J. Austral. Math. Soc. (*Series A*) **58** (1995), 312–357

ON SCHUR'S CONJECTURE

GERHARD TURNWALD

(Received 4 March 1992; revised 30 June 1992)

Communicated by R. Lidl

Abstract

We study polynomials over an integral domain R which, for infinitely many prime ideals P, induce a permutation of R/P. In many cases, every polynomial with this property must be a composition of Dickson polynomials and of linear polynomials with coefficients in the quotient field of R. In order to find out which of these compositions have the required property we investigate some number theoretic aspects of composition of polynomials. The paper includes a rather elementary proof of 'Schur's Conjecture' and contains a quantitative version for polynomials of prime degree.

1991 *Mathematics subject classification* (*Amer. Math. Soc.*): 11T06, 12E05.

Contents

Introduction

A polynomial $f(x)$ with coefficients in an integral domain R is said to be a *permutation polynomial* (abbreviated as p.p.) modulo an ideal I of R if the mapping induced on the residue class ring R/I is bijective. For $R = \mathbb{Z}$ it has long been known

that every composition of Dickson polynomials (defined in 1.1) with degrees coprime with 6 is a p.p. for infinitely many primes p (that is, is a p.p. mod(p)). Conversely, Schur proved in 1923 that every integral polynomial of prime degree which is a p.p. for infinitely many p is, up to linear transformations, a Dickson polynomial. The conjecture that every integral polynomial which is a p.p. for infinitely many p is a composition of linear polynomials and Dickson polynomials came to be known as 'Schur's Conjecture'. By means of very troublesome computations subsequent authors extended Schur's approach to prove the conjecture in more general cases, for example if the degree is a product of two odd prime powers. A breakthrough came in 1970 when M. Fried essentially proved a general version of the conjecture for every R which is the ring of algebraic integers of an algebraic number field. He observed that a polynomial which is a p.p. for infinitely many prime ideals can be written as a composition of indecomposable polynomials $f(x)$ such that the polynomial $(f(x) - f(y))/(x - y)$ is not absolutely irreducible. Schur's Conjecture thus follows from the implication '(iii) implies (i)' of (the number field case of) the following result.

THEOREM 1. *Let K be a field and $f(x) \in K[x]$ be a tame polynomial of degree $n > 1$. Then the following assertions are equivalent.*

(i) *$(f(x) - f(y))/(x - y)$ is absolutely irreducible.*

(ii) *$(f(x) - f(y))/(x - y)$ is irreducible over $K(\zeta)$ where ζ is a primitive n-th root of unity.*

(iii) *$f(x)$ is indecomposable and if n is an odd prime then we do not have $f(x) = \alpha D_n(a, x + b) + c$ for $\alpha, a, b, c \in K$ with $a = 0$ if $n = 3$.*

(Every polynomial is tame if char$K = 0$; if char$K = p > 0$ then all polynomials of degree less than p are tame (Definition 4.1); $f(x)$ is indecomposable if and only if it cannot be written as a composition of two polynomials of degree greater than one; $D_n(a, x)$ is the Dickson polynomial of degree n with parameter a.)

Theorem 1 also yields the following general form of Schur's Conjecture which applies to arbitrary subrings of the ring of algebraic integers of any number field and to polynomial rings (in one variable) over finite fields.

THEOREM 2. *Let K be the quotient field of an integral domain R such that R/I is finite for every non-zero ideal I and let $f(x) \in R[x]$ be a tame polynomial which is a p.p. for infinitely many prime ideals of R. Then $f(x)$ is a composition of linear polynomials $\alpha_i x + \beta_i \in K[x]$ and Dickson polynomials $D_{n_j}(a_j, x)$ with $a_j \in R$ where every n_j is an odd prime and $a_j = 0$ if $n_j = 3$.*

In the following three theorems we assume that R is the ring of algebraic integers of some number field K. In this situation we can make Theorem 2 much more precise.

THEOREM 3. *Let $f(x) \in R[x]$ be a composition of linear polynomials $\alpha_i x + \beta_i \in K[x]$ and Dickson polynomials $D_{n_j}(a_j, x)$ with $a_j \in R$. Choose $c \in R$, $c \neq 0$, such that $c\alpha_i, c\beta_i \in R$ for all i. Then $f(x)$ is a p.p. for infinitely many prime ideals of R if and only if $f(x)$ is a p.p. for some non-zero prime ideal not dividing* $\deg(f)\, c \prod c\alpha_i \prod_{a_j \neq 0} a_j$.

THEOREM 4. *Let $f(x) \in R[x]$ have leading coefficient a and degree $n > 1$. If n is not divisible by any ramified prime then the following conditions are equivalent:*

(i) *$f(x)$ is a p.p. mod P for infinitely many prime ideals P of R.*

(ii) *$a^{n-1} f(x) = (f_1 \circ \ldots \circ f_r)(ax)$ where $f_i(x) = D_{n_i}(a_i, x + b_i) + c_i$ with suitable $a_i, b_i, c_i \in R$ and odd primes n_i such that $a_i = 0$ if $n_i = 3$.*

(iii) *n is odd and $f(x)$ is a p.p. for every prime ideal P of degree one with $NP \equiv 2 \bmod n$ and $a \notin P$.*

THEOREM 5. *Let $f(x) \in R[x]$ have prime degree n and assume that the image of every coefficient under every embedding of K into $\mathbb{C}$ has modulus at most C; put $d = [K : \mathbb{Q}]$. If there exists a prime ideal P of norm at least $(nC)^{nd}$ such that $f(x)$ is a p.p. mod P then $n \geq 3$, $f(x)$ is linearly related (over K) to $D_n(a, x)$ for some $a \in K$, and $f(x)$ is a p.p. for infinitely many prime ideals.*

In Section 1 various properties of the Dickson polynomials are collected. In particular, the factorization of $D_n(a, x) - D_n(a, y)$ in $\bar{K}[x, y]$ is given. In Section 2 we study polynomials with coefficients in an integral domain with respect to composition. Moreover it is shown that if R is a Dedekind domain and n is not divisible by any ramified prime $D_n(a, x + b) + c \in R[x]$ implies $a, b, c \in R$ except for some special cases. In Section 3 we consider the Galois group G_f of $f(x) - t$ over $K(t)$. The connection between properties of $f(x)$ and properties of the permutation group G_f is an important ingredient for the proof of Theorem 1. As an application we present a general class of polynomials $f(x)$ such that G_f is the symmetric group and classify the polynomials for which G_f is solvable. This generalizes work of Hilbert and Ritt, respectively, for $K = \mathbb{C}$.

The main results are proved in Section 4. For the proof of Theorem 1 (=Theorem 4.5) use is made of two theorems of Burnside and Schur on primitive permutation groups. Theorem 2 follows from Lemma 4.10 and Theorem 4.9 where more general rings (including all Dedekind domains) are considered. The main tools of the proof are Theorem 1 and a special case of Weil's estimate of the number of points on an absolutely irreducible curve over a finite field. (See Remark 4.16.) Theorem 3 is obvious from Remark 4.21 and the equivalence of (i), (ii) in Theorem 4.30. Theorem 4.30 and Theorem 4.32 (both originating from the work of Matthews) are the main results of a considerable portion of Section 4 (starting with 4.21 and ending with 4.33) devoted to the problem of determining under which circumstances $D_n(1, x)^m$ is a p.p.

for infinitely many prime ideals in a given number field. Theorem 4 is contained in Theorem 4.34 which follows from Theorem 2 together with a generalization of Dirichlet's theorem on primes in an arithmetic progression. Theorem 5 is an immediate consequence of Theorem 4.17 (where additional information is provided) and Theorem 4.37. In Section 5 we conclude with comments on the history of Schur's Conjecture and its solution.

This work grew out of an attempt to give a short and reasonably self-contained proof of a correct version of Schur's Conjecture; with very few exceptions, the versions appearing in the literature are fallacious. The proof of Theorem 2, however, requires only a small portion of the results presented here. (See Remark 4.16) Apart from the mentioned theorems of Burnside, Schur, and Weil, only quite elementary results are needed. In particular, we do not employ the theory of Riemann surfaces. Special attention is paid to the fact that one cannot assume $\alpha_i x+\beta_i \in R[x]$ in Theorem 2.

A polynomial with coefficients in a field K is said to be *linearly related* to a Dickson polynomial if it is of the form $\alpha D_n(a, \gamma x+\delta)+\beta$ where $a, \alpha, \beta, \gamma, \delta$ belong to some extension field L of K (such that x is transcendental over L). If I is an ideal of an integral domain R then, as is usual in the case where R is a ring of algebraic integers, we call $|R/I|$ the *norm* of I and denote it by NI. If P is a non-zero prime ideal of a Dedekind domain R with quotient field K then, for every $a \in K$, $v_P(a)$ denotes the multiplicity of P in the fractional ideal (a). A rational prime p is called *ramified* (in K) if $v_P(p) > 1$ for some P. The sets $P(m, n; K)$ appearing in several results in Section 4 are defined in 4.21. $P(m, n; K)$ is the set of non-zero prime ideals P in K such that $D_n(1, x)^m$ is a p.p. mod P.

1. Dickson polynomials

R denotes an integral domain with quotient field K (with algebraic closure $\bar{K}$).

LEMMA 1.1. *For every $a \in R$ and every positive integer n there is a unique polynomial $D_n(a, x) \in R[x]$ such that $D_n(a, x+(a/x)) = x^n+(a/x)^n$. The polynomial $D_n(a, x)$ is monic of degree n and the coefficients are integral polynomials in a. The following properties hold (for all $a, b \in R$ and $m, n \geq 1$):*

(i) $D_1(a, x) = x$, $D_2(a, x) = x^2-2a$, $D_{n+2}(a, x) = xD_{n+1}(a, x)-aD_n(a, x)$.

(ii) $D_n(0, x) = x^n$, $D_{mn}(a, x) = D_m(a^n, D_n(a, x))$, $b^n D_n(a, x) = D_n(b^2 a, bx)$.

(iii) $D_n(a, x) = \sum_{k=0}^{[n/2]} (n/(n-k))\binom{n-k}{k}(-a)^k x^{n-2k}$; *$[n/2]$ denotes the largest integer $\leq n/2$. Thus $D_n(a, x) = x^n - nax^{n-2}+\cdots+(n/2)^2(-a)^{(n/2)-1}x^2+2(-a)^{n/2}$ for even n and $D_n(a, x) = x^n - nax^{n-2}+\cdots+n(-a)^{(n-1)/2}x$ for odd n.*

https://doi.org/10.1017/S1446788700038349 Published online by Cambridge University Press

(iv) *If* $p = \mathrm{char}R > 0$ *then* $D_{np}(a, x) = D_n(a, x)^p$.

PROOF. The uniqueness is clear. For $n = 1$ and $n = 2$ the polynomials x and $x^2 - 2a$, respectively, have the required property and inductively we see that this also holds for the polynomials defined by the recurrence relation, thus proving the existence of $D_n(a, x)$ and (i).

Obviously, $D_n(0, x) = x^n$; the second part of (ii) holds since $D_{mn}(a, x + (a/x)) = x^{mn} + (a/x)^{mn} = D_m(a^n, x^n + (a/x)^n)$ and the last part follows from $b^n D_n(a, x + (a/x)) = b^n(x^n + (a/x)^n) = (bx)^n + (b^2 a/bx)^n$.

From (i) it is immediately seen that $D_n(a, x)$ is a monic polynomial of degree n and the coefficients are integral polynomials in a. The explicit formula in (iii) is established inductively by a simple calculation using the recurrence relation.

Part (iv) follows from $x^{np} + (a/x)^{np} = (x^n + (a/x)^n)^p$.

DEFINITION 1.2. The unique polynomial $D_n(a, x)$ with $D_n(a, x + (a/x)) = x^n + (a/x)^n$ is called *Dickson polynomial* of degree n (with parameter $a \in R$).

REMARK 1.3. The Dickson polynomials are often defined by property (iii) of 1.1 and denoted by $g_n(a, x)$ or $g_n(x, a)$ (cf. [30, p.209; 31, p.355]). (Added in proof: In [61] the notation $D_n(x, a)$ is used.) Our defining equation is then derived by means of Waring's formula expressing $x^n + y^n$ as a polynomial in $x + y$ and xy. We immediately obtain this formula by noting that $x^n + y^n = x^n + (xy/x)^n = D_n(xy, x + y)$ (with $R = \mathbb{Z}[x, y]$).

There is a close connection between the Dickson polynomials and the Chebyshev polynomials $T_n(x)$ (characterized by $T_n(\cos\varphi) = \cos n\varphi$). The defining property easily yields $D_n(a, x) = 2(\sqrt{a})^n T_n(x/2\sqrt{a})$ if $a \neq 0$; hence $T_n(x) = D_n(1, 2x)/2$.

LEMMA 1.4. *Let* n *be a positive integer,* $a \in R$, *and* P *be a prime ideal of* R *of finite norm* $NP = |R/P|$. *Then* $D_n(a, x)$ *is a p.p. mod* P *if and only if* $a \notin P$, $((NP)^2 - 1, n) = 1$ *or* $a \in P$, $(NP - 1, n) = 1$.

For a proof we refer to [30, Ch.4,Thm.9.43] (for $a \notin P$) or [31, pp.351, 356]; note that R/P is a finite field and the reduction of $D_n(a, x)$ mod P is $D_n(\bar{a}, x)$ where $\bar{a} = a + P \in R/P$.

PROPOSITION 1.5. *Let* $f(x) = \sum_{k=0}^{n} a_k x^k$ *be a polynomial with integral coefficients and degree* $n > 3$. *Assume that for every* $r = 2, \ldots, n - 2$ *there are infinitely many primes* p *with* $p \equiv r \bmod n$ *such that* $f(x)$ *is a p.p. mod* p. *Then* $f(x) = \alpha D_n(a, \gamma x + \delta) + \beta$ *for some* $a, \alpha, \beta, \gamma, \delta \in \mathbb{Q}$. *If* $a_n = 1$ *and* $a_{n-1} = 0$ *then we may choose* $\alpha = \gamma = 1$, $\beta = f(0)$, $\delta = 0$, *and* $a \in \mathbb{Z}$.

https://doi.org/10.1017/S1446788700038349 Published online by Cambridge University Press

PROOF. If $n = n_1 n_2$ with $n_1, n_2 > 1$ then there are only finitely many primes p with $p \equiv n_1 \bmod n$. Since $2 \le n_1 \le n-2$, this is a contradiction. Hence n is a prime. We call $g(x) \in \mathbb{Q}[x]$ a *p.p. mod p* if, for some integer s not divisible by p, $sg(x)$ has integral coefficients and is a p.p. mod p; this extends our earlier definition.

The polynomial $f_1(x) = (f(x - (a_{n-1}/na_n)) - f(-a_{n-1}/na_n))/a_n$ is a p.p. mod p if and only if $f(x)$ is a p.p. mod p provided that p does not divide na_n. For suitable $a \in \mathbb{Q}$ the coefficients of x^n, x^{n-1}, and x^{n-2} in $f_1(x)$ and $D_n(a, x) = x^n - nax^{n-2} + \cdots$ coincide. Also $f_1(0) = D_n(a, 0) = 0$. From Lemma 1.4 we conclude that $D_n(a, x)$ is a p.p. for all primes p with $(p^2 - 1, n) = 1$ that do not divide the denominator of a. Hence, by Dirichlet's theorem, for every $r = 2, \ldots, n-2$ there are infinitely many p with $p \equiv r \bmod n$ such that $D_n(a, x)$ is a p.p. mod p. The first part of the assertion thus follows as soon as we can prove that for fixed a_{n-2} there is at most one polynomial $f(x) = x^n + \sum_{k=1}^{n-2} a_k x^k \in \mathbb{Q}[x]$ with the required property.

Assume that $f(x)$ has the indicated form and choose r with $2 \le r \le n-2$. Let $p > n$ be a prime not dividing the denominator of any coefficient of $f(x)$ such that $p \equiv r \bmod n$ and $f(x)$ is a p.p. mod p. Put $m = 1 + (p-r)/n$. Since $1 \le m < p-1$, the reduction of $f(x)^m \bmod p$ must have reduced degree $< p-1$ (cf. Thm.7.4 and the remark following Cor.7.5 of [31]). Since $f(x)^m$ has degree $nm < 2(p-1)$, this means that the numerator of the coefficient of x^{p-1} in $f(x)^m$ is divisible by p. Since this coefficient is the coefficient of $t^{n-(r-1)} = t^{nm-(p-1)}$ in $(1 + a_{n-2}t^2 + \cdots + a_0 t^n)^m$, it has the form $ma_{r-1} + g(a_r, \ldots, a_{n-2}, m)$ where $g(x_1, \ldots, x_{n-r})$ is a polynomial with rational coefficients which only depend on n and r. Note that only primes smaller than n can appear in the denominator of one of the coefficients. If d is the degree with respect to x_{n-r} then $n^d g(a_r, \ldots, a_{n-2}, m) = h(a_r, \ldots, a_{n-2}, mn, n)$ for some polynomial $h(x_1, \ldots, x_{n-r+1})$ with rational coefficients only depending on n and r. Thus the numerator of $mn^d a_{r-1} + h(a_r, \ldots, a_{n-2}, mn, n)$ is divisible by p and taking into account that $mn \equiv n - r \bmod p$ we conclude that the same holds for $n^{d-1}(n-r)a_{r-1} + h(a_r, \ldots, a_{n-2}, n-r, n)$. Since this number is independent of p (and we have infinitely many possibilities for p) it has to be zero. Hence a_{r-1} is uniquely determined by $a_r, \ldots, a_{n-2}$ and by induction on r we conclude that all coefficients $a_1, \ldots, a_{n-2}$ are uniquely determined by a_{n-2}.

It remains to prove the last part of the assertion. By what we have just seen we obtain $f(x) - f(0) = D_n(a, x)$ for some $a \in \mathbb{Q}$. Hence $D_n(a, x) = x^n - nax^{n-2} + \cdots + n(-a)^{(n-1)/2}x$ has integral coefficients and this implies $a \in \mathbb{Z}$ since n is a prime ≥ 5.

REMARK 1.6. This result is of course contained in Schur's theorem (that is, the special case of Theorem 2 for integral polynomials of prime degree) from [48], but the proof is much simpler. The main idea is due to Dickson [10, pp. 89–91]. A weaker version was proved by Wegner by a totally different argument (using non-elementary

auxiliary results) in [53].

PROPOSITION 1.7. *Let n be a positive integer and assume that there is a primitive n-th root ζ of unity in R. Put $\alpha_k = \zeta^k + \zeta^{-k}$, $\beta_k = \zeta^k - \zeta^{-k}$. Then for every $a \in R$ we have*

$$D_n(a, x) - D_n(a, y) = (x - y) \prod_{k=1}^{(n-1)/2} (x^2 - \alpha_k xy + y^2 + \beta_k^2 a)$$

if n is odd and otherwise

$$D_n(a, x) - D_n(a, y) = (x - y)(x + y) \prod_{k=1}^{(n-2)/2} (x^2 - \alpha_k xy + y^2 + \beta_k^2 a).$$

For $a \neq 0$ the quadratic factors are different from each other and irreducible in $R[x, y]$.

PROOF. Note that $x^n + y^n = D_n(xy, x + y)$ (cf. 1.3). If $\beta_k \neq 0$ we may replace x and y by $(\zeta^k x - y)/\beta_k$ and $(-\zeta^{-k} x + y)/\beta_k$, respectively, and obtain $(\zeta^k x - y)^n + (-\zeta^{-k} x + y)^n = \beta_k^n D_n(z_k, x)$ with $z_k = -(x^2 - \alpha_k xy + y^2)/\beta_k^2$. Note that the left side is symmetric in x, y since $(-\zeta^{-k} x + y)^n = (-x + \zeta^k y)^n$. Thus by interchanging x and y we conclude that $D_n(z_k, x) = D_n(z_k, y)$. Hence z_k is a zero of the polynomial $f(z) = D_n(z, x) - D_n(z, y)$ over $K(x, y)$.

Since $\zeta^j - \zeta^{-j} = \zeta^k - \zeta^{-k}$ holds if and only if $\zeta^j = \zeta^k$ or $\zeta^j = -\zeta^{-k}$, $\beta_j^2 = \beta_k^2$ holds if and only if $\zeta^j = \pm\zeta^k$ or $\zeta^j = \pm\zeta^{-k}$, that is, if and only if $2(j - k)$ or $2(j + k)$ is divisible by n. Hence the β_k^2 with $1 \leq k < n/2$ are different from each other and non-zero (since $\beta_0 = 0$).

