Bull. Aust. Math. Soc. **97** (2018), 47–53
doi:10.1017/S0004972717000648

AN INFINITE FAMILY OF NINTH DEGREE DIHEDRAL POLYNOMIALS

LENNY JONES✉ and TRISTAN PHILLIPS

(Received 10 May 2017; accepted 30 May 2017; first published online 14 August 2017)

Abstract

For any integer $m \neq 0$, we prove that $f(x) = x^9 + 9mx^6 + 192m^3$ is irreducible over $\mathbb{Q}$ and that the Galois group of $f(x)$ over $\mathbb{Q}$ is the dihedral group of order 18. Moreover, we show that for infinitely many values of m, the splitting fields for $f(x)$ are distinct.

2010 *Mathematics subject classification*: primary 12F10; secondary 11R09, 11R32, 12F12.

Keywords and phrases: dihedral group, Galois group, irreducible polynomial, Capelli.

1. Introduction

Unless stated otherwise, when we say a polynomial is *irreducible* or *reducible*, we mean over $\mathbb{Q}$, the rational numbers. In 1892, using his irreducibility theorem, Hilbert showed that there exist infinitely many irreducible polynomials with Galois group G for each $G \in \{S_n, A_n\}$, where S_n and A_n denote the symmetric and alternating groups of order n, respectively. Since then, many authors have used additional techniques, such as resolvents, class field theory, elliptic curves, factorisation over quadratic fields and factorisation modulo a prime, to obtain similar results for other groups (see, for example, [2, 5–7, 9–11]). In particular, Williamson [11] used a combination of such methods to prove that there exist infinitely many $t \in \mathbb{Q}$ such that the polynomial

$$x^9 - tx^8 + (-4t + 378)x^7 + (68t + 6804)x^6 + (288t + 33048)x^5 + (-1008t + 50544)x^4 + (-5184t + 7776)x^3 + (-5184t + 139968)x^2 + 279936x + 186624$$

has Galois group D_9, the dihedral group of order 18. In this paper, using only two theorems of Capelli and their generalisations due to Rédei, we find an explicit infinite family of irreducible ninth degree polynomials having Galois group D_9. More precisely, we prove the following theorem.

THEOREM 1.1. *Let $m \neq 0$ be an integer, and let*

$$f(x) = x^9 + 9mx^6 + 192m^3.$$

Then $f(x)$ is irreducible and $\mathrm{Gal}(f) \simeq D_9$, where $\mathrm{Gal}(f)$ is the Galois group of $f(x)$ and D_9 is the dihedral group of order 18. Moreover, there exist infinitely many values of m such that the splitting fields of $f(x)$ are distinct.

2. Preliminaries

Throughout this paper, $\Delta(f)$ denotes the discriminant over $\mathbb{Q}$ of the polynomial $f(x)$ and, if $f(x)$ is irreducible, $\mathrm{Gal}(f)$ denotes its Galois group. We now present some results of Capelli, without proof, that are needed to establish Theorem 1.1.

THEOREM 2.1. *Let K be a field and let $g(x), h(x) \in K[x]$ with $g(x)$ irreducible over K. Suppose that $g(\alpha) = 0$. Then $g(h(x))$ is reducible over K if and only if $h(x) - \alpha$ is reducible over $K(\alpha)$. Furthermore, if*

$$h(x) - \alpha = c_1 u_1(x)^{e_1} \cdots u_k(x)^{e_k},$$

where $c_1 \in K(\alpha)$ and the $u_j(x)$ are distinct monic irreducible polynomials in $K(\alpha)[x]$, then

$$g(h(x)) = c_2 \mathcal{N}(u_1(x))^{e_1} \cdots \mathcal{N}(u_k(x))^{e_k},$$

where $c_2 \in \mathbb{Q}$ and the norms $\mathcal{N}(u_j(x))$ are distinct monic irreducible polynomials in $K[x]$.

