ACTA ARITHMETICA
XVII (1970)

Conspectus materiae tomi XVII, fasciculi 2

La revue est consacrée à la Théorie des Nombres
The journal publishes papers on the Theory of Numbers
Die Zeitschrift veröffentlicht Arbeiten aus der Zahlentheorie
Журнал посвящен теории чисел

L'adresse de la Rédaction et de l'échange	Address of the Editorial Board and of the exchange	Die Addresse der Schriftleitung und des Austausches	Адрес Редакции и книгообмена

ACTA ARITHMETICA
ul. Śniadeckich 8, Warszawa 1

Les volumes IV et suivants sont à obtenir chez	Volumes from IV on are available at	Die Bände IV und die folgende sind zu beziehen durch	Томы IV и следующие можно получить через

Ars Polona, Krakowskie Przedmieście 7, Warszawa 1

Prix d'un fascicule	Prize of an issue	Preis für ein Heft	Цена номера
$. 4.00			

Les volumes I–III sont à obtenir chez	Volumes I–III are available at	Die Bände I–III sind zu beziehen durch	Томы I–III можно получить через

Johnson Reprint Corporation, 111 Fifth Ave., New York, N. Y.

PRINTED IN POLAND

WROCŁAWSKA DRUKARNIA NAUKOWA

On the theory of nth power residues and a conjecture of Kronecker

by

I. Gerst (Stony Brook, N. Y.)

1. Introduction. For given rational integers $n > 1$ and a, let $P(a)$ denote the set of rational primes p for which the congruence $x^n \equiv a \pmod p$ is solvable. In this paper, we consider the following question: How are two integers a and b related if $P(a)$ and $P(b)$ are essentially the same? Here the term *essentially the same* can be taken to mean: the same except for a finite number of primes; or, more generally, as we shall assume in the sequel: *the same except for a set of primes having Dirichlet density zero*. With this definition understood, we write $P(a) = P(b)$ when $P(a)$ and $P(b)$ are essentially the same.

The question we have posed arises naturally when one considers Kronecker's conjecture on polynomial equivalence in the binomial case (cf. § 4). However, independently of this application, the question is of basic interest in the theory of nth power residues; yet, there seems to be no treatment of it in the literature, at least in the general form stated here. One special case, though, has been the subject of fairly extensive research in recent years—namely, the case $b = 1$. Then, $P(b)$ is the set of all primes which we will designate by P, and the relation $P(a) = P$ is described by saying that $P(a)$ contains *almost all primes*. Our question becomes: What is the form of an integer a which is an nth power residue of almost all primes? The solution to this problem was given first by Trost [14] in 1934. Subsequent treatments as well as generalizations to algebraic number fields may be found in [1], [6], [12] (for $n = 2$, see also [8], [11]).

Our own results which resolve completely the question raised, are embodied in the following theorem whose proof will occupy the greater part of this paper:

Theorem 1. *Let n, a and b be rational integers with $n > 1$ and $ab \neq 0$. Then a necessary and sufficient condition that $P(a) = P(b)$ is that there exist a rational integer t with $0 < t < n$, $(t, n) = 1$ such that either*

(i) $ab^t = d^n$, *for some integer d, or, if $8 \mid n$,*

(ii) $ab^t = 2^{n/2} d^n$, *for some integer d.*

For the purpose of orientation, we make the following observations relative to Theorem 1.

(a) The sufficiency of the condition (i) or (ii) is proved by elementary means, and the proof yields the stronger conclusion that $P(a)$ and $P(b)$ differ at most in a finite number of primes. The possible exceptional primes which, perhaps, do not appear in both $P(a)$ and $P(b)$ are those odd primes which divide exactly one of a and b.

(b) It is possible that both conditions (i) and (ii) can be satisfied but, of course, for different values of t; e.g. $n = 8$, $a = 2$, $b = 2^3$, where $t = 1, 5$ yield the forms (ii) and (i) respectively.

(c) The symmetry of our hypothesis with respect to a and b leads us also to expect relations of the form (i) or (ii) in which the roles of a and b are interchanged. Indeed, such relations can be obtained by raising each member in (i) or (ii) to the sth power, where $0 < s < n$ and $st \equiv 1 (\mathrm{mod} n)$.

(d) The theorem holds as well without the condition $0 < t < n$. The form stated here has the advantage of indicating explicitly that conditions (i) or (ii) can be checked in a finite number of steps.

If we let $b = 1$ in Theorem 1, we get as a corollary (except for the trivial case $a = 0$) the result of Trost:

COROLLARY. *Let $n > 1$ and a be rational integers. Then a necessary and sufficient condition that $P(a) = P$ is that either*

(i) $a = d^n$ *for some integer* d, *or, if* $8 | n$,

(ii) $a = 2^{n/2} d^n$ *for some integer* d.

Our observation (a) above implies that actually $P(a)$ is P if condition (i) or (ii) of the Corollary is satisfied. The Corollary enables us to dispose of those values of a and b which were excluded from consideration in Theorem 1. For if, say, $b = 0$ then $P(b) = P$ and the form of a is given by the Corollary.

By comparing Theorem 1 and its Corollary, we infer

THEOREM 2. *Let n, a and b be rational integers with $n > 1$ and $ab \neq 0$. Then $P(a) = P(b)$ if and only if there exists an integer t with $0 < t < n$, $(t, n) = 1$ for which $P(ab^t) = P$.*

If it were possible to prove Theorem 2 directly, then Theorem 1 would follow from the Corollary. However we have been able to do this only in the case $n = 2$ (cf. the remark at the end of § 3).

Our proof of Theorem 1 makes use of fairly elementary properties of algebraic number fields, particularly cyclotomic fields, with one exception. This is the utilization of a result of Bauer (cf. Lemma 2) which relates to the unique determination of an algebraic number field by the set of prime divisors of any of its defining polynomials. Analogous considerations had been employed in some of the proofs of the Corollary cited previously. However, except for the application of a lemma found in [6], the details of our proof differ to a considerable extent from those given in these earlier papers, especially in the case when n is even. This is a consequence of the fact that we can no longer proceed, as in proving the Corollary, by first taking n to be a power of a prime.

In the next section, we assemble the background material concerning fields and prime divisors of polynomials which we will require. Theorem 1 is then proved in § 3. Finally, in § 4, we apply this theorem to settle the validity of the Kronecker conjecture for the case of monic, irreducible binomials; that is, we specify when two such polynomials which have essentially the same sets of prime divisors determine the same simple extension fields over the rationals. In particular, there result counter-examples to the conjecture which involve binomials of degree eight.

2. Preliminary lemmas. Throughout this paper we shall use the following notation. We denote the rational number field by Q, and for each integer $n \geq 1$, we set $\zeta_n = e^{2\pi i/n}$, and write Q_n for the corresponding cyclotomic field $Q(\zeta_n)$. The radical $\sqrt[n]{a}$ will mean, unless further specified, any fixed root of the equation $x^n - a = 0$. We shall use the symbol p, always, to denote a rational prime, while d, d', d_0, d_1, ..., will designate rational integers which are defined by the equation in which they appear and which need not be the same in different equations. The latter are used to avoid repetitions of the phrase "for some integer...". Finally, the "equality" $S = T$, where S and T are sets of rational primes will always be understood in the sense defined in the introduction. It is easily seen that "=" as used here is an equivalence relation.