If n is odd then (by Lemma 1.1(iii)) $f(z)$ has degree $(n - 1)/2$ and leading term $n(-1)^{(n-1)/2}(x - y)$; note that n is not divisible by the characteristic of K (since otherwise $\zeta^{n/p} = 1$ if $\mathrm{char} K = p > 0$). Hence $f(z) = n(-1)^{(n-1)/2}(x - y) \prod_{k=1}^{(n-1)/2}(z - z_k)$. Comparing the coefficient of x^n on both sides implies that $n(-1)^{(n-1)/2} = \prod_{k=1}^{(n-1)/2} \beta_k^2$ (which can also be easily derived from $n = \prod_{j=1}^{n-1}(1 - \zeta^j)$). Thus in $K[x, y, z]$ we obtain the identity $D_n(z, x) - D_n(z, y) = (x - y) \prod_{k=1}^{(n-1)/2}(x^2 - \alpha_k xy + y^2 + \beta_k^2 z)$.

If n is even then $f(z)$ has degree $(n - 2)/2$ and leading term $(n/2)^2(x^2 - y^2) \times (-1)^{(n-2)/2}$. Hence $f(z) = (n/2)^2(-1)^{(n-2)/2}(x^2 - y^2) \prod_{k=1}^{(n-2)/2}(z - z_k)$ and, for the same reason as above, $D_n(z, x) - D_n(z, y) = (x - y)(x + y) \prod_{k=1}^{(n-2)/2}(x^2 - \alpha_k xy + y^2 + \beta_k^2 z)$.

If there exists a factorization of $x^2 - \alpha_k xy + y^2 + \beta_k^2 a$ then it clearly has the form $(x - \zeta^k y + b_k)(x - \zeta^{-k} y + c_k)$ with suitable $b_k, c_k \in R$. Comparing coefficients gives $b_k + c_k = 0$, $\zeta^{-k} b_k + \zeta^k c_k = 0$, and $b_k c_k = \beta_k^2 a$. Hence $b_k = -c_k$, $c_k \beta_k = 0$, and $c_k^2 = -\beta_k^2 a$. This is only possible if $\beta_k = 0$ or $a = 0$.

REMARK 1.8. This result provides us with the factorization of $D_n(a, x) - D_n(a, y)$ in $\bar{K}[x, y]$ if n is not divisible by $\operatorname{char} K$. The general case is obtained by observing that $D_{np}(a, x) = D_n(a, x)^p$ and hence $D_{np}(a, x) - D_{np}(a, y) = (D_n(a, x) - D_n(a, y))^p$ if $p = \operatorname{char} K > 0$. Our proof simplifies William's proof for odd integers n and finite fields K given in [55].

Replacing y by 0 yields $D_n(a, x) = x \prod_{k=1}^{(n-1)/2}(x^2 + \beta_k^2 a)$ for odd n.

LEMMA 1.9. *Let L be any extension field of K (such that x is transcendental over L). Then for every positive integer n not divisible by* $\operatorname{char} K$ *we have:*

(i) *If $n \leq 3$ then every monic polynomial (over K) of degree n can be written in the form $D_n(a, x + b) + c$ with $a, b, c \in K$.*

(ii) *If $n \geq 3$ and $a, b, c \in L$ are such that the coefficients of $f(x) = D_n(a, x + b) + c$ belong to K then a, b, c belong to K and are uniquely determined by $f(x)$.*

(iii) *If $n \geq 3$ and $a, \alpha, \beta, \gamma, \delta \in L, \alpha\gamma \neq 0$, are such that the coefficients of $f(x) = \alpha D_n(a, \gamma x + \delta) + \beta$ belong to K then $f(x) = \alpha\gamma^n D_n(a/\gamma^2, x + \delta/\gamma) + \beta$ and $\alpha\gamma^n, a/\gamma^2, \delta/\gamma, \beta \in K$.*

PROOF. For $n = 1$ we have $x + a_0 = D_1(0, x) + a_0$ and for $n = 2$ we have $x^2 + a_1 x + a_0 = D_2(0, x + b) + c$ with $b = a_1/2$ and $c = a_0 - (a_1/2)^2$. Since $x^3 + a_2 x^2 + a_1 x + a_0 = D_3(a, x + b) + c$ with $a = (a_2/3)^2 - (a_1/3)$, $b = a_2/3$, and $c = a_0 - D_3(a, b)$, (i) is proved. (Note that $D_3(a, x) = x^3 - 3ax$.)

In the sequel we assume $n \geq 3$. If $f(x) = D_n(a, x + b) + c$ then by Lemma 1.1 we have $f(x) = (x + b)^n - na(x + b)^{n-2} + \cdots = x^n + nbx^{n-1} + (\binom{n}{2}b^2 - na)x^{n-2} + \cdots$ which implies that b and a belong to K (provided that $f(x) \in K[x]$) and are uniquely determined by $f(x)$. Hence this also holds for $c = f(0) - D_n(a, b)$, thus proving (ii).

Now assume that $f(x) = \alpha D_n(a, \gamma x + \delta) + \beta \in K[x]$. By Lemma 1.1, $f(x) = \alpha\gamma^n D_n(a/\gamma^2, x + \delta/\gamma) + \beta = \alpha\gamma^n(x + \delta/\gamma)^n - \alpha\gamma^{n-2}na(x + \delta/\gamma)^{n-2} + \cdots$. Hence $\alpha\gamma^n, \delta/\gamma, a/\gamma^2 (= \alpha\gamma^{n-2}na/(n\alpha\gamma^n))$, and $\beta = f(0) - \alpha\gamma^n D_n(a/\gamma^2, \delta/\gamma)$ belong to K.

LEMMA 1.10. *For every $n \geq 3$ there are integral polynomials $p_{nk}(x_0, \ldots, x_n)$, $0 \leq k \leq n$, such that, for arbitrary elements $a_0, \ldots, a_n$ of a field K whose characteristic does not divide n, $p_{nk}(a_0, \ldots, a_n) + n^{n-k}a_n^{n-k-1}a_k$ is the coefficient of x^k in $g(x) = D_n\left(((n-1)/2)a_{n-1}^2 - na_n a_{n-2}, x + a_{n-1}\right)$ and the following conditions are equivalent if $a_n \neq 0$:*

(i) $\sum_{k=0}^n a_k x^k = \alpha D_n(a, \gamma x + \delta) + \beta$ *for some $a, \alpha, \beta, \gamma, \delta$ in an extension field of K.*

(ii) $\sum_{k=0}^n a_k x^k + c = g(na_n x)/(n^n a_n^{n-1})$ *for suitable $c \in K$.*

(iii) $p_{nk}(a_0, \ldots, a_n) = 0$ *for all k with $1 \leq k \leq n - 3$.*

https://doi.org/10.1017/S1446788700038349 Published online by Cambridge University Press

PROOF. For every k with $0 \le k \le n$ let $q_{nk}(x_0, \dots, x_n)$ be the integral polynomial (independent of K) such that $q_{nk}(a_0, \dots, a_n)$ is the coefficient of x^k in $g(x)$ and set $p_{nk}(x_0, \dots, x_n) = q_{nk}(x_0, \dots, x_n) - n^{n-k}x_n^{n-k-1}x_k$. Note that the q_{nk} exist by Lemma 1.1. If (i) holds then by Lemma 1.9(iii) we may assume $a, \alpha, \beta, \gamma, \delta \in K$ and by Lemma 1.1(ii) we may assume $\gamma = na_n$. Then from $\alpha D_n(a, \gamma x + \delta) = \alpha\gamma^n x^n + \alpha n\gamma^{n-1}\delta x^{n-1} + \alpha n\gamma^{n-2}(((n-1)/2)\delta^2 - a)x^{n-2} + \cdots$ we obtain $\alpha = (n^n a_n^{n-1})^{-1}$, $\delta = a_{n-1}$, and $a = ((n-1)/2)a_{n-1}^2 - na_n a_{n-2}$. Hence (i) implies (ii). The converse is trivial.

Note that (ii) holds if and only if $n^n a_n^{n-1}a_k = (na_n)^k(p_{nk}(a_0, \dots, a_n) + n^{n-k}a_n^{n-k-1}a_k)$ for $1 \le k \le n$, that is, $p_{nk}(a_0, \dots, a_n) = 0$. By what we have seen above, this always holds for $n - 2 \le k \le n$. Hence (ii) and (iii) are equivalent.

The following result is required for the proof of Theorem 4.5. It constitutes an elementary substitute for Lemma 6 and Lemma 12 of [14].

LEMMA 1.11. *Let $f(x) \in K[x]$ be a monic polynomial of degree $n \ge 3$ and assume that for every $\eta \in \bar{K}$ such that $f(x) - \eta$ has multiple roots, one of the roots is simple, the remaining ones all have the same multiplicity r, and r is not divisible by* char$K$. *Then $f(x) = D_n(a, x + b) + c$ for some $a, b, c \in K$, $a \ne 0$, if n is not divisible by* char$K$.

PROOF. An element $\alpha \in \bar{K}$ is a zero of $f'(x)$ if and only if it is a zero of multiplicity $r > 1$ of $f(x) - \eta$ for some $\eta \in \bar{K}$ in which case it is a zero of multiplicity $r - 1$ of $f'(x)$. Hence every $\eta_i \in \bar{K}$ such that $f(x) - \eta_i$ has multiple roots accounts for $(r_i - 1)(n-1)/r_i$ roots of $f'(x)$. Since $f'(x)$ has just $n - 1$ roots and $(r_i - 1)/r_i \ge 1/2$, we have precisely two different values η_1, η_2 of this kind and $r_1 = r_2 = 2$. Consequently, char$K \ne 2$.

Hence $f(x) = (x - \alpha_i)g_i(x)^2 + \eta_i$ $(i = 1, 2)$ for some $\alpha_i, \eta_i \in \bar{K}$ with $\eta_1 \ne \eta_2$ and monic polynomials $g_i(x)$ of degree $(n-1)/2$. Putting $\lambda = (\alpha_2 - \alpha_1)/4$, $\mu = (\alpha_1 + \alpha_2)/2$, and replacing x by $x^2 + \mu + \lambda^2/x^2$ in the equation $(x - \alpha_1)g_1(x)^2 - (x - \alpha_2)g_2(x)^2 = \eta_2 - \eta_1$ yields $(u_1(x)/x^n)^2 - (u_2(x)/x^n)^2 = \eta_2 - \eta_1$ with $u_1(x) = x^n(x + \lambda/x)g_1(x^2 + \mu + \lambda^2/x^2)$ and $u_2(x) = x^n(x - \lambda/x)g_2(x^2 + \mu + \lambda^2/x^2)$. Note that $u_1(x)$ and $u_2(x)$ are monic polynomials of degree $2n$ with constant terms λ^n and $-\lambda^n$, respectively. Hence $u_1(x) + u_2(x)$ has leading term $2x^{2n}$ and $u_1(x) - u_2(x)$ has constant term $2\lambda^n$.

Since $(u_1(x) + u_2(x))(u_1(x) - u_2(x)) = (\eta_2 - \eta_1)x^{2n}$, we conclude $u_1(x) + u_2(x) = 2x^{2n}$, $u_1(x) - u_2(x) = 2\lambda^n$, and $\eta_2 - \eta_1 = 4\lambda^n$. Hence $u_1(x) = x^{2n} + \lambda^n$ and $f(x^2 + \mu + \lambda^2/x^2) = (u_1(x)/x^n)^2 + \eta_1 = x^{2n} + (\lambda/x)^{2n} + (\eta_1 + \eta_2)/2$. The definition of the Dickson polynomials now yields $f(x + \mu) = D_n(\lambda^2, x) + (\eta_1 + \eta_2)/2$. Hence $f(x) = D_n(a, x + b) + c$ with $a = \lambda^2$, $b = -\mu$, and $c = (\eta_1 + \eta_2)/2$. From Lemma 1.9(ii) we see that $a, b, c \in K$. Note that $a \ne 0$ since $4\lambda^n = \eta_2 - \eta_1 \ne 0$.

In order to prove Theorem 4.34 (or Theorem 3) the following results are only required for the ring R appearing there.

LEMMA 1.12. *Let R be a Dedekind domain. Assume that n is an odd integer and $v_P(n) < (n-1)/2$ for every non-zero prime ideal P. If $a \in K$ is such that $D_n(a, x) \in R[x]$ then $a \in R$.*

PROOF. We may assume that R is not a field. Then $n > 1$ and $n \neq 0$ in R. From $D_n(a, x) = x^n - nax^{n-2} + \cdots + n(-a)^{(n-1)/2}x$ we conclude that $na \in R$ and $na^{(n-1)/2} \in R$. Hence $a = b/n$ with $b \in R$ and $b^{(n-1)/2} \in n^{(n-3)/2}R$. The last relation implies that $v_P(b) \geq e \cdot (n-3)/(n-1) > e-1$ if $P^e | n$; hence $P^e | b$. Since this holds for all P we deduce that n divides b and $a \in R$.

REMARK 1.13. Let n be an odd prime and R be a Dedekind domain whose characteristic does not divide n. If $v_P(n) \geq (n-1)/2$ for some P (which is the case for $n = 5$ and $R = \mathbb{Z}[(1+\sqrt{5})/2]$) then, choosing $b \in R$ with $v_P(b) = v_P(n) - 1$ and $v_Q(b) \geq v_Q(n)$ for all prime ideals $Q \neq P$ that divide n, we have $D_n(b/n, x) \in R[x]$ although $b/n \notin R$. (Note that b exists by the Chinese remainder theorem.) To see this, observe that $n(b/n)^k \in R$ for all k with $1 \leq k \leq (n-1)/2$ since $v_P(n(b/n)^k) \geq v_P(n) - (n-1)/2 \geq 0$ and $v_Q(b/n) \geq 0$ for all $Q \neq P$. Since n is a prime, the coefficient of x^{n-2k} ($k \geq 1$) in $D_n(a, x)$ is an integral multiple of na^k (by Lemma 1.1(iii)). Hence $D_n(b/n, x) \in R[x]$.

The next result will be generalized in Theorem 2.8.

LEMMA 1.14. *Let R be a Dedekind domain. If $n > 3$ is an odd integer and $a, b, c \in K$ are such that $D_n(a, x+b) + c \in R[x]$ then $a, b, c \in R$ if $v_P(n) \leq 1$ for every non-zero prime ideal P.*

PROOF. We have $D_n(a, x+b) = (x+b)^n - na(x+b)^{n-2} + (n(n-3)/2)a^2(x+b)^{n-4} + \cdots = x^n + nbx^{n-1} + ((n(n-1)/2)b^2 - na)x^{n-2} + ((n(n-1)(n-2)/6)b^3 - n(n-2)ab)x^{n-3} + \cdots$. Thus $b = b'/n$, $a = a'/n^2$ with $a', b' \in R$ and $2a' \equiv (nb)^2(n-1) \equiv -b'^2 \bmod n$. We assume $n \neq 0$ in R since otherwise $R = K$. From $(n(n-1)(n-2)/6)b^3 - n(n-2)ab \in R$ we obtain $(n-1)(n-2)b'^3 \equiv 6(n-2)a'b' \bmod 6n^2$. Hence $2b'^3 \equiv -12a'b' \bmod n$ and together with $b'^2 \equiv -2a' \bmod n$ we obtain $4b'^3 \equiv 0 \bmod n$. By assumption this implies that n divides b' and thus $b \in R$. Then we also have $D_n(a, x) + c \in R[x]$. Since $D_n(a, 0) = 0$, we obtain $c \in R$ and $D_n(a, x) \in R[x]$. Hence $a \in R$ by 1.12.

2. Composition of polynomials

R denotes any integral domain. The quotient field is denoted by K.

DEFINITION 2.1. A polynomial $f(x) \in R[x]$ is called *decomposable over* R if $f(x) = g(h(x))$ for suitable polynomials $g(x), h(x) \in R[x]$ of degree > 1. Otherwise it is called *indecomposable*.

PROPOSITION 2.2. *For every extension field L of K (such that x is transcendental over L) we have:*

(i) *Each pair of nonconstant polynomials $g(x), h(x) \in L[x]$ is uniquely determined by the coefficients of $g(h(x))$, $h(0)$, the highest coefficient of $h(x)$, and the degree of $g(x)$, provided that the latter is not divisible by* $\operatorname{char} K$.

(ii) *Let $f(x) \in R[x]$ be a non-constant polynomial such that* $\deg(f)$ *is not divisible by* $\operatorname{char} K$. *If $f(x)$ is decomposable over L then $f(x)$ is decomposable over K. If $f(x) = g(h(x))$ with monic polynomials $g(x), h(x) \in L[x]$ and $h(0) = 0$ then the coefficients of $g(x)$ and $h(x)$ belong to the integral closure of R in K.*

PROOF. Let $g(x) = \sum_{i=0}^{m} a_i x^i \in L[x]$ and $h(x) = \sum_{j=0}^{n} b_j x^j \in L[x]$ be monic polynomials of degrees m and n, respectively, and assume that $b_0 = 0$ and m is not divisible by $\operatorname{char} K$. For every k with $1 \leq k < n$ the coefficient of x^{mn-k} in $g(h(x))$ has the form $mb_{n-k} + p_k(b_{n-k+1}, \ldots, b_n)$ for some integral polynomial $p_k(x_1, \ldots, x_k)$ whose coefficients only depend upon m. Hence all the b_j belong to the field generated by the coefficients of $g(h(x))$ and are uniquely determined by them. Consequently, this also holds for the a_i as is seen by a trivial inductive argument starting with the highest coefficient.

It is clear that (i) and the first part of (ii) follow from what we have just proved. Now assume that $f(x) = g(h(x))$ with monic polynomials $g(x), h(x)$ over L and $h(0) = 0$. If α is any root of $g(x)$ then the monic polynomial $h(x) - \alpha$ divides $f(x) = g(h(x))$. Hence the coefficients of $h(x) - \alpha$ are integral over R, that is the coefficients of $h(x)$ and α are integral over R. Since α was an arbitrary root the same conclusion holds for $g(x)$. According to what we have seen above the coefficients also belong to K.

COROLLARY 2.3. *Assume that R is integrally closed and $f(x) \in R[x]$ is a monic polynomial whose degree is not divisible by* $\operatorname{char} K$. *Then $f(x)$ is decomposable over R if and only if it is decomposable over some extension field L of K. In this case we have $f(x) = (f_1 \circ \cdots \circ f_r)(x) + f(0)$ with monic polynomials $f_i(x) \in R[x]$ such that $f_i(0) = 0$ and $f_i(x)$ is indecomposable over L.*

https://doi.org/10.1017/S1446788700038349 Published online by Cambridge University Press

PROOF. If $f(x)$ is decomposable over R then it is obviously decomposable over L. Conversely, if this holds then $f(x) = g(h(x))$ where $g(x), h(x) \in L[x]$ have degree > 1. We clearly may assume that $h(x)$ (and hence $g(x)$) is monic and $h(0) = 0$. Then by (ii) we have $g(x), h(x) \in R[x]$ and the assertion follows by induction.

PROPOSITION 2.4. *Assume that R is a unique factorization domain. Then for every $f(x) \in R[x]$ we have:*

(i) *If $\deg(f)$ is not divisible by $\operatorname{char} K$ then $f(x)$ is decomposable over R if and only if it is decomposable over some extension field of K.*

(ii) *Let $h(x) \in R[x]$ be a polynomial of unit content (that is, every common divisor of its coefficients is a unit) and $h(0) = 0$. Then there exists $g(x) \in R[x]$ with $f(x) = g(h(x))$ if and only if $h(x) - h(y)$ divides $f(x) - f(y)$ in $K[x, y]$.*

(iii) *Let $h(x) \in R[x]$ be a polynomial of unit content and $h(0) = 0$. If $g(x) \in K[x]$ is such that $g(h(x)) \in R[x]$ then $g(x) \in R[x]$.*

PROOF. Note that every polynomial over K can be written in the form $\alpha h(x)$ with $\alpha \in K$ such that $h(x) \in R[x]$ has unit content. Hence, if (iii) holds, then every polynomial over R which is indecomposable over R also is indecomposable over K. Thus the 'if' part of (i) follows from (iii) and Proposition 2.2. The converse is trivial.

Since $h(x) - h(y)$ divides $g(h(x)) - g(h(y))$ in $K[x, y]$, (iii) follows from (ii) (since $g(x)$ is uniquely determined by $g(h(x))$ and $h(x)$) and the 'only if' part of (ii) is proved. The 'if' part of (ii) holds trivially if $\deg(f) < \deg(h)$ and we proceed by induction on $\deg(f)$.

The well known Gauss lemma states that a product of polynomials in one variable with unit content has unit content. This is easily extended to polynomials in several variables. Just note that a polynomial of degree $< d$ in each variable x_i has the same coefficients as the polynomial in one variable obtained by substituting x^{d^i} for x_i.

Since $h(x) - h(y)$ has unit content we may thus conclude that $p(x, y) \in R[x, y]$ if $f(x) - f(y) = p(x, y)(h(x) - h(y))$. Put $f_1(x) = p(x, 0)$. Then $f(x) - f(0) = f_1(x)h(x)$ and $h(x) - h(y)$ divides $(f_1(x) - f_1(y))h(x) = (p(x, y) - f_1(y))(h(x) - h(y))$. Hence $h(x) - h(y)$ divides $f_1(x) - f_1(y)$ and by induction we get $f_1(x) = g_1(h(x))$ for some $g_1(x) \in R[x]$; note that $\deg(f_1) < \deg(f)$. Thus $f(x) = g(h(x))$ with $g(x) = xg_1(x) + f(0) \in R[x]$ as was to be shown.

