ACTA ARITHMETICA
XVII (1970)

The distribution of polynomials over finite fields

by

STEPHEN D. COHEN (Glasgow)

1. Introduction and notation. Let $k = \mathrm{GF}(q)$ be the finite field of order $q = p^b$, where p is a prime and b a positive integer. Let $f(x), g(x)$ be given polynomials in $k[x]$. The purpose of this paper is to give a unified treatment of several problems concerned with the distribution as a varies in k of polynomials of the form $f(x) - ag(x)$ whose prime factors have prescribed degrees and the extent to which this distribution depends on f and g. As particular cases of our theorems, results contained in [1], [8], [11] and [18] are completed and extended and a conjecture of Chowla [4] is established. The results are described in detail in § 2 after some necessary notation has been given.

In contrast to much of the previous work cited which uses the terminology of algebraic geometry, the approach adopted here is arithmetical, employing the ideas of algebraic number theory. Most earlier results have been proved using the deep theorem of Weil [15] concerning the Riemann hypothesis for function fields over a finite field in some form or another. Here (at one point only) we make an appeal to an arithmetical form of this theorem.

The following notation is adopted throughout. Let G be the Galois group of some polynomial $Q(y)$ $(= Q(y, t))$ of degree n over $k(t)$, where t is an indeterminate, with splitting field K. Regard G as a subgroup of S_n, the nth symmetric group (i.e. as a group of permutations of the roots of $Q(y) = 0$). Let G_λ be the set of elements of G having the same cycle pattern λ. For any $\sigma \in G$, let K_σ denote the subfield of K fixed under σ.

Further, let k' $(= \mathrm{GF}(q^f)$, for some $f)$, be the largest algebraic extension of k in K. Let $G^* = \{\sigma \in G, K_\sigma \cap k' = k\}$ and put $G^*_\lambda = G^* \cap G_\lambda$ for any cycle pattern λ. Note that $\sigma \in G^* \Leftrightarrow K_\sigma \cap k'(t) = k(t)$. Also, if $\sigma \in G$, let σ' denote the restriction of σ to k'.

If a non-zero polynomial $a(y)$ in $k[y]$ of degree n factorises into a product of a_d prime factors of degree d $(d = 1, \ldots, n)$, we shall say that $a(y)$ has cycle pattern $1^{a_1}, \ldots, n^{a_n}$ and identify this cycle pattern with the corresponding one of elements in S_n.

Finally, throughout this paper, all constants implied by O-terms will depend only on $n = \deg Q(y)$.

2. Statement of main results. Let $f(x), g(x) \in k[x]$. In most of what follows we could allow f, g to be almost completely arbitrary. Theorem 1, for example, remains valid as stated below under only the trivial restriction on f, g that they are both non-zero and not both constant. However, in order to avoid obscuring the discussion with irrelevant technical details and without real loss of generality, we shall assume throughout the remainder of this paper that f, g satisfy

$$\text{(2.1)} \qquad \begin{cases} (f,g) = 1; \quad n = \deg f > \deg g \geqslant 0; \quad f, g \text{ monic}; \\ f(x)/g(x) \neq f_1(x^p)/g_1(x^p) \quad \text{for any } f_1(x),\ g_1(x) \text{ in } k[x], \end{cases}$$

where (f, g) is the greatest common factor of f and g.

Indeed, we shall at all times be considering only monic polynomials.

In all our theorems, we shall take the $Q(y)$ of § 1 to be $f(y) - tg(y)$. The principal one is the following:

THEOREM 1. *Suppose that $f(x)$, $g(x)$ in $k[x]$ satisfy* (2.1) *and that $f(y) - tg(y)$ has Galois group G over $k(t)$. Then $\pi_\lambda(f, g, q)$, the number of polynomials of the form $f(x) - ag(x)$ ($a \in k$) with cycle pattern λ, satisfies*

$$\text{(2.2)} \qquad \pi_\lambda(f, g, q) = \frac{|G_\lambda^*|}{|G^*|} q + O(q^{1/2}),$$

where the implied constant depends only on n.

Note. It will be shown in § 3 (Lemma 1) that $|G^*| \neq 0$.

Now we may say that, with the notation of Theorem 1, "in general" $G^* (= G) = S_n$ (compare [1] and [17]). Moreover, if $\pi(d)$ is the total number of irreducible polynomials of degree d in $k[x]$ and $\lambda = 1^{a_1}, \ldots, n^{a_n}$, then it is easy to show by induction on n that the total number of square-free polynomials in $k[x]$ with cycle pattern λ is

$$\text{(2.3)} \qquad \prod_{d=1}^{n} \binom{\pi(d)}{a_d} = \frac{s_\lambda(n)}{n!} q^n + O(q^{n-1}),$$

(where $s_\lambda(n)$ is Cauchy's expression for the number of elements of cycle pattern λ in S_n) since $\pi(d) = d^{-1} q^d + O(q^{d/2})$. Since the total number of polynomials of degree n which are not square-free is q^{n-1} ([2]), it follows from Theorem 1 and (2.3) that, in general, as $q \to \infty$, $\pi_\lambda(f, g, q)/q$ tends to the proportion of polynomials of degree n in $k[x]$ with cycle pattern λ.

In describing the remaining results, we assume the notation of Theorem 1. We also define $G_i = \{\sigma \in G, \sigma \text{ contains an } i\text{-cycle}, i = 1, \ldots, n\}$, and put $G_i^* = G_i \cap G^*$. Thus, if $G^* = S_n$, then it is well-known that

$|G_1^*|/|G^*| = \mu_n$, where

$$\text{(2.4)} \qquad \mu_n = 1 - \frac{1}{2!} + \frac{1}{3!} - \ldots + (-1)^{n-1} \frac{1}{n!}$$

and

$$|G_n^*|/|G^*| = n^{-1}.$$

The next theorem is an immediate corollary of Theorem 1. In particular, when $g(x) = 1$ it becomes a more precise form of a theorem of Birch and Swinnerton-Dyer [1]. In their statement, (2.6) below was established but otherwise the coefficient of q in (2.5) was only proved to depend solely on the relevant Galois groups.

