TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 302, Number 1, July 1987

ON A PROBLEM CONCERNING PERMUTATION POLYNOMIALS

GERHARD TURNWALD

ABSTRACT. Let $S(f)$ denote the set of integral ideals I such that f is a permutation polynomial modulo I, where f is a polynomial over the ring of integers of an algebraic number field. We obtain a classification for the sets S which may be written in the form $S(f)$.

Introduction. A polynomial $f(x)$ with coefficients in a commutative ring R is said to be a permutation polynomial modulo an ideal I of R (abbreviated p.p. $\bmod I$) if the mapping induced on the residue class ring R/I is bijective. From now on we assume that R is the ring of algebraic integers in an algebraic number field K (of finite degree). Put $S_1(f) = \{P \mid P$ is a nonzero prime ideal such that $f(x)$ is a p.p. $\bmod P$ but not $\bmod P^2\}$, $S_2(f) = \{P \mid P$ is a nonzero prime ideal and $f(x)$ is a p.p. $\bmod P^2\}$. Then $f(x)$ is a p.p. $\bmod I$ $(\neq \{0\})$ if and only if every prime divisor of I belongs to $S_1(f) \cup S_2(f)$ and I is not divisible by the square of an element of $S_1(f)$ (cf. Lemma 1.1).

It is the purpose of this paper to describe the sets S_1, S_2 that may be written in the form $S_1(f), S_2(f)$ for some polynomial $f(x)$. Taking R to be the ring of rational integers yields the solution of problem II posed by Narkiewicz in [**4**, p. 13].

Denoting the absolute norm of an ideal I by NI $(= |R/I|)$, we obtain the following characterization:

THEOREM. *Let R be the ring of integers in the algebraic number field K. If S_1, S_2 are disjoint sets of nonzero prime ideals of R then there exists a polynomial $f(x) \in R[x]$ such that $S_i = S_i(f)$ $(i = 1, 2)$ if and only if one of the following conditions holds:*

(1) *S_1, S_2 are finite.*

(2) *For some squarefree positive integer n with $(n, 6) = 1$ we have*
S_1 is a finite set of prime ideals P such that $NP \not\equiv 1(n)$ or $2^{n-1} \equiv 0$ (P); S_2 differs from $\{P \mid (NP^2 - 1, n) = 1\}$ by at most finitely many elements.

(3) *For some positive integers m, n with $(n, 6) = (m, 2) = 1$, $mn > 1$, mn squarefree, we have*
S_1 differs from $\{P \mid (NP - 1, m) = (NP^2 - 1, n) = 1\}$ by at most finitely many prime ideals P with $NP \not\equiv 1(mn)$ or $2^{n-1} \equiv 0$ (P); S_2 is finite.

(Note that $2^{n-1} \equiv 0$ (P) is equivalent to $n > 1$ and $2 \equiv 0\,(P)$.) The theorem is an immediate consequence of Proposition 2.2, Proposition 2.13, and Proposition 4.8. For the "only if" part we make use of Fried's proof of Schur's conjecture. In §3

Received by the editors June 26, 1986.

1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 11T06; Secondary 11R09.

Key words and phrases. Permutation polynomials, Dickson-polynomials, Schur's conjecture, algebraic integers.

it is proved that the standard formulations of Fried's result are wrong, and a correct version is stated. In the final section (Corollary 5.5) we will prove that for $K = \mathbf{Q}$ the sets $\{P \mid (NP-1, m) = (NP^2-1, n) = 1\}$ differ by infinitely many elements for different pairs (m, n); in the general case this need not be true (Remark 5.6).

1. Let R be the ring of algebraic integers in an algebraic number field K (of finite degree). Since R/I is finite unless $I = \{0\}$, in order to prove that $f(x)$ is a p.p. $\bmod I$ it is sufficient to prove injectivity or surjectivity. As a consequence we note that $f(x)$ is a p.p. $\bmod J$ for every ideal $J \supset I$ if $f(x)$ is a p.p. $\bmod I \neq \{0\}$. (In the following by ideal we always mean nonzero ideal.)

1.1 LEMMA. *Let $f(x)$ be a polynomial with coefficients in R.*

(1) *If I_1, I_2 are relatively prime and $f(x)$ is a* p.p. $\bmod I_1, I_2$ *then $f(x)$ is a* p.p. $\bmod I_1 I_2$.

(2) *Let $f(x)$ be a* p.p. $\bmod P$ *for a prime ideal P. Then $f(x)$ is a* p.p. $\bmod P^2$ *if and only if $f'(a) \not\equiv 0\ (P)$ for all $a \in R$.*

(3) *If $f(x)$ is a* p.p. $\bmod P^2$ *then $f(x)$ is a* p.p. $\bmod P^n$ *for all n.*

PROOF. (1) Assume that $f(a) \equiv f(b)(I_1 I_2)$. Then from $f(a) \equiv f(b)(I_i)$ we obtain $a \equiv b(I_i)$ $(i = 1, 2)$. This implies $a \equiv b(I_1 I_2)$, since $I_1 \cap I_2 = I_1 I_2$.

(2), (3) If $f'(a) \equiv 0\,(P)$ then for $\pi \in P - P^2$ we have $a + \pi \not\equiv a\,(P^2)$ and $f(a+\pi) \equiv f(a) + f'(a)\pi \equiv f(a)(P^2)$. Hence $f(x)$ is not a p.p. $\bmod P^2$. Suppose that $f(x)$ is a p.p. $\bmod P^n$ for some $n \geq 1$. If $f(a) \equiv f(b)(P^{n+1})$ then we may conclude $a \equiv b\,(P^n)$. Hence $f(b) \equiv f(a) + f'(a)(b-a)(P^{n+1})$ and $f'(a)(b-a) \equiv 0\,(P^{n+1})$. Assuming that $f'(a) \not\equiv 0\,(P)$ for all elements a of R, we obtain $b - a \equiv 0\,(P^{n+1})$, i.e. $f(x)$ is a p.p. $\bmod P^{n+1}$. This proves (2) and (3).

(Lemma 1.1 is a special case of the results in [**3**, Chapter 4, §4].)

1.2 DEFINITION. Let P be a nonzero prime ideal. A polynomial is said to be of type 0 $\bmod P$ if it is not a p.p. $\bmod P$, of type 1 $\bmod P$ if it is a p.p. $\bmod P$ but not $\bmod P^2$, and of type 2 $\bmod P$ if it is a p.p. $\bmod P^2$.

1.3 REMARK. If $f(x) \equiv c \cdot g(x)(P)$ for some $c \not\equiv 0\ (P)$ then $f(x)$ and $g(x)$ are of the same type $\bmod P$. This follows immediately from case (2) of Lemma 1.1 and the obvious fact that multiplication by c induces a bijection $\bmod P^n$ for all n.

1.4 NOTATION. Let P be a nonzero prime ideal. For the P-adic valuation on K we write ν_P, i.e. $\nu_P(a)$ is the exponent of P in the factorization of the fractional ideal aR. By R_P we mean the corresponding valuation ring formed by all $a \in K$ with $\nu_P(a) \geq 0$.

1.5 REMARK. (1) As is well known, every element of R_P may be written in the form r/s for some $r \in R$, $s \in R - P$, and R_P is a local ring with maximal ideal $R_P P$. The inclusion mapping of R into R_P induces an isomorphism of R/P^n and $R_P/R_P P^n$ for all n. Hence $f(x) \in R[x]$ is a p.p. $\bmod P^n$ if and only if (interpreted as polynomial over R_P) it is a p.p. $\bmod R_P P^n$.

Let I be an ideal of an arbitrary commutative ring. Obviously, a composition of polynomials $f(x), g(x)$ (over the given ring) is a p.p. $\bmod I$ if and only if $f(x)$ and $g(x)$ are p.p. $\bmod I$.

Assume that $f(x) \in R[x]$ is written as a composition of polynomials $f_i(x) \in R_P[x]$. Then in order to investigate the type of $f(x) \bmod P$ we may ignore a linear factor $f_j(x) = ax + b$ with $\nu_P(a) = 0$, since in this case $ax + b$ is a p.p. $\bmod R_P P^n$ for all n.

(2) The intersection of the rings R_P (for all prime ideals P) is equal to R; i.e. an element a of K lies in R if and only if $\nu_P(a) \geq 0$ for all P (cf. [**2**, p. 14]).

2. For $f(x) \in R[x]$ we define $S_i(f)$ to be the set of all nonzero prime ideals P such that $f(x)$ is of type $i \bmod P$ $(i = 1, 2)$.

We denote the class number of K by h. Note that the hth power of any ideal of R is a principal ideal.

In the following by $P, P_i, \ldots$ we always mean nonzero prime ideals.

2.1 LEMMA. *Let m be a positive integer. The polynomial x^m is a* p.p. $\bmod P$ *if and only if $(NP-1, m) = 1$; x^m is a* p.p. $\bmod P^2$ *if and only if $m = 1$.*

PROOF. The multiplicative group of the finite field R/P is abelian of order $NP-1$. Hence x^m induces a bijection on this group if and only if $(NP-1, m) = 1$. Since $0^m = 0$, this proves the first part. If $m > 1$ then $0 \not\equiv \pi\,(P^2)$ and $0^m \equiv \pi^m\,(P^2)$ for $\pi \in P - P^2$; hence x^m is not a p.p. $\bmod P$.

2.2 PROPOSITION. *Let S_1, S_2 be finite disjoint sets of nonzero prime ideals of R. Then there are (infinitely many) polynomials $f(x) \in R[x]$ such that $S_i = S_i(f)$ (for $i = 1, 2$).*

PROOF. Let a be a generator of the hth power of the product of all prime ideals in S_1 (if S_1 is empty we define the product to be the unit ideal R). If $2a \not\equiv 0\,(P)$ then $f_1(x) = ((4ax+1)^2 - 1)/8a = 2ax^2 + x$ is of the same type $\bmod P$ as x^2 (by Remark 1.5), hence of type 0 (since $NP - 1$ is even for $2 \not\equiv 0\,(P)$). Otherwise we have $f_1(x) \equiv x\,(P)$ and $f_1(x)$ is of type 2 $\bmod P$. Let $n > 1$ be the hth power of a positive integer relatively prime to the numbers $NP - 1$ for all P dividing $2a$. Then $f_2(x) = (f_1(x) + 1)^n$ is of type 0 for $2a \not\equiv 0\,(P)$ and of type 1 for $2a \equiv 0\,(P)$.

