ACTA ARITHMETICA
IX (1964)

Polynomials of certain special types

by

H. DAVENPORT (Cambridge), D. J. LEWIS* (Ann Arbor, Mich.),
A. SCHINZEL (Warszawa)

1. Let $f(x)$ be a polynomial with integral coefficients. It is well known that if $f(x)$ is a kth power for every positive integer x, then $f(x) = (g(x))^k$ identically, where $g(x)$ has integral coefficients. For proofs and references, see Pólya and Szegö [8], Section VIII, Problems 114 and 190; also Fried and Suranyi [2].

In this connection, we shall prove the following general theorem:

THEOREM 1. *Let $f(x, y)$ be a polynomial with integral coefficients. Suppose that every arithmetical progression contains some integer x such that the equation $f(x, y) = 0$ has an integral solution in y. Then there exists a polynomial $g(x)$ with rational coefficients such that*

$$f(x, g(x)) = 0 \tag{1}$$

identically.

COROLLARY. *Let $k > 1$ be an integer and let $f(x)$ be a polynomial with integral coefficients. Suppose that every arithmetical progression contains some integer x such that $f(x)$ is a k-th power. Then $f(x) = (g(x))^k$ identically, where $g(x)$ is a polynomial with integral coefficients.*

Professor LeVeque raised the question (in conversation) whether, if $f(x)$ is representable as a sum of two squares for every positive integer x, or for every sufficiently large integer x, then $f(x)$ is identically a sum of two squares. We shall prove that this is true, and we shall deduce it from the following general theorem.

THEOREM 2. *Let K be any normal algebraic number field of degree n, with integral basis $\omega_1, \omega_2, \ldots, \omega_n$, and let*

$$N(u_1, u_2, \ldots, u_n) = \operatorname{norm}(u_1\omega_1 + u_2\omega_2 + \ldots + u_n\omega_n)$$

* This author was partially supported by a grant from the National Science Foundation.

denote the norm-form corresponding to K. Let $f(x)$ be a polynomial with rational coefficients, and suppose that every arithmetical progression contains an integer x such that

$$f(x) = N(u_1, u_2, \ldots, u_n)$$

for some rational numbers $u_1, u_2, \ldots, u_n$. Suppose further that either K is cyclic or the multiplicity of every zero of $f(x)$ is relatively prime to n. Then

$$f(x) = N\big(u_1(x), u_2(x), \ldots, u_n(x)\big)$$

identically, where $u_1(x), u_2(x), \ldots, u_n(x)$ are polynomials with rational coefficients.

We observe that the hypotheses on K are always satisfied if K is normal and of prime degree n.

The two alternatives in the hypothesis—one relating to K and the other to $f(x)$—are appropriate conditions to impose, in the sense that if both are violated, the conclusion may not hold. This is shown by the example (see § 6)

$$f(x) = x^2, \qquad K = Q(e^{2\pi i/8}),$$

where Q denotes the rational number field.

The property of $f(x)$ postulated in the theorem implies the solubility of the congruence

$$f(x) \equiv N(u_1, \ldots, u_n) \pmod m$$

in $u_1, \ldots, u_n$ for every integer x and every positive integer m. The congruence is to be understood in the multiplicative sense; see Hasse [3], 25, footnote*. If K is cyclic, then by a theorem of Hasse [4] this implies the apparently stronger statement that for every x we have

$$f(x) = N(v_1, \ldots, v_n)$$

for some rational $v_1, \ldots, v_n$. Thus when K is cyclic, we have three apparently different conditions on $f(x)$ which are in reality equivalent.

COROLLARY TO THEOREM 2. *Let $f(x)$ be a polynomial with integral coefficients, and suppose that every arithmetical progression contains an integer x such that $f(x)$ is a sum of two squares. Then*

$$f(x) = u_1^2(x) + u_2^2(x)$$

identically, where $u_1(x)$ and $u_2(x)$ are polynomials with integral coefficients.