THEOREM 2. *In the notation and under the assumptions of Theorem* 1, *$r(f, g)$, the number of distinct values of the rational function $f(x)/g(x)$ as x varies in k with $g(x) \neq 0$, satisfies*

$$\text{(2.5)} \qquad r(f, g) = \frac{|G_1^*|}{|G^*|} q + O(q^{1/2}).$$

Hence, "in general",

$$\text{(2.6)} \qquad r(f, g) = \mu_n q + O(q^{1/2}),$$

where μ_n is defined by (2.4).

In [1], it was also shown that if $g(x) = 1, f(x) = x^n + ax$ ($n \geqslant 2$, $a \neq 0$), then $G^* = S_n$ provided $p \nmid 2n(n-1)$. Hence a conjecture of Chowla [4] is established by the case $f(x) = x^n + x, g(x) = 1$, $q = p$, $m = 1$ of the following theorem which is concerned with the distribution of irreducible polynomials.

THEOREM 3. *Let $f(x)$, $g(x)$ in $k[x]$ satisfy* (2.1) *and let G^m be the Galois group of $f - tg$ over $\mathrm{GF}(q^m, t)$. Then $\pi(f, g, q, m)$, the number of irreducible polynomials of the form $g^m P(f/g)$, where P is any polynomial of degree m in $k[x]$, satisfies*

$$\pi(f, g, q, m) = \frac{|G_n^{m*}|}{m|G^{m*}|} q^m + O(q^{m/2}).$$

Hence, "in general" (when $G^{m*} = S_n$),

$$\pi(f, g, q, m) = \frac{1}{mn} q^m + O(q^{m/2}).$$

Theorem 3 follows easily from Theorem 1 and the fact, proved in [6], § 2, that

$$\pi(f, g, q^m, 1) = \sum_{\substack{rs = m \\ (n,s) = 1}} r\pi(f, g, q, r) = m\pi(f, g, q, m) + O(mq^{m/2}),$$

since clearly $\pi(f, g, q, r) \leqslant q^r$.

We remark that if K has genus 0, i.e. if $K = k'(x)$, where $f(x) - tg(x) = 0$, then in Theorems 1 and 2 and when $m = 1$ in Theorem 3, the $O(q^{1/2})$ terms may be replaced by $O(1)$. Indeed, in these circumstances, in his Glasgow thesis [5], the author has explicitly evaluated $\pi(f, g, q, m)$ for most of the simplest f, g possible. Some of these results have been published in [6].

Next we consider the connection between permutation functions and exceptional functions f/g, previously defined for $g(x) = 1$. A permutation polynomial $f(x)$ in $k[x]$ is one whose value set in k is precisely k, i.e. one for which $r(f, 1) = q$. More generally, we shall say that f/g is a *permutation function* over k if $r(f, g) = q$. This means that $g(x)$ is irreducible in $k[x]$. An exceptional polynomial $f(x)$ in $k[x]$ is one for which $\dfrac{f(Y)-f(X)}{Y-X}$ has no absolutely irreducible factors in $k[X, Y]$. More generally, we shall say that f/g is *exceptional* over k if

$$G_{f/g}(X, Y) = \frac{g(X)f(Y)-f(X)g(Y)}{Y-X} \tag{2.7}$$

has no absolutely irreducible factors in $k[X, Y]$.

Our methods are applied to yield natural proofs of Theorems 4 and 5 below. As a special case of Theorem 4, we could suppose that f/g is an injection mapping on its domain of definition with $s(n) = n$ and $\delta = 0$ in (2.8) below, and, in particular (when $g(x)$ is irreducible), that f/g is a permutation function so that $s(n) = 0$. In this last case, the result (with $g(x) = 1$) is due to Hayes [8]. When $g(x) = 1$, $q = p$ and $\delta = 0$ in (2.8), the theorem has also been proved by Williams, [18], Theorem 2.

THEOREM 4. *Suppose that $s(n)$ is a non-negative function of $n = 1, 2, 3, \ldots$ and that δ satisfies $0 \leqslant \delta < 1$. Then for each n there exists a constant $c_n = c_n(\delta, s)$ such that, if $q > c_n$ and if $f(x)$, $g(x)$ in $k[x]$ (in addition to (2.1)) satisfy*

$$|r(f, g) - q| \leqslant s(n)q^{\delta}, \tag{2.8}$$

then f/g is an exceptional function.

Under the restriction that $p > n$ and when $g(x) = 1$, Theorem 5, the converse to Theorem 4, has been proved by MacCluer [11].

THEOREM 5. *If f/g is an exceptional function over k, then it is a permutation function.*

Theorems 4 and 5 possess an immediate corollary which establishes a conjecture of Williams [18] in a stronger form. In the conjecture, $g(x) = 1$, $q = p$ and $\delta = 0$ in (2.8).

COROLLARY. *If f and g are as in Theorem 4 and $q > c_n$ (as defined there), then $g(x)$ is irreducible and f/g is a permutation function over k.*

As an extension of the concept of an exceptional function, we shall say that f/g is l-exceptional if (2.7) factorizes in $k[X, Y]$ into a product containing no absolutely irreducible factors except precisely $l-1$ linear factors (i.e. factors whose degree in X and in Y is 1). Thus f/g is exceptional if it is 1-exceptional. We shall finally indicate how the proofs of Theorems 4 and 5 may be modified to yield a proof of Theorem 6 below.

THEOREM 6. (i) *If f/g is l-exceptional over k, then*

$$\left| r(f, g) - \frac{q}{l} \right| \leqslant \frac{n^3}{l(n-\deg g)} \leqslant \frac{n^3}{l}. \tag{2.9}$$

(ii) *Suppose that $s(n)$ and δ are as in Theorem 4. Then for each n there exists a constant $d_n = d_n(\delta, s)$ such that, if $q > d_n$ and if $f(x)$, $g(x)$ in $k[x]$ satisfy*

$$\left| r(f, g) - \frac{q}{n} \right| \leqslant s(n)q^{\delta}, \tag{2.10}$$

then f/g is n-exceptional over k and hence (2.9) with $l = n$ holds.

