ACTA ARITHMETICA
XXXV (1979)

On the Galois groups of cubics and trinomials

by

PHYLLIS LEFTON (Purchase, N. Y.)

Introduction. A polynomial $f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_n$ with integer coefficients is said to be "with affect" if the Galois group G_f of its splitting field, considered as a permutation group on the roots of $f(x)$, is a proper subgroup of the symmetric group on n letters. In this paper we improve previous upper bounds for the number of monic polynomials of degree 3 with affect. More generally, we also consider trinomials of the form

$$f(x) = ax^n + bx^k + c$$

and count the number of these whose Galois group is a subgroup of the alternating group on n letters.

1. Preliminary lemmas. In this section, we obtain an upper bound for the number of integer points on ellipses and bounded sections of hyperbolas. The estimate also follows from a result in Lang ([10], Theorem 10).

LEMMA 1. *For an integer $d \neq 0$, the number of integer solutions (x, y) of*

$$x^2 - dy^2 = m \quad \text{with } |x|, |y| \leqslant M$$

is $\ll_\varepsilon m^\varepsilon$ for $d < 0$ and $\ll_\varepsilon (mdM)^\varepsilon$ for $d > 0$, for each $\varepsilon > 0$.

Proof. We may assume d is square free by absorbing into y any square factors. Let $a^2 - db^2 = m$. Then the integer

$$\alpha = a + b\sqrt{d} \tag{1.1}$$

of the quadratic field $K = Q(\sqrt{d})$ satisfies $N_{K/Q}\alpha = m$ where $N_{K/Q}\alpha = \alpha\bar{\alpha}$ and $\bar{\alpha} = a - b\sqrt{d}$. The principal ideal $\mathfrak{q} = (\alpha)$ then satisfies $N(\alpha) = m$. Thus, each integer point (a, b) on $x^2 - dy^2 = m$ gives a generator of a principal ideal $\mathfrak{q}$ with $N\mathfrak{q} = m$. The number of such principal ideals is $\ll_\varepsilon m^\varepsilon$ for each $\varepsilon > 0$. (See, for example, Narkiewicz [12], p. 143.) For each such principal ideal, therefore, it remains to estimate the number of generators α of form (1.1) with $a, b \in \boldsymbol{Z}$ and $|a|, |b| \leqslant M$.

Case 1. For $d<0$, K is an imaginary quadratic field, and so there are at most six generators for each principal ideal since K has at most six units. Therefore, for $d<0$, there are $\ll_\varepsilon m^\varepsilon$ integer solutions (x, y) of $x^2-dy^2=m$.

Case 2. For $d=1$, we are counting the number of integer solutions to $m=x^2-y^2=(x-y)(x+y)$. Since this gives a factorization of m, the number of such solutions is $\leqslant \tau(m) \ll_\varepsilon m^\varepsilon$. So the bound of the lemma holds in this case.

Case 3. For $d>1$, K is a real quadratic field. For each such α in (1.1) we get

$$|\alpha| \leqslant M(1+\sqrt{d}) \quad \text{and} \quad |\bar{\alpha}| \leqslant M(1+\sqrt{d}).$$

Since $|\alpha\bar{\alpha}| = |N_{K/Q}\alpha| \geqslant 1$, it follows that

$$\frac{1}{M(1+\sqrt{d})} \leqslant |\alpha| \leqslant M(1+\sqrt{d})$$

or

$$|\log|\alpha|| \leqslant \log\{M(1+\sqrt{d})\}. \tag{1.2}$$

If α_0 is one generator of $\mathfrak{q}$ of the form (1.1) then each generator is of the form $\alpha_\nu = \eta^\nu \alpha_0$ ($\nu = 0, \pm 1, \pm 2, \ldots$), where η is the fundamental unit of K. (We note that if $d \equiv 1 \bmod 4$, then all of these $\eta^\nu\alpha_0$ may not be in $\boldsymbol{Z}[d]$.) It follows from (1.2) with $\alpha = \alpha_\nu$, that

$$|\nu\log\eta + \log|\alpha_0|| \leqslant \log\{M(1+\sqrt{d})\}$$

or

$$\left|\nu + \frac{\log|\alpha_0|}{\log\eta}\right| \leqslant \frac{\log\{M(1+\sqrt{d})\}}{\log\eta}.$$

This shows that the integer ν belongs to an interval of length $\ll \dfrac{\log(Md)}{\log\eta}$ and so the number of such α_ν is $\ll_\varepsilon \dfrac{(Md)^\varepsilon}{\log\eta}$.

