J. Austral. Math. Soc. (*Series A*) **51** (1991), 473–482

QUARTIC NORMAL EXTENSIONS OF THE RATIONAL FIELD

TANG JIAN-ER

(Received 8 January 1990; revised 7 May 1990)

Communicated by J. H. Loxton

Abstract

There are two types of quartic normal extensions of the rational field, depending on the Galois group of the generating equation. All such extensions are described here in a uniquely parametrized form.

1991 *Mathematics subject classification* (*Amer. Math. Soc.*) 11 R 16.

It is well known that every quadratic extension of the rational field Q is normal. This is no longer true for quadratic extensions of a quadratic field, for example $Q(\sqrt[4]{2})$ is not normal over $\mathbb{Q}(\sqrt{2})$. Quadratic extensions are easy to describe: as D runs through all squarefree integers not equal to 1, $\mathbb{Q}(\sqrt{D})$ runs through all quadratic (normal) fields. In the following we shall describe all normal quartic fields.

In a sense the normal quartic extensions of $\mathbb{Q}$ are well known. Indeed the only transitive permutation groups of order 4 are the cyclic group

$$G_1 = \{I, (1234), (13)(24), (1432)\}$$

and the Klein group

$$G_2 = \{I, (12)(34), (13)(24), (14)(23)\}$$

and so adjunction of a root of a quartic equation to $\mathbb{Q}$ generates a normal extension only if the Galois group of the equation over $\mathbb{Q}$ is either G_1 or G_2. From here it follows easily that a quartic normal extensions is either of the form $\mathbb{Q}(\sqrt{a+b\sqrt{D}})$ where a, b are non-zero integers and D is a squarefree greater than 1, or of the form $\mathbb{Q}(\sqrt{A}, \sqrt{B})$ where A, B are distinct squarefree integers not equal to 1. Our purpose here is to find appropriate restrictions on these integers so as to obtain a unique description of the extensions.

THEOREM. *Quartic normal extensions* K *of the rational field* $\mathbb{Q}$ *are one of the following two types.*

1. *Let* D *be a squarefree integer greater than* 1 *with no prime factor of the form* $p \equiv -1 \pmod 4$; r, s, *an integer solution of* $r^2 + s^2 = D$ *with* $s > 0$; *and* k *an odd squarefree integer such that* $(k, D) = 1$. *Set* $\alpha = D + s\sqrt{D}$. *Then* $K = \mathbb{Q}(\sqrt{k\alpha})$.
2. *Let* A, B *be squarefree integers not equal to* 1 *with* $A < B$,

$$\max(|A|, |B|) < |AB|/(A, B)^2.$$

Then $K = \mathbb{Q}(\sqrt{A}, \sqrt{B})$.

The parameters D, s, k in the first case and A, B in the second case uniquely specify the extensions.

We need four lemmas.

LEMMA 1. *Given the quartic equation*

$$x^4 + ax^3 + bx^2 + cx + d = 0 \tag{1}$$

over $\mathbb{Q}$, *there exists a transformation* $y = u + vx + wx^2$, u, v, $w \in \mathbb{Q}$, *which transforms* (1) *into*

$$y^4 + py^2 + q = 0 \tag{2}$$

if and only if the Galois group of (1) *over* $\mathbb{Q}$ *is a subgroup of the dihedral group*

$$G = \{I, (13), (24), (12)(34), (13)(24), (14)(23), (1234), (1432)\}$$

where I *is the identity permutation.*

PROOF. Essentially this lemma is due to van der Ploeg [2], but not quite in such an explicit form and we give an independent proof. If there exist as transformation $y = u + vx + wx^2$ with rational coefficients, u, v, w such that (1) can be changed into (2) then (1) is soluble by extraction of square roots alone, hence its group is a subgroup of G. Conversely suppose that the Galois group of (1) is a subgroup of G. Let the four roots of (1) be x_1, x_2, x_3, x_4, then $\psi = x_1x_3 + x_2x_4$ is invariant under G and so $\psi \in \mathbb{Q}$. Hence ψ is a rational root of the Ferrari resolvent

$$z^3 - bz^2 + (ac - 4d)z - a^2d + 4bd - c^2 = 0.$$

Let σ_1, σ_2, σ_3 denote the elementary symmetric polynomials of the roots of (1); then

$$(x_1 - x_2 + x_3 - x_4)^2 = \sigma_1^2 - 4\sigma_2 + 4\psi,$$
$$(x_1 - x_2 + x_3 - x_4)(x_1^2 - x_2^2 + x_3^2 - x_4^2) = \sigma_1^3 - 4\sigma_1\sigma_2 + 4\sigma_3 + 2\sigma_1\psi.$$