For $g(x) = 1$, $q = p$, part (i) represents an improvement of Williams [18], Theorem 1, who proved (2.9) with $O(1)$ instead of n^3/l. We shall show, in fact, that if f/g is l-exceptional over k and $f(x) - ag(x)$ has no repeated roots, then, if $f(x) - ag(x)$ has a root in k, it has precisely l roots in k. For $g(x) = 1$, $q = p$, part (ii) was proved by Mordell [13] by showing that essentially the only possible form for $f(x)$ was x^n. However, if $g(x)$ is non-constant, the author has shown in [5] that other f/g are possible. Along with Theorem 4, part (ii) of Theorem 6 forms a partial converse to part (i). It seems fairly clear that the converse is false if $l \neq 1, n$.

3. Preliminary results. In this section we return to the general situation described in § 1. We assume that all algebraic extensions considered are separable. Because of (2.1), this is sufficient for our purposes.

LEMMA 1. *In the notation of § 1,*

$$|G^*| = \frac{\varphi(f)}{f}|G|,$$

where φ is Euler's function.

Proof. In the sequel, if F is a subfield of a field E, $G_{E/F}$ will denote the Galois group of E over F. Thus $G_{K/k'(t)}$ is the Galois group of $Q(y)$ over $k'(t)$. Since $k'(t)$ is a normal extension of $k(t)$, by the fundamental theorem of Galois theory we have that $G_{K/k'(t)}$ is a normal subgroup of G and

$$G/G_{K/k'(t)} \cong G_{k'(t)/k(t)} \cong G_{k'/k}, \tag{3.1}$$

the last group being cyclic of order f and with generator τ where $\tau(a) = a^q$ ($a \in k'$). The isomorphism between the first and third groups of (3.1) is that which takes $\sigma G_{K/k'(t)}$ on to σ'.

From the above, it is clear that $|G_{K/k'(t)}| = f^{-1}|G|$ and that G^* is the union of those cosets of $G_{K/k'(t)}$ in G which are mapped on to τ^i, where $(i,f)=1$. There being $\varphi(f)$ such cosets, the proof is complete.

We remark also that if $(i,f)=1$, then $\sigma\in G^* \Leftrightarrow \sigma^i\in G^*$.

In the notation of § 1, K is a galois extension of $k(t)$ of degree $\leqslant n!$. If we neglect infinite divisors, K, $k(t)$ (and all intermediate fields) possess a theory of divisors which in $k(t)$ corresponds to ordinary factorization in $k[t]$. We assume this divisibility theory in what follows.

Let $\mathfrak{P}$ be a prime in some subfield K^* of K and let $P(t)$ be the prime divisor in $k[t]$ divisible by $\mathfrak{P}$. We shall say that $\mathfrak{P}$ has degree $g(\mathfrak{P}) = g_{K^*/k(t)}(\mathfrak{P})$ if $g(\mathfrak{P}) = f_{K^*/k(t)}(\mathfrak{P})\deg P(t)$, where here $f_{K^*/k(t)}(\mathfrak{P})$ is the degree of the extension of the residue class field of $\mathfrak{P}$ in K^* over that of $P(t)$ in $k(t)$ and $\deg P(t)$ is the degree of $P(t)$ as a polynomial in $k[t]$. Thus $g_{K^*/k(t)}(\mathfrak{P})=1$ if and only if $\mathfrak{P}|t-a$ for some a in k and $t-a$ splits completely in K^*.

LEMMA 2. *In the above notation, if* $K^*\cap k' = \mathrm{GF}(q^{f_1})$, *where* $f_1>1$, *then*

$$g_{K^*/k(t)}(\mathfrak{P})>1.$$

Proof. Suppose, by way of contradiction, that $g_{K^*/k(t)}(\mathfrak{P})=1$ and therefore that $\mathfrak{P}|t-a$ $(a\in k)$. Then the prime in $k'(t)$ divisible by $\mathfrak{P}$ is also $t-a$. Now

$$\begin{aligned} g_{K^*/k(t)}(\mathfrak{P}) &= f_{K^*/k(t)}(\mathfrak{P}) = f_{K^*/k'(t)}(\mathfrak{P}) f_{k'(t)/k(t)}(t-a) \\ &\geqslant f_{k'(t)/k(t)}(t-a) = f_1 > 1, \end{aligned}$$

a contradiction and the lemma is proved.

Before stating the next lemma, we introduce some more notation. If F is a subfield of a field E and P and $\mathfrak{P}$ are primes in F and E respectively, then $\left(\frac{E/F}{P}\right)$ and $\left[\frac{E/F}{\mathfrak{P}}\right]$ will denote the Artin symbol and the Frobenius automorphism respectively. In addition, if $\sigma\in G$ (a group), $N(\sigma)$ will denote the normaliser of σ in G. The next lemma is based on MacCluer's work in the algebraic number field case, [12].

LEMMA 3. *In the usual notation, let* $t-a$ *be unramified in* K. *Then we have*

$$\left(\frac{K/k(t)}{t-a}\right) \subseteq G^*. \tag{3.2}$$

Moreover, if $\sigma\in G$ *has order* h *and is such that* $\sigma\in\left(\frac{K/k(t)}{t-a}\right)$, *then there are exactly* $|N(\sigma)|/h$ *first degree primes* P *in* K_σ *dividing* $t-a$ *and such that*

$$\left(\frac{K/K_\sigma}{P}\right) = \{\sigma\}.$$

Proof. We use here results contained, for example, in [16], § 4–10 or [3], pp. 163–165.

We first prove (3.2). Let $\sigma\in\left(\frac{K/k(t)}{t-a}\right)$ and $\mathfrak{P}(\epsilon K)|t-a$ be such that $\left[\frac{K/k(t)}{\mathfrak{P}}\right]=\sigma$. Then k' may be considered as a subfield of the residue class field of $\mathfrak{P}$ and so, by the definition of the Frobenius automorphism if $\alpha\in k'$ then $\sigma(\alpha)=\alpha^q$. It follows that $K\cap k' = k$ and that (3.2) holds.