In the particular case of Theorem 2, namely the case $K = Q(i)$, which is needed for this Corollary, our method of proof has much in common with that used by Lubelski [7] in his investigation of the primes p for which $f(x) \equiv 0 \pmod p$ is soluble.

It will be seen that in the conclusion of the Corollary, it is asserted that $u_1(x), u_2(x)$ have *integral* coefficients. In the more general Theorem 2, if it is postulated that $f(x)$ has integral coefficients and that $u_1, \ldots, u_n$ are integers, it is not in general possible to draw the conclusion with $u_1(x), \ldots, u_n(x)$ having integral coefficients. This is illustrated by the example (see § 6)

$$f(x) = 2x^2(x+1)^2 + 3x(x+1) + 4, \qquad K = Q(\sqrt{-23}).$$

However, it is possible to draw the conclusion stated above if the highest coefficient in $f(x)$ is 1. This can be proved by first comparing the highest terms on both sides, and then appealing to Gauss's lemma.

There are other problems, of the same general character as those considered in this paper, which we are quite unable to attack. The simplest of them is that in which $f(x)$ is representable as a sum of two integral cubes for every sufficiently large integer x.

2. Proof of Theorem 1. We note first that the hypothesis implies that every arithmetical progression contains infinitely many integers x such that the equation has an integral solution in y. For if d is the common difference of the progression, and x_0 is one integer with the property, there exists an integer $x_n \equiv x_0 + d^n \pmod{d^{n+1}}$ for $n = 1, 2, \ldots$ which has the property, and the integers x_n are all distinct.

We factorize $f(x, y)$ into a product of powers of polynomials which are irreducible over the rational field Q; by Gauss's lemma we can take these polynomials to have integral coefficients. We can omit any factor $f_0(x, y)$ for which the equation $f_0(x, y) = 0$ has only finitely many integral solutions, since its omission will not invalidate the hypothesis. We can also omit any factor which does not contain y. Hence we can take

$$f(x, y) = f_1(x, y) f_2(x, y) \ldots f_k(x, y), \tag{2}$$

where $f_1(x, y), \ldots, f_k(x, y)$ are irreducible over Q and are such that each of the equations $f_j(x, y) = 0$ has infinitely many integral solutions.

It follows from Hilbert's Irreducibility Theorem (Hilbert [5], p. 275; for references to later work, see Lang [6], pp. 163-164) that there exists an integer x_0 such that all the polynomials $f_j(x_0, y)$, considered as polynomials in y, are irreducible over Q and are of the same degree in y as $f_j(x, y)$. Suppose first that all these degrees are greater than 1, and let n_j denote the degree of $f_j(x_0, y)$ in y.

Let η be a root of $f_j(x_0, \eta) = 0$, and consider the prime ideal factorization of a rational prime p in $Q(\eta)$ and in its least normal extension $Q^*(\eta)$. Let d_r denote the density (in the Dirichlet series sense) of those primes which have exactly r prime ideal factors of the first degree in $Q(\eta)$. Then (Hasse [3], p. 129)

$$\sum_{r=0}^{n} d_r = 1, \qquad \sum_{r=0}^{n} r d_r = 1.$$

To prove that $d_0 > 0$, it will suffice to prove that $d_1 < 1$. Now any large prime p which has just one prime ideal factor of degree 1 in $Q(\eta)$ will have some prime ideal factor of degree greater than 1 in $Q(\eta)$, and so also in $Q^*(\eta)$. Since $Q^*(\eta)$ is normal, *all* prime ideal factors of p in $Q^*(\eta)$ will be of degree greater than 1, and the density of such p is exactly $1-1/n_j^*$, where n_j^* denotes the degree of $Q^*(\eta)$ (Hasse [3], pp. 138-139). Hence $d_1 \leqslant 1-1/n_j^*$, whence the result. In particular, there are infinitely many primes which have no prime ideal factor of the first degree in $Q(\eta)$.

