

the conclusion follows from (22), (23) and the multiplicative property of the norm.

Remark. In connection with Theorem 5 let us remark that the theorem of Bauer gives an answer to a question of D. H. Lehmer ([6], p. 436) concerning possible types of homogeneous polynomials  $F(x, y)$  of degree  $\frac{1}{2}\varphi(n)$  such that when  $(x, y) = 1$ , the prime factors of  $F(x, y)$  either divide  $n$  or are of the form  $nk \pm 1$ . (If  $f(x) = x^3 + x^2 - 2x - 1$ , then  $y^3 f(x/y)$  is an example of such polynomial for  $n = 7$ .) The answer is that

all such polynomials must be of the form  $A \prod_{i=1}^{\frac{1}{2}\varphi(n)} (x - a_i y)$ , where  $a_i$  runs through all conjugates of a primitive element of the field  $Q\left(2 \cos \frac{2}{n} \pi\right)$  and  $A$  is a rational integer.

Note added in proof. In connection with Theorem 2 a question arises whether solvable fields of degree  $p^2$  ( $p$  prime) are Bauerman. J. L. Alperin has proved that the answer is positive if the field is primitive and  $p > 3$ . P. Roquette has found a proof for the case where the Galois group of the normal closure is a  $p$ -group (oral communication).

#### References

- [1] M. Bauer, *Zur Theorie der algebraischen Zahlkörper*, Math. Ann. 77 (1916), pp. 353-356.
- [2] H. Davenport, D. J. Lewis and A. Schinzel, *Polynomials of certain special types*, Acta Arith. 9 (1964), pp. 107-116.
- [3] F. Gassmann, *Bemerkungen zu der vorstehenden Arbeit von Hurwitz*, Math. Zeitschr. 25 (1926), pp. 665-675.
- [4] M. Hall, *The Theory of Groups*, New York 1959.
- [5] H. Hasse, *Bericht über neuere Untersuchungen und Probleme aus der Theorie der Algebraischen Zahlkörper II*, Jahresber. der Deutschen Math. Vereinigung, 6 (1930).
- [6] D. H. Lehmer, *An extended theory of Lucas functions*, Ann. of Math. 31 (1930), pp. 419-448.
- [7] N. Tschebotarow und H. Schwerdtfeger, *Grundzüge der Galoisschen Theorie*, Groningen, Djakarta 1950.
- [8] H. Wielandt, *Finite Permutation Groups*, New York, London 1964.

Reçu par la Rédaction le 12. 3. 1965

## An extension of the theorem of Bauer and polynomials of certain special types

by

D. J. LEWIS\* (Ann Arbor, Mich.), A. SCHINZEL (Warszawa)  
and H. ZASSENHAUS (Columbus, Ohio)

1. For a given algebraic number field  $K$  let us denote by  $P(K)$  the set of those rational primes which have a prime ideal factor of the first degree in  $K$ . M. Bauer [1] proved in 1916 the following theorem:

If  $K$  is normal, then  $P(\Omega) \subset P(K)$  implies  $\Omega \supset K$ . (The converse implication is immediate).

In this theorem, inclusion  $P(\Omega) \subset P(K)$  can be replaced by a weaker assumption that the set of primes  $P(\Omega) - P(K)$  is finite, which following Hasse we shall denote by  $P(\Omega) \leq P(K)$ .

In the preceding paper [8], one of us has characterized all the fields  $K$  for which  $P(\Omega) \leq P(K)$  implies that  $\Omega$  contains one of the conjugates of  $K$  and has called such fields *Bauerian*. The characterization is in terms of the Galois group of the normal closure  $\bar{K}$  of  $K$  and is not quite explicit. Examples of non-normal Bauerian fields given in that paper are the following: fields  $K$  such that  $\bar{K}$  is solvable and  $\left(\frac{|\bar{K}|}{|K|}, |K|\right) = 1$ <sup>(1)</sup>, fields of degree 4. The aim of the present paper is to exhibit a class of Bauerian fields that contains all normal and some non-normal fields. We say that a field  $K$  has property (N) if there exists a normal field  $L$  of degree relatively prime to the degree of  $K$  such that the composition  $KL$  is the normal closure of  $K$ . We have

**THEOREM 1.** *If  $K$  and  $\Omega$  are algebraic number fields and  $K$  has property (N) then  $P(\Omega) \leq P(K)$  implies that  $\Omega$  contains one of the conjugates of  $K$ .*

\* This paper was written while the first author received support from the National Science Foundation.

