them is particularly efficient. But it seems that when step 2) reaches a period of slow convergence, application of step 1) speeds it up again. The constant 10 in step 1) was determined experimentally.

Remark. In every case where two fields were in fact isomorphic, it sufficed to perform our calculations modulo the smallest p-power exceeding 10^{20} to discover the determining relation.

(c) *Phase* III—*Computation of Galois Groups and Integral Bases.* At this point, a unique polynomial has been determined for each field F with $\Delta_F \leq 1,000,000$.

3.6: IBINDX (ALGEB). For each polynomial, the $\mathbb{Z}$-module index of the polynomial order in the maximal order, given by $\sqrt{(D_f/\Delta_F)}$, is computed.

3.7: IBTEXT (PASCAL). For each field, a basis for its ring of integers is computed, as described above under PQDISC.

The Galois group G of the field F is computed, according to the following method (due to Soicher [11], derived in part from Stauduhar [12]):

1) For $f(x) = x^4 - sx^3 + px^2 - qx + n$, its cubic resolvent is given by:
$h(y) = y^3 - py^2 + (sq - 4n)y + (-s^2n + 4pn - q^2)$.

2) If D_f is a square, then:
$G = V_4$ if h has a rational root;
$G = A_4$ otherwise.

3) If D_f is not a square, then:
$G = D_8$ or C_4 if h has a rational root;
$G = S_4$ otherwise.

4) If $G = D_8$ or C_4, then:
For integer root r of h, form polynomials
$g_1 = x^2 - rx + n$
$g_2 = x^2 - sx + (p - r)$.
Pick $g = g_1$ or g_2 so that D_g is not a square.
$G = C_4$ if $\mathbb{Q}(\sqrt{D_g}) = \mathbb{Q}(\sqrt{D_f})$
$G = D_8$ otherwise.

3.8: NCTEST (ALGEB). For each pair of polynomials f and g defining fields with equal discriminant, a prime p and a root r are determined such that p divides neither D_f nor D_g, f has root r modulo p, but g has no root modulo p (thereby proving that the fields defined by f and g are nonisomorphic; see [5]).

4. Results. All computations were done on a Digital Equipment VAX 8500 computer at the Computer Centre of Concordia University.

Because the Phase I software would otherwise produce large numbers of examples for fields with small discriminant, Phases I and II were run in seven parts, with distinct values of $\Delta_{\min}$ and $\Delta_{\max}$, as shown. "Count" gives the number of examples produced by each part of each phase.

		Phase I		Phase II	
$\Delta_{\min}$	$\Delta_{\max}$	time	count	time	count
0	15625	0 : 06	460	0 : 53	91
15625	31250	0 : 13	502	1 : 01	125
31250	62500	0 : 30	1081	2 : 09	284
62500	125000	1 : 17	2476	5 : 09	663
125000	250000	3 : 20	5557	11 : 09	1509
250000	500000	9 : 05	12011	24 : 32	3290
500000	1000000	27 : 08	26115	54 : 09	7111
	Totals	41 : 39	48202	99 : 02	13073

Among the 13,073 distinct fields there occur 12,089 different discriminants, with multiplicities as shown. For multiplicities 1, 2, and 3, the ten smallest field discriminants are given.

Multiplicity:	1	2	3	4	5	6	7
Frequency:	11250	709	119	9	1	0	1
Discriminants:	725	16448	35537	426725	270400		705600
	1125	28224	57600	462400			
	1600	30056	128357	473616			
	1957	37485	151717	608400			
	2000	42048	176400	658944			
	2048	44688	183872	833600			
	2225	48704	210649	878400			
	2304	50688	229577	967824			
	2525	55872	277429	998400			
	2624	62525	284445				

The data produced in Phase III of the computation—polynomial coefficients, Galois groups, and integral bases for each of the 13,073 distinct fields—is available from the authors on magnetic tape or IMB PC-compatible $5\frac{1}{4}$-inch floppy disks.