Denote the elements of S_2 by P_i and put $e_i = \nu_{P_i}(n)$; note that e_i is a multiple of h. Let b and c be generators of $\Pi P_i^{e_i+h}$ and $\Pi P_i^{e_i}$, respectively. Observe that b/c is integral, $\nu_{P_i}(b/c) > 0$, and n is a multiple of c (since $\nu_P(n) \geq \nu_P(c)$ for all P). Put $f_3(x) = (f_2(bx) - f_2(0))/(bc)$. Since

$$f_3(x) = (f_2'(0)bx + (\cdots)b^2x^2)/(bc) = (nbx + (\cdots)b^2x^2)/(bc) \equiv (n/c)x(P_i)$$

and $\nu_{P_i}(n/c) = 0$, we obtain that $f_3(x)$ is integral and of type 2 $\bmod P_i$. If $P \neq P_i$ for all i then (by Remark 1.5(1)) $f_3(x)$ is of the same type as $f_2(x)$, i.e. of type 1 for $P \in S_1$ or $2 \equiv 0\,(P)$ and of type 0 otherwise. Let d be a generator of the hth power of the product of all P with $P \notin S_2$, $P \notin S_1$, $2 \equiv 0\,(P)$. Then $f(x) = d \cdot f_3(x)$ is of type 2 for $P \in S_2$, of type 1 for $P \in S_1$, and of type 0 otherwise. Since there are infinitely many choices for n, this finishes the proof.

2.3 REMARK. In the special case where R is the ring of rational integers, the above result is due to Nöbauer ([**6**]; cf. [**3**, **4**]). His proof depends upon a deep theorem of Schur (cf. §3).

2.4 LEMMA. *Let $\{P_i | 1 \leq i \leq r\}$ be a finite set of nonzero prime ideals. For every $f(x) \in R[x]$ and for every positive integer n there is a polynomial $g(x) \in R[x]$ that is of the same type as $f(x) \bmod P_i$, and of the same type as $f(x)^n \bmod P$ if $P \neq P_i$ for all i.*

PROOF. Since $f(x)^n$ and $f(x)^{n^h}$ are of the same type $\bmod P$, we may assume n to be an hth power. Then $e_i = \nu_{P_i}(n)$ is divisible by h. Let a and b be generators of $\Pi P_i^{e_i+h}$ and $\Pi P_i^{e_i}$, respectively. Put

$$g(x) = ((af(x)+1)^n - 1)/(ab) = (nf(x) + a(\cdots))/b.$$

Note that $g(x)$ has integral coefficients. For $P = P_i$ we have $g(x) \equiv nf(x)/b(P)$ and $\nu_P(n/b) = 0$; hence $g(x)$ is of the same type as $f(x) \bmod P_i$. If $P \neq P_i$ for all i, then $g(x)$ is of the same type $\bmod P$ as $f(x)^n$ (by Remark 1.5).

2.5 DEFINITION.

$$D_n(a,x) = \sum_{k=0}^{[n/2]} \frac{n}{n-k}\binom{n-k}{k}(-a)^k x^{n-2k} \qquad (a \in R,\ n \geq 1)$$

is called Dickson-polynomial of order n.

$D_n(a,x)$ is characterized by the property $D_n(a, z+a/z) = z^n + (a/z)^n$ (cf. [**3**, p. 209]).

2.6 LEMMA. *The polynomial $D_n(a,x)$ has integral coefficients for every positive integer n and every $a \in R$. Assume $a \not\equiv 0\ (P)$. Then $D_n(a,x)$ is a* p.p. $\bmod P$ *if and only if $(NP^2-1,n) = 1$; $D_n(a,x)$ is a* p.p. $\bmod P^2$ *if and only if $(NP^2-1,n) = (NP,n) = 1$.*

PROOF. $D_n(a,x)$ is integral since

$$\frac{n}{n-k}\binom{n-k}{k} = \left(1+\frac{k}{n-k}\right)\binom{n-k}{k} = \binom{n-k}{k} + \binom{n-k-1}{k-1} \quad (\text{for } k \geq 1).$$

By Lemma 1.1, $D_n(a,x)$ is a p.p. $\bmod P^2$ if and only if it is a p.p. $\bmod P$ and the derivative (with respect to x) has no zero $\bmod P$. Hence the assertion follows from [**3**, Chapter 4, Theorem 9.43].

2.7 LEMMA. *Let $\{P_i \mid 0 \leq i \leq r\}$ be a finite set of nonzero prime ideals ($r \geq 0$). For every $f(x) \in R[x]$ and every odd $n \geq 1$ there is a polynomial $g(x) \in R[x]$ that is of the same type as $f(x)^n \bmod P_0$, of the same type as $f(x) \bmod P_i$ for $1 \leq i \leq r$, and of the same type as $D_n(1, f(x)) \bmod P$ if $P \neq P_i$ for all i.*

PROOF. $f(x)^n$ and $D_n(1,f(x))$ are of the same type $\bmod P$ as $f(x)^{n^h}$ and $D_{n^h}(1,f(x))$, respectively. Hence we may assume n to be an hth power. Then $e_i = \nu_{P_i}(n)$ is divisible by h. Let a, b, and c be generators of P_0^h, $\prod_{i>0} P_i^{e_i+h}$, and $\prod_{i>0} P_i^{e_i}$, respectively. Set $g(x) = (a^n/bc)D_n(1,(b/a)f(x))$. Since (for odd n) $D_n(1,x) = x^n + \cdots + n(-1)^{(n-1)/2}x$, we obtain

$$g(x) = \frac{a^n}{bc}(a^{-n}b^n f(x)^n + a^{-n+1}(\cdots)) \equiv \frac{b^{n-1}}{c} f(x)^n (P_0)$$

and

$$\begin{aligned} g(x) &= \frac{a^n}{bc}\left(n(-1)^{(n-1)/2}\frac{b}{a}f(x) + a^{-n}b^2(\cdots)\right) \\ &= a^{n-1}(-1)^{(n-1)/2}\frac{n}{c}f(x) + \frac{b}{c}(\cdots) \\ &\equiv a^{n-1}(-1)^{(n-1)/2}\frac{n}{c}f(x)(P_i) \end{aligned}$$

for $1 \leq i \leq r$. As $\nu_{P_0}(b) = \nu_{P_0}(c) = 0$ and $\nu_{P_i}(a) = \nu_{P_i}(n/c) = 0$ for $1 \leq i \leq r$, this implies that $g(x)$ is an integral polynomial of the same type as $f(x)^n \bmod P_0$

and of the same type as $f(x) \bmod P_i$ for $1 \leq i \leq r$; for all other P we have $\nu_P(a) = \nu_P(b) = \nu_P(c) = 0$ so that $g(x)$ is of the same type as $D_n(1, f(x))$ (by Remark 1.5).

2.8 LEMMA. *Let m, n be positive integers, n odd. Assume that (for some integer r) $f(x) \in R[x]$ is of the same type as $D_n(1,x)^m$ for $P \neq P_i$ $(0 \leq i \leq r)$. Suppose that $f(x)$ is of type* 2 $\bmod P_0$. *If $NP_0 - 1$ is not divisible by all primes dividing mn, there is a polynomial $g(x) \in R[x]$ that is of type* 1 $\bmod P_0$ *and of the same type as $f(x) \bmod P$ for $P \neq P_0$.*

PROOF. Let q be a prime dividing mn with $(NP_0 - 1, q) = 1$. By Lemma 2.4 we may choose $g_1(x) \in R[x]$ such that $g_1(x)$ is of the same type as $f(x) \bmod P_i$ $(1 \leq i \leq r)$ and of the same type as $f(x)^q \bmod P$ if $P \neq P_i$ for $1 \leq i \leq r$. If $q|m$ then $D_n(1,x)^{qm}$ is of the same type as $D_n(1,x)^m$ (cf. Lemma 2.1); hence $g_1(x)$ is of the same type as $f(x) \bmod P$ if $P \neq P_i$ for $0 \leq i \leq r$. Since $f(x)^q$ is of type 1 $\bmod P_0$, we may thus choose $g(x) = g_1(x)$ if $q \mid m$. Otherwise we have $q \mid n$. By Lemma 2.7 there is a polynomial $g_2(x)$ that is of the same type as $f(x)^q \bmod P_0$, of the same type as $f(x) \bmod P_i$ for $1 \leq i \leq r$, and of the same type as $D_q(1, f(x)) \bmod P$ if $P \neq P_i$ for $0 \leq i \leq r$. Since (for $q|n$) $D_q(1, D_n(1,x)^m)$ is of the same type as $D_n(1,x)^m$, $g_2(x)$ is of the same type as $f(x) \bmod P$ if $P \neq P_i$ for $0 \leq i \leq r$. Hence in case $q \mid n$ we may take $g(x) = g_2(x)$.

2.9 REMARK. If K is the field of rationals we are ready for the proof of Proposition 2.13. In the general case, however, prime ideals P with $2 \equiv 0\,(P)$ and $NP > 2$ give rise to additional complications. In order to cope with them, we need the following three lemmas; the first of these is required again (even for the rationals) in the proof of Lemma 4.7.