By a well-known principle of Dedekind, if q_j is such a prime (and is sufficiently large) we have

$$f_j(x_0, y) \not\equiv 0 \pmod{q_j} \tag{3}$$

for all integers y. There is such a prime q_j for each j. On the other hand, the hypothesis of the theorem implies that the arithmetical progression

$$x \equiv x_0 \pmod{q_1 q_2 \dots q_k}$$

contains an integer x such that $f(x, y) = 0$ for some integer y. But then $f_j(x, y) = 0$ for some j, whence

$$f_j(x_0, y) \equiv f_j(x, y) \equiv 0 \pmod{q_j},$$

contrary to (3).

It follows that there is some j for which $f_j(x, y)$ is linear in y, say

$$f_j(x, y) = yA(x) - B(x),$$

where $A(x)$, $B(x)$ are relatively prime polynomials with integral coefficients. There exist polynomials $A_1(x), B_1(x)$ with integral coefficients such that

$$A(x)A_1(x) + B(x)B_1(x) = c$$

identically, where c is a non-zero constant. If x is an integer for which there is an integer y satisfying $f_j(x, y) = 0$, then $A(x)$ must divide c,

and since this happens for infinitely many x, it follows that $A(x)$ is a constant. Hence

$$f_j(x, g(x)) = 0$$

identically, where $g(x)$ is the polynomial $B(x)/A$. This proves Theorem 1.

The deduction of the Corollary is immediate, since we get $f(x) = (g(x))^k$, where $g(x)$ has rational coefficients, and then it follows from Gauss's lemma that $g(x)$ has integral coefficients.

3. LEMMA 1. *Suppose that the hypotheses of Theorem 2 hold. Let*

$$f(x) = c(f_1(x))^{e_1}(f_2(x))^{e_2}\dots(f_m(x))^{e_m}, \tag{4}$$

where $c \neq 0$ is a rational number and $f_1(x), f_2(x), \dots, f_m(x)$ are distinct primitive polynomials with integral coefficients, each irreducible over Q, and where $e_1, e_2, \dots, e_m$ are positive integers. For any j, let q be a sufficiently large prime for which the congruence

$$f_j(x) \equiv 0 \pmod{q} \tag{5}$$

is soluble. If $(e_j, n) = 1$ then q factorizes completely in K into prime ideals of the first degree. If K is cyclic then q factorizes completely into prime ideals of the first degree in the unique subfield K_j of K of degree $n/(e_j, n)$.

Proof. Put

$$F(x) = f_1(x)f_2(x)\dots f_m(x).$$

Since the discriminant of $F(x)$ is not zero, there exist polynomials $\varphi(x)$, $\psi(x)$ with integral coefficients such that

$$F(x)\varphi(x) + F'(x)\psi(x) = D \tag{6}$$

identically, where D is a non-zero integer.

Let q be a large prime for which the congruence (5) is soluble, and let x_0 be a solution. By (6) we have $F'(x_0) \not\equiv 0 \pmod{q}$, whence

$$F(x_0 + q) \not\equiv F(x_0) \pmod{q^2}.$$

By choice of x_1 as either x_0 or $x_0 + q$, we can ensure that

$$f_j(x_1) \equiv 0 \pmod{q}, \qquad F(x_1) \not\equiv 0 \pmod{q^2},$$

whence

$$f_j(x_1) \not\equiv 0 \pmod{q^2} \quad \text{and} \quad f_i(x_1) \not\equiv 0 \pmod{q} \text{ for } i \neq j.$$

By the hypothesis of Theorem 2, there exists $x_2 \equiv x_1 \pmod{q^2}$ such that

$$f(x_2) = N(u_1, u_2, \dots, u_n) \tag{7}$$

for some rational $u_1, u_2, \ldots, u_n$. From the preceding congruences we have

$$f_j(x_2) \equiv 0 \pmod{q}, \quad f_j(x_2) \not\equiv 0 \pmod{q^2},$$
$$f_i(x_2) \not\equiv 0 \pmod{q} \quad \text{for} \quad i \neq j.$$