THEOREM 2.2. *Let K be a field and let $n \geq 2$ be an integer. Let $\alpha \in K$. Then $x^n - \alpha$ is reducible over K if and only if either there is a prime p dividing n such that $\alpha = \beta^p$ for some $\beta \in K$, or $4 \mid n$ and $\alpha = -4\beta^4$ for some $\beta \in K$.*

REMARK 2.3. When $K \subset \mathbb{C}$, Theorems 2.1 and 2.2 are due to Capelli. Rédei extended Theorem 2.2 to fields of positive characteristic, and also Theorem 2.1 to fields of positive characteristic when $g(x)$ is separable. Schinzel extended Theorem 2.1 further to include the case when $g(x)$ is purely inseparable. For more details, and a proof of the general version of Theorem 2.1, see [8].

We also require the following well-known facts.

THEOREM 2.4 [4]. *Suppose that $\deg(f(x)) = n$. If $f(x)$ is irreducible, then $\mathrm{Gal}(f)$ is isomorphic to a subgroup of the alternating group A_n if and only if $\sqrt{\Delta(f)} \in \mathbb{Z}$.*

THEOREM 2.5 [1]. *Let $f(x) \in \mathbb{Z}[x]$ be monic of degree n and let $\mathrm{Gal}(f)$ be the Galois group of $f(x)$ over $\mathbb{Q}$. Let p be a prime such that $\Delta(f) \not\equiv 0 \pmod{p}$. If $f(x)$ factors in $\mathbb{F}_p[x]$ as a product of irreducible factors of degrees $n_1, n_2, \ldots, n_t$, then $\mathrm{Gal}(f)$, when viewed as isomorphic to a subgroup of the symmetric group S_n, contains a permutation $\sigma_1\sigma_2\cdots\sigma_t$, where σ_i is a cycle of length n_i.*

REMARK 2.6. Theorem 2.5 is due to Dedekind.

https://doi.org/10.1017/S0004972717000648 Published online by Cambridge University Press

3. The Proof of Theorem 1.1

Proof of Theorem 1.1. Let $m \neq 0$ be an integer and define the polynomials:

$$\begin{aligned}
h_1(x) &:= x^2 \\
h_2(x) &:= x^3 \\
g(x) &:= x^3 + 9mx^2 + 192m^3 \\
G_1(x) &:= x^3 + 486m^2x^2 + 121257m^4x + 995328m^6 \\
f(x) &:= g(h_2(x)) = x^9 + 9mx^6 + 192m^3 \\
G(x) &:= G_1(h_1(x)) = x^6 + 486m^2x^4 + 121257m^4x^2 + 995328m^6 \\
F(x) &:= G(h_2(x)) = x^{18} + 486m^2x^{12} + 121257m^4x^6 + 995328m^6.
\end{aligned}$$

We claim that the polynomials $g(x)$, $G_1(x)$, $f(x)$, $G(x)$ and $F(x)$ are all irreducible. Although the arguments are similar, we provide at least a sketch of the details in each case.

Consider first $g(x) = x^3 + 9mx^2 + 192m^3$. Since

$$\Delta(g) = -2^8 3^5 5^2 m^6 < 0,$$

if follows that $g(x)$ has exactly one real zero. An easy computation in Maple shows that this zero is

$$(-3 \cdot 3^{2/3} - 3^{1/3} - 3)m \notin \mathbb{Z}.$$

Hence, $g(x)$ is irreducible.

Similarly, since

$$\Delta(G_1) = -2^{10} 3^{13} 5^6 11^2 m^{12} < 0,$$

we conclude that $G_1(x)$ has exactly one real zero

$$3(35 \cdot 3^{2/3} - 15 \cdot 3^{1/3} - 54)m^2 \notin \mathbb{Z},$$

so that $G_1(x)$ is irreducible.

To establish the irreducibility of $f(x)$, $G(x)$ and $F(x)$, the strategy is the same in each of these cases. We assume reducibility and achieve a contradiction using Theorems 2.1 and 2.2.