<sup>(1)</sup> We let  $(\cdot, \cdot)$  denote both the degree of the field over  $Q$  and the order of the group.



Not all fields  $K$  such that  $\bar{K}$  is solvable and  $\left(\frac{|\bar{K}|}{|K|}, |K|\right) = 1$  possess property (N). We have however

**THEOREM 2.** *If  $K$  is a number field such that  $\left(\frac{|\bar{K}|}{|K|}, |K|\right) = 1$  and the Galois group of  $\bar{K}$  is supersolvable, then  $K$  has property (N).*

In particular  $K$  can be any field of prime degree such that  $\bar{K}$  is solvable or any field generated by  $\sqrt[n]{a}$ , where  $a, n$  are rational integers and  $(n, \varphi(n)) = 1$ . The field  $Q(\sqrt[6]{2})$  does not possess property (N), it is however Bauerian. (It follows from a theorem of Flanders (cf. [7], Th. 167) and results of the preceding paper that  $Q(\sqrt[n]{a})$  is Bauerian if  $n \neq 0 \pmod{8}$ .) We have no example of non-normal field  $K$  with property (N), such that  $\bar{K}$  is non-solvable however one could construct such a field provided there are fields corresponding to every Galois group.

The original Bauer's theorem has been applied in [2] to characterize polynomials  $f(x)$  with the property that in every arithmetical progression there is an integer  $x$  such that  $f(x)$  is a norm of an element of a given normal field  $K$ . The method used in [2] can be modified in order to obtain

**THEOREM 3.** *Let  $K$  be a field having property (N) and let  $N_{K/Q}(\omega)$  denote the norm from  $K$  to the rational field  $Q$ . Let  $f(x)$  be a polynomial over  $Q$  such that the multiplicity of each zero of  $f(x)$  is relatively prime to  $|K|$ . If in every arithmetical progression there is an integer  $x$  such that*

$$f(x) = N_{K/Q}(\omega) \quad \text{for some } \omega \in K,$$

then

$$f(x) = N_{K/Q}(\omega(x)) \quad \text{for some } \omega(x) \in K[x].$$

The proofs of Theorems 1-3 given in § 3 are independent of the preceding paper [8] and assume only the original Bauer's theorem. They are preceded in § 2 by some lemmata of seemingly independent interest. Theorems 1 and 3 could be proved by the methods and results of [8]. We retain the present proofs since they use, as do the statements of the theorems, only the language of field theory. We refer to [8] for examples showing that an extension of the theorems to an arbitrary field  $K$  is impossible.

**2. LEMMA 1.** *Let fields  $K$  and  $L$  have the following properties:  $L$  is normal,  $(\text{degree } K, \text{degree } L) = 1$ ,  $KL$  is normal. Then for any field  $\Omega$  the inclusion*

$$(1) \quad \Omega L \supset KL$$

implies that  $\Omega$  contains one of the conjugates of  $K$ .

*Proof.* It follows from (1) that

$$(2) \quad \Omega KL = \Omega L.$$

Since  $KL$  is normal and  $L$  is normal, we have

$$(3) \quad |\Omega KL| = \frac{|\Omega| |KL|}{|\Omega \cap KL|},$$

$$(4) \quad |\Omega L| = \frac{|\Omega| |L|}{|\Omega \cap L|}.$$

(Cf. [6], § 19.5, Satz 1).

