ACTA ARITHMETICA
XI (1966)

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 $P(\Omega) \subset P(K)$ 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 [5] I shall denote by $P(\Omega) \leqslant P(K)$. An obvious question to ask is whether on omitting the assumption that K is normal it is true that $P(\Omega) \leqslant P(K)$ implies Ω contains a conjugate of K. This question was answered negatively by F. Gassmann [3] in 1926 when he gave an example of two non-conjugate fields Ω and K of degree 180 such that $P(\Omega) = P(K)$. The two fields found by Gassmann have the even more remarkable property $P_A(\Omega) = P_A(K)$ 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 $|K_1K_2| = |K_1||K_2|$, then K_1K_2 is also Bauerian ($|\ |$ denotes the degree). We have

THEOREM 1. *Let K, Ω be two algebraic number fields, $\overline{K}$ the normal closure of K, $\mathfrak{G}$ — its Galois group, $\mathfrak{H}$ and $\mathfrak{J}$ subgroups of $\mathfrak{G}$ belonging to K and $\Omega \cap \overline{K}$, respectively and $\mathfrak{H}_1, \mathfrak{H}_2, \ldots, \mathfrak{H}_n$ all the subgroups of $\mathfrak{G}$ conjugate to $\mathfrak{H}$. $P(\Omega) \leqslant P(K)$ is equivalent to $\mathfrak{J} \subset \bigcup_{i=1}^{n} \mathfrak{H}_i$.*

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

The second part of this theorem enables us to decide for any given field in a finite number of steps whether it is Bauerian 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 $(|\overline{K}|/|K|, |K|) = 1$ is Bauerian. Fields K of degree $n \geqslant 5$ such that the Galois group of $\overline{K}$ is the alternating group $\mathfrak{A}_n$ or the symmetric group $\mathfrak{S}_n$ are not Bauerian.*

Theorem 2 gives complete information about fields of degree $\leqslant 5$. For such fields, Bauerian fields coincide with solvable ones. The following example which I owe to Professor H. Zassenhaus shows that this is no longer true for fields of degree six. Let $\overline{K}$ be any field with group $\mathfrak{A}_4$ (such fields exist, cf. § 5) and let K belong to a subgroup $\mathfrak{H}$ of order two. Here $\bigcup \mathfrak{H}_i$ is itself a subgroup (the four-group) and clearly is not contained in any of the $\mathfrak{H}_i$. Taking Ω to be the field corresponding to $\bigcup \mathfrak{H}_i$ we see that Ω is normal and $\Omega \subset K$, thus in this case

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

This shows that the condition $P(\Omega) = P(K)$ is much weaker than the condition $P_A(\Omega) = P_A(K)$ for every A. The latter according to Gassmann [3] implies that $\overline{\Omega} = \overline{K}$ and $|\Omega| = |K|$.

The theorem of Bauer has been applied in [2] to characterize polynomials $f(x)$ with the property that for a given normal field K in every arithmetical progression there is an integer x such that $f(x)$ 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 $(|\overline{K}|/|K|, |K|) = 1$ and let $N_{K/Q}$ 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 x such that*

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

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

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

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

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

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*

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

then

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

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

THEOREM 5. *Let $K = Q\left(\sqrt{2\cos\frac{2}{7}\pi}\right)$, $f(x) = x^3+x^2-2x-1$. For every integer x, $f(x)$ is a norm of an integer in K, but $f(x)$ cannot be represented as $N_{K/Q}(\omega(x))$ for any $\omega(x) \in K(x)$.*

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 Professors D. J. Lewis, H. Zassenhaus and Dr. R. T. Bumby for their valuable suggestions and to Dr. Sedarshan Sehgal 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 $\left(\frac{\overline{K}}{p}\right)$ 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. $\mathfrak{C}$ being any class of conjugate elements in $\mathfrak{G}$, the set $\left\{p \in P(\Omega): \left(\frac{\overline{K}}{p}\right) = \mathfrak{C}\right\}$ is infinite if and only if $\mathfrak{C} \subset \bigcup_{j=1}^{m} \mathfrak{J}_j$, where $\mathfrak{J}_j$ $(j = 1, 2, \ldots, m)$ are all the subgroups of $\mathfrak{G}$ conjugate to $\mathfrak{J}$.