Let $h(x)$ be a non-constant polynomial with rational integer coefficients. A prime p for which the congruence $h(x) \equiv 0 (\mathrm{mod} p)$ is solvable is called a prime divisor of $h(x)$. The set of all prime divisors of $h(x)$ will be denoted by $P(h)$. Further, if $\deg h(x) = n$, let $P_i(h)$, $i = 1, 2, \ldots, n$, denote the set of primes for which $h(x) \equiv 0 (\mathrm{mod} p)$ has exactly i incongruent solutions. Thus $P(h)$ will be the union of the sets $P_i(h)$. In terms of this notation which we shall employ henceforth, what we called $P(a)$ in the introduction is now denoted by $P(f)$ where $f(x) = x^n - a$.

Next, if K is an algebraic number field, define $P(K)$ as the set of rational primes p such that the factorization of p into prime ideals in K contains at least one prime ideal factor of the first degree. The two sets $P(h)$ and $P(K)$ which we have defined are related to each other when $h(x)$ is irreducible over Q and has a primitive element of K as a root. In that case, it is well-known [5] that $P(h) = P(K)$. It is also known [9], that if $h(x)$, of degree n, is irreducible over Q, and K is the splitting field of $h(x)$, then $P_n(h) = P(K)$.

We require an extension of this last result to the case where $h(x)$ is reducible over Q. This is provided by the following lemma in which we use the term separable polynomial to mean one without multiple roots.

LEMMA 1. *Let $h(x)$ be a separable polynomial of degree $n \geqslant 1$ with rational integer coefficients, and let K be the splitting field of $h(x)$. Then*

$$P_n(h) = P(K).$$

Proof. Let $h = h_1 h_2 \dots h_s$, where the h_i are distinct irreducible polynomials over Q with integer coefficients and $\deg h_i = n_i$. Then, taking into account the non-vanishing of the discriminant of $h(x)$, it is easily seen that

$$P_n(h) = \bigcap_{i=1}^{s} P_{n_i}(h_i). \tag{1}$$

For each $i = 1, 2, \dots, s$, let K_i be the splitting field of h_i. Evidently K is the compositum of the K_i. But then we have

$$P(K) = \bigcap_{i=1}^{s} P(K_i). \tag{2}$$

(This result is known for $s = 2$, [9], and follows easily for any s by induction.) A comparison of (1) and (2) establishes the lemma.

Remark. In Lemma 1, $P_n(h)$ and $P(K)$ actually differ in at most a finite set of primes; and the same observation applies to the other equalities between sets of primes listed thus far. However, we shall not require these stronger results in our proof of Theorem 1.

We quote next the following special case of a theorem of Bauer ([2], [3]), which is basic in our considerations:

LEMMA 2. *Let K and L be two algebraic number fields which are normal over Q and for which $P(K) = P(L)$. Then $K = L$.*

In the remainder of this section, we discuss certain results pertaining to special algebraic number fields.

We begin by mentioning some facts regarding the irreducibility over Q of the polynomial $h(x) = x^n - c$, where c is an integer (cf. [4], [15] for proofs). It is known that $h(x)$ is irreducible if and only if $h_1(x) = x^{p^l} - c$ is irreducible for each prime power p^l in the canonical factorization of n. For $h_1(x)$ to be reducible, we must have either $c = d^p$, or, if $p = 2$, $l \geqslant 2$, $c = -4d^4$.

Using these results, we can deduce several elementary but nonetheless useful assertions concerning the normality over Q of the field $Q(\sqrt[n]{c})$. These we find convenient to formalize as

LEMMA 3. *Let n and m be natural numbers, and let $c \neq 0$ be a rational integer which is assumed to be positive when n is even. Let $\sqrt[n]{c}$ denote the real (real, positive) value of the radical if n is odd (even). Suppose, respectively, that (a) $\sqrt[n]{c}$ is of degree n; (b) $n = p^m$, p odd; (c) $n = 2^m$. Then $Q(\sqrt[n]{c})$, is normal over Q if and only if the following conditions hold in the respective cases:*

(a) *$n = 1$ or 2;*
(b) *$c = d^{p^m}$;*
(c) *either $c = d^{2^m}$, or $c = d^{2^{m-1}}$ with d not a square.*

Proof. We consider only the necessity of the conditions stated since the sufficiency is trivial.

Statement (a) is immediate since for $n \geqslant 3$, the real field $Q(\sqrt[n]{c})$ has at least one conjugate field which is complex.

To prove (b) and (c), write c in the form $c = d^{p^r}$, where r is a non-negative integer and d is not a perfect pth power. When $p = 2$, we may assume $d > 0$. Then $Q(\sqrt[p^m]{c}) = Q(\theta)$, where $\theta = (d)^{1/p^{m-r}}$ and the real (real, positive) value of the radical is taken when p is odd (even). By the results on irreducibility just discussed, $\deg \theta = \max(1, p^{m-r})$, and so, in view of part (a) of this lemma, we must have $p^{m-r} \leqslant 2$; that is, $r \geqslant m$ for arbitrary p, or $r = m-1$ when $p = 2$. Our proof is complete.

The following lemma, except for a trivial modification, is a special case of a result given by Flanders ([6], Lemma 5). We refer to his paper for a proof.

LEMMA 4. *Let n, a and b be rational integers with $n > 1$ and $ab \neq 0$, and let $Q_n(\sqrt[n]{a}) = Q_n(\sqrt[n]{b})$. Then $ab^t = \gamma^n$ where t is a rational integer with $0 < t < n$, $(t, n) = 1$, and $\gamma \in Q_n$.*

We complete this section by quoting a result which is known from the theory of cyclotomy (cf. [17]).

LEMMA 5. *Let $n \geqslant 3$ be a rational integer whose canonical factorization is $n = 2^m q_1^{a_1} q_2^{a_2} \dots q_s^{a_s}$, where the q_i are distinct odd primes, $m \geqslant 0$ and $a_i > 0$, $i = 1, 2, \dots, s$. Then the quadratic subfields of Q_n are given by $Q(\sqrt{l})$ with*

$$l = (-1)^e 2^{e_0} \prod_{i=1}^{s} (-1)^{e_i (q_i - 1)/2} q_i^{e_i},$$

where

$$e = e_0 = 0 \quad \text{if} \quad m = 0, 1;$$

$$e_0 = 0 \quad \text{if} \quad m = 2;$$

and otherwise e, e_0 and each e_i can take either the value 0 or 1 except that not all of them can be zero simultaneously.

3. Proof of Theorem 1. We start by establishing the sufficiency of the conditions given in Theorem 1, as the proof will serve to illustrate a line of reasoning occurring at several points in this section. It suffices to consider condition (ii) since it will be clear that a similar argument applies even more readily in the case of condition (i).

For the remainder of the paper, we use the notation $f = x^n - a$, $g = x^n - b$. Thus, we must show that $P(f) = P(g)$. Actually, we shall prove that for each $i = 1, 2, \ldots, n$, $P_i(f)$ and $P_i(g)$ differ at most in a finite number of primes.

