Can. J. Math., Vol. XLII, No. 3, 1990, pp. 491–507

BICYCLIC BICUBIC FIELDS

CHARLES J. PARRY

1. Introduction. There is an extensive body of literature on the bicyclic biquadratic fields. These fields provide the simplest examples of abelian noncyclic extensions of Q. In sharp contrast, there is a dearth of literature on the bicyclic bicubic extensions of the rational numbers. These fields together with the abelian noncyclic octic extensions provide the next simplest abelian noncyclic extensions.

In this article, we shall study abelian bicyclic bicubic extensions of Q of degree 9. Hasse [**4**, v–ix] has stated as important objectives: the computation of an integral basis, the determination of class number and the calculation of fundamental units for abelian fields. In this article, we will solve the first problem completely, and show that the solution to the unit problem leads to a solution of the class number problem. Moreover, we shall give a method for determining the unit group up to a subgroup which has index 1 or 3 and so determine the class number up to a factor of 3.

2. Notation and terminology. The following notation will be used throughout this article.

Q: Rational number field.
$\zeta = e^{2\pi i/3}$: Primitive cube root of unity.
$k = Q(\zeta)$: Third cyclotomic field.
K: Bicyclic bicubic extension of Q of degree 9.
K_i $(i = 1, 2, 3, 4)$: Cyclic cubic subfields of K.
f: Conductor of K.
f_i $(i = 1, 2, 3, 4)$: Conductor of the field K_i.
$L_i = K_i(\zeta)$.
$L = K(\zeta)$.
$N_{E/F}$: Norm function for the extension E/F.
$S_{E/F}$: Trace function for the extension E/F.
D_F: Discriminant of the field F over Q.
h: Class number of K.
h_i: Class number of K_i $(i = 1, 2, 3, 4)$.
U: Unit group of K.
U_i: Unit group of K_i $(i = 1, 2, 3, 4)$.
$V = U_1U_2U_3U_4$: Product of subgroups in U.
$\bar{\alpha}$: Complex conjugate of a complex number α.

Received November 28, 1988.
AMS (1980) subject classification: 12A50.

An integer $(x + y\sqrt{-3})/2$ of k is said to be *normalized* if either $x \equiv 2, y \equiv 0 \pmod 3$ or $x = 3x_0, y = 3y_0$ with $x_0 \equiv 2, y_0 \not\equiv 0 \pmod 3$. A normalized integer is said to be *strongly normalized* if $y > 0$.

LEMMA 1. *If α is an integer of k relatively prime to 3 then α has exactly one normalized associate. If $(\alpha, 9) = 3$, then α has exactly two normalized associates.*

Proof. Since there are exactly six units in k, the lemma follows by an examination of cases.

COROLLARY. *If α is an integer of k, which is not a rational integer, with $(\alpha, 9) = 1$ (respectively 3), then α has exactly one (respectively two) associate(s) β such that either β or $\bar{\beta}$ (but not both) is strongly normalized.*

Proof. If β is normalized and not a rational integer, then exactly one of β or $\bar{\beta}$ is strongly normalized.

3. Integral basis. It follows from Gras [**1**], Hasse [**2**] or Maki [**5**] that the field K_i $(i = 1, 2, 3, 4)$ generated by the roots of a polynomial

$$q_i(x) = x^3 - (f_i/3)x - f_i a_i/27$$

where $4f_i = a_i^2 + 27b_i^2$ and $\alpha_i = (a_i + 3b_i\sqrt{-3})/2$ is strongly normalized. It will be shown that α_3 and α_4 can be determined from α_1 and α_2.

LEMMA 2. *Let $d = (f_1, f_2), \delta = (\alpha_1, \bar{\alpha}_2)$ and $\gamma = 1/3(\alpha_1, \alpha_2)$ or $\gamma = (\alpha_1, \alpha_2)$ according as 3 divides both of α_1 and α_2 or not. Then $N_{k/Q}(\delta\gamma) = d$ and there exist integers β_1 and β_2 of k such that $\alpha_1 = \gamma\delta\beta_1$ and $\alpha_2 = \gamma\bar{\delta}\beta_2$. Moreover, either $\gamma\beta_1\beta_2 = \rho$ or 3ρ where ρ is a square free integer of k relatively prime to 3 and divisible by no rational integer.*

Proof. First note that $N_{k/Q}(\alpha_i) = f_i$ is square free except for a possible factor of 9 and α_i is an integer of k. Since the integers of k form a UFD, we can write

$$\alpha_1 = \pi_0^{e_1}\pi_1\pi_2\ldots\pi_r\pi_{r+1}\ldots\pi_s\pi_{s+1}\ldots\pi_t\epsilon_1$$

$$\alpha_2 = \pi_0^{e_2}\pi_1\pi_2\ldots\pi_r\bar{\pi}_{r+1}\ldots\bar{\pi}_s\pi'_{s+1}\ldots\pi'_u\epsilon_2$$

where $\pi_0 = (-3 + 3\sqrt{-3})/2$ and $\pi_1, \ldots, \pi_t, \pi'_{s+1}, \ldots, \pi'_u$ are distinct, nonconjugate, normalized primes of k which do not divide 3, ϵ_1, ϵ_2 are units of k, and e_1, $e_2 \in \{0, 1\}$. Since the product of normalized integers, not divisible by 3, is again normalized and since α_1 is normalized, we see $\epsilon_1 = 1$ when $e_1 = 0$. Similarly, $\epsilon_2 = 1$ when $e_2 = 0$. If $e_1 = 1$, then by dividing both sides of the expression for α_1 by 3 and examining congruences modulo 3, we see $\epsilon_1 = 1$ or $(-1+\sqrt{-3})/2$ according as $b_1 \equiv 1$ or $2 \pmod 3$. Similarly, when $e_2 = 1, \epsilon_2 = 1$ or $(-1 + \sqrt{-3})/2$ according as $b_2 \equiv 1$ or $2 \pmod 3$. Let $m = \min\{e_1, e_2\}$ and note

$$\delta = \pi_0^m\pi_{r+1}\ldots\pi_s$$

$$\gamma = \pi_1\ldots\pi_r.$$

Setting

$$\beta_1 = \pi_0^{e_1-m}\pi_{s+1}\dots\pi_t\epsilon_1 \quad \text{and} \quad \beta_2 = \pi_0^{e_2-m}\pi'_{s+1}\dots\pi'_u\epsilon_2\epsilon^m$$

where $\epsilon = (-1-\sqrt{-3})/2$, the result follows.

