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 $(=\max(|a_0|,\ldots,|a_{n-1}|))\le N$ 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 $s(\ge 1)$ coefficients are allowed to vary. Provided only that $s\ge 2$ and with the obvious exceptions mentioned below we show that the number of such polynomials of height $\le N$ 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 $s\ge 2$). We draw particular attention to the fact that, if $s\ge 2$, 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 $\le N$ 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 $f(X)\ne g(X^r)$ for any polynomial g and any $r>1$. Then instead of considering an arbitrary

Received August 30, 1977.

polynomial of fixed degree n, we shall, equivalently, assume that F is primitive of degree n and look at $F(X^r)$ for arbitrary $r \geq 1$. Finally we shall not restrict ourselves to monic polynomials.

Notation. For convenience, we list most of the notation to be used here.

k, K algebraic number fields with K/k normal.

E, L general fields.

$G(L/E)$ (where $E \subseteq L$) the Galois group of L over E.

$\mathbf{Z}_k$ integers of k.

$|\alpha|$ (where $\alpha \in \mathbf{Z}_k$) height of $\alpha = |N_{k/\mathbf{Q}}(\alpha)|$.

$|\boldsymbol{\alpha}|$ (where $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_s) \in \mathbf{Z}_k^s$) $\max_{1 \leq i \leq s} |\alpha_i|$.

$\mathbf{Z}_k(N)$ the set of integers in k of height $\leq N$ if $k = \mathbf{Q}$; in general, any maximal subset whose members are non-associate or differ by a root of unity.

$\mathfrak{p}; \mathfrak{P}$ prime ideals in k; K.

$|\mathfrak{p}|$ $N_{k/\mathbf{Q}}(\mathfrak{p})$.

$k_q; \bar{k}_q$ (where q is a prime power) the finite field of order q; its algebraic closure.

$k_\mathfrak{p}$ the residue class field of $\mathfrak{p}$ in k (thus $\cong k_{|\mathfrak{p}|}$).

f a polynomial of degree n in $L[X]$ (where L is a specified field), possibly involving a set of parameters $A = \{\alpha_0, \ldots, \alpha_n\}$.

$f_\mathbf{t}; f_{\boldsymbol{\alpha}}$ (where $\mathbf{t}$ is an ordered set of s indeterminates and $\boldsymbol{\alpha} \in L^s$) f as above but in $L(\mathbf{t})[X]$; the same polynomial under the specialisation $\mathbf{t} \rightarrow \boldsymbol{\alpha}$. (If $s = 1$, write $f_t; f_\alpha$.)

$F; F_\mathbf{t}$ (where $\mathbf{t} \subseteq A$) the particular polynomial $\sum_{i=0}^n \alpha_i X^i$; the same polynomial with the members of $\mathbf{t}$ regarded as indeterminates.

$f(T, \Phi)$ (where $T \subseteq A$, $\Phi \subseteq L$) the set of polynomials f obtained by letting the members of T vary in Φ.

$f^{(r)}$ the polynomial $f(X^r)$.

$\delta = \delta(f, r, L)$; $\eta = \eta(\delta)$ the least divisor δ of r such that a_0/a_n is an r/δ-*th* power in L, where $f(X) = a_n X^n + \cdots + (-1)^n a_0$; $(a_0/a_n)^{\delta/r}$

$\Pi_{K/k}(x)$; $M_{K/k}(F_\mathbf{t}, x)$ the set of all $\mathfrak{p}$ with $|\mathfrak{p}| \leq x$ which split completely in K; the subset for which $\mathfrak{p} | \alpha_0$ or such that $F_\mathbf{t} \pmod{\mathfrak{p}}$ is not primitive of degree n.

$x, \mathbf{x} = (x_1, \ldots, x_n)$ a root and the set of roots of $f(X) = 0$ (or $f_\mathbf{t}(X) = 0$). (No confusion could arise with the use of x in $\Pi_{K/k}(x)$, etc.)

$y, \mathbf{y} = (y_1, \ldots, y_n)$ a root and a set of n roots of $f(X^r) = 0$ such that $y_i^r = x_i$, $i = 1, \ldots, n$.

$G(f, L)$ the Galois group of f over L regarded as a group of permutations of $\mathbf{x}$.

$H_r(f, L)$ $G(f^{(r)}, L(\mathbf{x}))$. (Thus $G(f, L) \cong G(f^{(r)}, L)/H_r(f, L)$.)

$D(f)$ the discriminant of $f = a^{2n-2} \prod_{i \neq j} (x_i - x_j)$, where a is the leading coefficient of f.

S_n, A_n the symmetric and alternating groups of order n.

C_d a cyclic group of order d.

ζ, ζ_r a *primitive* rth root of unity (in the appropriate field).

2. Statement of main results

Let k be an algebraic number field and K a finite, normal extension (possibly with $K = k$). Our principal result concerns the distribution of the Galois groups over K of polynomials in $\mathbf{Z}_k[X]$ for which a prescribed set of coefficients vary in $\mathbf{Z}_k(N)$.

THEOREM 1. *Let $F_{\mathbf{t}}(X)(=\sum_{i=0}^{n} \alpha_i X^i)$ be a primitive polynomial in $\mathbf{Z}_k[\mathbf{t}, X]$, where $\mathbf{t}$ is a prescribed subset of $\{\alpha_0, \ldots, \alpha_n\}$ of cardinality $s \geq 1$ and $\alpha_0\alpha_n \neq 0$. Let $r \geq 1$ and $\mathcal{G} = G(F_{\mathbf{t}}^{(r)}, K(\mathbf{t}))$. Then the number of polynomials in $F(\mathbf{t}, \mathbf{Z}_k(N))$ for which $G(F^{(r)}/K)$ is not isomorphic to $\mathcal{G}$ is $\ll N^{s-1/2} \log N$. Here, if $s \geq 2$ and provided only that*

$$|M_{K/k}(F_{\mathbf{t}}, N^{1/2})| \leq \tfrac{1}{2}|\Pi_{K/k}(N^{1/2})|, \qquad (1)$$

the implied constant depends only on rn and K. If $s = 1$, the implied constant is independent of N.

Further, if $s \geq 2$, $\delta = \delta(F_{\mathbf{t}}, r, K(\zeta_r))$ and $\varepsilon = [K(\zeta_r) : K]$ (thus $\varepsilon \mid \phi(r)$), then $\mathcal{G}$ is a group of order $n!r^{n-1}\delta\varepsilon$ which is such that

$$\mathcal{G}/\mathcal{H} \cong S_n \times G(K(\zeta_r)/K), \quad \text{where} \quad \mathcal{H} \cong C_r^{n-1} \times C_\delta.$$

Notes. (i) Of course, $|F(\mathbf{t}, \mathbf{Z}_{\mathbf{Q}}(N))| = (2N+1)^s$ while, in general,

$$|F(\mathbf{t}, \mathbf{Z}_k(N)| \sim c_k N^s \quad \text{as} \quad N \to \infty.$$

(ii) Trivially, $\delta(F_{\mathbf{t}}, r, K(\zeta_r)) = r$ if α_0 or $\alpha_n \in \mathbf{t}$.

(iii) In fact, $\mathcal{G} = G(F_{\mathbf{t}'}^{(r)}, K(\mathbf{t}'))$, where $\mathbf{t}'$ is obtained from $\mathbf{t}$ by adding the non-zero members of $\{\alpha_0, \ldots, \alpha_n\} \setminus \mathbf{t}$ (but excluding α_0 and α_n if they both $\notin \mathbf{t}$).

(iv) The restriction (1) is very mild. In particular, if only polynomials of height $\leq N$ are being considered it can be omitted since in that case

$$|M_{K/k}(F_{\mathbf{t}}, N^{1/2})| \ll \log N.$$

(v) If $s = 1$, the group $\mathcal{G}$, in general, depends on F_t even if $r = 1$. However, in many cases it can be shown, using a test such as Lemma 8 below, that, if F_t is primitive, then $G(F_t, K(t)) = S_n$. In this connection, Hering [14] has shown that, if F_t is a primitive trinomial of the form $a_n X^n + a_u X^u + a_0$, where t is a_0, a_u or a_n, then $G(F_t, \mathbf{Q}(t)) = S_n$.

(vi) In the case $s \geq 2$, $r = 1$ the estimate for the number of exceptional polynomials in Theorem 1 can be improved to $\ll N^{s-1/2} \log^{1-\gamma} N$, where $\gamma > 0$, as in [12]. We omit the details.