Set $y_i = u + vx_i + wx_i^2$, $i = 1, 2, 3, 4$. Then the quartic equation with roots y_1, y_2, y_3, y_4 has the form (2) provided that $y_1 + y_2 + y_3 + y_4 = 0$ and $y_1 - y_2 + y_3 - y_4 = 0$, that is

$$4u + v\sigma_1 + w(\sigma_1^2 - 2\sigma_2) = 0, \; v(x_1 - x_2 + x_3 - x_4) + w(x_1^2 - x_2^2 + x_3^2 - x_4^2) = 0.$$

Multiplying the second equation by $x_1 - x_2 + x_3 - x_4$, we get

$$v(\sigma_1^2 - 4\sigma_2 + 4\psi) + w(\sigma_1^3 - 4\sigma_1\sigma_2 + 4\sigma_3 + 2\sigma_1\psi) = 0,$$

giving the rational solution

$$u = \frac{1}{2}a^2b + ac - 2b^2 + \left(-\frac{1}{2}a^2 + 2b\right)\psi, \; v = a^3 - 4ab + 4c + 2a\psi,$$
$$w = a^2 - 4b + 4\psi.$$

It follows that (1) can be changed into (2) by the transformation $y = u + vx + wx^2$.

LEMMA 2. *All integer solutions of*

$$x^2 + y^2 = z^4 \tag{4}$$

are obtained by one of the following:

1. $x = k^2(u^4 - 6u^2v^2 + v^4)$, $y = 4k^2uv(u^2 - v^2)$, $z = k(u^2 + v^2)$ *where* $(u, v) = 1$, $u + v \equiv 1 \pmod 2$, k *any integer*;

2. $x = D(m^2 - n^2)$, $y = 2Dmn$, $z = Dl$, *where* $D > 1$ *is squarefree with no prime factor* $\equiv -1 \pmod 4$ *and* m, n, l *are integers satisfying* $m^2 + n^2 = Dl^2$.

This is essentially due to Euler, see [1, p. 621]. It can be obtained directly from the parametric solution of Pythagorean triples. Solutions of $m^2 + n^2 = Dl^2$ of course always exist.

LEMMA 3. *Let* $D > 1$ *be squarefree with no prime factors of the form* $p \equiv -1 \pmod 4$, $d | D$, $d > 0$ *with* $d \equiv D \pmod 2$; r, s, t *an integer solution of* $r^2 + s^2 = Dt^2$ *with* $(r, s) = 1$. *Then the equation* $x^2 + y^2 = D$ *has an integer solution* x, y *such that* $(rx + sy, sx - ry) = d$.

PROOF. Since $(r, s) = 1$, t cannot be even or have a prime factor $p \equiv -1 \pmod 4$. Let $r + is = (a + ib)(e + if)(u + iv)^2$ be a factorization in the

https://doi.org/10.1017/S1446788700034637 Published online by Cambridge University Press

Gaussian domain such that $a^2+b^2=d$, $u^2+v^2=t$, $(u,v)=1$. This factorisation can clearly be accomplished so that no (odd) prime factor p of (D,t) divides $(e+if)(u+iv)$. Set $x+iy=(a+ib)(e-if)$, then $x^2+y^2=D$ and

$$\begin{aligned}(r+is)(x-iy) &= rx+sy+i(sx-ry)\\ &= (a^2+b^2)(e+if)^2(u+iv)^2 = d(e+if)^2(u+iv)^2.\end{aligned}$$

Since $(e+if)(u+iv)$ has no rational integer divisor, $(rx+sy, sx-ry)=d$.