REMARK 2.5. Decomposition of polynomials over fields has been studied quite extensively and satisfactory results (due to Ritt for $K = \mathbb{C}$) concerning uniqueness are known ([30, Ch. 4; 46, pp. 12–39]). The first part of (ii) of Proposition 2.2 is well known (cf. [30, p. 139] or [46, p. 14]). The second part has been proved by Wegner in a slightly weaker form for $R = \mathbb{Z}$ and $L = \mathbb{Q}$ ([52, p. 9]); our proof is much easier. If $\deg(f)$ is divisible by $\operatorname{char} K$ then Proposition 2.2 need not hold. This is shown

by choosing ([46, p. 15]) $K = \mathbb{F}_2$, $g(x) = x^2 + \alpha^{-1}x$, and $h(x) = x^2 + \alpha x$, where $\alpha^3 + \alpha + 1 = 0$; then $f(x) = g(h(x)) = x^4 + x^2 + x \in K[x]$ but $g(x), h(x) \notin K[x]$ and $f(x)$ is indecomposable over K. Note that (i) fails since α is not unique. (Added in proof: The author provided an infinite class of examples in his review MR91j: 11106 of [8]. See [57, §4] for more information on this topic.)

It is hard to believe that Proposition 2.4(i) has not been noticed before, but I can give only one reference where a pertinent statement can be found. In [1], which is a preliminary version of [2], it is claimed that an easy modification of the argument in [12] (where (ii) is proved in the case that R is a field) would show that (i) holds for arbitrary rings. Proposition 2.6 demonstrates that this assertion is incorrect. (In [2] only fields are considered and the conspicuous fact that all decompositions over $\mathbb{Q}$ considered there involve integral polynomials only is not commented on at all.)

Let R be the ring of algebraic integers of a number field K. Fried has observed that every $f(x) \in R_P[x]$ (where $R_P = \{r/s : r \in R,\ s \notin P\}$) which is decomposable over K admits a decomposition into polynomials in $R_P[x]$ provided that $\deg(f) \notin P$ ([14, Lemma 10]). Proposition 2.4(i) shows that the assertion holds without this restriction; note that R_P is a principal ideal domain.

The content $C(f)$ of a polynomial f (in several variables) with coefficients in an arbitrary integral domain is defined to be the ideal generated by these. As an immediate consequence of a theorem of Hurwitz (concerning $\mathbb{Z}$-modules rather than ideals) we obtain $C(gh)C(h)^r = C(g)C(h)^{r+1}$ for suitable r. ([25, p. 203]; for a more precise result see [51].) Hence $C(h) = R$ implies $C(gh) = C(g)$ and this easily shows that h divides a polynomial f (with coefficients in R) over R if and only if it divides f over K. Thus (ii) and (iii) of Proposition 2.4 remain valid in general if h is assumed to satisfy $C(h) = R$ (instead of having unit content), whereas the following result shows that (i) even fails if R is a ring of algebraic integers unless it is a unique factorization domain. (It should be noted that h may have unit content although $C(h) \neq R$.)

PROPOSITION 2.6. *Let R be the ring of algebraic integers of a number field K of class number greater than one. Then for every prime q there is a polynomial $f(x) \in R[x]$ of degree q^2 that is decomposable over K and indecomposable over R.*

PROOF. We start by remarking that there are infinitely many non-principal prime ideals in R. For if all prime ideals different from $P_1, \ldots, P_r$ are principal then choosing $\pi_i \in P_i - P_i^2$ we may find $a_i \in R$ with $a_i \equiv \pi_i \bmod P_i$ and $a_i \equiv 0 \bmod P_j$ for all $j \neq i$ by the Chinese remainder theorem ($i, j = 1, \ldots, r$). Then the principal ideal (a_i) is equal to P_i times some prime ideals different from $P_1, \ldots, P_r$ which implies that P_i is principal.

Thus there exists an unramified prime p such that $(p) = P_1 \cdots P_g$ for (distinct) prime ideals P_i where P_1 is non-principal; hence $g \geq 2$. Choose $s_2, \ldots, s_g \geq 1$ such that $\prod_{i>1} P_i^{s_i}$ is principal and $\sum_{i>1} s_i$ is minimal. Let a be a generator of this ideal. Since $p \in P_1$ we have $P_1 = (b, p)$ for some $b \in R$. Then b is not divisible by P_i for $i \geq 2$.

All the coefficients of $f(x) = (a/p)(bx^q + px^{q-1})^q$ belong to R since $p|ab$. Assume that $f(x)$ is decomposable over R. Then there are polynomials $g(x), h(x) \in R[x]$ of degree q with $f(x) = g(h(x))$ and $h(0) = 0$. Let c be the leading coefficient of $h(x)$. Then from Proposition 2.2(i) we conclude $g(x) = (a/p)(bx/c)^q$ and $h(x) = c(x^q + px^{q-1}/b)$. Hence $ab^q/(pc^q)$ and cp/b belong to R, that is $d = cp/b$ belongs to R and d^q divides ap^{q-1}. Hence $(d) = \prod_{i>1} P_i^{s_i'}$ with $qs_i' \leq s_i + q - 1$; note that $s_i' \geq 1$ since P_i does not divide b for $i > 1$. From $s_i + q - 1 \leq qs_i$ with equality holding only for $s_i = 1$ we obtain $\sum_{i>1} s_i' < \sum_{i>1} s_i$ unless $s_i = 1$ for all $i > 1$. The minimality of $\sum_{i>1} s_i$ implies that the latter condition holds. But then from $(p) = P_1(a)$ we conclude that P_1 is principal, a contradiction. Thus $f(x)$ is indecomposable over R (although it obviously is decomposable over K).

REMARK 2.7. If we additionally assume that $q \geq h$ and $(q - 1, h) = 1$, where h denotes the class number of K, then we may even choose $f(x)$ to be a composition of linear polynomials and powers. This will be needed later in 4.36.

By the remark at the beginning of the preceding proof there exists a non-principal prime ideal P_0 with $q \notin P_0$. Let $c \neq 0$ be an element of P_0^2 and choose $b \in P_0$ with $(b, qc) = P_0$. Note that there is no prime ideal P that divides both b and q. Let $P_0, \ldots, P_r$ be the prime ideals P such that $v_P(c) > v_P(b)$. According to the Chinese remainder theorem there exists $a' \in R$ with $v_{P_i}(a') = q(q-1)(v_{P_i}(c) - v_{P_i}(b))$ for all i. Let $s_P < h$ be the residue of $v_P(a')$ mod h if $P \neq P_0, \ldots, P_r$ and $s_P = v_P(a')$ otherwise; then $\prod P^{s_P}$ is a principal ideal. Let a be a generator of this ideal and set $f(x) = ab^{-q}c^{-q(q-1)}((bx+c)^q - c^q)^q$. Note that $f(x) \in R[x]$ since $a(b/c)^{q(q-1)} \in R$.

Assume that $f(x)$ is decomposable over R. Then $f(x) = g(h(x))$ with polynomials $g(x), h(x) \in R[x]$ of degree q and $h(0) = 0$. By Proposition 2.2(i) we obtain $g(x) = a(b/c)^{q(q-1)}d^{-q}x^q$ and $h(x) = d((x + c/b)^q - (c/b)^q)$ if d is the leading coefficient of $h(x)$. Hence $a(b/c)^{q(q-1)}d^{-q} \in R$ and $dq(c/b)^{q-1} \in R$. Taking into account that $v_P(q) = 0$ if $v_P(b) > 0$, this implies that $\alpha = d(c/b)^{q-1}$ and a/α^q both belong to R. Hence $(q-1)(v_P(c) - v_P(b)) \leq v_P(\alpha) \leq v_P(a)/q$ for all P. If $P \neq P_0, \ldots, P_r$ we conclude $v_P(\alpha) = 0$ since $v_P(a) < h \leq q$; if $P = P_i$ then $v_P(\alpha) = (q-1)(v_P(c) - v_P(b))$ since $v_P(a) = q(q-1)(v_P(c) - v_P(b))$. Thus we must have $(\alpha)P_0^{q-1} = (c)^{q-1}$, since $v_{P_0}(b) = 1$ and P_0 is the only common prime divisor of b, c. Hence P_0^{q-1} is a principal ideal. Since $(q-1, h) = 1$, also P_0 is a principal ideal, a contradiction. Hence $f(x)$ is indecomposable over R.

THEOREM 2.8. *Let R be a Dedekind domain with quotient field $K \neq R$ and let n be a positive integer which is not divisible by any ramified prime. Assume that a, b, c belong to some extension field of K and all coefficients of $D_n(a, x+b)+c$ belong to R. Then $a, b, c \in R$ unless we have one of the following exceptional cases (for n, a, b and suitable c):*

(i) $n = 1$.
(ii) $n = 2$ *and* $2b \in R$.
(iii) $n = 3$ *and* $9a, 3b \in R$, $9a \equiv (3b)^2 \bmod 3$.
(iv) $n = 4$ *and* $8a, 2b \in R$, $8a \equiv (2b)^2 \bmod 2$.
(v) $n = 6$ *and* $3a, b \in R$.
(vi) $n = 8$ *and* $2a, b \in R$.

PROOF. For fixed a, b, c we set $f_k(x) = D_k(a, x+b) - D_k(a, b)$ for all $k \geq 1$. We have to prove that $f_n(x) \in R[x]$ if and only if $a, b \in R$ or one of the exceptional cases occurs. For $n \leq 2$ the assertion immediately follows from $f_1(x) = x$ and $f_2(x) = x^2 + 2bx$. From $f_3(x) = x^3 + 3bx^2 + (3b^2 - 3a)x$ we see that $f_3(x) \in R[x]$ implies that (iii) holds; conversely, from (iii) we obtain $f_n(x) \in R[x]$. Now let $n = 4$ and note that $f_4(x) = x^4 + 4bx^3 + (6b^2 - 4a)x^2 + (4b^3 - 8ab)x$. Hence $f_4(x) \in R[x]$ implies $2b \in R$ since $4b \in R$ and $2^4 b^3 = 4b(6b^2 - 4a) - 2(4b^3 - 8ab) \in R$; note that 2 is unramified. Moreover, $8a \in R$ and $8a \equiv (2b)^2 \bmod 2$ since $3(2b)^2 - 8a \in 2R$. Thus $f_4(x) \in R[x]$ implies (iv); it is easy to see that the converse is also true.

The rest of the proof is based on the following three observations (where m, n mean arbitrary positive integers):

(1) $f_{mn}(x) \in R[x]$ implies $f_n(x) \in R[x]$.
(2) $f_{2n}(x) \in R[x]$ holds if and only if $f_n(x) \in R[x]$ and $2D_n(a, b) \in R$.
(3) If $b \in R$ and $f_n(x) \in R[x]$ then $D_n(a, x) - D_n(a, 0) \in R[x]$.

By Lemma 1.1(ii) we have $D_{mn}(a, x+b) = D_m(a^n, D_n(a, x+b))$ and thus $f_{mn}(x) = g_{m,n}(f_n(x))$ with $g_{m,n}(x) = D_m(a^n, x + D_n(a, b)) - D_{mn}(a, b)$. Note that $f_n(0) = 0$ and $f_n(x), g_{m,n}(x)$ are monic. Hence $f_{mn}(x) \in R[x]$ implies $g_{m,n}(x), f_n(x) \in R[x]$ by Proposition 2.2(ii) (since $n \neq 0$ in R); the converse is trivial. This proves (1) and (2) since $g_{2,n}(x) = x^2 + 2xD_n(a, b)$; (3) is easy to see.

From Lemma 1.14 we know that $f_p(x) \in R[x]$ implies $a, b \in R$ if $p > 3$ is an unramified prime. By (1) it thus remains to show that for $n = 6, 8$ only the specified exceptions are possible while for $n = 9, 12, 16$ we must have $a, b \in R$ if $f_n(x) \in R[x]$.

If $n = 6$ and $f_6(x) \in R[x]$ then, by (2), $f_3(x) \in R[x]$ and $2b^3 - 6ab = 2D_3(a, b) \in R$; hence $9a, 3b \in R$ and $(3b)^3 \equiv -3^3(2b^3 - 6ab) \equiv 0 \bmod 3$. Since 3 is unramified, this yields $b \in R$ and then the last condition of (iii) gives $3a \in R$, that is, (v) holds. Conversely, (v) implies $f_6(x) \in R[x]$ by (2) and (iii). Similarly, if $n = 8$ and $f_n(x) \in R[x]$ then $8a, 2b \in R$, $8a \equiv (2b)^2 \bmod 2$, and $2(2b)^4 - 4 \cdot 8a(2b)^2 + (8a)^2 =$

$2^5 D_4(a,b) \equiv 0 \bmod 2^4$. Now $(8a)^2 \equiv (2b)^4 \bmod 2$ yields $(2b)^4 \equiv 0 \bmod 2$ and thus $b \in R$ (since 2 is unramified). Consequently, $(8a)^2 \equiv 2^5 D_4(a,b) \equiv 0 \bmod 2^4$ and hence also $2a \in R$. Conversely, from $2a, b \in R$ we obtain $f_8(x) \in R[x]$ since $f_4(x) \in R[x]$ and $2D_4(a,b) \in R$.

Let $n = 9$ and assume $f_9(x) \in R[x]$. From $f_9(x) = (x+b)^9 - 9a(x+b)^7 + \cdots = x^9 + 9bx^8 + (36b^2 - 9a)x^7 + (84b^3 - 63ab)x^6 + \cdots$ we get $b = b'/9$ and $a = a'/81$ with $a', b' \in R$ such that $4b'^2 \equiv a' \bmod 9$ and $84b'^3 \equiv 63a'b' \bmod 9^3$, that is, $4b'^3 \equiv 3a'b' \bmod 3^5$. From the last congruence we get $b' \in 3R$ (since $b'^3 \in 3R$ and 3 is unramified) and thus $a' \in 9R$ which implies $b' \in 9R$. Hence $b \in R$ and, by (3), $D_9(a,x) \in R[x]$; this yields $a \in R$ since the coefficient of x is $9a^4$.

For $n = 12$ from (1) and our results for $n = 3$ and $n = 4$ we immediately get $a, b \in R$ if $f_n(x) \in R[x]$. If $n = 16$ then by (1) and (vi) we conclude $2a, b \in R$. Hence, by (3), we have $D_{16}(a,x) - D_{16}(a,0) \in R[x]$ which implies $a \in R$ since the coefficient of x^2 is equal to $-2^6 a^7$ and 2 is unramified.

LEMMA 2.9. *Assume that R is integrally closed and $f(x) \in R[x]$ is a monic polynomial such that $f(x) = (\tilde{f}_1 \circ \cdots \circ \tilde{f}_r)(x)$ for $\tilde{f}_i(x) = \alpha_i D_{n_i}(\tilde{a}_i, \gamma_i x + \delta_i) + \beta_i$ with suitable positive integers n_i and elements $\tilde{a}_i, \alpha_i, \beta_i, \gamma_i, \delta_i$ in some extension field of K. If $n = \deg(f) \geq 1$ is not divisible by* char$K$ *then $f(x) = (f_1 \circ \cdots \circ f_r)(x)$ for $f_i(x) = D_{n_i}(a_i, x + b_i) + c_i \in R[x]$ with suitable $a_i, b_i, c_i \in K$ and $a_i = 0$ if and only if $\tilde{a}_i = 0$.*

PROOF. The assertion is trivial if $n = 1$. For $n > 1$ we may assume that $n_i > 1$ for all i. Let $f_r(x) = (\tilde{f}_r(x) - \tilde{f}_r(0))/(\alpha_r \gamma_r^{n_r})$. Since $f_r(x)$ is monic and $f_r(0) = 0$, Proposition 2.2(ii) implies that the coefficients of $(\tilde{f}_1 \circ \cdots \circ \tilde{f}_{r-1})(\alpha_r \gamma_r^{n_r} f_r(x) + \tilde{f}_r(0))$ and $f_r(x)$ belong to R if $r > 1$; for $r = 1$ we trivially have $f_r(x) \in R[x]$. If $n_r \geq 3$ then $f_r(x) = D_{n_r}(a_r, x + b_r) + c_r$ with $a_r, b_r, c_r \in K$ and $a_r = \tilde{a}_r/\gamma_r^2$ by Lemma 1.9(iii); if $n_r = 2$ and $f_r(x) = x^2 + d_r x$ then for every $a_r \in K$ we have $f_r(x) = D_2(a_r, x + b_r) + c_r$ with $b_r = d_r/2 \in K$ and suitable $c_r \in K$. Thus in any case we obtain $f_r(x) = D_{n_r}(a_r, x + b_r) + c_r$ with $a_r, b_r, c_r \in K$ and $a_r = 0$ if and only if $\tilde{a}_r = 0$. The assertion then follows by induction.

3. The Galois group of $f(x) - t$ over $K(t)$

We consider a polynomial $f(x)$ of degree $n \geq 2$ with coefficients in a field K. We assume that $f(x)$ is not a polynomial in x^p if $p =$ char$K > 0$. Then $f(x) - t$ is irreducible and separable over the function field $K(t)$; t and x are understood to be algebraically independent over K. The splitting field is denoted by L and the Galois group $G_f = G(L|K(t))$ is viewed as a permutation group of the roots $\xi_1, \ldots, \xi_n$ of $f(x) = t$.

https://doi.org/10.1017/S1446788700038349 Published online by Cambridge University Press

LEMMA 3.1. *G_f is primitive if and only if $f(x)$ is indecomposable over K.*

PROOF. G_f is primitive if and only if the stabilizer G_1 of ξ_1 is a maximal subgroup of G_f. This is the case if and only if there is no proper intermediate field between the fixed field $K(\xi_1)$ of G_1 and $K(f(\xi_1)) = K(t)$. From Lüroth's theorem it is not hard to see that the intermediate fields are precisely the fields $K(h(\xi_1))$ with $h(x) \in K[x]$ such that $f(x) = g(h(x))$ for some $g(x) \in K[x]$. (Cf. [30, p. 273]; note that the assumption $\mathrm{char}K = 0$ is not needed.) This proves our assertion since $K(\xi_1)$ has degree $\deg(h)$ over $K(h(\xi_1))$.

LEMMA 3.2. *G_f is doubly transitive if and only if $\Phi(x, y) = (f(x) - f(y))/(x - y) \in K[x, y]$ is irreducible.*

PROOF. The transitive group G_f is doubly transitive if and only if the stabilizer G_1 of ξ_1 is transitive on $\{\xi_2, \ldots, \xi_n\}$, that is, if and only if $\xi_2, \ldots, \xi_n$ are conjugate over the fixed field $K(\xi_1)$ of G_1. Denoting the leading coefficient of $f(x)$ by a we have $\Phi(x, \xi_1) = a(x - \xi_2) \cdots (x - \xi_n)$. Hence the last condition is equivalent to the irreducibility of $\Phi(x, \xi_1) \in K(\xi_1)[x]$. Since x and ξ_1 are algebraically independent over K this means that $\Phi(x, y) \in K(y)[x]$ is irreducible. By Gauss' lemma this is equivalent to the irreducibility of $\Phi(x, y) \in K[x, y]$, since $\Phi(x, y)$ has no non-constant factor which is independent of x for otherwise $f(x) = f(\alpha)$ for a root α of this factor over $\bar{K}$.

LEMMA 3.3. *G_f contains an n-cycle if n is not divisible by* $\mathrm{char}K$.

PROOF. If $\sigma : F_1 \longrightarrow F_2$ is an isomorphism of fields then the Galois group of a polynomial over F_1 (considered as a permutation group of the roots) is canonically isomorphic with the Galois group of the polynomial over F_2 which is obtained by applying σ to its coefficients. Thus it is sufficient to prove that the Galois group of $f(x) - t^n \in K(t^n)[x]$ contains an n-cycle.

Let F be the field of formal Laurent series $\sum_{k \geq k_0} c_k/t^k$ with $c_k \in \bar{K}$. We may regard $K(t)$ (and hence $K(t^n)$) as a subfield of F. Choose $\alpha \in \bar{K}$ with $\alpha^n = 1/a$ where a is the leading coefficient of $f(x)$. Then we may find $\eta(t) = \alpha t + \sum_{k \geq 0} c_k/t^k \in F$ such that $f(\eta(t)) = t^n$. For if $\eta(t)$ has the indicated form then $f(\eta(t)) = t^n(1 + \sum_{k \geq 0} d_k/t^{k+1})$ with $d_k = nc_k/\alpha + p_k(c_0, \ldots, c_{k-1})$ where each p_k is a polynomial with coefficients in K independent of the c_i; p_0 denotes a constant. Hence the c_k may be (uniquely) determined such that all d_k vanish.