For the purpose of this argument, let us call a prime p *admissible* if p is odd and $p \nmid ab$. If p is admissible, then (ii) of Theorem 1 considered modulo p implies in terms of some set of indices that

$$\operatorname{ind} a + t \operatorname{ind} b \equiv \frac{n}{2} \operatorname{ind} 2 + n \operatorname{ind} d \pmod{p-1}. \tag{3}$$

Suppose also that $p \in P_i(f)$ for some $i = 1, 2, \ldots, n$. Recall from the theory of binomial congruences that for $p \nmid a$, $f \equiv 0 \pmod p$ is solvable precisely when $(n, p-1) \mid \operatorname{ind} a$, and when solvable has exactly $(n, p-1)$ incongruent roots. Thus, we must have the relations $i = (n, p-1)$ and $i \mid \operatorname{ind} a$. It follows that $p \in P_i(f)$ is possible only if i is an even divisor of n, but then, using the relations just given, we can deduce from (3) that

$$t \operatorname{ind} b \equiv 0 \pmod i. \tag{4}$$

This is clear if $i \mid n/2$. When $i \nmid n/2$, then $8 \mid i$, and so $p \equiv 1 \pmod 8$. Thus, ind 2 is even, since 2 is a quadratic residue of p, and (4) again follows.

In view of the condition $(t, n) = 1$, (4) yields $i \mid \operatorname{ind} b$, that is, $p \in P_i(g)$. Since the roles of f and g can be interchanged in our argument, we have shown that $P_i(f)$ and $P_i(g)$, for each i, either contain no admissible primes or they contain the same admissible primes. Our assertion above is therefore established. As $P_1(f)$ and $P_1(g)$ each contain $p = 2$, and also contain, respectively, those primes which divide a and b respectively, our remark (a) in the introduction follows.

We turn now to the more difficult task of substantiating the necessity of the conditions in Theorem 1; that is, given that

$$P(f) = P(g), \tag{5}$$

we will show that either condition (i) or (ii) follows. Our earlier remark about the solutions of binomial congruences leads to the following observation: for $p \nmid a$, the number of incongruent roots of a solvable congruence $f \equiv 0 \pmod p$ depends only on n and p (not on a). As an immediate consequence, we get from (5) that $P_i(f) = P_i(g)$ for each $i = 1, 2, \ldots, n$. In particular,

$$P_n(f) = P_n(g). \tag{6}$$

Let K and L be the splitting fields of f and g respectively. Plainly, $K = Q(\sqrt[n]{a}, \zeta_n)$ and $L = Q(\sqrt[n]{b}, \zeta_n)$. Now, since $ab \neq 0$, we may apply Lemma 1 to get $P_n(f) = P(K)$, $P_n(g) = P(L)$. Then, from (6) and Lemma 2, we find $K = L$. Since also $K = Q_n(\sqrt[n]{a})$ and $L = Q_n(\sqrt[n]{b})$, there exists, by Lemma 4, a rational integer t with $0 < t < n$, $(t, n) = 1$ for which

$$ab^t = \gamma^n, \quad \gamma \in Q_n. \tag{7}$$

We proceed to examine the condition (7) more closely. For future application, we emphasize at this point the fact that (7) was deduced from the single condition (6).

In the remainder of this section, we shall use the following notation: $c = ab^t$; $n = 2^m k$, $m \geqslant 0$, k odd; if $k > 1$, we write $k = q_1^{a_1} q_2^{a_2} \ldots q_s^{a_s}$ with the q_i distinct odd primes and the $a_i > 0$.

It is convenient to divide the discussion into three cases according to the power of 2 which divides n.

Case 1: n odd. Denote by q^j any one of the powers $q_i^{a_i}$ which divide k. From (7), we infer that the equation $x^{q^j} - c = 0$ has a root $\gamma' = \gamma^{n/q^j}$ which is in Q_n. Since the roots of this equation are all of the form $\zeta_{q^j}^r \sqrt[q^j]{c}$ where $\sqrt[q^j]{c}$ can be taken to be real and r is a rational integer, it follows that $\sqrt[q^j]{c}$ is in Q_n. Thus, $Q(\sqrt[q^j]{c})$ is a real subfield of Q_n which must be normal over Q since Q_n is Abelian. By Lemma 3, this is possible only if $c = d^{q^j}$. As c is of this form for each q_i, we conclude, by comparing powers of the same prime which divide each of these forms, that $c = d_1^n$. This is (i), and our proof is complete.

Remark. In this case, we have actually shown that condition (i) follows from the single condition $P_n(f) = P_n(g)$; or, put another way, that the condition $P_n(f) = P_n(g)$ implies $P_i(f) = P_i(g)$ for each i, $1 \leqslant i \leqslant n-1$. Such an implication is no longer true, in general, for n even. We give counter examples from each of the cases remaining to be considered.

Example 1. Let $n = 10$, $a = 5^2$, $b = 5^3$. Then $(10, p) = 10$ iff $p \equiv 1 \pmod{10}$, and, since 5 is a quadratic residue of primes in this class, we have

$$\operatorname{ind} a + \operatorname{ind} b \equiv 5 \operatorname{ind} 5 \equiv 0 \pmod{10}.$$

Thus $P_{10}(f) = P_{10}(g)$.

On the other hand, for primes $p \equiv 3 \pmod{10}$ where $(10, p) = 2$, and 5 is a quadratic non-residue of p, we find $\operatorname{ind} a + \operatorname{ind} b \equiv 1 \pmod 2$. Thus each prime p in this class is in exactly one of $P_2(f)$ and $P_2(g)$ and so $P_2(f) \neq P_2(g)$.

EXAMPLE 2. Let $n = 12$, $a = 3^2$, $b = 3^4$. The relation $P_{12}(f) = P_{12}(g)$ is established by the procedure of Example 1. When $p \equiv 5 \pmod{12}$, then $(12, p) = 4$ and, clearly, every such prime is in $P_4(g)$. But since 3 is a quadratic non-residue of p, $4 \nmid \operatorname{ind} a$, and thus no such prime is in $P_4(f)$, i. e., $P_4(f) \neq P_4(g)$.

We conclude from these examples that for n even we cannot expect to prove Theorem 1 using (6) alone, but that we must also take into account the other relations $P_i(f) = P_i(g)$, $i = 1, 2, \ldots, n-1$ which we know to hold. Stated in other terms, it will not suffice to consider solely the primes $p \equiv 1 \pmod n$ of the principal class modulo n. It is this circumstance which will complicate the proofs in the remaining cases. It is no coincidence that $(n, a) > 1$, $(n, b) > 1$ in the above examples for it will be apparent from our argument later that the procedure of Case 1 goes through essentially unchanged when $(n, a) = (n, b) = 1$.

Case 2: $n = 2k$. If $k = 1$, then $Q_n = Q$ and from (7) we get $c = d^2$, as required.

Hence, assume $k > 1$. The argument used in Case 1 applies here as well for each of the prime powers dividing n. By considering the odd prime powers, we find again that $c = d^k$. Using the prime 2, we conclude that $x^2 - c$ has its roots in Q_n. There are two possibilities here which we consider in turn.

(a) $c = d_1^2$.

When coupled with the preceding assertion, $c = d^k$, (a) implies that $c = d_2^n$, so that condition (i) holds here.