Since clearly  $|KL| = |K| |L|$ , we get from (2), (3) and (4)

$$(5) \quad |\Omega \cap KL| = |K| |\Omega \cap L|.$$

Let  $\mathfrak{G}$  be the Galois group of  $KL$ . And let  $\mathfrak{H}, \mathfrak{I}, \mathfrak{N}$  be subgroups of  $\mathfrak{G}$  corresponding to  $K, \Omega \cap KL$  and  $L$ , respectively.

In view of (5)

$$[\mathfrak{G} : \mathfrak{H}][\mathfrak{G} : \mathfrak{I}], \quad \text{thus } |\mathfrak{I}||\mathfrak{H}| \quad \text{and} \quad (|\mathfrak{I}|, |\mathfrak{N}|) = 1.$$

On the other hand, since  $\mathfrak{H}\mathfrak{N} = \mathfrak{G}$ , and  $\mathfrak{N}$  is normal, it can be easily shown that

$$\mathfrak{I}\mathfrak{N} = (\mathfrak{I}\mathfrak{N} \cap \mathfrak{H})\mathfrak{N}.$$

Thus  $\mathfrak{I}$  and  $\mathfrak{I}\mathfrak{N} \cap \mathfrak{H}$  are two representative subgroups of  $\mathfrak{I}\mathfrak{N}$  over  $\mathfrak{N}$  and by Theorem 27 ([9], Chapter IV) they are conjugate. The theorem in question had been deduced from the conjecture now proven [3] that all groups of odd orders are solvable. It follows that  $\mathfrak{I}$  is contained in a certain conjugate of  $\mathfrak{H}$ , thus  $\Omega \cap KL$  contains a suitable conjugate of  $K$  and the same applies to  $\Omega$ , q. e. d.

The first two assumptions of Lemma 1 are necessary as shown by the following examples

1.  $K = Q(e^{2\pi i/3}), L = Q(\sqrt[3]{2}), \Omega = Q(e^{2\pi i/3}\sqrt[3]{2})^2,$
2.  $K = Q(i), L = Q(\sqrt{2}), \Omega = Q(\sqrt{-2}).$

As to the third assumption, namely that  $KL$  is normal, we can show that it is necessary provided that there exists a field with Galois group  $\mathfrak{G}$ , where  $\mathfrak{G}$  is the wreath product of  $\mathfrak{S}_4$  acting on 4 isomorphic copies of the simple group  $\mathfrak{G}_{168}$ . Then in the counterexample,  $K$  is a field of degree  $7^4$  corresponding to the wreath product of  $\mathfrak{S}_4$  acting on 4 isomorphic copies of a subgroup  $\mathfrak{H}$  of  $\mathfrak{G}_{168}$  of index 7,  $L$  is a normal field of degree 24 corresponding to the product of 4 copies of  $\mathfrak{G}_{168}$ . The construction of  $\Omega$

(\*) We owe this example to Mr. Surinder Sehgal.

and the proof that it furnishes a counterexample is complicated and will be omitted.

LEMMA 2. *In any supersolvable group  $\mathcal{G}$  for each set  $\Pi$  of primes either there is a normal  $\Pi$ -subgroup  $\neq 1$  or there is a normal Hall<sup>(\*)</sup>  $\hat{\Pi}$ -group  $\neq 1$  ( $\hat{\Pi}$  is the set of all prime divisors of  $|\mathcal{G}|$  not contained in  $\Pi$ ).*

Proof. If this lemma would be false, then there would be a supersolvable group  $\mathcal{G} \neq 1$  of minimal order for which it would be false.