Thus, to obtain the estimate in the lemma for $d>1$, it suffices to prove the following fact about $\log\eta$.

PROPOSITION 1. *If η is the fundamental unit of a real quadratic field K, then $\log\eta \geqslant c > 0$, where c is a constant independent of K.*

Proof. We show that η is not close to 1. A quadratic unit η satisfies an equation

$$\eta^2 - a\eta \pm 1 = 0$$

with $a \in \boldsymbol{Z}$. From this, we get

$$a = \eta \pm \bar{\eta}.$$

For η close to 1, this would give a close to 2 or 0. Since a is an integer, this would force $a=2$ or $a=0$. We would then have $\eta=1$, a contradiction. Thus, η is not close to 1. Hence, for any quadratic unit $\eta>1$, and, in particular for the fundamental unit, we have $\log\eta \geqslant c$, where c is a positive constant. This proves the proposition and hence the lemma.

Remark. It is easily seen that the estimate $(mdM)^\varepsilon$ in Lemma 1 also holds if x and y are $\ll M^l$ for some $l \geqslant 1$. In that case, the constant implied by $\ll$ depends upon l as well as ε.

LEMMA 2. *If $Q(x, y)$ is a quadratic polynomial with integer coefficients of absolute value $\leqslant N$ and nonzero discriminant, then there are $\ll_\varepsilon (MN)^\varepsilon$ integer solutions (x, y) of $Q(x, y)=0$ with $|x|, |y| \leqslant M$.*

Proof. Write

$$Q(x, y) = ax^2+bxy+cy^2+dx+ey+f.$$

It is easily seen that the condition $Q(x, y)=0$ can also be written as

$$x'^2 - Dy'^2 = m \tag{1.3}$$

where $D = b^2-4ac$, $x' = -Dy+2ae-bd$, $y' = 2ax+by+d$ and $m = -D(d^2-4af)+(2ae-bd)^2$. Each solution (x, y) of $Q(x, y)=0$, with $|x|, |y| \leqslant M$, gives a solution (x', y') of (1.3) with $|x'|, |y'| \ll MN^2$. By Lemma 1 and the preceding remark, the number of such integer solutions of (1.3) is $\ll_\varepsilon (MN^2m)^\varepsilon \ll_\varepsilon (MN)^\varepsilon$.

We also remark here that the estimate $(MN)^\varepsilon$ in this lemma holds if x and y are $\ll M^l$ for some $l \geqslant 1$ and if the coefficients are $\ll N^k$ for some $k \geqslant 1$.

2. Cubics with affect. We now apply the results of Section 1 to the following problem considered by van der Waerden. Denote by $R_n(N)$ (respectively $E_n(N)$) the number of monic nth degree polynomials

$$f(x) = x^n + a_1x^{n-1} + \ldots + a_n$$

with integer coefficients bounded in absolute value by N, for $N \geqslant 1$, which are reducible (respectively, which are with affect). Clearly $R_n(N) \leqslant E_n(N)$. Van der Waerden [17], and later Specht [14], showed that

$$\begin{aligned} R_n(N) &\ll N^{n-1} && (n \geqslant 3) \\ &\ll N\log N && (n=2). \end{aligned} \tag{2.1}$$

For $E_n(N)$, van der Waerden [17] gave the estimate

$$E_n(N) \ll N^{n-\frac{c}{\log\log N}} \quad \text{with } c = \frac{1}{6(n-2)},$$

and he suggested, based on a partly heuristic argument for $n=3$, that

$$E_n(N) \ll N^{n-1} \quad (n \geqslant 3).$$

Knobloch [8], [9] improved van der Waerden's estimate for $E_n(N)$ to

$$E_n(N) \ll N^{n-c} \quad \text{with } c = \frac{1}{18n(n!)^3}.$$

Using the large sieve in several variables, Gallagher [3] obtained

$$E_n(N) \ll N^{n-\frac{1}{2}}\log N.$$

In this section we show that

$$E_3(N) \ll_\varepsilon N^{2+\varepsilon}$$

for each $\varepsilon > 0$, and also obtain nontrivial upper bounds for the number of certain fourth and fifth degree polynomials whose Galois group is a subgroup of A_n, the alternating group on n letters.

