Glasgow Math. J. **48** (2006) 553–556. © 2006 Glasgow Mathematical Journal Trust.
doi:10.1017/S0017089506003272. Printed in the United Kingdom

PROBABILISTIC GALOIS THEORY FOR QUARTIC POLYNOMIALS

RAINER DIETMANN

Institut für Algebra und Zahlentheorie, Pfaffenwaldring 57, D-70550 Stuttgart, Germany
e-mail: dietmarr@mathematik.uni-stuttgart.de

(Received 10 March, 2006; revised 17 July, 2006; accepted 31 July, 2006)

Abstract. We prove that there are only $O(H^{3+\epsilon})$ quartic integer polynomials with height at most H and a Galois group which is a proper subgroup of S_4. This improves in the special case of degree four a bound by Gallagher that yielded $O(H^{7/2}\log H)$.

2000 *Mathematics Subject Classification.* 11C08, 11R16, 11R32.

1. Introduction. On probabilistic grounds, one should expect that ‘almost all’ polynomials have the full symmetric group as Galois group acting on the roots. More precisely, let

$$\begin{aligned} E_n(H) = \#\{(a_1, \ldots, a_n) \in \mathbf{Z}^n : |a_i| \leq H\, (1 \leq i \leq n) \text{ and} \\ X^n + a_1X^{n-1} + \ldots + a_n \text{ does not have Galois group } S_n\}. \end{aligned}$$

Then van der Waerden [**8**] showed that

$$E_n(H) \ll_n H^{n-6/((n-2)\log\log H)}.$$

Later, Knobloch [**4**], [**5**] improved this to

$$E_n(H) \ll_n H^{n-c_n}$$

with

$$c_n = \frac{1}{18n(n!)^3}.$$

Finally, using the large sieve, Gallagher [**2**] proved that

$$E_n(H) \ll_n H^{n-1/2}\log H.$$

Since there are only $O_{n,\epsilon}(H^{n-1+\epsilon})$ polynomials like the above that are not irreducible over $\mathbf{Q}$ (see [**1**]), one could conjecture that $E_n(H) \ll_{n,\epsilon} H^{n-1+\epsilon}$. This conjecture has been confirmed by Lefton [**6**] for $n = 3$. In this note we tackle the case $n = 4$, building on Lefton’s ideas and using an explicit characterization for Galois groups of polynomials of degree four.

THEOREM. $E_4(H) \ll_\epsilon H^{3+\epsilon}$.

https://doi.org/10.1017/S0017089506003272 Published online by Cambridge University Press

Note that Wong [**10**, Theorem 1.4] obtained the same result conditionally, assuming the *abc*-conjecture, the Birch–Swinnerton-Dyer conjecture and the generalized Riemann hypothesis for the L-functions of elliptic curves over $\mathbf{Q}$. In fact, in his main result Wong considered the problem of bounding the number of quartic fields with bounded discriminant having Galois group A_4 and gave both a strong conditional result using the hypotheses from above and a weaker unconditional result. It is our aim to show that the bound for $E_4(H)$ from above can be proved by an elementary method without using any further hypotheses, utilizing bounds for the number of points on conics (see Lemma 4) rather than on elliptic curves as in [**10**, Lemma 2.1]. Our main tool is the following characterization of quartic polynomials having Galois group S_4.

Lemma 1. *Let $f(x) = x^4 + ax^3 + bx^2 + cx + d \in \mathbf{Q}[X]$ be irreducible and*

$$r(x) = x^3 - bx^2 + (ac - 4d)x - (a^2d - 4bd + c^2)$$

be the cubic resolvent of f. Then the splitting field of f over $\mathbf{Q}$ has Galois group S_4 if and only if r is irreducible over $\mathbf{Q}$ and the discriminant of f is not a square in $\mathbf{Q}$.

Proof. This follows from Theorem 1 in [**3**].

