On a theorem of Bauer and some of its applications

by

A. SCHINZEL (Warszawa)

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 $P(Q) \subset P(K)$ implies $Q \supset K$ (the converse implication is immediate).

In this theorem inclusion $P(Q) \subset P(K)$ can be replaced by a weaker assumption that the set of primes $P(Q)$ is finite, which following Hasse [5] I shall denote by $P(Q) \leq P(K)$. An obvious question to ask is whether on omitting the assumption that $K$ is normal it is true that $P(Q) \leq P(K)$ implies $Q$ contains a conjugate of $K$. This question was answered negatively by F. Gasmann [3] in 1926 when he gave an example of two non-conjugate fields $Q$ and $K$ of degree 180 such that $P(Q) = P(K)$. The two fields found by Gassmann have the even more remarkable property $P_Q(Q) = P_Q(K)$ 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 $A$.

The first aim of this paper is to characterize all fields $K$ for which the extension of Bauer's theorem mentioned above is nevertheless true. Such fields will be called Bauerian. It follows easily from the definition that if $K_1, K_2$ are two Bauerian fields and $|K_1| \leq |K_2|$, then $K_1$ is also Bauerian (denotes the degree). We have

**Theorem 1.** Let $K, Q$ be two algebraic number fields, $R$ the normal closure of $K$, $\mathfrak{G}$ — its Galois group, $\mathfrak{S}$ and $\mathfrak{Z}$ subgroups of $\mathfrak{G}$ belonging to $K$ and $Q$ respectively and $\mathfrak{S}_1, \mathfrak{S}_1', \ldots, \mathfrak{S}_n$ all the subgroups of $\mathfrak{G}$ conjugate to $\mathfrak{S}$. $P(Q) \leq P(K)$ is equivalent to $\mathfrak{S} \subset \bigcup_{i=1}^n \mathfrak{S}_i$.

The field $K$ is Bauerian if and only if every subgroup of $\mathfrak{G}$ contained in $\bigcup_{i=1}^n \mathfrak{S}_i$ is contained in one of the $\mathfrak{S}_i$.

The second part of this theorem enables us to decide for any given
field in a finite number of steps whether it is Baurian or not. A field $K$ is said to be solvable if the Galois group of its normal closure is solvable. We obtain in particular

**Theorem 2.** Every cubic and quartic field and every solvable field $K$, such that $(|K|/|K|, |K|) = 1$ is Baurian. If $K$ is of degree $n > 5$ such that the Galois group of $K$ is the alternating group $S_3$ or the symmetric group $S_n$, are not Baurian.

Theorem 2 gives complete information about fields of degree $n = 5$. For such fields, Baurian fields coincide with solvable ones. The following example which I owe to Professor H. Hasse shows that this is no longer true for fields of degree six. Let $K$ be any field with group $S_3$ (such fields exist, cf. § 5) and let $K$ belong to a subgroup $S_3$ of order two. Here $S_3$ is itself a subgroup (the four-group) and clearly is not contained in any of the $S_3$. Taking $O$ to be the field corresponding to $S_3$, we see that $O$ is normal and $O < K$, thus in this case

$$P(O) = P(K) \quad \text{but} \quad \overline{O} \neq K \quad \text{and} \quad |O| \neq |K|.$$  

This shows that the condition $P(O) = P(K)$ is much weaker than the condition $P_A(O) = P_A(K)$ for every $A$. The latter according to Gaussmann [3] implies that $O \subseteq K$ and $|O| \neq |K|$.

The theorem of Bauer has been applied in [2] to characterize polynomials $f(x)$ with the property that for a given field $K$ in every arithmetical progression there is an integer $a$ such that $f(a)$ is a norm of an element of $K$. The same method combined with Theorem 2 gives

**Theorem 3.** (i) Let $K$ be a cubic or quartic field or a solvable field such that $(|K|/|K|, |K|) = 1$ and let $N_{K/O}$ denote the norm from $K$ to the rational field $Q$. Let $f(x)$ be a polynomial with rational coefficients, and suppose that every arithmetical progression contains an integer $a$ such that

$$f(x) = N_{K/O}(a) \quad \text{for some} \quad a \in K.$$  

If either $n = |K|$ is square-free or the multiplicity of every zero of $f(x)$ is relatively prime to $n$, then $f(x) = N_{K/O}(a(x))$ identically for some $a(x) \in K[x]$.