(b) $c \neq d_1^2$.

Then $Q(\sqrt{c})$ is a quadratic subfield of Q_n and by Lemma 5

$$c = u d_2^2, \tag{8}$$

with

$$u = \prod_{i=1}^{s} (-1)^{e_i (q_i - 1)/2} q_i^{e_i}, \tag{9}$$

where each e_i is either 0 or 1 except that not all e_i are zero simultaneously.

We show next that (8) and (9) imply the existence of a set of primes, S, of positive Dirichlet density, such that each prime of S is in exactly one of the sets $P_2(f), P_2(g)$. This conclusion is incompatible with the relation $P_2(f) = P_2(g)$ which we know to hold, and so subcase (b) is seen to be impossible.

In order to describe S, we assume that the q_i have been ordered so that $q_1 < q_2 < \ldots < q_s$. Then S consists of those primes p which satisfy the following conditions:

(α) $p \nmid ab$;

(β) $p \equiv 1 \pmod 4$;

(γ) if q_l is the first q_i for which $e_i = 1$ in (9), let $p \equiv n_l \pmod{q_l}$, where n_l is a quadratic non-residue modulo q_l;

(δ) for all other q_i for which $e_i = 1$ in (9), let $p \equiv r_i \pmod{q_i}$ where r_i is a quadratic residue modulo q_i and $r_i \not\equiv 1 \pmod{q_i}$;

(ε) for those q_i for which $e_i = 0$ in (9), let $p \equiv m_i \pmod{q_i}$ where m_i is any reduced residue modulo q_i such that $m_i \not\equiv 1 \pmod{q_i}$.

It is clear that S consists of the primes in a reduced residue class modulo $4q_1 q_2 \ldots q_s$ with a finite number of exceptions, and thus, as is well-known, the Dirichlet density of S exists and is positive. It follows from our definition of S that for $p \in S$ and for each $i = 1, 2, \ldots, s$, $q_i \nmid (p-1)$, and so we have

$$(n, p-1) = 2, \quad p \in S. \tag{10}$$

Furthermore, we assert that for u in (9)

$$\left(\frac{u}{p}\right) = -1, \quad p \in S. \tag{11}$$

($\left(\frac{u}{p}\right)$ = Legendre symbol.)

For, by applying the Quadratic Reciprocity Law and taking account of the conditions (α)–(ε), we find after a simple calculation that $(u/p) = (n_l/q_l)$.

Now, for $p \in S$, consider (8) modulo p and transform to indices. Then

$$\operatorname{ind} c \equiv \operatorname{ind} a + t \operatorname{ind} b \equiv \operatorname{ind} u + 2 \operatorname{ind} d_2 \pmod{(p-1)}.$$

We have that t and $\operatorname{ind} u$ are both odd, the latter by virtue of (11). Thus

$$\operatorname{ind} a + \operatorname{ind} b \equiv 1 \pmod 2,$$

and therefore exactly one of $\operatorname{ind} a$, $\operatorname{ind} b$ is divisible by 2. Together with (10), this means that p belongs to exactly one of $P_2(f), P_2(g)$. Our proof is complete.

Case 3: $n = 2^m k$, $m \geq 2$. We show first that $c > 0$. Assume the contrary and let $c_1 = -c$, so that $c_1 > 0$. Equation (7) now implies that $x^{2^m} + c_1$ has a root ϱ ($= \gamma^k$) which is in Q_n. We may write $\varrho = \zeta_{2^{m+1}}^{r} \sqrt[2^m]{c_1}$, where the radical has its real, positive value and r is an odd integer. It follows that $\sqrt[2^m]{c_1} \in Q_{2n}$, and so, by an argument used previously, $Q(\sqrt[2^m]{c_1})$

is normal over Q. Then, by Lemma 3, either (a) $c_1 = d^{2^m}$, or (b) $c_1 = d^{2^{m-1}}$, d not a square. We will show that both (a) and (b) lead to contradictions.

If (a) obtains, then it follows that $\zeta_{2^{m+1}}^r = \varrho/\sqrt[2^m]{c_1} \in Q_n$. This is impossible, for it would mean that $Q_n = Q_{2n}$, contrary to the fact that $[Q_{2n}: Q] = 2[Q_n: Q]$ for the values of n under consideration.

The remaining condition (b) can be shown to lead to a contradiction of the known relation $P_2(f) = P_2(g)$, in the same manner as this was done in Case 2. This time we choose for the set S those primes p with $p \nmid ab$, $p \equiv 3 \pmod 4$, and $p \equiv m_i \pmod{q_i}$ for each q_i dividing k, where m_i is any reduced residue modulo q_i such that $m_i \not\equiv 1 \pmod{q_i}$. The condition $(n, p-1) = 2$ for $p \in S$ is easily verified; and in view of the fact that $\operatorname{ind}(-1)$ is odd for $p \in S$, (b) leads directly to the congruence $\operatorname{ind} a + \operatorname{ind} b \equiv 1 \pmod 2$. The details are left to the reader.

In the remainder of this section we may therefore assume that $c > 0$. From (7) there now follows, by an argument already used several times, the result that the real field $Q(\sqrt[2^m]{c})$ is normal over Q. By Lemma 3, we must have either (α) $c = d^{2^m}$, or (β) $c = d^{2^{m-1}}$, d not a square, where we may suppose also that $d > 0$.

If (β) holds, then $Q(\sqrt{d})$ is a real, quadratic subfield of Q_n and so, by virtue of Lemma 5, $d = 2^w u d_1^2$, where u is an odd, positive, square-free divisor of n, and $w = 0$ if $m = 2$, while $w = 0$ or 1 if $m \geqslant 3$. Here $2^w u > 1$. Thus, in subcase (β),

$$c = (2^w u)^{2^{m-1}} d_1^{2^m}. \tag{12}$$

It will be convenient in what follows to treat conditions (α) and (β) simultaneously. We achieve this by allowing also the value $2^w u = 1$ in (12).

Now, c is also of the form $c = d_2^k$ (cf. Case 2). A comparison of this form and (12) leads readily to

$$ab^t = (2^w u)^{n/2} d^n, \tag{13}$$

where we reiterate that $0 < t < n$, $(t, n) = 1$, $w = 0$ or 1 with $w \neq 1$ if $m = 2$, and u is an odd, positive, square-free divisor of n. In (13), if $w = 0$, $u = 1$, we get condition (i) of Theorem 1, while if $w = 1$, $u = 1$ we get (ii). Observe that this last possibility can occur only if $m \geqslant 3$.

Can we actually have (13) with $u > 1$? Certainly this is not possible if $k = 1$ and so our theorem is established in this case.

Hence, suppose $k > 1$. Then it turns out, in contrast to Case 2, that we may very well have $u > 1$ in (13) even when the other conditions $P_i(f) = P_i(g)$, $1 \leqslant i \leqslant n-1$ hold. This fact further complicates the proof in this case. As an illustration, consider the example when $n = 12$, $a = 3$, $b = 3^5$. Then with $t = 1$, $ab^t = 3^6$ which is of the form (13) with $w = 0$, $u = 3$. But note that with $t = 7$, $ab^t = (27)^{12}$, which is in the form of condition (i), and so $P(f) = P(g)$.