LEMMA 4. *Let D_1, D_2 be squarefree integers greater than 1 with no prime factors $p\equiv -1 \pmod 4$; r_i, s_i, $t_i (i=1,2)$ integers satisfying $r_i^2+s_i^2=D_it_i^2$, $(s_i,t_i)=1$; and k_1, k_2 squarefree integers. Set*

$$\theta_i = \sqrt{k_i\left(t_iD_i+s_i\sqrt{D_i}\right)},$$

$i=1,2$. Then $\mathbb{Q}(\theta_1)=\mathbb{Q}(\theta_2)$ if and only if $D_1=D_2$ and

$$(5)\qquad \frac{k_2(t_1t_2D+r_1r_2+\eta s_1s_2)}{2k_1D},\ \frac{k_2(t_1t_2D-r_1r_2-\eta s_1s_2)}{2k_1D}$$

are rational squares for $\eta=+1$ or -1, where $D=D_1=D_2$.

PROOF. Note that if either of the expressions (5) is a rational square then so is the other, since

$$\begin{aligned}(t_1t_2D+r_1r_2+\eta s_1s_2)(t_1t_2D-r_1r_2-\eta s_1s_2) &= t_1^2t_2^2D^2-(r_1r_2+\eta s_1s_2)^2\\ &= (r_1s_2-\eta r_2s_1)^2.\end{aligned}$$

Suppose that $D_1\neq D_2$, then $\sqrt{D_1}\in\mathbb{Q}(\theta_1)$ but $\sqrt{D_1}\notin\mathbb{Q}(\theta_2)$. Therefore if $\mathbb{Q}(\theta_1)=\mathbb{Q}(\theta_2)$ we must have $D_1=D_2=D$ and there exists u, v, w, $x\in\mathbb{Q}$ such that $\theta_2^{(j)}=u+v\theta_1^{(j)}+w\theta_1^{(j)2}+x\theta_1^{(j)3}$, $j=0,1,2,3$ where θ_i', θ_i'', θ_i''' are the conjugates of θ_i, $i=1,2$. Since $\theta_i''=-\theta_i$, $\theta_i'''=-\theta_i'$, we have $u=0$, $w=0$ hence

$$\theta_2=v\theta_1+x\theta_1^3,\ \theta_2'=v\theta_1'+x\theta_1'^3,\ \theta_2''=-v\theta_1-x\theta_1^3,\ \theta_2'''=-v\theta_1'-x\theta_1'^3.$$

Consequently $\sigma_2=-v^2(\theta_1^2+\theta_1'^2)-2vx(\theta_1^4+\theta_1'^4)-x^2(\theta_1^6+\theta_1'^6)$,

$$\sigma_4=\theta_1^2\theta_1'^2(v^2+vx(\theta_1^2+\theta_1'^2)+x^2\theta_1^2\theta_1'^2)^2$$

where σ_2, σ_4 are the elementary symmetric polynomials of the $\theta_2^{(j)}$. Hence v and x satisfy

$$(6)\qquad t_1v^2+2k_1(2t_1^2D-r_1^2)vx+k_1^2(4t_1^3D^2-3t_1r_1^2D)x^2=\frac{k_2t_2}{k_1}$$

and

$$v^2 + 2k_1 t_1 D v x + k_1^2 r_1^2 D x^2 = \xi \frac{k_2 r_2}{k_1 r_1}, \ \xi = +1 \text{ or } -1. \tag{7}$$

Multiplying (6) by $\sqrt{D}$, (7) by r_1 and adding we obtain

$$(t_1\sqrt{D} + r_1)(v + k_1(2t_1 D - r_1\sqrt{D})x)^2 = \frac{k_2}{k_1}(t_2\sqrt{D} + \xi r_2)$$

hence

$$v + k_1(2t_1 D - r_1\sqrt{D})x = \pm\frac{1}{s_1}\sqrt{\frac{k_2}{k_1}(t_2\sqrt{D} + \xi r_2)(t_1\sqrt{D} - r_1)} \tag{8}$$

for some sign on the right hand side.