PROPOSITION 3. *Let $f_i = df_i'$ for $i = 1,2$ and $N_{k/Q}(\delta) = c$, $N_{k/Q}(\gamma) = g$. Then $f_3 = gf_1'f_2'$ and $f_4 = cf_1'f_2'$. Moreover $\alpha_3 = \pm\bar{\gamma}\beta_1\beta_2$ or $\alpha_3 = \pm\gamma\bar{\beta}_1\bar{\beta}_2$ and $\alpha_4 = \pm\bar{\delta}\beta_1\bar{\beta}_2$ or $\alpha_4 = \pm\delta\bar{\beta}_1\beta_2$.*

Proof. By the cubic formula, $K_i = Q(\theta_i)$ for $i = 1,2$ where

$$\theta_i = 1/3(\sqrt[3]{f_i\alpha_i} + \sqrt[3]{f_i\bar{\alpha}_i}).$$

Also

$$\theta_i' = 1/3(\zeta\sqrt[3]{f_i\alpha_i} + \zeta^2\sqrt[3]{f_i\bar{\alpha}_i}) \quad \text{and} \quad \theta_i'' = 1/3(\zeta^2\sqrt[3]{f_i\alpha_i} + \zeta\sqrt[3]{f_i\bar{\alpha}_i})$$

are the conjugates of θ_i and are also contained in K_i. Now

$$L_i = k(\sqrt[3]{f_i\alpha_i}) = k(\sqrt[3]{f_i\bar{\alpha}_i})$$

and since there are exactly 4 cubic intermediate fields between k and L, we may number L_3 and L_4 so that

$$L_3 = k(\sqrt[3]{f_1\alpha_1f_2\alpha_2}) \quad \text{and} \quad L_4 = k(\sqrt[3]{f_1\alpha_1f_2\bar{\alpha}_2}).$$

Now

$$\begin{aligned} f_1\alpha_1f_2\alpha_2 &= df_1'\gamma\delta\beta_1df_2'\gamma\bar{\delta}\beta_2 \\ &= d^2f_1'f_2'\delta\bar{\delta}\gamma^2\beta_1\beta_2 \\ &= (cg)^2cf_1'f_2'\gamma^2\beta_1\beta_2 \\ &= c^3g(\gamma\bar{\gamma})f_1'f_2'\gamma^2\beta_1\beta_2 \\ &= (c\gamma)^3gf_1'f_2'\bar{\gamma}\beta_1\beta_2 \end{aligned}$$

so

$$L_3 = K(\sqrt[3]{gf_1'f_2'\bar{\gamma}\beta_1\beta_2}) = K(\sqrt[3]{f_3\alpha_3}).$$

Since $gf_1'f_2'\bar{\gamma}\beta_1\beta_2$ and $f_3\alpha_3$ are both cube free integers of k, it follows that $f_3 = gf_1'f_2'$ and $\alpha_3 = \pm\bar{\gamma}\beta_1\beta_2$ or $\alpha_3 = \pm\gamma\bar{\beta}_1\bar{\beta}_2$. Similarly, $f_4 = cf_1'f_2'$ and $\alpha_4 = \pm\bar{\delta}\beta_1\bar{\beta}_2$ or $\alpha_4 = \pm\delta\bar{\beta}_1\beta_2$.

COROLLARY 1. *For any prime p, either p divides none or exactly 3 of the conductors f_1, f_2, f_3, f_4.*

https://doi.org/10.4153/CJM-1990-025-8 Published online by Cambridge University Press

COROLLARY 2. *We may choose* f_1 *with* $(f_1, 3) = 1$. *If this is done then*

$$\alpha_3 = \bar{\gamma}\beta_1\beta_2 \quad or \quad \alpha_3 = \gamma\bar{\beta}_1\bar{\beta}_2 \quad and \quad \alpha_4 = \bar{\delta}\beta_1\bar{\beta}_2 \quad or \quad \alpha_4 = \delta\bar{\beta}_1\beta_2.$$

Proof. The first statement is immediate form Corollary 1. Under the hypothesis $(f_1, 3) = 1$, $e_1 = 0$ in the proof of Lemma 2. Hence $\epsilon_1 = 1$ and so β_1 will be normalized. Also $m = 0$ so that δ is normalized. If $e_2 = 0$ then all of γ, $\bar{\gamma}$, β_1, $\bar{\beta}_1$, β_2, $\bar{\beta}_2$ and α_3 are normalized so the sign in the equation $\alpha_3 = \pm\bar{\gamma}\beta_1\beta_2$ or $\alpha_3 = \pm\gamma\bar{\beta}_1\bar{\beta}_2$ must be positive. If $e_2 = 1$ and $\alpha_3 = \pm\bar{\gamma}\beta_1\beta_2$ then divide both sides of the equation by 3 and take congruences modulo 3. Since $\bar{\gamma}$, β_1 and $(\beta_2/\pi_0\epsilon_2)$ are normalized this reduces to

$$2 + b_3\sqrt{-3} \equiv \pm(-1 + \sqrt{-3})\epsilon_2 \pmod 3.$$

Recall $\epsilon_2 = 1$ or $(-1 + \sqrt{-3})/2$, but in either case the sign must be positive. Similarly, the sign must be positive if $\alpha_3 = \pm\gamma\bar{\beta}_1\bar{\beta}_2$. Likewise the sign in the equation for α_4 must be positive.

THEOREM 4. *The discriminant* D_K *is given by*

$$D_K = \begin{cases} (9p_1p_2\dots p_n)^6 & \text{if } 3|f_2 \\ (p_1p_2\dots p_n)^6 & \text{if } 3\nmid f_2 \end{cases}$$

where $p_1, p_2, \dots, p_n$ *are the distinct prime divisors of* f_1f_2 *other than* 3. *Moreover,*

$$f = \begin{cases} 9p_1p_2\dots p_n & \text{if } 3|f_2 \\ p_1p_2\dots p_n & \text{if } 3\nmid f_2. \end{cases}$$

Proof. A prime p ramifies in K if and only if $p|f_1$ or $p|f_2$. Moreover, in K $(p) = (P_1P_2P_3)^3$ with $N_{K/Q}(P_i) = p$ or $(p) = P_1^3$ with $N_{K/Q}(P_1) = p^3$ where each P_i is a prime ideal of K. If $p \neq 3$, Dedekind's formula shows that the different $\Delta_{K/Q}$ is exactly divisible by $(P_1P_2P_3)^2$ or by P_1^2 depending on the factorization of p. In either case p^6 is the exact power of p dividing the discriminant D_K. If $3 \nmid f_2$ then $3 \nmid D_K$ and we are done. If $3|f_2$ then $(3) = P^3$ in K_2 where P is a prime ideal of norm 3. Since P^4 exactly divides the different $\Delta_{K_2/Q}$ and $(\Delta_{K/K_2}, 3) = 1$, it follows that P^4 exactly divides $\Delta_{K/Q}$. Hence 3^{12} exactly divides the discriminant D_K.

The conductor f of K is clearly the least common multiple of the conductors f_i of the fields $K_i (i = 1, 2, 3, 4)$. Thus f has the stated value.

COROLLARY. $D_K = D_{K_1}D_{K_2}D_{K_3}D_{K_4}$.

If $3|f_1$ *let* $p_i(x) = q_i(x)$ *and otherwise set*

$$p_i(x) = x^3 - x^2 + \frac{1 - f_i}{3}x - \frac{f_i(a_i - 3) + 1}{27} \quad \text{for } i = 1, 2, 3, 4.$$

https://doi.org/10.4153/CJM-1990-025-8 Published online by Cambridge University Press

*Let θ_i be a root of $p_i(x)$ then Maki [**5**] shows that $1, \theta_i, \theta_i'$ form an integral basis for K_i/Q where θ_i' is a conjugate of θ_i.*

LEMMA 5. *The basis $1, \theta_1, \theta_1', \theta_2, \theta_2', \theta_3, \theta_3', \theta_4, \theta_4'$ for K/Q has discriminant $3^6 D_{K_1} D_{K_2} D_{K_3} D_{K_4}$.*

Proof. A straight forward, but tedious calculation using the standard representation of the discriminant as a determinant, gives the result.