In order to complete the proof of Theorem 1 in this case, we must show that although there may be relations (13) with $u > 1$, nevertheless there always exists at least one such relation in which $u = 1$. Our approach will be indirect. Hence, suppose that for all integers t with $0 < t < n$, $(t, n) = 1$ for which ab^t is of the form given by (13), that we have $u > 1$. (There will be at least one such relation (13), as we have shown.) Then we will obtain a contradiction by proving that $P_i(f) \neq P_i(g)$ for a suitable i.

Let j, $1 \leqslant j \leqslant s$, denote the minimum number of odd primes q_i which divide u in all relations of the form (13), and let us call relation (13) *minimal* if u is a product of exactly j primes. Select one such minimal relation. By re-indexing the q_i, we may suppose that the corresponding $u = q_1 q_2 \dots q_j$. Write $u_1 = q_1 q_2 \dots q_{j-1}$ if $j \geqslant 2$ and $u_1 = 1$ if $j = 1$.

Now consider all minimal relations (13) in which $u_1 \mid u$. Select a maximal set of such relations which have distinct u's, by arbitrarily choosing one relation in each group of relations having equal u's. Let r be the number of relations in the maximal set. Plainly, $1 \leqslant r \leqslant s-j+1$.

Without loss of generality, we may write the relations in the maximal set as

$$\begin{aligned} ab^{t_1} &= (2^{w_1} u_1 q_j)^{n/2} d_1^n, \\ ab^{t_2} &= (2^{w_2} u_1 q_{j+1})^{n/2} d_2^n, \\ &\dots\dots\dots\dots\dots \\ ab^{t_r} &= (2^{w_r} u_1 q_{j+r-1})^{n/2} d_r^n. \end{aligned} \tag{14}$$

In (14) the t_i and w_i are, of course, subject to the conditions imposed upon t and w in (13).

We consider two subcases.

Subcase A: $r = s-j+1$. We will show that $P_{n_0}(f) \neq P_{n_0}(g)$, where $n_0 = 2^m q_1^{a_1} \dots q_{j-1}^{a_{j-1}}$ ($n_0 = 2^m$, if $j = 1$).

Let $f_0 = x^{n_0} - a$, $g_0 = x^{n_0} - b$, and suppose that $P_{n_0}(f_0) = P_{n_0}(g_0)$. Then all of our previous considerations apply with n_0 for n, and we get for some t_0 with $0 < t_0 < n_0$, $(t_0, n_0) = 1$ that

$$ab^{t_0} = (2^{w_0} u_0)^{n_0/2} d_0^{n_0}.$$

Here $w_0 = 0$ or 1 except that $w_0 \neq 1$ for $m = 2$, and u_0 is an odd, positive, square-free divisor of n_0. From (13), since $n/2$ is a multiple of n/n_0, it follows that

$$ab^t = (d')^{n/n_0}.$$

Now determine an integer t' by the conditions

$$t' \equiv t_0 \pmod{n_0}, \quad t' \equiv t \pmod{n/n_0}, \quad 0 < t' < n.$$

Then it may be verified readily that

$$ab^{t'} = (2^{w_0}u_0)^{n/2}d^n.$$

Since $(t', n) = 1$, we have here a relation of the form (13) in which u has at most $j-1$ distinct primes as divisors. This is impossible by our definition of j.

Thus $P_{n_0}(f_0) \neq P_{n_0}(g_0)$. Then there exists a set of primes S having a positive upper Dirichlet density, such that for $p \in S$ we have

$$(n_0, p-1) = n_0, \tag{15}$$

with n_0 dividing exactly one of $\operatorname{ind} a$, $\operatorname{ind} b$. If also $(n, p-1) = n_0$, it would follow that $P_{n_0}(f) \neq P_{n_0}(g)$. We proceed to establish $(n, p-1) = n_0$.

For $p \in S$, the first relation in (14) yields the congruence

$$\operatorname{ind} a + t_1 \operatorname{ind} b \equiv \frac{n}{2} \operatorname{ind} u_1 q_j \pmod{n_0}, \tag{16}$$

since $\operatorname{ind} 2$ is even when $w_1 = 1$. Now $2 \nmid \operatorname{ind} u_1 q_j$. For otherwise, (16) would imply that both $\operatorname{ind} a$ and $\operatorname{ind} b$ are divisible by n_0. Thus $(u_1 q_j/p) = -1$. From (15), we have that $p \equiv 1 \pmod{q_l}$, $l = 1, 2, \ldots, j-1$, $p \equiv 1 \pmod 4$, and so

$$-1 = \left(\frac{u_1 q_j}{p}\right) = \left(\frac{p}{q_j}\right).$$

As a consequence, $p \not\equiv 1 \pmod{q_j}$. By using the other relations in (14), an identical conclusion is reached for each of $q_{j+1}, \ldots, q_s$. From these facts, we see that $(n, p-1) = n_0$, as was to be proved.

Subcase B: $1 \leqslant r \leqslant s-j$. If $r = s-j$, then the proof in Subcase A goes through but using $f_1 = x^{n_1} - a$, $g_1 = x^{n_1} - b$ with $n_1 = n_0 q_s^{w_s}$ in place of f_0, g_0. Here $P_{n_1}(f_1) = P_{n_1}(g_1)$ is impossible since we can deduce from it a relation of the form (13) with $u = u_1 q_s$, contrary to the maximality of r in (14).

Hence, suppose $1 \leqslant r \leqslant s-j-1$. Then there will be at least two primes in the set $S_1 = \{q_{j+r}, q_{j+r+1}, \ldots, q_s\}$. Now, consider all relations of the form (13) in which the prime factors of u belong to either S_1 or $S_2 = \{q_1, q_2, \ldots, q_{j-1}\}$. If any such relations exist, then, since u must have at least j prime factors, it follows from the maximality of r in (14) that u will have at least two prime factors from S_1. Write $u = u'u''$ where the prime factors of u' and u'' are in the sets S_1 and S_2 respectively, and form a set T consisting of all the distinct u''s which arise in this way. We note that T may be the null set.

Our goal is to study the set T in order to arrive at additional relations of the form (13) which are analogous to those given in (14). In so doing, it will be useful to think of a typical element u' of T as being a "combination" of its constituent prime factors, the latter being considered as the "objects" in the combination. To facilitate the use of this viewpoint, it will be convenient to simplify our notation and to denote $q_{j+r}, \ldots, q_s$ respectively by $1, 2, \ldots, l$ where $l = s-j-r+1$ so that $l \geqslant 2$. Then we may describe T as follows: T is a set of combinations without repetitions of the l objects $1, 2, \ldots, l$ taken at least two at a time.

Concerning T, we next state a purely combinatorial lemma which will enable us to complete the proof for this subcase. We use the term combination to mean combination without repetition.