Hence

$$f(x_2) \equiv 0 \pmod{q^{e_j}}, \quad f(x_2) \not\equiv 0 \pmod{q^{e_j+1}}. \tag{8}$$

Let the prime ideal factorization of q in K be

$$q = \mathfrak{q}_1 \mathfrak{q}_2 \ldots \mathfrak{q}_l; \tag{9}$$

the factors are distinct since q is supposed to be sufficiently large. We note that l divides n because K is a normal field, and that

$$N\mathfrak{q}_i = q^{n/l}. \tag{10}$$

Write the prime ideal factorization of $u_1\omega_1 + \ldots + u_n\omega_n$ in K in the form

$$u_1\omega_1 + \ldots + u_n\omega_n = \mathfrak{q}_1^{a_1} \ldots \mathfrak{q}_l^{a_l} \mathfrak{a}\mathfrak{b}^{-1},$$

where $\mathfrak{a}, \mathfrak{b}$ are ideals in K which are relatively prime to q. Then

$$N(u_1\omega_1 + \ldots + u_n\omega_n) = \pm q^{n(a_1+\ldots+a_l)/l} N\mathfrak{a}(N\mathfrak{b})^{-1}, \tag{11}$$

and $N\mathfrak{a}, N\mathfrak{b}$ are relatively prime to q.

It follows from (7), (8), (11) that

$$n(a_1 + \ldots + a_l)/l = e_j,$$

whence

$$\frac{n}{(e_j, n)} \text{ divides } l.$$

If $(e_j, n) = 1$ we get that n divides l, whence $l = n$ and it follows from (9) and (10) that q factorizes completely in K into prime ideal factors of the first degree.

Now suppose that K is cyclic[1]. The Galois group of K is a cyclic group $\mathscr{G}$ of order n; it has a unique subgroup $\mathscr{H}$ of order n/l, and each $\mathfrak{q}_i$ is invariant under the automorphisms of $\mathscr{H}$. The subgroup $\mathscr{H}$ determines a subfield L of K, of degree l, and $\mathscr{H}$ is the Galois group of K relative to L. A prime ideal factor of q in L cannot split further in K, since any such factors would be derived from one another by the automorphisms of $\mathscr{H}$ and so would not be distinct. Hence the factorization of q in L is also of the form (9). Comparison of norms shows that the $\mathfrak{q}_i$, considered as prime ideals in L, are of the first degree.

The unique subfield K_j of K, of degree $n/(e_j, n)$, is a subfield of L, and therefore q also factorizes completely in K_j, the number of prime ideal factors being equal to the degree of K_j and each being of the first degree.

This completes the proof of Lemma 1.

LEMMA 2. *Let $G(x)$ be a polynomial with integral coefficients, irreducible over Q, and let $G(\theta) = 0$. Let J be any subfield of $Q(\theta)$. Then*

$$G(x) = aN_J\big(H(x)\big) \tag{12}$$

identically, where $H(x)$ is a polynomial over J, and N_J denotes the norm from J to Q, extended in the obvious way to apply to $J[x]$, and a is rational.

Proof. Let ω be a generating element of J and let $\omega^{(1)} = \omega, \ldots, \omega^{(m)}$ be the conjugates of ω, where m is the degree of J. Since J is contained in $Q(\theta)$, we have

$$\omega = g(\theta),$$

where g is a polynomial with rational coefficients. Thus $G(x)$ has a zero in common with the polynomial

$$\prod_{j=1}^{m} \big(g(x) - \omega^{(j)}\big), \tag{13}$$

which has rational coefficients, and since $G(x)$ is irreducible, it must divide this polynomial.

The factors of (13) are relatively prime in pairs, since their differences are non-zero constants. Hence the polynomials

$$H^{(j)}(x) = \big(G(x), g(x) - \omega^{(j)}\big)$$

are relatively prime in pairs, and since each of them divides $G(x)$, their product must divide $G(x)$. Thus

$$G(x) = A(x) \prod_{j=1}^{m} H^{(j)}(x) = A(x) N_J\big(H^{(1)}(x)\big).$$

The norm on the right is a non-constant polynomial with rational coefficients, so it follows from the irreducibility of $G(x)$ that $A(x)$ is a constant. This proves the result.