(ii) Let $K$ be a field of degree $n > 5$, $n \neq 6$ such that the Galois group of $K$ is alternating $S_3$ or symmetric $S_n$. Then there exists an irreducible polynomial $f(x)$ such that for every integer $a$ and some $a(x) \in K[x]$, $f(x) = N_{K/O}(a(x))$ but $f(x)$ cannot be represented as $N_{K/O}(a(x))$ for any $a(x) \in K[x]$.

Since every group of square-free order is solvable, we get immediately from Theorem 3 (i).

**Corollary.** Let $K$ be a field such that $|K|$ is square-free and let $f(x)$ be a polynomial with rational coefficients. If every arithmetical progression contains an integer $x$ such that $f(x) = N_{K/O}(a(x))$ for some $a(x) \in K$, then $f(x) = N_{K/O}(a(x))$ identically for some $a(x) \in K[x]$.

If $f(x)$ is to be represented only as a norm of a rational function, not of a polynomial the conditions on the field $K$ can be weakened. We have

**Theorem 4.** Let $K$ be a field of degree $n = p$ or $p^2$ ($p$ prime) and let $g(x)$ be a rational function over $Q$. If in every arithmetical progression there is an integer $x$ such that

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

then

$$g(x) = N_{K/Q}(a(x)) \quad \text{for some} \quad a(x) \in K.$$

There exist fields of degree $6$ for which an analogue of Theorem 4 does not hold. We have in fact

**Theorem 5.** Let $K = Q(\sqrt[3]{2 \cos \frac{2\pi}{3}})$, $f(x) = x^3 + x^2 - 2x - 1$. For every integer $a$, $f(a)$ is a norm of an integer in $K$, but $f(x)$ cannot be represented as $N_{K/Q}(a(x))$ for any $a(x) \in K[x]$.

The proofs of Theorems 1 and 2 are given in § 2, those of Theorems 3, 4 and 5 in § 3, 4 and 5, respectively.

I shall like to express my thanks to Professor J. D. Lewis, H. Hasse and Dr. B. R. Bumby for their valuable suggestions and to Dr. S. Seshadri Sebal whom I owe the proof of Lemma 3.

2. **Proof of Theorem 1.** This proof follows easily from a generalization of Bauer's theorem given by Hasse [5], p. 144. For a given prime $p$, let $\left(\frac{x}{p}\right)$ be the Artin symbol (the class of conjugate elements of $\mathfrak{G}$, to which $p$ belongs). The theorem in question can be stated in our notation in the following way. $C$ being any class of conjugate elements in $\mathfrak{G}$, the set $\left\{ p \in P(Q) ; \left(\frac{x}{p}\right) = C \right\}$ is infinite if and only if $C \subseteq \bigcup_{j=1}^{m} \mathfrak{S}_j$, where $\mathfrak{S}_j$ (for $j = 1, 2, \ldots, m$ are all the subgroups of $\mathfrak{G}$ conjugate to $\mathfrak{S}$).

Suppose now that $P(O) \subseteq P(K)$ and let $C$ be any class of conjugate elements of $\mathfrak{G}$ such that $C \subseteq \bigcup_{j=1}^{m} \mathfrak{S}_j$. By the theorem of Hasse, the set $\left\{ p \in P(Q) ; \left(\frac{x}{p}\right) = C \right\}$ is infinite and since $P(O) \subseteq P(K)$ the same applies to $\left\{ p \in P(K) ; \left(\frac{x}{p}\right) = C \right\}$. Applying the theorem in the opposite direction and with $X$ instead of $O$ we infer that $C \subseteq \bigcup_{j=1}^{m} \mathfrak{S}_j$. The set $\bigcup_{j=1}^{m} \mathfrak{S}_j$ consists of
the union of full conjugate classes. Hence $\bigcup_{i=1}^{n} S_i = S_1$ and a fortiori $S_1 \subseteq S_i$.

In order to prove the converse implication, let us notice that according to [5], p. 164, the symmetric difference

\[ P(K) + P(K) = \bigcup_{i=1}^{n} S_i \]

is finite.