2.10 LEMMA. *Let $R(a)$ denote the resultant of $D_n'(a,x)$ and $\frac{1}{2}D_n''(a,x)$. Then $R(a) = n^{3n-6}(-a)^{(n-1)(n-2)/2}$ for $n > 1$.*

PROOF. Assume $a \neq 0$. Since $D_n'(a,x)$ has leading coefficient n, we have $R(a) = n^{n-2}\prod_{k=1}^{n-1}\frac{1}{2}D_n''(a,\eta_k')$ if $\eta_1', \ldots, \eta_{n-1}'$ are the zeros of $D_n'(a,x)$. Let $T_n(x)$ denote the nth Chebyshev-polynomial defined by $T_n(\cos\phi) = \cos n\phi$; $T_n(x)$ is a polynomial of degree n with leading coefficient 2^{n-1}. Alternatively, we may write $T_n((z+z^{-1})/2) = (z^n + z^{-n})/2$ (for any complex number z). Putting $\xi = \sqrt{a}(z + 1/z)$ this implies

$$\begin{aligned} D_n(a,\xi) &= D_n(a, \sqrt{a}z + a/\sqrt{a}z) = (\sqrt{a}z)^n + (a/\sqrt{a}z)^n \\ &= 2(\sqrt{a})^n T_n((z+z^{-1})/2) = 2(\sqrt{a})^n T_n(\xi/2\sqrt{a}) \end{aligned}$$

for infinitely many complex numbers ξ. Hence $D_n(a,x) = 2(\sqrt{a})^n T_n(x/2\sqrt{a})$. From $T_n'(\cos\phi) = n(\sin n\phi)/(\sin\phi)$ it is easily seen that the zeros of $T_n'(x)$ are given by $\eta_k = \cos(k\pi/n)$ for $k = 1, \ldots, n-1$. Since $D_n'(a,x) = (\sqrt{a})^{n-1}T_n'(x/2\sqrt{a})$ and $D_n''(a,x) = \frac{1}{2}(\sqrt{a})^{n-2}T_n''(x/2\sqrt{a})$, we obtain

$$R(a) = n^{n-2}\prod_{k=1}^{n-1}\frac{1}{4}(\sqrt{a})^{n-2}T_n''(\eta_k).$$

Substituting $\phi = k\pi/n$ in $T_n''(\cos\phi) = -n(n\cos n\phi\sin\phi - \sin n\phi\cos\phi)/\sin^3\phi$ gives

$$T_n''(\eta_k) = \frac{-n(n\cos(k\pi)\sin(k\pi/n))}{\sin^3(k\pi/n)} = -n^2(-1)^k(1-\eta_k^2)^{-1}.$$

From $T_n'(x) = 2^{n-1}n\prod_{k=1}^{n-1}(x-\eta_k)$ we derive $T_n'(1) = 2^{n-1}n\prod_{k=1}^{n-1}(1-\eta_k)$ and $T_n'(-1) = (-1)^{n-1}2^{n-1}n\prod_{k=1}^{n-1}(1+\eta_k)$; on the other hand, the formula $T_n'(\cos\phi) = n(\sin n\phi)/(\sin\phi)$ easily yields $T_n'(1) = n^2$ and $T_n'(-1) = (-1)^{n-1}n^2$. Hence

$$\prod_{k=1}^{n-1}(1-\eta_k^2)^{-1} = \frac{(-1)^{n-1}2^{2(n-1)}n^2}{T_n'(1)T_n'(-1)} = \frac{2^{2(n-1)}}{n^2}$$

and

$$\begin{aligned}R(a) &= n^{n-2}(\tfrac{1}{4}(\sqrt{a})^{n-2}(-n^2))^{n-1}(-1)^{n(n-1)/2}2^{2(n-1)}/n^2\\ &= n^{3n-6}a^{(n-1)(n-2)/2}(-1)^{(n-1)(n-2)/2}.\end{aligned}$$

Since $R(a)$ is a polynomial in a, the result is also true for $a=0$ (and may be verified easily since $D_n(0,x) = x^n$).

2.11 LEMMA. *Fix $\xi \in R$ and let $n > 1$ be an odd integer. If $D(\xi)$ denotes the discriminant of the polynomial defined by $g(a) = D_n'(a,\xi)$, then $D(\xi) = \pm n^{3(n-3)/2}\xi^{(n-1)(n-3)/2}$.*

PROOF. We will use several results obtained in the proof of Lemma 2.10. From $D_n'(a,x) = nx^{n-1} + \cdots + n(-a)^{(n-1)/2}$ we see that $g(a)$ is a polynomial of degree $(n-1)/2$ with leading coefficient $\pm n$. We already noted that $D_n'(a,x) = (\sqrt{a})^{n-1}T_n'(x/2\sqrt{a})$. Hence

$$\begin{aligned}\frac{dg}{da}(a) &= \frac{n-1}{2}(\sqrt{a})^{n-3}T_n'\left(\frac{\xi}{2\sqrt{a}}\right) + (\sqrt{a})^{n-1}T_n''\left(\frac{\xi}{2\sqrt{a}}\right)\frac{-\xi}{4a\sqrt{a}}\\ &= \frac{a^{(n-3)/2}}{2}\left((n-1)T_n'\left(\frac{\xi}{2\sqrt{a}}\right) - \frac{\xi}{2\sqrt{a}}T_n''\left(\frac{\xi}{2\sqrt{a}}\right)\right).\end{aligned}$$

Since $T_n'(\xi/2\sqrt{a}) = 0$ if and only if $\xi/2\sqrt{a} = \eta_k = \cos(k\pi/n)$ for some $k = 1,\ldots,n-1$, the zeros of $g(a) = D_n'(a,\xi)$ are just the numbers $(\xi/2\eta_k)^2$ for $k = 1,\ldots,(n-1)/2$. Thus we obtain

$$\begin{aligned}D(\xi) &= \pm n^{(n-5)/2}\prod_{k=1}^{(n-1)/2}\frac{dg}{da}\left(\left(\frac{\xi}{2\eta_k}\right)^2\right)\\ &= \pm n^{(n-5)/2}\prod_{k=1}^{(n-1)/2}\frac{1}{2}\left(\frac{\xi}{2\eta_k}\right)^{n-3}(-\eta_k)T_n''(\eta_k)\\ &= \pm n^{(n-5)/2}2^{-(n-2)(n-1)/2}\xi^{(n-3)(n-1)/2}\prod_{k=1}^{(n-1)/2}\frac{T_n''(\eta_k)}{\eta_k^{n-4}}.\end{aligned}$$

From $\eta_{n-k} = -\eta_k$ and $T_n''(-x) = -T_n''(x)$ we derive

$$\left(\prod_{k=1}^{(n-1)/2}\frac{T_n''(\eta_k)}{\eta_k^{n-4}}\right)^2 = \left(\prod_{k=1}^{n-1}\eta_k\right)^{-n+4}\prod_{k=1}^{n-1}T_n''(\eta_k).$$

Note that

$$\prod_{k=1}^{n-1}\eta_k = \frac{(-1)^{n-1}T_n'(0)}{2^{n-1}n} = \frac{(-1)^{n-1}\sin(n\pi/2)}{2^{n-1}} = (-1)^{(n-1)/2}2^{-(n-1)}$$

and

$$\prod_{k=1}^{n-1} T_n''(\eta_k) = (-n^2)^{n-1}(-1)^{n(n-1)/2}\prod_{k=1}^{n-1}(1-\eta_k^2)^{-1} = n^{2(n-1)}(-1)^{(n-1)/2}\frac{2^{2(n-1)}}{n^2}.$$

Hence

$$\left(\prod_{k=1}^{(n-1)/2}\frac{T_n''(\eta_k)}{\eta_k^{n-4}}\right)^2 = 2^{(n-1)(n-4)}(-1)^{(n-4)(n-1)/2}(-1)^{(n-1)/2}n^{2(n-2)}2^{2(n-1)}$$
$$= 2^{(n-1)(n-2)}n^{2(n-2)}$$

and

$$D(\xi) = \pm n^{(n-5)/2}\xi^{(n-3)(n-1)/2}n^{n-2} = \pm n^{3(n-3)/2}\xi^{(n-1)(n-3)/2}.$$

2.12 LEMMA. *Assume that (for some $r \geq 0$) P_i, $1 \leq i \leq r$, are distinct divisors of* 2 *such that $(NP_i - 1, n) > 1$ for some positive odd integer n. Then for every odd $m \geq 1$ there is a polynomial $f(x) \in R[x]$ of degree mn with the following properties*:

(1) *$f(x)$ is of type* $1 \bmod P_i$ $(1 \leq i \leq r)$.
(2) *$f(x)$ is of the same type* $\bmod P$ *as $D_n(1,x)^m$ for all but finitely many P.*
(3) *The leading coefficient of $f(x)$ is not divisible by P if $P \neq P_i$ for all i.*

PROOF. Set $f(x) = D_n(1,x)^m$ for $r = 0$. In the following we assume $r \geq 1$. The multiplicative group of R/P_i is cyclic of order $NP_i - 1$. Hence we may choose $a_i \in R$ corresponding to a primitive $(NP_i - 1, n)$th root of unity. We then have $a_i \not\equiv 0, 1 (P_i)$ and

$$D_n(a_i, a_i + 1) = D_n(a_i, a_i + (a_i/a_i)) = a_i^n + (a_i/a_i)^n = a_i^n + 1 \equiv 0\,(P_i).$$

Hence we obtain $D_n'(a_i, a_i + 1) \equiv 0\,(P_i)$, since $D_n(a,x) \equiv xD_n'(a,x)(P_i)$ (note that $D_n(a,x)$ contains only odd powers of x). Suppose that a' and β are elements of R such that $a' \equiv a_i\,(P_i)$ and $\beta \equiv a_i + 1\,(P_i)$ for all i (these exist by the Chinese Remainder Theorem). Then $D_n'(a', \beta) \equiv 0\,(P_i)$ and $a', \beta \not\equiv 0\,(P_i)$. By Lemma 2.11 the discriminant of the polynomial defined by $g(a) = D_n'(a, \beta)$ does not vanish $\bmod P_i$ (since $n \not\equiv 0\,(2)$ and $\beta \not\equiv 0\,(P_i)$). Hence $g(a') \equiv 0\,(P_i)$ implies $(dg/da)(a') \not\equiv 0\,(P_i)$. Assume that $a^{(k)}$ is an element of R such that $g(a^{(k)}) \equiv 0\,(P_i^k)$ and $(dg/da)(a^{(k)}) \not\equiv 0\,(P_i)$ for all i. Apply the Chinese Remainder Theorem to obtain a solution $d = d^{(k+1)}$ of the system $(dg/da)(a^{(k)}) \cdot d \equiv -g(a^{(k)})\,(P_i^{k+1})$; note that $d \equiv 0\,(P_i^k)$. Then

$$g(a^{(k)} + d) \equiv g(a^{(k)}) + (dg/da)(a^{(k)}) \cdot d \equiv 0\,(P_i^{k+1}) \quad (\text{for } k \geq 1)$$

and

$$(dg/da)(a^{(k)} + d) \equiv (dg/da)(a^{(k)}) \not\equiv 0\,(P_i) \quad \text{for all } i.$$

Hence inductively we may find $a \in R$ with $a \equiv a' \not\equiv 0\,(P_i)$ and $D_n'(a, \beta) = g(a) \equiv 0\,(P_i^{h+1})$ for all i.

