JOURNAL OF NUMBER THEORY 15, 137–142 (1982)

A Parametric Family of Quintic Polynomials with Galois Group D_5

G. ROLAND, N. YUI,* AND D. ZAGIER

Mathematisches Institut der Universität Bonn, 5300 Bonn, West Germany

Communicated by the Editors

Received September 12, 1980

We give a parametric family of quintic polynomials of the form $x^5 + ax + b$ ($a, b \in \mathbb{Q}$) with dihedral Galois group D_5. Some properties of the fields defined by these polynomials are also described.

The goal of this paper is to give explicitly an infinite family of quintic fields with dihedral Galois group.

THEOREM 1. *The quintic polynomials of the form $x^5 + ax + b$, $(a, b \in \mathbb{Q})$ with Galois group D_5 are given parametrically by*

$$a = \frac{5\alpha^4}{4}(\beta^2 + 1)^2(\beta^2 + \beta - 1)(\beta^2 - \beta - 1),$$

$$b = \frac{\alpha^5}{2}(\beta^2 + 1)^3(\beta^2 + \beta - 1)(2\beta - 1)(\beta + 2)$$

with $\alpha, \beta \in \mathbb{Q}$, $\alpha \neq 0$, $\beta \neq \frac{1}{2}, -2$.[1]

Proof. Let $f(x) = x^5 + ax + b \in \mathbb{Q}[x]$ and let $\mathrm{Gal}(f)$ be its Galois group over $\mathbb{Q}$. Then the necessary and sufficient conditions for $\mathrm{Gal}(f) \cong D_5$ are the following:

(i) $f(x)$ is irreducible over $\mathbb{Q}$.

(ii) The discriminant $D_f = 4^4a^5 + 5^5b^4$ of $f(x)$ is a perfect square.

(iii) $f(x)$ is solvable by radicals.

Indeed, the necessity is clear. For the sufficiency, observe that (i) implies

*Current address: Department of Mathematics, The Ohio State University, Columbus, Ohio 43210.

[1] We must confine ourselves to those $\alpha, \beta \in \mathbb{Q}$ for which $f(x)$ is irreducible over $\mathbb{Q}$. This was pointed to us by Lenstra Jr.

0022-314X/82/040137-05$02.00/0

that $\mathrm{Gal}(f)$ has an element of order 5 acting transitively on the set of zeros of $f(x)$, and (ii) guarantees that $\mathrm{Gal}(f) \subseteq A_5$. The transitive subgroups of A_5 are Z_5, D_5 and A_5. But condition (iii) excludes A_5, and since $df/dx = 5x^4 + a$ has at least two imaginary zeros, $\mathrm{Gal}(f)$ contains an involution, so $\mathrm{Gal}(f) \not\cong Z_5$. Therefore, $\mathrm{Gal}(f) \cong D_5$.

Weber [2, p. 676] (see also Čebotarev [1, p. 344]) proved that $x^5 + ax + b$ is solvable by radicals if and only if a and b are of the form

$$a = \frac{5^5\lambda\mu^4}{(\lambda-1)^4(\lambda^2-6\lambda+25)}, \qquad b = \frac{5^5\lambda\mu^5}{(\lambda-1)^4(\lambda^2-6\lambda+25)}$$

with $\lambda, \mu \in \mathbb{Q}, \lambda \neq 1, \mu \neq 0$. Making the change of variables

$$\lambda = 5\,\frac{u+1}{u-1}, \qquad \frac{5\mu}{\lambda-1} = v,$$

we can rewrite this equivalently as

$$a = \frac{5}{4}\,\frac{(u+1)(u-1)}{u^2+4}\,v^4, \qquad b = \frac{1}{2}\,\frac{(u+1)(2u+3)}{u^2+4}\,v^5.$$

The discriminant of f is then given by

$$D_f = \frac{5^6(u+1)^4(2u^3+4u^2+11u+8)^2}{2^4(u^2+4)^5}\,v^{20}.$$

Hence D_f is a perfect square if and only if u^2+4 is a perfect square, i.e., if $u = \beta - 1/\beta$ with some $\beta \in \mathbb{Q}$. Setting $\alpha = v/(\beta^2+1)$, we recover the formula of the theorem.