THEOREM 1. *Let $I(N)$ be the number of irreducible polynomials $f(x) = ax^3+bx^2+cx+d$ $(a \neq 0)$ with integer coefficients bounded in absolute value by N, for $N \geqslant 1$, with affect. Then, for each $\varepsilon > 0$, we have*

$$I(N) \ll_\varepsilon N^{3+\varepsilon}.$$

Proof. The discriminant D_f of $f(x)$ equals

$$D_f = b^2c^2 - 4ac^3 - 4b^3d - 27a^2d^2 + 18abcd.$$

Since $f(x)$ is irreducible, G_f is transitive and therefore equals A_3, the alternating group on three letters. Hence (Jacobson [7], p. 91) D_f is the square of a rational integer. This condition gives the equation

$$b^2c^2 - 4ac^3 - 4b^3d - 27a^2d^2 + 18abcd = z^2 \tag{2.2}$$

for some $z \in \mathbf{Z}$.

If one thinks of a, b, c, d, and z as variables, then the number of integer points (a, b, c, d, z) satisfying (2.2) is $\geqslant 2I(N)$. Therefore, it suffices to obtain an upper bound for the number of integer solutions of (2.2).

Now, (2.2) is a quadratic equation in d and z:

$$27a^2d^2 + (4b^3 - 18abc)d + 4ac^3 - b^2c^2 + z^2 = 0. \tag{2.3}$$

If we fix a, b, and c, then, by Lemma 2, the number of integer points (d, z) on (2.3) is $\ll_\varepsilon N_1^\varepsilon$ for each $\varepsilon > 0$. Therefore, for $\varepsilon > 0$, we get

$$I(N) \ll_\varepsilon \sum_{|a|,|b|,|c| \leqslant N} N^\varepsilon \ll_\varepsilon N^\varepsilon.$$

THEOREM 2. *For each $\varepsilon > 0$, we have*

$$E_3(N) \ll_\varepsilon N^{2+\varepsilon}.$$

Proof. We may assume that $f(x)$ is irreducible since $R_3(N) \ll N^2$ by (2.1). Therefore, $G_f = A_3$ and $D_f = z^2$ for some $z \in \mathbf{Z}$. So letting $a = 1$ in the previous proof, we get the result.

We note that the exponent in Theorem 2 is nearly best possible because if $a_3 = 0$, then $f(x)$ is reducible. Hence a lower bound for $E_3(N)$ is N^2.

This approach of using the discriminant and counting integer points on ellipses does not seem to work to estimate $E_n(N)$ if $n > 3$. Nevertheless, it does give nontrivial estimates for the number of certain fourth and fifth degree polynomials f with G_f a subgroup of the alternating group.

THEOREM 3. *The number of polynomials $f(x) = ax^4+bx^2+cx+d$ with a, b, c, $d \in \mathbf{Z}$, $a \neq 0$, $|a|$, $|b|$, $|c|$, $|d| \leqslant N$, and $G_f \subseteq A_4$ is $\ll_\varepsilon N^{3+\varepsilon}$ for each $\varepsilon > 0$.*

Proof. Using the formula for the discriminant of f (van der Waerden [18], § 58) and the fact that it is the square of an integer, we get

$$27a^2(c^2)^2 + pc^2 + q + z^2 = 0$$

where $p = 4ab^3 - 144a^2bd$ and $q = 128a^2b^2d^2 - 16ac^4d - 256a^3d^3$ and $z \in \mathbf{Z}$. This equation is a quadratic in c^2 and z. As in the cubic case, we count the number of integer pairs (c, z) on this ellipse, for fixed a, b, and d. As before, the number of such pairs is $\ll_\varepsilon N^\varepsilon$ for each $\varepsilon > 0$. Then, we sum this number over a, b, and d to obtain the stated upper bound.