When $s = 1$, Theorem 1 is a special case of the following more general result in which $f_t(X)$ is an arbitrary polynomial in $\mathbf{Z}_k[t, X]$, not necessarily irreducible.

THEOREM 2. *Let $f_t(X) \in \mathbf{Z}_k[t, X]$. Then the number of α in $\mathbf{Z}_k(N)$ for which $G(f_\alpha, K) \neq G(f_t, K(t))$ is $O_{f_t, K}(N^{1/2} \log N)$.*

3. Preliminary results

We need a version of the large sieve in $\mathbf{Z}_k^s$. For each prime ideal $\mathfrak{p}$ of k, let $W(\mathfrak{p})$ be a subset of $\mathbf{Z}_k^s/\mathfrak{p}\mathbf{Z}_k^s$ $(\cong k_{\mathfrak{p}}^s)$ of cardinality $\omega(\mathfrak{p})$ so that $0\le\omega(\mathfrak{p})\le|\mathfrak{p}|^s$. For each $\boldsymbol{\alpha}\in\mathbf{Z}_k^s$ let $P(\boldsymbol{\alpha}, x)$ denote the number of $\mathfrak{p}$ with $|\mathfrak{p}|\le x$ for which $\boldsymbol{\alpha}$ $(\operatorname{mod}\mathfrak{p})\in W(\mathfrak{p})$ and put $P(x)=\sum_{|\mathfrak{p}|\le x}\omega(\mathfrak{p})/|\mathfrak{p}|^s$. The following result extends Lemma A of [12] to general algebraic number fields.

LEMMA 1. *For $N\ge x^2$, we have $\sum_{|\boldsymbol{\alpha}|\le N}(P(\boldsymbol{\alpha}, x)-P(x))^2\ll N^sP(x)$, where the implied constant depends only on k and s.*

Proof. A combination of the method of Lemma A of [12] with that used, for example, by Wilson [19] in proving the general large sieve inequality gives the result. Accordingly, we indicate only a brief outline of the proof.

For any $\mathfrak{p}$ in k and $\boldsymbol{\gamma}$ in $\mathbf{Z}_k^s/\mathfrak{p}\mathbf{Z}_k^s$, put

$$S(\boldsymbol{\gamma}/\mathfrak{p})=\sum_{|\boldsymbol{\alpha}|\le N}c(\boldsymbol{\alpha})e[(\mathrm{Tr}\,\boldsymbol{\alpha}\cdot\boldsymbol{\gamma}^*)/p],$$

where the $c(\boldsymbol{\alpha})$ are complex numbers, $\boldsymbol{\alpha}\cdot\boldsymbol{\gamma}$ is the inner product in $\mathbf{Z}_k^s$, Tr denotes the trace taken over $\mathbf{Q}$, $e(x)=\exp(2\pi ix/p)$ and $\boldsymbol{\gamma}^*$ $(\in\mathbf{Z}_k^s)$ is defined by $\boldsymbol{\gamma}^*\equiv\boldsymbol{\gamma}\ (\operatorname{mod}\mathfrak{p})$, $\boldsymbol{\gamma}^*\equiv\mathbf{0}\ (\operatorname{mod} p/\mathfrak{p})$, p being the rational prime divisible by $\mathfrak{p}$. Then, with reference to [19], as in §7 but applying the results of §4 with $S(\mathbf{x})$ an exponential form in sn variables, we obtain

$$\sum_{|\mathfrak{p}|\le x}\sum_{\boldsymbol{\gamma}}|S(\boldsymbol{\gamma}/\mathfrak{p})|^2\ll(x^{2s}+N^s)\sum_{|\boldsymbol{\alpha}|\le N}|c(\boldsymbol{\alpha})|^2,$$

in which $\boldsymbol{\gamma}$ is summed over $\mathbf{Z}_k^s/\mathfrak{p}\mathbf{Z}_k^s$. Now apply the argument of [12, p. 93–94] with $\phi_{\mathfrak{p}}(\boldsymbol{\alpha})$ the characteristic function of $W(\mathfrak{p})$ (so that

$$\phi_{\mathfrak{p}}(\boldsymbol{\alpha})=\sum_{\boldsymbol{\gamma}}c_{\mathfrak{p}}(\boldsymbol{\gamma})e[(\mathrm{Tr}\,\boldsymbol{\alpha}\cdot\boldsymbol{\gamma}^*)/\mathrm{p}],$$

say) and

$$c(\boldsymbol{\alpha})=\sum_{|\mathfrak{p}|\le x}\sum_{\gamma\ne 0}c_{\mathfrak{p}}(\boldsymbol{\gamma})e[(\mathrm{Tr}\,\boldsymbol{\alpha}\cdot\boldsymbol{\gamma}^*)/p]$$

to get the result.

We now describe the situation which prevails for the principal application of the lemma. First we define a concept which was used in [6] and [12]. If a polynomial f in $L[X]$ of degree n factorises into a product of *distinct*, irreducible factors in $L[X]$, there being λ_i factors of degree i, $i=1,2,\ldots$ $(\sum_i i\lambda_i=n)$, we shall say that f is of *splitting type* or has (*factor*) *cycle pattern* $\lambda=(1^{\lambda_1}, 2^{\lambda_2},\ldots)$ (*of degree n*), where we usually shall omit those i for which $\lambda_i=0$. We write this as $\lambda(f)=\lambda$. For example, if f splits completely in L, then $\lambda(f)=(1^n)$.

Let $\mathbf{t}=(t_1,\ldots,t_s)$ and $f_{\mathbf{t}}(X)$ be a square-free polynomial in $\mathbf{Z}_k[\mathbf{t},X]$ so that $D(f_{\mathbf{t}})\neq 0$. Let $\boldsymbol{\alpha}\in k^s$ and $\mathfrak{p}$ be such that $f_{\boldsymbol{\alpha}}(X)\pmod{\mathfrak{p}}$ also has degree n and $\mathfrak{p}\nmid D(f_{\boldsymbol{\alpha}})$. Then the splitting type of $f_{\boldsymbol{\alpha}}(X)$ in $k_{\mathfrak{p}}[X]$ of degree n is defined. Call it $\lambda_{\mathfrak{p}}(f_\alpha)$. Clearly $\lambda_{\mathfrak{p}}(f_\alpha)$ depends only on $\boldsymbol{\alpha}\pmod{\mathfrak{p}}$ and can be interpreted as the splitting type (in the obvious sense) of $\mathfrak{p}$ in $k(x)$ where $f_{\boldsymbol{\alpha}}(x)=0$. Indeed, if K/k is a normal extension and $\mathfrak{p}$ splits completely in K with $\mathfrak{P}\mid\mathfrak{p}$, then, since $K_{\mathfrak{P}}\cong k_{\mathfrak{p}}$, $\lambda_{\mathfrak{p}}(f_{\boldsymbol{\alpha}})$ is also the splitting type of $\mathfrak{P}$ in $K(x)$. Moreover, the incidence of a given splitting type λ among $\lambda_{\mathfrak{p}}(f_{\boldsymbol{\alpha}})$ as $\boldsymbol{\alpha}$ and $\mathfrak{p}$ vary depends on $G(f_{\mathbf{t}},k_{\mathfrak{p}}(t))$ and $G(f_{\boldsymbol{\alpha}},K)$ respectively. Our method involves the former dependence (in the shape of Lemma 2 below) together with an application of Lemma 1 with, for any λ,

$$W_\lambda(\mathfrak{p})=\begin{cases}\{\boldsymbol{\alpha}\in\mathbf{Z}_k^s/\mathfrak{p}\mathbf{Z}_k^s,\ \lambda_{\mathfrak{p}}(f_{\boldsymbol{\alpha}})\text{ is defined and equals }\lambda\} & \\ & \text{if }\mathfrak{p}\text{ splits completely in }K,\\ \phi & \text{otherwise.}\end{cases}\tag{2}$$

The next result is the Čebotarëv density theory for function fields as given in [6, Prop A.3]. (See also [3], [4], [10].)

Lemma 2. *Let $f_t(X)\in k_q[t,X]$ have splitting field E over $k_q(t)$ where $E/k_q(t)$ is galois. Put*

$$G^*=G^*(f_t,k_q(t)=\{\sigma\in G(f_t,\bar{k}_q(t)):\bar{k}_q\cap E^\sigma=k_q\},$$

where E^σ is the fixed field of σ. Let λ be a splitting type or cycle pattern of degree n and let G_λ^* denote the subset of G^* comprising elements with cycle pattern λ. Then the number of α in k_q for which f_α has splitting type λ (or, equivalently, for which the Frobenius class

$$\left(\frac{E/k_q(t)}{t-\alpha}\right)$$

is a subset of G_λ^*) is

$$(|G_\lambda^*|/|G^*|)q+O(q^{1/2}),$$

where the implied constant depends only on the degree and genus of $E/k_q(t)$.