LEMMA 6. *Let T be defined as above. Then there exists a combination $\sigma = \lambda_1 \lambda_2 \ldots \lambda_h$, $h \geqslant 1$, where the λ_i are chosen from $1, 2, \ldots, l$, having the following two properties:*

(a) *any combination of $\lambda_1, \ldots, \lambda_h$ taken v at a time, where $2 \leqslant v \leqslant h$, is not in T (in particular, $\sigma \notin T$);*

(b) *if λ' is any one of $1, 2, \ldots, l$ which is not a λ_i, $i = 1, 2, \ldots, h$, then there exists an element of T which is of the form $\lambda_{i_1}\lambda_{i_2}\ldots\lambda_{i_e}\lambda'$, $e \geqslant 1$.*

Assuming the truth of this lemma for the moment, let us proceed with our main argument. By re-indexing $q_{j+r}, \ldots, q_s$ if necessary, suppose that $q' = q_{j+r}q_{j+r+1}\cdots q_{j+r+h-1}$ is the product corresponding to the combination σ of Lemma 6. Observe, for later use, that λ' of property (b) will then correspond to any one of the primes $q_{j+r+h}, \ldots, q_s$.

Now consider

$$f' = x^{n'} - a, \quad g' = x^{n'} - b, \quad \text{where} \quad n' = 2^m q_1^{a_1} \ldots q_{j-1}^{a_{j-1}} q_{j+r}^{a_{j+r}} \ldots q_{j+r+h-1}^{a_{j+r+h-1}}.$$

We assert that $P_{n'}(f') \neq P_{n'}(g')$. For, suppose that $P_{n'}(f') = P_{n'}(g')$. Then, by the procedure of Subcase A, we construct a relation of the form (13) where u is a divisor of n'. In particular, some divisor q'' of q' having at least two prime factors will be a factor of u; that is to say, $q'' \in T$. By property (a) of Lemma 6, this is impossible, and our assertion is established. Thus, there exists a set of primes S having positive upper Dirichlet density such that for $p \in S$, $(n', p-1) = n'$, and n' divides exactly one of $\operatorname{ind} a$, $\operatorname{ind} b$. To complete our proof, we will show that also $(n, p-1) = n'$, since this means that $P_{n'}(f) \neq P_{n'}(g)$.

The fact that $p \not\equiv 1 \pmod q$ for $q = q_j, q_{j+1}, \ldots, q_{j+r-1}$, is obtained exactly as in Subcase A. If $h = l = s-j-r+1$, that is, if T is the null set, then we are finished. Otherwise, we must show that this same congruential property holds also for $q = q_{j+r+h}, q_{j+r+h+1}, \ldots, q_s$. For each such prime q, property (b) of Lemma 6 insures the existence of a relation

$$ab^t = (2^w u_0' u_0'' q)^{n/2} d^n$$

as in (13), where the prime factors of u_0' and u_0'' are in the sets $S_3 = \{q_{j+r}, q_{j+r+1}, \ldots, q_{j+r+h-1}\}$ and S_2 respectively. Since each prime

in S_2 and S_3 divides $p-1$, we have here the same situation as in the proof of Subcase A, and we conclude, as before, that $(p/q) = -1$, so that $p \not\equiv 1 \pmod q$.

There remains the

Proof of Lemma 6. We construct σ by the following sieve-like algorithm which yields a σ with $\lambda_1 = 1$. Consider the pairs 1λ where λ ranges successively over $2, 3, \ldots, l$. Either all of these pairs are in T, in which case take $\sigma = 1$; or there is a first pair $1\lambda_2$ which is not in T. In the latter case, consider next the triples $1\lambda_2\lambda$ where λ ranges successively over $\lambda_2+1, \lambda_2+2, \ldots, l$. Determine, if it exists, the first λ say $\lambda = \lambda_3$ for which none of $1\lambda, \lambda_2\lambda, 1\lambda_2\lambda$ is in T (these are all of the combinations of $1, \lambda_2, \lambda$ involving λ, taken at least two at a time). If no such λ exists, then take $\sigma = 1\lambda_2$. Otherwise, consider the quadruples $1\lambda_2\lambda_3\lambda$ where λ ranges over $\lambda_3+1, \lambda_3+2, \ldots, l$. We continue in this fashion, stopping whenever there is no choice for λ, and going on to the next higher combination when there is. Eventually the process ends and it is clear that the resulting σ will satisfy property (a) of the lemma. But also (b) holds. For, if λ' is not one of the λ's in σ, then, for some i, $\lambda_i < \lambda' < \lambda_{i+1}$ (if $i = h$, omit the second inequality). But, in view of our algorithm, this means that some combination of $1, \lambda_2, \ldots, \lambda_i, \lambda'$ taken at least two at a time and involving λ' is in T. This is (b). If T is the null set, note that we get $\sigma = 123\ldots l$.

Remark. Theorem 1 and its Corollary are so similar in appearance that one is led naturally to consider the possibility of deriving the Theorem from the Corollary. In fact, we can do this when $n = 2$. In this case, assuming $p \nmid ab$, $P(f) = P(g)$ implies that $(a/p) = (b/p) = 1$ for $p \in P_1$, where P_1 is $P(f) \cap P(g)$. Also $(a/p) = (b/p) = -1$ for $p \in P_2$, where P_2 is $P - (P(f) \cup P(g))$. Since $P_1 \cup P_2 = P$, $(ab/p) = 1$ for almost all primes p and our result follows via the Corollary.

For $n > 2$, this approach would require that we establish certain properties of the higher reciprocity symbols. Though the nature of these properties can be inferred explicitly from Theorem 1, they appear recondite at the moment and so we leave this matter open for the time being.

4. The Kronecker conjecture. In this section we consider only non-constant polynomials with rational integer coefficients which are irreducible over Q. Two such polynomials $h_1(x)$ and $h_2(x)$ will be called *equivalent* — in symbols $h_1 \sim h_2$ — if $h_1(\alpha) = 0$ and $h_2(\beta) = 0$ where α and β are both primitive elements of the same algebraic number field K. Equivalent polynomials are of the same degree and determine the same set of simple field extensions over Q.

Now, it is well-known that if $h_1(x) \sim h_2(x)$ then $P(h_1) = P(h_2)$, [5].

More precisely, if $\deg h_1 = \deg h_2 = n$, then $P_i(h_1) = P_i(h_2)$ for $i = 1, 2, \ldots, n$. In fact, $P_i(h_1)$ and $P_i(h_2)$ differ only in a finite number of primes.

It was conjectured by Kronecker [10] that the converse proposition is also true; that is, $P_i(h_1) = P_i(h_2)$, $i = 1, 2, \ldots, n$, implies that $h_1(x) \sim h_2(x)$. The Kronecker conjecture is not true in general as was shown by Gassmann [7] in 1926. He proved the existence of two inequivalent polynomials of degree 180 which not only satisfy the required conditions but also factor in the same way modulo p for all except a finite number of primes p. (See also Schinzel [13] who gives a cubic h with $P(h) = P(h_1)$, $h_1 = h(x^5)$.) Nevertheless, it is of interest to determine under what conditions the Kronecker conjecture will hold for specific classes of polynomials. In this section, as an application of our previous results, we carry out this investigation for the class of monic binomials(1).

Let f and g have their previous meanings, except that now a and b are integers for which f and g are irreducible over Q (cf. § 2). As a consequence, we note that $\zeta_n^r \sqrt[n]{a}$, $r = 0, 1, \ldots, n-1$ will be a complete set of conjugates for $\sqrt[n]{a}$ over Q, with similar results for $\sqrt[n]{b}$. We assume that the conditions $P_i(f) = P_i(g)$, $i = 1, 2, \ldots, n$, hold. For binomials, as we have shown, these n conditions are equivalent to the single condition $P(f) = P(g)$ and thus we need refer only to the latter in discussing the Kronecker conjecture for f and g. The case $n = 1$ being trivial, we take $n \geqslant 2$.