Writing $\beta = m/n$ $(m, n \in \mathbb{Z}, (m, n) = 1)$, $d = 2n^2/\alpha$, we can rewrite a and b in the theorem in the form

$$\begin{aligned} a &= 20(m^2+n^2)^2(m^2+mn-n^2)(m^2-mn-n^2)/d^4, \\ b &= 16(m^2+n^2)^3(m^2+mn-n^2)(2m-n)(m+2n)/d^5 \end{aligned} \tag{1}$$

with $m, n \in \mathbb{Z}$, $d \in \mathbb{Q}^\times$. Since the substitution $a \mapsto \rho^4 a$, $b \mapsto \rho^5 b$ $(\rho \in \mathbb{Q}^\times)$ does not change the field generated by $f(x)$, the choice of d does not matter. The easiest choice is $d = 1$; the "best" choice is to take for d the largest integer such that the numbers a, b defined by (1) are integral. This d has the form $d = 2^i 5^j d_1 d_2$, where $i, j \in \{0, 1\}$ and d_1, d_2 are the largest natural numbers with $d_1^2 \mid m^2+n^2$, $d_2^5 \mid m^2+mn-n^2$. Then (1) becomes

$$\begin{aligned} a &= 2^{2-4i}5^{1-4j} \cdot d_2 \cdot (m^2-mn-n^2) \cdot E^2 \cdot F, \\ b &= 2^{4-5i}5^{-5j} \cdot d_1 \cdot (2m-n)(m+2n) \cdot E^3 \cdot F \end{aligned} \tag{2}$$

with

$$E = \frac{m^2 + n^2}{d_1^2}, \qquad F = \frac{m^2 + mn - n^2}{d_2^5},$$

and the formula for the discriminant becomes

$$D_f = 2^{16-20i} 5^{6-20j} \cdot (2m^6 + 4m^5 n + 5m^4 n^2 - 5m^2 n^4 + 4mn^5 - 2n^6)^2 \cdot E^{10} \cdot F^4. \tag{3}$$

Let $f (= f_{m,n})$ be the polynomial $x^5 + ax + b$ with a and b as in (2). Set K $(= K_{m,n}) = \mathbb{Q}[\alpha]/(f(\alpha))$ and N the normal closure of K (splitting field of $f(x)$). Denote by L the unique quadratic subfield of N. We list without proofs some of the properties of the field $K_{m,n}$.

$$\begin{tikzcd}
& N \arrow[dl, dash, "5"'] \arrow[dr, dash, "2"] & \\
L \arrow[dr, dash, "2"'] & & K = K_{m,n} \arrow[dl, dash, "5"] \\
& \mathbb{Q} &
\end{tikzcd}$$

(a) We have $L = \mathbb{Q}(\sqrt{-5(m^2+n^2)})$. Thus a quadratic field L corresponds to some $K_{m,n}$ if and only if L is imaginary quadratic and no prime $\equiv 3 \pmod 4$ divides the discriminant of L. In particular, 2 always is ramified in L.

(b) For $p \neq 5$, we have

$$p = \mathfrak{p}^5 \ (N\mathfrak{p} = p) \Leftrightarrow p \mid F,$$

$$p = \mathfrak{p}_1 \mathfrak{p}_2^2 \mathfrak{p}_3^2 \ (N\mathfrak{p}_i = p) \Leftrightarrow p \mid 2E,$$

p unramified otherwise.