Suppose now that $P(\Omega) \leqslant P(K)$ and let $\mathfrak{C}$ be any class of conjugate elements of $\mathfrak{G}$ such that $\mathfrak{C} \subset \bigcup_{j=1}^{m} \mathfrak{J}_j$. By the theorem of Hasse, the set $\left\{p \in P(\Omega): \left(\frac{\overline{K}}{p}\right) = \mathfrak{C}\right\}$ is infinite and since $P(\Omega) \leqslant P(K)$ the same applies to $\left\{p \in P(K): \left(\frac{\overline{K}}{p}\right) = \mathfrak{C}\right\}$. Applying the theorem in the opposite direction and with K instead of Ω we infer that $\mathfrak{C} \subset \bigcup_{i=1}^{n} \mathfrak{H}_i$. The set $\bigcup_{j=1}^{m} \mathfrak{J}_j$ consists of the union of full conjugate classes. Hence $\bigcup_{j=1}^{m} \mathfrak{J}_j \subset \bigcup_{i=1}^{n} \mathfrak{H}_i$ and a fortiori $\mathfrak{J} \subset \bigcup_{i=1}^{n} \mathfrak{H}_i$.

In order to prove the converse implication, let us notice that according to [5], p. 144, the symmetric difference

(1) $$P(K) \dot{-} \left\{p: \left(\frac{\bar{K}}{p}\right) \subset \bigcup_{i=1}^{n} \mathfrak{H}_i\right\} \text{ is finite}$$

and similarly

(2) $$P(\Omega \frown \bar{K}) \dot{-} \left\{p: \left(\frac{\bar{K}}{p}\right) \subset \bigcup_{j=1}^{m} \mathfrak{J}_j\right\} \text{ is finite.}$$

Hence if $\mathfrak{J} \subset \bigcup_{i=1}^{n} \mathfrak{H}_i$ we get $\bigcup_{j=1}^{m} \mathfrak{J}_j \subset \bigcup_{i=1}^{n} \mathfrak{H}_i$ and by (1) and (2) $P(\Omega \frown \bar{K}) \leqslant P(K)$ and a fortiori $P(\Omega) \leqslant P(K)$.

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 $\mathfrak{G}$ belongs to some field and this field can be set as Ω.

Proof of Theorem 2. Suppose first that the Galois group of $\bar{K}$ is solvable and $(|\bar{K}|/|K|, |K|) = 1$. Let $\mathfrak{H}$ be the subgroup of $\mathfrak{G}$ belonging to K and let Π be the set of all primes dividing $|\mathfrak{H}|$, i.e. the order of $\mathfrak{H}$. If for a subgroup $\mathfrak{J}$, $\mathfrak{J} \subset \bigcup_{i=1}^{n} \mathfrak{H}_i$, then clearly $\mathfrak{J}$ is a Π-group. Since $\mathfrak{H}$ is a maximal Π-group by a theorem of P. Hall (cf. [4], Th. 9.3.1) $\mathfrak{J}$ must be contained in one of $\mathfrak{H}_i$. This shows according to Theorem 1 that field K is Bauerian. In particular every cubic field and any quartic field K having $\mathfrak{A}_4$ as Galois group of $\bar{K}$ is Bauerian. Is remains to consider quartic fields K such that Galois group of $\bar{K}$ is either dihedral group of order 8 or $\mathfrak{S}_4$. In the first case $\bigcup_{i=1}^{4} \mathfrak{H}_i$ consists of 3 elements and does not contain any subgroup except the $\mathfrak{H}_i$ and the identity group. In the second case $\mathfrak{H}_i$ $(i = 1, 2, 3, 4)$ is the ith stability group and $\bigcup_{i=1}^{4} \mathfrak{H}_i$ contains besides the $\mathfrak{H}_i$ and the identity group only cyclic subgroups of order two or three. These are clearly contained in one of the $\mathfrak{H}_i$. Thus every quartic field is Bauerian.

In order to prove that fields K of degree $n \geqslant 5$ such that $\mathfrak{A}_n$ or $\mathfrak{S}_n$ is Galois group of $\bar{K}$ are not Bauerian we consider the following subgroups of $\mathfrak{A}_n$:

(3) $$\begin{aligned} &\{(123), (12)(45)\} \times \mathfrak{A}_{n-5} && \text{for } n = 5 \text{ or } n \geqslant 8, \\ &\{(12)(34), (12)(56)\} && \text{for } n = 6, \\ &\{(12345), (1243)(67)\} && \text{for } n = 7. \end{aligned}$$

They are contained in the union of stability subgroups of $\mathfrak{S}_n$ 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*

(4) $$f(x) = cf_1(x)^{e_1} f_2(x)^{e_2} \dots f_m(x)^{e_m}$$

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

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

is solvable.