Note. The genus if $E/k_q(t)$ is bounded by a constant depending on the total degree of $f_t(X)$.

The reader should observe that G^* (and not G) occurs in Lemma 2. This is a complicating factor which particularly causes difficulties when $s=1$ or when $r>1$. Moreover, our desire to achieve as uniform a result as possible (when $s\geq 2$) also compels us to take extra care.

4. The case $s=1$

We require two lemmas before embarking on the proof of Theorem 2. The first enables us to replace K by $\bar{K}$, its algebraic closure in $L\{t\}=K(t,x)$, thus ensuring that $L\{t\}/\bar{K}(t)$ is a regular extension and making for an easier application of Lemma 2.

LEMMA 3. *Let $L\{t\}$ be the splitting field of a square-free polynomial $f_t(X)$ in $\mathbf{Z}_K[t]$, where K is an algebraic number field (or, more generally, any field of characteristic 0). Denote the algebraic closure of K in $L\{t\}$ by $\bar{K}$ and suppose that the specialisation $t \to \alpha$ takes $L\{t\}$ onto $L\{\alpha\}$. Then $\bar{K} \subseteq L\{\alpha\}$ except for a number of values of α bounded by a constant depending only on the total degree of f_t.*

Proof. Let $x_1, \ldots, x_n$ be the roots of $f_t(X)=0$. By a standard argument based on the bounded number of fields between $K(t)$ and $K(t, x_1, x_2)$, it follows that, for some bounded integer a, $K(t, x_1, x_2) = K(t, x_1 + ax_2)$. An induction argument shows that $L\{t\} = K(t, \mathbf{x}) = K(t, z)$, where $z = \sum_{i=1}^n a_i x_i$ for certain bounded integers a_i. Let g be the minimal polynomial of z over $K(t)$. Then g is irreducible of bounded degree ($=m$, say) and height and hence $D(g)$ has bounded degree in t. Suppose that $(t-\alpha) \nmid D(g)$ (so that $t-\alpha$ is unramified in $L\{t\}$ and the leading coefficient of g does not vanish when $t=\alpha$). Then (see e.g. [8, III §1.4]), the conjugates $z_1, \ldots, z_m$ of z have *distinct* Puiseux expansions

$$z_i(t) = z_i = \sum_{j=0}^{\infty} \beta_{ij}(t-\alpha)^j, \qquad i = 1, \ldots, m, \beta_{ij} \in K(\beta_{i0}).$$

Specialising $t \to \alpha$ and noting that the $z_i(\alpha)$ are distinct members of $L\{\alpha\}$ since $t-\alpha$ is unramified, we see that the β_{i0} ($\in L\{\alpha\}$) are not fixed by any non-identical automorphism in $G(\bar{K}/K)$. Hence $\bar{K} \subseteq K(\beta_{10}, \ldots, \beta_{m0}) = L\{\alpha\}$.

A special case of the next lemma occurs in [1]. See also [11].

LEMMA 4. *In the situation of Lemma 3, suppose that $L\{t\}/K(t)$ is a regular extension (so that $\bar{K} = K$). Then, for almost all $\mathfrak{P}$ in K,*

$$G(f_t, K(t)) = G(f_t, K_{\mathfrak{P}}(t)).$$

Proof. Suppose that $D(f_t)$ is non-zero (mod $\mathfrak{P}$) (which is the case for almost all $\mathfrak{P}$). Then, by Galois theory there exists $z \in L\{t\}$ such that

$$G(f_t, K_{\mathfrak{P}}(t)) \cong G(L\{t\}/K(t, z)).$$

Also suppose that z has minimal polynomial g_t over $K(t)$ of degree >1. Then $g_t(X)$ is absolutely irreducible in $K(t, X)$ but is reducible in $K_{\mathfrak{P}}(t, X)$. By Noether's lemma ([15, III Prop 7] or [11, Lemma 11]) this can happen for only finitely many $\mathfrak{P}$.

Note. It would be useful to apply a quantitative version of Noether's lemma. This would yield an estimate for the number of exceptional f_α in Theorem 2 involving a constant dependent only on the total degree and height of f_t and on $\bar{K}$.

Proof of Theorem 2. It is obvious that f_t may be assumed to be squarefree. Let $\bar{k}$ be the algebraic closure of k in $L\{t\}$, the splitting field of f_t over $k(t)$. Suppose, in fact that the theorem is true when $\bar{k} \subseteq K$. We could then derive the general case as follows. Put $\bar{K} = K\bar{k}$. Then the number of α in $\mathbf{Z}_k(N)$ for which $G(f_\alpha/\bar{K}) \neq G(f_t/\bar{K}(t))$ is $\ll N^{1/2} \log N$. Moreover, by Lemma 3, for almost all α, $\bar{K} \subseteq KL\{\alpha\}$. Apart from these exceptional α, it is clear that $G(f_\alpha/K) \cong G(f_t/K(t))$ since $G(\bar{K}/K) \cong G(\bar{K}(t)/K(t))$.

It suffices therefore to assume that $\bar{k} \subseteq K\ (= \bar{K})$. Thus $KL\{t\}/K(t)$ is a regular extension. We apply Lemma 1 with $s = 1$ and $W_\lambda(\mathfrak{p})$ given by (2) with $\lambda = (1^n)$. By the prime ideal theorem in $K\{\alpha\}$[1],

$$P_\lambda(\alpha, x) \sim m_\alpha^{-1} |\Pi_{K/k}(x)| \sim (dm_\alpha)^{-1}(x/\log x), \tag{3}$$

where $m_\alpha = |G(f_\alpha, K)|$ and $d = [K : k]$.

We now estimate $P_\lambda(x)$. Suppose that $\mathfrak{p}$ splits completely in K and that $\mathfrak{P} \mid \mathfrak{p}$. By Lemma 4, for almost all $\mathfrak{p}$, $G(f_t, K(t)) \cong G(f_t, K_{\mathfrak{P}}(t) \cong G(f_t, k_{\mathfrak{p}}(t))$. Apart from these exceptional $\mathfrak{p}$, we have, by Lemma 2,

$$\omega_\lambda(\mathfrak{p}) = m^{-1}q + O(q^{1/2}), \quad \text{where} \quad q = |\mathfrak{p}| \quad \text{and} \quad m = |G(f_t, K(t))|.$$

Hence, by the prime ideal theorem

$$P_\lambda(x) \sim (md)^{-1}(x/\log x), \tag{4}$$

since $\sum_{|\mathfrak{p}| \leq x} |\mathfrak{p}|^{-1/2} \ll x^{1/2}$. Suppose α is such that $m_\alpha < m$. Combining (3) and (4) we have for $x = N^{1/2}$ and N sufficiently large

$$P_\lambda(\alpha, N^{1/2}) - P_\lambda(N^{1/2}) > (2\,dn!)^{-1} P_\lambda(N^{1/2}), \tag{5}$$

since $m \leq n!$. But Lemma 1 and (4) imply that (5) can hold for at most $\ll N^{1/2} \log N$ values of α and the theorem follows.

Note. If $K = \mathbf{Q}$ and $G(f_t, \mathbf{Q}(t))$ is known to be S_n, we could have proceeded as in [12, p. 98] making our appeal to the prime ideal theorem unnecessary. However, we shall require this alternative approach in §5 for $s \geq 2$.

5. The case $s \geq 2$

We begin with two lemmas whose proofs are deferred to §§6–8. The first, a purely field-theoretical result, is included to deal with the case $r > 1$ and involves a general field L which, for convenience, is assumed to contain all *r-th* roots of unity for a given *r*. The reader is referred to §1 for details of the notation.

LEMMA 5. *Let* $F(X)$ $(= \sum_{i=0}^{n} \alpha_i X^i)$ *in* $L[X]$, *where* $L(\zeta_r) = L$ *and* $\alpha_0 \alpha_n \neq 0$, *be such that* $G(F, L) = S_n$. *Suppose that* char $L \nmid r$ *and that* $\delta = \delta(F, r, L)$,

[1] This step can only be justified on the Generalized Riemann Hypothesis. However, the theorem is true unconditionally; an effective version should appear in a future paper.