Let ε be a primitive n-th root of unity. We have just proved that there are $\eta_j(t) = \alpha\varepsilon^j t + \cdots \in F$ with $f(\eta_j(t)) = t^n$ for every integer j; thus F contains n different roots of $f(x) - t^n$. Let σ be the automorphism of F which maps $\sum_{k \geq k_0} c_k/t^k$ onto

$\sum_{k\geq k_0} c_k\varepsilon^{-k}/t^k$. Then $\sigma(\eta_j(t)) = \eta_{j+1}(t)$ for all j since $\sigma(\eta_j(t)) = \alpha\varepsilon^{j+1}t + \cdots$ and $K(t^n)$ belongs to the fixed field of σ. Thus the Galois group of $f(x) - t^n$ over $K(t^n)$ contains an n-cycle.

LEMMA 3.4. *G_f contains an element with cycle type $(e_1, \ldots, e_r)$ if $e_1 \cdots e_r$ is not divisible by* char$K$ *and $e_1, \ldots, e_r$ are the multiplicities of the roots of $f(x) - c \in \bar{K}[x]$ for some $c \in \bar{K}$.*

PROOF. Let F be the field of formal Laurent series $\sum_{k\geq k_0} c_k t^k$ with $c_k \in \bar{K}$ and let e be the least common multiple of the e_i. By the remark at the start of the proof of Lemma 3.3 it is sufficient to show that the Galois group of $f(x) - c - t^e$ over the subfield $K(c + t^e)$ of F has an element of the desired cycle type.

Let $\alpha_1, \ldots, \alpha_r$ be the roots with multiplicities $e_1, \ldots, e_r$ of $f(x) - c$ and denote the coefficient of $(x - \alpha_i)^{e_i}$ in the expansion of $f(x) - c$ into powers of $x - \alpha_i$ by b_i. For every i we choose $\beta_i \in \bar{K}$ with $\beta_i^{e_i} = 1/b_i$. Let ε be a primitive e-th root of unity in $\bar{K}$. Then for every i and every integer j there is $\eta_{ij}(t) = \alpha_i + \beta_i\varepsilon^{je/e_i}t^{e/e_i} + \cdots \in F$ such that $f(\eta_{ij}(t)) = c + t^e$. Just note that for $\eta(t) = \alpha_i + \sum_{k\geq 1} c_k t^{ke/e_i}$ we have $f(\eta(t)) = c + b_i c_1^{e_i} t^e + t^e \sum_{k\geq 1} d_k t^{ke/e_i}$ with $d_k = b_i e_i c_1^{e_i - 1} c_{k+1} + p_k(c_1, \ldots, c_k)$ where p_k is a polynomial with coefficients in $\bar{K}$ independent of $c_1, c_2, \ldots$; hence for every $c_1 \neq 0$ we may (uniquely) determine c_k for $k \geq 2$ such that $f(\eta(t)) = c + b_i c_1^{e_i} t^e$.

Thus F contains $e_1 + \cdots + e_r = n$ different roots $\eta_{ij}(t)$ of $f(x) - c - t^e$. The automorphism σ of F which maps $\sum_{k\geq k_0} c_k t^k$ onto $\sum_{k\geq k_0} c_k\varepsilon^k t^k$ leaves $K(c + t^e)$ invariant and $\sigma(\eta_{ij}(t)) = \eta_{i,j+1}(t)$ for all i, j; hence σ induces a permutation of the roots that has cycle type $(e_1, \ldots, e_r)$.

REMARK 3.5. For $K = \mathbb{C}$ Lemma 3.1 is due to Ritt ([41, p. 53]; cf. [11] for an extension to char$K = 0$ and $K = \bar{K}$). The ('if' part of the) general version has been observed by Fried ([14, Lemma 2]; cf. [13, p. 109] for $K = \mathbb{Q}$). Lemma 3.2 is implicit in the work of Fried ([14, p. 46]). Lemma 3.3 and Lemma 3.4 have long been known for $K = \mathbb{C}$; in this case they have been derived by considering the Riemann surface of the inverse function of $f(x)$.

For $K = \mathbb{C}$, G_f is frequently called the 'monodromy group' of $f(x)$. Wegner states ([52, p. 8]) that according to a theorem of Ritt in [43] a polynomial with rational coefficients with imprimitive monodromy group is decomposable over $\mathbb{Q}$. He proves that the polynomial is decomposable over $\mathbb{Z}$ if it is monic and decomposable over $\mathbb{Q}$ (cf. Remark 2.5). Hence $f(x) \in \mathbb{Z}[x]$ is decomposable over $\mathbb{Z}$ if it is monic and has imprimitive monodromy group. Kurbatov (who refers to Wegner several times) uses this result but gives [43] as a reference ([28, p. 17]). One should remark, however, that Ritt exclusively deals with the case $K = \mathbb{C}$ and does not mention the fact that decomposability over $\mathbb{C}$ implies decomposability over $\mathbb{Q}$; cf. Proposition 2.2(ii). The

theorem concerning the connection of decomposability and imprimitivity is proved in [41]; in [43, p. 403] Ritt merely restates this result.

The preceding lemmas are required for the proof of Theorem 4.5. The rest of Section 3 is not needed in Section 4. In 3.6 and 3.11 we make use of some results on primitive permutation groups.

THEOREM 3.6. *Assume that $f'(x)$ has a simple root in $\bar{K}$ and $f(\alpha_1) \neq f(\alpha_2)$ if $\alpha_1, \alpha_2 \in \bar{K}$ are distinct roots of $f'(x)$. Then $G_f = S_n$ if* char$K$ *does not divide n.*

PROOF. Note that char$K \neq 2$ since otherwise $f''(x) = 0$. Let α be a simple root of $f'(x)$. Then $f(x) - f(\alpha) = (x - \alpha)^2 f_0(x)$ where $f_0(x) \in \bar{K}[x]$ has no multiple roots and $f_0(\alpha) \neq 0$. Thus Lemma 3.4 implies that G_f contains a transposition. The symmetric group S_n is the only primitive permutation group of degree n which contains a transposition (cf. [54, p. 34]; [24, p .171]); hence in view of Lemma 3.1 it remains to prove that $f(x)$ is indecomposable over K.

If $f(x)$ is decomposable then $f(x) = g(h(x))$ for some $g(x) \in K[x]$ with degree $r > 1$ and some monic polynomial $h(x) \in K[x]$ with degree $s > 1$. Choose $\beta, \gamma \in \bar{K}$ such that $g'(\beta) = 0$ and $h(\gamma) = \beta$. (Note that $\deg(g') = r - 1 \geq 1$ since r is not divisible by char$K$.) Since $f'(\gamma) = g'(\beta)h'(\gamma) = 0$ and $f(\gamma) = g(\beta)$, our assumptions imply that for every β there is precisely one choice for γ. Hence for every β with $g'(\beta) = 0$ there is a (unique) γ such that $h(x) = (x - \gamma)^s + \beta$. Since this equation implies that $-s\gamma$ is the coefficient of x^{s-1} in $h(x)$, γ and $\beta = h(\gamma)$ are uniquely determined. Thus $g'(x) = b(x - \beta)^{r-1}$ for some $b \in \bar{K}$ and $f'(x) = g'(h(x))h'(x) = bs(x - \gamma)^{rs-1}$ which contradicts the assumption that $f'(x)$ has a simple root.

COROLLARY 3.7. *Let n, k be integers with $n > k \geq 1$ and $(n, k) = 1$. If $nk(n - k)$ is not divisible by* char$K$ *then, for arbitrary non-zero $a, b \in K$, the polynomial $x^n + ax^k + bt$ has Galois group S_n over $K(t)$.*

PROOF. Let $f(x) = -(x^n + ax^k)/b$. Then $f(x)$ is not a polynomial in x^p if $p =$ char$K > 0$ and all non-zero roots of $f'(x) = -x^{k-1}(nx^{n-k} + ak)/b$ are simple. If $\alpha \neq 0$ is a root of $f'(x)$ then $\alpha^{n-k} = -ak/n$ and $f(\alpha) = -(n - k)a\alpha^k/bn$; hence $f(\alpha) \neq 0 = f(0)$ and α is uniquely determined by $f(\alpha)$ since $(n - k, k) = 1$. Thus $x^n + ax^k + bt = -b(f(x) - t)$ has Galois group S_n over $K(t)$ by Theorem 3.6; note that char$K \neq 2$.

COROLLARY 3.8. *Let $n \geq 2$ and assume that $n(n - 1)$ is not divisible by* char$K$. *Then, for arbitrary non-zero $a, b \in K$, $x^n + atx + bt$ has Galois group S_n over $K(t)$.*

PROOF. Choose u with $u^{n-1}t = 1$; then $K(u)$ is an extension field of $K(t)$ and the Galois group of $\varphi(x) = x^n + atx + bt$ over $K(u)$ is a subgroup of the Galois group of $\varphi(x)$ over $K(t)$ (if this exists at all). Hence it is sufficient to prove that the former is S_n and this follows from Corollary 3.7 since $\varphi(x) = u^{-n}((ux)^n + a(ux) + bu)$. (And from this it also follows that $\varphi(x)$ is irreducible and separable over $K(u)$ and hence over $K(t)$.)

REMARK 3.9. Theorem 3.6 has been stated by Hilbert for $K = \mathbb{C}$ (and $f(x) \in \mathbb{Z}[x]$) under the additional assumption that all roots of $f'(x)$ are simple ([23, p. 124]); for finite fields this has been proved by Birch and Swinnerton-Dyer together with a related result if n is a prime ([3, Lemma 3]). Corollary 3.7 is due to Hering in the case $K = \mathbb{Q}$ ([22, p. 134]). Corollary 3.8 is related to a result of Matzat for $K = \mathbb{Q}$ ([33, p. 84]). In all cases the proof depends upon the theory of Riemann surfaces (over $\mathbb{C}$). Hayes [58] has used the Hurwitz genus formula for proving a special case of Corollary 3.7 if $K = \mathbb{F}_p$. Corollary 3.7 fails for $(n, k) > 1$ since then the Galois group is imprimitive by Lemma 3.1.

LEMMA 3.10. *Let $g(x), h(x) \in K[x]$ have degrees ≥ 2 and assume that neither $g(x)$ nor $h(x)$ is a polynomial in x^p if $p = \mathrm{char}K > 0$. Then this also holds for $g(h(x))$ and $G_{g\circ h}$ is solvable if and only if G_g and G_h are solvable.*

PROOF. By assumption, $g'(x)$ and $h'(x)$ have positive degree; hence $g(h(x))$ is not a polynomial in x^p if $p = \mathrm{char}K > 0$ since the derivative $g'(h(x))h'(x)$ has positive degree.

Assume that $G_{g\circ h}$ is solvable and let ξ be an element of the splitting field such that $g(h(\xi)) = t$. Then G_g is solvable since $h(\xi)$ is a root of $g(x) = t$. Observe that G_h is canonically isomorphic with the Galois group of $h(x) - h(\xi)$ over $K(h(\xi))$. Hence G_h is solvable since this polynomial has the root ξ in a solvable extension of $K(h(\xi))$.

Conversely, let G_g and G_h be solvable. Let $\xi_1, \ldots, \xi_r$ be the roots of $g(x) = t$ and $\xi_{i1}, \ldots, \xi_{is}$ be the roots of $h(x) = \xi_i$ $(i = 1, \ldots, r)$ in some fixed algebraic closure of $K(t)$. By assumption, $L = K(\xi_1, \ldots, \xi_r)$ is a solvable extension of $K(t)$. Since G_h is isomorphic with the Galois group of $h(x) = \xi_i$ over $K(\xi_i)$, $K(\xi_{i1}, \ldots, \xi_{is})$ is a solvable extension of $K(\xi_i)$ for every $i = 1, \ldots, r$. Hence $L(\xi_{i1}, \ldots, \xi_{is})$ is a solvable extension of $L = L(\xi_i)$ for every $i = 1, \ldots, r$ and the same holds for the splitting field of $g(h(x)) = t$ since it is the compositum of the fields $L(\xi_{i1}, \ldots, \xi_{is})$. Thus the splitting field is solvable over $K(t)$ because it is a solvable extension of a solvable extension of $K(t)$.

THEOREM 3.11. *Assume that* $\mathrm{char}K = 0$ *or* $\mathrm{char}K > n = \deg(f)$. *Then the following properties are equivalent:*

https://doi.org/10.1017/S1446788700038349 Published online by Cambridge University Press

(i) *G_f is solvable.*

(ii) *$f(x)$ is a composition of polynomials $f_i(x) \in K[x]$ each of which has degree 4 or is of the form $\alpha_i D_{n_i}(a_i, x + b_i) + c_i$ with $\alpha_i, a_i, b_i, c_i \in K$ and prime n_i.*

(iii) *$f(x)$ is a composition of polynomials $f_i(x)$ over some extension field of K such that each of these has degree 4 or is linearly related to a Dickson polynomial.*

PROOF. Assume that G_f is solvable and write $f(x) = (f_1 \circ \cdots \circ f_r)(x)$ with indecomposable polynomials $f_i(x) \in K[x]$ of degree > 1. By Lemma 3.1 and Lemma 3.10 the Galois group G_{f_i} of $f_i(x) - t$ over $K(t)$ is primitive and solvable for every $i = 1, \ldots, r$; hence $n_i = \deg(f_i)$ is a prime power (cf. [24, p. 159; 39, p. 25]). Moreover, G_{f_i} contains an n_i-cycle by Lemma 3.3; thus by a theorem of Ritt we conclude that $n_i = 4$ or n_i is a prime ([42, p. 27]; cf. [24, pp. 169, 250]). If n_i is a prime then the identity is the only element of G_{f_i} with more than one fixed point (cf. [24, p. 163]) and this easily implies that each element is an n_i-cycle or has cycle type $(1, r, \ldots, r)$ for some $r \geq 1$. Thus by Lemma 3.4 we see that, for every $c \in \bar{K}$, $f_i(x) - c$ is an n_i-th power or has one simple root and $(n_i - 1)/r$ roots of multiplicity r. If the first case occurs for some $c = c_i$ then $f_i(x) = \alpha_i(x + b_i)^{n_i} + c_i$ for some $\alpha_i \in K$ and $b_i \in \bar{K}$; this implies $b_i, c_i \in K$ and $f_i(x) = \alpha_i D_{n_i}(0, x + b_i) + c_i$. If always the second case holds then $n_i \geq 3$ and $f_i(x) = \alpha_i D_{n_i}(a_i, x + b_i) + c_i$ for suitable $\alpha_i, a_i, b_i, c_i \in K$ by Lemma 1.11. Hence (ii) follows from (i).

In view of Lemma 3.10, in order to prove the converse it is sufficient to show that G_f is solvable if $n = 4$ or $f(x) = D_n(a, x)$. This is clear for $n = 4$ since S_4 is solvable. If $f(x) = D_n(a, x)$ then G_f is solvable since $f(x) = t$ has the root $v + a/v$ where $v^n = u$ for some u with $t = u + a^n/u$, that is, one can get a root by adjoining radicals to the ground field $K(t)$.

We complete the proof by showing that (iii) implies (ii); the converse is trivial. If (iii) holds then $f(x) = (f_1 \circ \cdots \circ f_r)(x)$ where all $f_i(x)$ have the specified properties; for $r > 1$ we also may assume that $f_r(x)$ is monic and $f_r(0) = 0$. Hence for $r > 1$ by Proposition 2.2(ii) (with K instead of R) we have $(f_1 \circ \cdots \circ f_{r-1})(x) \in K[x]$ and $f_r(x) \in K[x]$; if $r = 1$ then the latter holds trivially. If $f_r(x)$ is linearly related to a Dickson polynomial, then Lemma 1.9 yields $f_r(x) = \alpha_r D_{n_r}(a_r, x + b_r) + c_r$ with suitable $\alpha_r, a_r, b_r, c_r \in K$. Thus inductively we see that $f(x)$ satisfies (ii), taking into account that (for $n_r > 1$) $D_{n_r}(a_r, x)$ can be written as a composition of polynomials of the same kind with prime degree by Lemma 1.1(ii).

REMARK 3.12. It is sufficient to assume that $f(x)$ is tame (see Definition 4.1 and Remark 4.2). The implication '(i) implies (ii)' for $K = \mathbb{C}$ is due to Ritt ([42, p. 27]) who also investigated under which circumstances a polynomial over $\mathbb{C}(t)$ has solvable Galois group. If $K = \bar{\mathbb{Q}}$ and G_f is abelian then, according to Fried,

$f(x) = a(x-b)^n + c$ for suitable a, b, c ([13, p. 102]).

4. The main results

R denotes an integral domain with quotient field K (with algebraic closure $\bar{K}$).

DEFINITION 4.1. A polynomial $f(x) \in K[x]$ of degree $n \geq 1$ is called *tame* (over K) if and only if char$K$ neither divides n nor the multiplicity of a zero of $f(x) - c \in \bar{K}[x]$ for any $c \in \bar{K}$.

REMARK 4.2. Clearly, $f(x)$ is tame if char$K = 0$ or char$K > n$. It is very easy to see that $g(h(x))$ is tame if and only if $g(x), h(x)$ are tame; we omit the proof here. If L is some extension field of K (such that x is transcendental over L) then $f(x)$ is tame over K if and only if it is tame over L; for, if $\alpha_1, \ldots, \alpha_r \in \bar{L}$ are the distinct zeros of $f(x) - c$ (with $c \in \bar{L}$), there exists a ring-homomorphism over K from $K[\alpha_1, \ldots, \alpha_r, c]$ into $\bar{K}$ such that $\alpha_1, \ldots, \alpha_r$ have distinct images ([29, p. 256]). (This fact will only be used in 4.11.)

The term 'tame' has been used by Fried in [14] with a slightly different meaning. For $p = \text{char}K > 0$ he demands [14, p. 42] that $(p, n) = 1$ and $(p, m+1) = 1$ for every m which is a multiplicity of a zero of $f'(x)$. If $\alpha \in \bar{K}$ is a zero of $f'(x)$ with multiplicity m then α is a zero of $f(x) - f(\alpha)$ with multiplicity $e \geq 2$ and if $(p, e) = 1$ then $m = e - 1$. Hence a polynomial that is tame in our sense is also tame in the sense of Fried. Taking $f(x) = x^p(x+1)$ shows that the converse fails; here we have $m = e = p$ for the unique root $\alpha = 0$ of $f'(x)$. Fried's proof of Lemma 5 ([14, p. 44]) requires our definition of 'tame'.

In order to prove Theorem 4.5 (=Theorem 1) we need two theorems on permutation groups.

LEMMA 4.3. *If a transitive permutation group of prime degree n is not doubly transitive then it may be identified with a group of permutations of $\mathbb{Z}/n\mathbb{Z}$ which are induced by linear polynomials.*

This result of Burnside is proved in [24, pp. 609, 163], [39, p. 53] and [61, p. 127].

LEMMA 4.4. *Let G be a primitive permutation group of degree n. If G contains an n-cycle then G is doubly transitive or n is a prime.*

A proof of this theorem of Schur can be found in [49], [54, Theorem 25.3], and [61, p. 126]. (Wielandt proves that $\mathbb{Z}/n\mathbb{Z}$ is a B-group (defined in 25.1) if n is composite and it is easy to see that then G has to be doubly transitive. Instead of appealing to

23.7 (which, as W. Knapp has kindly pointed out to me, is apparently not applicable) in line 17 of p.66, one should observe that the subgroup has $1+a$ elements; this yields the desired contradiction, since $1 < 1+a < p = |U|$.)

THEOREM 4.5. *Let $f(x) \in K[x]$ be a tame polynomial of degree $n > 1$ and set $\Phi_f(x, y) = (f(x) - f(y))/(x - y) \in K[x, y]$. Then the following assertions are equivalent:*

(i) *$\Phi_f(x, y)$ is irreducible over $\bar{K}$.*
(ii) *$\Phi_f(x, y)$ is irreducible over $K(\zeta)$ where ζ is a primitive n-th root of unity.*
(iii) *$f(x)$ is indecomposable over K and if n is an odd prime then we do not have $f(x) = \alpha D_n(a, x + b) + c$ for $\alpha, a, b, c \in K$ with $a = 0$ if $n = 3$.*

PROOF. We may assume $n \geq 3$ since the assertion is trivial for $n = 2$. If (i) holds then clearly (ii) also holds; note that ζ exists since char$K$ does not divide n. If (ii) holds then $f(x)$ obviously is indecomposable over K and for $n > 3$ from Proposition 1.7 we see that $f(x)$ is not linearly related to a Dickson polynomial; if $n = 3$ then we clearly cannot have $f(x) = \alpha D_n(0, x + b) + c = \alpha(x + b)^3 + c$.