If $(e_j, n) = 1$ then $q \in P(K)$. If n is square-free then $q \in P(K_j)$ where K_j is any subfield of K of degree $n/(e_j, n)$. (Such subfields exist).

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

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

identically, where D is a non-zero integer.

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

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

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

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

whence

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

By the hypothesis of Theorem 3, there exists $x_2 \equiv x_1 \pmod{q^2}$ such that

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

From the preceding congruences we have

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

Hence

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

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

If $\bar{K}$ is solvable and $(|\bar{K}|/|K|, |K|) = 1$, let

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

be the prime ideal factorization of q in $\bar{K}$; the factors are distinct since q is supposed to be sufficiently large. We note that l divides n because $\bar{K}$ is a normal field and that

$$N_{\bar{K}/Q}\mathfrak{q}_i = q^{n/g}. \tag{10}$$

Write the prime ideal factorization of ω in K in the form

$$(\omega) = \mathfrak{q}_1^{a_1}\mathfrak{q}_2^{a_2} \ldots \mathfrak{q}_g^{a_g}\mathfrak{a}\mathfrak{b}^{-1},$$

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

$$N_{K/Q}(\omega) = \pm q^{n(a_1+a_2+\ldots+a_g)/g} N_{K/Q}\mathfrak{a}(N_{K/Q}\mathfrak{b})^{-1} \tag{11}$$

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

$$n(a_1+a_2+\ldots+a_g)/g = e_j,$$

whence

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

If $(e_j, n) = 1$ we get that n divides g. Let $\mathfrak{G}_s$ be the splitting group of the ideal $\mathfrak{q}_1$. We have $[\mathfrak{G}:\mathfrak{G}_s] = g$, thus $|\mathfrak{G}_s|$ divides $\frac{|\mathfrak{G}|}{n}$, that is the order of the group $\mathfrak{H}$ belonging to field K. Since

$$\left(n, \frac{|\mathfrak{G}|}{n}\right) = \left(n, \frac{|\bar{K}|}{n}\right) = 1$$

it follows from the theorem of Hall, that $\mathfrak{G}_s$ is contained in one of the conjugates of H. Therefore the splitting field F_s of $\mathfrak{q}_1$ contains a conjugate of K and since $q \epsilon P(F_s)$, $q \epsilon P(K)$.

Suppose now that n is square-free and let $\mathfrak{G}_s$ and F_s have the same meaning as before. Since

$$\left(\frac{|\mathfrak{G}|}{n}(e_j, n), \frac{n}{(e_j, n)}\right) = 1$$

there exist in $\mathfrak{G}$, by the theorem of Hall, subgroups of order $\frac{|\mathfrak{G}|}{n}(e_j, n)$ and they are all conjugate. Moreover since $|\mathfrak{G}_s| \mid \frac{|\mathfrak{G}|}{n}(e_j, n)$, $|\mathfrak{G}_s|$ must be contained in one of them, thus F_s must contain a subfield K' of $\bar{K}$ of degree $\frac{n}{(n, e_j)}$.

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

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 $\bar{K}$ be represented as the permutation group on the n fields conjugates to K: $K_1, K_2, \ldots, K_n$. Consider a subfield Ω of $\bar{K}$ belonging to a subgroup $\mathfrak{J}_n$ of $\mathfrak{A}_n$ defined by formula (3). It is clear that if $\mathfrak{H}_{ni}$ denotes the subgroup of $\mathfrak{G}$ belonging to K_i, then

$$\frac{|\mathfrak{J}_n|}{|\mathfrak{J}_n \cap \mathfrak{H}_{ni}|} = \begin{cases} 3 & \text{for } i = 1, 2, 3, \\ 2 & \text{for } i = 4 \text{ or } 5, \\ n-5 & \text{for } i = 6, \ldots, n \end{cases} \quad (n = 5 \text{ or } n \geqslant 8),$$
$$\frac{|\mathfrak{J}_n|}{|\mathfrak{J}_n \cap \mathfrak{H}_{ni}|} = \begin{cases} 5 & \text{for } i \leqslant 5, \\ 2 & \text{for } i = 6 \text{ or } 7 \end{cases} \quad (n = 7). \tag{12}$$