Similarly subtracting r_1 times (7) from $\sqrt{D}$ times (6) we obtain

$$v + k_1(2t_1 D + r_1\sqrt{D})x = \pm\frac{1}{s_1}\sqrt{\frac{k_2}{k_1}(t_2\sqrt{D} - \xi r_2)(t_1\sqrt{D} + r_1)}$$

for some sign on the right. Eliminating v we have

$$2k_1 r_1 s_1 \sqrt{D} x = \pm\sqrt{\frac{k_2}{k_1}(t_2\sqrt{D} - \xi r_2)(t_1\sqrt{D} + r_1)} \pm\sqrt{\frac{k_2}{k_1}(t_2\sqrt{D} + \xi r_2)(t_1\sqrt{D} - r_1)}$$

for one of the four possible choices of sign on the right. Squaring gives

$$(k_1 r_1 s_1 x)^2 = \frac{k_2}{2k_1 D}(t_1 t_2 D - \xi r_1 r_2 - \xi\eta s_1 s_2).$$

Conversely suppose that for some $\eta = \pm 1$ it is true that $(k_2/2k_1 D) \times (t_1 t_2 D - \xi r_1 r_2 - \xi\eta s_1 s_2)$ is a rational square for both $\xi = +1$ and $\xi = -1$. Then

$$x = \frac{1}{k_1 r_1 s_1}\sqrt{\frac{k_2}{2k_1 D}(t_1 t_2 D - \xi r_1 r_2 - \xi\eta s_1 s_2)}$$

defines a rational number for $\xi = \pm 1$. Define v by (8) with some sign on the right. Then v and x satisfy (6) and (7) as seen by reversing all calculations. But then v is rational. For multiplying (7) by t_1 and subtracting from (6) we obtain

$$vx = \frac{k_2}{2k_1^2 r_1 s_1^2}(t_2 r_1 - \xi r_2 t_1) - 2k_1 t_1 D x^2$$

and rationality of v follows. Hence $\theta_2 = v\theta_1 + x\theta_1^3 \in \mathbb{Q}(\theta_1)$ and is easily seen to be of the form $\theta_2 = \sqrt{k_2(t_2 D + s_2\sqrt{D})}$.

https://doi.org/10.1017/S1446788700034637 Published online by Cambridge University Press

We are now ready to prove our theorem. We first show that the extensions described in the theorem are indeed normal. In the case of the first type extension let $r^2+s^2=D$, $r>0$, $s>0$, $D>1$ squarefree with no prime factors $\pm-1 \pmod 4$. Let k be squarefree and set $\theta=\sqrt{k\alpha}$, $\alpha=D+s\sqrt{D}$. Its conjugates are

$$\theta'=\sqrt{k(D-s\sqrt{D})}=r(\theta^2-kD)/s\theta,\ \theta''=-\theta,\ \theta'''=-\theta',$$

therefore $\mathbb{Q}(\theta,\theta',\theta'',\theta''')=\mathbb{Q}(\theta)$ is normal. In the case of the second type extension let A, B be squarefree, not equal to 1, $\theta=\sqrt{A}+\sqrt{B}$. Clearly, $\mathbb{Q}(\sqrt{A},\sqrt{B})=\mathbb{Q}(\theta)$ is a quartic extension and the conjugates are

$$\theta'=\sqrt{A}-\sqrt{B}=(A-B)/\theta,\ \theta''=-\theta,\ \theta'''=-\theta'.$$

Therefore $\mathbb{Q}(\theta,\theta',\theta'',\theta''')=\mathbb{Q}(\theta)$ is normal.

Now adjunction of a root of (1) to $\mathbb{Q}$ can generate a quartic normal extension only if the Galois group of the equation is either

$$G_1=\{I,(1234),(13)(24),(1432)\}$$

or

$$G_2=\{I,(12)(34),(13)(24),(14)(23)\},$$

over $\mathbb{Q}$. By Lemma 1 there exists a transformation $y=u+vx+wx^2$ over $\mathbb{Q}$ such that (1) is changed into (2). Therefore we may assume that our quartic normal field is generated by a root of an equation of the form (2). We may also assume that the coefficients p, q in (2) are integers, otherwise multiply y by a suitable integer to get rid of the denominator.