It therefore only remains to prove the latter assertion. We shall use H to denote the subgroup of G generated by σ. (Thus $|H|=h$.) Let $\mathfrak{P}(\epsilon K)|t-a$ be such that $\left[\frac{K/k(t)}{\mathfrak{P}}\right]=\sigma$. Then any prime divisor (in K) of $t-a$ has the form $\tau\mathfrak{P}$ for some $\tau\in G$. Moreover

$$\left[\frac{K/k(t)}{\tau\mathfrak{P}}\right] = \tau^{-1}\sigma\tau \quad\text{and}\quad \tau^{-1}\sigma\tau=\sigma \Leftrightarrow \tau\in N(\sigma).$$

Further, the decomposition group of $\mathfrak{P}$ is precisely H, i.e. $\tau\mathfrak{P}=\mathfrak{P}\Leftrightarrow\tau\in H$. Hence there are exactly $[N(\sigma):H]$ distinct primes $\mathfrak{P}|t-a$ such that $\left[\frac{K/k(t)}{\mathfrak{P}}\right]=\sigma$. But, since K_σ is the decomposition field of such a $\mathfrak{P}$, each such $\mathfrak{P}$ regarded as an element of K_σ is a prime divisor P with $g_{K_\sigma/k(t)}(P)=1$ and, of course, satisfying $\left(\frac{K/K_\sigma}{P}\right)=\{\sigma\}$. The proof is complete.

The crucial appeal to the Riemann hypothesis for function fields is made in the next lemma.

LEMMA 4. *In the usual notation, let* $k(t)\subseteq K^*\subseteq K$ *be a tower of fields such that* K *is a cyclic extension of* K^* *of degree* h *whose Galois group is generated by* σ *where* σ (ϵG) *is actually in* G^*. *Then* $\pi_\sigma(d)$, *where* $d|h$, *the number of first degree primes* P *of* K^* *for which* $\left(\frac{K/K^*}{P}\right)$ *has order* d, *satisfies*

$$\pi_\sigma(d) = \begin{cases} \dfrac{f}{\varphi(f)}\cdot\dfrac{\varphi(d)}{h}q+O(q^{1/2}), & \text{if } (f,h/d)=1, \\ 0, & \text{otherwise.} \end{cases} \tag{3.3}$$

(Note that necessarily $f|h|n!$. See also addendum.)

Proof. For all $h_1|h$, let $K^*_{h_1}$ be the fixed field under σ^{h_1}. Thus $K^*_1=K^*$ and $K^*_h=K$. Also $G_{K/K^*_{h_1}}$ (= Galois group of K over $K^*_{h_1}$) is the group generated by σ^{h_1} and $[K^*_{h_1}:K^*]=h_1$. Then ([16], p. 182),

a prime P in K^* (unramified in K) splits completely in $K^*_{h_1}$

$$\Leftrightarrow \left(\frac{K/K^*}{P}\right) \epsilon G_{K/K^*_{h_1}},$$

$$\text{i.e.} \Leftrightarrow \left(\frac{K/K^*}{P}\right) = \sigma^{sh_1} \text{ (for some } s),$$

$$\text{i.e.} \Leftrightarrow \text{the order of } \left(\frac{K/K^*}{P}\right) \text{ divides } h/h_1.$$

Hence $M(h_1)$, the number of first degree primes in $K^*_{h_1}$ (excluding infinite ones and those ramified in K) is

$$\sum_{s|(h/h_1)} h_1 \pi_\sigma(s) = \sum_{s|d} (h/d)\pi_\sigma(s). \tag{3.4}$$

Now if $K^*_{h_1} \cap k'$ contains k strictly (i.e. if $(h,f) > 1$), then $M(h_1) = 0$ by Lemma 2. On the other hand, if $K^*_{h_1} \cap k' = k$ (i.e. if $(h,f) = 1$), then the Riemann hypothesis (see, e.g. [7], p. 306) asserts that $M'(h_1)$, the number of first degree prime divisors (including infinite and ramified ones) in $K^*_{h_1}$ satisfies

$$|M'(h_1) - (q+1)| \leqslant 2gq^{1/2} \tag{3.5}$$

$$= O(q^{1/2}), \tag{3.6}$$

where g is the genus of $K^*_{h_1}$.

Since the numbers of ramified primes and of infinite primes under consideration are $\leqslant n!^2 = O(1)$, if follows from (3.4) and (3.6) that

$$\sum_{s|(h/h_1)} h_1 \pi_\sigma(s) = \begin{cases} q + O(q^{1/2}), & (h_1, f) = 1, \\ 0, & \text{otherwise} \end{cases}$$

and therefore

$$\sum_{s|d} (h/d)\pi_\sigma(s) = \begin{cases} q + O(q^{1/2}), & (f, h/d) = 1, \\ 0, & \text{otherwise}. \end{cases} \tag{3.7}$$

We now use induction on d to establish (3.3). First, putting $d = 1$ in (3.7) yields (3.3) in this case since $(f, h) = f$. Assume therefore that (3.3) holds for all $d' < d$. If $\big(f, (h/d)\big) > 1$, then $\big(f, (h/s)\big) > 1$ for all $s|d$ and hence (3.3) and (3.7) together yield $\pi_\sigma(d) = 0$. Suppose therefore that $\big(f, (h/d)\big) = 1$. Then (3.7) becomes

$$\sum_{\substack{s|d \\ (f,(h/s))=1}} (h/d)\pi_\sigma(s) = q + O(q^{1/2}),$$

i.e. by (3.3)

$$\frac{fq}{d\varphi(f)} \sum_{\substack{s|d \\ (f,(h/s))=1}} \varphi(s) + \frac{h}{d}\left(\pi_\sigma(d) - \frac{f}{\varphi(f)} \cdot \frac{\varphi(d)}{f} q\right) = q + O(q^{1/2}). \tag{3.8}$$

But,

$$\sum_{\substack{s|d \\ (f,(h/s))=1}} \varphi(s) = \sum_{s|d_1} \varphi(h's),$$

where $h = h'h''$, the prime factors of h' being those of f and $(h'', f) = 1$ so that $d = h'd_1$, $(d_1, f) = 1$. Hence

$$\sum_{s|d_1} \varphi(h's) = \varphi(h') \sum_{s|d_1} \varphi(s) = \varphi(h')d_1.$$

Now

$$\frac{f}{d\varphi(f)} \varphi(h')d_1 = \frac{f}{\varphi(f)} \cdot \frac{\varphi(h')}{h'} = 1,$$

since $f|h$. Consequently, (3.8) and the following remarks imply that (3.3) holds for all d. This completes the proof.