$\eta=\eta(\delta)$. *Then, either*

(i) $$H_r(f,L)=\begin{cases} C_r^{n-1}\times C_\delta & \text{if } \delta \text{ is odd or } \sqrt{\eta D(F)}\notin L,\\ C_r^{n-1}\times C_{\delta/2} & \text{if } \delta \text{ is even and } \sqrt{\eta D(F)}\in L,\end{cases}$$

or

(ii) *for some prime* $p\mid r$, *if* $F^{(p)}(y)=0$, *then* $H_p(F, L(y))$ *is trivial.*

LEMMA 6. *Suppose that* char $k_q > nr$ *where* $n\geq 2$. *Let* $\tau=\{v,u,\ldots\}$ *be a subset of* $\{0,1,\ldots,n\}$ *of cardinality* $s\geq 2$ *written in increasing order* (*so that* $0\leq v<u\leq n$) *and such that* $\tau\neq\{v,n\}$ *with* $v>0$. *Put*

$$f(X)=\sum_{\substack{i=0\\ i\neq v}}^{n}\alpha_i X^i+\alpha_v g(X),\quad \textit{where}\quad g(X)=\begin{cases}X^u+X^v & \textit{if}\quad v>0\\ 1 & \textit{if}\quad v=0\end{cases}$$

and assume that, if $\mathbf{t}=\{\alpha_i, i\in\tau\}$, *then* $f_{\mathbf{t}}$ *is primitive of degree* n *in* $k_q[\mathbf{t}, X]$. *Then for all but* $O_n(q^{s-3/2})$ *polynomials* f_t *in* $f_t(\mathbf{t}-\{\alpha_v\}, k_q)$ (*where* $t=\alpha_v$), *the following properties hold*:

(i) $G(f_t, \bar{k}_q(t))=S_n$;

(ii) $D(f_t)$ *in* $\bar{k}_q(t)$ *has a non-repeated linear factor* $\neq t$;

(iii) *for all primes* $p\mid r$, $H_p(f_t, \bar{k}_q(t,y))$ *is non-trivial.*

Note. If $v>0$, our proof shows that actually (i)–(iii) hold with at most $O_n(q^{s-2})$ exceptions.

Proof of Theorem 1 ($s\geq 2$).We may suppose that, if $\alpha_n\in\mathbf{t}$, then so does α_0, for otherwise we could consider $X^nF(1/X)$. Assume first of all that $K(\zeta_r)=K$. The result is then trivial if $n=1$ and $4\nmid r$. If $n=1$ and $4\mid r$, then $G(x^r-\alpha, K)=\mathscr{G}$ unless α or -4α is a d-*th* power, where $d\mid r$, $d>1$ and the result is clear. So assume $n>1$. We write the subscripts of the members of $\mathbf{t}$ as$\prime\tau$ in Lemma 6.

By Lemma 5, $G(F^{(r)}, K)=\mathscr{G}$ for F in $F(\mathbf{t}, \mathbf{Z}_k)$ unless one of the following (I)–(IV) holds:

(I) $G(F,K)\neq S_n$;

(II) $\sqrt{\eta D(F)}\in K$, where $\eta=\eta(\delta(F,r,K))$;

(III) for some $p\mid r$, $H_p(F, K(y))$ is trivial for some y with $F^{(p)}(y)=0$;

(IV) α_0 or $\alpha_n\in\mathbf{t}$ and $\delta(F,r,K)<r$.

Now (IV) occurs for at most

$$O_k(N^{s-1}\sum_{\substack{d\mid r\\ d>1}}N^{1/d})=O_{k,r}(N^{s-1/2})$$

polynomials F in $F(\mathbf{t}, \mathbf{Z}_k(N))$ and so can be disregarded. The incidence of cases (I)–(III) will be estimated by three distinct applications of Lemma 1 with $x=N^{1/2}$. We may describe the various sets $W(\mathfrak{p})$ as follows. Put

$$\mathscr{S}=\Pi_{K/k}(N^{1/2})\backslash(M_{K/k}(F_{\mathbf{t}}, N^{1/2})\cup\{\mathfrak{p}, \text{char } k_{\mathfrak{p}}\leq nr\}).$$

Suppose $\mathfrak{p} \in \mathscr{S}$. Then, for any cycle pattern λ of degree n, define

$$W_1(\mathfrak{p})(=W_1^{\lambda}(\mathfrak{p})) = \{\boldsymbol{\alpha} \in \mathbf{Z}_k^s/\mathfrak{p}\mathbf{Z}_k^s \colon \lambda_{\mathfrak{p}}(F_{\boldsymbol{\alpha}}) = \lambda\}. \tag{8}$$

Similarly, put

$$W_2(\mathfrak{p}) = \{\boldsymbol{\alpha} \colon \eta D(F_{\boldsymbol{\alpha}}) \text{ (mod } \mathfrak{p}) \text{ is not a square in } k_{\mathfrak{p}}\}, \tag{9}$$

where $\eta = \eta(\delta(F_{\boldsymbol{\alpha}}, r, K))$, recalling that $K_{\mathfrak{P}} = k_{\mathfrak{p}}$ so that $\eta \in k_{\mathfrak{p}}$. Finally, for any prime $p \mid r$, take the $f_{\mathbf{t}}$ of §3 to be $F_{\mathbf{t}}$ and $F_{\mathbf{t}}^{(p)}$ in turn and define

$$W_3(\mathfrak{p}) \; (= W_3^{(p)}(\mathfrak{p})) = \{\boldsymbol{\alpha} \colon \lambda_{\mathfrak{p}}(F_{\boldsymbol{\alpha}}) = (1^n) \quad \text{but} \quad \lambda_{\mathfrak{p}}(F_{\boldsymbol{\alpha}}^{(p)}) = (1^{\lambda 1}, p^{\lambda p}),$$
$$\text{where} \quad 1 \leq \lambda_p \leq n-1 \quad \text{and} \quad \lambda_1 + p\lambda_p = pn\}. \tag{10}$$

To complete these definitions, let $W(\mathfrak{p}) = \phi$ if $\mathfrak{p} \notin \mathscr{S}$. The following observation is important. With f as in Lemma 6 and $\mathfrak{p} \in \mathscr{S}$ we have $f(\mathbf{t}, k_{\mathfrak{p}}) = F(\mathbf{t}, k_{\mathfrak{p}})$ so that (8)–(10) are unaltered if we replace F by f in them. We may therefore use Lemma 6 to evaluate $\omega_i(\mathfrak{p})$, $i = 1, 2, 3$ (defined as in §3), for each $\mathfrak{p} \in \mathscr{S}$.

In particular, by Lemma 6(i) and Lemma 2 we have

$$\omega_1^{(\lambda)}(\mathfrak{p}) = c_\lambda q^s + O_n(q^{s-1/2}), \tag{11}$$

where $q = |\mathfrak{p}|$ and $c_\lambda = |(S_n)_\lambda|/n! > 0$.

Next, to estimate $\omega_2(\mathfrak{p})$, consider any $f_t \in f_t(\mathbf{t} - \{\alpha_v\}, k_{\mathfrak{p}})$ $(t = \alpha_v)$ which is not one of the exceptions to Lemma 6. By Lemma 6(ii), if $\eta = \eta(\delta(f_t, r, k_{\mathfrak{p}}))$, then $\eta D(f_t)$ is not a perfect square in $k_{\mathfrak{p}}(t)$. Hence, if we now regard α_v as an element of k_q $(\cong k_{\mathfrak{p}})$ and $\eta = \eta(\delta(f_{\alpha_v}, r, k_q))$, the number of α_v in k_q for which $\eta D(f_{\alpha_v})$ is not a square is $\frac{1}{2}q + O_n(q^{1/2})$, by a result of Perel'muter [16]. It follows by Lemma 6 that

$$\omega_2(\mathfrak{p}) = \tfrac{1}{2}q^s + O_n(q^{s-1/2}), \quad \mathfrak{p} \in \mathscr{S}. \tag{12}$$

To complete this stage we estimate $\omega_3^{(p)}(\mathfrak{p})$. This is more difficult. Again consider any $f_t \in f_t(\mathbf{t} - \{\alpha_v\}, k_{\mathfrak{p}})$ which is not an exception to Lemma 6. Taken together, all three conclusions of Lemma 6 imply that, in Lemma 5, (6) must hold, i.e. that

$$H_p(f_t, \bar{k}_{\mathfrak{p}}(t)) = C_p^{n-1} \times C_{\delta'}, \tag{13}$$

where

$$\delta' = \delta(f_t, p, \bar{k}_{\mathfrak{p}}) = \begin{cases} p & \text{if} \quad v = 0 \ \ \text{(so certainly if } n = 2), \\ 1 & \text{if} \quad v = 0, \end{cases}$$

while

$$H_p(f_t, k_{\mathfrak{p}}(t)) = C_p^{n-1} \times C_{\delta''}, \tag{14}$$

where

$$\delta''=\delta(f_t, p, k_{\mathfrak{p}})=\begin{cases}1 & \text{if} \quad v>0 \quad \text{and} \quad ((-1)^n\alpha_0/\alpha_n)^{1/\mathfrak{p}}\in k_q,\\ p & \text{otherwise.}\end{cases}$$