Suppose the group of (2) is G_1. We first show that the extension K is of the following type:

1* Let D be as in type 1, r, s, t an integer solution of $r^2+s^2=Dt^2$ with $s>0$, $t>0$, $(s,t)=1$; and k a squarefree integer. Then $K=\mathbb{Q}(\theta)$ where $\theta=\sqrt{k(tD+s\sqrt{D})}$. Let τ_1, τ_2, τ_3, τ_4 be the elementary symmetric polynomials of the roots y_1, y_2, y_3, y_4 of (2), then $\tau_1=0$, $\tau_2=p$, $\tau_3=0$, $\tau_4=q$, therefore

$$(y_1+y_2-y_3-y_4)(y_1-y_2+y_3-y_4)(y_1-y_2-y_3+y_4)=\tau_1^3-4\tau_1\tau_2+8\tau_3=0.$$

The roots can be arranged so that $y_1-y_2+y_3-y_4=0$ say, and since $\tau_1=0$, we get

$$y_3=-y_1,\ y_4=-y_2,\ y_1^2+y_2^2=-\tau_2=-p,\ y_1^2y_2^2=\tau_4=q.$$

Consider $\psi=(1/16)(y_1+iy_2-y_3-iy_4)^4$ over $\mathbb{Q}(i)$. It belongs to G_1 and so its value is

$$\begin{aligned}\psi=(y_1+iy_2)^4&=(y_1^2+y_2^2)^2-8y_1^2y_2^2\pm 4i\sqrt{y_1^2y_2^2[(y_1^2+y_2^2)^2-4y_1^2y_2^2]}\\&=p^2-8q\pm 4i\sqrt{q(p^2-4q)}\in\mathbb{Q}(i).\end{aligned}$$

But p and q are integral, so there exists an integer T such that $q(p^2-4q) = T^2$, hence $(p^2-8q)^2+(4T)^2 = p^4$. By Lemma 2, one of the following two conditions holds.

1. There exist integers u, v with $(u, v) = 1$, $u+v \equiv 1 \pmod 2$, and an integer $k \neq 0$ such that $p = k(u^2+v^2)$ and

$$p^2-8q = k^2(u^4-6u^2v^2+v^4) \text{ or } 4k^2uv(u^2-v^2).$$

2. There exists a squarefree integer $D > 1$ with no prime factor $\equiv -1 \pmod 4$, and integers m, n, l satisfying $m^2+n^2 = Dl^2$, such that $p = Dl$ and $p^2-8q = D(m^2-n^2)$ or $2Dmn$. In Case 1 we have $q = k^2u^2v^2$ or $(1/8)k^2(u^2-2uv-v^2)^2$. If (2) is

$$y^4+k(u^2+v^2)y^2+k^2u^2v^2 = 0 \quad \text{then } (y^2+ku^2)(y^2+kv^2) = 0,$$

and the equation is reducible and does not generate a quartic field. So (2) is

$$y^4+k(u^2+v^2)y^2+\frac{1}{8}k^2(u^2-2uv-v^2)^2 = 0,$$

its roots are

$$y = (\pm 1/2)\sqrt{-k[2(u^2+v^2) \pm \sqrt{2}(u^2+2uv-v^2)]}$$

with independent $\pm$ signs. By definition u^2+v^2 and $u^2+2uv-v^2$ are coprime,

$$(u^2+2uv-v^2)^2+(u^2-2uv-v^2)^2 = 2(u^2+v^2)^2,$$

and so $\mathbb{Q}(y)$ is an extension of type 1^* with $D = 2$, $t = u^2+v^2$, $s = |u^2+2uv-v^2|$.