Suppose that $f(x)$ is reducible and $g(\alpha) = 0$. Then

$$f(x) = N(x - \beta) \cdot N(x^2 + \beta x + \beta^2),$$

where $\alpha = \beta^3$ for some $\beta \in \mathbb{Q}(\alpha)$, and $N(x - \beta) \in \mathbb{Z}[x]$ and $N(x^2 + \beta x + \beta^2) \in \mathbb{Z}[x]$ have respective degrees of three and six. Let n_0 be the constant term of $N(x - \beta)$. If β_2, β_3 are the conjugates of $\beta := \beta_1$ and α_2, α_3 are the conjugates of $\alpha := \alpha_1$, it follows that

$$n_0 = -\beta_1\beta_2\beta_3 = -\alpha_1^{1/3}\alpha_2^{1/3}\alpha_3^{1/3} = -(\alpha_1\alpha_2\alpha_3)^{1/3} = -(-192m^3)^{1/3} \notin \mathbb{Z},$$

which contradicts the fact that $n_0 \in \mathbb{Z}$. Thus, $f(x)$ is irreducible.

https://doi.org/10.1017/S0004972717000648 Published online by Cambridge University Press

Suppose that $G(x)$ is reducible and that $G_1(\alpha) = 0$. Arguing as before,

$$G(x) = \mathcal{N}(x-\beta)\cdot\mathcal{N}(x+\beta),$$

where $\alpha = \beta^2$ for some $\beta \in \mathbb{Q}(\alpha)$, and $\mathcal{N}(x-\beta) \in \mathbb{Z}[x]$, $\mathcal{N}(x-\beta) \in \mathbb{Z}[x]$ both have degree three. Let n_0 be the constant term of $\mathcal{N}(x-\beta)$. Then, calculating n_0 as before, we arrive at the contradiction

$$n_0 = -(-192m^3)^{1/3} \notin \mathbb{Z}.$$

Hence, $G(x)$ is irreducible.

Finally, suppose that $F(x)$ is reducible and that $G(\alpha) = 0$. Then

$$F(x) = \mathcal{N}(x-\beta)\cdot\mathcal{N}(x^2+\beta x+\beta^2),$$

where $\alpha = \beta^3$ for some $\beta \in \mathbb{Q}(\alpha)$ and $\mathcal{N}(x-\beta)$ and $\mathcal{N}(x^2+\beta x+\beta^2)$ are monic polynomials in $\mathbb{Z}[x]$ of respective degrees six and 12. If n_0 is the constant term of $\mathcal{N}(x-\beta)$, we arrive at the contradiction

$$n_0 = -(-995328m^6)^{1/3} \notin \mathbb{Z}$$

since $995328 = 2^{12}3^5$. Therefore, $F(x)$ is irreducible.

Let L be the splitting field of $f(x)$ over $\mathbb{Q}$. By Descartes' rule of signs, $f(x)$ has exactly one real zero θ. Clearly, $\mathbb{Q}(\theta) \subset L$ and, since $f(x)$ is irreducible, $[\mathbb{Q}(\theta):\mathbb{Q}] = 9$. But $\mathbb{Q}(\theta) \subset \mathbb{R}$, so $\mathbb{Q}(\theta) \neq L$ and thus $[L:\mathbb{Q}] \geq 18$. Let $\theta_1, \theta_2, \ldots, \theta_9$ be the zeros of $f(x)$ and let γ be such that $F(\gamma) = 0$. Then, using a computer algebra system, it is straightforward to check that

$$\theta_1 = \frac{\gamma^{16} + 60m\gamma^{13} + 234m^2\gamma^{10} + 31860m^3\gamma^7 - 145611m^4\gamma^4 + 6713280m^5\gamma}{5702400m^5}$$

$$\theta_2 = \frac{9\gamma^{16} + 32m\gamma^{13} + 4086m^2\gamma^{10} + 23328m^3\gamma^7 + 1039761m^4\gamma^4 + 5272128m^5\gamma}{3801600m^5}$$

$$\theta_3 = \frac{-17\gamma^{16} + 60m\gamma^{13} - 7938m^2\gamma^{10} + 31860m^3\gamma^7 - 1908333m^4\gamma^4 + 3862080m^5\gamma}{5702400m^5}$$

$$\theta_4 = \frac{2\gamma^{16} + 963m^2\gamma^{10} + 256743m^4\gamma^4 - 356400m^5\gamma}{712800m^5}$$

$$\theta_5 = \frac{-\gamma^{16} - 454m^2\gamma^{10} - 115529m^4\gamma^4}{211200m^5}$$

$$\theta_6 = \frac{9\gamma^{16} - 32m\gamma^{13} + 4086m^2\gamma^{10} - 23328m^3\gamma^7 + 1039761m^4\gamma^4 - 5272128m^5\gamma}{3801600m^5}$$