LEMMA 3 (Bauer). *Let J be a normal number field and let k be any number field. Suppose that every sufficiently large prime which has at least one prime ideal factor of the first degree in k also has at least one prime ideal factor of the first degree in J. Then J is contained in k.*

Proof. See Bauer [1] or Hasse [3], pp. 138 and 141.

[1] In dealing with this case we do not need to exclude the possibility that $(e_j, n) = 1$.

4. Proof of Theorem 2. Let $f(x)$ be the polynomial of the theorem, and $f_j(x)$ any one of its irreducible factors, as in (4). Let θ be any zero of $f_j(x)$ and q any large prime which has at least one prime ideal factor of the first degree in $Q(\theta)$. Then by Dedekind's theorem the congruence

$$f_j(x) \equiv 0 \pmod q$$

is soluble.

If $(e_j, n) = 1$, it follows from Lemma 1 that q factorizes completely in the field K. By Lemma 3, with $J = K$ and $k = Q(\theta)$, this implies that K is contained in $Q(\theta)$. It follows now from Lemma 2, with $G(x) = f_j(x)$, that $f_j(x)$ is expressible identically in the form

$$f_j(x) = a_j N_K\big(H_j(x)\big),$$

as in (12). Hence

$$\big(f_j(x)\big)^{e_j} = a_j^{e_j} N_K\big(H_j^{e_j}(x)\big) = b_j N_K\big(H_j^*(x)\big). \tag{14}$$

Now suppose that K is cyclic. It follows from Lemma 1 that q factorizes completely in the field K_j. By Lemma 3 with $J = K_j$ and $k = Q(\theta)$, this implies that K_j is contained in $Q(\theta)$. It follows now from Lemma 2, with $G(x) = f_j(x)$, that $f_j(x)$ is expressible identically in the form

$$f_j(x) = a_j N_{K_j}\big(H_j(x)\big).$$

Now

$$N_K\big(H_j(x)\big) = \big\{N_{K_j}\big(H_j(x)\big)\big\}^{(e_j, n)},$$

since the degree of K relative to K_j is (e_j, n). Hence

$$\big(f_j(x)\big)^{e_j} = a_j^{e_j}\big\{N_K\big(H_j(x)\big)\big\}^{e_j/(e_j, n)} = b_j N_K\big(H_j^*(x)\big). \tag{15}$$

The conclusions (14) and (15), reached on the two alternative hypotheses, are the same. By (4) and the multiplicative property of the norm, we have

$$f(x) = a N_K\big(h(x)\big),$$

where $h(x)$ is a polynomial over K. By the hypothesis of the theorem, taking x to be a suitable integer, we infer that a is the norm of an element α of K. Putting

$$\alpha h(x) = \omega_1 u_1(x) + \ldots + \omega_n u_n(x),$$

we obtain

$$f(x) = N\big(u_1(x), \ldots, u_n(x)\big)$$

identically.

5. Proof of the Corollary to Theorem 2. It follows from the theorem, on taking $K = Q(i)$, that

$$f(x) = U_1^2(x) + U_2^2(x),$$

where U_1, U_2 are polynomials with rational coefficients. Let

$$U_1(x) + iU_2(x) = \alpha v(x),$$

where $v(x)$ is a primitive polynomial whose coefficients are integers in $Q(i)$ and α is an element of $Q(i)$. Then

$$f(x) = |\alpha|^2 v(x)\bar{v}(x).$$

Since $v(x)$ and $\bar{v}(x)$ are both primitive and $f(x)$ has integral coefficients, it follows from Gauss's lemma that $|\alpha|^2$ is an integer. But $|\alpha|^2$ is a sum of two rational squares, and so it must be a sum of two integral squares, i.e. $|\alpha|^2 = |\beta|^2$, where β is an integer in $Q(i)$. Putting