(1)

and similarly

\[ P(Q \cap K) + P(Q \cap K) = \bigcup_{i=1}^{n} S_i \]

is finite.

(2)

Hence if $S_1 \subseteq S_i$, we get $S_1 \subseteq S_i$ and by (1) and (2) $P(Q \cap K) = P(K)$.

This completes the proof of the first part of Theorem 1. The second part follows immediately from the first after taking into account that every subgroup of $G$ belongs to some field and this field can be set as $D$.

Proof of Theorem 2. Suppose first that the Galois group of $K$ is solvable and $(Kf/K, K)$ is an $H$-group. Let $S$ be the subgroup of $G$ belonging to $K$ and let $H$ be the set of all primes dividing $|S|$, i.e., the order of $S$.

If for a subgroup $S_i$, $S_i \subseteq S_i$, then clearly $S_1$ is an $H$-group. Since $S'_i$ is a maximal $H$-group by a theorem of P. Hall (cf. [4], Th. 0.3.1) $S_1$ must be contained in one of $S_i$. This shows according to Theorem 1 that field $K$ is芭uerian. In particular every cubic field and any quartic field $K$ having $S'_i$ as Galois group of $K$ is芭uerian. It remains to consider quartic fields $K$ such that Galois group of $K$ is either dihedral group of order 8 or $S_4$. In the first case $S_i \subseteq S_i$ consists of 3 elements and does not contain any subgroup except the $S_i$ and the identity group. In the second case $S_i \subseteq S_i$ is the 6th stability group and $S_i \subseteq S_i$ contains besides the $S_i$ and the identity group only cyclic subgroups of order two or three. These are clearly contained in one of the $S_i$. Thus every quartic field is芭uerian.

In order to prove that fields $K$ of degree $n > 5$ such that $S'_i$ or $S_i$ is not芭uerian we consider the following subgroups of $S_i$:

\[ ((123), (12)(45)) \times S_{n-5} \quad \text{for} \quad n = 5 \text{ or } n = 8, \]

\[ ((12)(34), (12)(56)) \quad \text{for} \quad n = 6, \]

\[ ((12)(34)(5), (12)(34)(67)) \quad \text{for} \quad n = 7. \]

They are contained in the union of stability subgroups of $S_i$, but not in any one of them, and the desired result follows immediately from the second part of Theorem 1.

3. Lemma 1. Suppose that the hypotheses of Theorem 3 (i) hold. Let

\[ f(x) = c_1(x)f_1(x)^{e_1}\cdots f_m(x)^{e_m} \]

where $c \neq 0$ is a rational number and $f_1(x), f_2(x), \ldots, f_m(x)$ are relatively prime polynomials with integer coefficients each irreducible over $Q$ and $\epsilon_1, \epsilon_2, \ldots, \epsilon_m$ are positive integers. For any $j$, let $\varphi$ be a sufficiently large prime for which the congruences

\[ f_j(x) \equiv 0 \mod \varphi \]

is solvable.

If $(\epsilon_1, n) = 1$ then $\varphi \in P(K)$, If $n$ is square-free then $q \in P(K)$, where $K$ is any subfield of $K$ of degree $n$. All subfields exist.

Proof. Put $F(x) = f_1(x)f_2(x)\cdots f_m(x)$. Since the discriminant of $F(x)$ is not zero, there exist polynomials $\varphi(x), \psi(x)$ with integral coefficients such that

\[ F(x)\varphi(x) + F'(x)\psi(x) = D \]

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

Let $\varphi$ be a large prime for which the congruence (5) is solvable and let $x_0$ be a solution. By (6) we have $F(x_0) \not\equiv 0 \mod \varphi$, whence

\[ F(x_0 + q) \not\equiv F(x_0) \mod \varphi^2. \]

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

\[ f_j(x_0) \equiv 0 \mod \varphi, \quad F(x_0) \not\equiv 0 \mod \varphi^2, \]

whence

\[ f_j(x_0) \equiv 0 \mod \varphi^2 \quad \text{and} \quad f_k(x_0) \equiv 0 \mod \varphi^2 \quad \text{for} \quad i \neq j. \]

By the hypothesis of Theorem 3, there exists $x_0 \equiv x_0 \mod \varphi^2$ such that

\[ \varphi \equiv x_0 \equiv x_0 \mod \varphi^2 \]