2. Preparations.

Lemma 2. *Let $f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_n \in \mathbf{C}[X]$. Then all roots $z \in \mathbf{C}$ of the equation $f(z) = 0$ satisfy the inequality*

$$|z| \leq \frac{1}{\sqrt[n]{2} - 1} \cdot \max_{1 \leq k \leq n} \sqrt[k]{\left| \frac{a_k}{a_0\binom{n}{k}} \right|}.$$

Proof. This is Theorem 3 in § 27 of [**7**].

Lemma 3. *Let $N(H)$ be the number of tuples $(a, b, c, d) \in \mathbf{Z}^4$ with*

$$0 \leq |a|, |b|, |c|, |d| \leq H \tag{1}$$

such that the polynomial

$$f(x) = x^3 - bx^2 + (ac - 4d)x - (a^2d - 4bd + c^2)$$

is reducible over $\mathbf{Q}$. Then $N(H) \ll H^3$.

Proof. If f is reducible over $\mathbf{Q}$ then, by Gauss's Lemma, also over $\mathbf{Z}$. (Because $\deg f = 3$ this means that f has an integer zero x.) Moreover, by Lemma 2, $x \ll H$. Hence

$$N(H) \ll \sum_{|x| \ll H} \sum_{|d| \ll H} M(x, d, H),$$

where $M(x, d, H)$ denotes the number of $(a, b, c) \in \mathbf{Z}^3$ satisfying (1) such that

$$x^3 - bx^2 + (ac - 4d)x - (a^2d - 4bd + c^2) = 0. \tag{2}$$

https://doi.org/10.1017/S0017089506003272 Published online by Cambridge University Press

Suppose first that $x^2 - 4d = 0$. Then (2) yields

$$x^3 + (ac - 4d)\,x - (a^2d + c^2) = 0, \tag{3}$$

and so for fixed x and d with $x^2 - 4d = 0$ there are clearly at most $O(H)$ tuples (a, c) with $|a|, |c| \le H$ and satisfying (3). Furthermore, b can be chosen arbitrarily as long as $|b| \le H$. All together, this gives

$$M(x, d, H) \ll H^2$$

if $x^2 - 4d = 0$. Now suppose that $x^2 - 4d \neq 0$. Then (2) yields

$$b = \frac{x^3 + (ac - 4d)x - (a^2d + c^2)}{x^2 - 4d}.$$

Assume first that $|x^2 - 4d| \ge H$. Then clearly

$$\begin{aligned} M(x, d, H) \le \#\{(a, c) \in \mathbf{Z}^2 &: 0 \le |a|, |c| \le H \text{ and} \\ &x^3 + (ac - 4d)x - (a^2d + c^2) \equiv 0 \pmod{|x^2 - 4d|}\} \\ \ll H. \end{aligned} \tag{4}$$

Now suppose that $|x^2 - 4d| \le H$. Then $|x| \ll \sqrt{H}$, and for given P with $1 \le P \le H$ clearly

$$\#\{(x, d) \in \mathbf{Z}^2 : |x|, |d| \ll H \text{ and } P \le |x^2 - 4d| \le 2P\} \ll P\sqrt{H}.$$

Further, if $P \le |x^2 - 4d| \le 2P$ then, analogously to (4), we have

$$M(x, d, H) \ll \frac{H^2}{P}.$$

Collecting our findings from above, we conclude that

$$\begin{aligned} N(H) &\ll \sum_{|x| \ll H} \left(\sum_{\substack{|d| \ll H: \\ x^2 - 4d = 0}} M(x, d, H) + \sum_{\substack{|d| \ll H: \\ x^2 - 4d \neq 0}} M(x, d, H) \right) \\ &\ll H^3 + \sum_{\substack{|x|, |d| \ll H: \\ |x^2 - 4d| \ge H}} H + \sum_{P} \sum_{\substack{|x|, |d| \ll H: \\ P \le |x^2 - 4d| \le 2P}} \frac{H^2}{P} \\ &\ll H^3 + H^{5/2} \log H \\ &\ll H^3. \end{aligned}$$