THEOREM 6. *An integral basis for K/Q consists of $1, \theta_1, \theta_1', \theta_2, \theta_2', \theta_5, \theta_6, \theta_7, \theta_8$ where*

$$\theta_5 = 1/3[-\epsilon + \epsilon\theta_1 + \theta_2 + \theta_3 + \theta_4]$$

$$\theta_6 = 1/3[-\epsilon + \epsilon\theta_1' + \theta_2 + \theta_3' + \theta_4']$$

$$\theta_7 = 1/3[\epsilon\theta_1 + \theta_2' + \theta_3' - \theta_4 - \theta_4']$$

$$\theta_8 = 1/3[\epsilon\theta_1' + \theta_2' - \theta_3 - \theta_3' + \theta_4]$$

and $\epsilon \equiv f_2 (\mathrm{mod}\, 3)$ is 0 or 1.

Proof. First we need to show that θ_5, θ_6, θ_7 and θ_8 are integers. Since $3 \nmid f_1$ it follows from Cardan's formula, (see [**6**, p. 179])

$$\theta_1 = 1/3[1 + \sqrt[3]{f_1\alpha_1} + \sqrt[3]{f_1\bar{\alpha}_1}]$$

and for $i = 2, 3, 4$

$$\theta_i = 1/3[\epsilon + \sqrt[3]{f_i\alpha_i} + \sqrt[3]{f_i\bar{\alpha}_i}].$$

Here we choose conjugates so that

$$\theta_i' = 1/3[\epsilon' + \zeta\sqrt[3]{f_i\alpha_i} + \zeta^2\sqrt[3]{f_i\bar{\alpha}_i}]$$

where $\epsilon' = 1$ or ϵ according as $i = 1$ or $i > 1$.

Now by Corollary 2 to Proposition 3,

$$\begin{aligned}\theta_1\theta_2 &= 1/9[\epsilon(1 + \sqrt[3]{f_1\alpha_1} + \sqrt[3]{f_1\bar{\alpha}_1}) + \sqrt[3]{f_2\alpha_2} + \sqrt[3]{f_2\bar{\alpha}_2} \\ &\quad + \sqrt[3]{f_1f_2\alpha_1\alpha_2} + \sqrt[3]{f_1f_2\bar{\alpha}_1\bar{\alpha}_2} + \sqrt[3]{f_1f_2\alpha_1\bar{\alpha}_2} + \sqrt[3]{f_1f_2\bar{\alpha}_1\alpha_2}] \\ &= 1/3[-\epsilon/3 + \epsilon\theta_1 + \theta_2 \\ &\quad + c/3(\gamma\sqrt[3]{f_3\alpha_3} + \bar{\gamma}\sqrt[3]{f_3\bar{\alpha}_3}) + g/3(\delta\sqrt[3]{f_4\alpha_4} + \bar{\delta}\sqrt[3]{f_4\bar{\alpha}_4})],\end{aligned}$$

where we are assuming for the moment that $\alpha_3 = \bar{\gamma}\beta_1\beta_2$ and $\alpha_4 = \bar{\delta}\beta_1\bar{\beta}_2$. Since $(f_1, 3) = 1$, Lemma 2 shows that both γ and δ are relatively prime to 3 and are normalized. Thus

$$\gamma = 1/2(u + v\sqrt{-3}) \quad \text{and} \quad \delta = 1/2(r + s\sqrt{-3}) \quad \text{with } u, v, r, s \in Z$$
$$\text{and } u \equiv r \equiv 2 (\mathrm{mod}\, 3) \quad \text{and} \quad v \equiv s \equiv 0 (\mathrm{mod}\, 3).$$

Now

$$\theta_1\theta_2 = 1/3\Big[-\epsilon/3 + \epsilon\theta_1 + \theta_2 + \frac{cu}{6}(\sqrt[3]{f_3\alpha_3}$$
$$+ \sqrt[3]{f_3\bar{\alpha}_3}) + \frac{cv\sqrt{-3}}{6}(\sqrt[3]{f_3\alpha_3} - \sqrt[3]{f_3\bar{\alpha}_3}) + \left(\frac{gr}{6}\right)(\sqrt[3]{f_4\alpha_4} + \sqrt[3]{f_4\bar{\alpha}_4})$$
$$+ \frac{gs\sqrt{-3}}{6}(\sqrt[3]{f_4\alpha_4} - \sqrt[3]{f_4\bar{\alpha}_4})\Big]$$
$$= 1/3\Big[-\epsilon\left(1/3 + \frac{cv}{2} + \frac{gs}{2} + \frac{cu}{6} + \frac{gr}{6}\right) + \epsilon\theta_1 + \theta_2 + \frac{cu\theta_3}{2}$$
$$+ \frac{cv}{2}(\theta_3 + 2\theta_3') + \frac{gr}{2}\theta_4 + \frac{gs}{2}(\theta_4 + 2\theta_4')\Big]$$
$$= 1/3\Big[-\epsilon\left(\frac{cv}{2} + \frac{gs}{2} + 1/3\left(1 + \frac{cu}{2} + \frac{gr}{2}\right)\right) + \epsilon\theta_1 + \theta_2$$
$$+ \frac{c(u+v)}{2}\theta_3 + cv\theta_3' + \frac{g(r+s)}{2}\theta_4 + gs\theta_4'\Big].$$

By an analysis of cases $cu + gr \equiv -2ru(r+u) \equiv 4 \pmod 9$, so that

$$0 \equiv 3\theta_1\theta_2 \equiv -\epsilon + \epsilon\theta_1 + \theta_2 + \theta_3 + \theta_4 \pmod 3.$$

Hence

$$\theta_5 = 1/3(-\epsilon + \epsilon\theta_1 + \theta_2 + \theta_3 + \theta_4)$$

is an integer of K. If $\alpha_3 = \bar{\gamma}\beta_1\beta_2$ and/or $\alpha_4 = \delta\bar{\beta}_1\beta_2$ then the signs are changed on the cv and/or gs terms respectively. Since these terms vanish modulo 3, the same proofs holds. Since θ_6, θ_7 and θ_8 are conjugates of θ_5, they are also integers of K.

By direct computation, the index of the basis 1, θ_1, θ_1', θ_2, θ_2', θ_5, θ_6, θ_7, and θ_8, relative to the basis of Lemma 5, is 3^{-3}. Therefore the new basis has discriminant equal to $D_{K/Q}$ and so is an integral basis for K/Q.

4. Class number considerations. The following class number relation is immediate from [**7**].

PROPOSITION 7. *$3^5h = Q^*\ h_1h_2h_3h_4$ where $Q^* = [U : U_1U_2U_3U_4] = [U : V]$.*

LEMMA 8. *$Q^* = 3^a$ with $0 \leqq a \leqq 5$.*

Proof. Let G denote the Galois group of K/Q and G_i denote the Galois groups of K/K_i for $i = 1, 2, 3, 4$.