THEOREM 4. *The number of polynomials $f(x) = x^4+bx^2+cx+d$ with b, c, $d \in \mathbf{Z}$, $|b|$, $|c|$, $|d| \leqslant N$, and $G_f \subseteq A_4$ is $\ll_\varepsilon N^{2+\varepsilon}$ for each $\varepsilon > 0$.*

Proof. Put $a = 1$ in the proof of Theorem 3.

THEOREM 5. *The number of polynomials $f(x) = x^5+bx^3+cx+d$ with b, c, $d \in \mathbf{Z}$, $|b|$, $|c|$, $|d| \leqslant N$ and $G_f \subseteq A_5$ is $\ll_\varepsilon N^{2+\varepsilon}$ for each $\varepsilon > 0$.*

Proof. The discriminant of this quintic, which can be found in Cohn [2], is a quadratic in d^2. Setting it equal to the square of an integer, we have

$$5^5(d^2)^2 + pd^2 + q = z^2$$

for some $z \in \mathbf{Z}$, where $p = 108b^5 + 2000bc^2 - 900b^3c$ and $q = 16b^4c^3 - 128b^2c^4 + 256c^5$. As in the cubic and quartic cases, we count the number of integer pairs (d, z) with $|d| \leqslant N$, on this hyperbola, for fixed b and c. It follows from Lemma 2 that the number of such pairs is $\ll_\varepsilon N^\varepsilon$ for each $\varepsilon > 0$. Summing over b and c, we obtain the stated upper bound.

3. Trinomials. In this section we obtain a nontrivial upper bound for the number $J_{k,n}(M)$ of trinomials $f(x) = ax^n + bx^k + c$ with $n > k > 0$ and $a \neq 0$ which satisfy the following conditions:

(a) $a, b, c \in \mathbf{Z}$ and $|a|, |b|, |c| \leqslant M$, for $M \geqslant 1$.

(b) The Galois group of the splitting field of $f(x)$, considered as a permutation group on the roots of $f(x)$, is a subgroup of the alternating group on n letters.

We show that $J_{k,n}(M) \ll_{\varepsilon,n} M^{2+\varepsilon}$ for each $\varepsilon > 0$.

The formula for the discriminant of $f(x)$ was given previously by Heading [6], Goodstein [4], and Swan [15] in the monic case, and by

Artin ([1], p. 130), Samuel ([13], § 2.7), and Masser [11] for the case $a = 1$ and $k = 1$. In the general case, the formula takes the following form.

Trinomial discriminant formula. Let $f(x) = ax^n + bx^k + c$, $a \neq 0$, $n > k > 0$. Then

$$D_f = (-1)^{\frac{1}{2}n(n-1)} a^{n-k-1} c^{k-1} \{n^N a^K c^{N-K} + (-1)^{N-1}(n-k)^{N-K} k^K b^N\}^d \tag{3.1}$$

where $d = (n, k)$, $n = Nd$, and $k = Kd$.

Using this formula, we obtain the following result.

THEOREM 6. *For each* $\varepsilon > 0$,

$$J_{k,n}(M) \ll_\varepsilon M^{2+\varepsilon}.$$

Proof. We may assume that neither a, b, nor c equals zero, since the number of such trinomials with either a, b, or $c = 0$ is $\ll M^2$.

From (3.1),

$$D_f = \pm a^{n-k-1} c^{k-1} E^d$$

where $\pm = (-1)^{\frac{1}{2}n(n-1)}$, $d = (n, k)$, $N = n/d$, $K = k/d$, and

$$E = n^N a^K c^{N-K} + (-1)^{N-1}(n-k)^{N-K} k^K b^N. \tag{3.2}$$

Case 1: d odd. If d is odd, then for some $F \in \mathbf{Z}[a, b, c]$,

$$F^{-2} D_f = \pm a^{N-K-1} c^{K-1} E. \tag{3.3}$$

Under the present hypothesis that $G_f \subseteq A_n$, it follows from Galois theory (Jacobson [7], p. 91) that D_f is the square of a rational integer. Hence, the same holds for the right-hand side of (3.3).