$$\theta_7 = \frac{2\gamma^{16} + 963m^2\gamma^{10} + 256743m^4\gamma^4 + 356400m^5\gamma}{712800m^5}$$

$$\theta_8 = \frac{-17\gamma^{16} - 60m\gamma^{13} - 7938m^2\gamma^{10} - 31860m^3\gamma^7 - 1908333m^4\gamma^4 - 3862080m^5\gamma}{5702400m^5}$$

$$\theta_9 = \frac{\gamma^{16} - 60m\gamma^{13} + 234m^2\gamma^{10} - 31860m^3\gamma^7 - 145611m^4\gamma^4 - 6713280m^5\gamma}{5702400m^5}.$$

https://doi.org/10.1017/S0004972717000648 Published online by Cambridge University Press

Thus, $L \subseteq \mathbb{Q}(\gamma)$. Since $F(x)$ is irreducible, $[\mathbb{Q}(\gamma) : \mathbb{Q}] = 18$, which implies that $[L : \mathbb{Q}] \leq 18$. Hence, $[L : \mathbb{Q}] = 18$ and $L = \mathbb{Q}(\gamma)$. Since

$$\Delta(f) = 2^{36}3^{26}5^6m^{24},$$

it follows from Theorem 2.4 that

$$\mathrm{Gal}(f) \simeq \mathbb{Z}_9 \rtimes \mathbb{Z}_2 \simeq D_9 \quad \text{or} \quad \mathrm{Gal}(f) \simeq (\mathbb{Z}_3 \times \mathbb{Z}_3) \rtimes \mathbb{Z}_2,$$

because D_9 and $(\mathbb{Z}_3 \times \mathbb{Z}_3) \rtimes \mathbb{Z}_2$ are the only transitive subgroups of A_9 of order 18 [3]. To see that $\mathrm{Gal}(f) \simeq D_9$, let p be a prime such that $\Delta(f) \not\equiv 0 \pmod{p}$ and $y^3 \equiv 3 \pmod{p}$ has no solutions. Suppose that $f(x)$ is reducible over $\mathbb{F}_p$. Then, by Theorems 2.1 and 2.2, we argue as before to deduce that

$$-(-192m^6)^{1/3} = 2^2 3^{1/3} m^2 \in \mathbb{F}_p,$$

which contradicts the fact that 3 is not a cube in $\mathbb{F}_p$. Hence, $f(x)$ is irreducible over $\mathbb{F}_p$ and thus, by Theorem 2.5, we conclude that $\mathrm{Gal}(f)$ contains an element of order 9. Since $(\mathbb{Z}_3 \times \mathbb{Z}_3) \rtimes \mathbb{Z}_2$ contains no element of order 9, it follows that $\mathrm{Gal}(f) \simeq D_9$.

We now show that there exist infinitely many values of m for which the splitting fields of $f(x)$ are distinct. Let $p \neq q$ be primes, and let

$$f_p(x) = x^9 + 9px^6 + 192p^3 \quad \text{and} \quad f_q(x) = x^9 + 9qx^6 + 192q^3,$$

with respective splitting fields L_p and L_q. Let $r = -(3^{5/3} + 3^{1/3} + 3)$. As we have seen,

$$g_p(pr) = 0 = g_q(qr).$$

Thus,

$$f_p(p^{1/3}r^{1/3}) = 0 = f_q(q^{1/3}r^{1/3}),$$

since $f_p(x) = g_p(x^3)$ and $f_q(x) = g_q(x^3)$. Suppose that $L_p = L_q$. Then

$$M := \mathbb{Q}(r, (p/q)^{1/3}) \subset L_p,$$

where M is a totally real field with $[M : \mathbb{Q}] = 9$. Since L_p contains a unique totally real subfield of degree nine, it follows that

$$\mathbb{Q}(p^{1/3}r^{1/3}) = M = \mathbb{Q}(q^{1/3}r^{1/3}).$$

Since $\mathrm{Gal}(f) \simeq D_9$, we know that M contains a unique subfield K with $[K : \mathbb{Q}] = 3$. Consequently,