Note that if the genus of K is 0, then if follows from (3.5) that we may replace the $O(q^{1/2})$ of (3.3) by $O(1)$. We remark also that in our application we require only the value of $\pi_\sigma(h)$.

4. Proof of Theorem 1. In this section, we assume the notations and conventions of Theorem 1 and specialize the results of § 3 to this case. Thus K is a splitting field of the irreducible polynomial $f(y) - tg(y)$ of degree n over $k(t)$ with Galois group G. If x is any root of this polynomial, we have a tower of fields $k(t) \subseteq k(x) \subseteq K$ where $[k(x): k(t)] = n$ and K is a Galois extension of $k(t)$ with $[K: k(t)] \leqslant n!$. In $k(x)$, the divisibility theory of § 3 has the following properties. The units are generated by k and the $(< n)$ prime factors of $g(x)$ (the valuations corresponding to which lie over the infinite valuation of $k(t)$). The integers (respectively, primes) are associates of polynomials (respectively, irreducible polynomials prime to $g(x)$) in $k[x]$. We agree to identify associate elements of $k[x]$.

It is clear that $\pi_\lambda(f, g, q)$ is simply the number of first degree polynomials in $k[t]$ which have cycle pattern λ regarded as elements of $k[x]$. The number of ramified $t - a$ is clearly $O(1)$ and so as far as the estimate of Theorem 1 is concerned can be neglected. The connection between cycle patterns of polynomials and of automorphisms is established in the next lemma.

LEMMA 5. *In the above notation $f(y) - ag(y)$ (with no repeated roots) has cycle pattern λ if and only if*

$$\left(\frac{K/k(t)}{t-a}\right) \subseteq G_\lambda.$$

Proof. Let $\sigma \in \left(\frac{K/k(t)}{t-a}\right)$. It is sufficient to show that if σ has cycle pattern λ then so does $f(y)-ag(y)$. Accordingly, suppose that σ consists of l cycles of length h_i $(i=1,\dots,l)$, where $\sum_{i=1}^{l} h_i = n$, so that

$$\sigma = (x_1, \sigma x_1, \dots, \sigma^{h_1-1}x_1)\dots(x_l, \sigma x_l, \dots, \sigma^{h_l-1}x_l),$$

where $x_1, \dots, x_l$ are certain roots of $f(y)-tg(y)$ in K.

Now the residue class field of $t-a$ is (isomorphic to) $k = \mathrm{GF}(q)$. Also, if $\mathfrak{P}$ is a prime of K dividing $t-a$ and such that $\left[\frac{K/k(t)}{\mathfrak{P}}\right] = \sigma$, then the residue class field $K_{\mathfrak{P}}$ of $\mathfrak{P}$ is a finite extension of k. For any element U in K, let U' denote its image in $K_{\mathfrak{P}}$. Thus $t' = a$.

We have

$$f(y)-tg(y) = \prod_{i=1}^{l}\prod_{j=0}^{h_i-1}(y-\sigma^j x_i).$$

Passing to the residue class field $K_{\mathfrak{P}}$, we have by the definition of $\left[\frac{K/k(t)}{\mathfrak{P}}\right]$

$$f(y)-ag(y) = \prod_{i=1}^{l}\prod_{j=0}^{h_i-1}(y-x_i'^{q^j}), \tag{4.1}$$

where $x_i'^{q^{h_i}} = x_i'$ $(i=1,\dots,l)$. From the fact that $f(y)-ag(y)$ has no repeated roots and the well-known form of irreducible polynomials in $k[y]$, it follows from (4.1) that

$$P_i(y) = \prod_{j=0}^{h_i-1}(y-x_i'^{q^j})$$

is an irreducible polynomial of degree h_i in $k[y]$ and that $P_i(y) \neq P_j(y)$, $i \neq j$. This completes the proof.

Proof of Theorem 1. In what follows we omit the $O(1)$ terms arising from ramified primes. By Lemma 5, we have

$$\pi_\lambda(f,g,q) = \sum_{\left(\frac{K/k(t)}{t-a}\right)\subseteq G_\lambda \atop a\in k} 1 = \sum_{\left(\frac{K/k(t)}{t-a}\right)\subseteq G_\lambda^* \atop a\in k} 1, \qquad \text{by (3.2)} \tag{4.2}$$

$$= \sum_{\sigma\in G_\lambda^*} \frac{h}{l(\sigma)|N(\sigma)|} \sum_{\left(\frac{K/K_\sigma}{P}\right)=\sigma \atop g(P)=1} 1,$$

by Lemma 3, where h is the order of σ and $l(\sigma)$ is the number of elements in the conjugacy class containing σ. Since $|N(\sigma)| = |G|/l(\sigma)$, we have from (4.2) that

$$\pi_\lambda(f,g,q) = \frac{h}{|G|}\sum_{\sigma\in G_\lambda^*}\sum_{\left(\frac{K/K_\sigma}{P}\right)=1 \atop g(P)=1} 1 \tag{4.3}$$

holds. Now if $(i,h)=1$ then σ has the same cycle pattern as σ^i and, by the remark following Lemma 1 is in G_λ^* if and only if σ^i is. We deduce from this and (4.3) that

$$\begin{aligned}\pi_\lambda(f,g,q) &= \frac{h}{|G|\varphi(h)}\sum_{\sigma\in G_\lambda^*}\sum_{\left(\frac{K/K_\sigma}{P}\right)=\sigma^i,(i,h)=1 \atop g(P)=1} 1 \qquad (4.4)\\ &= \frac{h}{|G|\varphi(h)}\sum_{\sigma\in G_\lambda^*}\pi_\sigma(h)\\ &= \frac{h}{|G|\varphi(h)}\cdot\frac{f}{\varphi(f)}\cdot\frac{\varphi(h)}{h}|G_\lambda^*|q+O(q^{1/2}),\end{aligned}$$

by Lemma 4. Simplifying (4.4) and applying Lemma 1 in turn yields

$$\pi_\lambda(f,g,q) = \frac{f}{\varphi(f)}\cdot\frac{|G_\lambda^*|}{|G|}q+O(q^{1/2}) = \frac{|G_\lambda^*|}{|G^*|}q+O(q^{1/2}).$$

The proof of Theorem 1 is complete.