If  $\Pi$  or  $\hat{\Pi}$  are empty then the statement is trivial. Let  $\Pi$  and  $\hat{\Pi}$  be non-empty. Since  $\mathcal{G} \neq 1$ , there is a maximal normal subgroup  $\mathfrak{M} \neq \mathcal{G}$ . Since  $\mathcal{G}$  is solvable  $[\mathcal{G} : \mathfrak{M}]$  is a prime  $p$ . If  $\mathfrak{M}$  contains a normal  $\Pi$ -subgroup  $\mathfrak{N} \neq 1$ , then  $\langle \mathfrak{N}^{\mathcal{G}} \rangle$  is a normal  $\Pi$ -subgroup  $\neq 1$  of  $\mathcal{G}$ , a contradiction. Hence  $\mathfrak{M}$  contains no normal  $\Pi$ -subgroup. Since  $\mathfrak{M}$ , a subgroup of a supersolvable group, itself is supersolvable, it follows from the minimal property of  $\mathcal{G}$  that  $\mathfrak{M}$  contains a normal Hall  $\hat{\Pi}$ -group  $\mathfrak{S}$ . A normal Hall subgroup of a solvable group is the unique subgroup of its order (cf. [4], Th. 9.3.1). Therefore  $\mathfrak{S}$  must be a characteristic subgroup of  $\mathfrak{M}$  and hence a normal subgroup of  $\mathcal{G}$ . If  $p \in \Pi$  then  $\mathfrak{S}$  is normal Hall  $\hat{\Pi}$ -group of  $\mathcal{G}$ , a contradiction. Hence  $p \in \hat{\Pi}$ . It follows that

(6) *the index of every maximal normal subgroup of  $\mathcal{G}$  is a prime number belonging to  $\hat{\Pi}$ .*

Now let  $\mathfrak{N} \neq 1$  be a minimal normal subgroup of  $\mathcal{G}$ . Since  $\mathcal{G}$  is supersolvable, it follows that  $\mathfrak{N}$  is of prime order, say  $q$ . Since we have assumed  $\mathcal{G}$  does not have a normal  $\Pi$ -subgroup,  $q \in \hat{\Pi}$ . Suppose  $\mathcal{G}/\mathfrak{N}$  contains a normal  $\Pi$ -subgroup  $\mathfrak{H}/\mathfrak{N} \neq 1$ . Since  $\mathfrak{H}$  is solvable it contains a  $q$ -complement  $\mathfrak{S} \neq 1$ . The group  $\mathfrak{S}$  is a Hall  $\Pi$ -subgroup of  $\mathfrak{H}$ . If  $\mathfrak{S}$  is normal in  $\mathfrak{H}$ , it follows (cf. [4], Th. 9.3.1) that  $\mathfrak{S}$  is a characteristic subgroup of  $\mathfrak{H}$  and hence  $\mathfrak{S} \neq 1$  would be a normal  $\Pi$ -subgroup of  $\mathcal{G}$  contrary to hypothesis. It follows that  $\mathfrak{S}$  is not normal in  $\mathfrak{H}$ . In particular  $\mathfrak{S}$  does not commute elementwise with  $\mathfrak{N}$ . Thus  $\mathfrak{S}$  is not contained in  $\mathfrak{Z}_{\mathfrak{H}}$  the centralizer of  $\mathfrak{N}$ .

The group  $\mathfrak{Z}_{\mathfrak{H}}$  is normal in  $\mathcal{G}$ . It follows that the index  $[\mathcal{G} : \mathfrak{Z}_{\mathfrak{H}}]$  is divisible by a prime  $r \in \Pi$ .

On the other hand, the factor group of the normalizer over the centralizer satisfies

$$\mathfrak{N}_{\mathfrak{H}}/\mathfrak{Z}_{\mathfrak{H}} \cong \mathcal{G}/\mathfrak{Z}_{\mathfrak{H}}$$

so that it is isomorphic to a subgroup of the automorphism group of the cyclic group  $\mathfrak{N}$ . Hence  $\mathcal{G}/\mathfrak{Z}_{\mathfrak{H}}$  is abelian and therefore contains a normal subgroup  $\mathfrak{M}_1/\mathfrak{Z}_{\mathfrak{H}}$  of index  $r$ . Hence  $\mathcal{G}$  contains a maximal normal subgroup

(\*) A Hall subgroup is a subgroup whose order and index are relatively prime.

$\mathfrak{M}_1$ , of prime index  $r$ , where  $r \in \Pi$ , contrary to (6). It follows that  $\mathcal{G}/\mathfrak{N}$  does not contain a nontrivial normal  $\Pi$ -subgroup.