Relative Distribution of Galois Groups

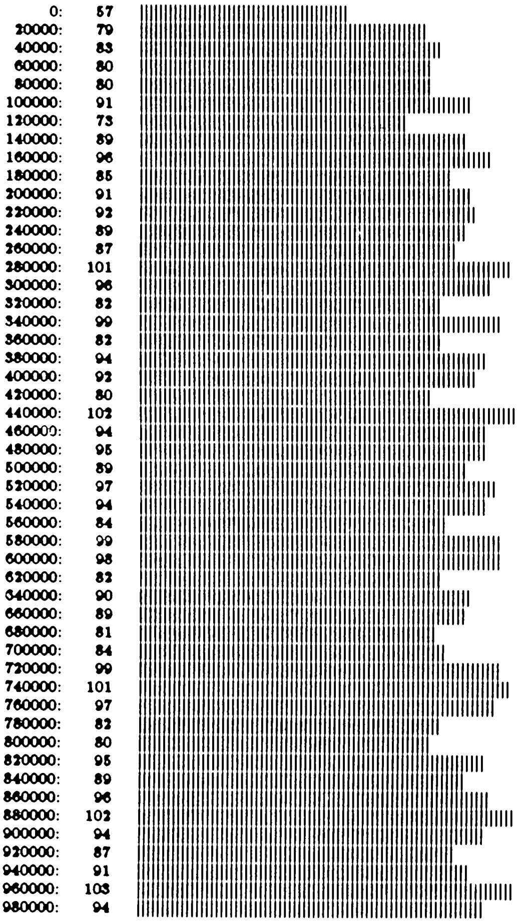
Group:	C_4	V_4	D_8	A_4	S_4
Fields:	59	196	4486	31	8301
Percent:	0.45	1.50	34.31	0.24	63.50

Distribution of Galois Groups by Field Discriminant

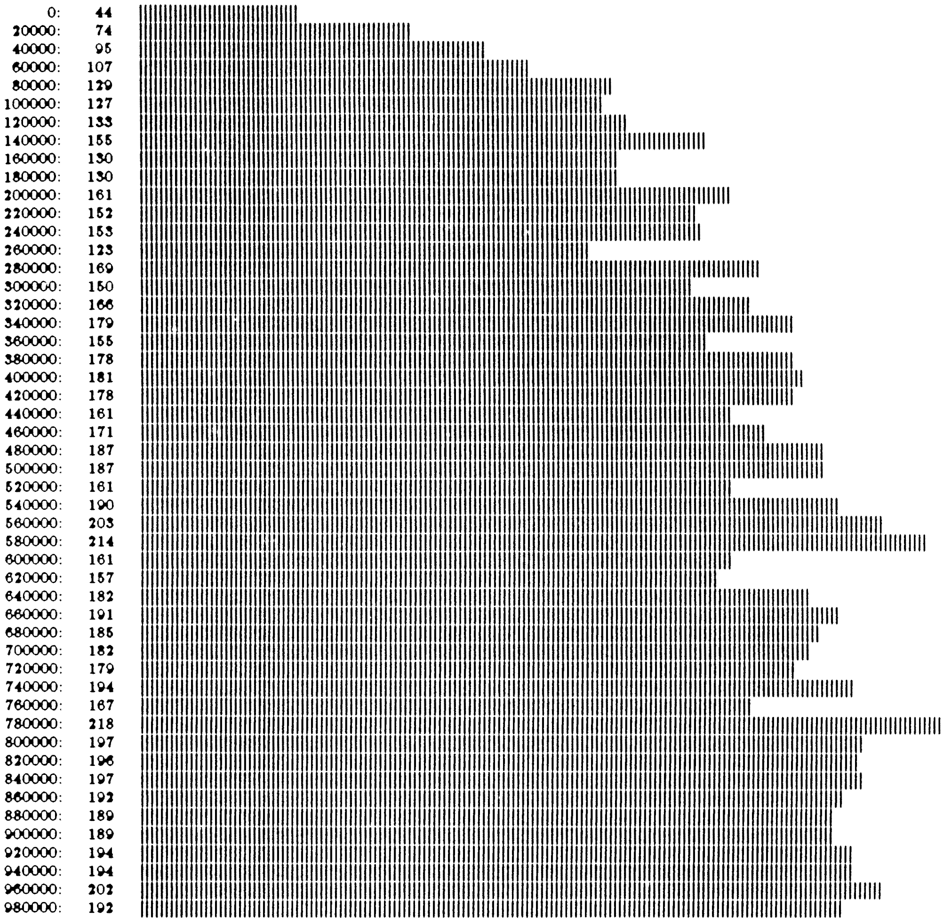
```
               C4                V4                           A4

      0:   11  |||||||||||   24  ||||||||||||||||||||||||  2  ||
  50000:    4  ||||          18  ||||||||||||||||||        2  ||
 100000:    5  |||||         13  |||||||||||||             1  |
 150000:    1  |             10  ||||||||||                2  ||
 200000:    3  |||           12  ||||||||||||              1  |
 250000:    6  ||||||        11  |||||||||||               3  |||
 300000:    4  ||||          10  ||||||||||                1  |
 350000:    3  |||            9  |||||||||                 2  ||
 400000:    1  |              8  ||||||||                  2  ||
 450000:    3  |||           10  ||||||||||                3  |||
 500000:    0                 5  |||||                     4  ||||
 550000:    3  |||            7  |||||||                   1  |
 600000:    1  |             10  ||||||||||                0
 650000:    0                 6  ||||||                    1  |
 700000:    3  |||           11  |||||||||||               1  |
 750000:    2  ||             8  ||||||||                  0
 800000:    2  ||             8  ||||||||                  1  |
 850000:    3  |||            6  ||||||                    2  ||
 900000:    3  |||            5  |||||                     1  |
 950000:    1  |              5  |||||                     1  |
```