Note that when $K = k'(x)$, it follows from the concluding remark of § 3, that the $O(q^{1/2})$ term in (2.2) may be replaced by $O(1)$.

5. Permutation functions and exceptional functions. We assume throughout this section the notation and conventions of § 2 and § 4. Equivalent criteria for f/g to be exceptional are described in the next lemma. We remark that if follows from (5.3) below that G_1^* is never empty.

Lemma 6. *The following three statements are equivalent*:

(i) *f/g is exceptional over k.*

(ii) *All automorphisms in G_1^* contain exactly one 1-cycle.*

(iii) $G^* = G_1^*$.

Proof. It is sufficient to prove (i) $\Leftrightarrow$ (ii) and (ii) $\Leftrightarrow$ (iii). Recall that $\sigma\in G^*$ if and only if

$$\sigma'(a) = a \Leftrightarrow a\in k.$$

(i) $\Rightarrow$ (ii). Suppose that $\sigma\in G_1^*$ but that σ fixes different roots x, x_1 of $f(y)-tg(y)$ in K. Let

$$G_{f/g}(x,y) = G_1(x,y)\dots G_l(x,y) \tag{5.1}$$

be the prime decomposition of $G_{f/g}(x, y)$ (defined by (2.7)) in $k[x, y]$, where $y - x_1 | G_1(x, y)$, say, in $K[y]$. Then since f/g is exceptional $G_1(x, y) = H_1(x, y) \dots H_r(x, y)$ in $k'(x, y)$, where $r \geqslant 2$ and $y - x_1 | H_1(x, y)$, say. Now, since $\sigma(x) = x$, σ, regarded as an automorphism of $K[y]$, fixes $G_1(x, y)$. Hence $\sigma\{H_1(x, y)\} | G_1(x, y)$ in $k'[x, y]$. Also $\sigma\{H_1(x, y)\} \neq H_1(x, y)$ since otherwise $H_1(x, y) \in k(x, y)$ which contradicts the fact that $r > 1$. Hence $\sigma\{H_1(x, y)\} = H_2(x, y)$, say. Therefore $y - \sigma x_1 | H_2(x, y)$, i.e. $y - x_1 | H_2(x, y)$, which is impossible by separability. Hence (ii) must hold.

(ii) $\Rightarrow$ (i). Suppose that (ii) holds but that f/g is not exceptional. Let $\sigma \in G_1^*$ and let x be the unique root of $f(y) - tg(y)$ fixed by σ. Then $G_{f/g}(x, y)$ may be expressed in the form (5.1) in $k(x, y)$, where $G_1(x, y)$ (say) is even irreducible in $k'(x, y)$. Let x_1 be a root of $G_1(x, y) = 0$. Then so also is σx_1 and (by (ii)) $\sigma x_1 \neq x_1$. Since $G_1(x, y)$ is irreducible in $k'(x, y)$, there exists a $k'(x)$-automorphism ϱ in G such that $\varrho x_1 = \sigma x_1$. Hence

$$\varrho^{-1}\sigma x_1 = x_1 \quad \text{and} \quad \varrho^{-1}\sigma x = x. \tag{5.2}$$

However, since ϱ' is the identity automorphism on k', $(\varrho^{-1}\sigma)' = \sigma'$ and so $\varrho^{-1}\sigma$ (in G) actually belongs to G^*. Thus (5.2) contradicts (ii) and consequently f/g must be exceptional.

(ii) $\Leftrightarrow$ (iii). Let $x_1, \dots, x_n$ be the roots of $f(y) - tg(y)$ in K. Also, in this proof, let

$$G_{(i)} = \{\sigma \in G\colon\ \sigma(x_i) = x_i\}, \quad i = 1, \dots, n,$$

and put

$$G_{(i)}^* = G_{(i)} \cap G^*.$$

Then since $[k(x_i)\colon k(t)] = n$, we have, by the fundamental theorem of Galois theory, $|G_{(i)}| = |G|/n$. Also, since obviously $k(x_i) \cap k' = k$, it follows from Lemma 1 that

$$|G_{(i)}^*| = \frac{\varphi(f)}{f}|G_{(i)}| = \frac{\varphi(f)}{fn}|G| = \frac{|G^*|}{n}. \tag{5.3}$$

Now evidently

$$G_1^* = \bigcup_{i=1}^{n} G_{(i)}^*.$$

Hence

$$|G_1^*| \leqslant \sum_{i=1}^{n} |G_{(i)}^*| = |G^*|$$

(by (5.3)), with equality if and only if the $G_{(i)}^*$ are pairwise disjoint, i.e. if and only if (ii) holds. This completes the proof.

Indeed a very similar argument to that used to prove the equivalence of (i) and (ii) above yields the fact that the following statements, (i)' and (ii)', are also equivalent. (Recall that $G_1^* \neq \varphi$.)

(i)' *f/g is l-exceptional.*

(ii)' *Whenever σ and τ are (not necessarily distinct) automorphisms of G_1^* with one 1-cycle in common, they possess precisely l 1-cycles in common.*

We turn now to the proofs of Theorems 4 and 5.

Proof of Theorem 4. Suppose that f, g are such that (2.8) holds. Let n_i $(i = 1, \dots, n)$ be the number of polynomials of the form $f(y) - ag(y)$ $(a \in k)$ possessing exactly i distinct roots in k. Then clearly

$$\Big|\sum_{i=1}^{n} in_i - q\Big| = \deg g \leqslant n, \tag{5.4}$$

while (2.8) is equivalent to

$$\Big|\sum_{i=1}^{n} n_i - q\Big| \leqslant s(n)q^{\delta}. \tag{5.5}$$

Subtracting (5.5) from (5.4), we obtain

$$\sum_{i=2}^{n} n_i \leqslant \sum_{i=2}^{n} (i-1)n_i \leqslant s(n)q^{\delta} + n. \tag{5.6}$$