It remains to prove that (iii) implies (i). If $f(x) = \alpha D_3(a, x + b) + c$ with $a \neq 0$ then $\Phi_f(x, y)$ is absolutely irreducible (by Proposition 1.7); hence (by Lemma 1.9(i)) in the sequel we may assume that $f(x)$ satisfies (iii) and $n > 3$. Then $f(x)$ is indecomposable over $\bar{K}$ by Proposition 2.2(ii) and the Galois group G_f of $f(x) - t$ over $\bar{K}(t)$ is primitive by Lemma 3.1. Assume that (i) fails; then G_f is not doubly transitive by Lemma 3.2. Since G_f contains an n-cycle by Lemma 3.3, from Lemma 4.4 we conclude that n is a prime. Hence Lemma 4.3 yields that G_f can be identified with a group of permutations of $\mathbb{Z}/n\mathbb{Z}$ induced by linear polynomials. Thus the identity is the only element of G_f with more than one fixed point and this easily implies that each element is an n-cycle or has cycle type $(1, r, \ldots, r)$ for some $r \geq 1$. Hence by Lemma 3.4 we see that, for every $c \in \bar{K}$, $f(x) - c$ is an n-th power or has one simple root and $(n - 1)/r$ roots of multiplicity r. If the first case occurs for c then $f(x) = \alpha(x + b)^n + c$ for some $\alpha, b \in \bar{K}$; this implies $\alpha, b, c \in K$ and $f(x) = \alpha D_n(0, x + b) + c$, contrary to hypothesis. If the second case always holds then Lemma 1.11 yields the desired contradiction. (These arguments have already been used in the proof of 3.11.)

REMARK 4.6. The implication '(iii) implies (i)' is due to Fried for $K = \bar{K}$ and $n > 3$ ([14, p. 45]); he also makes use of the theorems of Burnside and Schur. Fried essentially requires that $f(x)$ is not linearly related to x^n or $D_n(1, x)$. (Note that we have $D_n(a, x) = (\sqrt{a})^n D_n(1, x/\sqrt{a})$ by Lemma 1.1(ii).) This assumption forces $n > 3$. Fried's theorem is restated in [46, p. 57] for char$K = 0$ in the form of an equivalence (although Fried did not claim the converse); the exceptional case $n = 3$

has been overlooked there. The equivalence of (i) and (ii) is a special case of [30, p. 195, Lemma 8.5]. A version of Theorem 4.5 for finite fields is a crucial ingredient in Cohen's recent proof of the Chowla – Zassenhaus conjecture [6].

If $f(x)$ is not tame then (iii) may hold although (i) fails. Set $f(x) = x^p - x$ with $p = \mathrm{char}K > 0$. Then $f(x)$ is indecomposable since the degree is a prime and not of the form $\alpha D_p(a, x+b)+c$ since this is a polynomial in x^p; recall that $D_p(a, x) = x^p$. Nevertheless, $\Phi_f(x, y) = (x - y)^{p-1} - 1$ splits into linear factors over the prime field of K and thus is reducible if $p > 2$. For $K = \bar{\mathbb{F}}_p$, less trivial examples (due to Cohen) are given by $f(x) = x(x^{(p-1)/d} - c)^d$ where $1 < d \mid (p-1)$ and $c \neq 0$; all irreducible factors of $\Phi_f(x, y)$ have degree d ([8, Theorem 2.1]). Cohen's results in [7, 8] (concerning the question when $\Phi_f(x, y)$ has linear or quadratic factors) perhaps indicate that n must be a power of p if (iii) holds while (i) fails. (There is a gap in the argument of [8] but the main result holds if $f(x)$ is indecomposable over $\bar{\mathbb{F}}_p$.) (Added in proof: Counterexamples are provided by a recently discovered class of indecomposable polynomials over $\mathbb{F}_2$, see [56].)

In order to prove Theorem 2 we have to know that $f(x)$ is not a p.p. mod P if the reduction of $\Phi_f(x, y)$ mod P is absolutely irreducible and $|R/P|$ is sufficiently large. This is a simple consequence of the following (weak) version of Weil's estimate of the number of points on an absolutely irreducible curve over a finite field.

LEMMA 4.7. *Let N be the number of zeros of an absolutely irreducible polynomial $\Phi(x, y) \in \mathbb{F}_q[x, y]$ of total degree $d \geq 1$. If $q > 250d^5$ then $|N - q| < \sqrt{2d^5 q}$.*

An elementary (but still difficult) proof may be found in [47, p. 92]. Much nicer and better bounds are known; for example $|N - q - 1| \leq (d-1)(d-2)\sqrt{q} + d$ holds for all q ([19, Theorem 4.9]) and this will be used in the proof of Theorem 4.17 for $n = 5, 7$. (Added in proof: See [60] for the correction of a mistake in [19].)

LEMMA 4.8. *Assume that $f_1(x), \ldots, f_r(x) \in K[x]$ are polynomials such that $f(x) = (f_1 \circ \cdots \circ f_r)(x)$ has coefficients in R. Let I be an ideal of finite norm and assume that $a_1 f_1(x), \ldots, a_r f_r(x) \in R[x]$ for some $a_i \in R$ which are invertible* mod I. *Then $f(x)$ is a p.p.* mod I *if and only if all the $a_i f_i(x)$ are p.p.* mod I.

PROOF. Set $a = a_1 \cdots a_r$ and choose $b \in R$ with $ab \equiv 1 \bmod I$. Note that $a_i f_i(x)$ is a p.p. mod I if and only if $g_i(x) = abf_i(x)$ is a p.p. mod I. A composition of functions on the finite set R/I is bijective if and only if all these functions are bijective. Hence $g(x) = (g_1 \circ \cdots \circ g_r)(x)$ is a p.p. mod I if and only if all the $g_i(x)$ are p.p. mod I. It is therefore sufficient to prove that $f(x) \equiv g(x) \bmod I$ and this is easily seen by multiplying both sides with a sufficiently large power of ab.

https://doi.org/10.1017/S1446788700038349 Published online by Cambridge University Press

THEOREM 4.9. *Assume that, for every non-zero $a \in R$, the prime ideals of finite norm which contain a have bounded norm. Let $f(x) \in R[x]$ be a tame polynomial which is a p.p. for prime ideals of arbitrarily large finite norm.*

Then $f(x)$ is a composition of linear polynomials $\alpha_i x + \beta_i \in K[x]$ and Dickson polynomials $D_{n_j}(a_j, x)$ with $a_j \in R$ where every n_j is an odd prime and $a_j = 0$ if $n_j = 3$.

PROOF. We may assume that $n = \deg(f) > 1$. If $f(x)$ is a p.p. mod P then $\Phi_f(\xi, \eta) = (f(\xi) - f(\eta))/(\xi - \eta) \not\equiv 0 \bmod P$ if $\xi \not\equiv \eta \bmod P$; hence the number of zeros of $\Phi_f(x, y) = f'(x) + (x - y)(\ldots) \bmod P$ is at most $\deg(f') = n - 1$ if $na_n \notin P$ where a_n denotes the leading coefficient of $f(x)$. Thus Lemma 4.7 implies that the reduction of $\Phi_f(x, y) \bmod P$ is not absolutely irreducible if $|R/P|$ is finite and sufficiently large. Hence there are prime ideals P of arbitrarily large finite norm such that the reduction of $\Phi_f(x, y) \bmod P$ is not absolutely irreducible.

A polynomial $\Phi(x, y) = \sum_{i+j \le d} a_{ij} x^i y^j$ of degree $d \ge 1$ with coefficients in a field F is absolutely irreducible if and only if there is no common zero over $\bar{F}$ of the polynomials $p_{ij} = c_{ij} - a_{ij}$ $(0 \le i, j \le d)$ where c_{ij} is the coefficient of $x^i y^j$ in

$$\sum_{i_1 + j_1 < d} u_{i_1 j_1} x^{i_1} y^{j_1} \sum_{i_2 + j_2 < d} v_{i_2 j_2} x^{i_2} y^{j_2}$$

(and the $u_{i_1 j_1}$, $v_{i_2 j_2}$ are independent variables). By Hilbert's Nullstellensatz this holds if and only if there are polynomials q_{ij} with coefficients in F such that $1 = \sum p_{ij} q_{ij}$.

Assume that $\Phi_f(x, y)$ is absolutely irreducible and let p_{ij}, q_{ij} be defined as above. Choose $a \in R$ such that a is divisible by the leading coefficient of $f(x)$ and the polynomials aq_{ij} have coefficients in R. Then, for every prime ideal P with $a \notin P$, the reduction of $\Phi_f(x, y) \bmod P$ has the same degree as $\Phi_f(x, y)$ and is absolutely irreducible since (by the above remark applied to $F = R/P$) otherwise the polynomials p_{ij} must have a common zero mod P which is obviously not the case. Thus the reduction of $\Phi_f(x, y) \bmod P$ is absolutely irreducible for every P with sufficiently large finite norm, a contradiction to what we have proved before.

Hence $\Phi_f(x, y)$ is not absolutely irreducible. If $f(x)$ is indecomposable over K then Theorem 4.5 implies that n is an odd prime and $f(x)$ is linearly related to $D_n(a, x)$ for some $a \in K$ with $a = 0$ if $n = 3$. By Lemma 1.1(ii) we even may assume $a \in R$, thus finishing the proof in the case that $f(x)$ is indecomposable.

In the general case we write $f(x) = (f_1 \circ \cdots \circ f_r)(x)$ with indecomposable non-linear polynomials $f_i(x) \in K[x]$. Note that all $f_i(x)$ are tame (cf. Remark 4.2). Choose $a \in R$, $a \neq 0$, such that $af_i(x) \in R[x]$ for all i. Our assumptions imply that there are prime ideals P of arbitrarily large finite norm such that $a \notin P$ and $f(x)$ is a p.p. mod P. Hence, by Lemma 4.8, each of the polynomials $af_i(x)$ satisfies the same requirements as $f(x)$. Thus, by what we have seen above, $f(x)$ is a composition of polynomials of the required kind.

Theorem 2 is an immediate consequence of Theorem 4.9 and the following fact.

LEMMA 4.10. *Let R be an integral domain such that R/I is finite for every ideal $I \neq \{0\}$. Then for every non-zero $a \in R$ the number of ideals containing a is finite and for every positive integer m the number of ideals of norm m is finite.*

PROOF. Let a be a non-zero element of R. There is a one-to-one correspondence between the ideals I of R with $a \in I$ and the ideals of R/aR. Since $|R/aR|$ is finite, a is contained in only finitely many ideals. If I is an ideal of norm m then (by elementary group theory) $m(1 + I)$ is the zero element of R/I, that is, $m \in I$. Thus for $\mathrm{char}K = 0$ it follows that there are only finitely many possibilities for I if m is fixed.

Now assume that $p = \mathrm{char}K > 0$. If every element of R is algebraic over the prime field $\mathbb{F}_p$ then R is a field and the assertion is trivial. Hence we may suppose that R contains the polynomial ring $R_0 = \mathbb{F}_p[t]$. Let I be an ideal of R with $|R/I| = m$ and put $I_0 = R_0 \cap I$. Since R_0/I_0 can be canonically embedded into R/I, we have $|R_0/I_0| \leq m$. Hence $I_0 \neq \{0\}$ and there are only finitely many possibilities for I_0; note that $|R_0/I_0| \leq m$ holds if and only if I_0 is generated by a polynomial of degree r with $p^r \leq m$. Since I contains I_0, from the first part of the proof we conclude that only finitely many ideals I yield the same I_0. Thus the number of ideals I with $|R/I| = m$ is finite. (Cf. Remark 4.13).

COROLLARY 4.11. *Let q be a power of a prime p and let $f(x) \in \mathbb{F}_q[x]$ be tame. If $f(x)$ is a p.p. for infinitely many finite extension fields of $\mathbb{F}_q$ then it is a composition of linear polynomials $\alpha_i x + \beta_i \in \mathbb{F}_q[x]$ and Dickson polynomials $D_{n_j}(a_j, x)$ with $a_j \in \mathbb{F}_q$ where every n_j is an odd prime and $a_j = 0$ if $n_j = 3$.*

PROOF. For every $r \geq 1$ there exists an irreducible polynomial over $\mathbb{F}_q$ of degree r and thus a prime ideal P of $R = \mathbb{F}_q[t]$ with $R/P \cong \mathbb{F}_{q^r}$. We interprete $f(x)$ as a polynomial over R. Then the reduction of $f(x)$ mod P is $f(x)$ again and thus $f(x)$ is a p.p. mod P if and only if $f(x)$ is a p.p. of $\mathbb{F}_{q^r}$. Hence $f(x)$ is a p.p. mod P for infinitely many P and the assertion is seen to follow from Theorem 2 and Lemma 2.9 (applied to $\mathbb{F}_q$); note that $f(x)$ is tame over the quotient field of R (by Remark 4.2).

REMARK 4.12. It is not always true that, under the hypotheses of Theorem 4.9 (or Theorem 2), $f(x)$ is a composition of linear polynomials $\alpha_i x + \beta_i \in R[x]$ and Dickson polynomials $D_{n_j}(a_j, x) \in R[x]$; even for $R = Z$ and prime degree one can find counterexamples ([50, Section 3]).

Theorem 4.9 is essentially due to Fried in the case where R is the ring of algebraic integers of some number field ([14, Theorem 2]); cf. Section 5. We have derived

Theorem 4.9 in almost the same way from the implication '(iii) implies (i)' of Theorem 4.5 as he did.

Fried also stated that a polynomial which is tame and exceptional over a finite field K is a composition of polynomials $\alpha_i x^{n_i} + \beta_i \in \bar{K}[x]$ and Chebyshev polynomials $T_n(x)$ ([16, Theorem 1]); $f(x)$ is called exceptional if $\Phi_f(x, y) \in K[x, y]$ has no absolutely irreducible factor. By means of Lemma 4.7 it is easy to see that $f(x)$ is exceptional if $f(x)$ is a p.p. for infinitely many finite extension fields of K and $\deg(f)$ is not divisible by $p = \mathrm{char}K$ (cf. the first lines in the proof of [30, p. 200, Theorem 4.9]). Conversely, every exceptional polynomial over a finite field is a p.p. for infinitely many finite extensions of this field; this is an easy consequence of a theorem of Cohen that states that every exceptional polynomial over a finite field is a p.p of this field ([5, Theorem 5]; cf. also [30, p.192; 31, p.363]). (Added in proof: See [62, p. 68] for a simple proof of a result of Wan from which, as Wan has pointed out, Cohen's theorem can be derived.) Hence Fried's result is more or less the same as Corollary 4.11; his argument is somewhat different.

REMARK 4.13. If all elements of R are algebraic integers in some number field then $|R/I|$ is finite for every ideal $I \neq \{0\}$. This is seen by observing that the constant term $a \in \mathbb{Z}$ of the minimal polynomial of any non-zero element of I belongs to I and thus $|R/I| \leq |R/aR|$ is finite since R is a finitely generated $\mathbb{Z}$-module. (Note that R is a $\mathbb{Z}$-submodule of the ring of algebraic integers in K which is a free Z-module with $[K : \mathbb{Q}] < \infty$ generators.)

The rings R such that $|R/I|$ is finite for every non-zero ideal I are called *residually finite* (abbreviated as r.f.) and studied in [4]. An integral domain R is r.f. if and only if every non-zero prime ideal is finitely generated and has finite norm [4, p. 93]. It is clear that every r.f. domain is Noetherian and every non-zero prime ideal is maximal. If R is a Noetherian integral domain then R is r.f. if and only if the integral closure of R is r.f. [4, p. 96]; this generalizes our example given above.

If R is only required to be Noetherian then the first part of Lemma 4.10 may fail; consider the end of the following remark. The second part, however, remains true by [45, Proposition 13]; I am indebted to Peter Schmid for this information.

REMARK 4.14. Theorem 4.9 applies to every Dedekind domain R since every non-zero $a \in R$ belongs to only finitely many ideals. The following example shows that the conclusion fails if we merely assume that $f(x)$ is a p.p. for infinitely many prime ideals.

Let $n > 3$ be a prime and set $f(x) = x^n + x$. Then $f(x)$ is a p.p. of $\mathbb{R}$ and is not a composition of Dickson polynomials and linear polynomials with coefficients in some extension field of $\mathbb{R}$ (since $f(x)$ is indecomposable and clearly not linearly related to

a Dickson polynomial). We may view $f(x)$ as a polynomial over $R = \mathbb{R}[t]$; x, t are understood to be independent variables. For every $a \in \mathbb{R}$ the ideal $P = (t - a)$ of R is a maximal ideal and R/P is isomorphic to $\mathbb{R}$. Since the reduction of $f(x)$ mod P is $f(x)$ again, we see that $f(x)$ is a p.p. mod P. Hence $f(x)$ is a p.p. for infinitely many prime ideals although it is not a composition of Dickson polynomials and linear polynomials.

Not even for Noetherian domains may one omit the first hypothesis in Th. 4.9. For, if the reduction mod 2 of $g(t) \in \mathbb{Z}[t]$ is irreducible and has degree d, then $P = (2, g(t))$ is a prime ideal of $R = \mathbb{Z}[t]$ with norm 2^d. Clearly, $f(x) = x^2$ is a p.p. mod P although the conclusion of 4.9 fails.

REMARK 4.15. Theorem 4.9 (Theorem 2) need not hold for non-tame polynomials. As an example, let $R = \mathbb{F}_p[t]$ and $f(x) = x^p + x$ where p is an odd prime. If r is an odd integer then $(p^r - 1)/(p - 1)$ is odd and hence there is no $a \in \mathbb{F}_{p^r}$ with $a^{p-1} = -1$ since $a^{p^r-1} = 1$ for $a \neq 0$. Thus from $f(x) - f(y) = (x - y)((x - y)^{p-1} + 1)$ we see that $f(x)$ is a p.p. of $\mathbb{F}_{p^r}$ for odd r. Hence, as we have seen in the proof of Corollary 4.11, $f(x)$ is a p.p. mod P for suitable P with arbitrarily large norm. Also, every non-zero ideal of R has finite norm. Nevertheless, $f(x)$ is not a composition of linear polynomials and Dickson polynomials, since the degree p is a prime and $D_p(a, x) = x^p$.

REMARK 4.16. It is worth while pointing out that for the proof of Theorem 4.9 (and Theorem 2) not too much of what we have done so far is actually needed. We have seen in 4.9 (and 4.10) that the desired result follows from Theorem 4.5, Weil's estimate quoted in 4.7, the elementary Lemma 4.8, and some simple considerations employing Hilbert's Nullstellensatz. From 4.5 we only make use of the implication '(iii) implies (i)' which depends on 1.11, the first part of 2.2(ii), 3.1 – 3.4, and the theorems of Burnside and Schur quoted in 4.3 and 4.4. All the information we need about Dickson polynomials is contained in the basic results 1.1 and 1.9 which are sufficient for the proof of 1.11; we do not even need Lemma 1.4. Theorem 4.5 is only required for the same K as appearing in Theorem 2 (or 4.9). In the proof of Theorem 5 (or 4.17), however, 4.5 is applied to finite fields.

The rest of Section 4 is devoted to 'quantitative' versions and the converse of Theorem 4.9 in the number field case.

THEOREM 4.17. *Let R be the ring of algebraic integers in a number field K of degree d. Let $f(x) = \sum_{k=0}^{n} a_k x^k \in R[x]$ have prime degree n and let C be a real number such that the image of every coefficient under every embedding of K into $\mathbb{C}$ has modulus at most C. Then we have:*

https://doi.org/10.1017/S1446788700038349 Published online by Cambridge University Press

(i) *If $f(x)$ is a p.p. for some prime ideal P of norm at least $(nC)^{nd}$ then $n > 2$ and $f(x) = (D_n(a, a_n x + b) + c)/a_n^{n-1}$ with $a = (((n-1)/2n)a_{n-1}^2 - a_n a_{n-2})/n$, $b = a_{n-1}/n$, and suitable $c \in K$; $a = 0$ if $n = 3$. Moreover, $na_n \notin P$ and $n^2 a \in (R \setminus P) \cup \{0\}$. If n is unramified then $a, b, c \in R$.*

(ii) *Assume that $a_n = 1$ and $a_{n-1} = 0$. If $f(x)$ is a p.p. for some prime ideal of norm at least $(n\sqrt{C})^{nd}$ then $n > 2$ and $f(x) = D_n(a, x) + a_0$ with $a = -a_{n-2}/n$.*

PROOF. For $\alpha \in K$ we define $\|\alpha\| = \max\{|\alpha^{(1)}|, \dots, |\alpha^{(d)}|\}$ where $\alpha^{(1)}, \dots, \alpha^{(d)}$ are the images of α under the embeddings of K into $\mathbb{C}$; $\|.\|$ is a norm on the vector space K over $\mathbb{Q}$ and $\|\alpha\beta\| \le \|\alpha\|\|\beta\|$. We extend the definition by putting $\|\sum_{j=0}^{m} \alpha_j x^j\| = \max\{\|\alpha_0\|, \cdots, \|\alpha_m\|\}$; this yields a norm on the vector space $K[x]$ over $\mathbb{Q}$. If $\alpha \in R$ and $\alpha \neq 0$ then $\|\alpha\| \ge 1$ since $\alpha^{(1)} \cdots \alpha^{(d)} \in \mathbb{Z}$. If $\alpha \neq 0$ belongs to an ideal I of R then $\|\alpha\|^d \ge NI$; this follows from $NI \le NA = |\alpha^{(1)} \cdots \alpha^{(d)}| \le \|\alpha\|^d$ for $A = \alpha R$.