From the preceding congruences we have

\[ f_j(x_0) \equiv 0 \mod \varphi^2, \quad f_j(x_0) \equiv 0 \mod \varphi^2, \quad f_k(x_0) \equiv 0 \mod \varphi^2 \quad \text{for} \quad i \neq j. \]

Hence

\[ f(x_0) \equiv 0 \mod \varphi^2, \quad F(x_0) \equiv 0 \mod \varphi^2. \]

Acta Arithmetica XLIII
If \( n = 4 \) and \( q \) does not belong to \( P(K) \), then \( q \) remains prime in \( K \) or factors into two prime ideals of degree two. In either case \( q \) divides \( N(\omega) \) for any \( \omega \in K \) in an even power. In view of (4) and (8) this contradicts the assumption that \( (\epsilon, n) = 1 \).

If \( K \) is solvable and \( (|K|/|K|, |K|) = 1 \), let

\[
q = q_1 q_2 \ldots q_t
\]

be the prime ideal factorization of \( q \) in \( K \); the factors are distinct since \( q \) is supposed to be sufficiently large. We note that \( t \) divides \( n \) because \( K \) is a normal field and that

\[
N_{K/Q} q_i = q_i^{n/\epsilon_i}
\]

Write the prime ideal factorization of \( \omega \) in \( K \) in the form

\[
(\omega) = q_1^{\alpha_1} q_2^{\alpha_2} \ldots q_t^{\alpha_t} b^{-1},
\]

where \( a, b \) are ideals in \( K \) which are relatively prime to \( q \). Then

\[
N_{K/Q}(\omega) = \pm q_1^{n - \alpha_1 + \ldots + a_t} q_2^{n - \alpha_2 + \ldots + a_t} b^{-1} N_{K/Q}(q_1^{\alpha_1} q_2^{\alpha_2} \ldots q_t^{\alpha_t} b^{-1})^{-1}
\]

and \( N_{K/Q} q_i, N_{K/Q} b \) are relatively prime to \( q \). It follows from (7), (8) and (11) that

\[
n(\alpha_1 + \alpha_2 + \ldots + \alpha_t) \mid q = \epsilon_i,
\]

whence

\[
\frac{n}{(\epsilon_i, n)} \mid q.
\]

If \( (\epsilon, n) = 1 \) we get that \( n \) divides \( q \). Let \( \mathfrak{G}_q \) be the splitting group of the ideal \( q \). We have \([\mathfrak{G}_q : \mathfrak{G}_q] = q\), thus \( \mathfrak{G}_q \) divides \( \mathfrak{G}_n \), that is the order of the group \( \mathfrak{G}_n \) belonging to field \( K \). Since

\[
\left( n, \frac{|\mathfrak{G}_n|}{n} \right) = \left( n, \frac{|K|}{n} \right) = 1
\]

it follows from the theorem of Hall, that \( \mathfrak{G}_q \) is contained in one of the conjugates of \( H \). Therefore the splitting field \( F_q \) of \( q \) contains a conjugate of \( K \) and since \( q \in P(K) \), \( q \in P(K) \).

Suppose now that \( n \) is square-free and let \( \mathfrak{G}_q \) and \( F_q \), have the same meaning as before. Since

\[
\left( \frac{|\mathfrak{G}_n|}{n} (\epsilon_i, n), \frac{n}{(\epsilon_i, n)} \right) = 1
\]

there exist in \( \mathfrak{G}_n \), by the theorem of Hall, subgroups of order \( \frac{n}{(\epsilon_i, n)} \) and they are all conjugate. Moreover since \( (\mathfrak{G}_n)_{(\epsilon_i, n)} \mathfrak{G}_n \) must be contained in one of them, thus \( F_q \), must contain a subfield \( K' \) of \( K \) of degree \( \frac{n}{(\epsilon_i, n)} \).

Since all such fields are conjugate, and since \( q \in P(\mathfrak{G}_n) \) it follows that \( q \in P(K_i) \), where \( K_i \) is any subfield of \( K \) of degree \( \frac{n}{(\epsilon_i, n)} \). Such fields exist again by the theorem of Hall since \( \left( \frac{|\mathfrak{G}_n|}{n}, \left( \frac{n}{(\epsilon_i, n)} \right) \right) = 1 \).