LEMMA 4. *Let $Q(X, Y) \in \mathbf{Z}[X, Y]$ be a quadratic polynomial with nonzero discriminant and coefficients bounded in modulus by H. Then*

$$\#\{(x, y) \in \mathbf{Z}^2 : |x|, |y| \le P \text{ and } Q(x, y) = 0\} \ll_\epsilon (PH)^\epsilon.$$

Proof. This is Lemma 2 in [**6**].

https://doi.org/10.1017/S0017089506003272 Published online by Cambridge University Press

3. Proof of the Theorem. Since there are only $O(H^{3+\epsilon})$ polynomials $x^4+ax^3+bx^2+cx+d$ satisfying (1) that are reducible over $\mathbf{Q}$ we may in the following assume that our polynomials of this type are irreducible. By Lemma 3 and Lemma 1, it suffices to show that

$$\begin{aligned}&\#\{(a,b,c,d)\in\mathbf{Z}^4 : |a|,|b|,|c|,|d|\leq H \text{ and the discriminant}\\ &\text{of } x^4+ax^3+bx^2+cx+d \text{ is a square in } \mathbf{Q}\}\ll_\epsilon H^{3+\epsilon}.\end{aligned} \tag{5}$$

Now x^4+px^2+qx+r has discriminant

$$D=16p^4r-4p^3q^2-128p^2r^2+144pq^2r-27q^4+256r^3 \tag{6}$$

(see [**9**, § 64]), so that

$$x^4+ax^3+bx^2+cx+d=\left(x+\frac{a}{4}\right)^4+\left(b-\frac{3}{8}a^2\right)x^2+\left(c-\frac{a^3}{16}\right)x+d-\frac{a^4}{256}$$

has discriminant (6) where

$$p=b-\frac{3}{8}a^2,\ q=c-\frac{a^3}{16},\ r=d-\frac{a^4}{256}. \tag{7}$$

Fix a,b,d with $|a|,|b|,|d|\leq H$. There are $O(H^3)$ possibilities of doing so. Then if D is a square in $\mathbf{Q}$, then by (6) and (7) we conclude that

$$2^{24}(-27(q^2)^2+(144pr-4p^3)q^2+16p^4r-128p^2r^2+256r^3)=y^2,$$

for some integer y. This is a quadratic equation in q^2 and so, by Lemma 4, there are at most $O(H^\epsilon)$ solutions with $q^2\ll H^6$ and thus at most $O(H^\epsilon)$ solutions with $c=q+a^3/16\ll H$. Hence the quantity on the left side of (5) can be bounded by $H^{3+\epsilon}$, and we are done.

REFERENCES

1. K. Dörge, Abschätzung der Anzahl der reduziblen Polynome, *Math. Ann.* **160** (1965), 59–63.

2. P. X. Gallagher, The large sieve and probabilistic Galois theory, in *Analytic number theory* (Amer. Math. Soc., 1973), 91–101.

3. Luise-Charlotte Kappe and Bette Warren, An elementary test for the Galois group of a quartic polynomial, *Amer. Math. Monthly* **96** (1989), 133–137.

4. H. W. Knobloch, Zum Hilbertschen Irreduzibilitätssatz, *Abh. Math. Sem. Univ. Hamburg* **19** (1955), 176–190.

5. H. W. Knobloch, Die Seltenheit der reduziblen Polynome, *Jber. Deutsch. Math. Verein.* **59** (1956), Abt. 1, 12–19.

6. Phyllis Lefton, On the Galois groups of cubics and trinomials, *Acta Arith.* **XXXV** (1979), 239–246.

7. Morris Marden, *Geometry of polynomials*, second edition, Mathematical Surveys, No. 3 (American Mathematical Society, 1966).

8. B. L. van der Waerden, Die Seltenheit der reduziblen Gleichungen und die Gleichungen mit Affekt, *Monatsh. Math.* **43** (1936), 137–147.

9. B. L. van der Waerden, *Algebra I* (Springer Verlag, 1991).

10. Siman Wong, Densities of quartic fields with even Galois groups, *Proc. Amer. Math. Soc.* **133** (2005), 2873–2881.

https://doi.org/10.1017/S0017089506003272 Published online by Cambridge University Press