Now, if $f_t^{(p)}(y)=0$, (13) and (14) clearly imply that

$$H_p(f_t, \bar{k}_{\mathfrak{p}}(t, y))=C_p^{n-2}\times C_{\delta'} \quad \text{and} \quad H_p(f_t, \bar{k}_{\mathfrak{p}}(t, y))=C_p^{n-2}\times C_{\delta''}.$$

By [4, Lemma 1] and invoking the notation of Lemma 2, we therefore have

$$\begin{aligned}&|H_p(f_t, k_{\mathfrak{p}}(t, y)\cap G^*(f_t, k_{\mathfrak{p}}(t))|\\ &\quad=\begin{cases}p^{n-1} & \text{if} \quad v=0,\\ p^{n-2} & \text{if} \quad v>0 \text{ and } ((-1)^n\alpha_0/\alpha_n)^{1/\mathfrak{p}}\in k_{\mathfrak{p}},\\ (p-1)p^{n-2} & \text{otherwise}\end{cases}\\ &\quad>1.\end{aligned} \tag{15}$$

Observe that a non-identical member of $H_{\mathfrak{p}}(f_t, k_{\mathfrak{p}}(t, y)$, has cycle pattern $(1^{\lambda_1}, p^{\lambda_p})$, where $1\le\lambda_p\le n-1$, yet is trivial when restricted to $k_{\mathfrak{p}}(t, \mathbf{x})$. We may conclude from Lemma 2 and (15) that

$$\omega_3^{(p)}(\mathfrak{p})>(n!\,p^n)^{-1}q^s+O_{nr}(q^{s-1/2}). \tag{16}$$

We are now almost ready to apply Lemma 1. For each $i=1, 2, 3$ define $P_i(\boldsymbol{\alpha}, x)$, $P_i(x)$ as in the lemma. In each case, by (11), (12), (16), we have

$$P_i(N^{1/2})>c\,|\mathscr{S}|+R, \tag{17}$$

where $c=(n!\,p^n)^{-1}$ and $|R|\le\sum_{|\mathfrak{p}|\le N^{1/2}}|\mathfrak{p}|^{-1/2}=O_k(N^{1/4})$. Moreover, our hypothesis (1) implies that $|\mathscr{S}|>\frac{1}{2}|\Pi_{K/k}(N^{1/2})|+O(1)$. Employing these estimates in (17) together with the prime ideal theorem, we obtain

$$P_i(N^{1/2})>\tfrac{1}{2}cd^{-1}(N^{1/2}/\log N), \quad d=[K\colon k], \tag{18}$$

provided $N>N_0(K, nr)$.

We deduce from (18) by Lemma 1 that, for $i=1, 2, 3$, $P_i(\boldsymbol{\alpha}, N^{1/2})=0$ for at most $N^{s-1/2}\log N$ values of $\boldsymbol{\alpha}$ with $|\boldsymbol{\alpha}|\le N$. In particular, for each λ, this is true for P_1^λ. The argument on p. 98 of [12] yields the conclusion that possibility (I) above occurs for at most $N^{s-1/2}\log N$ members of $F(\mathbf{t}, \mathbf{Z}_k(N))$. Next, taking $i=2$, note that $P_2(\boldsymbol{\alpha}, N^{1/2})\ne 0$ implies that, for some $\mathfrak{p}$, $\eta(\delta(F_\alpha, r, K))D(F_{\boldsymbol{\alpha}})$ is not a square in $K_{\mathfrak{P}}$ and so, *a priori*, not a square in K. Thus (II) does not hold. Similarly, if $P_3(\boldsymbol{\alpha}, N^{1/2})\ne 0$ then (III) is not the case. This proves the theorem in the case $K=K(\zeta_r)$.

The deduction of the general case is not difficult. Put $K_1=K(\zeta_r)$. By the above and since K_1 is determined by K and r, we have that with $O_{K,rn}(N^{s-1/2}\log N)$ exceptions, all members F of $F(\mathbf{t}, \mathbf{Z}_k(N))$ satisfy

$$G(F, K_1)=S_n \quad \text{and} \quad H_r(F, K_1)=C_r^{n-1}\times C_\delta,$$

where $\delta = \delta(F_{\mathbf{t}}, r, K_1)$. Since K_1 is contained in the splitting field of $F\ (\neq \alpha_n X^n)$ over K, the theorem follows.

6. Proof of Lemma 5

Clearly we can assume that $r > 1$ and also that $n > 1$ for then (ii) holds. First note that since $L(\zeta_r) = L$, for any $\theta \in L$ a subfield of $L(\theta^{1/r})$ has the form $L(\theta^{d/r})$ where $d \mid r$. The first part of the proof is based on an argument of Richards [17]. As defined in §1, let $F(X) = (X - x_1) \cdots (X - x_n)$, where $y_i^r = x_i$, $i = 1, \ldots, n$. Observe that $(y_1 \cdots y_n)^d \in L$ if and only if $\delta \mid d$.

Now, if the conclusion (6) of the lemma holds then, for each $m = 0, \ldots, n$ we have

$$G(L(\mathbf{x}, y_1, \ldots, y_m)/L(\mathbf{x})) = \begin{cases} 1 & m = 0, \\ C_r^{m-1}, & 1 \leq m < n, \\ C_r^{n-1} \times C_\delta, & m = n. \end{cases} \tag{19}$$

Suppose, in fact, that (6) is false and fix m $(0 \leq m \leq n-1)$ as the largest integer for which (19) is true. Then the fact that $L(\zeta_r) = L$ means that

$$y_{m+1}^d \in L(\mathbf{x}, y_1, \ldots, y_m)$$

for some $d \mid r$ with $d < r$. Indeed, if $m = n-1$, then $d \mid \delta$ with $d < \delta$. Assume for the time being that $m > 0$. Let $\mathbf{j}$ denote any integral vector $(j_1, \ldots, j_m)$, where $0 \leq j_i \leq r-1$, $i = 1, \ldots, m$ and $\mathbf{Y}^{\mathbf{j}}$ the typical monomial $y_1^{j_1} \cdots y_m^{j_m}$. By (19), the set of all $\mathbf{Y}^{\mathbf{j}}$ forms a basis of the extension $L(\mathbf{x}, y_1, \ldots, y_m)/L(\mathbf{x})$. Hence there exist $h_{\mathbf{j}}(x) \in L(x)$ such that

$$y_{m+1}^d = \sum_{\mathbf{j}} h_{\mathbf{j}}(\mathbf{x}) \mathbf{Y}^{\mathbf{j}}. \tag{20}$$

Suppose $\mathbf{j}' \neq \mathbf{j}''$ are such that $h_{\mathbf{j}'}(\mathbf{x}) h_{\mathbf{j}''}(\mathbf{x}) \neq 0$ with $j_1' \neq j_1''$, say. Now (19) implies that there exists an automorphism $\sigma \in G(L(\mathbf{y})/L)$ such that

$$\sigma(y_1) = \zeta y_1,\ \sigma(y_i) = y_i, \quad i = 2, \ldots, m,\ \sigma(x_i) = x_i, \quad m < i \leq n,$$

where $\zeta = \zeta_r$, a *primitive* rth root of unity. In particular, $\sigma(y_{m+1}^d) = \zeta^e y_{m+1}^d$ for some integer e. Applying σ to (20) we get

$$\begin{aligned} 0 &= \zeta^e y_{m+1}^d - \sigma(y_{m+1}^d) \\ &= (\zeta^e - \zeta^{j_1'}) h_{\mathbf{j}'} \mathbf{Y}^{\mathbf{j}'} \\ &\quad + (\zeta^e - \zeta^{j_1''}) h_{\mathbf{j}''} \mathbf{Y}^{\mathbf{j}''} + (\text{terms in } \mathbf{Y}^{\mathbf{j}} \text{ for each } \mathbf{j} \neq \mathbf{j}', \mathbf{j}''). \end{aligned} \tag{21}$$

However, $\zeta^e - \zeta^{j_1'}$ and $\zeta^e - \zeta^{j_1''}$ are not both 0; hence (21) contradicts the fact that the $\mathbf{Y}^{\mathbf{j}}$ form a basis of $L(\mathbf{x}, y_1, \ldots, y_m)/L(\mathbf{x})$. Consequently, there exists $\mathbf{j}$ such that

$$y_{m+1}^d = h_{\mathbf{j}}(\mathbf{x}) y_1^{j_1} \cdots y^{j_m}$$

and hence that

$$x_{m+1}^{d}=h_{\mathbf{j}}^{r}(\mathbf{x})x_{1}^{j_1}\cdots x^{j_m}. \qquad (22)$$

From (22) we deduce the existence of integers $d_1,\ldots,d_n$ not all 0 with $0\leq d_i\leq r-1$ $(i=1,\ldots,n-1)$, $0\leq d_n\leq \delta-1$ such that

$$x_1^{d_1}\cdots x_n^{d_n}\in L_r(\mathbf{x})=\{r\text{th powers in } L(\mathbf{x})\}. \qquad (23)$$

Further (23) remains valid when $m=0$.