Proof of Theorem 3(i). Lemma 1 being established the proof does not differ from the proof of Theorem 2 of [2]. Instead of Lemma 3 of that paper which was the original Bauer theorem one uses Theorem 2. Proof of Theorem 3(ii). Let the Galois group of \( K \) be represented as the permutation group on the \( n \) fields conjugates to \( K: K_1, K_2, \ldots, K_n \). Consider a subfield \( \mathcal{O} \) of \( K \) belonging to a subgroup \( \mathfrak{G}_n \) of \( \mathfrak{G}_n \) defined by formula (3). It is clear that \( \mathfrak{G}_n \) denotes the subgroup of \( \mathfrak{G}_n \) belonging to \( K_i \), then

\[
\frac{[\mathfrak{G}_n]}{[\mathfrak{G}_n \cap \mathfrak{G}_n \cap \mathfrak{G}_n]} = \begin{cases} 3 & \text{for } i = 1, 2, 3, \\ 2 & \text{for } i = 4 \text{ or } 5, \quad (n = 5 \text{ or } n \geq 8), \\ n - 5 & \text{for } i = 6, \ldots, n \end{cases}
\]

(12)

We have

\[
\frac{[\mathfrak{G}_n]}{[\mathfrak{G}_n \cap \mathfrak{G}_n \cap \mathfrak{G}_n]} = \begin{cases} 5 & \text{for } i \leq 5, \\ 2 & \text{for } i = 6 \text{ or } 7 \quad (n = 7). \end{cases}
\]

and the equalities (12) mean that \( P(x) \) — the polynomial generating \( K \) factorizes in \( \mathcal{O} \) into irreducible factors of degrees 3, 2 and \( n - 5 \) (\( n = 5 \) or \( n \geq 8 \)) or 3 and 2 (\( n = 7 \)). It follows by the theorem of Kronecker and Kneser (cf. [7], p. 239) that \( f(x) \) — the polynomial generating \( \mathcal{O} \) factorizes in \( K \) into irreducible factors of degrees \( \frac{1}{n} \) and \( \frac{2}{n} \) or \( \frac{3}{n} \) and \( \frac{n - 5}{n} \) (\( n = 5 \) or \( n \geq 8 \)) or \( \frac{1}{n} \) and \( \frac{2}{n} \) (\( n = 7 \)). The norms of these factors with respect to \( K \) are \( f'(x), f'(x), f^{(2)}(x) \) (\( n = 5 \) or \( n > 8 \)) and \( f'(x), f^{(2)}(x) \) (\( n = 7 \)).
4. Theorem 2. Suppose that the hypotheses of Theorem 4 hold. Let
\[ g(a) = c_1 f_1(a)^{e_1} f_2(a) f_3(a) \cdots f_m(a)^{e_m}, \]
where \( c \neq 0 \) is a rational number and \( f_1(a), f_2(a), \ldots, f_m(a) \) are relatively prime polynomials with integral coefficients each irreducible over \( Q \) and where \( e_1, e_2, \ldots, e_m \) are integers relatively prime to \( n \). For any \( j \) let \( g \) be a sufficiently large prime for which the congruence
\[ f_j(a) \equiv 0 \pmod{g} \]
is solvable. Then \( g \) factorizes in \( K \) into a product of ideals, whose degrees are relatively prime.

**Proof.** We infer as in the proof of Lemma 1 that there exists an integer \( a \) with the following properties
\[ g(a) = N_{K/Q}(a) \quad \text{for some } a \in K, \]
\[ g(a) = q^{ab-1}, \quad \text{where } a, b \text{ are integers and } (ab, q) = 1. \]
Let \( q = p_1 p_2 \cdots p_n \) be the factorization of \( q \) in \( K \), the factors are distinct since \( q \) is sufficiently large and let \( N_{K/Q} p_i = q^i \). Clearly
\[ \sum_{i=1}^n f_i = n. \]
Write the prime ideal factorization of \( \omega \) in \( K \) in the form
\[ \omega = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n} \]
where \( (ab, q) = 1 \). Then
\[ N_{K/Q} a = q^{a_1+\ldots+a_n-1} N_{K/Q} Q(a) \]
and
\[ N_{K/Q} b = a \text{ are relatively prime to } g. \]
It follows from (14), (15) and (17) that
\[ a_1 f_1 + a_2 f_2 + \ldots + a_n f_n = \eta. \]
Thus \( (f_1, f_2, \ldots, f_n) \mid \eta \). Since \( (s_1, s_2) = 1, (f_1, f_2, \ldots, f_n) = 1, \eta \), and \( q \), the orbits are therefore all divisible by \( p \). On the other hand, for every triple \( a, \beta, \gamma \) either \( a = p \) or there exists a \( k \) such that \( 1 \leq k < p \) and \( ka + \beta = 0 (mod p) \). In either case \( P_{a, \beta, \gamma} \) leaves at least \( p \) letters fixed.