For any subgroup H of G, let $\tilde{H}$ denote the sum of the elements of H in the integral group ring ZG. The direct norm relation

$$\tilde{G}_1 + \tilde{G}_2 + \tilde{G}_3 + \tilde{G}_4 = 3e + \tilde{G},$$

where e is the identity of G, shows that for any unit ϵ of K, $\epsilon^3 \in V$. Hence $Q^* = 3^a$ with $0 \leqq a \leqq 8$.

Suppose now $\epsilon \in U$ with $\epsilon \notin V$ and that $\epsilon^3 \in U_i$, for some $i = 1, 2, 3, 4$. Set $\epsilon^3 = \epsilon_0$ and note since $\epsilon \notin U_i$, $K = K_i(\epsilon) = K_i(\sqrt[3]{\epsilon_0})$. But K_i does not contain the third roots of unity so $K_i(\sqrt[3]{\epsilon_0})/K_i$ is a nonnormal extension, while K/K_i is a normal extension. Thus $\epsilon^3 \notin U_i$. Now choose bases B for U and B^* for V such that $B^* = (\epsilon_1, \epsilon_2, \ldots, \epsilon_8)$ where ϵ_{2i-1} and ϵ_{2i} form a basis for U_i with $i = 1, 2, 3, 4$. We may assume that all elements of B and B^* are positive. Let A denote the 8×8 matrix which expresses the cubes of the elements of B in terms of the elements of B^*. Then by changing only the basis B, we may assume that A is a triangular matrix. Now $Q^* \cdot \det A = 3^8$. Replacing ϵ_i with ϵ_i^{-1} if necessary, we may assume that the diagonal elements a_{ii} are all positive and so $a_{ii} = 1$ or 3. It follows from the remarks above that $a_{11} = a_{22} = 3$. Suppose that $a_{33} = 1$, then $e^3 = \epsilon\epsilon_3$ for some units e of K and ϵ of K_1. If σ is a generator of G_1 then

$$e^{3(1-\sigma)} = e_3^{(1-\sigma)}$$

again contradicting the above remarks. Hence $a_{33} = 3$, so 3^3 divides det A and the lemma follows.

The class number of a cyclic cubic field is relatively prime to 3 if, and only if, the conductor of the field has exactly one prime divisor. An analogous result is obtained for bicubic fields. When the conductor f of K has exactly two prime divisors, set $f = pq$ where $p \neq 3$ is prime and either $q \neq p$ is a prime of $q = 9$.

THEOREM 9. *The abelian bicubic field K has class number relatively prime to* 3 *if, and only if, $f = pq$ (as above) has exactly two prime divisors such that not both p and q are cubic residues of one another.*

Proof. By Hasse [**3**, p. 98] the number of ambiguous classes for K/K_i is given by

$$a_{K/K_i} = 3^{d+q^*-3} h_i$$

where d is the number of primes of K_i which ramify in K and $3^{q^*} = (N(\beta) : U_i^3)$ where $N(\beta)$ denotes the subgroup of the unit group U_i of K_i consisting of norms of elements of K. Note that q^* must be 0, 1 or 2. Now $(3, h) = 1$ if, and only if, $(3, a_{K/K_i}) = 1$ for some $i = 1, 2, 3, 4$. Assume that the conductor of K has exactly two prime divisors and let p, q be as above. We may choose K_1 and K_2 so that K_1 has conductor p and K_2 has conductor q. If q is not a cubic residue modulo p then q (or 3 when $q = 9$) stays prime in K_1 and so q (or 3) is the only prime divisor of K_1 which ramifies in K. Thus

$$d = 1 \quad \text{and} \quad a_{K/K_1} = 3^{q^*-2}h_1.$$

But $3 \nmid h_1$ and $q^* \leqq 2$, so $q^* = 2$. Hence $3 \nmid a_{K/K_1}$, so $(3, h) = 1$. A similar argument can be given when p is not a cubic residue modulo q.

Conversely, assume $(3, h) = 1$. If $9|h_i$ for some i, then class field theory shows that $3|h$. Thus for each $i = 1, 2, 3, 4$ the conductor of K_i has at most two prime divisors. Since any prime divisor of the conductor of K, divides the conductors of exactly 3 of the subfields K_i, it follows that the conductor of K can have at most two prime divisors, and so has exactly two prime divisors. Let p and q be as above, but suppose that both are cubic residues of one another. Then p splits into three distinct prime divisors in K_2 and q (or 3) splits into 3 distinct prime divisors in K_1. Thus $d = 3$ for each of the extensions K/K_1 and K/K_2, hence

$$a_{K/K_i} = 3^{q_i^*}h_i,$$

so $q_1^* = q_2^* = 0$. Now $9 \nmid h_i$, for any i, while h_1, h_2 are relatively prime to 3 and h_3, h_4 are divisible by 3, so Proposition 7 shows $Q^* = 3^3$. If A is the matrix described in the proof of Lemma 8, then $\det A = 3^5$. Hence the diagonal entry $a_{ii} = 1$ for some $i \leqq 6$. For such an i,

$$e_i^3 = \epsilon_1^{b_1}\epsilon_2^{b_2}\ldots\epsilon_{i-1}^{b_{i-1}}\epsilon_i$$

where e_i is a unit of K and $0 \leqq b_j \leqq 2$. In the proof of Lemma 8, it was shown that the right hand side of the equation must contain units from at least two fields K_j. Thus $b_k \not\equiv 0$ for some k with $1 \leqq k \leqq 4$. Now $\epsilon_k \in K_j$ for $j = 1$ or 2 and

$$N_{K/K_j}(e_i) = \epsilon_{2j-1}^{b_{2j-1}}\epsilon_{2j}^{b_{2j}},$$

but $k = 2j - 1$ or $2j$, and so $q_j^* \geqq 1$, contradicting $q_j^* = 0$. Thus not both p and q can be cubic residues of one another.

COROLLARY 1. *There are infinitely many fields K with class number not divisible by* 3 *and for each of these fields $Q^* = 27$.*

COROLLARY 2. *If p and q are distinct primes congruent to* 1 *modulo* 3 *or $q = 9$ and not both p and q are cubic residues of one another, then any cyclic cubic field K_i of conductor pq has class number $h_i \equiv 3 (\mathrm{mod}\, 9)$.*

Proof. Let K be the bicubic abelian field with conductor pq. It follows from Theorem 9 that $h_i \not\equiv 0 (\mathrm{mod}\, 9)$. Suppose $h_i = 3h'$, then h' is the order of the 3-complement of the ideal class group of K_i. Call this group H' and decompose it into orbits under the action of the Galois group $G(K_i/Q)$. Each orbit, except the identity, has length 3 so $h' \equiv 1 (\mathrm{mod}\, 3)$. Hence $h_i \equiv 3 (\mathrm{mod}\, 9)$.

COROLLARY 3. *If p and q are distinct primes congruent to* 1 *modulo* 3 *or* $q = 9$ *and both p and q are cubic residues of one another, then any cyclic cubic field K_i with conductor pq has class number* $h_i \equiv 0 \pmod 9$.