We have

$$\frac{|\mathfrak{J}_n|}{|\mathfrak{J}_n \cap \mathfrak{H}_{ni}|} = \frac{|K_i\Omega|}{|\Omega|}$$

and the equalities (12) mean that $F(x)$ — the polynomial generating K factorizes in Ω into irreducible factors of degrees 3, 2 and $n-5$ ($n = 5$ or $n \geqslant 8$) or 5 and 2 ($n = 7$). It follows by the theorem of Kronecker and Kneser (cf. [7], p. 239) that $f(x)$ — the polynomial generating Ω factorizes in K into irreducible factors of degrees $3\frac{|\Omega|}{n}$, $2\frac{|\Omega|}{n}$ and $(n-5)\frac{|\Omega|}{n}$ ($n = 5$ or $n \geqslant 8$) or $\frac{5}{n}|\Omega|$ and $\frac{2}{n}|\Omega|$ ($n = 7$). The norms of these factors with respect to K are $f^3(x)$, $f^2(x)$, $f^{n-5}(x)$ ($n = 5$ or $n > 8$) and $f^5(x)$,

$f^2(x)$ $(n = 7)$. None of them is $f(x)$, thus $f(x)$ cannot be represented as a norm of a polynomial over K. On the other hand $f(x) = f^3(x)/f^2(x) = f^5(x)/\big(f^2(x)\big)^2$, whence it follows by the multiplicative property of the norm that $f(x)$ is a norm of a rational function over K and so for every integer x, $f(x) = N_{K/Q}(\omega)$ for some $\omega \in K$.

4. LEMMA 2. *Suppose that the hypotheses of Theorem 4 hold. Let*

$$g(x) = cf_1(x)^{e_1}f_2(x)^{e_2}\dots f_m(x)^{e_m}, \tag{13}$$

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

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

is soluble. Then q 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 x_2 with the following properties

$$g(x_2) = N_{K/Q}(\omega) \quad \text{for some } \omega \in K, \tag{14}$$

$$g(x_2) = q^{e_j}ab^{-1}, \quad \text{where } a, b \text{ are integers and } (ab, q) = 1. \tag{15}$$

Let $q = \mathfrak{p}_1\mathfrak{p}_2\dots\mathfrak{p}_l$ be the factorization of q in K, the factors are distinct since q is sufficiently large and let $N_{K/Q}\mathfrak{p}_i = q^{f_i}$. Clearly

$$\sum_{i=1}^{l} f_i = n. \tag{16}$$

Write the prime ideal factorization of ω in K in the form

$$(\omega) = \mathfrak{p}_1^{a_1}\mathfrak{p}_2^{a_2}\dots\mathfrak{p}_l^{a_l}\mathfrak{a}\mathfrak{b}^{-1},$$

where $(\mathfrak{a}\mathfrak{b}, q) = 1$. Then

$$N_{K/Q} = \pm q^{a_1f_1+a_2f_2+\dots+a_lf_l}N_{K/Q}\mathfrak{a}(N_{K/Q}\mathfrak{b})^{-1} \tag{17}$$

and $N_{K/Q}\mathfrak{a}, N_{K/Q}\mathfrak{b}$ are relatively prime to q. It follows from (14), (15) and (17) that

$$a_1f_1 + a_2f_2 + \dots + a_lf_l = e_j.$$

Thus $(f_1, f_2, \dots, f_l)|e_j$ and by (16) $(f_1, f_2, \dots, f_l)|n$. Since $(e_j, n) = 1$, $(f_1, f_2, \dots, f_l) = 1$, q. e. d.

LEMMA 3. *Let $\mathfrak{J}$ be a group of permutations of n letters, where $n = p$ or p^2 (p — prime). If the lengths of orbits of $\mathfrak{J}$ are not coprime there exists in $\mathfrak{J}$ a permutation whose disjoint cycles are of lengths $\lambda_1, \lambda_2, \dots, \lambda_\varrho$ where $(\lambda_1, \lambda_2, \dots, \lambda_\varrho) \neq 1$.*

Proof (due to Sedarshan Sehgal). Let the lengths of orbits of $\mathfrak{J}$ be $l_1, l_2, \dots, l_r$. Since $l_1+l_2+\dots+l_r = n$, if $(l_1, l_2, \dots, l_r) \neq 1$, we must have $p|l_i$ $(i = 1, 2, \dots, r)$. Thus the order of group $\mathfrak{J}$ is divisible by p and it contains a Sylow subgroup S_p. Moreover, the lengths of orbits of S_p are again divisible by p (cf. [8], Theorem 3.4). The number of these orbits r' is $< n/p < p$. Permutations of S_p leave on the average r' letters fixed (ibid. Theorem 3.9). Since the identity fixes n letters there must be a permutation in S_p which fixes less than p letters. Since $|S_p|$ has no prime factor less than p, the permutation in question leaves no letter fixed and all its disjoint cycles must have lengths divisible by p, q. e. d.