(a) n even, k odd. In this case N is even and K is odd. Therefore, it follows from (3.3) that $\pm E = z^2$ for some $z \in \mathbf{Z}$. Explicitly, from (3.2), this becomes

$$\pm n^N a^K c^{N-K} = z^2 \pm (n-k)^{N-K} k^K (b^{N/2})^2,$$

where $\pm = (-1)^{N/2}$. Now for fixed a and c, we see that

$$x = z \quad \text{and} \quad y = b^{N/2}$$

is an integer solution of

$$m = x^2 - dy^2$$

where $m = \pm n^N a^K c^{N-K}$ and $d = \mp (n-k)^{N-K} k^K$.

The number of such integer solutions is $\ll_\varepsilon M^\varepsilon$ by Lemma 1. It therefore follows that

$$J_{k,n}(M) \ll_{\varepsilon,n} \sum_{|a|,|c| \leqslant M} M^\varepsilon \ll_{\varepsilon,n} M^{2+\varepsilon}.$$

(b) n odd, k even. Here N is odd and K is even. As in (a), it follows from (3.2) that $\pm cE = z^2$ for some $z \in \mathbf{Z}$, or, explicitly,

$$\pm (n-k)^{N-K} k^K b^N c = z^2 \mp n^N c^{N-K+1} (a^{K/2})^2$$

where $\pm = (-1)^{(N-1)/2}$. Now by fixing b and c we see that

$$x = z \quad \text{and} \quad y = a^{K/2}$$

is an integer solution of

$$m = x^2 - dy^2$$

where $m = \pm (n-k)^{N-K} k^K b^N c$ and $d = \pm n^N c^{N-K+1}$.

The rest of the proof is identical to that for (a) except that we sum over b and c.

(c) n odd, k odd. It follows easily from (3.1) that the discriminants of $f(x) = ax^n + bx^k + c$ and $g(x) = cx^n + bx^{n-k} + a$ are equal. We also note that if k is odd, then $n-k$ is even, if n is odd. Therefore (c) follows from (b) by interchanging a with c and k with $(n-k)$ (i.e., by applying (b) to $g(x)$).

Case 2: d even. If d is even, then for some $F \in \mathbf{Z}[a, b, c]$,

$$F^{-2} D_f = \pm ac$$

and so

$$(a+c)^2 - (a-c)^2 = \pm 4z^2$$

for some $z \in \mathbf{Z}$. On fixing $a + c$ there are $\ll_\varepsilon M^\varepsilon$ values of $a - c$, by Lemma 1. Hence there are $\ll_\varepsilon M^{1+\varepsilon}$ values of (a, c) and therefore $\ll_\varepsilon M^{2+\varepsilon}$ values of (a, b, c), as required.

Acknowledgment. The author would like to thank Professor Patrick X. Gallagher for his encouragement and generous help during this research. Thanks is also given to Dr. Kenneth S. Williams for referring the author to the articles by Masser, Heading, and Goodstein on the trinomial discriminant formula, which was arrived at independently by the author.

References

[1] E. Artin, *Theory of algebraic numbers*, Göttingen 1959.

[2] H. Cohn, *A numerical study of quintics of small discriminant*, Communications on Pure and Applied Mathematics, VIII (1955), pp. 377–386.

[3] P. X. Gallagher, *The large sieve and probabilistic Galois Theory*, Proceedings of Symposia in Pure Mathematics XXIII (1969, A. M. S.).

[4] R. L. Goodstein, *The discriminant of a certain polynomial*, Math. Gaz. 53 (1969), pp. 60–61.