By Theorem 1, at least one of the conditions (i) and (ii) must hold, the latter, of course, only if $8 \mid n$. For convenience, we list these again: (i) $ab^t = d^n$, (ii) $ab^t = 2^{n/2} d^n$. Our problem, therefore, is reduced to the determination of exactly when (i) or (ii) implies $f \sim g$. The results are embodied in the next three theorems and state that, apart from one exceptional case, the Kronecker conjecture is true if and only if condition (i) holds.

THEOREM 3. *Let $n = 2^m k$, with $0 \leqslant m \leqslant 2$ and k odd. Then $P(f) = P(g)$ implies $f \sim g$.*

Proof. For these values of n, only (i) can hold. Let $\theta = \sqrt[n]{a}$, $\varphi = \sqrt[n]{b}$. By taking nth roots in (i) we find that $\theta\varphi^t = d\zeta_n^r$, where r is some integer. Write $\theta_1 = \theta\zeta_n^{-r}$. Then θ_1 is a root of f, and $\theta_1 = d/\varphi^t \in Q(\varphi)$. Since both θ_1 and φ are of degree n over Q we must have $Q(\theta_1) = Q(\varphi)$ and so $f \sim g$. The proof is complete.

Before proceeding to consider the remaining values of n, we note that when n is even, then both (i) and (ii) imply that $ab > 0$. It is con-

(1) The case of a binomial with leading coefficient different from 1 is easily reduced to the monic case, but we do not stop to do this here.

venient to treat separately cases corresponding to the possible signs of a and b.

THEOREM 4. *Let $n = 2^m k$, $m \geqslant 3$, k odd, and let $a > 0$, $b > 0$. Then $P(f) = P(g)$ implies $f \sim g$ if and only if condition* (i) *holds.*

Proof. That (i) implies $f \sim g$, has been proved in Theorem 3. Hence suppose (ii) holds but not (i). Suppose also that $f \sim g$. We will show this assumption leads to a contradiction.

Let $\theta = \sqrt[n]{a}$, $\varphi = \sqrt[n]{b}$, where now the real, positive values of the radicals are meant. Taking nth roots in (ii), we get

$$\theta\varphi^t = d\sqrt{2}, \quad d > 0. \tag{17}$$

Since $\pm\theta$, $\pm\varphi$ respectively, are the only real roots of f and g respectively, we must have $Q(\theta) = Q(\varphi)$. It follows from (17) that $\sqrt{2} \in Q(\varphi)$. Thus φ is of degree $n/2$ over $Q(\sqrt{2})$. Now, if $N(\ )$ denotes the norm with respect to $Q(\sqrt{2})$, we find that $N(\varphi) = \zeta_n^r\sqrt{b}$ for some integer r. Since $N(\varphi) \in Q(\sqrt{2})$, we infer that ζ_n^r must be real and hence equal to ± 1. Then $\sqrt{b} \in Q(\sqrt{2})$, which means that

$$b = 2d_1^2. \tag{18}$$

Now, for the t of condition (ii), let $t_1 = t + n/2$ if $t < n/2$, and $t_1 = t - n/2$ if $t > n/2$. Then, using (ii) and (18), we find in the respective cases that

$$ab^{t_1} = \begin{cases} (2d_1 d)^n & (t < n/2); \\ (d/d_1)^n = d_2^n & (t > n/2). \end{cases}$$

Since $(t_1, n) = 1$ and $0 < t_1 < n$, we have here, in each case, a relation of the form (i), contrary to our hypothesis. The proof is now complete.

The remaining case to be considered is preceded by the following:

LEMMA 7. *Let e be a positive integer which is not a square, and let ϱ be a root of unity. Further, let $\beta = \varrho\sqrt{e}$ be of degree 2 over Q. Then one of the following cases must occur:*

(a) $\beta = \pm\sqrt{e}$;

(b) $\beta = \pm\sqrt{-e}$;

(c) $e = 2d^2$, $\beta = \pm(1 \pm i)d \quad (i = \sqrt{-1})$;

(d) $e = 3d^2$, $\beta = \pm(3 \pm i\sqrt{3})d/2$.

Proof. The hypothesis implies that ϱ^2 is a root of unity which is of degree 1 or 2 over Q, and so it is one of ± 1, $\pm i$, $\pm\zeta_3$, $\pm\zeta_3^2$. The lemma now follows in a straightforward manner and we leave the details to the reader.

THEOREM 5. *Let $n = 2^m k$, $m \geqslant 3$, k odd, and let $a < 0$, $b < 0$. Then $P(f) = P(g)$ implies $f \sim g$ if and only if either* (a) *condition* (i) *holds, or* (b) *condition* (ii) *holds and $a = -d_1^2$, $b = -d_2^2$ for some integers d_1 and d_2.*

Proof. When (a) holds, then $f \sim g$ follows as before. Hence let (b) hold and suppose, as we may, that $d_1 > 0$, $d_2 > 0$. For the t of condition (ii), choose r_1 such that $r_1 + t \equiv n/4 \pmod{2n}$. Note that r_1 will be odd. Now let $\theta = \zeta_{2n}^{r_1}(d_1)^{2/n}$, $\varphi = \zeta_{2n}(d_2)^{2/n}$, where the real, positive values of the radicals are taken. It is easily verified that θ and φ are roots of f and g respectively. To prove that $f \sim g$, it suffices to show that $\theta \in Q(\varphi)$.

From (ii), we have that

$$\theta\varphi^t = d\zeta_n^v\sqrt{2}, \tag{19}$$

where v is an integer with $0 \leqslant v < n$, and $d > 0$. But also

$$\theta\varphi^t = \zeta_n^{n/8}(d_1 d_2^t)^{n/2}.$$

A comparison of this equation and (19) shows that $\zeta_n^{(v-n/8)} > 0$, from which $v = n/8$ results. Thus, (19) becomes

$$\theta\varphi^t = d\zeta_8\sqrt{2}. \tag{20}$$

Next, observe that $\zeta_8\sqrt{2} \in Q(i)$ since $\zeta_8 = (1+i)/\sqrt{2}$. But also $Q(i) \subset Q(\varphi)$, in view of $\varphi^{n/2} = d_2 i$. We conclude from (20) that $\theta \in Q(\varphi)$, and the sufficiency of (b) is established.

We are left with the case when (ii) holds but not (i), and not both a and b are negatives of squares, say $b \neq -d_2^2$. We will assume again that $f \sim g$ and show this leads to a contradiction.

Let $b_1 = -b$. This time, we take as a root of g the quantity $\varphi = \zeta_{2n}\sqrt[n]{b_1}$, where the real, positive value of the radical is meant. By our assumption, there exists a root θ of f for which $Q(\theta) = Q(\varphi)$. For these values of θ and φ, (ii) again yields a relation (19).