Since  $\mathcal{G}/\mathfrak{N}$  is also supersolvable, it follows from the minimal property of  $\mathcal{G}$  that  $\mathcal{G}/\mathfrak{N}$  contains a normal Hall  $\hat{\Pi}$ -subgroup, say  $\mathfrak{H}/\mathfrak{N}$ . But then  $\mathfrak{H}$  is a normal Hall  $\hat{\Pi}$ -subgroup of  $\mathcal{G}$ , contrary to hypothesis.

Not all solvable groups possess the property enunciated in the lemma, e.g.  $\mathcal{G}_4$ . On the other hand groups possessing this property need not be solvable, e.g. the direct product of  $\mathcal{U}_5$  and  $\mathcal{Z}_{30}$ . We have not found another well known class of finite groups which possess the property besides supersolvable groups.

LEMMA 3. *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*

$$G(x) = aN_{J/Q}(H(x))$$

identically, where  $H(x)$  is a polynomial over  $J$ .

Proof: See [2], Lemma 2.

3. Proof of Theorem 1. Let  $L$  be a normal field such that  $(|K|, |L|) = 1$  and  $KL = \bar{K}$ . Assume that  $P(\Omega) \leq P(K)$ . We have

$$(7) \quad P(\Omega L) \subset P(\Omega) \cap P(L) \leq P(K) \cap P(L).$$

Let  $q$  be a large prime,  $q \in P(K) \cap P(L)$  and let

$$q = q_1 q_2 \dots q_r$$

be its factorization in  $\bar{K}$ . Since  $\bar{K}$  is normal we have

$$N_{\bar{K}/Q}(q_i) = q^{i|\bar{K}|/q}$$

Now, let  $\mathfrak{p}$  be the prime ideal factor of  $q$  of degree 1 in  $L$ . We have

$$(8) \quad N_{\bar{K}/Q}\mathfrak{p} = N_{L/Q}N_{KL/L}\mathfrak{p} = q^{|\bar{K}|}.$$

On the other hand,

$$\mathfrak{p} = q_{i_1} q_{i_2} \dots q_{i_s},$$

whence

$$(9) \quad N_{\bar{K}/Q}\mathfrak{p} = \prod_{j=1}^s N_{\bar{K}/Q} q_{i_j} = q^{i|\bar{K}|/q}.$$

It follows from (8) and (9) that

$$|K| = \frac{|\bar{K}|}{g} s = \frac{|K| |L|}{g} s;$$

hence

$$(10) \quad |L| |g|.$$

In this proof that fact that  $L$  is normal has not been used, thus by symmetry

$$|K||g.$$

Since  $(|K|, |L|) = 1$ ,  $|K||L|g$ , thus  $g = |KL| = |\bar{K}|$  and  $q \in P(KL)$ . This shows that  $P(K) \cap P(L) \leq P(KL)$  and we get from (7)

$$P(\Omega L) \leq P(KL).$$

By the theorem of Bauer it follows that  $\Omega L \supset KL$  and by Lemma 1,  $\Omega$  contains a conjugate of  $K$ , q. e. d.

**Proof of Theorem 2.** Let  $\mathfrak{G}$  be the Galois group of  $\bar{K}$ ,  $\mathfrak{H}$  the subgroup of  $\mathfrak{G}$  belonging to  $K$ ,  $\Pi$  the set of primes dividing the order of  $\mathfrak{H}$ . Since  $|\mathfrak{G}| = nm$ , with  $(n, m) = 1$ ,  $\mathfrak{H}$  is a Hall  $\Pi$ -subgroup of  $\mathfrak{G}$  and hence (cf. [4], Th. 9.3.1) any normal  $\Pi$ -subgroup of  $\mathfrak{G}$  is a subgroup of  $\mathfrak{H}$ . By Lemma 2 either there is in  $\mathfrak{G}$  a normal  $\Pi$ -subgroup  $\neq 1$  or there is a normal Hall  $\hat{\Pi}$ -subgroup. The first case is impossible since then  $\mathfrak{H}$  would contain a non-trivial normal subgroup of  $\mathfrak{G}$ , thus there would be a normal field between  $K$  and  $\bar{K}$ . Therefore, there is in  $\mathfrak{G}$  a normal subgroup  $\mathfrak{N}$  such that  $|\mathfrak{N}||\mathfrak{H}| = |\mathfrak{G}|$ . Let  $L$  be the field belonging to  $\mathfrak{N}$ . Clearly  $L$  is normal,  $(|K|, |L|) = 1$ ,  $KL = \bar{K}$  and therefore the field  $K$  has property (N), q. e. d.