Let P be a prime ideal with $NP \ge (n\sqrt{C})^{nd}$. Note that $C \ge 1$ and $NP = p^f$ with $f \le d$ (where $p = \mathrm{char} R/P$); hence $p > n$ and $n \notin P$. From $a_n \neq 0$ and $\|a_n\|^d \le C^d < NP$ we also get $a_n \notin P$.

Suppose that $f(x)$ is a p.p. mod P. Taking into account that a polynomial of degree 2 can only be a p.p. over a field of characteristic 2, we obtain $n > 2$. Obviously, $n^2 a \in R$ and $\|n^2 a\| \le ((n-1)/2 + n)C^2 < (nC)^n$; hence $NP \ge (nC)^{nd}$ implies $n^2 a \notin P$ or $a = 0$. If $n = 3$ then $f(x)$ trivially has the indicated form and in order to prove the remaining part of (i) we may suppose $NP \ge (3C)^{3d}$. From $3a_3 \notin P$, Lemma 1.1(ii), and Lemma 4.8 we see that $f(x)$ is a p.p. mod P if and only if this holds for $D_3(9a, x)$. Thus from Lemma 1.4 we conclude that $9a \in P$. Hence $a = 0$ and from $(x + b)^3 + c = a_3^2 f(x/a_3) \in R[x]$ we get $3b, 3b^2 \in R$; hence $b \in R$ (and $c \in R$) if 3 is unramified. This proves the assertion for $n = 3$; in the sequel we thus assume $n \ge 5$.

Now let P be any non-zero prime ideal such that $na_n \notin P$ and $f(x)$ is a p.p. mod P. We have already observed at the beginning of the proof of Theorem 4.9 that the number N of zeros of $\Phi_f(x, y) = (f(x) - f(y))/(x - y)$ mod P is at most $n - 1$. Hence the reduction of $\Phi_f(x, y)$ mod P is not absolutely irreducible provided that $q + 1 - (n-2)(n-3)\sqrt{q} - (n-1) > n - 1$, where $q = NP$, according to the estimate quoted after Lemma 4.7; this inequality holds if $q > n^2(n-1)^2$. The weaker estimate quoted in Lemma 4.7 gives $q > 250(n-1)^5$; note that then $q - \sqrt{2(n-1)^5 q} > q(1 - 1/\sqrt{125}) > n - 1$. The smaller bound $n^2(n-1)^2$ will in fact only be needed for $n = 5, 7$; otherwise we would have to replace $(nC)^{nd}$ by a larger number.

Let P be a prime ideal of norm at least $(n\sqrt{C})^{nd}$ such that $f(x)$ is a p.p. mod P; recall that $na_n \notin P$. Since $NP > n^4$, the above argument shows that the reduction of $\Phi_f(x, y)$ mod P is not absolutely irreducible and thus the reduction of $f(x)$ mod

P (which is indecomposable as it has prime degree) is linearly related to a Dickson polynomial by Theorem 4.5. Lemma 1.10 shows that $p_{nk}(a_0, \dots, a_n) \equiv 0 \bmod P$ for $1 \le k \le n-3$ where $p_{nk}(a_0, \dots, a_n) + n^{n-k}a_n^{n-k-1}a_k$ is the coefficient of x^k in $D_n(a', x+b')$ with $a' = ((n-1)/2)a_{n-1}^2 - na_na_{n-2}$ and $b' = a_{n-1}$. If $p_{nk}(a_0, \dots, a_n) = 0$ for all k then Lemma 1.10 gives $f(x) + c' = D_n(a', na_nx + b')/(n^n a_n^{n-1}) = D_n(a, a_nx+b)/a_n^{n-1}$ with $a = a'/n^2, b = b'/n$, and suitable c'. (We have used Lemma 1.1(ii) here.) Putting $c = -a_n^{n-1}c'$ we then have $D_n(a, x+b) + c = a_n^{n-1}f(x/a_n) \in R[x]$; if n is unramified then Lemma 1.14 yields $a, b, c \in R$. Hence it is sufficient to prove that $p_{nk}(a_0, \dots, a_n) = 0$ for $1 \le k \le n-3$.

By assumption we have $\|f(x)\| \le C$ and thus $\|a'\| \le (3n-1)C^2/2, \|b'\| \le C$. Put $C_j = \|D_j(a', x+b')\|$ for every $j \ge 1$. Note that $\|p_{nk}(a_0, \dots, a_n) + n^{n-k}a_n^{n-k-1}a_k\| \le C_n$ and hence $\|p_{nk}(a_0, \dots, a_n)\| \le (nC)^{n-1} + C_n$ for all $k \ge 1$. Thus (i) is proved as soon as we know that $((nC)^{n-1} + C_n)^d < NP$.

From the recurrence relation in Lemma 1.1(i) we obtain $C_{j+2} \le (1 + \|b'\|)C_{j+1} + \|a'\|C_j$ for all $j \ge 1$ and $C_1 = \|x + b'\| \le C, C_2 = \|(x+b')^2 - 2a'\| \le 3nC^2$. Let ρ be the positive solution of $x^2 - (1+C)x - (3nC^2/2) = 0$. Then $C_1 \le 2\rho, C_2 \le 2\rho^2$ and inductively from $C_{j+2} \le (1+C)C_{j+1} + (3nC^2/2)C_j$ we conclude that $C_j \le 2\rho^j$ for all $j \ge 1$. From $C \ge 1$ we obtain $\rho \le C(1 + \sqrt{1 + 3n/2})$ and thus it remains to prove that $(nC)^{n-1} + 2(1 + \sqrt{1+3n/2})^n C^n < (nC)^n$. This is easily seen to hold since $n^{n-1} < n^n/2$ and $(1 + \sqrt{1+3n/2})^n \le (\sqrt{2} + \sqrt{2+3n})^n/4 \le n^n/4$ for $n > 5$ and $5^4 + 2 \cdot 4^5 < 5^5$.

Finally, let $a_n = 1$ and $a_{n-1} = 0$. Then $a' = -na_{n-2}$ and $b' = 0$. This gives the sharper estimates $\|p_{nk}(a_0, \dots, a_n)\| \le n^{n-1}C + C_n$ and $C_{j+2} \le C_{j+1} + nCC_j, C_1 = 1$, $C_2 \le 2nC$. Similarly as above let now ρ be the positive root of $x^2 - x - nC = 0$; note that $\sqrt{nC} \le \rho \le (1 + \sqrt{n})\sqrt{C}$. Again, we have $C_j \le 2\rho^j$ for all $j \ge 1$ and $n^{n-1}C + C_n \le n^{n-1}C + 2(1+\sqrt{n})^n C^{n/2} < (n\sqrt{C})^n$ since $n^{n-1} \le n^n/5$ and $1 + \sqrt{n} < n\sqrt[5]{2/5}$ for $n \ge 5$. Thus for $NP \ge (n\sqrt{C})^{nd}$ we have $\|p_{nk}(a_0, \dots, a_n)\|^d < NP$ for all k and (ii) follows as above.

REMARK 4.18. A similar result holds for arbitrary n if the bound $(nC)^{nd}$ is replaced by $q_0(n, C)^d$ for some suitable effectively computable $q_0(n, C)$. Let $n = n_1 \cdot \ldots \cdot n_r$ for some integers $n_i > 1$. Then inductively one may construct integral polynomials $p_k(x_0, \dots, x_n)$, $1 \le k \le k(n_1, \dots, n_r)$, such that a polynomial of degree n with coefficients $a_0, \dots, a_n$ can be written in the form $a_n f_1 \circ \cdots \circ f_r$ with $f_i(x) = D_{n_i}(\alpha_i, x + \beta_i) + \gamma_i$ (for suitable $\alpha_i, \beta_i, \gamma_i$) if and only if $p_k(a_0, \dots, a_n) = 0$ for all k. (Cf. Lemma 1.10 and the proof of Proposition 2.2.) Choose $q_0(n, C)$ so large that for all possible factorizations $n = n_1 \cdot \ldots \cdot n_r$ with (not necessarily distinct) primes n_i and for all the corresponding polynomials p_k we have $\|p_k(a_0, \dots, a_n)\| < q_0(n, C)$ provided that $\|a_0\|, \dots, \|a_n\| \le C$; we also assume that $q_0(n, C)$ is greater than C and $n^2(n-1)^2$. Then a simple modification of the preceding proof shows that $f(x)$ is a composition

https://doi.org/10.1017/S1446788700038349 Published online by Cambridge University Press

of linear polynomials and Dickson polynomials if it is a p.p. for some prime ideal of norm at least $q_0(n, C)^d$. Apparently the actual determination of $q_0(n, C)$ amounts to troublesome computations and yields very large bounds; hence we do not carry this out in detail.

For $R = \mathbb{Z}$ we can obtain a result for arbitrary n by a different approach using Theorem 4.5 for $K = \mathbb{Q}$ rather than for finite fields. By Proposition 2.4(i) every $f(x) \in \mathbb{Z}[x]$ is a composition of $f_i(x) \in \mathbb{Z}[x]$ which are indecomposable over $\mathbb{Q}$. In order to avoid difficulties (similar to those indicated above) we assume that we have a bound for the coefficients of the $f_i(x)$ rather than for $f(x)$. This yields a generalization of Theorem 4.17 if $f(x)$ is indecomposable; if $f(x)$ has prime degree then Theorem 4.17 gives a much better bound, however.

We need an effective result relating the absolute irreducibility of a polynomial in two variables with the absolute irreducibility of its reduction mod p for suitable p. A result of this type which is rather simple to prove may be found in [47, p. 193]. In order to get a reasonable bound we prefer to use the following immediate consequence of a theorem of Ruppert [44, Satz B].

LEMMA 4.19. *Let $\Phi(x, y) \in \mathbb{Z}[x, y]$ be a polynomial of degree $d \geq 1$ and let C be an upper bound for the absolute values of the coefficients. If $\Phi(x, y)$ is absolutely irreducible then the reduction of $\Phi(x, y)$ mod p is absolutely irreducible provided that $p > (d^3C)^{d^2-1}$.*

THEOREM 4.20. *Let $f_1(x), \ldots, f_r(x) \in \mathbb{Z}[x]$ be non-linear polynomials which are indecomposable over $\mathbb{Q}$ and let C be an upper bound for the absolute values of all the coefficients. If $f(x) = (f_1 \circ \cdots \circ f_r)(x)$ is a p.p. mod p for some prime $p > (n-1)^{3n(n-2)}C^{n(n-2)}$ then each $f_i(x)$ has prime degree and is linearly related to a Dickson polynomial.*

PROOF. By Lemma 1.9(i) we may assume $n > 3$. If $f(x)$ is a p.p. mod p then each of the $f_i(x)$ is a p.p. mod p. We may thus suppose that $f(x)$ is indecomposable and we have to prove that n is a prime and $f(x)$ is linearly related to a Dickson polynomial. By Theorem 4.5 this holds if $\Phi_f(x, y)$ is not absolutely irreducible. Note that $\Phi_f(x, y)$ has degree $d = n - 1$ and all coefficients are also coefficients of $f(x)$. Thus by Lemma 4.19 it remains to prove that the reduction of $\Phi_f(x, y)$ mod p is not absolutely irreducible. If this is not the case then by Lemma 4.7 the number of zeros of $\Phi_f(x, y)$ mod P is larger than d since $p > d^{24} > 250d^5$, $p - \sqrt{2d^5p} > d$, and the reduction of $\Phi_f(x, y)$ mod p has degree at most d. We have already observed at the beginning of the proof of Theorem 4.9 (and used in 4.17) that this is impossible if $f(x)$ is a p.p. mod p and $(na_n, p) = 1$, where a_n denotes the leading coefficient of $f(x)$; the last condition holds since $p > n$ and $p > C$, thus completing the proof.

REMARK 4.21. For the rest of Section 4, R is assumed to be the ring of algebraic integers of a number field K; P always denotes some non-zero prime ideal of R. Put $P(m, n; K) = \{P : (NP - 1, m) = (NP^2 - 1, n) = 1\}$ for positive integers m, n; if it is clear which field is meant we may only write $P(m, n)$. (We prefer to write NP^2 instead of $(NP)^2$; this causes no problem since $N(IJ) = N(I)N(J)$.) By Lemma 1.4, $P \in P(m, n)$ if and only if $D_n(1, x)^m$ is a p.p. mod P.

Let $f(x) \in R[x]$ be a composition of linear polynomials $\alpha_i x + \beta_i \in K[x]$ and Dickson polynomials $D_{n_j}(a_j, x)$ with $a_j \in R$; we have seen that this applies whenever $f(x)$ is a p.p. for infinitely many P. Choose $c \in R$, $c \neq 0$, such that $c\alpha_i, c\beta_i \in R$ for all i and let P be a prime ideal with $c\prod c\alpha_i \prod_{a_j \neq 0} a_j \notin P$. Lemma 4.8 implies that $f(x)$ is a p.p. mod P if and only if all the $D_{n_j}(a_j, x)$ are p.p. mod P. Let $m = \prod_{a_j = 0} n_j$ and $n = \prod_{a_j \neq 0} n_j$; an empty product is understood to be 1. Lemma 1.4 shows that all the $D_{n_j}(a_j, x)$ are p.p. mod P if and only if $P \in P(m, n)$. Hence $f(x)$ is a p.p. mod P if and only if $P \in P(m, n)$.

In particular, $\{P : f(x)$ is a p.p. mod $P\}$ differs from $P(m, n)$ by finitely many elements only. A precise description of the possible exceptions is contained in [50]. Clearly, every $P(m, n)$ is equal to some $P(m', n')$ where $m'n'$ is square-free; moreover, $P(m, n)$ is finite if mn is even. If $K = \mathbb{Q}$ then the sets $P(m, n)$ with odd square-free mn differ from each other by infinitely many elements unless they belong to the same parameters; this is not true in the general case ([50, Section 5])

In the sequel (up to 4.33) we investigate under which circumstances $P(m, n; K)$ is infinite for positive integers m, n. Corollary 4.28 is required for the proof of 4.34 which includes Theorem 4. From 4.21 and the main result 4.32 one can easily deduce Theorem 3.

It is clear that $(m, 2) = (n, 6) = 1$ is a necessary condition; for $K = \mathbb{Q}$ it is also sufficient since then $p \in P(m, n)$ if $p \equiv 2 \bmod mn$ and by Dirichlet's theorem there are infinitely many p of this kind. We note that $P(m, n; K)$ is infinite if $P(m, n; K')$ is infinite for some extension field K' of K; more precisely, if $P' \in P(m, n; K')$ then $P \in P(m, n; K)$ for $P = P' \cap K$ since NP' is a power of NP. The converse holds if $K' \cap \mathbb{Q}(\zeta_{mn})$ is contained in K; this is not so easy to see, however. (Cf. 4.30 for a proof of this observation of Matthews.)

PROPOSITION 4.22. *Let d be a positive integer and $K = \mathbb{Q}(\zeta_d)$ (where ζ_d denotes a primitive d-th root of unity). Then for arbitrary positive integers m, n the following conditions are equivalent:*

(i) *$P(m, n)$ is infinite.*
(ii) *$P(m, n)$ contains some P with $6d \notin P$.*
(iii) *$(m, 2d) = (n, 6d) = 1$.*
(iv) *$P(m, n)$ contains infinitely many prime ideals of degree one.*

https://doi.org/10.1017/S1446788700038349 Published online by Cambridge University Press

PROOF. If (i) holds then (ii) is trivial. If $6d \notin P$ then $NP \equiv 1 \bmod 2$, $NP^2 \equiv 1 \bmod 3$, and $NP \equiv 1 \bmod d$; recall that only divisors of d ramify and the degree of an unramified odd prime p is the smallest positive integer f with $p^f \equiv 1 \bmod d$. Hence $P \in P(m, n)$ implies (iii).

Assume that (iii) holds. Then by Dirichlet's theorem there are infinitely many odd primes p with $p \equiv 1 \bmod d$ and $p \equiv 2 \bmod mn$. If P divides p then we have $NP = p$ and $NP \equiv 2 \bmod mn$. Hence there are infinitely many P with $NP = p$ and $P \in P(m, n)$. This finishes the proof since (i) is a trivial consequence of (iv).

PROPOSITION 4.23. *Let $K = \mathbb{Q}(\sqrt{d})$ where d is a square-free integer. Then the following conditions are equivalent:*

(i) *$P(m, n)$ is infinite.*
(ii) *$P(m, n)$ contains some P with $6 \notin P$ and, if $d = 5$, $5 \notin P$.*
(iii) *$(m, 2) = (n, 6) = 1$ and $(m, 3) = 1$ if $d = -3$, and $(n, 5) = 1$ if $d = 5$.*
(iv) *$P(m, n)$ contains infinitely many prime ideals of degree one.*

PROOF. We recall that every ramified prime divides $4d$ and an unramified odd prime p has degree one if and only if $(\frac{d}{p}) = 1$ where $(\frac{d}{p})$ denotes the Legendre symbol. Without further notice we make frequent use of the law of quadratic reciprocity. If P is a prime ideal then in the sequel p always denotes the corresponding rational prime.

Trivially, (i) implies (ii). If $6 \notin P$ then $NP \equiv 1 \bmod 2$ and $NP^2 \equiv 1 \bmod 3$; hence $P \in P(m, n)$ is only possible if $(m, 2) = (n, 6) = 1$, $NP \equiv 2 \bmod 3$ if $3|m$, and $NP \not\equiv \pm 1 \bmod 5$ if $5|n$. For $d = -3$ we cannot have $NP \equiv 2 \bmod 3$ since this clearly implies $p \equiv 2 \bmod 3$ and then $NP = p^2 \equiv 1 \bmod 3$ since $(\frac{d}{p}) = (\frac{p}{3}) = -1$; hence $(m, 3) = 1$. For $d = 5$ and $5 \notin P$ we cannot have $NP \not\equiv \pm 1 \bmod 5$ since this implies that $NP = p$ and for $p \equiv \pm 2 \bmod 5$ we have $(\frac{d}{p}) = (\frac{p}{5}) = -1$; hence $(n, 5) = 1$. Thus (ii) implies (iii).

Assume that (iii) holds. We have to show that there are infinitely many primes p such that $(\frac{d}{p}) = 1$ and $(p - 1, m) = (p^2 - 1, n) = 1$. For $d = -3$ this holds if $p \equiv 1 \bmod 3$ and $p \equiv 2 \bmod mn$; by Dirichlet's theorem there are infinitely many p with this property. For $d = 5$ we may choose $p \equiv 4 \bmod 5$ and $p \equiv 2 \bmod m'n$ where m' is the product of the prime divisors > 5 of m. For $d \equiv 0 \bmod 2$ we set $d' = |d|/2$ and take $p \equiv 1 \bmod 8$ if $(\frac{2}{d'}) = 1$, $p \equiv 5 \bmod 8$ if $(\frac{2}{d'}) = -1$, and $p \equiv 2 \bmod mnd'$. (The Jacobi symbol $(\frac{2}{d'})$ means $\prod(\frac{2}{p_i})$ if $d' = \prod p_i$.)

Now assume that d is odd and is divisible by some prime $q \geq 7$. Let $d' = |d|/q$ and choose $a \not\equiv \pm 1 \bmod q$ such that $(\frac{a}{q}) = (\frac{2}{d'})$; this is possible since there are $(q - 1)/2 \geq 3$ quadratic (non-)residues mod q. Then we may take $p \equiv 1 \bmod 8$, $p \equiv a \bmod q$, and $p \equiv 2 \bmod mnd'/q^r$ where $r \geq 0$ is the largest integer such that $q^r | mn$. It remains to consider the case that $d \neq -3, 5$ is odd and has no prime factor ≥ 7, that is, $d = \pm 1, 3, -5$, or ± 15. Here the requirements are satisfied if we choose

https://doi.org/10.1017/S1446788700038349 Published online by Cambridge University Press

$p \equiv 1 \bmod 4$ if $d = \pm 1, \pm 15$, $p \equiv 3 \bmod 4$ if $d = 3, -5$, and $p \equiv 2 \bmod 15mn$. Hence in all cases (iv) holds. Obviously, (iv) implies (i).

REMARK 4.24. The equivalence of (i) and (iii) in Proposition 4.22 and in Proposition 4.23 is due to Matthews ([32, p. 258]); his proof is different. The special cases $m = 1$ or $n = 1$ were treated earlier in [35, §4].

In the sequel we employ some elementary properties of the Frobenius automorphism σ associated with an unramified prime ideal P of R if K is a Galois extension of $\mathbb{Q}$. Then σ is the unique element of the Galois group $G(K|\mathbb{Q})$ such that $\sigma(a) \equiv a^p \bmod P$ for all $a \in R$; σ generates the decomposition group of P. All the (conjugate) prime ideals belonging to p have conjugate Frobenius automorphisms. We also use the fact that for every $\sigma \in G(K|\mathbb{Q})$ there are infinitely many prime ideals P with Frobenius automorphism σ; this is a special case of the famous Chebotarev density theorem (cf. [26, p. 182]). (Except for the latter, the necessary background can be found either explicitly or implicitly in many basic texts on algebraic number theory, for example in [40].)