[5] G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*, Oxford University Press, London 1965.
[6] J. Heading, *The discriminant of an equation of n-th degree*, Math. Gaz. 51 (1967), pp. 324–326.
[7] N. Jacobson, *Lectures in abstract algebra*, Vol, 3. *Theory of fields and Galois theory*, Van Nostrand, Princeton 1964.
[8] H. W. Knobloch, *Zum Hilbertschen Irreduzibilitätssatz*, Abh. Math. Sem. Univ. Hamburg 19 (1955), pp. 176–190.
[9] — *Die Seltenheit der reduziblen Polynome*, Jber. Deutsch. Math. Verein. 59 (1956), Abt. 1, pp. 12–19.
[10] S. Lang, *Introduction to Diophantine approximations*, Addison-Wesley, 1966.
[11] D. W. Masser, *The discriminants of special equations*, Math. Gaz. 50 (1966), pp. 158–160.
[12] W. Narkiewicz, *Elementary and analytic theory of algebraic numbers*, Polish Scientific Publishers, Warszawa 1973.
[13] P. Samuel, *Algebraic theory of numbers*, Hermann, Paris 1970.
[14] W. Specht, *Zur Zahlentheorie der Polynome*, S. B. Math. Nat. Kl. Bayer. Akad. Wiss., (1951), pp. 139–146.
[15] R. Swan, *Factorization of polynomials over finite fields*, Pacific J. Math. 12 (1962), pp. 1099–1106.
[16] B. L. van der Waerden, *Die Seltenheit der Gleichungen mit Affekt*, Math. Ann. 109 (1934), pp. 13–16.
[17] — *Die Seltenheit der reduziblen Gleichungen und die Gleichungen mit Affekt*, Monatsh. Math. 43 (1936), pp. 137–147.
[18] — *Modern algebra*, Vol. I, Ungar, New York 1953.

DEPARTMENT OF MATHEMATICS
MANHATTANVILLE COLLEGE
Purchase, New York, U.S.A.

Received on 21. 6. 1976
and in revised form on 7. 1. 1977 (856)

ACTA ARITHMETICA
XXXV (1979)

Ω-estimates in lattice point theory

by

BOHUSLAV DIVIŠ

Let $Q(u) = Q(u_1, u_2, \ldots, u_r) = \sum_{i,l=1}^{r} a_{il} u_i u_l$ be a positive definite quadratic form in $r \geqslant 2$ variables with real symmetric coefficient matrix of determinant D. Let $b = (b_1, b_2, \ldots, b_r)$ be a system of real numbers satisfying $0 \leqslant b_l < 1$ $(l = 1, 2, \ldots, r)$. For $x > 0$, let us denote by $A_Q(b; x)$ the number of lattice points $m = (m_1, m_2, \ldots, m_r)$ with integral coordinates m_l $(l = 1, 2, \ldots, r)$ satisfying the inequality $Q(m+b) \leqslant x$, that is

$$A_Q(b; x) = \sum_{Q(m+b) \leqslant x} 1.$$

Geometrically, the ellipsoid $Q(m+b) \leqslant x$ has center at the point $-b$ Obviously, $A_Q(b; x)$ is asymptotically equal to

$$V_Q(b; x) = V_Q(x) = \frac{\pi^{r/2} x^{r/2}}{\sqrt{D}\,\Gamma(\frac{1}{2}r+1)},$$

the volume of the ellipsoid $Q(u+b) \leqslant x$, which is clearly independent of b. Let us put

$$P_Q(b; x) = A_Q(b; x) - V_Q(x).$$

Since the form Q and the center $-b$ will be considered fixed, we shall simply write $A(x)$, $V(x)$ and $P(x)$ instead of $A_Q(b; x)$, $V_Q(b; x)$ and $P_Q(b; x)$. We shall study the function $P(x)$, and more generally

$$P_\varrho(x) = \frac{1}{\Gamma(\varrho)} \int_0^x P(y)(x-y)^{\varrho-1} dy \quad \text{for} \quad \varrho > 0, \quad P_0(x) = P(x).$$

The functions $A_\varrho(x)$ and $V_\varrho(x)$ are defined analogously. Finally, let us put

$$M_\varrho(x) = \int_0^x P_\varrho^2(y)\, dy \quad \text{for} \quad \varrho \geqslant 0, \quad M(x) = M_0(x)$$