Let α be a generator of $\prod P_i^h$ and put $f_1(x) = (D_n(a, \alpha x + \beta) - D_n(a, \beta))/\alpha^2$. Then

$$f_1(x) = \frac{1}{\alpha^2}\left(\sum_{k=1}^{n}\frac{1}{k!}D_n^{(k)}(a,\beta)\alpha^k x^k\right) \equiv \frac{1}{2!}D_n''(a,\beta)x^2(P_i),$$

since $\nu_{P_i}(D'_n(a,\beta)) > h = \nu_{P_i}(\alpha)$ and $\nu_{P_i}((1/k!)D_n^{(k)}(a,\beta)) \geq 0$. By Lemma 2.10 the resultant of $D'_n(a,x)$ and $\frac{1}{2}D''_n(a,x)$ does not vanish mod P_i (since $n \not\equiv 0\,(2)$ and $a \not\equiv 0\,(P_i)$). Thus $\nu_{P_i}(D'_n(a,\beta)) > 0$ implies $\nu_{P_i}((1/2!)D''_n(a,\beta)) = 0$. Hence $f_1(x)$ is mod P_i of the same type as x^2, i.e. of type 1; $f_1(x)$ is of the same type mod P as $D_n(a,x)$ if $P \neq P_i$ for all i (Remark 1.5). Set

$$f(x) = \frac{(\alpha f_1(x)+1)^m - 1}{\alpha} = \sum_{k=1}^{m} \binom{m}{k} \alpha^{k-1} f_1(x)^k$$

for an odd integer $m \geq 1$. Then $f(x)$ is of type 1 mod P_i since $m \not\equiv 0\,(P_i)$, $f(x) \equiv m f_1(x)\,(P_i)$, and $f_1(x)$ is of type 1 mod P_i. If $P \neq P_i$ for all i then $f(x)$ is of the same type mod P as $f_1(x)^m$, hence of the same type as $D_n(a,x)^m$. Thus (by Lemma 2.6) $f(x)$ is of the same type mod P as $D_n(1,x)^m$ if $a \not\equiv 0\,(P)$ and $P \neq P_i$ for all i. The leading coefficient of $f(x)$ is equal to $\alpha^{(n-1)m-1}$, hence divisible by P if and only if $P = P_i$ for some i.

2.13 PROPOSITION. *Let S_1, S_2 be disjoint sets of nonzero prime ideals of R. Then in the following cases we may find $f(x) \in R[x]$ such that $S_i = S_i(f)$ ($i = 1,2$):*

(1) *There is a squarefree positive odd integer n such that:*

S_1 is a finite set of prime ideals P with $NP \not\equiv 1\,(n)$ or $2^{n-1} \equiv 0\,(P)$; S_2 differs from $\{P \mid (NP^2-1,n) = 1\}$ by at most finitely many elements.

(2) *There are positive odd integers m,n with $mn > 1$ and mn squarefree such that:*

S_1 differs from $\{P \mid (NP-1,m) = (NP^2-1,n) = 1\}$ by at most finitely many prime ideals P with $NP \not\equiv 1(mn)$ or $2^{n-1} \equiv 0\,(P)$; S_2 is finite.

PROOF. Put $g(x) = D_{n^h}(1,x)$ in case (1), $g(x) = D_{n^h}(1,x)^{m^h n^h}$ in case (2). Let S'_i ($i = 0,1,2$) be disjoint finite sets of nonzero prime ideals and assume $NP \not\equiv 1\,(mn)$ or $2^{n-1} \equiv 0\,(P)$ for every $P \in S'_1$, setting $m = 1$ in case (1). Then, by comparison with Lemma 2.1 and Lemma 2.6, we have to show the existence of a polynomial $f(x) \in R[x]$ that is of type i mod P for $P \in S'_i$ ($i = 0,1,2$) and of the same type as $g(x)$ otherwise.

In order to simplify the notation we will write S_i instead of S'_i. Put $S_{11} = \{P \in S_1 \mid NP \equiv 1\,(mn)\}$, $S_{12} = S_1 - S_{11}$. If $P \in S_{11}$ then $2^{n-1} \equiv 0\,(P)$; hence, if S_{11} is not empty we must have $n > 1$, $2 \equiv 0\,(P)$, and $(NP-1,n) > 1$ for all $P \in S_{11}$. Thus, by Lemma 2.12, we may find a polynomial $f_1(x)$ of degree $d = \deg(g(x))$ such that $f_1(x)$ is of type 1 mod P for $P \in S_{11}$, $f_1(x)$ is of the same type mod P as $g(x)$ for $P \notin T$, and the leading coefficient is not divisible by P if $P \notin S_{11}$; T here means a finite set of prime ideals which we may assume to contain $S_0 \cup S_1 \cup S_2$. Denote by T_i the set of all $P \in T - (S_0 \cup S_1 \cup S_2)$ such that $g(x)$ is of type i mod P ($i = 0,1,2$). Let b be a generator of the product of the powers $P^{\nu_P(d)+h}$ for all $P \in T - (S_0 \cup S_{11} \cup T_0)$ (note that d is an hth power); let c be a generator of the product of the powers P^h for all $P \in T - S_{11}$. Then for

$$f_2(x) = b^{2d-2} c \left(f_1\left(\frac{x}{b} + \frac{1}{b^2}\right) - f_1\left(\frac{1}{b^2}\right)\right)$$

we have, denoting the leading coefficient of $f_1(x)$ by a,

$$f_2(x) \equiv b^{2d-2}c\left(a\left(\frac{x}{b}+\frac{1}{b^2}\right)^d - a\left(\frac{1}{b^2}\right)^d\right) \equiv a\frac{c}{b}(dx+b(\cdots)) \equiv a\frac{cd}{b}x\,(P)$$

for every divisor P of b, since $b \equiv 0\,(P)$ implies $c \equiv 0\,(P)$. Note that, for these P, $\nu_P(a) = 0$ and $\nu_P(b) = \nu_P(c) + \nu_P(d)$. Thus (by Remark 1.5) $f_2(x)$ is an integral polynomial of type 0 mod P for $P \in S_0 \cup T_0$, of type 2 mod P for $P \in T - (S_0 \cup S_{11} \cup T_0)$, and of the same type mod P as $f_1(x)$ for $P \notin T - S_{11}$.

For $P \in T_1$ we have $mn > 1$ and $(NP - 1, mn) = 1$ (by Lemma 2.1 and Lemma 2.6); for $P \in S_{12}$ we have $NP \not\equiv 1\,(mn)$. Since mn is squarefree this implies that, for every $P \in S_{12} \cup T_1$, $NP - 1$ is not divisible by all primes dividing mn. Note that d has the same prime factors as mn, and $f_2(x)$ is of the same type as $g(x)$ with at most finitely many exceptions. Thus, by Lemma 2.8, we may find a polynomial $f(x)$ that is of type 1 mod P for $P \in S_{12} \cup T_1$ and of the same type as $f_2(x)$ otherwise. Hence $f(x)$ is of type 0 mod P for $P \in S_0 \cup T_0$, of type 1 mod P for $P \in S_{11} \cup S_{12} \cup T_1 = S_1 \cup T_1$, of type 2 mod P for $P \in S_2 \cup T_2$, and of the same type mod P as $g(x)$ for $P \notin T$. Since $g(x)$ is of type i mod P for $P \in T_i$, $f(x)$ is (as desired) of type i mod P for $P \in S_i$ $(i = 0, 1, 2)$ and of the same type as $g(x)$ otherwise.

3. In order to complete the proof of the Theorem, we require a deep result that was conjectured by Schur and (essentially) proved by Fried.

Suppose that $f(x) \in R[x]$ is a p.p. mod P for infinitely many prime ideals P of R. Then "Schur's Conjecture" is usually stated in one of the following forms:

(A) $f(x)$ is a composition of cyclic polynomials $ax^m + b \in R[x]$ and Dickson-polynomials $D_n(a, x)$ $(a \in R,\ n \geq 1)$.

(B) $f(x)$ is a composition of cyclic polynomials $ax^m + b \in R[x]$ and Chebyshev-polynomials $T_n(x)$.

Unfortunately, both versions are wrong: Set $f(x) = q^{-2}D_q(1, qx) = q^{q-2}x^q + \cdots + (-1)^{(q-1)/2}x$ for some rational prime $q > 3$. Lemma 2.6 (together with Remark 1.5) implies that $f(x)$ is a p.p. mod p for every $p \equiv 2\,(q)$. Hence (by Dirichlet's Theorem) $f(x)$ is a p.p. for infinitely many primes. Since the degree of $f(x)$ is a prime, (A) implies $f(x) = \alpha D_q(a, \beta x + \gamma) + \delta$ for some rational integers $a, \alpha, \beta, \gamma, \delta$. Equating the leading coefficients yields $\alpha\beta^q \equiv 0\,(q)$. Hence $\alpha D_q(a, \beta x + \gamma) + \delta$ reduces to a constant mod q, which contradicts $f(x) \equiv (-1)^{(q-1)/2}x\,(q)$. Applying (B) we must have $f(x) = \alpha T_q(\beta x + \gamma) + \delta = 2^{q-1}\alpha\beta^q x^q + \cdots$; the contradiction arises in the same way as above.