LEMMA 4.25. *Let L be a Galois extension of $\mathbb{Q}$ containing K and assume that p is unramified in L. Then the degree of every prime ideal P in K belonging to p is the smallest positive integer f such that $\sigma^f \in G(L|K)$ where σ is the Frobenius automorphism of any prime ideal in L lying above P.*

PROOF. Let σ be the Frobenius automorphism of Q where Q lies above P. We use the relation $f(Q|p) = f(Q|P)f(P|p)$ for the residue class degrees and note that the residue class degrees involving Q are the orders of the corresponding decomposition groups, that is, $f(Q|p) = |G_Q|$ and $f(Q|P) = |G_Q \cap G(L|K)|$ where $G_Q = \langle\sigma\rangle$. If f is the smallest positive integer with $\sigma^f \in G(L|K)$ then $\langle\sigma\rangle \cap G(L|K) = \langle\sigma^f\rangle$ and thus $f(P|p) = f$.

COROLLARY 4.26. *Let K be a subfield of $L = \mathbb{Q}(\zeta_d)$ and, for every integer a with $(a, d) = 1$, let σ_a denote the automorphism of L determined by $\sigma_a(\zeta_d) = \zeta_d^a$. Then the degree of a prime ideal P in K with $d \notin P$ is the smallest f such that K belongs to the fixed field of σ_{p^f}; K belongs to the fixed field of σ_{NP}.*

PROOF. It is well known (and easy to see from the definition taking into account that $\mathbb{Z}[\zeta_d]$ is the ring of algebraic integers of L) that every prime ideal in L belonging to p has Frobenius automorphism σ_p. Hence the degree f is the smallest positive integer such that $\sigma_{p^f} = \sigma_p^f \in G(L|K)$. This proves the first part; the second part follows since $NP = p^f$.

https://doi.org/10.1017/S1446788700038349 Published online by Cambridge University Press

LEMMA 4.27. *Let K be any number field and F be a Galois extension of $\mathbb{Q}$. Then for every $\sigma \in G(F|\mathbb{Q})$ the following properties are equivalent:*

(i) *There are infinitely many primes p such that σ is the Frobenius automorphism of some prime ideal in F belonging to p and p is divisible by some prime ideal in K with degree one.*

(ii) *σ is conjugate to some element of $G(F|F \cap K)$.*

PROOF. Let L be a Galois extension of $\mathbb{Q}$ which contains F and K. If (i) holds then there is a prime p which is unramified in L, is divisible by a prime ideal P in K with degree one, and the Frobenius automorphism of every prime ideal in F belonging to p is conjugate to σ. By Lemma 4.25, the Frobenius automorphism τ of any prime ideal in L lying above P belongs to $G(L|K)$ and thus the corresponding prime ideal in F has Frobenius automorphism $\tau|_F \in G(F|F \cap K)$; thus (ii) holds since σ is conjugate to $\tau|_F$.

Since (i) remains unchanged if σ is replaced by some conjugate, we may assume $\sigma \in G(F|F \cap K)$ for the proof that (ii) implies (i). Then we may find $\tau \in G(L|K)$ with $\tau|_F = \sigma$ since every element of $G(F|F \cap K)$ is the restriction to F of some element of $G(FK|K)$. By the Chebotarev density theorem there are infinitely many prime ideals in L with Frobenius automorphism τ. For each of these the corresponding prime ideal in F has Frobenius automorphism $\sigma = \tau|_F$ and, by Lemma 4.25, the corresponding prime ideal in K has degree one. Hence (i) holds.

COROLLARY 4.28. *Let a, n be positive integers with $(n, a) = 1$. If n is not divisible by any ramified prime of K then there are infinitely many prime ideals P of degree one with $NP \equiv a \bmod n$.*

PROOF. We have $F \cap K = \mathbb{Q}$ for $F = \mathbb{Q}(\zeta_n)$ since $\mathbb{Q}$ is the only number field without ramified primes and every prime that ramifies in F divides n. Recall that every prime ideal in F belonging to p has Frobenius automorphism σ_p. Hence by Lemma 4.27 there are infinitely many prime ideals P in K with $NP = p$ and $\sigma_p = \sigma_a$, that is, $p \equiv a \bmod n$.

PROPOSITION 4.29. *Let m, n, d be positive integers and, for every integer a with $(a, d) = 1$, let σ_a denote the automorphism of $\mathbb{Q}(\zeta_d)$ determined by $\sigma_a(\zeta_d) = \zeta_d^a$. Then for every subfield K of $\mathbb{Q}(\zeta_d)$ the following conditions are equivalent:*

(i) *$P(m, n; K)$ is infinite.*

(ii) *There exists an integer a with $(a - 1, m) = (a^2 - 1, n) = (a, mnd) = 1$ such that K belongs to the fixed field of σ_a.*

https://doi.org/10.1017/S1446788700038349 Published online by Cambridge University Press

PROOF. Assume that (i) holds and let a be the norm of some prime ideal in $P(m, n; K)$ that does not divide mnd. Then $(a-1, m) = (a^2-1, n) = (a, mnd) = 1$ and, by Corollary 4.26, K belongs to the fixed field of σ_a, thus proving (ii).

Conversely, assume that a has the properties specified in (ii). By Dirichlet's theorem there are infinitely many primes p with $p \equiv a \bmod mnd$. By Corollary 4.26, each of the corresponding prime ideals P has degree one; note that $\sigma_p = \sigma_a$. Hence $NP \equiv a \bmod mnd$ and thus $P \in P(m, n; K)$.

THEOREM 4.30. *For every number field K and arbitrary positive integers m, n the following conditions are equivalent:*

(i) *$P(m, n; K)$ is infinite.*
(ii) *$P(m, n; K)$ contains some P with $mn \notin P$.*
(iii) *$P(m, n; K_{ab})$ is infinite where K_{ab} is the maximal abelian subfield of K.*
(iv) *$P(m, n; K \cap \mathbb{Q}(\zeta_{mn}))$ is infinite.*
(v) *$P(m, n; K)$ contains infinitely many prime ideals of degree one.*
(vi) *$G(F|F \cap K) \not\subseteq \bigcup_{p|m} G(F|\mathbb{Q}(\zeta_p)) \cup \bigcup_{p|n} G(F|\mathbb{Q}(\zeta_p + \zeta_p^{-1}))$ where $F = \mathbb{Q}(\zeta_{mn})$.*

PROOF. It is clear that (i) implies (ii), (iii), and (iv). It is also clear that each of these implies that $P(m, n; K \cap \mathbb{Q}(\zeta_{mn}))$ contains some prime ideal that does not divide mn and we proceed to show that this condition implies (v). If a denotes the norm of a prime ideal with this property then we have $(a-1, m) = (a^2-1, n) = 1$ and $(a, mn) = 1$. Moreover, Corollary 4.26 yields that $K \cap \mathbb{Q}(\zeta_{mn})$ belongs to the fixed field of the automorphism σ_a of $\mathbb{Q}(\zeta_{mn})$ determined by $\sigma_a(\zeta_{mn}) = \zeta_{mn}^a$. Hence Lemma 4.27 (with $F = \mathbb{Q}(\zeta_{mn})$) implies the existence of infinitely many p such that $\sigma_p = \sigma_a$ and p is divisible by some prime ideal P in K with degree one. (Here we have again used the fact that σ_p is the Frobenius automorphism of every prime ideal in $\mathbb{Q}(\zeta_{mn})$ belonging to p.) Note that $\sigma_p = \sigma_a$ implies $p \equiv a \bmod mn$; hence $NP = p$ and $P \in P(m, n; K)$, thus proving (v). Since (i) follows trivially from (v), this establishes the equivalence of (i),...,(v).

We finish the proof by showing that (vi) holds if and only if $\sigma_a \in G(F|F \cap K)$ for some integer a with $(a-1, m) = (a^2-1, n) = (a, mn) = 1$; by Proposition 4.29 this condition is equivalent to (iv). It is sufficient to prove that, for every prime p with $p|mn$ and every integer a with $(a, mn) = 1$, $(a-1, p) = 1$ holds if and only if $\sigma_a \notin G(F|\mathbb{Q}(\zeta_p))$ and $(a^2-1, p) = 1$ holds if and only if $\sigma_a \notin G(F|\mathbb{Q}(\zeta_p + \zeta_p^{-1}))$. We may assume that $\zeta_p = \zeta_{mn}^{mn/p}$. The first part follows by noting that $\sigma_a \in G(F|\mathbb{Q}(\zeta_p))$ holds if and only if $\zeta_p^a = \sigma_a(\zeta_p) = \zeta_p$, that is, $a \equiv 1 \bmod p$. Similarly, $\sigma_a \in G(F|\mathbb{Q}(\zeta_p + \zeta_p^{-1}))$ holds if and only if $\zeta_p^a + \zeta_p^{-a} = \sigma_a(\zeta_p + \zeta_p^{-1}) = \zeta_p + \zeta_p^{-1}$ which is equivalent to $\zeta_p^a = \zeta_p^{\pm 1}$, that is, $a \equiv \pm 1 \bmod p$.

https://doi.org/10.1017/S1446788700038349 Published online by Cambridge University Press

LEMMA 4.31. *Let K be a number field and let m, n be coprime positive integers. If every prime dividing n is unramified in K then $K \cap \mathbb{Q}(\zeta_m) = K \cap \mathbb{Q}(\zeta_{mn})$.*

PROOF. Let K' be any subfield of $\mathbb{Q}(\zeta_{mn})$ such that all primes dividing n are unramified in K'. Let p be any prime that ramifies in $\mathbb{Q}(\zeta_n)$. Then $p|n$ and p is unramified in $K'(\zeta_m)$ since it is unramified in K' and in $\mathbb{Q}(\zeta_m)$. Hence there is no prime that ramifies in $K'(\zeta_m) \cap \mathbb{Q}(\zeta_n)$. Thus $K'(\zeta_m) \cap \mathbb{Q}(\zeta_n) = \mathbb{Q}$ and $[K'(\zeta_m) : \mathbb{Q}] = [\mathbb{Q}(\zeta_{mn}) : \mathbb{Q}(\zeta_n)]$. Since we may choose $K' = \mathbb{Q}$ this implies that in the general case we have $K'(\zeta_m) = \mathbb{Q}(\zeta_m)$ and thus $K' \subseteq \mathbb{Q}(\zeta_m)$. Taking $K' = K \cap \mathbb{Q}(\zeta_{mn})$ then yields the assertion.

THEOREM 4.32. *Let m, n, m', n' be positive integers such that $(m', 2) = (n', 6) = 1$ and no prime dividing $m'n'$ is ramified in K. Then $P(m, n; K)$ is infinite if and only if $P(mm', nn'; K)$ is infinite; $P(m', n'; K)$ is infinite.*

PROOF. If $P(mm', nn'; K)$ is infinite then trivially $P(m, n; K)$ is infinite. In order to prove the converse, by induction it is clear that one may suppose that m' is a prime and $n' = 1$ or the other way round. We obviously have $P(mm', nn'; K) = P(m, n; K)$ if $m'|mn$, $n' = 1$ or $m' = 1$, $n'|n$; if $m' = 1$ and n' occurs with multiplicity $r \geq 1$ in m then $P(mm', nn'; K) = P(m/n'^r, nn'; K)$ and $P(m/n'^r, n; K) \supseteq P(m, n; K)$. Hence it is sufficient to prove the assertion under the restriction $(d, d') = 1$ where $d = mn$ and $d' = m'n'$.

Since $P(m, n; K \cap \mathbb{Q}(\zeta_d))$ is infinite, by Proposition 4.29 there exists an integer a with $(a - 1, m) = (a^2 - 1, n) = (a, mn) = 1$ such that $K \cap \mathbb{Q}(\zeta_d)$ belongs to the fixed field of σ_a. By Dirichlet's theorem there are infinitely many primes p with $p \equiv a \bmod d$ and $p \equiv 2 \bmod d'$; for each of these we have $(p - 1, mm') = (p^2 - 1, nn') = 1$. By Corollary 4.26, every prime ideal in $K \cap \mathbb{Q}(\zeta_d)$ belonging to some p with $p \equiv a \bmod d$ has norm equal to p since $\sigma_p = \sigma_a$. Hence $P(mm', nn'; K \cap \mathbb{Q}(\zeta_d))$ is infinite. Taking into account that $K \cap \mathbb{Q}(\zeta_d) = K \cap \mathbb{Q}(\zeta_{dd'})$ by Lemma 4.31, the first part of the assertion follows from Theorem 4.30. The second part follows by noting that $P(1, 1; K)$ is infinite.

REMARK 4.33. Recall that $P(m, n; K)$ is the set of non-zero prime ideals P in K such that $D_m(1, x)^n$ is a p.p. mod P. As an immediate corollary of the equivalence of (i) and (vi) in Theorem 4.30 we obtain that x^p is a p.p. for infinitely many prime ideals if and only if $\mathbb{Q}(\zeta_p) \not\subseteq K$, and $D_p(1, x)$ is a p.p. for infinitely many prime ideals if and only if $\mathbb{Q}(\zeta_p + \zeta_p^{-1}) \not\subseteq K$; here p denotes a prime. This result is due to Matthews ([32, p. 254]). Theorem 4.32 is equivalent to [32, Proposition 6.3] (the proof of which is not convincing since it depends on Section 3; see below). Proposition 4.29 is closely related to [32, Theorem 5.3] and it is easy to deduce the latter from the former([61,

p. 142]). (Note that the last $\equiv$ in (iii) of [32, Theorem 5.3] has to be replaced by $\not\equiv$. Moreover, a part of (iii) is already included in (ii).) Lemma 4.27 is a special case of a theorem of Hasse (cf. [21, §25.7]); an obvious modification of our proof yields the full result.

Matthews claims that $D_n(1, x)^m$ is a p.p. for infinitely many prime ideals in K if and only if this holds for the maximal abelian subfield of K ([32, §3]). This is in fact true by Theorem 4.30. Matthews relies upon a result of Fried to which he reduces the problem by rather sketchy arguments, to say the least. (It should be stressed that [32] is quite detailed and readable except for Section 3.) Fried states that a polynomial $f(x)$ over K is a p.p. for infinitely many prime ideals in K if and only if a certain property involving some subgroups of the Galois group of $f(x) - t$ over $K(t)$ holds ([17, Prop. 2.1]). The main ingredients of the proof are the Chebotarev density theorem and a result of his own which is quoted as Proposition 1 of [16]. But this proposition apparently only has little relevance for the problem and the proof of Theorem 1 of [16] indicates that Fried really means Proposition 1 stated without proof at the end of [15], a paper that is not cited in [17].

Matthews points out that an easy extension of a result of Niederreiter and Lo ([35, Theorem 3.7]), together with the reduction to the abelian case, implies that $P(m, n; K)$ is infinite unless $(p-1)|d$ for some $p|m$, or $(p-1)|2d$ for some $p|n$ where d denotes the degree of K ([32, Proposition 6.9]).

THEOREM 4.34. *Let R be the ring of algebraic integers of some number field K and let $f(x) \in R[x]$ be a polynomial with leading coefficient a and degree $n > 1$. If n is not divisible by any ramified prime then the following conditions are equivalent:*

(i) *$f(x)$ is a p.p. mod P for infinitely many prime ideals P of R.*

(ii) *$f(x) = (f_1 \circ \cdots \circ f_r)(x)$ where each of the $f_i(x)$ has coefficients in an extension field L of K and is linearly related to $D_{n_i}(a_i, x)$ for some odd integer n_i and $a_i \in L$ such that $a_i = 0$ if $3|n_i$.*

(iii) *$a^{n-1} f(x) = (f_1 \circ \cdots \circ f_r)(ax)$ where $f_i(x) = D_{n_i}(a_i, x+b_i)+c_i$ with suitable $a_i, b_i, c_i \in R$ and odd primes n_i such that $a_i = 0$ if $n_i = 3$.*

(iv) *n is odd and $f(x)$ is a p.p. for every $P \in P(3^r, n'; K)$ with $a \notin P$ where $n = 3^r n'$ and $(3, n') = 1$ $(r \geq 0)$.*

(v) *n is odd and $f(x)$ is a p.p. for every prime ideal P of degree one with $NP \equiv 2 \bmod n$ and $a \notin P$.*

PROOF. If (i) holds then (ii) follows from Theorem 4.9. If (ii) holds then by Lemma 1.1(ii) we may assume that all the n_i are primes. Since $g(x) = a^{n-1} f(x/a)$ is a monic polynomial with coefficients in R, by Lemma 2.9 we conclude that $g(x) = (g_1 \circ \ldots \circ g_r)(x)$ with $g_i(x) = D_{n_i}(a_i, x + b_i) + c_i \in R[x]$ where $a_i, b_i, c_i \in K$ and $a_i = 0$ if $n_i = 3$. If $n_i > 3$ then $a_i, b_i, c_i \in R$ by Lemma 1.14. If $n_i = 3$ then $a_i = 0$,

https://doi.org/10.1017/S1446788700038349 Published online by Cambridge University Press

3 is unramified, and from $g_i(x) = (x + b_i)^3 + c_i$ we easily get $b_i \in R$ and $c_i \in R$. Hence (iii) holds. Now assume that $f(x)$ has a representation as in (iii). Then n is odd and, by Lemma 1.4 and Lemma 4.8, $f(x)$ is a p.p. mod P if $P \in P(3^r, n'; K)$ and $a \notin P$; hence (iii) implies (iv). Every prime ideal P with $NP \equiv 2 \bmod n$ belongs to $P(3^r, n'; K)$; hence (iv) implies (v). By Corollary 4.28 there are infinitely many prime ideals P of degree one such that $NP \equiv 2 \bmod n$ if $(n, 2) = 1$; hence (v) implies (i).

COROLLARY 4.35. *Let $f_i(x) \in R[x]$ be a polynomial of degree $n_i \geq 1$, $1 \leq i \leq r$, and assume that $n_1 \cdots n_r$ is not divisible by any ramified prime. Then $(f_1 \circ \cdots \circ f_r)(x)$ is a p.p. for infinitely many prime ideals if and only if this holds for $f_1(x), \ldots, f_r(x)$.*

PROOF. The 'if'-part follows from 4.34 if $n_1 \cdots n_r > 1$. The rest is trivial.

REMARK 4.36. From Remark 4.21, Proposition 4.22, and Proposition 4.23 it is clear that the conclusion of Corollary 4.35 holds without restriction in the case that K is a quadratic or a cyclotomic field (or $\mathbb{Q}$). Assume that n is the product of three distinct odd primes; Matthews has proved that, for a suitable subfield K of $\mathbb{Q}(\zeta_n)$, x^d is a p.p. for infinitely many prime ideals for every proper divisor d of n while this fails for $d = n$ ([32, Proposition 6.5]). (This can, of course, be deduced from 4.29.) Hence in general one cannot drop the restriction on the degrees. Moreover, Matthew's observation shows that the example given by the reviewer of [35] in MR 80k:12002 for illustrating a result of Fried is wrong.

If n is divisible by a ramified prime then (v) no longer implies (i) in Theorem 4.34. As an example, choose $K = \mathbb{Q}(\zeta_n)$ and $f(x) = x^n$ for some odd prime n; note that $NP \equiv 0, 1 \bmod n$ for every P. On the other hand, $f(x) = x^n$ may satisfy (i) even if $NP \not\equiv 2 \bmod n$ for all P. This is shown by taking $K = \mathbb{Q}(\sqrt{n})$ where n is a prime with $n \equiv 5 \bmod 8$. Note that $NP \equiv 2 \bmod n$ implies $NP = p$ since 2 is a quadratic non-residue mod n and $p \equiv 2 \bmod n$ implies that p is unramified and $NP = p^2$ since $(\frac{n}{p}) = -1$. But (i) holds since $P(n, 1; K)$ is infinite by Proposition 4.23.

Assume that $f(x)$ satisfies condition (i) of Theorem 4.34 and $\deg(f)$ is not a prime; then $f(x)$ is decomposable over K by (iii). Nevertheless, $f(x)$ may be indecomposable over R. Consider a field K with odd class number $h > 1$ (for an example see [40, p. 285]). If p is a prime such that $p-1$ exceeds the degree d of K then $\mathbb{Q}(\zeta_p)$ is not contained in K and thus x^p is a p.p. for infinitely many prime ideals of K (see Remark 4.33). Choose p such that also $p \equiv 2 \bmod h$. Then Remark 2.7 shows the existence of a polynomial $f(x) \in R[x]$ of degree p^2 which is indecomposable over R and a composition of x^p and linear polynomials with coefficients in K. This gives an example of the desired kind (cf. Lemma 4.8). By 2.4(i), the situation is different if $h = 1$.