We denote by Δ_K (Δ_L) the discriminant of K (L). In the first case we have $p^4 \parallel \Delta_K$. In the second case we have $v_p(\Delta_K) = 2v_p(\Delta_L)$ (=2 if $p \neq 2$, 4 or 6 if $p = 2$). In the last case, of course, $p \nmid \Delta_K$. Finally, the ramification of 5 is given as follows:

$$5 \text{ unramified} \Leftrightarrow m \equiv 3n \pmod 5 \quad \text{or} \quad m \equiv 57n \pmod{125} \quad \text{and} \quad 5 \mid E$$

$$5 = \mathfrak{p}_1 \mathfrak{p}_2^2 \mathfrak{p}_3^2 \Leftrightarrow m \equiv 3n \pmod 5 \quad \text{or} \quad m \equiv 57n \pmod{125} \quad \text{and} \quad 5 \nmid E$$

$$5 = \mathfrak{p}^5 \Leftrightarrow m \not\equiv 3n \pmod 5,\ m \not\equiv 57n \pmod{125}.$$

(c) Let Δ_L denote the discriminant of L (so $\Delta_L = -20E$ or $\Delta_L = -5E$). Then the splitting of non-ramified primes is given by

$$\left(\frac{\Delta_L}{p}\right) = -1 \Leftrightarrow p = \mathfrak{p}_1 \mathfrak{p}_2 \mathfrak{p}_3 \qquad (N\mathfrak{p}_1 = p,\ N\mathfrak{p}_2 = N\mathfrak{p}_3 = p^2),$$

$$\left(\frac{\Delta_L}{p}\right) = 1 \Leftrightarrow p = \mathfrak{p} \qquad (N\mathfrak{p} = p^5) \quad \text{or} \quad p = \mathfrak{p}_1 \mathfrak{p}_2 \mathfrak{p}_3 \mathfrak{p}_4 \mathfrak{p}_5\ (N\mathfrak{p}_i = p).$$

The density of the three kinds of primes are 50%, 40% and 10%. If $(\Delta_L/p) = 1$, then $Q(x, y) = p$ for some quadratic form Q of discriminant Δ_L and some $x, y \in \mathbb{Z}$ (this representation is essentially unique). Then the question whether p is inert or splits completely depends on Q and on congruences on x, y modulo $25F$ (at most). We illustrate the situation with some examples.

EXAMPLE 1. $m = 1$, $n = 1$, $f(x) = x^5 - 5x + 12$. In this case, $E = 2$, $F = 1$ and $L = \mathbb{Q}(\sqrt{-10})$. Here 2 and 5 are the only ramified primes (5 ramifies both in $L/\mathbb{Q}$ and N/L) and for $p \neq 2, 5$ we have

$$p = \mathfrak{p}_1 \mathfrak{p}_2 \mathfrak{p}_3\ (N\mathfrak{p}_1 = p, N\mathfrak{p}_2 = N\mathfrak{p}_3 = p^2) \Leftrightarrow \left(\frac{-10}{p}\right) = -1,$$

$$p \text{ inert} \Leftrightarrow p = x^2 + 10y^2 \text{ or } 2x^2 + 5y^2 \text{ with } 5 \nmid y,$$

$$p \text{ splits} \Leftrightarrow p = x^2 + 250z^2 \text{ or } 2x^2 + 125z^2.$$

In particular, if $p = N(\xi)$ ($\xi \in \mathbb{Z} + \mathbb{Z}\sqrt{-10}$), then p splits if and only if $\xi^4 \equiv 1 \pmod 5$.

EXAMPLE 2. $m = 3, n = 1$, $f(x) = x^5 + 11x + 44$. In this case, $E = 10$, $F = 11$ and $L = \mathbb{Q}(\sqrt{-2})$. Here 2 and 11 ramify and for $p \neq 2, 11$ we have

$$p = \mathfrak{p}_1 \mathfrak{p}_2 \mathfrak{p}_3\ (N\mathfrak{p}_1 = p, N\mathfrak{p}_2 = N\mathfrak{p}_3 = p^2) \Leftrightarrow p \equiv 5 \text{ or } 7 \pmod 8,$$