Suppose now that f/g is not exceptional over k. Then by Lemma 6 (ii), and since $G_1^* \neq \varphi$, there exists $\sigma \in G^*$ whose cycle pattern λ contains more than one 1-cycle. Hence $|G_\lambda^*| \geqslant 1$. Moreover, since the number of $f(y) - ag(y)$ with repeated roots is $\leqslant n^2$, then it follows from (5.6) that

$$\pi_\lambda(f, g, q) \leqslant e_n q^{\delta},$$

where $e_n = s(n) + 2n^2$. Hence, if g_n is the constant implied by (2.2), we have

$$\begin{aligned} \frac{q}{n!} \leqslant \frac{|G_\lambda^*|}{|G^*|}q \leqslant \left|\frac{|G_\lambda^*|}{|G^*|}q - \pi_\lambda(f, g, q)\right| + \pi_\lambda(f, g, q) \\ \leqslant g_n q^{1/2} + e_n q^{\delta} \leqslant (g_n + e_n)q^{\varepsilon}, \end{aligned} \tag{5.7}$$

where $\frac{1}{2} \leqslant \varepsilon = \max(\frac{1}{2}, \delta) < 1$. We deduce from (5.7) that

$$q \leqslant c_n(\delta, s),$$

where

$$c_n = [n!(g_n + e_n)]^{1/(1-\varepsilon)}.$$

This proves the theorem.

Proof of Theorem 5. The only new difficulty encountered here is the consideration of $f(x) - ag(x)$ when $t - a$ is ramified in K. If $\mathfrak{P}$ is

a prime in K dividing such a $t-a$ then, although there is no unique Frobenius automorphism corresponding to $\mathfrak{P}$, there do exist σ in G with the defining property of the Frobenius automorphism, [16], p. 179. The first part of Lemma 3 is easily modified to show that such a σ is in G^*. Moreover, the proof of Lemma 5 indicates that, in this case, to each 1-cycle in σ there corresponds a (not necessarily distinct) linear factor of $f(y)-ag(y)$ (even though the 1-cycles may not account for all the linear factors of $f(y)-ag(y)$).

Suppose now that f/g is exceptional. Then by Lemma 6, $G^* = G_1^*$. Hence by Lemma 5 and the above remarks, each polynomial $f(y)-ag(y)$ possesses at least one linear factor (and exactly one if $f(y)-ag(y)$ has distinct roots). Hence for all a in k, there exists θ in k such that $f(\theta) = ag(\theta)$ and $g(\theta) \neq 0$, since $(f, g) = 1$. Hence g is irreducible in $k[x]$ and $f(\theta)/g(\theta) = a$. Thus f/g is a permutation function (and so $f(y)-ag(y)$ has exactly one linear factor for all a). This completes the proof.

Proof of Theorem 6 (sketch). (i). The proof is similar to that of Theorem 5. If f/g is l-exceptional then, by the remarks following Lemma 6 and by Lemma 5, all polynomials $f(y)-ag(y)$ with a linear factor and no repeated roots have precisely l distinct roots in k. There are thus at most n^2 such polynomials with l' roots in k where $1 < l' \neq l$. After some calculation using these facts and the fact that to each θ in k, not a root of g, corresponds some a with $f(\theta) = ag(\theta)$, we obtain the inequalities (2.9). See also addendum.

(ii). This part of the proof is similar to that of Theorem 4. If n_i $(i = 1, \ldots, n)$ is as in that proof, then (5.4) holds and (2.10) is equivalent to

$$\left| \sum_{i=1}^{n} n_i - \frac{q}{n} \right| \leqslant s(n) q^{\delta}. \tag{5.8}$$

From (5.4) and (5.8) we deduce that

$$\sum_{i=1}^{n-1} n_i \leqslant \sum_{i=1}^{n-1} (n-i) n_i \leqslant n s(n) q^{\delta} + n. \tag{5.9}$$

(With (5.9) compare (5.6).) Assuming now that f/g is not n-exceptional, we can show, as in Theorem 4, but using (ii)' (following Lemma 6) and (5.9), that q is bounded. This completes the proof.

6. Examples. In general, it is a difficult task to find the Galois group of $f-tg$ or even to factorize $G_{f/g}(X, Y)$ (defined by (2.7)). Nevertheless, in this section, we select certain f, g which can be used to illustrate our results. In all of the examples we assume the notation of § 2.

In (a) and (b) below, we have $n = 4$ and let n_i $(i = 0, 1, 2, 4)$ be the number of $f(x)-ag(x)$ $(a \in k)$ which are irreducible in $k[x]$ apart

from i linear factors. In addition, let n_3 be the number of such polynomials which have cycle pattern 2^2 in $k[x]$. For convenience, if the roots of $f-tg$ in K are named in order as $x_1, \ldots, x_4$, then an element in G is to be considered as a permutation of these subscripts $1, \ldots, 4$. We shall neglect error terms.

(a) This example demonstrates what can happen if $G^* \neq G$. We consider simultaneously the cases $f/g = x^4$ and (in brackets, where different) $f/g = (x^4-1)/x^2$. If x is a root of $f-tg$ in K and $i^2 = -1$, then $K = k(x, i)$ and all the roots are x, ix, $-x$, $-ix$ (x, $-x$, ix^{-1}, $-ix^{-1}$).

If $q \equiv 1 \pmod 4$, then $i \in k$, $G = G^*$ and

(6.1)

$$G = \{(1234), (1432), (13)(24), (1)\} \quad (\{(12)(34), (14)(23), (13)(24), (1)\}).$$

Hence by Theorem 1,

$$n_i/q = \tfrac{1}{2}, 0, 0, \tfrac{1}{4}, \tfrac{1}{4} \ (0, 0, 0, \tfrac{3}{4}, \tfrac{1}{4}), \qquad i = 0, \ldots, 4. \tag{6.2}$$

On the other hand, if $q \equiv -1 \pmod 4$, then $i \notin k$ so that, although all the automorphisms in (6.1) are in G, they are not in G^* since they fix i. In fact, we now have $G^* = \varrho G$, where G is given by (6.1) and $\varrho = (12)(34)$ $((1324))$, which takes i on to $-i$. Hence

$$G^* = \{(13), (24), (12)(34), (14)(23)\} \ (\{(1423), (1324), (12), (34)\})$$

and so

$$n_i/q = 0, 0, \tfrac{1}{2}, \tfrac{1}{2}, 0 \ (\tfrac{1}{2}, 0, \tfrac{1}{2}, 0, 0), \qquad i = 0, \ldots, 4. \tag{6.3}$$

We now focus our comparison on the distribution of irreducibles. Thus, it follows from (6.2) and (6.3) that $q \equiv 1 \pmod 4$, then $n_0 \neq 0$ $(= 0)$, while if $q \equiv -1 \pmod 4$, then $n_0 = 0$ $(\neq 0)$, even though $G_4 \neq \emptyset$ in this case for $f/g = x^4$.