Fried seems to assert that (see [**1**, Theorem 2]):

(C) $f(x)$ is a composition of cyclic polynomials $ax^m + b \in K[x]$ and Chebyshev-polynomials $T_n(x)$.

The Chebyshev-polynomials are defined in Fried's introduction by

$$T_n(x) = 2^{-n-1}((x + \sqrt{x^2+4})^n + (x - \sqrt{x^2+4})^n).$$

They next appear at the top of p. 49 where the relation

$$T_n((z + z^{-1})/2) = (z^n + z^{-n})/2$$

is said to be obtained by putting $2z = x + \sqrt{x^2 - 4}$, and the formula $T_n'(x) = n(z^{2n} - 1)/(z^2 - 1)z^{n-2}$ is given five lines later. Since, as the reader may check, each two of these formulas are incompatible, it is not quite clear which polynomials Fried actually means. Implicitly in the proof of Lemma 13 he again uses the relation $T_n((z + z^{-1})/2) = (z^n + z^{-n})/2$. We will agree to use this as a definition (in accordance with the notation used in the proof of Lemma 2.10). The formulas should then read $T_n(x) = ((x + \sqrt{x^2 - 1})^n + (x - \sqrt{x^2 - 1})^n)/2$, $z = x + \sqrt{x^2 - 1}$, and $T_n'(x) = n(z^{2n} - 1)/(z^2 - 1)z^{n-1}$. In view of $T_n(x) = \frac{1}{2}D_n(1, 2x)$ (cf. the proof of Lemma 2.10), a weaker version of (C) is given by

(C′) $f(x)$ is a composition of cyclic polynomials $ax^m + b \in K[x]$ and Dickson-polynomials $D_n(a', x)$ for some fixed $a' \in K$.

Next we prove that (C′) is wrong: Choose $a \in R$ such that a'/a is not a square in K (it is easy to see that this is possible). Since for any rational prime $q > 3$ $f(x) = q^{-2}D_q(a, qx)$ is a p.p. $\bmod p$ for infinitely many p, (C′) implies $q^{-2}D_q(a, qx) = \alpha D_q(a', \beta x + \gamma) + \delta$ for some $\alpha, \beta, \gamma, \delta \in K$, $\alpha\beta \neq 0$. Since x^{q-1} does not occur on the left side, we immediately obtain $\gamma = 0$. Comparison of the coefficients of x^q and x^{q-2} then yields $q^{q-2} = \alpha\beta^q$ and $q^{-2}(-aq)q^{q-2} = \alpha(-a'q)\beta^{q-2}$. Thus $a'/a = (\beta/q)^2$ is a square, contrary to hypothesis.

Now it seems appropriate to have a closer look at Fried's paper [**1**]: Theorem 2 is essentially a consequence of Weil's estimate of the number of zeros of an absolutely irreducible polynomial in two variables over a finite field, and Theorem 1 which states that $\Phi(x, y) = (f(x) - f(y))/(x - y)$ is absolutely irreducible if $f(x) \in K[x]$ is indecomposible and neither cyclic nor a Chebyshev-polynomial. (By Hilbert's Nullstellensatz it is then easy to see that except for finitely many prime ideals P the reduction of $\Phi(x, y) \bmod P$ is absolutely irreducible over the finite field R/P.) But, as can be seen from the proof of Theorem 1, $f(x)$ is in fact required to be not of the form $\alpha(\gamma x + \delta)^n + \beta$ or $\alpha T_n(\gamma x + \delta) + \beta$ for $\alpha, \beta, \gamma, \delta \in \overline{K}$, where $\overline{K}$ denotes the algebraic closure of K.

3.1 LEMMA. *Let $f(x)$ be a polynomial with coefficients in K. If $f(x) = \alpha D_n(a, \gamma x + \delta) + \beta$ for some $\alpha, \beta, \gamma, \delta, a \in \overline{K}$, then there are $\alpha', \beta', \gamma', \delta' \in K$, $a' \in R$ such that $f(x) = \alpha' D_n(a', \gamma' x + \delta') + \beta'$ $(n \geq 1)$.*

PROOF. Since $D_n(r/s, x) = s^{-n}D_n(sr, sx)$, it is sufficient to find $\alpha', \beta', \gamma', \delta', a' \in K$ such that $f(x) = \alpha' D_n(a', \gamma' x + \delta') + \beta'$. We assume $\alpha\gamma \neq 0$ and $n > 1$, the remaining cases being trivial.

The leading coefficient of $f(x)$ is $\alpha\gamma^n$ and the coefficient of x^{n-1} is $\alpha n \gamma^{n-1}\delta$ (since x^{n-1} does not occur in $D_n(a, x)$). Hence $\alpha\gamma^n$ and δ/γ are elements of K.

In case $n = 2$ from

$$\alpha D_2(a, \gamma x + \delta) + \beta = \alpha(\gamma x + \delta)^2 - 2\alpha a + \beta = \alpha\gamma^2(x + \delta/\gamma)^2 - (2\alpha a - \beta)$$

we conclude $2\alpha a - \beta \in K$. Hence $f(x) = \alpha\gamma^2 D_2((2\alpha a - \beta)/2\alpha\gamma^2, x + \delta/\gamma)$ is a representation of the required form.

For $n > 2$ the expansion of $f(x)$ into powers of $x + \delta/\gamma$ is of the form $f(x) = \alpha\gamma^n(x + \delta/\gamma)^n - \alpha a n \gamma^{n-2}(x + \delta/\gamma)^{n-2} + \cdots$ from which we conclude $a/\gamma^2 \in K$. This completes the proof, since

$$f(x) = \alpha D_n(a, \gamma(x + \delta/\gamma)) + \beta = \alpha\gamma^n D_n(a/\gamma^2, x + \delta/\gamma) + \beta$$

(which obviously implies $\beta \in K$).

Noting that $x^m = D_m(0,x)$ and $T_n(x) = \frac{1}{2}D_n(1,2x)$, Lemma 3.1 allows us to formulate Fried's theorem in the following way:

3.2 THEOREM (SCHUR'S CONJECTURE). *Let R be the ring of integers of an algebraic number field (of finite degree) K. If $f(x) \in R[x]$ is a* p.p. mod P *for infinitely many prime ideals P, then $f(x)$ is a composition of cyclic polynomials $\alpha x^m + \beta$ with $\alpha, \beta \in K$ and Dickson-polynomials $D_n(a,x)$ with $a \in R$, $a \neq 0$.*

3.3 REMARK. It is easy to see that $D_{n_1 n_2}(a,x) = D_{n_1}(a^{n_2}, D_{n_2}(a,x))$. Hence the degrees of the Dickson-polynomials $D_n(a,x)$ may be assumed to be primes. The same holds, of course, for the polynomials $\alpha x^m + \beta$.

Schur proved Theorem 3.2 (for the field of rationals) for polynomials of prime degree and conjectured the result for arbitrary degrees ([**7**]; $D_n(a,x)$ in Schur's paper means $D_n(-a,x)$ in our notation). He did not explicitly mention that in a representation like $f(x) = \alpha D_n(a, \gamma x + \delta) + \beta$ $\alpha, \beta, \gamma, \delta$ need not be integral; this seems to have caused misunderstandings. As indicated above, in a large number of papers, reviews, and books, wrong versions of Schur's Conjecture are stated. In fact, I have seen just one paper with a correct statement [**6**].

4. It remains to show that the sets $S_i(f)$ $(i = 1,2)$ belong to one of the specified types. By Fried's theorem we may restrict ourselves to polynomials $f(x) \in R[x]$ that are composed of linear polynomials $\alpha x + \beta \in K[x]$, powers x^m, and Dickson-polynomials $D_n(a,x)$.

4.1 NOTATION. Let P be a nonzero prime ideal. For $f(x) = \sum a_k x^k \in K[x]$ we put $\nu_P(f(x)) = \min_k \nu_P(a_k)$. As is well known, this definition yields a valuation on $K(x)$.

4.2 LEMMA. *Suppose that $\nu_P(f(x) - f(0)) = \nu_P(f(x))$ for some nonconstant $f(x) \in K[x]$. Then for arbitrary $c_0, \dots, c_n \in K$ the relation $\nu_P(\sum_{i=0}^n c_i f(x)^i) = \min_i \nu_P(c_i f(x)^i)$ holds.*

PROOF. Let j be the largest index such that $\nu_P(a_j) = \nu_P(f(x))$ where a_j denotes the coefficient of x^j in $f(x)$. By assumption we have $j > 0$. Note that the coefficient of x^{ij} in $f(x)^i$ has order $\nu_P(a_j^i) = \nu_P(f(x)^i)$ and the coefficients of the higher powers of x have larger orders. Hence for $k > i$ and $c_i \neq 0$ the order of the coefficient of x^{kj} in $c_i f(x)^i$ is larger than $\nu_P(c_i f(x)^i)$; for $k = i$ the order is equal to $\nu_P(c_i f(x)^i)$. Put $\nu = \min_i \nu_P(c_i f(x)^i)$ and let k be the largest index with $\nu = \nu_P(c_k f(x)^k)$. Then the coefficient of x^{kj} in $\sum_{i=0}^k c_i f(x)^i$ has order ν, which implies $\nu_P(\sum_{i=0}^k c_i f(x)^i) = \nu$. Since $\nu_P(c_i f(x)^i) > \nu$ for $i > k$, we obtain

$$\nu_P\left(\sum_{i=0}^n c_i f(x)^i\right) = \nu = \min_i \nu_P(c_i f(x)^i).$$

4.3 DEFINITION. For a fixed nonzero prime ideal P and a fixed element $\pi \in P - P^2$ we set $f(x)^* = \pi^{-\nu_P(f(x)-f(0))}(f(x) - f(0))$ for every $f(x) \in K[x]$. (Note that $f(x)^*$ is an element of $R_P[x]$.)

