ON A CONJECTURE OF SCHUR

Michael Fried

The main purpose of this paper is to prove a conjecture due to I. Schur [11, p. 125]. Let K be a number field, finite-dimensional over the rational field $\mathbb{Q}$. If $f(x)$ denotes an element of the polynomial domain $K[x]$, then we may reduce the polynomial, modulo any prime $\mathfrak{p}$ (of the ring of integers of K) that does not appear in the denominators of the coefficients of $f(x)$. Let $V_{\mathfrak{p}}(f)$ denote the values assumed by $f(x)$, modulo $\mathfrak{p}$. An inspection of $V_{\mathfrak{p}}(f)$ for only a few primes cannot be expected to contribute immensely to our knowledge of $f(x)$. However, Schur conjectured that *if* $V_{\mathfrak{p}}(f)$ *consists of all cosets modulo* $\mathfrak{p}$, *for infinitely many primes* $\mathfrak{p}$ *of* K, *then* $f(x)$ *is a composition of polynomials of two special types:*

(i) $ax^n + b$ (*cyclic polynomials*),

(ii) $T_n(x) = 2^{-n-1}\{(x + (x^2+4)^{1/2})^n + (x - (x^2+4)^{1/2})^n\}$ (*Chebychev polynomials*).

In the lemma at the end of Section 1, we shall show that if $f(x) \in \mathbb{Q}[x]$ is a composition of polynomials of type (i) and (ii) such that the degree of f is relatively prime to 6, then f is one-to-one (mod p) for infinitely many rational primes p. The condition (deg f, 6) = 1 will also be shown to be necessary. The elegant part of the argument is due to H. Davenport.

That Schur's conjecture is true is our Theorem 2, which follows from our Theorem 1. Theorem 1 is formulated over a fixed field of any characteristic. At the beginning of Section 2, we make certain calculations that have as one consequence our Theorem 3. Let $\mathfrak{k}$ be a finite field, and let $f(x) \in \mathfrak{k}[x]$ be a tame polynomial (see Definition 2). The gist of Theorem 3 is that the polynomial

$$\phi(x, y) = \frac{f(x) - f(y)}{x - y}$$

has an absolutely irreducible factor (as a polynomial in $\mathfrak{k}[x, y]$) in extremely general circumstances, unless $f(x)$ is a composition of polynomials of type (i) and (ii). If the degree of f is small in comparison with the order of $\mathfrak{k}$, then the condition that $\phi(x, y)$ have no absolutely irreducible factors is equivalent to f being one-to-one. This can easily be seen from the proof of Theorem 2, in conjunction with a theorem of MacCluer (see the remarks following Theorem 3).

Actually, Schur himself made many contributions to the problem. In particular, by methods quite different from ours he was able to prove the conjecture for polynomials of prime degree, in the case where $K = \mathbb{Q}$. However, our Lemma 9, which will be used in subsequent work, strengthens even this result.

An analogue of the Schur conjecture is proved in [6]. Let $g_1(x), \cdots, g_\ell(x)$ be in $K[x]$, and assume that $\bigcup_1^\ell V_{\mathfrak{p}}(g_i)$ fills out all cosets modulo $\mathfrak{p}$, for all but a finite

Received October 3, 1968.

This research was supported in part by the Army Research Office - Durham, grant ARO-D-21-124-G892.S1.