Write $\alpha = \zeta_n^v\sqrt{2}$, and let $\deg\alpha = l$. Then, since $\sqrt{2} \in Q_8$, $\alpha \in Q_n$. Also from (19), $\alpha \in Q(\varphi)$, and so $l \mid n$, and φ is of degree n/l over $Q(\alpha)$. If $N_\alpha(\ )$ denotes the norm with respect to $Q(\alpha)$, we have, for some integer v_1, that $N_\alpha(\varphi) = \zeta_{2n}^{v_1}\sqrt[l]{b_1} \in Q(\alpha)$. We conclude that $\sqrt[l]{b_1} \in Q_{2n}$, and then, by a familiar argument, that $Q(\sqrt[l]{b_1})$ is normal over Q.

In view of both the irreducibility of $x^n + b_1$ over Q and the fact that $b_1 \neq d_2^2$, we infer from the criteria given in § 2, that also $x^l - b_1$ is irreducible over Q, that is, $\sqrt[l]{b_1}$ is of degree l. But then by Lemma 3(a) we must have $l = 2$, since clearly $l > 1$. Thus α is quadratic over Q.

We now apply Lemma 7 to α. Since $e = 2$ here, we find that $Q(\alpha)$ is one of the fields $Q(\sqrt{2})$, $Q(\sqrt{-2})$, $Q(i)$. Next, apply Lemma 7 to $\beta = \zeta_{2n}^{v_1}\sqrt{b_1}$ which we know to be in $Q(\alpha)$ and which is of degree 2 over Q, since $b_1 \neq d_2^2$. Then, by examining the values of β which must occur, we see that $b_1 = 2d^2$ is the only possible condition which is compatible with $\beta \in Q(\alpha)$. But then, exactly as in Theorem 4, we get the contradiction that also condition (i) can be shown to hold.

EXAMPLE. By means of Theorems 4 and 5, it is easy to construct examples of polynomials f and g for which the Kronecker conjecture is false. These must necessarily be of degree not less than 8, but this minimal degree is easily attained. Consider the pair $f = x^8 - 3\cdot 2^4$, $g = x^8 - 3^7$, where both f and g are irreducible since neither a nor b is a square. It is easily verified that condition (ii) holds with $t = 1$, but that condition (i) does not hold for $t = 3, 5, 7$. Thus $P(f) = P(g)$, but f and g are not equivalent by Theorem 4. Moreover, as Professor A. Schinzel has indicated to me, the binomials f and g have the Gassmann property of factoring in the same way modulo p for all but a finite number of primes. Or, equivalently, if $K = Q(\sqrt[8]{3\cdot 2^4})$ and $L = Q(\sqrt[8]{3^7})$ are simple extension fields determined by f and g respectively, then K and L are non-conjugate and $P_A(K) = P_A(L)$ for every A, where $P_A(K)$ denotes the set of those rational primes which decompose into prime ideals in K in a prescribed way A. Since K and L (and other fields like them of degree 8 determined by using Theorems 4 and 5) thus furnish the simplest known examples of fields having this property, it is of interest to sketch a proof.

We apply the following theorem of Gassmann ([7], [9]) where it is understood that the ground field is Q.

If K and L are algebraic number fields then the following conditions are equivalent:

(a) $P_A(K) = P_A(L)$ *for every* A.

(b) *K and L determine the same normal field N, and if G, G_1 and G_2 denote respectively the Galois group of N and the subgroups belonging to K and L, then for every conjugacy class C of G, $G_1 \cap C$ and $G_2 \cap C$ have the same number of elements.*

In the present case, the normal fields of K and L are the splitting fields of f and g respectively. Since $P_8(f) = P_8(g)$, it follows from Lemmas 1 and 2 that K and L have the same normal field, say N. As $N = Q_8(\sqrt[8]{3\cdot 2^4})$, and as it is readily established that f remains irreducible over Q_8, the Galois group G of N is of order 32. Then, using known results on the groups of binomial equations, (cf. [16], v. 1, p. 180) it follows that G is isomorphic to the group of linear substitutions $x' = cx + d$ modulo 8,

where $c = 1, 3, 5, 7$ and $d = 0, 1, \ldots, 7$. The subgroups G_1 and G_2 belonging to K and L respectively may be found in the usual way and we get $G_1 = \{x, 3x, 5x, 7x\}$, $G_2 = \{x, 3x+4, 5x+4, 7x\}$. It is now a straightforward computation to determine the conjugacy classes C_i of G and to verify that, indeed, $G_1 \cap C_i$ and $G_2 \cap C_i$, for each i, have the same number of elements.

We close this section with a result that follows from our Theorems 3–5 and which we have not seen elsewhere.

THEOREM 6. *For irreducible polynomials f and g, we have $f \sim g$, if and only if either* (a) $ab^t = d^n$ *or, if* $8 \mid n$, (b) $ab^t = 2^{n/2}d^n$ *with* $a = -d_1^2$, $b = -d_2^2$. *Here t is an integer with* $0 < t < n$, $(t, n) = 1$.

References

[1] N. C. Ankeny and C. A. Rogers, *A conjecture of Chowla*, Ann. of Math. 53 (1951), pp. 541–550.

[2] M. Bauer, *Über einen Satz von Kronecker*, Archiv der Math. und Physik, Bd. 6, pp. 218–219.

[3] — *Zur Theorie der algebraischen Zahlkörper*, Math. Ann. 77 (1916), pp. 353–356.

[4] A. Capelli, *Sulla riducibilità dell equazioni algebriche*, Rendiconti Napoli 1897/98.

[5] R. Dedekind, *Über den Zusammenhang zwischen der Theorie der Ideale und der Höheren Kongruenzen*, Göttinger Ahhandl., 23 (1878), pp. 3–37.

[6] H. Flanders, *Generalization of a theorem of Ankeny and Rogers*, Ann. of Math. 57 (1953), pp. 392–400.

[7] F. Gassmann, *Bemerkungen zur vorstehenden Arbeit von Hurwitz*, Math. Zeitschr. 25 (1926), pp. 665–675.

[8] M. Hall, *Quadratic residues in factorization*, Bull. Amer. Math. Soc. 39 (1933), pp. 758–764.

[9] H. Hasse, *Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper*, 2nd ed., vol. 2, Würzburg 1965, pp. 138–146.

[10] L. Kronecker, *Über die Irreducibilität von Gleichungen*, Monatsbericht, Akademie der Wissen., 1880, pp. 155–163.

[11] W. J. LeVeque, *Topics in Number Theory*, vol. 1, Reading, Mass., 1956, pp. 74–77.

[12] H. B. Mann, *Introduction to Algebraic Number Theory*, Columbus, Ohio, 1955, pp. 145–158.

[13] A. Schinzel, *On a theorem of Bauer and some of its applications*, Acta Arith. 11 (1966), pp. 333–344.

[14] E. Trost, *Zur Theorie der Potenzreste*, Nieuw Arch. Wiskunde, 18 (1934), pp. 58–61.

[15] K. Th. Vahlen, *Über Reductible Binome*, Acta Math. 19 (1895), pp. 195–198.

[16] B. L. van der Waerden, *Moderne Algebra*, New York 1943.

[17] H. Weber, *Lehrbuch der Algebra*, 2nd ed., vol. 2, New York 1961, pp. 69–100.

Received on 17. 5. 1969