

ON THE GALOIS GROUPS OF CUBICS AND TRINOMIALS

BY PHYLLIS LEFTON¹

Communicated by Hyman Bass, May 9, 1976

A polynomial

$$(1) \quad f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_n \quad (a_i \in \mathbf{Z})$$

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. The purpose of this note is to give an improved upper bound for the number of monic polynomials of degree three with affect. More generally, we also give an upper bound for the number of trinomials f of degree n for which G_f is a subgroup of the alternating group A_n on n letters. Details will appear elsewhere [6].

Previous upper bounds for the number $E_n(N)$ of monic polynomials of degree n with integer coefficients bounded in absolute value by N , which are with affect, have been given by van der Waerden [10], Knobloch [5], and Gallagher [2]. The best estimate obtained so far for the general case is $E_n(N) \ll N^{n-1/2} \log N$ given by Gallagher [2]. Van der Waerden [10] has conjectured that $E_n(N) \ll N^{n-1}$, a bound which does hold for the reducible polynomials if $n \geq 3$ [10]. Our results are as follows.

THEOREM 1. For each $\epsilon > 0$, $E_3(N) \ll_{\epsilon} N^{2+\epsilon}$.

THEOREM 2. Let $J_{k,n}(N)$ denote the number of trinomials

$$(2) \quad f(x) = ax^n + bx^k + c$$

with $a, b, c \in \mathbf{Z}$ and $|a|, |b|, |c| \leq N$, for $N \geq 1$, for which G_f is a subgroup of A_n . Then for each $\epsilon > 0$, $J_{k,n}(N) \ll_{\epsilon,n} N^{2+\epsilon}$.

The proofs of these two theorems are similar. It is well known that the discriminant D_f of (1) has the property that $D_f \in \mathbf{Z}[a_0, a_1, \dots, a_n]$. Moreover, if $G_f \subseteq A_n$, then D_f is the square of a rational integer, i.e.

$$(3) \quad D_f = z^2 \quad (z \in \mathbf{Z}).$$

AMS (MOS) subject classifications (1970). Primary 12A20, 12A55; Secondary 10B05, 12A25.

Key words and phrases. Galois group, symmetric group, alternating group, with affect, cubic, trinomial, discriminant, quadratic field, norm, ideal.

¹These results are taken from the author's Columbia University Ph.D. thesis. She was supported by a Columbia University Faculty Fellowship and an NSF Graduate Fellowship.

Copyright © 1976, American Mathematical Society

In both theorems then, we think of z and the coefficients of f as variables and count the number of possible integer solutions of (3). We do this by means of the following

LEMMA. For a fixed integer $d \neq 0$, there are $\ll_{\epsilon, d} (Mm)^\epsilon$ integer solutions (x, y) of

$$(4) \quad x^2 - dy^2 = m$$

with $|x|, |y| \ll M$.

This lemma is useful because after some computational manipulation, equations (3), for both the cubic and the trinomial, can be put into form (4).

We prove this lemma from an estimate for the number of ideal solutions to norm equations in number fields. We show that if K is a number field of degree n , and $m \in \mathbb{Z}$, then the number $R_K(m)$ of ideals of K with norm m is given by

$$(5) \quad R_K(m) \ll_\epsilon m^\epsilon,$$

for each $\epsilon > 0$. If $d \neq 1$, then (4) is a norm form in the quadratic field $Q(\sqrt{d})$. By applying (5) and taking into account the units in real quadratic fields, we obtain the estimate in the lemma.

In the course of the proof of Theorem 2, we also give a new proof of the following formula.

TRINOMIAL DISCRIMINANT FORMULA. Let $f(x) = ax^n + bx^k + c$, $a \neq 0$, $n > k > 0$. Then the discriminant D_f of $f(x)$ is given by

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

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

This formula was given previously by Heading [4] and Goodstein [3] in the monic case, and by Artin [1], Samuel [8], and Masser [7] for the case $a = 1$ and $k = 1$. Details of our proof will appear in [6].

ACKNOWLEDGEMENT. The author wishes to thank Professor P. X. Gallagher for his assistance during this research.

REFERENCES

1. E. Artin, *Theory of algebraic numbers*, Lecture notes (Math. Inst., 1956/57), Striker, Göttingen, 1959. MR 24 #A1884.
2. P. X. Gallagher, *The large sieve and probabilistic Galois theory*, Analytic Number Theory (Proc. Sympos. Pure Math., vol. 24), Amer. Math. Soc., Providence, R. I., 1973, pp. 91–101.
3. R. L. Goodstein, *The discriminant of a certain polynomial*, Math. Gaz. 53 (1969), 60–61.
4. J. Heading, *The discriminant of an equation of n th degree*, Math. Gaz. 51 (1967), 324–326.
5. H. W. Knobloch, *Zum Hilbertschen Irreduzibilitätssatz*, Abh. Math. Sem. Univ. Hamburg 19 (1955), 176–190. MR 16, 798.
6. P. Lefton, *On the Galois groups of cubics and trinomials*, Acta Arith. (to appear).

7. D. W. Masser, *The discriminants of special equations*, Math. Gaz. **50** (1966), 158–160.
8. P. Samuel, *Algebraic theory of numbers*, Hermann, Paris, 1967; English transl., Houghton, Mifflin, Boston, 1970. MR **35** #6643; **42** #177.
9. B. L. van der Waerden, *Die Seltenheit der Gleichungen mit Affekt*, Math. Ann. **109** (1934), 13–16.
10. ———, *Die Seltenheit der reduziblen Gleichungen und der Gleichungen mit Affekt*, Monatsh. Math. **43** (1936), 137–147.

DEPARTMENT OF MATHEMATICS, BELFER GRADUATE SCHOOL OF SCIENCE,
YESHIVA UNIVERSITY, NEW YORK, NEW YORK 10033