$$\beta v(x) = u_1(x) + iu_2(x),$$

where u_1, u_2 are polynomials with (rational) integral coefficients, we get

$$f(x) = u_1^2(x) + u_2^2(x).$$

6. Two examples. (1) Suppose that

$$f(x) = x^2, \qquad K = Q(e^{2\pi i/8}).$$

We prove first that every square is expressible as a value of the norm form of K. This norm form is

$$N(u_1 + \sqrt{i}\,u_2 + iu_3 + \sqrt{i^3}\,u_4) = (u_1^2 - u_3^2 + 2u_2u_4)^2 + (u_2^2 - u_4^2 - 2u_1u_3)^2.$$

Plainly 2^2 is representable with $u_1 = u_3 = 0$, $u_2 = u_4 = 1$.

Also if p is a prime and $p \equiv 1 \pmod 4$ then $p = a^2 + b^2$ and p^2 is representable with $u_1 = u_3 = 0$, $u_2 = a$, $u_4 = b$. Finally, if $p \equiv 3 \pmod 4$ then p is representable either as $a^2 - 2b^2$ or as $a^2 + 2b^2$, and we take $u_1 = b$, $u_3 = \pm b$, $u_2 = a$, $u_4 = 0$.

On the other hand, x^2 is not representable in the form

$$x^2 = N\big(u_1(x), \ldots, u_4(x)\big),$$

where $u_1(x), \ldots, u_4(x)$ are polynomials with rational coefficients. For if the greatest degree of any of these polynomials is $g \geqslant 1$, then the coefficient of x^{4g} on the right is $N(c_1, \ldots, c_4)$, where $c_1, \ldots, c_4$ are rational numbers, not all zero, and this coefficient is not 0.

In this example, K is normal but not cyclic, and the multiplicity of the zero of $f(x)$ is not relatively prime to the degree (namely 4) of K.

(2) Suppose that

$$f(x) = 2x^2(x+1)^2+3x(x+1)+4, \qquad K = Q(\sqrt{-23}).$$

Here the norm form of K is

$$N(u_1, u_2) = u_1^2+u_1u_2+6u_2^2.$$

For every integer x we have $x(x+1) = 2t$, where t is an integer, and

$$f(x) = 8t^2+6t+4 = N(t+2, t).$$

On the other hand, if $u_1(x)$, $u_2(x)$ are polynomials in x with *integral* coefficients, the coefficient of the highest power of x in $N(u_1(x), u_2(x))$ is an integer of the form

$$a^2+ab+6b^2,$$

and cannot be 2, since the least positive integer other than 1 represented by this form is 6.

References

[1] M. Bauer, *Zur Theorie der algebraischen Zahlkörper*, Math. Annalen 77 (1916), pp. 353-356.

[2] E. Fried and J. Suranyi, *Neuer Beweis eines zahlentheoretischen Satzes über Polynome*, Matematikai Lapok 11 (1960), pp. 75-84.

[3] H. Hasse, *Bericht über Klassenkörpertheorie II*, Jahresber. der Deutschen Mathematiker-Vereinigung, supplementary vol. 6 (1930).

[4] — *Beweis eines Satzes und Widerlegung einer Vermutung über das allgemeine Normenrestsymbol*, Göttinger Nachrichten, 1931, pp. 64-69.

[5] D. Hilbert, *Über die Irreduzibilität ganzer rationaler Funktionen mit ganzzahligen Koeffizienten*, Ges. Abhandlungen II, pp. 264-286.

[6] S. Lang, *Diophantine Geometry*, New York and London, 1962.

[7] S. Lubelski, *Zur Reduzibilität von Polynomen in der Kongruenztheorie*, Acta Arithmetica 1 (1936), pp. 169-183 and 2 (1938), pp. 242-261.

[8] G. Pólya and G. Szegö, *Aufgaben und Lehrsätze aus der Analysis*, II.

Reçu par la Réduction le 6. 4. 1963