Distribution of Galois Group D_8 by Field Discriminant



Distribution of Galois Group S_4 by Field Discriminant



Mathematisches Institut
Universität Düsseldorf
4000 Düsseldorf, West Germany
E-mail: buchmann@ dd0rud81.bitnet

Department of Computer Science
Concordia University
Montréal, Québec H3G 1M8, Canada
E-mail: ford@ conu1.bitnet

1. J. BUCHMANN & D. FORD, "Determining isomorphism of algebraic number fields." (Unpublished manuscript.)

2. J. W. S. CASSELS, *An Introduction to the Geometry of Numbers*, Springer-Verlag, Heidelberg, 1971.

3. B. N. DELONE & D. K. FADDEEV, *The Theory of Irrationalities of the Third Degree*, Transl. Math. Monographs, vol. 10, Amer. Math. Soc., Providence, R.I., 1964.

4. D. FORD, *On the Computation of the Maximal Order in a Dedekind Domain*, Ph.D. Dissertation, Ohio State University, 1978.

→ IRVING GERST & JOHN BRILLHART, "On the prime divisors of a polynomial," *Amer. Math. Monthly*, v. 78, 1971, pp. 250–266.

6. H. J. GODWIN, "Real quartic fields with small discriminant," *J. London Math. Soc.*, v. 31, 1956, pp. 478–485.

→ A. K. LENSTRA, H. W. LENSTRA, JR. & L. LOVASZ, "Factoring polynomials with rational coefficients," *Math. Ann.*, v. 261, 1982, pp. 515–534.

8. J. MARTINET, "Méthodes géométriques dans la recherche des petits discriminants," *Sém. de Théorie des Nombres*, Paris 1983–84, Birkhäuser, Basel, 1985, pp. 147–179.

9. M. POHST, "Berechnung kleiner Diskriminanten total reeler algebraischer Zahlkörper," *J. Reine Angew. Math.*, v. 278/279, 1975, pp. 278–300.

10. M. POHST, "On the computation of number fields of small discriminants including the minimum discriminant of sixth degree fields," *J. Number Theory*, v. 14, 1982, pp. 99–117.

11. LEONARD SOICHER, private communication, 1987.

12. R. P. STAUDUHAR, "The determination of Galois groups," *Math. Comp.*, v. 27, 1973, pp. 981–996.

13. H. ZASSENHAUS, "Ein Algorithmus zur Berechnung einer Minimalbasis über gegebener Ordnung," in *Funktionalanalysis*, Birkhäuser, Basel, 1967, pp. 90–103.

14. H. ZASSENHAUS, "On the second round of the maximal order program," in *Applications of Number Theory to Numerical Analysis*, Academic Press, New York, 1972, pp. 398–431.