Proof. Let K be the bicubic abelian field with conductor pq. By Theorem 9, the class number h of K is divisible by 3. Hence 3 divides $a_{K/K_i} = 3^{d+q^*-3}h_i$, but $d = 0$ and $q^* \leqq 2$. Thus $9|h_i$.

5. The unit index. In this section we study the unit index $(U : V)$. According to Hasse [**2**] we may choose the fundamental units ϵ_{2i-1} and ϵ_{2i} of K_i to be conjugates. The following lemma provides a basis for the study of the unit index.

LEMMA 10. *For each* $i = 1, 2, 3, 4$, *there exists a cube free positive integer b_i and an integer B_i of K_i with*

$$\epsilon_{2i-1}\epsilon_{2i}^2 = b_i/B_i^3 \quad \textit{and} \quad N_{K_i/Q}(B_i) = b_i.$$

Moreover, $b_i \neq 1$, *b_i is uniquely determined and* $b_i|f_i^2$.

Proof. Let $G(K_i/Q) = (\sigma)$, where σ is chosen so that $\epsilon_{2i} = \epsilon_{2i-1}^{\sigma}$. By Hilbert's Theorem 90, there exists an integer B of K_i with $\epsilon_{2i-1} = B^{1-\sigma}$. Since B is unique up to rational multiples, we may assume it is divisible by no rational prime and that it has positive norm. Since $(B) = (B^{\sigma})$ as ideals of K_i, it follows that only ramified primes of K_i can divide B. Since no rational primes can divide B, the ramified primes can only divide B to the first or second power. Hence $b_i = N_{K_i/Q}(B)$ is a cube free positive divisor of f_i^2. Now $\epsilon_{2i} = \epsilon_{2i-1}^{\sigma} = B^{\sigma-\sigma^2}$ so that

$$\epsilon_{2i-1}\epsilon_{2i}^{-1} = B^{1-2\sigma+\sigma^2} = B^{1+\sigma+\sigma^2}/B^{3\sigma} = b_i/B^{3\sigma}.$$

Set $B_i = \epsilon_{2i}^{-1}B^{\sigma}$, then

$$\epsilon_{2i-1}\epsilon_{2i}^2 = b_i/(\epsilon_{2i}^{-1}B^{\sigma})^3 = b_i/B_i^3.$$

Suppose now that

$$\epsilon_{2i-1}\epsilon_{2i}^2 = a/A^3$$

where a is a positive cube free integer and A is an element of K_i. Then

$$(A/B_i)^3 = (a/b_i),$$

so a/b_i must be a rational cube. Since both a and b_i are positive cube free integers, $a/b_i = 1$ and so $a = b_i$.

Since ϵ_{2i-1} and ϵ_{2i} form a fundamental system of units of K_i, it follows that $b_i \neq 1$.

LEMMA 11. *The unit index* $(U : V)$ *is a divisor of* 3^3.

Proof. Lemma 8 shows that $(U : V)$ divides 3^5. If the index is 3^5 then by examining the matrix A described in the proof of Lemma 8, it is seen that the equation

$$e^3 = \epsilon_1^a \epsilon_2^b \epsilon_3^c \epsilon_4$$

has a solution e in K with $0 \leqq a, b, c \leqq 2$. The proof of Lemma 8 shows that not both a and b can be zero. However,

$$e^{3(1-\sigma_2)} = \epsilon_1^{a+b} \epsilon_2^{-a+2b}$$

and

$$e^{3(1-\sigma_1)} = \epsilon_3^{c+1} \epsilon_4^{-c+2} \quad \text{where } G(K/K_i) = (\sigma_i) \text{ for } i = 1, 2.$$

It follows that $a \equiv 2b$ and $c \equiv 2 (\bmod 3)$. Hence

$$e_1^3 = (\epsilon_1 \epsilon_2^2)^a (\epsilon_3^2 \epsilon_4)$$

has a solution e_1 in K with $a = 1$ or 2. Lemma 10 shows that $x^3 = b_1^a b_2^2$ has a solution x in K, so $b_1^a b_2^2$ must be a cube of a rational integer. Thus the prime divisors of b_1 and b_2 must be identical. Suppose p is any prime divisor of b_1, then $p | f_1$. Since p divides exactly three of the conductors f_1, f_2, f_3 and f_4, we may number the fields so that $p \dagger f_2$. Thus $p \dagger b_2$ and so the above equation has no solution. Hence $(U : V)$ divides 3^4.

Suppose now $(U : V) = 3^4$, then the matrix A of Lemma 8 shows that

$$e^3 = \epsilon_1^a \epsilon_2^b \epsilon_3^c \epsilon_4^d \epsilon_5$$

has a solution e in K with $0 \leqq a, b, c, d \leqq 2$. The proof of Lemma 8 shows that at least one of a or b and at least one of c or d is nonzero. Now

$$e^{3(1-\sigma_1)} = \epsilon_3^{c+d} \epsilon_4^{-c+2d} \epsilon_5 \epsilon_6^{-1}$$

and

$$e^{3(1-\sigma_2)} = \epsilon_1^{a+b} \epsilon_2^{-a+2b} \epsilon_5^2 \epsilon_6.$$

Since $\epsilon_5 \epsilon_6^{-1}$ and $\epsilon_5^2 \epsilon_6$ cannot be cubes in K,

$$a + b \not\equiv 0 \not\equiv c + d (\bmod 3).$$

The argument given above shows that b_1, b_3 and b_2, b_3 have identical sets of prime divisors, so b_1 and b_2 have the same prime divisors. This contradicts the way K_1 and K_2 were chosen above. Thus $(U : V)$ is a divisor of 27.

Let W denote the units e of K such that $e \in V$ or

$$(1) \qquad e^3 = \epsilon_1^{a_1}\epsilon_2^{2a_1}\epsilon_3^{a_2}\epsilon_4^{2a_2}\epsilon_5^{a_3}\epsilon_6^{2a_3}\epsilon_7^{a_4}\epsilon_8^{2a_4}$$

where a_1, a_2, a_3, a_4 are any integers.

LEMMA 12. *If $e \in U$ then $e^{1-\tau} \in W$ for any $\tau \in G(K/Q)$.*

Proof. Suppose $e = \epsilon_1^{a_1} \dots \epsilon_8^{a_8}$ then

$$e^{3(1-\tau)} = \epsilon_1^{a_1(1-\tau)} \dots \epsilon_8^{a_8(1-\tau)}.$$

For each $i = 1, 2, 3, 4$ the terms $(\epsilon_{2i-1}^{a_{2i-1}}\epsilon_{2i}^{a_{2i}})^{1-\tau}$ will be one of

$$1, \epsilon_{2i-1}^{a_{2i-1}+a_{2i}}\epsilon_{2i}^{-a_{2i-1}+2a_{2i}} \quad \text{or} \quad \epsilon_{2i-1}^{2a_{2i-1}-a_{2i}}\epsilon_{2i}^{a_{2i-1}+a_{2i}}.$$

Thus $e^{1-\tau} \in W$.