Suppose that in (23) not all the d_i's are equal with $d_1\neq d_2$, say. Since $G(L(\mathbf{x})/L)=S_n$, this group contains the transposition $\sigma=(x_1x_2)$. Application of σ to (23) yields

$$(x_1/x_2)^{d_1-d_2}\in L_r(\mathbf{x}),\quad 0\leq d_1,\quad d_2\leq r-1. \qquad (24)$$

If follows from (24) that for some $u\mid r$ with $u<r$ we have $(x_1/x_2)^u\in L_r(x)$. Since $G(L(\mathbf{x})/L)$ is certainly 2-transitive, we deduce that $(x_i/x_j)^u\in L_r(\mathbf{x})$ for any pair of roots x_i, x_j. Hence $(y_i/y_j)\in L(\mathbf{x})$ and (ii) holds for any prime $p\mid(r/u)$.

It remains to discuss the case in which $d_1=\cdots=d_n$ $(<\delta)$ in (23). In fact, if d is now the least positive integer for which $(x_1\cdots x_n)^d\in L_r(\mathbf{x})$, then certainly $d\mid\delta$. Equivalently, we have $(y_1\cdots y_n)^d\in L(\mathbf{x})$ and so $\beta=((-1)^n\alpha_0/\alpha_n)^{d/r}\in L(\mathbf{x})\,L$. By Galois theory

$$(G(L(\mathbf{x})/L))/(G(L(\mathbf{x})/L(\beta)))\cong G(L(\beta)/L)\cong C_{\delta/d},$$

where $\delta/d\geq 2$. But $G(L(\mathbf{x})/L=S_n$ has A_n as its commutator subgroup whence $G(L(\mathbf{x})/L)=A_n$. On the other hand $G(L(\mathbf{x})/L(\sqrt{D(F)}))=A_n$. Accordingly, $\delta=2d$ and $L(\sqrt{D(F)})=L(\beta)$ from which it follows easily that $\sqrt{D(F)}/\beta\in L$ and hence that $D(F)=\eta(\delta)$ (square in L) which implies that (7) holds. This completes the proof.

7. Some results on algebraically closed fields

Our goal in this section is to provide some results concerning the algebraically closed field $\bar{k}_q(t)$ necessary for a proof of Lemma 6. In fact, we shall consider the general situation in which L is an arbitrary algebraically closed field and n is an integer with char $L>n$. (This restriction on characteristic could easily be weakened but it suffices for our purpose and facilitates the discussion.) The work is related to material in [1], [5] and [13].

It is convenient to use a concept of the cycle pattern or splitting type of a polynomial differing from that introduced in §3. Suppose that the polynomial $f(X)$ of degree n in $L[X]$ has a prime decomposition involving μ_i (linear) factors of multiplicity i for each $i=1,2,3,\ldots$ so that $\sum_i i\mu_i=n$. We shall say that f has *(repeated) cycle pattern* $\mu=(1^{\mu_1},2^{\mu_2},\ldots)$ *of degree* n and write $\mu(f)=\mu$. Indeed, even if $g(X)$ $(\neq 0)\in L[X]$ has degree $d<n$, introduce an element ∞ and define $\mu(g)$ to be the cycle pattern of $(X-\infty)^{n-d}g(X)$.

LEMMA 7. *Let g, h be relatively prime polynomials in $L[X]$ with $n = \deg g > \deg h \geq 0$. Put $f_t = g + th$ and for $\alpha \in L' = L \cup \{\infty\}$ extend the meaning of f_α to L' by defining $f_\infty = h$. Then each $\alpha \in L'$ induces a permutation σ_α in $G(f_t, L(t))$ having cycle pattern $\mu(f_\alpha)$. Moreover, for any β in L', $G(f_t, L(t))$ can be generated by the set of σ_α, $\alpha \neq \beta$.*

Proof. At various points this involves the theory of local fields for which we refer to [2, Chapter 1].

For $\alpha \in L$ let P_α denote the prime divisor of $L(t)$ corresponding to $t - \alpha$ and let P_∞ be the "infinite" prime. Suppose $f_t(x) = 0$ and let $\{e_i\}$, say, be the set of ramification numbers (included in accordance with their multiplicity) of the ramified primes in $L(x)$. Since all ramification is tame and $L(x)$ has genus 0, it follows from the Hurwitz genus formula that

$$\sum_i (e_i - 1) = \text{degree of the different of } L(x) = 2n - 2.$$

On the other hand $t - \alpha = -f_\alpha(x)/h(x)$ $(\alpha \in L)$ and so P_α is ramified to at least the extent that $f_\alpha(x)$ has repeated factors in $L[x]$. Similarly, the ramification of P_∞ is at least as great as the cycle pattern of $f_\infty(x) = h(x)$. Moreover, if $\{e_i'\}$ is the set of all multiplicities of the factors (including infinite factors) in any $f_\alpha(\alpha \in L')$, then, by considering the formal derivative $(g/h)'$ and taking into account the multiplicity of $x - \infty$, we see that

$$\sum_i (e_i' - 1) = (n + \deg g - 1) + (n - \deg g - 1) = 2n - 2.$$

Accordingly, the ramification of P_α in $L(x)$ can be read off from $\mu(f_\alpha)$. Furthermore, if $L_\alpha(t)$ denotes the P_α-adic completion of $L(t)$ (the field of formal power series in $t - \alpha$ or $1/t$ if $\alpha = \infty$) then $\lambda(f_t)$ the splitting type (in the original sense) of f_t over $L_\alpha(t)$ is the same as $\mu(f_\alpha)$.

Next consider the extension $L(\mathbf{x})$, where $\mathbf{x}$ is a complete set of roots of $f_t(X) = 0$. Then P_α is ramified in $L(\mathbf{x})$ if and only if it is ramified in $L(x)$. Let $\mathcal{P}$ be a ramified prime in $L(\mathbf{x})$ such that $\mathcal{P}$ divides P_α in $L(t)$ and denote by $L_\alpha(\mathbf{x})$ the $\mathcal{P}$-adic completion of $L(x)$. Then the ramification number of $\mathcal{P}$ over $L(t)$ is given by $e = [L_\alpha(\mathbf{x}): L_\alpha(t)]$ and, in fact, $L_\alpha(\mathbf{x}) = L_\alpha(t, (t - \alpha)^{1/e})$. Thus $G(L_\alpha(\mathbf{x})/L_\alpha(t))$ is cyclic being generated by $\sigma_\alpha: (t - \alpha)^{1/e} \to \zeta_e (t - \alpha)^{1/e}$. Obviously, σ_α acting on the roots of f_t over $L_\alpha(t)$ has cycle pattern $\lambda(f_t)$ $(= \mu(f_\alpha)$ as shown above). Since clearly $G(f_t, L_\alpha(t))$ can be regarded as a subgroup of $G(f_t, L(t))$, the existence of σ_α is established.

For the remaining part, without loss of generality, we set $\beta = \infty$ and let H be the subgroup of $G(f_t, L(t))$ generated by the decomposition groups of all the ramified primes $\mathcal{P}$ of $L(\mathbf{x})$ not dividing P_α, i.e. H is generated by $\{\sigma_\alpha, \alpha \neq \beta\}$. Let E be the fixed field of H. The only prime of $L(t)$ which can ramify in $E/L(t)$ is P_∞. By the Hurwitz formula, $2g_E - 2 = -2m + \deg \mathcal{D}_E$, where $m=[E: L(t)]$ and g_t and $\mathscr{D}_E$ are the genus and different of E. Let $e_1, \ldots, e_u$ be the ramification numbers of all primes of E dividing P_∞. Since all ramification is tame

$$m-u=\sum_{i=1}^{u}(e_i-1)=\deg \mathscr{D}_E=2g_E-2+2m.$$

Therefore $m+u=2-2g_E$. Since $g_E \geq 0$ then $m=u=1$. Hence $E=L(t)$ and the proof is complete.