In Case 2 we have

$$q = (1/4)Dn^2 \text{ or } (1/8)D(m-n)^2.$$

If (2) is $y^4+Dly^2+(1/4)Dn^2 = 0$, its roots are

$$y = (\pm 1/2)\left(\sqrt{-lD+n\sqrt{D}} \pm \sqrt{-lD-n\sqrt{D}}\right)$$

with $m^2+n^2 = Dl^2$, hence $\mathbb{Q}(y)$ is an extension of type 1^* with $t = |l|/(l, n)$, $s = |n|/(l, n)$, $r = m/(l, n)$, $k = (-l/|l|)(l, n)$. If (2) is $y^4+Dly^2+(1/8)D(m-n)^2 = 0$ and D is odd then

$$y = (\pm 1/2)\sqrt{-l(2D) \pm (m+n)\sqrt{2D}}.$$

By the equality $(m+n)^2+(m-n)^2 = 2Dl^2$, $\mathbb{Q}(y)$ is an extension of type 1^* with $t = |l|/(l, m+n)$, $s = |m+n|/(l, m+n)$, $k = (-l/|l|)(l, m+n)$.

Similarly if D is even, since $(m \pm n)^2 \mp 2mm = Dl^2$, $m+n$ and $m-n$ must be even,

$$y = \pm\sqrt{-l(D/2) \pm ((m+n)/2)\sqrt{D/2}}$$

and by the equality $((m+n)/2)^2 + ((m-n)/2)^2 = (D/2)l^2$, $\mathbb{Q}(y)$ is again an extension of type 1^* with $t = |l|/(l, (m+n)/2)$, $s = |m+n|/2(l, (m+n)/2)$, $k = (-l/|l|)(l, (m+n)/2)$. It follows that if the group of (2) is G_1 then adjunction of its roots to $\mathbb{Q}$ generates an extension of type 1^*.

Next we show that any extension of type 1^* is of type 1. So suppose $r^2 + s^2 = Dt^2$, $(s, t) = 1$, k squarefree, $\theta = \sqrt{k(tD + s\sqrt{D})}$. If here $2|k$, set $\beta = tD + r\sqrt{D}$, $\overline{\beta} = tD - r\sqrt{D}$, then $\theta = \sqrt{k\beta/2} + \sqrt{k\overline{\beta}/2}$ with $(t, r) = 1$ (since $(t, s) = 1$) and clearly $\mathbb{Q}(\theta) = \mathbb{Q}(\sqrt{k\beta/2})$. So we may assume $2 \nmid k$. Let $(k, D) = d$, $k = k_1 d$, then $(k_1, D) = 1$ and $2 \nmid k_1$, $2 \nmid d$ hence $D/d + D \equiv 0 (\mathrm{mod}\, 2)$. By Lemma 3, the equation $x^2 + y^2 = D$ has an integer solution x, y such that $(rx + sy, sx - ry) = D/d$. Now

$$(rx+sy)^2 + (sx-ry)^2 = (r^2+s^2)(x^2+y^2) = (tD)^2$$

hence there exist integers u, v with $(u, v) = 1$, $u + v \equiv 1 (\mathrm{mod}\, 2)$ such that $rx + sy = (D/d)(u^2 - v^2)$ or $(D/d)(2uv)$, $tD = (D/d)(u^2 + v^2)$. If $rx + sy = (D/d)(u^2 - v^2)$, set $\eta = \sqrt{k_1(D + y\sqrt{D})}$ and apply Lemma 4 with

$$\theta_1 = \eta(r_1 = x, s_1 = y, t_1 = 1)$$

and

$$\theta_2 = \theta(r_2 = r, s_2 = s, t_2 = t, k_2 = k).$$

The expressions (5) in Lemma 4 and u^2, v^2 respectively hence by the Lemma, $\mathbb{Q}(\eta) = \mathbb{Q}(\theta)$. Similarly if $rx + sy = (D/d)(2uv)$ then $sx - ry = (D/d)(u^2 - v^2)$ and setting $\eta = \sqrt{k_1(D + x\sqrt{D})}$ we can apply Lemma 4 with $\theta_1 = \eta$ $(r_1 = y, s_1 = x, t_1 = 1)$, $\theta_2 = \theta$. The expressions in (5) are now v^2, u^2 respectively, and we again conclude that $\mathbb{Q}(\eta) = \mathbb{Q}(\theta)$. In either case the extension is of type 1. (Since $\mathbb{Q}(\sqrt{k\alpha}) = \mathbb{Q}(\sqrt{k\overline{\alpha}})$, $\overline{\alpha} = D - s\sqrt{D}$, we may assume at any rate $s > 0$).