THEOREM 13. *W is a subgroup of U and $(W : V) = 3^{4-\tau}$ where r is the rank of the $n \times 4$ matrix $M = (m_{ij})$ over Z_3 where*

$$b_i = p_1^{m_{1i}} p_2^{m_{2i}} \dots p_n^{m_{ni}}$$

for $i = 1, 2, 3, 4$. Here $p_1, \dots, p_n$ denote the distinct prime divisors of the conductor f of K. Moreover, either

$$(U : V) = (W : V) = 1, 3 \text{ or } 9 \quad \text{or} \quad (U : V) = 3(W : V) = 27.$$

Proof. Clearly, W is a subgroup of U. It follows from Lemma 10 that (1) has a solution for a_1, a_2, a_3, a_4 if and only if $b_1^{a_1}b_2^{a_2}b_3^{a_3}b_4^{a_4}$ is the cube of a rational number. But this is equivalent to

$$m_{11}a_1 + m_{12}a_2 + m_{13}a_3 + m_{14}a_4 \equiv 0 (\operatorname{mod} 3)$$

$$\cdot \quad \cdot \quad \cdot$$

$$m_{n1}a_1 + m_{n2}a_2 + m_{n3}a_3 + m_{n4}a_4 \equiv 0 (\operatorname{mod} 3).$$

The number independent solutions is the dimension of the null space of M over Z_3. This is $4 - r$. Hence $(W : V) = 3^{4-r}$.

Let p_1 be a prime divisor of b_1, then p_1 divides f_1. Since any prime divides none or exactly 3 of f_1, f_2, f_3 and f_4, we may assume p_1 does not divide f_2. Let p_2 be a prime divisor of b_2. Then the upper left hand corner of M is the 2×2 matrix $\begin{bmatrix} m_{11} & 0 \\ m_{21} & m_{22} \end{bmatrix}$ where $m_{11}m_{22} \not\equiv 0 (\operatorname{mod} 3)$. Thus the rank of M is at least 2. Hence $(W : V) = 3^{4-r}$ divides 9.

Next it will be shown that $(U : V)$ divides $3(W : V)$. First assume that $(U : V) = 27$ then the matrix A of Lemma 8 shows that the equation

$$e^3 = \epsilon_1^{a_1}\epsilon_2^{a_2}\epsilon_3^{a_3}\epsilon_4^{a_4}\epsilon_5^{a_5}\epsilon_6 \tag{2}$$

has a solution e in K with $0 \leqq a_i \leqq 2$. Assume that $e \notin W$ and note that

$$e^{3(1-\sigma_1)} = \epsilon_3^{a_3+a_4}\epsilon_4^{-a_3+2a_4}\epsilon_5^{a_5+1}\epsilon_6^{-a_5+2}$$

and

$$e^{3(1-\sigma_2)} = \epsilon_1^{a_1+a_2}\epsilon_2^{-a_1+2a_2}\epsilon_5^{2a_5-1}\epsilon_6^{a_5+1}.$$

Since $e \notin W$, we may assume that $a_5 \not\equiv 2 (\bmod 3)$ so that $a_5+1 \not\equiv 0 (\bmod 3)$. Thus both $e^{1-\sigma_1}$ and $e^{1-\sigma_2}$ are in W and must be independent. Hence $(W : V) = 9$. Suppose now that $e \in W$, then 3 divides $(W : V)$. Since $(U : V) = 3^3$, the equation

$$e_1^3 = \epsilon_1^{c_1}\epsilon_2^{c_2}\epsilon_3^{c_3}\epsilon_4^{c_4}\epsilon_5^{c_5}\epsilon_6^{c_6}\epsilon_7 \tag{3}$$

has a solution in K for some c_i with $0 \leqq c_i \leqq 2$. Now

$$e_1^{3(1-\sigma_1)} = \epsilon_3^{c_3+c_4}\epsilon_4^{-c_3+2c_4}\epsilon_5^{c_5+c_6}\epsilon_6^{-c_6+2c_6}\epsilon_7\epsilon_8^{-1}.$$

Thus not both of $c_3 + c_4$ and $c_5 + c_6$ can be congruent to 0 modulo 3, so $e_1^{(1-\sigma_1)}$ is in W. Now e and $e_1^{(1-\sigma_1)}$ are independent elements of W so $(W : V) = 9$.

Assume now that $(U : V) = 9$ then either equation (2) or equation (3) has a solution in K and as above $(W : V)$ is divisible by 3.

Finally, we show $(U : V) = (W : V)$ when $(W : V) = 1$ or 3. First assume that $(W : V) = 1$. Suppose there exists an $e \in U$ with $e \notin W$. Then

$$e^3 = e_1^{a_1} \dots \epsilon_8^{a_8} \quad \text{with } a_{2i-1} \not\equiv 2a_{2i} (\bmod 3) \quad \text{for some } i = 1, 2, 3, \text{or } 4.$$

Let $j \neq i$ be 1, 2, 3 or 4 and let σ be a nonidentity element of $G(K/K_j)$ then the expression for $e^{3(1-\sigma)}$ involves either the terms

$$\epsilon_{2i-1}^{a_{2i-1}+a_{2i}}\epsilon_{2i}^{-a_{2i-1}+2a_{2i}} \quad \text{or} \quad \epsilon_{2i-1}^{2a_{2i-1}-a_{21}}\epsilon_{2i}^{a_{2i-1}+a_{2i}}.$$

Thus $e^{(1-\sigma)} \in W$, but not in V, contradicting the hypothesis that $(W : V) = 1$. Thus $U = W$ and so $(U : V) = 1$.

Now assume that $(W : V) = 3$. Then there is exactly one unit and its square (where exponents are reduced (mod 3)), of the form $e_0 = \epsilon_1^{c_1} \dots \epsilon_8^{c_8}$ where $c_i = 0, 1$ or 2 are not all zero and $c_{2i-1} \equiv 2c_{2i} (\bmod 3)$, such that e_0 is the cube of another unit of U. Suppose that $(U : W) > 1$. Then there exists $e \in U$ with $e \notin W$ and $e^3 = \epsilon_1^{a_1} \dots \epsilon_8^{a_8}$ where each $a_i = 0, 1$ or 2 and $a_{2j-1} \not\equiv 2a_{2j} (\bmod 3)$

for some $j = 1, 2, 3$ or 4. In the proof of Lemma 8, it was shown that $c_i \neq 0$ for units ϵ_i from at least two fields K_i. Choose $t \neq j$ such that $c_{2t} \not\equiv 0 (\bmod 3)$. Let σ be a generator of $G(K/K_t)$, then by Lemma 12, $e^{1-\sigma} \in W$. However, the expression for $e^{3(1-\sigma)}$ does not involve either ϵ_{2t-1} or ϵ_{2t}, so $e^{3(1-\sigma)} \neq e_0$ or e_0^2. This implies that $(W : V) > 3$, a contradiction. Thus $(U : W) = 1$ and $(U : V) = (W : V) = 3$.

COROLLARY. *If f has exactly two distinct prime divisors then $(W : V) = 9$ and if f has exactly three prime divisors then $(W : V) = 3$ or 9.*

Proof. If f has exactly two distinct prime divisors then M is a 2×4 matrix and so has rank at most 2. But it was shown in the proof of Theorem 13 that M always has rank at least 2, so $r = 2$ and $(W : V) = 9$. If f has exactly 3 prime divisors then M is a 3×4 matrix so has rank 2 or 3. Thus $(W : V) = 3$ or 9.