Remark. If $n \neq p, p^2$, there exist groups of degree n for which the lemma does not hold, as shown by the following construction. Let $n = pq$, where p — prime and $q > p$. We put

$$\mathfrak{J} = \{P_{\alpha,\beta,\gamma}\}_{\substack{\alpha=1,2,\dots,p\\ \beta=1,2,\dots,p\\ \gamma=1,2,\dots,p(q-p-1)}},$$

where

$$P_{\alpha,\beta,\gamma} = (1, 2, \dots, p)^{\alpha}\prod_{k=1}^{p}\big(kp+1, \dots, (k+1)p\big)^{k\alpha+\beta}(p^2+p+1, \dots, pq)^{\gamma}.$$

The orbits here are $(1, 2, \dots, p), \dots, (p^2+1, \dots, p^2+p)$, $(p^2+p+1, \dots, pq)$, their lengths are therefore all divisible by p. On the other hand, for every triple α, β, γ either $\alpha = p$ or there exists a k such that $1 \leqslant k \leqslant p$ and $k\alpha+\beta = 0 \pmod{p}$. In either case $P_{\alpha,\beta,\gamma}$ leaves at least p letters fixed.

Proof of Theorem 4. Let the Galois group $\mathfrak{G}$ of $\overline{K}$ be represented as a permutation group on the n fields conjugate to K. Let $f_j(x)$ be any one of irreducible factors of $g(x)$ as in (13), Ω_j be a field generated by a root of $f_j(x)$ and $\mathfrak{J}_j$ be a subgroup of $\mathfrak{G}$ belonging to field $\Omega_j \cap \overline{K}$. By the theorem of Hasse quoted in the proof of Theorem 1 for every class $\mathfrak{C} \subset \bigcup\mathfrak{J}$ (summation over all conjugates of $\mathfrak{J}_j$), there exist infinitely many primes $q \in P(\Omega_j)$ such that $\left(\frac{\overline{K}}{q}\right) = \mathfrak{C}$. 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 $\mathfrak{C}$. Thus in every permutation of $\mathfrak{J}_j$, the lengths of the cycles are relatively prime. By Lemma 3 this implies that the lengths of the orbits of $\mathfrak{J}_j$ are relatively prime.

Let $k(x)$ be an irreducible polynomial over Q, whose root generates K. $\mathfrak{J}_j$ is the Galois group of the equation $k(x) = 0$ over Ω_j. The lengths of the orbits of $\mathfrak{I}_j$ are equal to the degrees or irreducible factors of $k(x)$ over Ω_j. Thus

$$k(x) = k_{j1}(x)k_{j2}(x)\ldots k_{jr_j}(x)$$

where k_{ji} is a polynomial irreducible over Ω_j of degree $|k_{ji}|$ and

(18) $$(|k_{j1}|, |k_{j2}|, \ldots, |k_{jr}|) = 1.$$

By the theorem of Kronecker and Kneser it follows that

$$f_j(x) = c_j f_{j1}(x) f_{j2}(x)\ldots f_{jr}(x), \quad \text{where} \quad c_j \in Q,$$

(19) $$f_{ji} \in K[x] \quad \text{and} \quad N_{K/Q} f_{ji}(x) = \left(\frac{f_j(x)}{c_j}\right)^{|k_{ji}|}.$$

In view of (18), there exist integers a_i $(i = 1, 2, \ldots, r)$ such that

(20) $$\sum_{i=1}^{r} a_i |k_{ji}| = 1.$$

We get from (19) and (20)

(21) $$f_j(x) = c_j N_{K/Q} \prod_{i=1}^{r} f_{ji}^{a_i}(x).$$

It follows from (13), (21) and the multiplicative property of the norm that

$$g(x) = aN_{K/Q} h(x), \quad \text{where} \quad h(x) \in K(x).$$

By the hypothesis of the theorem taking x to be a suitable integer, we infer that $a = N_{K/Q}(\alpha)$, where $\alpha \in K$. Putting $\omega(x) = \alpha h(x)$ we obtain $g(x) = N_{K/Q}(\omega(x))$, identically, q. e. d.