$$p \text{ inert} \Leftrightarrow p = x^2 + 2y^2, xy \not\equiv 0 \pmod{11},$$

$$p \text{ splits} \Leftrightarrow p = 121x^2 + 2y^2 \text{ or } x^2 + 242y^2.$$

EXAMPLE 3. $m = 2, n = 1$, $f(x) = x^5 + 2500x + 120000$. (Note that $f(x)$ is equivalent to $4x^5 + x + 5$.) In this case, $E = 5$, $F = 5$ and $L = \mathbb{Q}(\sqrt{-1}) = \mathbb{Q}(i)$. Here for $p \neq 2, 5$ we have

$$p = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3 \; (N\mathfrak{p}_1 = p, N\mathfrak{p}_2 = N\mathfrak{p}_3 = p^2) \Leftrightarrow p \equiv 3 \pmod 4,$$

$$p \text{ inert} \Leftrightarrow p = x^2 + y^2,\; 25 \nmid xy(x-y)(x+y),$$

$$p \text{ splits} \Leftrightarrow p = x^2 + 625z^2 \text{ or } 313z^2 - 2zt + 2t^2.$$

Thus the smallest prime which splits in K is 313.

EXAMPLE 4. If m and n are relatively prime integers with $m \equiv 3n \pmod 5$ or $m \equiv 57n \pmod{125}$ and $m^2 + mn - n^2$ equal to a fifth power times a power of 5, then (b) and (c) above imply that N/L is unramified and hence that the class number of L is divisible by 5. These Diophantine equations/congruences can be solved parametrically by

$$m + n\omega = \omega^{-2}(r + s\omega)^5 \qquad ((r, s) = 1, r \not\equiv 2s \pmod 5)$$

and

$$m + n\omega = \omega^{-2}(r + s\omega)^5 \sqrt{5} \qquad ((r, s) = 1, r \equiv 3s \pmod 5)),$$

respectively, where $\omega = (1 + \sqrt{5})/2$. Explicitly, this gives

(i) $m = f(r, s)$, $n = f(s, -r)$, $m^2 + n^2 = 5\Delta(r, s)$,

(ii) $m = -f(r, s) + 2f(s, -r)$, $\quad n = 2f(r, s) + f(s, -r)$, $\quad m^2 + n^2 = 25\Delta(r, s)$ with $f(r, s) = 2r^5 - 5r^4s + 10r^3s^2 + 5rs^4 + s^5$ and

$$\begin{aligned}\Delta(r, s) = (f(r, s)^2 + f(s, -r)^2)/5 &= r^{10} - 6r^9s + 18r^8s^2 - 24r^7s^3 \\ &\quad + 42r^6s^4 + 42r^4s^6 + 24r^3s^7 + 18r^2s^8 + 6rs^9 + s^{10}.\end{aligned}$$

We deduce:

THEOREM 2. *If r and s are coprime integers with $r \not\equiv 2s \pmod 5$, then the class number of the imaginary quadratic field $\mathbb{Q}(\sqrt{-\Delta(r, s)})$ is divisible by 5. If $r \equiv 3s \pmod 5$, then the same holds for $\mathbb{Q}(\sqrt{-5\Delta(r, s)})$.*

Since $\Delta(-r + 2s, 2r + s) = 5^5\Delta(r, s)$ (this follows from the identity $\Delta = 5A^5 - 5A^3B^2 + AB^4$, where $A = r^2 + s^2$, $B = r^2 + rs - s^2$), we see that in fact at least one of the class numbers in question is divisible by 5 for *any* integers r, s.

We give some numerical examples:

r	s		m	n	m^2+mn-n^2	m^2+n^2	$h(\mathbb{Q}(\sqrt{-5(m^2+n^2)}))$
1	1	(i)	13	21	1	5×122	10
1	2	(i)	144	233	-1	$5^2 \times 3001$	80
		(ii)	322	521	5	$5^3 \times 3001$	40
3	1	(i)	367	269	11^5	$5^2 \times 8282$	120
		(ii)	171	1003	-5×11^5	$5^3 \times 8282$	60

References

1. N. Čebotarev, "Grundzüge der Galoisschen Theorie," Noordhoff, Groningen, 1950.
2. H. Weber, "Lehrbuch der Algebra," Chelsea, New York.

Printed in Belgium