6. Computation of $(W : V)$. The value of $(W : V)$ can be determined if the values of b_1, b_2, b_3 and b_4 of Lemma 10 are known. In this section we give a method for computing these b_i's. To simplify notation we let $\epsilon = \epsilon_{2i-1}$ for $i = 1, 2, 3$, or 4 and $\epsilon' = \epsilon_{2i}$, ϵ'' denote the conjugates of ϵ. Using the notation of Lemma 10, $G(K_i/Q) = (\sigma)$ and $\epsilon' = \epsilon^{\sigma}$, $\sigma'' = \epsilon^{\sigma^2}$.

LEMMA 14. *Not both of $\beta = 1 + \epsilon + \epsilon\epsilon'$ and $\gamma = 1 + \epsilon + \epsilon\epsilon''$ can be zero. If $\beta \neq 0$ then $\epsilon = \beta^{1-\sigma}$ and if $\gamma \neq 0$ then $\epsilon = \gamma^{1-\sigma^2}$.*

Proof. Since $\beta - \gamma = \epsilon(\epsilon' - \epsilon'')$ and $\epsilon' \neq \epsilon''$, it follows that $\beta \neq \gamma$ and so at least one is nonzero. Note that

$$\epsilon\beta^{\sigma} = \epsilon(1 + \epsilon' + \epsilon'\epsilon'') = \epsilon + \epsilon\epsilon' + 1 = \beta$$

so $\epsilon = \beta^{1-\sigma}$ when $\beta \neq 0$, similarly, $\epsilon = \gamma^{1-\sigma^2}$ when $\gamma \neq 0$.

LEMMA 15. *Let $S(\epsilon) = s$ and $S(\epsilon^{-1}) = t$ where S denotes the trace of K_i/Q. Then $\beta\gamma'' = s + t + 3$. Hence one of β or γ is zero if, and only if, $s + t + 3 = 0$.*

Proof.

$$\begin{aligned}\beta\gamma'' &= (1 + \epsilon + \epsilon\epsilon')(1 + \epsilon'' + \epsilon'\epsilon'') \\ &= 3 + \epsilon + \epsilon' + \epsilon'' + \epsilon\epsilon' + \epsilon\epsilon'' + \epsilon'\epsilon'' \\ &= 3 + S(\epsilon) + S(\epsilon^{-1}) \\ &= 3 + s + t.\end{aligned}$$

LEMMA 16.

$$N(\beta) = 6 + 3S(\epsilon) + 3S(\epsilon^{-1}) + S(\epsilon\epsilon'^{-1}) \quad \textit{and}$$
$$N(\gamma) = 6 + 3S(\epsilon) + 3S(\epsilon^{-1}) + S(\epsilon^{-1}\epsilon')$$

where N denotes the norm of K_i/Q.

Proof. By direct computation

$$\begin{aligned} N(\beta) = \beta\beta'\beta'' &= (1+\epsilon+\epsilon\epsilon')(1+\epsilon'+\epsilon'\epsilon'')(1+\epsilon''+\epsilon\epsilon'') \\ &= 6+3(\epsilon+\epsilon'+\epsilon'')+3(\epsilon\epsilon'+\epsilon'\epsilon''+\epsilon\epsilon)+(\epsilon\epsilon'^2+\epsilon'\epsilon''^2+\epsilon^2\epsilon'') \\ &= 6+3S(\epsilon)+3S(\epsilon^{-1})+S(\epsilon\epsilon'^{-1}) \\ &= 6+3s+3t+S(\epsilon\epsilon'^{-1}) \end{aligned}$$

since $\epsilon\epsilon'^2 = \epsilon'\epsilon''^{-1}$ and $S(\epsilon'\epsilon''^{-1}) = S(\epsilon\epsilon'^{-1})$. A similar computation gives the expression for $N(\gamma)$.

LEMMA 17.

$$S(\epsilon\epsilon'^{-1})+S(\epsilon^{-1}\epsilon') = st-3 \quad \textit{and} \quad S(\epsilon\epsilon'^{-1})\cdot S(\epsilon^{-1}\epsilon') = 9+s^3+t^3-6st.$$

Proof. Since $s\cdot\epsilon^{-1} = 1+\epsilon^{-1}\epsilon'+\epsilon^{-1}\epsilon''$,

$$st = sS(\epsilon^{-1}) = S(s\epsilon^{-1}) = 3+S(\epsilon^{-1}\epsilon')+S(\epsilon\epsilon'^{-1}).$$

Also

$$\begin{aligned} S(\epsilon^{-1}\epsilon')\cdot S(\epsilon\epsilon'^{-1}) &= 3+S(\epsilon^3)+S(\epsilon^{-3}) \\ &= 3+sS(\epsilon^2)-tS(\epsilon)+3+tS(\epsilon^{-2})-sS(\epsilon^{-1})+3 \\ &= 9+s(s^2-2t)-st+t(t^2-2s)-st \\ &= 9+s^3+t^3-6st. \end{aligned}$$

LEMMA 18.

$$S(\epsilon^{-1}\epsilon') = (st-3-D)/2 \quad \textit{and} \quad S(\epsilon\epsilon'^{-1}) = (st-3+D)/2$$

where $D^2 = 18st-4s^3-4t^3+s^2t^2-27$. (The sign of D is not specified.)

Proof. Set $w = S(\epsilon^{-1}\epsilon')$ and $v = S(\epsilon\epsilon'^{-1})$. By Lemma 17,

$$w+v = st-3 \quad \text{and} \quad wv = 9+s^3+t^3-6st.$$

Hence w and v are roots of the quadratic equation $y^2+(3-st)y+9+s^3+t^3-6st$. The roots are

$$y = 1/2(st-3\pm D)$$

https://doi.org/10.4153/CJM-1990-025-8 Published online by Cambridge University Press

where

$$D^2 = (3 - st)^2 - 4(9 + s^3 + t^3 - 6st)$$
$$= 18st - 4s^3 - 4t^3 + s^2t^2 - 27.$$

Note that D is the discriminant of $f(x) = x^3 - sx^2 + tx - 1$, which has ϵ as a root. Thus D is a perfect square.

PROPOSITION 19.

$$N(\beta) = 6 + 3s + 3t + 1/2(st - 3 + D) \quad \textit{and}$$
$$N(\gamma) = 6 + 3s + 3t + 1/2(st - 3 - D)$$

for some choice of the sign of D. Moreover,

$$N(\beta)N(\gamma) = (s + t + 3)^3.$$

Proof. Lemmas 16 and 18 give the values of $N(\beta)$ and $N(\gamma)$. It follows from Lemma 15 that

$$N(\beta)N(\gamma) = N(\beta)N(\gamma'')$$
$$= N(\beta\gamma'') = N(s + t + 3) = (s + t + 3)^3.$$

PROPOSITION 20. *Let $b = b_i$ of Lemma 10. If $\beta \neq 0$ then b is the cube free positive kernel of $N(\beta)$. If $\gamma \neq 0$ then b is the cube free kernel of $N(\gamma^2)$.*

Proof. If $\beta \neq 0$ then $\beta^{1-\sigma} = \epsilon$ and so

$$\epsilon\epsilon'^2 = \frac{N(\beta)}{(\beta^{\sigma^2})^3} = b_0 \left(\frac{a}{\beta^{\sigma^2}}\right)^3$$

where b_0 is the positive cube free kernel of $N(\beta)$. The uniqueness of Lemma 10 shows that $b = b_0$.