**Proof of Theorem 3.** Let

$$(11) \quad f(x) = c f_1(x)^{e_1} f_2(x)^{e_2} \dots f_r(x)^{e_r},$$

where  $c \neq 0$  is a rational number and  $f_1(x), f_2(x), \dots, f_r(x)$  are coprime polynomials with integral coefficients, each irreducible over  $Q$  and where  $e_1, e_2, \dots, e_r$  are non-zero integers. Put

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

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

$$(12) \quad F(x)A(x) + F'(x)B(x) = D,$$

identically, where  $D$  is a non-zero integer.

Let  $\theta$  be a zero of some  $f_j(x)$  and set  $\Omega = Q(\theta)$ . Let  $L$  be a normal field postulated by the assumption that  $K$  has property (N) and let  $q \in P(\Omega L)$  be a large prime. Clearly  $q \in P(\Omega)$  and by the theorem of Dedekind, the congruence

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

is soluble. Let  $x_0$  be a solution. By (12) we have  $F'(x_0) \not\equiv 0 \pmod{q}$ , whence

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

By choosing  $x_1$  to be either  $x_0$  or  $x_0 + q$ , we can ensure that

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

whence  $f_j(x_1) \not\equiv 0 \pmod{q^2}$  and  $f_i(x_1) \equiv 0 \pmod{q}$  for  $i \neq j$ . By the hypothesis of the theorem there exists  $x_2 \equiv x_1 \pmod{q^2}$  such that

$$(13) \quad f(x_2) \equiv N_{K/Q}(\omega) \quad \text{for some } \omega \in K.$$

From the preceding congruences we have

$$(14) \quad f(x_2) \equiv 0 \pmod{q^{e_j}}, \quad f(x_2) \not\equiv 0 \pmod{q^{e_j+1}}.$$

Let the prime ideal factorization of  $q$  in  $\bar{K} = KL$  be

$$q = q_1 q_2 \dots q_\sigma.$$

Since  $\bar{K}$  is normal, we have

$$N_{\bar{K}/Q} q_i = q^{|\bar{K}|/g}.$$

Write the prime ideal factorization of  $\omega$  in  $\bar{K}$  in the form

$$(\omega) = q_1^{a_1} q_2^{a_2} \dots q_\sigma^{a_\sigma} \mathfrak{A} \mathfrak{B}^{-1},$$

where  $\mathfrak{A}, \mathfrak{B}$  are ideals in  $K$  relatively prime to  $q$ . Then

$$(15) \quad N_{K/Q}(\omega) = q^{|\bar{K}|(a_1 + a_2 + \dots + a_\sigma)/g} N_{K/Q}(\mathfrak{A}) N_{K/Q}(\mathfrak{B})^{-1}$$

and  $N_{K/Q}(\mathfrak{A}), N_{K/Q}(\mathfrak{B})$  are relatively prime to  $q$ .

