ILLINOIS JOURNAL OF MATHEMATICS
Volume 23, Number 1, March 1979

# THE DISTRIBUTION OF THE GALOIS GROUPS OF INTEGRAL POLYNOMIALS

BY
S. D. COHEN

## 1. Introduction and notation

Using the large sieve in an argument of van der Waerden [18], P. X. Gallagher [12] has shown that the number $E_n(N)$ of polynomials

$$F(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0$$

with integer coefficients and height $(= \max(|a_0|, \ldots, |a_{n-1}|)) \leq N$ whose Galois group over $\mathbf{Q}$ is less than the symmetric group is $\ll N^{n-1/2} \log N$, where the implied constant depends only on $n$. Indeed, a refinement of the basic argument yields a slight improvement to $E_n(N) \ll N^{n-1/2} \log^{1-\gamma} N$, where $0 < \gamma \sim 1/2\pi n$ as $n \to \infty$. For $n = 3$ see [20].

In this paper we suppose that some of the coefficients $a_i$ are fixed and that only members of a given set of $s(\geq 1)$ coefficients are allowed to vary. Provided only that $s \geq 2$ and with the obvious exceptions mentioned below we show that the number of such polynomials of height $\leq N$ which have Galois group less than the symmetric group is $\ll N^{s-1/2} \log N$. The exceptional cases occur when *all* the polynomials concerned are divisible by $X$ or belong to $\mathbf{Z}[X^r]$ for some $r > 1$. However even in these cases or in the case $s = 1$ we prove that all but $\ll N^{s-1/2} \log N$ such polynomials have the same Galois group (which we describe explicitly when $s \geq 2$). We draw particular attention to the fact that, if $s \geq 2$, then the above estimates are uniform in $F$ of given degree, i.e. do not depend on the fixed $a_i$. If $s = 1$, the implied constant depends on $F$.

By way of comparison, it follows from results stated by Fried [11] in the case $s = 1$ that the number of merely reducible polynomials $F$ of height $\leq N$ with one varying coefficient is $\ll N^{1/2}$. See also Dörge [7] for further estimates, generally inferior, but not as dependent on the fixed coefficients.

In the sequel we shall make some modifications to the situation as described. In particular, our method requires us to examine Galois groups over a normal extension of $\mathbf{Q}$ rather than $\mathbf{Q}$ itself. Accordingly, we shall assume that the coefficients are integers in an algebraic number field $k$ and consider Galois groups over $K$, where $K/k$ is a finite normal extension. Next, let us say that any polynomial $f(X)$ is *primitive* if $f(X) \neq g(X^r)$ for any polynomial $g$ and any $r > 1$. Then instead of considering an arbitrary

Received August 30, 1977.