4.4 LEMMA. *Let $f(x), g(x)$ be nonconstant polynomials over K. Then $g(f(x))^* = g(\alpha x + \beta)^* \circ f(x)^*$ for some $\alpha, \beta \in K$, $\alpha \neq 0$.*

PROOF. Define α,β by $f(x)=\alpha f(x)^*+\beta$. For $g(\alpha x+\beta)=\sum_{k=0}^n c_k x^k$ and $\nu=\nu_P(\sum_{k=1}^n c_k x^k)$ we have $g(\alpha x+\beta)^*=\pi^{-\nu}\sum_{k=1}^n c_k x^k$. Lemma 4.2 implies $\nu=\nu_P(\sum_{k=1}^n c_k(f(x)^*)^k)$, since $\nu_P(f(x)^*)=0$ and $f^*(0)=0$. Thus

$$g(f(x))^*=\left(\sum_{k=0}^n c_k(f(x)^*)^k\right)^*=\pi^{-\nu}\sum_{k=1}^n c_k(f(x)^*)^k=g(\alpha x+\beta)^*\circ f(x)^*.$$

4.5 REMARK. Let $f(x)$ be a polynomial with coefficients in R_P and choose $c\in R$ with $\nu_P(c)=0$ such that $c\cdot f(x)\in R[x]$. We shall say that $f(x)$ is of type $i \bmod P$ if $c\cdot f(x)$ is of type $i \bmod P$ according to Definition 1.2 ($i=0,1,2$). Since, by Remark 1.5, $f(x)$ is a p.p. $\bmod R_P P^n$ if and only if $c\cdot f(x)$ is a p.p. $\bmod P^n$, this definition is independent of the choice of c (and extends our earlier definition if $f(x)\in R[x]$), and polynomials $f_1(x), f_2(x)$ with $f_1(x)\equiv f_2(x)(R_P P)$ are of the same type $\bmod P$ (cf. Remark 1.3).

4.6 LEMMA. *Suppose $\alpha,\beta\in K$, $\alpha\neq 0$, and $m\not\equiv 0\,(P)$. Then $((\alpha x+\beta)^m)^*$ is of the same type* $\bmod P$ *as x or x^m.*

PROOF. In case $\nu_P(\alpha)\le\nu_P(\beta)$ we write $\alpha=\pi^\nu\alpha_1$, $\beta=\pi^\nu\beta_1$ with $\nu=\nu_P(\alpha)$. Note that $((\alpha x+\beta)^m)^*=((\alpha_1 x+\beta_1)^m)^*$ and $((\alpha_1 x+\beta_1)^m)^*=(\alpha_1 x+\beta_1)^m-\beta_1^m$ (since $\nu_P(\alpha_1)=0$, $\nu_P(\beta_1)\ge 0$). Hence $((\alpha x+\beta)^m)^*$ is of the same type as $(\alpha_1 x+\beta_1)^m-\beta_1^m$, i.e. of the same type as x^m.

Now assume $\nu_P(\alpha)>\nu_P(\beta)$. Then

$$\nu_P\left(\binom{m}{k}\alpha^k\beta^{m-k}x^k\right)>\nu_P(\alpha\beta^{m-1})=\nu_P(m\alpha\beta^{m-1}x)$$

for $k>1$, which implies $((\alpha x+\beta)^m)^*\equiv(m\alpha\beta^{m-1}x)^*(R_P P)$. Hence, by Remark 4.5, $((\alpha x+\beta)^m)^*$ is of the same type $\bmod P$ as x.

4.7 LEMMA. *Assume $2\not\equiv 0\,(P)$ and let n be an odd positive integer with $n\not\equiv 0\,(P)$; suppose $a,\alpha,\beta\in K$, $a\alpha\neq 0$. Then $D_n(a,\alpha x+\beta)^*$ is of type* $0 \bmod P$ *or of the same type as x or x^n.*

PROOF. Let k be the largest integer such that $2k\le\nu_P(a)$. Then we have $a\pi^{-2k}=b/c$ for some $b,\ c\in R$ with $\nu_P(b)\le 1$, $\nu_P(c)=0$. Since

$$D_n(a,\alpha x+\beta)=D_n(bc(\pi^k/c)^2,\alpha x+\beta)=(\pi^k/c)^n D_n(bc,(c/\pi^k)(\alpha x+\beta)),$$

$D_n(a,\alpha x+\beta)^*$ is of the same type $\bmod P$ as $D_n(bc,(c/\pi^k)(\alpha x+\beta))^*$. Hence we may restrict ourselves to the case $a\in R$, $\nu_P(a)\le 1$.

Since n is odd, we may write $D_n(a,x)=\sum_{k=1}^n d_k x^k$ with $d_1=n(-a)^{(n-1)/2}$, $d_{2k}=0$, $d_n=1$; note that $\nu_P(d_k)\ge\nu_P(a^{(n-k)/2})$.

We first consider the case $\nu_P(\alpha)\le\nu_P(\beta)$. If $\nu_P(\alpha)>0$ then for $k>1$ we obtain

$$\begin{aligned}\nu_P(d_k((\alpha x+\beta)^k-\beta^k))&=\nu_P(d_k)+k\nu_P(\alpha)\ge\frac{n-k}{2}\nu_P(a)+k\nu_P(\alpha)\\&>\frac{n-1}{2}\nu_P(a)+\nu_P(\alpha)=\nu_P(d_1\alpha x),\end{aligned}$$

since $(k-1)\nu_P(\alpha)>(k-1)/2\ge((k-1)/2)\nu_P(a)$. Hence $D_n(a,\alpha x+\beta)^*\equiv(d_1\alpha x)^*(R_P P)$. Thus, by Remark 4.5, $D_n(a,\alpha x+\beta)^*$ is of the same type $\bmod P$ as x. In case $\nu_P(\alpha)=0$ we obtain $\nu_P(D_n(a,\alpha x+\beta)-D_n(a,\beta))=0$, since the leading coefficient α^n has order 0. Hence $D_n(a, \alpha x + \beta)^* = D_n(a, \alpha x + \beta) - D_n(a, \beta)$ is of the same type as $D_n(a, x)$. Note that $D_n(a, x)$ is of the same type $\bmod P$ as x^n for $a \equiv 0\,(P)$. For $a \not\equiv 0\,(P)$ Lemma 2.6 implies that $D_n(a, x)$ is of type 0 or type 2, since $(NP, n) = 1$. Thus the assertion is proved for $\nu_P(\alpha) = 0$. In case $\nu_P(\alpha) < 0$ we have $\nu_P(d_k((\alpha x+\beta)^k - \beta^k)) \geq \nu_P(\alpha^k) > \nu_P(\alpha^n) = \nu_P(d_n((\alpha x+\beta)^n - \beta^n))$ for $k < n$. Hence $D_n(a, \alpha x + \beta)^* \equiv (d_n((\alpha x + \beta)^n - \beta^n))^*(R_P P)$, which (by Remark 4.5) implies that $D_n(a, \alpha x+\beta)^*$ is of the same type $\bmod P$ as $(x+\beta/\alpha)^n - (\beta/\alpha)^n$, i.e. of the same type as x^n.

Now we assume $\nu_P(\alpha) > \nu_P(\beta)$. For $\nu_P(\beta) > 0$ we have

$$\begin{aligned}\nu_P(d_k((\alpha x + \beta)^k - \beta^k)) &\geq \nu_P(d_k \alpha \beta^{k-1}) > \nu_P(a^{(n-k)/2} \alpha \beta^{(k-1)/2}) \\ &\geq \nu_P(a^{(n-k)/2} \alpha a^{(k-1)/2}) = \nu_P(d_1 \alpha x)\end{aligned}$$

if $k > 1$ (k odd). Hence $D_n(a, \alpha x + \beta)^* \equiv (d_1 \alpha x)^*(R_P P)$, which implies that $D_n(a, \alpha x + \beta)^*$ is of the same type $\bmod P$ as x. In case $\nu_P(\beta) < 0$ we have $\nu_P(d_k((\alpha x + \beta)^k - \beta^k)) \geq \nu_P(d_k \alpha \beta^{k-1}) > \nu_P(\alpha \beta^{n-1})$ for $k < n$. Since the coefficient of x^k in $d_n((\alpha x + \beta)^n - \beta^n)$ has order at least $\nu_P(\alpha\beta^{n-1})$ with equality holding if and only if $k = 1$, we obtain $D_n(a, \alpha x + \beta)^* \equiv (d_n n \alpha \beta^{n-1} x)^*(R_P P)$. Hence $D_n(a, \alpha x + \beta)^*$ is of the same type $\bmod P$ as x.

In the remaining case $\nu_P(\alpha) > \nu_P(\beta) = 0$ we write

$$D_n(a, \alpha x + \beta) - D_n(a, \beta) = \sum_{k=1}^{n} \frac{1}{k!} D_n^{(k)}(a, \beta) \alpha^k x^k.$$

If $\nu_P(D_n'(a, \beta)) > 0$ and $\nu_P(\frac{1}{2} D_n''(a, \beta)) > 0$ then the resultant of $D_n'(a, x)$ and $\frac{1}{2} D_n''(a, x)$ must vanish $\bmod P$. Hence Lemma 2.10 yields $a \equiv 0\ (P)$. Since in this case $D_n'(a, x) \equiv n x^{n-1}\ (P)$, $D_n'(a, \beta) \equiv 0\,(R_P P)$ implies $\nu_P(\beta) > 0$, contrary to hypothesis. Thus $\nu_P(D_n'(a, \beta)) = 0$ or $\nu_P(\frac{1}{2} D_n''(a, \beta)) = 0$. Since

$$\nu_P\left(\frac{1}{k!} D_n^{(k)}(a, \beta)\right) \geq 0$$

for all k, we obtain

$$\begin{aligned}\nu_P\left(\frac{1}{k!} D_n^{(k)}(a, \beta) \alpha^k\right) &\geq 3\nu_P(\alpha) > 2\nu_P(\alpha) \\ &\geq \min\left\{\nu_P(D_n'(a, \beta)\alpha), \nu_P(\tfrac{1}{2} D_n''(a, \beta)\alpha^2)\right\}\end{aligned}$$

for $k > 2$. Hence

$$D_n(a, \alpha x + \beta)^* \equiv (D_n'(a, \beta)\alpha x + \tfrac{1}{2} D_n''(a, \beta)\alpha^2 x^2)^*(R_P P).$$

It is easy to see that for $2 \not\equiv 0\,(P)$ a quadratic polynomial with ($\bmod P$) nonvanishing leading coefficient is of type $0 \bmod P$ (cf. Lemma 2.1). Thus $D_n(a, \alpha x + \beta)^*$ is of type 0 or of the same type as x.