The above proof has been adapted from the work of Hayes [13]. Alternatively, we could have derived the lemma along the lines of [1] but employing the abstract Riemann surface for $f_t(x)$ over $L(x)$ and Puiseux expansions, cf. [9]-[11].

For the next two lemmas we require a definition. A polynomial $f(X) \in L[X]$ will be called *simple* if it is square-free apart, possibly, from a linear factor of multiplicity 2, i.e. if $\mu(f)=(1^n)$ or $(1^{n-2}, 2)$. (In [5], in place of simple the term *normal* was used.)

LEMMA 8. *In the situation of Lemma* 7, *suppose f_α is simple for all* (*finite*) *$\alpha \in L$. Then $G(f_t, L(t))=S_n$ and $D(f_t)$ is square-free.*

Proof. By Lemma 7 with $\beta=\infty$, $G(f_t, L(t))$ is generated by transpositions. It is, of course, a transitive group and consequently must be S_n. The rest is clear since any prime in $L(x)$ can have ramification number at most 2.

The main application of the next lemma (which is a modification of results in [5]) is to show that under certain conditions $G(F_{\mathbf{t}}, L(\mathbf{t}))=S_n$. We define a concept used in its statement. A set of polynomials $g_0, \ldots, g_s$ $(s \geq 1)$ in $L[X]$ is *totally composite* if there exist polynomials $h_0, \ldots, h_s \in L[X]$ with $d=\max_i \deg h_i>1$ and a rational function $\phi=(\phi_1/\phi_2)$, where $\phi_1, \phi_2 \in L[X]$ with $\max(\deg \phi_1, \deg \phi_2)>1$, such that $g_i=\phi_2^d h_i(\phi)$, $i=0, \ldots, s$.

LEMMA 9. *Let $g_0, \ldots, g_s$ $(s \geq 2)$ be a set of relatively prime polynomials in $L[X]$, linearly independent over L, not totally composite and with*

$$n=\max_i \deg g_i>\deg g_s \geq 0.$$

Assume that the highest common factor $(g_0-\beta_0 g_s, \ldots, g_{s-1}-\beta_{s-1} g_0)$ is simple for all $\boldsymbol{\beta}=(\beta_0, \ldots, \beta_{s-1}) \in L^s$ except possibly $\boldsymbol{\beta}=\mathbf{0}$. Then for all $\boldsymbol{\alpha}=(\alpha_1, \ldots, \alpha_{s-1})$ not belonging to a certain set of hyperplanes in L^{s-1} (*bounded in number by a constant dependent only on n*), *the polynomial*

$$f_\alpha=(g_0+\alpha_1 g_1+\cdots+\alpha_{s-1} g_{s-1})+\alpha g_s$$

is simple if $\alpha \in L \backslash\{0\}$ while f_0/g (*where $g=(g_0, \ldots, g_{s-1})$*) *is simple, indeed square-free, if $\boldsymbol{\alpha}$ is not also on a curve of bounded degree.*

Proof. Basically the proof is a straightforward modification of Lemmas 6 and 7 of [5] with the simplification here that char $L>n$. The fact that g need not be simple means only that we may have to exclude from consideration throughout values of x for which $g_i(x)=0$ simultaneously for all $i=0,\ldots,s-1$. Since $(g, g_s)=1$ this only affects f_0. Observing that all the error terms $O(q^{s-2})$ in [5] arose from consideration of $\boldsymbol{\alpha}$ on a bounded number of hyperplanes, we obtain the results on simplicity.

Further f_0/g is square-free unless $D(f_0/g)=0$. But when $\boldsymbol{\alpha}$ is regarded as a set of indeterminates f_0/g is clearly square-free so that $D(f_0/g)=0$ determines a curve as required.

8. Proof of Lemma 6

Assume that char $k_q > nr$ throughout. We write L for $\overline{k_q}$ and use the results of §7.

We discuss first the case $v>0$; thus we consider the set

$$\mathcal{S}=f_t(\mathbf{t}-\{\alpha_v\}, k_q) \quad \text{where} \quad f_t(X)=\sum_{\substack{i=0\\ i\neq v}}^{n}\alpha_i X^i + t(X^u+X^v),$$

(where $u\neq n$). Apply Lemma 9 with

$$g_0(X)=\sum_{i\notin\tau}\alpha_i X^i, \quad g_i(X)=X^{w_i} \quad \text{where} \quad \tau\backslash\{u,v\}=\{w_1,\ldots,w_{s-2}\},$$
$$g_{s-1}(X)=X^u, \qquad g_s(X)=X^u+X^v, \quad v>0.$$

Since $X\nmid(g_0-\beta g_s)$ for all $\beta\in L$ and that part of $\gamma X^u+\delta X^v$ prime to X is square-free then $(g_0-\beta_0 g_s,\ldots,g_{s-1}-\beta_{s-1}g_s)$ is square-free and so simple for all $(\beta_0,\ldots,\beta_{s-1})$ in L^s. The other conditions of Lemma 9 are clearly satisfied. By Lemmas 8 and 9, $G(f_t, L(t))=S_n$ and $D(f_t)$ is square-free for all but $O_n(q^{s-2})f_t$ in $\mathcal{S}$, i.e. certainly (i) and (ii) of Lemma 6 hold.

To establish (iii) of Lemma 6, let p be a prime dividing r. Suppose that f is one of the non-exceptional members of $\mathcal{S}$ for which (i) and (ii) hold. By Lemma 5, if (iii) does not hold, then $H_p(f, L(t, y))$ is trivial. We show that the latter is not the case by considering the permutation $\sigma_\infty\in G(f_t^{(p)}, L(t))$ constructed in Lemma 7. Since $X^{pu}+X^{pv}=(X^{p(u-v)}+1)X^{pv}$ and $X^{p(u-v)}+1$ is square-free, σ_∞ has cycle pattern $(1^{p(u-v)}, pv, p(n-u))$ (where possibly $v\geq n-u$) while ρ (which is defined to be σ_∞^p restricted to $G(f_t, L(t))$) has cycle pattern $(1^{u-v}, v, n-u)$. Let the roots $\mathbf{x}$ of $f_t(X)=0$ be numbered so that

$$\rho=(x_1\cdots x_v)(x_{n-u+1}\cdots x_n).$$

Then $y_i=x_i^{1/p}$ and ζ a primitive pth root of unity can be chosen in such a way that

$$\sigma=(Y_1\zeta Y_1\cdots\zeta^{p-1}Y_1)(Y_2\zeta^j Y_2\cdots\zeta^{j(p-1)}Y_2),$$

where $Y_1=y_1\cdots y_v$, $Y_2=y_{u+1}\cdots y_n$ and $1\leq j\leq p-1$. Put

$$m=\text{l.c.m.}\,\{v, n-u\}$$

so that $p \nmid (m/v, m/(n-u))$. Then σ^m fixes $L(\mathbf{x})$. On the other hand σ'^m fixes y_u but does not fix at least one of y_1 or y_n. Hence $H_p(f_t, L(y_u))$ is not trivial. This completes the proof in this case.

To the extent that we could, by means of Lemmas 7–9, show directly that (i)–(iii) of Lemma 6 hold simultaneously, the above argument is fortuitous. Unfortunately when $v=0$ this does not seem possible and we are compelled to modify the discussion. We employ a final lemma. It contains the device of appealing to the distribution of $(n-1)$-cycles to overcome the difficulty of dealing with (possibly) non-regular extensions.