$$\mathbb{Q}((p/q)^{1/3}) = \mathbb{Q}(r) = \mathbb{Q}(3^{1/3}).$$

Therefore, there exist $c_1, c_2, c_3 \in \mathbb{Q}$ such that

$$(p/q)^{1/3} = c_1 + c_2 3^{1/3} + c_3 3^{2/3}. \tag{3.1}$$

Raising both sides of (3.1) to the third power and equating coefficients, we get the system of equations

$$\begin{aligned} 3c_1^2c_2 + 9c_1c_3^2 + 9c_2^2c_3 &= 0 \\ 3c_1^2c_3 + 3c_1c_2^2 + 9c_2c_3^2 &= 0 \\ c_1^3 + 18c_1c_2c_3 + 3c_2^3 + 9c_3^3 &= p/q, \end{aligned}$$

https://doi.org/10.1017/S0004972717000648 Published online by Cambridge University Press

to which Maple provides the three solutions:

$$\{c_2 = 0, c_3 = c_3, p = 9c_3^3 q, c_1 = 0, q = q\},$$
$$\{c_3 = 0, c_2 = c_2, p = 3c_2^3 q, c_1 = 0, q = q\},$$
$$\{p = c_1^3 q, c_2 = 0, c_3 = 0, q = q, c_1 = c_1\}.$$

Each of these possibilities results in a contradiction. For example, consider the second solution and let $c_2 = u/v$, where $u, v \in \mathbb{Z}$ with $\gcd(u, v) = 1$. Then

$$pv^3 = 3u^3 q.$$

If $p = 3$, then $q^{1/3} = v/u \in \mathbb{Q}$, which is impossible. If $p \neq 3$, then $u = pu_1$, for some $u_1 \in \mathbb{Z}$, so that

$$v^3 = 3p^2 u_1^3 q,$$

which implies that $(3p^2 q)^{1/3} = v/u_1 \in \mathbb{Q}$, another contradiction. The other possibilities can be handled in a similar manner. Hence, $L_p \neq L_q$, and the proof is complete. □

Acknowledgement

The authors appreciate the comments and expeditious review of the referee.

References

[1] J. A. Beachy and W. D. Blair, *Abstract Algebra*, 3rd edn (Waveland Press, Inc., Long Grove, IL, 2005).
[2] S. Brown, B. Spearman and Q. Yang, 'On sextic trinomials with Galois group C_6, S_3 or $C_3 \times S_3$', *J. Algebra Appl.* **12**(1) (2013), Article ID 1250128, 9 pages.
[3] G. Butler and J. McKay, 'The transitive groups of degree up to eleven', *Comm. Algebra* **11**(8) (1983), 863–911.
[4] H. Cohen, *A Course in Computational Algebraic Number Theory* (Springer, Berlin, 2000).
[5] J. Harrington and L. Jones, 'The irreducibility of power compositional sextic polynomials and their Galois groups', *Math. Scand.* **120**(2) (2017), 181–194.
[6] J. Ide and Lenny Jones, 'Infinite families of A_4-sextic polynomials', *Canad. Math. Bull.* **57**(3) (2014), 538–545.
[7] C. U. Jensen, A. Ledet and N. Yui, 'Generic polynomials', in: *Constructive Aspects of the Inverse Galois Problem*, Mathematical Sciences Research Institute Publications, 45 (Cambridge University Press, Cambridge, 2002).
[8] A. Schinzel, *Polynomials with Special Regard to Reducibility*, Encyclopedia of Mathematics and its Applications, 77 (Cambridge University Press, Cambridge, 2000).
[9] B. Spearman and K. Williams, 'Quartic trinomials with Galois groups A_4 and V_4', *Far East J. Math. Sci.* **2**(5) (2000), 665–672.
[10] B. Spearman and K. Williams, 'The simplest D_4-octics', *Int. J. Algebra* **2**(1–4) (2008), 79–89.
[11] C. J. Williamson, 'Odd degree polynomials with dihedral Galois groups', *J. Number Theory* **34**(2) (1990), 153–173.

LENNY JONES, Department of Mathematics,
Shippensburg University, Shippensburg, PA 17257, USA
e-mail: lkjone@ship.edu

TRISTAN PHILLIPS, Department of Mathematics,
Shippensburg University, Shippensburg, PA 17257, USA
e-mail: tp7924@ship.edu

https://doi.org/10.1017/S0004972717000648 Published online by Cambridge University Press