4.8 PROPOSITION. *Put $S_i = S_i(f)$ ($i = 1, 2$) for some $f(x) \in R[x]$. Then S_1, S_2 are disjoint and one of the following conditions holds:*

(1) *S_1, S_2 are finite.*

(2) *For some squarefree positive integer n with $(n, 6) = 1$ we have*

S_1 is a finite set of prime ideals P such that $NP \not\equiv 1\,(n)$ or $2^{n-1} \equiv 0\,(P)$; S_2 differs from $\{P \mid (NP^2 - 1, n) = 1\}$ by at most finitely many elements.

(3) *For some positive integers* m, n *with* $(m,2) = 1$, $(n,6) = 1$, $mn > 1$, mn *squarefree, we have*

S_1 *differs from* $\{P \mid (NP-1,m) = (NP^2-1,n) = 1\}$ *by at most finitely many prime ideals* P *such that* $NP \not\equiv 1\,(mn)$ *or* $2^{n-1} \equiv 0\,(P)$; S_2 *is finite.*

PROOF. Assume that S_1, S_2 are not both finite. Then, by Fried's Theorem 3.2, we have $f(x) = (f_r \circ \cdots \circ f_1)(x)$ where each $f_j(x)$ is of the form (i) $\alpha x + \beta$ ($\alpha, \beta \in K$, $\alpha \neq 0$), (ii) x^m ($m > 1$), or (iii) $D_n(a,x)$ ($n > 1$, $a \in R$, $a \neq 0$). Put $\alpha_j = \alpha, \beta_j = \beta$, $m_j = n_j = a_j = 1$ in case (i); $m_j = m$, $\alpha_j = \beta_j = n_j = a_j = 1$ in case (ii); $n_j = n$, $a_j = a$, $\alpha_j = \beta_j = m_j = 1$ in case (iii). There are only finitely many prime ideals P such that $\nu_P(\alpha_j) \neq 0$, $\nu_P(\beta_j) < 0$, or $\nu_P(a_j) \neq 0$ for some j. By Remark 1.5, for all other prime ideals P, $f(x)$ is of the same type $\bmod P$ as the composition of all polynomials x^{m_j} and $D_{n_j}(a_j, x)$ in arbitrary order. By Lemma 2.6, $D_n(a,x)$ and $D_n(1,x)$ are of the same type $\bmod P$ for $\nu_P(a) = 0$. Since $D_{n_1 n_2}(1,x) = D_{n_1}(1, D_{n_2}(1,x))$ (for arbitrary n_1, n_2), we conclude that, except for finitely many prime ideals, $f(x)$ is of the same type $\bmod P$ as $D_n(1,x)^{m'}$ where n, m' denote the product of the different prime factors of $\prod n_j$, $\prod m_j$, respectively ($n = 1$ if $\prod n_j = 1$, $m' = 1$ if $\prod m_j = 1$). As (by Lemma 2.1 and Lemma 2.6) x^2, $D_2(1,x)$, $D_3(1,x)$ are p.p. for only finitely many prime ideals, we must have $(m',2) = (n,6) = 1$.

Suppose $m' = 1$ first. Since $S_1(D_n(1,x))$ is finite and $S_2(D_n(1,x))$ differs from $\{P \mid (NP^2-1,n) = 1\}$ only by finitely many elements (cf. Lemma 2.6), S_1 and S_2 are of the type specified in (2) provided that $NP \not\equiv 1\,(n)$ or $2^{n-1} \equiv 0\,(P)$ for every $P \in S_1$. If $n = 1$ then S_1 is empty, since $f(x)$ is linear. If $n > 1$, we have to show $NP \not\equiv 1\,(n)$ for every $P \in S_1$ with $2 \not\equiv 0\,(P)$.

For $m' > 1$ let m be the product of the primes dividing m' that do not divide n. Then $(m,2) = 1$, mn is squarefree, and $mn > 1$. By Lemma 2.1 and Lemma 2.6, $D_n(1,x)^{m'}$ and $D_n(1,x)^{mn}$ are of the same type $\bmod P$ for all P. Since $S_1(D_n(1,x)^{mn}) = \{P \mid (NP-1,m) = (NP^2-1,n) = 1\}$ and $S_2(D_n(1,x)^{mn})$ is empty, S_1 and S_2 are of the type specified in (3) provided that $NP \not\equiv 1\,(mn)$ or $2^{n-1} \equiv 0\,(P)$ for every $P \in S_1$.

Since $m' = 1$ implies $m_j = 1$ for all j, it is no longer necessary to distinguish the cases $m' = 1$ and $m' > 1$: It suffices to prove that $NP - 1$ is not divisible by all prime factors of $\prod m_j \cdot \prod n_j$ if $P \in S_1$, where we may assume $2 \not\equiv 0\,(P)$ if $\prod n_j > 1$. (Note that mn is squarefree.)

Let $P \in S_1$, and assume $2 \not\equiv 0\,(P)$ if $\prod n_j > 1$. Since $\nu_P(f(x) - f(0)) > 0$ would imply that $f(x)$ is constant $\bmod P$, we obtain $f(x)^* = f(x) - f(0)$ (in the notation of Definition 4.3). Hence $(f_r \circ \cdots \circ f_1)(x)^* = f(x)^*$ is of type 1 $\bmod P$. Let j be the smallest index such that $(f_j \circ \cdots \circ f_1)(x)^*$ is of type 1 $\bmod P$. Then, by Lemma 4.4, there are $\alpha, \beta \in K, \alpha \neq 0$, such that $f_j(\alpha x + \beta)^*$ is of type 1 $\bmod P$. Since a linear polynomial is never of type 1, $f_j(x)$ is of the form (ii) or (iii).

Suppose $f_j(x) = x^{m_j}$, $m_j > 1$. For $m_j \not\equiv 0\,(P)$ Lemma 4.6 implies that x^{m_j} is of type 1 $\bmod P$; hence (by Lemma 2.1) $NP - 1$ is relatively prime to m_j. If $m_j \equiv 0\,(P)$ then $NP - 1$ is not divisible by the prime factor $p = \operatorname{char} R/P$ of m_j. Now assume $f_j(x) = D_{n_j}(a_j, x)$; then $2 \not\equiv 0\,(P)$ since $n_j > 1$. For $n_j \not\equiv 0\,(P)$ Lemma 4.7 implies that x^{n_j} is of type 1 $\bmod P$. Hence, as above, we conclude that $NP - 1$ is not divisible by all prime factors of n_j, thus finishing the proof.

4.9 REMARK. If p is a rational prime with $p \equiv 1\,(m)$ then $(NP-1, m) \equiv 0\,(m)$ for every prime ideal P of R belonging to p. Thus, by Dirichlet's Theorem, for $m > 1$ there are infinitely many primes P such that $D_m(a, x)$ and x^m are not p.p. mod P. Hence, by Fried's Theorem 3.2 and Remark 1.5, for any polynomial $f(x)$ of degree at least 2, there are infinitely many P such that $f(x)$ is not a p.p. mod P. (This result has, of course, a more elementary proof: [**5**, Theorem 2.4].)

5. We are going to discuss how the sets $\{P \mid (NP-1, m) = (NP^2-1, n) = 1\}$ differ from each other for different pairs (m, n). We require the following generalization of Dirichlet's Theorem. (This result has probably been noticed long ago, but I could find only one reference: It is a special case of Corollary 2 in E. Fogel's paper *On the distribution of prime ideals*, Acta Arith. **7** (1961/62), 255–269.)

5.1 THEOREM. *Let m be a positive integer. If A is an ideal of R with $(NA, m) = 1$ then there exist infinitely many prime ideals P (of relative degree 1) such that $NP \equiv NA\,(m)$.*

PROOF. Let $\sigma_1, \ldots, \sigma_n$ be the imbeddings of K into the field of complex numbers. Then for $a \in R$, $a \neq 0$, the norm $N(a)$ of the principal ideal (a) is equal to $\pm \prod_{i=1}^{n} \sigma_i(a)$. Assume that a, b are nonzero elements of R such that $a \equiv b\,(m)$ and $\sigma_i(a/b) > 0$ for every real imbedding σ_i. Then we have $N(a) \equiv N(b)\,(m)$, since $\sigma_i(a) \equiv \sigma_i(b)(m)$ and $\prod_{i=1}^{n} \sigma_i(a) / \prod_{i=1}^{n} \sigma_i(b) > 0$.

Suppose that A and P belong to the same ray-class with respect to the modulus of K determined by m and the product of the real infinite primes of K. Then $(a)P = (b)A$ for some $a, b \in R$ with $(a, m) = (b, m) = 1$, $a \equiv b\,(m)$, and $\sigma(a/b) > 0$ for every real imbedding σ. By the above remark we have $N(a) \equiv N(b)\,(m)$; moreover, $(N(a), m) = 1$. Hence from $N(a) \cdot NP = N(b) \cdot NA$ we obtain $NP \equiv NA\,(m)$. This concludes the proof since, by a well-known generalization of Dirichlet's Theorem (cf. [**2**, Chapter V, Theorem 10.3]), every ray-class contains infinitely many prime ideals P (of degree 1).