If $\gamma \neq 0$ then $\gamma^{1-\sigma^2} = \epsilon$ and so

$$\epsilon\epsilon'^2 = \frac{(\gamma^\sigma)^3}{N(\gamma)} = N(\gamma^2)\left(\frac{\gamma^\sigma}{N(\gamma)}\right)^3.$$

The uniqueness of Lemma 10 shows that b is the cube free kernel of $N(\gamma^2)$.

7. Four examples. In the Corollary to Theorem 13, it was shown that $(W : V) = 9$ when f has exactly two prime divisors. From Theorem 13, one would generally expect $(W : V) = 3$ when f has 3 prime divisors and $(W : V) = 1$ when f has 4 or more prime divisors. While it appears to be almost certain that this index assumes each of the values 1 and 3 infinitely often, we have not been able to prove this. Four examples are described below. In two of these f has three prime divisors, but $(W : V) = 9$ for the first and $(W : V) = 3$ for the second. In the final two examples f has 4 prime divisors, but the unit index is 3 in one and 1 in the other.

Example 1.

$$f = 9709 = 7 \cdot 19 \cdot 73$$

$$f_1 = 133 = 7 \cdot 19, \alpha_1 = \frac{-10 + 4(3\sqrt{-3})}{2}, b_1 = 7^2$$

$$f_2 = 511 = 7 \cdot 73, \alpha_2 = \frac{37 + 5(3\sqrt{-3})}{2}, b_2 = 7^2$$

$$f_3 = 1387 = 19 \cdot 73, \alpha_3 = \frac{65 - 7(3\sqrt{-3})}{2}, b_3 = 19^2 \cdot 73^2$$

$$f_4 = 9709 = 7 \cdot 19 \cdot 73, \alpha_4 = \frac{197 + 3\sqrt{-3}}{2}, b_4 = 7 \cdot 19 \cdot 73$$

$$M = \begin{pmatrix} 2 & 2 & 0 & 1 \\ 0 & 0 & 2 & 1 \\ 0 & 0 & 2 & 1 \end{pmatrix} \text{ has rank 2, so } (W : V) = 9.$$

Example 2.

$$f = 819 = 9 \cdot 7 \cdot 13$$

$$f_1 = 9, \alpha_1 = \frac{-3 + 3\sqrt{-3}}{2}, b_1 = 3$$

$$f_2 = 91 = 7 \cdot 13, \alpha_2 = \frac{-16 + 2(3\sqrt{-3})}{2}, b_2 = 13$$

$$f_3 = 819 = 9 \cdot 7 \cdot 13, \alpha_3 = \frac{-3 + 11(3\sqrt{-3})}{2}, b_3 = 7^2 \cdot 13^2$$

$$f_4 = 819 = 9 \cdot 7 \cdot 13, \alpha_4 = \frac{51 + 5(3\sqrt{-3})}{2}, b_4 = 3^2 \cdot 7^2$$

$$M = \begin{pmatrix} 1 & 0 & 0 & 2 \\ 0 & 0 & 2 & 2 \\ 0 & 1 & 2 & 0 \end{pmatrix} \text{ has rank 3, so } (W : V) = 3.$$

Example 3.

$$f = 15561 = 9 \cdot 7 \cdot 13 \cdot 19$$

$$f_1 = 819 = 9 \cdot 7 \cdot 13, \alpha_1 = \frac{-57 + 3\sqrt{-3}}{2}, b_1 = 3 \cdot 7^2 \cdot 13^2$$

$$f_2 = 1197 = 9 \cdot 7 \cdot 19, \alpha_2 = \frac{-66 + 4(3\sqrt{-3})}{2}, b_2 = 3^2 \cdot 19^2$$

$$f_3 = 1729 = 7 \cdot 13 \cdot 19, \alpha_3 = \frac{29 + 15(3\sqrt{-3})}{2}, b_3 = 7^2 \cdot 13 \cdot 19^2$$

$$f_4 = 2223 = 9 \cdot 13 \cdot 19, \alpha_4 = \frac{87 + 7(3\sqrt{-3})}{2}, b_4 = 3 \cdot 19$$

$$M = \begin{pmatrix} 1 & 2 & 0 & 1 \\ 2 & 0 & 2 & 0 \\ 2 & 0 & 1 & 0 \\ 0 & 2 & 2 & 1 \end{pmatrix} \text{ has rank 3, so } (W : V) = 3.$$

Example 4.

$$f = 15561 = 9 \cdot 7 \cdot 13 \cdot 19$$

$$f_1 = 819 = 9 \cdot 7 \cdot 13, \alpha_1 = \frac{24 + 10(3\sqrt{-3})}{2}, b_1 = 7 \cdot 13$$

$$f_2 = 1197 = 9 \cdot 7 \cdot 19, \alpha_2 = \frac{69 + 3\sqrt{-3}}{2}, b_2 = 3 \cdot 7^2 \cdot 19^2$$

$$f_3 = 1729 = 7 \cdot 13 \cdot 19, \alpha_3 = \frac{83 + 3\sqrt{-3}}{2}, b_3 = 7^2 \cdot 13 \cdot 19^2$$

$$f_4 = 2223 = 9 \cdot 13 \cdot 19, \alpha_4 = \frac{33 + 17(3\sqrt{-3})}{2}, b_4 = 3 \cdot 13^2 \cdot 19$$

$$M = \begin{pmatrix} 0 & 1 & 0 & 1 \\ 1 & 2 & 2 & 0 \\ 1 & 0 & 1 & 2 \\ 0 & 2 & 2 & 1 \end{pmatrix} \text{ has rank 4, so } (W : V) = 1.$$

References

1. M. N. Gras, *Méthodes et algorithmes pour le calcul numérique du nombre de classes et des unité des extensions cubiques cycliques de Q*, J. Reine Angew. Math. *277*(1975), 89–116.
2. H. Hasse, *Arithmetische Bestimmung von Grundeinheit und Klassenzahl in zyklischen kubischen und biquadratischen Zahlkörpern*, Abh. Deutsch. Akad. Wiss. Berlin *2* (1948), 1–95.
3. ——— *Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper*, Würzburg, Wien (1970).
4. ——— *Über die Klassenzahl abelscher Zahlkörper*, Berlin (1952).
5. S. Maki, *The determination of units in real cyclic sextic fields* (Berlin, Heidelberg, New York, 1980).
6. B. L. Van Der Waerden, *Modern algebra* (New York, 1964).
7. C. D. Walter, *Kuroda's class number relation*, Acta Arithmetica *35* (1979), 41–51.

Virgina Polytechnic Institute and State University,
Blacksburg, Virginia