LEMMA 10. *Suppose* $F_{\{\alpha_u,\alpha_0\}}(X)$ $(=\sum_{i=0}^n \alpha_i X^i)$ *in* $k_q[\alpha_0, \alpha_u, X]$ *is primitive of degree n. Then all but* $O_n(q^{1/2})$ *members* F_t *of* $F_t(\{\alpha_u\}, k_q)$ $(t=\alpha_0)$ *satisfy*:

(i) $G(F_t, L(t)) = S_n$,

(ii) *the part of* $D(F_t)$ *prime to t is square-free,*

(iii) *the part of* F_0 *prime to X is square-free.*

Proof. Case (i) $u \neq n$. In Lemma 9 put

$$g_0(X) = \sum_{\substack{i=1 \\ i\neq u}}^{n} \alpha_i X^i, \quad g_1(X)=1, \quad g_2(X)=X^u.$$

Then $(g_0-\beta_0 g_2, g_1-\beta_1 g_2)$ is square-free for all $(\beta_0, \beta_1)\in L^2$ and the other conditions of Lemma 9 are obviously satisfied. Hence, if $f_t = g_0+\alpha_0 - tg_1$ then $G(f_t, L(t)) = S_n$ for all but $O_n(1)$ members f_t of $f_t(\alpha_0, k_q)$. We conclude using Lemma 2 that the number of F in $F(\{\alpha_0, \alpha_u\}, k_q)$ for which the splitting type $\lambda(F) = (1, n-1)$ is

$$q^2/n(n-2)! + O_n(q^{3/2}). \tag{25}$$

The estimate (25) has been established by first fixing α_0 and letting α_u vary and then letting α_0 vary. To obtain our result we perform this procedure in the opposite order and compare the answer with (25). Specifically, apply Lemma 9 with g_0 as before but with $g_1(X)=X^u$, $g_2(X)=1$. Then $(g_0-\beta_0, g_1-\beta_1)$ is square-free provided $(\beta_0, \beta_1)\neq(0,0)$. Consequently for all but $O_n(1)$ values of α_u in k_q, $g_0(X)+\alpha_u X^u+\alpha_0$ is simple for all $\alpha_0 \neq 0$ while $g_0(X)+\alpha_u X^u$ is square-free apart from a factor X^w where $X^w = (g_0(X), X^u)$ so that $1\leq w\leq u\leq n-1$. So in the first place assertion (iii) holds. Moreover, by Lemma 7, for a non-exceptional α_u, if $t=\alpha_0$, then $D(F_t)$ is square-free apart from a factor t^{w-1} and $G(F_t, L(t))$ is generated by transpositions along with a w-cycle. In particular assertion (ii) of the lemma is valid. Further, since

$$G(F_t, k_q(t)) \supseteq G(F_t, L(t))$$

the former group contains a transposition. Now $G(F_t, k_q(t))$ may or may not contain an $(n-1)$-cycle. First, suppose that it does. Then, being transitive in addition to possessing an $(n-1)$-cycle and a transposition, it follows by a simple, well-known argument that $G(F_t, k_q(t)) = S_n$. In this case, $G(F_t, L(t))$ being a normal subgroup of $G(F_t, k_q(t))$ if not S_n must be A_n which is impossible by (ii). (An exceptional case (which occurs when $n = 4$) that $G(F_t, L(t))$ is a dihedral group can be ruled out by Theorem 1 of [9] or by easy direct arguments.) We conclude that $k_q(\mathbf{x})/k_q(t)$ is a regular extension with $G(F_t, k_q(t)) = S_n$ and consequently that for such an F_t, $\lambda(F_{\alpha_0}) = (1, n-1)$ for

$$q/n(n-2)! + O_n(q^{1/2}) \tag{26}$$

values of α_0. On the other hand, if $G(F_t, k_q(t))$ does not contain an $(n-1)$-cycle then $\lambda(F_{\alpha_0}) \neq (1, n-1)$ for all α_0. Comparison of (25) and (26) then implies that $G(F_t, k_q(t))$ must contain an $(n-1)$-cycle for all but $O_n(q^{1/2})$ values of α_u, whence $G(F_t, L(t)) = S_n$ for all but $O_n(q^{1/2})$ values of α_u.

Case (ii) $u = n$. This time in Lemma 9, take

$$g_0(X) = X^n, \quad g_1(X) = 1, \quad g_2(X) = \sum_{i=1}^{n} \alpha_i X^i.$$

Then $(X^n - \beta_0 g_2, 1 - \beta_1 g_2)$ divides $\beta_1 X^n - \beta_0$ but is prime to X and so is square-free. Therefore for all but $O_n(1)$ values of α_0,

$$G(X^n + \alpha_0 + tg_2(X), L(t)) = S_n.$$

Hence the number of pairs (α_0, α_n) for which $\lambda(X^n + \alpha_0 + \alpha_n g_2(X)) = (1, n-1)$ is given by (25). It is easy to see that (25) is therefore also a valid estimate for the number of F in $F(\{\alpha_0, \alpha_n\}, k_q)$ for which $\lambda(F) = (1, n-1)$. The remainder of the proof follows exactly as in case (i).

Finally we give the proof of Lemma 6 for the case $v = 0$. It follows from Lemma 10 (and Lemma 6 of [5]) that, if $f_t = \sum_{i=1, i\neq u}^{n} \alpha_i X^i + t$, as in the statement of Lemma 6, then f_t satisfies assertions (i) and (ii) for all but $O(q^{s-3/2})$ members of $f_t(\mathbf{t} - \{\alpha_0\}, k_q)$. Moreover, by Lemma 10(iii), for some w with $1 \leq w \leq n-1$, f_0/X^w is square-free and prime to X. To demonstrate the non-triviality of $H_p(f_t, L(t, y))$ for any $p \mid r$, consider the permutation $\sigma_0 \in G(f_t^{(p)}, L(t, y))$ constructed in Lemma 7. We have, for an appropriate choice of $y_i = x_i^{1/p}$ and $\zeta = \zeta_p$,

$$\sigma_0 = (Y \zeta Y \cdots \zeta^{p-1} Y), \quad Y = y_1 \cdots y_w.$$

Hence $\sigma_0^w \in H_p(f_t, L(t, y_n))$ but $\sigma_0^w(y_1) \neq y_1$. Consequently $H_p(f_t, L(t, y))$ is non-trivial and the proof is completed as in the case $v > 0$.

References

1. B. J. Birch and H. P. F. Swinnerton-Dyer, *Note on a problem of Chowla*, Acta Arith., vol. 5 (1959), pp. 417–423.
2. J. W. S. Cassels and A. Fröhlich (Editors), *Algebraic number theory*, Academic Press, London and New York, 1967.

3. S. D. Cohen, *The distribution of polynomials over finite fields*, Acta Arith., vol. 17 (1970), pp. 255–271.
4. ———, *The distribution of polynomials over finite fields, II*, Acta Arith., vol. 20 (1972), pp. 53–62.
5. ———, *Uniform distribution of polynomials over finite fields*, J. London Math. Soc. (2), vol. 6 (1972), pp. 93–102.
6. S. D. Cohen and R. W. K. Odoni, *The Farey density of norm subgroups of global fields* (II), Glasgow Math. J., vol. 18 (1977), pp. 57–67.
7. K. Dörge, *Über die Steltenheit der reduziblen Polynome*, Math. Ann., vol. 95 (1926), pp. 247–256.
8. M. Eichler, *Introduction to the theory of algebraic numbers and functions*, Academic Press, New York and London, 1966.
9. M. Fried, *On a conjecture of Schur*, Michigan Math. J., vol. 17 (1970), pp. 41–55.
10. ———, *Arithmetical properties of function fields* (*II*), Acta Arith., vol. 25 (1974), pp. 225–258.
11. ———, *On Hilbert's Irreducibility Theorem*, J. Number Theory, vol. 6 (1974), pp. 211–231.
12. P. X. Gallagher, *The large sieve and probabalistic Galois theory*, Proc. Sympos. Pure Math., Amer. Math. Soc., vol. 24 (1973), pp. 91–101.
13. D. R. Hayes, *The Galois group of* $x^n + x - t$, Duke Math. J., vol. 40 (1973), pp. 459–461.
14. H. Hering, *Über Koeffizientenbeschränkungen affektloser Gleichungen*, Math. Ann., vol. 195 (1972), pp. 121–136.
15. S. Lang, *Diophantine Geometry*, Interscience, New York and London, 1962.
16. G. I. Perel'muter, *On certain sums of characters*, Uspektii Matematicheskikh Nauk., vol. 18 (1963), pp. 145–149.
17. I. Richards, *An application of Galois theory to elementary arithmetic*, Advances in Math., vol. 13 (1974), pp. 268–273.
18. B. L. van der Waerden, *Die Steltenheit der Gleichungen mit Affekt*, Math. Ann., vol. 109 (1934), pp. 13–16.
19. R. J. Wilson, *The large sieve in algebraic number fields*, Mathematika, vol. 16 (1969), pp. 189–204.
20. P. Lefton, *On the Galois groups of cubics and trinomials*, Bull. Amer. Math. Soc., vol. 82 (1976), pp. 754–756.
21. J. H. Smith, *General trinomials having symmetric Galois group*, Proc. Amer. Math. Soc., vol. 63 (1977), pp. 208–212.

University of Glasgow
Glasgow, Scotland