**Proof of Theorem 4.** Let the Galois group \( G \) of \( K \) be represented as a permutation group on the \( n \) fields conjugate to \( K \). Let \( f_j(a) \) be any one of irreducible factors of \( g(a) \) as in (13), \( \Omega_j \) be a field generated by a root of \( f_j(a) \) and \( \Sigma_j \) be a subgroup of \( G \) belonging to field \( \Omega_j \). By the theorem of Hase quoted in the proof of Theorem 1 for every class \( C \in \cup \Sigma \) (summation over all conjugates \( \Sigma_j \)) there exist infinitely many primes \( q \in P(\Omega_j) \) such that \( \frac{K}{q} = C \). If such a prime is sufficiently large, we infer by the principle of Dedekind and Lemma 2 that \( q \) factorizes in \( K \) into prime ideals of relatively prime degrees. The degrees in question are equal to the lengths of the cycles in the decomposition of class \( C \). Thus in every permutation of \( \Sigma_j \), the lengths of the cycles are relatively prime. By Lemma 3 this implies that the lengths of the orbits of \( \Sigma_j \) are relatively prime.

Let \( k(a) \) be an irreducible polynomial over \( Q \), whose root generates \( K \). \( \Sigma_j \) is the Galois group of the equation \( k(a) = 0 \) over \( \Omega_j \). The lengths
of the orbits of \( \mathcal{O} \) are equal to the degrees or irreducible factors of \( k(x) \) over \( \Omega \). Thus
\[
k(x) = k_1(x)k_2(x) \cdots k_p(x)
\]
where \( k_i \) is a polynomial irreducible over \( \Omega \) of degree \( |k_i| \) and
\[
|k_i|, |k_{i2}|, \ldots, |k_p| = 1.
\]
By the theorem of Kronecker and Kneser it follows that
\[
f_i(x) = \xi f_i(x) f_i(x) \cdots f_i(x), \quad \text{where} \quad \xi \in \mathbb{Q},
\]
\[
f \in K[x] \quad \text{and} \quad N_{K|O}(f) = \left( f_i(x) \right)^{2|k_i|}. \tag{19}
\]
In view of (18), there exist integers \( a_i \) (\( i = 1, 2, \ldots, r \)) such that
\[
\sum_{i} a_i |k_i| = 1. \tag{20}
\]
We get from (19) and (20)
\[
f(x) = \xi N_{K|O} \prod_{i=1}^{r} f_i(x). \tag{21}
\]
It follows from (13), (21) and the multiplicative property of the norm that
\[
g(x) = a N_{K|O} h(x), \quad \text{where} \quad h(x) \in K(x).
\]
By the hypothesis of the theorem taking \( z \) to be a suitable integer, we infer that \( a = N_{K|O}(a) \), where \( a \in K \). Putting \( a(x) = a h(x) \) we obtain
\[
g(x) = N_{K|O}(a(x)), \quad \text{identically, } q. e. d.
\]
**Lemma 4.** The class number of the \( K = Q(\sqrt{2 \cos^2 \pi}) \) is one and the rational primes \( p \) factorize in \( K \) in the same way as the polynomial \( f(x^2) \) factorizes mod \( p \).