(b) Here we take q odd, $g =$ a constant, $f =$ any quartic polynomial and derive and complete the work of McCann and Williams [10] who estimated n_1, n_2, n_4. It is clear that without loss of generality, we may take $f(x) = x^4 + ax^2 + bx$. We have discussed the case $a = b = 0$ and omit this case from now on. Otherwise it is fairly evident that $G = G^*$. We consider two cases.

(i) $b \neq 0$. Here since

$$G_{f/g}(X, Y) = (Y+X)(Y^2+X^2) + a(Y+X) + b$$

is easily seen to be absolutely irreducible in $k[X, Y]$, then $3 \mid [K: k(t)]$ while, of course, $4 \mid [K: k(t)]$. Hence $|G| = [K: k(t)] \geqslant 12$. Now, since the discriminant of $f(y)-t$, being a cubic polynomial in t, is certainly not

a square in $k(t)$, then $G \neq A_4$, the alternating subgroup of S_4 (see [14], p. 251). Hence $G = S_4$. We therefore have

$$n_i/q = \tfrac{1}{4}, \tfrac{1}{3}, \tfrac{1}{4}, \tfrac{1}{8}, \tfrac{1}{24}, \qquad i = 0, \ldots, 4.$$

(ii) $b = 0$. Here

$$G_{f/g}(X, Y) = (Y+X)(Y^2+X^2+a).$$

Hence, if x is one root of $f(y)-t$, then the four roots are $x, -x, \theta, -\theta$, where $\theta^2+x^2+a = 0$. Moreover, $[K: k(t)] = 8$ and it is easy to verify that G is the quaternion group

$$\{(1), (12), (13), (13)(24), (12)(34), (14)(23), (1423), (1324)\}$$

generated by (12), (34) and (13)(24). It follows that $n_i/q = \tfrac{1}{4}, 0, \tfrac{1}{4}, \tfrac{3}{8}, \tfrac{1}{8}$.

(c). Finally, we obtain a class of permutation functions in which $g(x)$ is non-constant. In fact, put $f/g = x^p/(x^{p-1}+1)$ (p odd). Then

$$G_{f/g}(X, Y) = (YX)^{p-1}+(Y-X)^{p-1} = \prod_{i=0}^{p-2}\left(YX-\zeta^{2i+1}(Y-X)\right),$$

where ζ is a primitive $2(p-1)$th root of unity. It is easy to show that $\zeta \in k$ if and only if $q = p^b$, where b is even. Hence, if b is odd, then f/g is exceptional and so a permutation function, by Theorem 5. If b is even, then f/g is p-exceptional, and so, by Theorem 6, $|r(f, g)-p^{b-1}| \leqslant p$. Indeed, in this case, $r(f, g) = p^{b-1}$ exactly.

Addendum. To the hypotheses of Lemma 4 we must also add the assumption that the number of ramified first degree primes in K is $\leqslant n!^2$ (or indeed any specific function of n). This holds in the situation of Theorem 1, since there (by [16], p. 178) the number of ramified primes in $k(t) \leqslant$ degree in t of the discriminant of $f(y)-tg(y) \leqslant (n-\deg g)(n-1)$. This latter fact is also used to establish the inequality (2.9) in the proof of Theorem 6.

References

[1] B. J. Birch and H. P. F. Swinnerton-Dyer, *Note on a problem of Chowla*, Acta Arith. 5 (1959), pp. 417–423.

[2] L. Carlitz, *The arithmetic of polynomials in a Galois field*, Amer. J. Math. 54 (1932), pp. 39–50.

[3] J. W. S. Cassels and A. Fröhlich (Editors), *Algebraic Number Theory*, London 1967.

[4] S. Chowla, *A note on the constructions of finite Galois fields* GF(p^n), J. Math. Anal. Appl. 15 (1966), pp. 53–54.

[5] S. D. Cohen, Thesis, Glasgow University 1969.

[6] — *On irreducible polynomials of certain types in finite fields*, Proc. Cambridge Phil. Soc. 16(1969), pp. 335–344.

[7] M. Eichler, *Introduction to the theory of algebraic numbers and functions*, New York 1966.

[8] D. R. Hayes, *A geometric approach to permutation polynomials over a finite field*, Duke Math. J. 34 (1967), pp. 293–305.

[9] P. A. Leonard, *On constructing quartic extensions of* GF(p), Norske Vid. Selsk. Forh. (Trondheim), 40 (1967), pp. 96–97.

[10] K. McCann and K. S. Williams, *The distribution of the residues of a quartic polynomial*, Glasgow Math. J. 8 (1967), pp. 67–88.

[11] C. R. MacCluer, *On a conjecture of Davenport and Lewis concerning exceptional polynomials*, Acta Arith. 12 (1967), pp. 289–299.

[12] — *A reduction of the Čebotarev density theorem to the cyclic case*, Acta Arith. 15 (1968), pp. 45–47.

[13] L. J. Mordell, *A congruence problem of E. G. Straus*, J. London Math. Soc. 38 (1963), pp. 108–110.

[14] N. Tschebotarow und H. Schwerdtfeger, *Grundzuge der Galois'schen Theorie*, Groningen 1950.

[15] A. Weil, *Sur les courbes algébriques et les variétés qui s'en déduisent*, Actualités Sci. et Ind. 1041, Paris 1948.

[16] E. Weiss, *Algebraic Number Theory*, New York 1963.

[17] K. S. Williams, *On general polynomials*, Cand. Math. Bull. 10 (1967), pp. 579–583.

[18] — *On extremal polynomials*, Cand. Math. Bull. 10 (1967), pp. 585–594.

UNIVERSITY OF GLASGOW
Glasgow, W. 2, U. K.

Received on 16. 7. 1969