It follows from (13), (14) and (15) that

$$|K|(a_1 + a_2 + \dots + a_\sigma)/g = e_j, \quad \text{thus } |K||e_j g.$$

However, we assumed  $(|K|, e_j) = 1$ , whence  $|K||g$ . On the other hand  $q \in P(L)$  and so by the argument in the paragraph culminating with (10),  $|L||g$ . Since  $(|K|, |L|) = 1$ ,  $|K||L|g$ , thus  $g = |KL|$  and  $q \in P(KL)$ . This shows that  $P(\Omega L) \leq P(KL)$ . By the theorem of Bauer it follows that  $\Omega L \supset KL$  and by Lemma 1,  $\Omega$  contains a conjugate of  $K$ , say  $K'$ . Applying Lemma 3 with  $G(x) = f_j(x)$ ,  $J = K'$  we conclude that

$$f_j(x) = a_j N_{K'/Q}(H_j(x)),$$

where  $H_j(x)$  is a polynomial over  $K'$ . Clearly

$$f_j(x) = a_j N_{K/Q}(H'_j(x)),$$

where  $H'_j(x)$  is a conjugate of  $H_j$  with coefficients in  $K$ .

By (11) and the multiplicative property of the norm, we get

$$f(x) = a N_{K/Q}(h(x)),$$

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  $\alpha$  of  $K$ . Putting  $\omega(x) = \alpha h(x)$ , we obtain  $f(x) = N_{K/Q}(\omega(x))$ , identically, q. e. d.

## References

- [1] M. Bauer, *Zur Theorie der algebraischen Zahlkörper*, Math. Ann. 77 (1916), pp. 353-356.  
 [2] H. Davenport, D. J. Lewis and A. Schinzel, *Polynomials of certain special types*, Acta Arith. 9 (1964), pp. 107-116.  
 [3] W. Feit and J. G. Thompson, *Solvability of groups of odd order*, Pacific J. Math. 13 (1963), pp. 775-1029.  
 [4] M. Hall, *The Theory of Groups*, New York 1959.  
 [5] H. Hasse, *Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper II*, Jahresber. der Deutschen Math. Vereinigung 6 (1930).  
 [6] O. Haupt, *Einführung in die Algebra II*, Leipzig 1954.  
 [7] H. Mann, *Introduction to Algebraic Number Theory*, Columbus 1955.  
 [8] A. Schinzel, *On a theorem of Bauer and some of its applications*, Acta Arith., this volume, pp. 333-344.  
 [9] H. Zassenhaus, *The Theory of Groups*, (second edition), New York 1958.

Reçu par la Rédaction le 12. 3. 1965

## Quadratic Diophantine equations with a parameter

by

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

We have proved in [2] the following result: Let  $f(t)$  be a polynomial with integral coefficients and suppose that every arithmetical progression contains an integer  $t$  such that  $F(x, y, t) = x^2 + y^2 - f(t) = 0$ . Then  $F(x(t), y(t), t) = 0$  identically, where  $x(t)$  and  $y(t)$  are polynomials with integral coefficients. This can be extended to  $F(x, y, t) = x^2 + \Delta y^2 - f(t)$  provided  $x(t), y(t)$  are allowed to have rational coefficients. An example is given in [5] showing that an analogous theorem does not hold for a general polynomial  $F(x, y, t)$  even if we assume solubility for all integers  $t$ , and the question is raised there of the connection between the solubility of  $F(x, y, t) = 0$  in rationals  $x, y$  for a suitable  $t$  from every arithmetical progression and the solubility in rational functions  $x(t), y(t)$  (cf. also [4], Problems 5 and 6). In this paper we prove (Theorem 2) that such a connection does exist if  $F(x, y, t)$  is of degree at most two in  $x$  and  $y$ . Whether, under the last assumption, the solubility in integers implies the solubility in polynomials with rational coefficients we do not know even in the simple case

$$F(x, y, t) = a(t)xy + b(t)x + c(t)$$

(a solution in polynomials with integral coefficients need not exist as is shown by the example  $a(t) = 0, b(t) = 2, c(t) = t(t+1)$ ). On the other hand, it is easy to deduce from our Theorem 2 the result on sums of two squares mentioned at the beginning.

We start with a theorem on quadratic forms over  $Q(t)$ , where  $Q$  denotes the rational field.

**THEOREM 1.** *Let  $a(t), b(t)$  be polynomials with integral coefficients. Suppose that every arithmetical progression contains some integer  $t$  such that the equation*

$$(1) \quad a(t)x^2 + b(t)y^2 = z$$