**Proof.** The field \( K = Q(\sqrt{2 \cos^2 \pi}) \) is a cyclic field of discriminant \( 7^2 \). \( 2 \) remains a prime in this field, hence \( 2 \cos^2 \pi = (2 \cos^2 \pi)^2 - 2 \) is in \( O \) a quadratic non-residue mod 4. Since \( 2 \cos^2 \pi \) is a unit, it follows by the conventional methods that 1, \( \sqrt{2 \cos^2 \pi} \) is an integral basis for \( K \) over \( \Omega \), thus \( \Delta_{K|O} \) equals \( 8 \cos^2 \pi \) and for the discriminant of \( K \) we obtain a value
\[
\Delta_{K|O} = \Delta_{K|O}(\Delta_{K|O}) = 2^4 \cdot 7^4.
\]
This number coincides with the discriminant of \( f(x^2) \), which has \( \sqrt{2 \cos^2 \pi} \) as one of its zeros. Therefore, by the principle of Dedekind the factorization of primes in \( K \) is the same as factorization of \( f(x^2) \) mod \( p \). In particular we have
\[
(2) = \mathfrak{P}_1, \quad N \mathfrak{P}_1 = 8,
\]
\[
(3) = \mathfrak{P}_1 \mathfrak{P}_3, \quad N \mathfrak{P}_3 = N \mathfrak{P}_1 = 3^3,
\]
\[
(5) = \mathfrak{P}_1 \mathfrak{P}_5, \quad N \mathfrak{P}_5 = N \mathfrak{P}_1 = 5^3,
\]
\[
(7) = \mathfrak{P}_1 \mathfrak{P}_7, \quad N \mathfrak{P}_7 = N \mathfrak{P}_1 = 7.
\]
Now, by the theorem of Minkowski, in every class of ideals of \( K \) there is an ideal with norm not exceeding
\[
\left( \frac{4 \cdot 11}{\pi} \right)^{1/2} \approx 9.03 < 11.
\]
If therefore the field \( K \) had class number greater than 1, then there would be a non-principal ideal with a norm < 11. This is however impossible since
\[
(2) = (2 \cos^2 \pi + \sqrt{2 \cos^2 \pi}),
\]
\[
(7) = (1 + 2 \cos^2 \pi + \sqrt{2 \cos^2 \pi})(1 + 2 \cos^2 \pi - \sqrt{2 \cos^2 \pi}).
\]
**Proof of Theorem 5.** Since the degree of \( f(x) \) is not divisible by 6, \( f(x) \) cannot be represented as \( N_{K|O}(a(x)) \), where \( a(x) \neq K(x) \). It remains to show that for every integer \( a, f(x) = N_{K|O}(a) \) for some integer \( a \in K \).

Let
\[
f(x) = \pm p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}
\]
where \( a_i \) are positive integers. Since the discriminant of \( K = Q(2 \cos^2 \pi) \) coincides with the discriminant of \( f(x) \), by the principle of Dedekind each prime \( p_i \) has a prime ideal factor \( \mathfrak{P}_i \) of first degree in \( K \).

Since \( \mathfrak{P}_i \) of first degree, there exists a rational integer \( x_i \) such that \( \mathfrak{P}_i = a_i \mathfrak{P}_i \) and we get \( f(x_i) \equiv 0 \pmod{p_i} \). By Lemma 4, \( p_i \neq P(K) \) and since every ideal of \( K \) is principal,
\[
p_i = \pm N_{K|O} \alpha_i,
\]
where \( \alpha_i \) is an integer of \( K \). Since
\[
-1 = N_{K|O}(\sqrt{2 \cos^2 \pi}),
\]
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 $P(x, y)$ of degree $4 \phi(n)$ such that when $(x, y) = 1$, the prime factors of $P(x, y)$ either divide $n$ or are of the form $nk \pm 1$. (If $f(x) = x^n + 2x - 1$, then $y^2 f(x/y)$ is an example of such polynomial for $n = 7$.) The answer is that all such polynomials must be of the form $A \prod \left( x - a_i y \right)$, where $a_i$ runs through all conjugates of a primitive element of the field $\mathbb{Q} \left( 2 \cos \frac{2}{n} \right)$ 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 Bauerian. J. L. Alperin has proved that the answer is positive if the field is primitive and $p > 3$. P. Rémond has found a proof for the case where the Galois group of the normal closure is a $p$-group (oral communication).

References


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 $\Omega \subset K$. (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 $P(\Omega) = P(K)$ 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 $K$ is solvable and $X_{P(\Omega)}^2 - 1 = (1)$, 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.

(1) We let $d$ denote both the degree of the field over $Q$ and the order of the group.