To show uniqueness of the parameters s, k, suppose that

$$\eta_1 = \sqrt{k_1(D + s_1\sqrt{D})},$$

$$\eta_2 = \sqrt{k_2(D + s_2\sqrt{D})}, \ \mathbb{Q}(\eta_1) = \mathbb{Q}(\eta_2).$$

By Lemma 4 (and changing the sign of s_1 if necessary)

$$(k_2/2k_1D)(D + r_1r_2 + s_1s_2)$$

https://doi.org/10.1017/S1446788700034637 Published online by Cambridge University Press

is a square. Now $r_1^2+s_1^2=D$, $r_2^2+s_2^2=D$, hence

$$(r_1r_2+s_1s_2)^2+(r_1s_2-r_2s_1)^2=D^2.$$

Set $(r_1r_2+s_1s_2, D)=d$, then there exist integers u, v satisfying $(u, v)=1$, $u+v\equiv 1(\bmod 2)$ such that $r_1r_2+s_1s_2=d(u^2-v^2)$ or $d(2uv)$, $D=d(u^2+v^2)$. Suppose $r_1r_2+s_1s_2=d(u^2-v^2)$, then

$$k_2(D+r_1r_2+s_2s_2)/2k_1D=k_2u^2/k_1(u^2+v^2)$$

hence $k_1k_2(u^2+v^2)$ is a square. But $(k_1, D)=1$, $(k_2, D)=1$ and k_1, k_2, D are squarefree therefore $k_1=k_2$ and $u^2+v^2=1$, $d=D$. But then $r_1r_2+s_1s_2=D$, $r_1s_2-s_1r_2=0$ which together with $r_1^2+s_1^2=D$, $r_2^2+s_2^2=D$ give $r_1=r_2$, $s_1=s_2$.

If $r_1r_2+s_1s_2=d(2uv)$ then

$$\frac{k_2}{2k_1D}(D+r_1r_2+s_1s_2)=\frac{(u+v)^2k_2}{2k_1(u^2+v^2)},\ 2k_1k_2(u^2+v^2) \text{ is a square.}$$

As before, it implies $k_1=k_2$, $u^2+v^2=2$, $D=2d$, $r_1r_2+s_1s_2=2d=D$, $r_1s_2-s_1r_2=0$ hence $r_1=r_2$, $s_1=s_2$.

Finally suppose that the group of (2) is G_2. Then all three quantities $\psi_1=y_1y_2+y_3y_4$, $\psi_2=y_1y_3+y_2y_4$, $\psi_3=y_1y_4+y_2y_3$ belong to G_2 and are roots of the Ferrari resolvent of (2),

$$z^3-pz^2-4qz+4pq=0. \tag{9}$$

Hence (9) has three rational roots. But (9) is $(z-p)(z^2-4q)=0$ and so q is a square f^2. Since G_2 is transitive, the roots

$$y=\pm\frac{1}{2}(\sqrt{-p+2f}\pm\sqrt{-p-2f})$$

of (2) are quartic algebraic numbers. Let

$$-p+2f=m^2M,\ -p-2f=n^2N$$

where M, N are squarefree. Then the field is generated by any two of the squareroots of M, N, $MN/(M, N)^2$. Exactly one of these three numbers has a largest absolute value. Denoting by A, B the other two we may assume $A<B$, $\max(|A|, |B|)<|AB|/(A, B)^2$ and we obtain $\mathbb{Q}(y)=\mathbb{Q}(\sqrt{A}, \sqrt{B})$, an extension of type 2. Uniqueness of the parameters A, B is obvious.

Acknowledgement

The author wishes to thank Professor G. Szekeres for his help in rewriting this paper.

References

[1] L. E. Dickson, *History of the theory of numbers, Vol.* 2 (Chelsea, New York, 1952)
[2] C. E. van der Ploeg, 'Duality in non-normal quartic fields', *Amer. Math. Monthly* **94** (1987), 279–284.

Department of Information
The Shanghai University of Finance and Economics
Shanghai
China

https://doi.org/10.1017/S1446788700034637 Published online by Cambridge University Press