If we do not assume that every prime dividing n is unramified then we cannot conclude that the a_i in (iii) of Theorem 4.34 can be chosen in R even if n is a prime. For every prime $p > 3$ there is a number field K whose degree is not divisible by the degree $(p-1)/2$ of $\mathbb{Q}(\zeta_p + \zeta_p^{-1})$, such that p has ramification index at least $(p-1)/2$. This follows immediately from a well-known theorem of Hasse which states that (under obvious restrictions) there are infinitely many number fields where a finite number of primes have prescribed decompositions [20]; we only need the special case where a single prime is given (proved earlier by Ore in [38, §4]). In Remark 1.13 it was shown that there exists $a \in K$ with $f(x) = D_p(a, x) \in R[x]$ although $a \notin R$. According to Remark 4.33 and Lemma 4.8, $f(x)$ is a p.p. mod P for infinitely many prime ideals. It is easy to see that $f(x)$ is not of the form $\alpha D_p(a', \gamma x + \delta) + \beta$ with $a', \alpha, \beta, \gamma, \delta \in R$. (Otherwise from Lemma 1.9 we obtain $\alpha\gamma^n = 1$, $a'/\gamma^2 = a$, $\delta = 0$, and $\beta = 0$; hence γ is a unit and $a \in R$, a contradiction.)

THEOREM 4.37. *Let R be the ring of algebraic integers of a number field K of degree d, let $f(x) \in R[x]$ be a polynomial of prime degree n, and let C be a real number such that the image of every coefficient under every embedding of K into $\mathbb{C}$ has modulus at most C. Then $f(x)$ is a p.p. for infinitely many prime ideals in K if and only if $f(x)$ is a p.p. for some prime ideal of norm at least $(nC)^{nd}$.*

PROOF. Assume that $f(x) = \sum_{k=0}^{n} a_k x^k$ is a p.p. for some prime ideal of norm $\geq (nC)^{nd}$. By Theorem 4.17 we infer that $f(x) = (D_n(a, a_n x + b) + c)/a_n^{n-1}$ with $n^2 a, nb \in R$ and $c \in K$; clearly, $n^k c \in R$ for large k. Moreover, by 4.17, $f(x)$ is a p.p. for some P such that $(*)$ $na_n \notin P$ and $n^2 a \notin P \setminus \{0\}$. Now let P be any prime ideal with property $(*)$. Taking into account that $D_n(a, x) = D_n(n^2 a, nx)/n^n$ (by Lemma 1.1(ii)), Lemma 4.8 shows that $f(x)$ is a p.p. mod P if and only if $D_n(n^2 a, x)$ is a p.p. mod P. By Lemma 1.4 the last condition is equivalent to $P \in P(m, n/m)$ where $m = 1$ if $a \neq 0$ and $m = n$ if $a = 0$. In particular, $P(m, n/m)$ contains some P with $m \cdot n/m \notin P$ and is thus infinite according to Theorem 4.30. Hence $f(x)$ is a p.p. for infinitely many prime ideals; the converse is obvious.

REMARK 4.38. It is clear from the proof of 4.17 that the bound $(nC)^{nd}$ is not best possible; it is not clear how far away it is from the optimal bound.

5. Historical remarks

Dickson showed that $D_n(a, x)$ is a p.p. for all primes p such that $(p^2 - 1, n) = 1$. Conversely, by very elementary means he proved that a polynomial with integral coefficients and prime degree $n > 3$ is linearly related to $D_n(a, x)$ (for a suitable

https://doi.org/10.1017/S1446788700038349 Published online by Cambridge University Press

integer a) if it is a p.p. for all (sufficiently large) p with $(p^2 - 1, n) = 1$ ([10, p. 89]; cf. Proposition 1.5).

In 1923 Schur [48] proved that the same conclusion holds if it is only assumed that $f(x) = \sum_{k=0}^{n} a_k x^k$ is a p.p. for infinitely many primes. He first notes that $\tilde{f}(x) = n^n a_n^{n-1}(f((x - a_{n-1})/na_n) - f(-a_{n-1}/na_n))$ has integral coefficients, is monic, and the coefficient of x^{n-1} and the constant term both vanish; hence without loss of generality $f(x)$ can be assumed to have these properties. Then by rather tricky arguments (involving the Lagrange inversion formula) he proves that at most $n - 2$ of the branches of the inverse function of $f(x)$ can be linearly independent. Schur proceeds by showing that if n is a prime then every element of the monodromy group can be represented by a linear polynomial; he also remarks that an application of Burnside's theorem quoted in 4.3 would shorten the argument. From this he concludes that $f(x) = x^n$ or, for every ramification point x_0, $f(x) - f(x_0)$ has one simple root and $n - 1$ roots of multiplicity $r > 1$ (cf. Lemma 1.11). In the latter case $f(x)$ is shown to satisfy the same second order linear differential equation as the Chebyshev polynomial of degree n and this finally yields $f(x) = D_n(a, x)$ for a suitable integer a. ($D_n(a, x)$ in [48] means $D_n(-a, x)$ in our notation.) Thus if $f(x)$ is not assumed to be 'normed' as above then one gets $f(x) = \alpha D_n(a, \gamma x + \delta) + \beta$. Schur did not explicitly mention that one cannot suppose that $a, \alpha, \beta, \gamma, \delta$ are integers; this has given rise to many misunderstandings (cf. [50, §3]).

Schur calls n a Dickson number if every polynomial of degree n which is a p.p. for infinitely many primes can be written as a composition of linear polynomials and Dickson polynomials of odd degree. In the introduction of [48] he states that in a later publication he would prove that n is a Dickson number provided that every composite divisor d of n has the following property:

(P_d) Every primitive permutation group of degree d which contains a d-cycle is doubly transitive.

He notes that, by making use of a theorem of Burnside, this immediately implies that every prime power is a Dickson number and announces a proof that the same conclusion holds for every product of two prime powers. It should be stressed that no conjecture is made to the effect that every integer n is a Dickson number, that is that 'Schur's Conjecture' holds.

Years later, Schur [49] proved that (P_d) holds for every integer d which is not a prime; this result has been used in Section 4. So one wonders whether Schur knew how to prove 'Schur's Conjecture'; apparently the promised proof mentioned above was never published.

In 1928 Wegner extended Schur's proof for prime n to odd prime powers and products of two distinct odd primes in his thesis [52], written under the supervision of Schur. Since on the very first page of the text Schur's result is reported to yield

$f(x) = \alpha D_n(a, \gamma x+\delta)+\beta$ with integers $a, \alpha, \beta, \gamma, \delta$, it is tempting to believe that not even Schur was fully aware of the fact that this is not true. Wegner mentioned that no proof had been published for the claim made in [48] to the effect that every product of two (odd) prime powers is a Dickson number and he planned to deal with this case in a later publication, but this project apparently was never realized. Wegner makes use of the result of Ritt according to which a polynomial with imprimitive monodromy group is decomposable (cf. Remark 3.5). The proof then proceeds inductively by showing (by means of elementary but quite involved computations) that the monodromy group of $f(x)$ is imprimitive; double transitivity plays no part.

Twenty years later Kurbatov extended the method of Schur and Wegner to apply to some more general classes of integers including products of two odd prime powers ([27, 28]). His proof proceeds inductively by showing that the monodromy group is solvable. It should be remarked that from [27] and [28] it is not clear at all why this implies the assertion. In order to complete the argument one needs Ritt's results from [42] concerning polynomials with solvable monodromy group (cf. Theorem 3.11); these are not mentioned by Kurbatov. Though in principle quite elementary, Kurbatov's proof consists of very long and complicated computations. (It seems that in fact the solvability of the considered monodromy groups is established inductively by proving that they are imprimitive and thus belong to decomposable polynomials; this would of course imply the assertion concerning Dickson numbers.) Although meanwhile the validity of (P_d) was established for all composite d, Kurbatov does not mention this fact and the connection with Dickson numbers claimed by Schur.

In 1963 Davenport and Lewis showed that the degree of an exceptional polynomial over $\mathbb{F}_p$ must be odd or divisible by p; they also showed that the reduction of a p.p. mod p is exceptional if the degree is small compared with p. ([9, pp. 59-60]; cf. Remark 4.12). Hence it follows that every even n is a Dickson number; this observation is due to the referee of [37] (see p.438).

The breakthrough came in 1970 with the work of Fried [14], who essentially proved Schur's Conjecture for arbitrary number fields. Unfortunately, his formulation of the result caused serious misunderstandings; it took a long time until this became clear, since in most applications (such as in [34, pp. 21-23]) finite exceptional sets of prime ideals do not matter (cf. [50, §3]). Also the style of proof may be a reason why nearly all published versions of Fried's theorem are wrong (the latest example I am aware of is [36]). Fried employs the theory of Riemann surfaces to prove some results for $K = \mathbb{C}$ and recommends a careful reading of the (apparently unpublished) thesis of Fulton in order to see that these results hold for arbitrary fields; he also adds that Fulton's thesis relies heavily on Grothendieck's theory of formal schemes. (Fried remarks that for the proof of Schur's Conjecture only $\mathbb{C}$ needs to be considered ([14, p. 43]). This is true, but requires a modification of some arguments. In particular, his Lemma 1 is not sufficient for this purpose.) It is interesting to note that in [14] no mention is

made of the previous results of Wegner and Kurbatov; it is also not mentioned that Schur was aware of a connection of Schur's Conjecture with his theorem on primitive permutation groups which is an essential ingredient of Fried's proof (and the proof presented here).

Fried also studied rational functions which are permutational functions for infinitely many primes ([17, 18]). Here the results are not as satisfactory as for polynomials. In [17] the problem is solved for rational functions of prime degree as far as their ramification behaviour is concerned. One should note, however, that this does not give a complete answer for rational functions over $\mathbb{Q}$. Let $f_n(x)$ be the Rédei-function of degree $n > 1$ associated with a monic integral polynomial with roots α, β and discriminant D; then $f_n(x)$ induces a permutation mod p if $(\frac{D}{p}) = -1$ and $(p+1, n) = 1$ (cf. [36]). Since $f_n(x) = l^{-1} \circ x^n \circ l$ where $l(x) = (x+\alpha)/(x+\beta)$ (as can be seen from an equation on p.62 of [36]), $f_n(x)$ is the same as x^n from Fried's point of view. (Incidentally, this remark shows that according to [17] there must be further classes of rational functions which induce permutations for infinitely many primes, thus answering a question posed in [36].) Nevertheless, $f_n(x)$ can induce permutations for infinitely many p with $p \equiv 1 \bmod n$ while x^n never is a p.p. in this situation.

Note added in proof

(March 1995.) After the completion of the manuscript I became aware of a paper of Kljačko [59] which has only recently appeared in Russian and which I could not find in Mathematical Reviews. I am indebted to Rex Matthews for sending me a copy of a hand-written translation which he had produced in 1981. Let $f(x)$ be an indecomposable polynomial over an algebraically closed field K and assume that $\mathrm{char}K$ does not divide the degree of $f(x)$. Let G be a Galois group of $f(x) - t$ over $K(t)$. Theorem 1 of [59] states that either G is doubly transitive or $f(x)$ has prime degree and is linearly related to a pure power or a Chebyshev polynomial. If this is true then in Theorem 4.5 (and hence in Theorem 4.9, Corollary 4.11, Theorem 1, and Theorem 2) it is sufficient to assume that the degree of the polynomial is not divisible by the characteristic. Unfortunately, there seems to be an irreparable flaw in [59]. The difference of a Galois extension can be expressed in terms of higher ramification groups. In formula (12) of [59] this result is applied to the extension obtained by adjoining a zero of $f(x) - t$ to $K(t)$, although this is not a Galois extension.

The 'Characteristic $p > 3$ Theorem' of Fried, Guralnick, and Saxl [57] implies that every exceptional polynomial $f(x)$ of prime degree n over a finite field is linearly related to a Dickson polynomial if the characteristic p does not divide n (and if $p > 3$). Unfortunately, an exchange of email with Mike Fried has revealed that the proof is

based on an error and it is not clear whether the result is true.

By a concatenation of unfortunate circumstances, the publication of this paper has been delayed for many years. The final version differs only little from the first version written in 1989. Meanwhile a considerable portion of it has been incorporated into [61].

References

[1] D. R. Barton and R. Zippel, 'Polynomial decomposition', in: *Proceedings of the 1976 ACM Symposium on Symbolic and Algebraic Computation* (SYMSAC 76; August 10-12, 1976, Yorktown Heights, New York; Ed.: R. D. Jenks), pp. 356–358.

[2] ———, 'Polynomial decomposition algorithms', *J. Symbolic Comput.***1** (1985), 159–168.

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

[4] K. L. Chew and S. Lawn, 'Residually finite rings', *Canad. J. Math.* **22** (1970), 92–101.

[5] S. D. Cohen, 'The distribution of polynomials over finite fields', *Acta Arith.* **17** (1970), 255–271.

[6] ———, 'Proof of a conjecture of Chowla and Zassenhaus on permutation polynomials', *Canad. Math. Bull.* **33** (1990), 230–234.

[7] ———, 'The factorable core of polynomials over finite fields', *J. Austral. Math. Soc. (Series A)* **49** (1990), 309–318.

[8] ———, 'Exceptional polynomials and the reducibility of substitution polynomials', *Enseign. Math.* **36** (1990), 53–65.

[9] H. Davenport and D. J. Lewis, 'Notes on congruences I', *Quart. J. Math. Oxford Ser. (2)* **14** (1963), 51–60.

[10] L. E. Dickson, 'The analytic representation of substitutions on a power of a prime number of letters with a discussion of the linear group', *Ann. of Math.* **11** (1896/97), 65–120, 161–183.

[11] F. Dorey and G. Whaples, 'Prime and composite polynomials', *J. Algebra* **28** (1974), 88-101.

[12] A. Evyatar and D. B. Scott, 'On polynomials in a polynomial', *Bull. London Math. Soc.* **4** (1972), 176–178.

[13] M. Fried, 'Arithmetical properties of value sets of polynomials', *Acta Arith.* **15** (1968/69), 91–115.

[14] ———, 'On a conjecture of Schur', *Michigan Math. J.* **17** (1970), 41-55.

[15] ———, 'On a theorem of MacCluer', *Acta Arith.* **25** (1973/74), 121–126.

[16] ———, 'Arithmetical properties of function fields (II). The generalized Schur problem', *Acta Arith.* **25** (1973/74), 225–258.

[17] ———, 'Galois groups and complex multiplication', *Trans. Amer. Math. Soc.* **235** (1978), 141–163.

[18] ———, 'Exposition on an arithmetic group-theoretic connection via Riemann's existence theorem', *Proc. Sympos. Pure Math.* 37 (1980), 571–602.

[19] M. Fried and M. Jarden, *Field arithmetic*, Ergebnisse der Mathematik und ihrer Grenzgebiete, 3. Folge, Band 11 (Springer, New York, 1986).

[20] H. Hasse, 'Zwei Existenztheoreme über algebraische Zahlkörper', *Math. Ann.* **95** (1926), 229–238.

[21] ———, *Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper. Teil II: Reziprozitätsgesetz*, 2.Auflage (Physica-Verlag, Würzburg, 1965).

[22] H. Hering, 'Über Koeffizientenbeschränkungen affektloser Gleichungen', *Math. Ann.* **195** (1972), 121–136.

[23] D. Hilbert, 'Ueber die Irreducibilität ganzer rationaler Functionen mit ganzzahligen Koefficienten', *J. Reine Angew. Math.* **110** (1892), 104–129. (*Gesammelte Abhandlungen II* (Springer, Berlin, 1970) pp. 264–286.)
[24] B. Huppert, *Endliche Gruppen I*, Die Grundlehren der mathematischen Wissenschaften in Einzeldarstellungen 134, (Springer, Berlin, 1967).
[25] A. Hurwitz, 'Über einen Fundamentalsatz der arithmetischen Theorie der algebraischen Grössen', in: *Mathematische Werke II* (Birkhäuser, Basel, 1933), pp. 198–207.
[26] G. Janusz, *Algebraic number fields* (Academic Press, New York, 1973).
[27] V. A. Kurbatov, 'Generalization of Schur's theorem concerning a class of algebraic functions', *Mat. Sb.* **21** (63)(1947), 133–140 (in Russian); *Amer. Math. Soc. Transl. Ser. 2* **37** (1964), 1–11.
[28] ———, 'On the monodromy group of an algebraic function', *Mat. Sb.* **25** (67)(1949), 51–94 (in Russian); *Amer. Math. Soc. Transl. Ser. 2* **36** (1964), 17–62.
[29] S. Lang, *Algebra*, (Addison-Wesley, Reading, 1965).
[30] H. Lausch and W. Nöbauer, *Algebra of polynomials* (North-Holland, Amsterdam, 1973).
[31] R. Lidl and H. Niederreiter, *Finite fields*, Encyclopedia of Mathematics and its Applications 20 (Addison-Wesley, Reading, 1983) (Reprinted 1987 by Cambridge University Press).
[32] R. Matthews, 'Permutation polynomials over algebraic number fields', *J. Number Theory* **18** (1984), 249–260.
[33] B. H. Matzat, *Konstruktive Galoistheorie*, Lecture Notes in Math. 1284 (Springer, Berlin, 1987).
[34] W. Narkiewicz, *Uniform distribution of sequences of integers in residue classes*, Lecture Notes in Math. 1087 (Springer, Berlin, 1984).
[35] H. Niederreiter and S. K. Lo, 'Permutation polynomials over rings of algebraic integers', *Abh. Math. Sem. Univ. Hamburg* **49** (1979), 126–139.
[36] R. Nöbauer, 'Rédei-Funktionen und das Schur'sche Problem', *Arch. Math.* **52** (1989), 61–65.
[37] W. Nöbauer, 'Polynome, welche für gegebene Zahlen Permutationspolynome sind', *Acta Arith.* **11** (1966), 437–442.
[38] Ö. Ore, 'Zur Theorie der Eisensteinschen Gleichungen', *Math. Z.* **20** (1924), 267–279.
[39] D. Passman, *Permutation groups* (Benjamin, New York, 1968).
[40] P. Ribenboim, *Algebraic numbers* (Wiley, New York, 1972).
[41] J. F. Ritt, 'Prime and composite polynomials', *Trans. Amer. Math. Soc.* **23** (1922), 51–66.
[42] ———, 'On algebraic fuctions which can be expressed in terms of radicals', *Trans. Amer. Math. Soc.* **24** (1923), 21–30.
[43] ———, 'Permutable rational functions', *Trans. Amer. Math. Soc* **25** (1923), 399–448.
[44] W. Ruppert, 'Reduzibilität ebener Kurven', *J. Reine Angew. Math.* **369** (1986), 167–191.
[45] P. Samuel, 'About Euclidean rings', *J. Algebra* **19** (1971), 282–301.
[46] A. Schinzel, *Selected topics on polynomials* (University of Michigan Press, Ann Arbor, 1982).
[47] W. M. Schmidt, *Equations over finite fields: An elementary approach*, Lecture Notes in Math. 536 (Springer, Berlin, 1976).
[48] I. Schur, 'Über den Zusammenhang zwischen einem Problem der Zahlentheorie und einem Satz über algebraische Funktionen', *S.-B. Preuss. Akad. Wiss. Berlin* (1923), 123–134.
[49] ———, *Zur Theorie der einfach transitiven Permutationsgruppen*, (S.-B. Preuss. Akad. Wiss. Berlin, 1933), 598–623.
[50] G. Turnwald, 'On a problem concerning permutation polynomials', *Trans. Amer. Math. Soc.* **302** (1987), 251–267.
[51] A. I. Uzkov, 'Additional information concerning the content of the product of polynomials', *Math. Notes* **16** (1974), 825–827.
[52] U. Wegner, *Über die ganzzahligen Polynome, die für unendlich viele Primzahlmoduln Permutationen liefern* (Dissertation, Berlin, 1928).
[53] ———, 'Über einen Satz von Dickson', *Math. Ann.* **105** (1931), 790–792.

[54] H. Wielandt, *Finite permutation groups* (Academic Press, New York, 1964).
[55] K. S. Williams, 'Note on Dickson's permutation polynomials', *Duke Math. J.* **38** (1971), 659–665.

Additional references

[56] S. D. Cohen and R. W. Matthews, 'A class of exceptional polynomials', *Trans. Amer. Math. Soc.* **345** (1994), 897–909.
[57] M. D. Fried, R. Guralnick and J. Saxl, 'Schur covers and Carlitz's conjecture', *Israel J. Math.* **82** (1993), 157–225.
[58] D. R. Hayes, 'The Galois group of $x^n + x - t$', *Duke Math. J.* **40** (1973), 459–461.
[59] A. A. Kljačko, 'Monodromy groups of polynomial mappings', in: *Studies in Number Theory*, No. 6, (Izdat. Saratov. Univ., Saratov, 1975), pp. 82–91 (in Russian).
[60] D. B. Leep and C. C. Yeomans, 'The number of points on a singular curve over a finite field', *Arch. Math.* **63** (1994), 420–426.
[61] R. Lidl, G. L. Mullen, and G. Turnwald, *Dickson polynomials*, Pitman Monographs and Surveys in Pure and Applied Mathematics 65, (Longman, Essex, 1993).
[62] G. Turnwald, 'A new criterion for permutation polynomials', *Finite Fields Appl.* **1** (1995), 64–82.

Mathematisches Institut der Universität
Auf der Morgenstelle 10
D-72076 Tübingen
Germany