5.2 REMARK. If K is the mth cyclotomic field, then $NP \equiv 1\,(m)$ for all unramified primes P.

More generally, assume that K is an abelian extension of $\mathbf{Q}$ and m is divisible by sufficiently high powers of the ramified primes. Then Artin's Reciprocity Law (cf. [**2**, Chapter V, Theorem 5.7]), applied to the modulus determined by m and the infinite prime of $\mathbf{Q}$, shows that the residue classes mod m corresponding to norms NA of ideals A of R generate a subgroup of index $(K : \mathbf{Q})$ in the group of prime residue classes mod m. Hence for $K \neq \mathbf{Q}$ not every prime residue class mod m contains norms of ideals of R. Suppose that p is a prime with $p \equiv 1\,(m)$. Then p has trivial Artin-automorphism, which implies $p = NP$ for every prime ideal P corresponding to p. Let m' be an integer with $(m, m') = 1$. By Dirichlet's Theorem there are infinitely many primes p with $p \equiv a\,(m')$, $p \equiv 1\,(m)$ for every a with $(a, m') = 1$. Thus we obtain:

If K is abelian and m' is relatively prime to the discriminant of K, then every prime residue class mod m' contains infinitely many primes which are norms of prime ideals of R.

5.3 DEFINITION. K satisfies hypothesis (H_1) if, for every pair of relatively prime integers m_1, m_2 and ideals A_i with $(NA_i, m_i) = 1$ $(i = 1, 2)$, there exists an ideal A such that $NA \equiv NA_i\,(m_i)$.

K satisfies hypothesis (H_2) if, for every odd prime q such that $\{P|(NP-1,q)=1\}$ is infinite, the set $\{P|(NP-1,q)=1,\ (NP^2-1,q)>1\}$ is infinite.

5.4 PROPOSITION. *Assume that K satisfies hypothesis* (H_1) *and put* $P(m,n)=\{P \mid (NP-1,m)=(NP^2-1,n)=1\}$ *for arbitrary integers* m,n.

Let m_i, n_i be positive odd integers such that $m_i n_i$ is squarefree ($i=1,2$). *If the sets $P(m_1,n_1)$, $P(m_2,n_2)$ are infinite, but differ by at most finitely many elements, then $m_1n_1=m_2n_2$; if K satisfies* (H_2) *then we may conclude* $m_1=m_2$, $n_1=n_2$.

PROOF. Suppose that q is a prime with $m_1n_1\equiv 0\,(q)$, $m_2n_2\not\equiv 0\,(q)$. Choose $P_2\in P(m_2,n_2)$ with $m_2n_2\not\equiv 0\,(P_2)$. By ($\mathrm{H}_1$) there exists an ideal A with $NA\equiv NP_2(m_2n_2)$, $NA\equiv 1\,(q)$. If P is a prime ideal with $NP\equiv NA\,(m_2n_2q)$ then $P\in P(m_2,n_2)$ and $P\notin P(m_1,n_1)$ (since $(NP-1,m_1n_1)\equiv 0\,(q)$). Hence there exist at most finitely many P with $NP\equiv NA(m_2n_2q)$, which contradicts Theorem 5.1. Thus, by symmetry, m_1n_1 and m_2n_2 have the same prime factors; hence $m_1n_1=m_2n_2$.

Suppose that q is a prime with $n_1\equiv 0\,(q)$, $m_2\equiv 0\,(q)$. Since $\{P \mid (NP-1,q)=1\}$ contains the infinite set $P(m_2,n_2)$, hypothesis (H_2) yields the existence of a prime ideal P_1 with $(NP_1-1,q)=1$, $(NP_1^2-1,q)>1$, and $q\not\equiv 0\,(P_1)$. Choose $P_2\in P(m_2,n_2)$ with $m_2n_2\not\equiv 0\,(P_2)$. Then, by ($\mathrm{H}_1$), there exists an ideal A with $NA\equiv NP_1\,(q)$, $NA\equiv NP_2\,(m_2n_2/q)$. If P is a prime ideal with $NP\equiv NA(m_2n_2)$ then $P\notin P(m_1,n_1)$ and $P\in P(m_2,n_2)$, since $(NP^2-1,q)>1$ and $(NP-1,q)=(NP-1,m_2/q)=(NP^2-1,n_2)=1$. Hence there exist at most finitely many P with $NP\equiv NA(m_2n_2)$, which contradicts Theorem 5.1. Thus $n_1\equiv 0(q)$ implies $n_2\equiv 0\,(q)$ (since $m_2n_2\equiv 0\,(n_1)$). Hence, by symmetry, $n_1=n_2$ and $m_1=m_2$.

5.5 COROLLARY. *Assume $K=\mathbf{Q}$ and let m_i,n_i be positive odd integers with $(n_i,3)=1$ and m_in_i squarefree* ($i=1,2$). *Then $P(m_1,n_1)$ and $P(m_2,n_2)$ differ by infinitely many elements unless $m_1=m_2$ and $n_1=n_2$.*

PROOF. For $K=\mathbf{Q}$, (H_1) is valid by the Chinese Remainder Theorem. Let q be an odd prime. By Dirichlet's Theorem there exist infinitely many primes p with $p\equiv -1\,(q)$. Thus (H_2) holds, since $p\equiv -1\,(q)$ implies $(p-1,q)=(-2,q)=1$ and $(p^2-1,q)=q>1$. The sets $P(m_i,n_i)$ are infinite, since for $p\equiv 2\,(m_in_i)$ we have $(p-1,m_i)=(1,m_i)=1$ and $(p^2-1,n_i)=(3,n_i)=1$. Hence the assertion follows from Proposition 5.4.

5.6 REMARK. (1) Remark 5.2 implies that (H_1) holds if K is a cyclotomic field or if K is abelian and the discriminant has only one prime factor.

(2) Proposition 5.4 need not hold if hypothesis (H_1) fails. As an example, take $K=\mathbf{Q}(\sqrt{5q})$ for some prime $q>5$ with $q\equiv 1\,(4)$. Recall that for $K=\mathbf{Q}(\sqrt{d})$ we have $NP=p$ if $(\frac{d}{p})=1$ and $NP=p^2$ if $(\frac{d}{p})=-1$ (where $(\frac{d}{p})$ is Legendre's symbol). Every prime p with $p\equiv 2\,(5)$, $(\frac{p}{q})=-1$ belongs to $P(1,5)$, since

$$\left(\frac{5q}{p}\right)=\left(\frac{5}{p}\right)\left(\frac{q}{p}\right)=\left(\frac{p}{5}\right)\left(\frac{p}{q}\right)=1$$

and $(p^2-1,5)=(3,5)=1$. Hence, by Dirichlet's Theorem, $P(1,5)$ is infinite. Suppose $P\in P(1,5)$ and $5q\not\equiv 0\ (P)$. Since $(a^4-1,5)=5$ for $(a,5)=1$, we must have $NP=p$ and $(\frac{p}{5})=-1$. Thus we obtain $p\not\equiv 1\,(q)$ from

$$\left(\frac{5q}{p}\right)=\left(\frac{p}{5}\right)\left(\frac{p}{q}\right) \quad\text{and}\quad \left(\frac{1}{q}\right)=1;$$

hence $(NP-1,q)=1$. This means that $P(1,5)$ and $P(q,5)$ are infinite and differ at most by the finitely many prime divisors of $5q$.

(3) If (H_2) fails for the prime q, then $P(q,1)$ and $P(1,q)$ are infinite and differ by only finitely many elements. As an example, take $K=\mathbf{Q}(\sqrt{-q})$ for some prime $q>3$ with $q\equiv 3\,(4)$. Note that

$$\left(\frac{-q}{p}\right)=(-1)^{(p-1)/2}\left(\frac{q}{p}\right)=\left(\frac{p}{q}\right)$$

for every odd prime p. Let P be a prime ideal with $q\not\equiv 0\,(P)$. Then NP is a quadratic residue $\bmod q$, since $NP=p$ implies $(\frac{p}{q})=(\frac{-q}{p})=1$. Hence $(\frac{-1}{q})=(-1)^{(q-1)/2}=-1$ implies $NP\not\equiv -1\,(q)$. If p is a prime with $p\equiv 4\,(q)$ then $(\frac{-q}{p})=(\frac{p}{q})=1$. Thus for a prime ideal P dividing p we have $NP=p$ and $(NP-1,q)=(3,q)=1$. Hence, by Dirichlet's Theorem, $P(q,1)$ is infinite and (H_2) fails since, as we have seen above, $(NP^2-1,q)=(NP-1,q)(NP+1,q)=(NP-1,q)$ for every P with $q\not\equiv 0\,(P)$.

(4) If K is the mth cyclotomic field then $NP\equiv 1\,(m)$ for every prime ideal P with $m\not\equiv 0\,(P)$. Hence $P(m,n)$ is finite for every n $(m>1)$.

Note that $P(m,1), P(1,n)$ are infinite if and only if $x^m, D_n(1,x)$ are p.p. $\bmod P$ for infinitely many P, respectively. In [**5**, §3], sufficient conditions are given such that powers or Dickson-polynomials are p.p. $\bmod P$ for infinitely many P; if K is a quadratic or cyclotomic field then necessary and sufficient conditions are known [**5**, §§4–5]. For prime degree the general problem was settled by R. Matthews (*Permutation polynomials over algebraic number fields*, J. Number Theory **18** (1984), 249–260). He also showed that $P(m,n)$ is infinite if and only if the corresponding set for the maximal abelian subfield of K is infinite.

REFERENCES

1. M. Fried, *On a conjecture of Schur*, Michigan Math. J. **17**(1970), 41–55.
2. G. Janusz, *Algebraic number fields*, Academic Press, New York, 1973.
3. H. Lausch and W. Nöbauer, *Algebra of polynomials*, North-Holland, Amsterdam, 1973.
4. W. Narkiewicz, *Uniform distribution of sequences of integers in residue classes*, Lecture Notes in Math., vol. 1087, Springer-Verlag, 1984.
5. H. Niederreiter and S. K. Lo, *Permutation polynomials over rings of algebraic integers*, Abh. Math. Sem. Univ. Hamburg **49** (1979), 126–139.
6. W. Nöbauer, *Polynome, welche für gegebene Zahlen Permutationspolynome sind*, Acta Arith. **11** (1966), 437–442.
7. 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.

MATHEMATISCHES INSTITUT DER UNIVERSITÄT, AUF DER MORGENSTELLE 10, D-7400 TÜBINGEN, FEDERAL REPUBLIC OF GERMANY