LEMMA 4. *The class number of the* $K = Q(\sqrt{2\cos\frac{2}{7}\pi})$ *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 $\Omega = Q(2\cos\frac{2}{7}\pi)$ is a cyclic field of discriminant 7^2. 2 remains a prime in this field, hence $2\cos\frac{2}{7}\pi = (2\cos\frac{8}{7}\pi)^2 - 2$ is in Ω a quadratic non-residue mod 4. Since $2\cos\frac{2}{7}\pi$ is a unit, it follows by the conventional methods that $1, \sqrt{2\cos\frac{2}{7}\pi}$ is an integral basis for K over Ω, thus $d_{K/\Omega}$ equals $(8\cos\frac{2}{7}\pi)$ and for the discriminant of K we obtain a value

$$d_{K/Q} = d_{\Omega/Q}^2 N_{\Omega/Q}(d_{K/\Omega}) = 2^6\cdot 7^4.$$

This number coincides with the discriminant of $f(x^2)$, which has $\sqrt{2\cos\frac{2}{7}\pi}$ 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

$$(2) = \mathfrak{P}_1^2, \qquad N\mathfrak{P}_1 = 8,$$
$$(3) = \mathfrak{P}_2\mathfrak{P}_3, \qquad N\mathfrak{P}_2 = N\mathfrak{P}_3 = 3^3,$$
$$(5) = \mathfrak{P}_4\mathfrak{P}_5, \qquad N\mathfrak{P}_4 = N\mathfrak{P}_5 = 5^3,$$
$$(7) = \mathfrak{P}_6^3\mathfrak{P}_7^3, \qquad N\mathfrak{P}_6 = N\mathfrak{P}_7 = 7.$$

Now, by the theorem of Minkowski, in every class of ideals of K there is an ideal with norm not exceeding

$$\left(\frac{4}{\pi}\right)^2 \frac{6!}{6^6}\sqrt{d_{K/Q}} < 11.$$

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

$$(2) = \left(2\cos\tfrac{8}{7}\pi + \sqrt{2\cos\tfrac{8}{7}\pi}\right)^2,$$
$$(7) = \left(1 + 2\cos\tfrac{8}{7}\pi + \sqrt{2\cos\tfrac{2}{7}\pi}\right)^3\left(1 + 2\cos\tfrac{8}{7}\pi - \sqrt{2\cos\tfrac{2}{7}\pi}\right)^3.$$

Proof of Theorem 5. Since the degree of $f(x)$ is not divisible by 6, $f(x)$ cannot be represented as $N_{K/Q}(\omega(x))$, where $\omega(x) \in K(x)$. It remains to show that for every integer x, $f(x) = N_{K/Q}(\omega)$ for some integer $\omega \in K$. Let

(22) $$f(x) = \pm p_1^{a_1} p_2^{a_2} \ldots p_k^{a_k}$$

where a_i are positive integers. Since the discriminant of $\Omega = Q(2\cos\frac{2}{7}\pi)$ 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 Ω. Since

$$(2\cos\tfrac{2}{7}\pi)(2\cos\tfrac{4}{7}\pi)(2\cos\tfrac{8}{7}\pi) = 1,$$

at least one of the factors on the left hand side is a quadratic residue mod $\mathfrak{P}_i$. It follows that for some $x_0 \in \Omega$

$$f(x_0^2) = (x_0^2 - 2\cos\tfrac{2}{7}\pi)(x_0^2 - 2\cos\tfrac{4}{7}\pi)(x_0^2 - 2\cos\tfrac{8}{7}\pi) \equiv 0 \pmod{\mathfrak{P}_i}.$$

Since $\mathfrak{P}_i$ is of first degree, there exists a rational integer x_1 such that $x_1 \equiv x_0 \pmod{\mathfrak{P}_i}$ and we get $f(x_1^2) \equiv 0 \pmod{p_i}$. By Lemma 4, $p_i \in P(K)$ and since every ideal of K is principal,

(23) $$p_i = \pm N_{K/Q}\,\omega_i,$$

where ω_i is an integer of K. Since

$$-1 = N_{K/Q}(\sqrt{2\cos\tfrac{2}{7}\pi}),$$

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 $F(x, y)$ 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 Bauerian. 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. Tschebotaröw 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

ACTA ARITHMETICA
XI (1966)

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 $P(\Omega) \leqslant P(K)$.

In the preceding paper [8], one of us has characterized all the fields K for which $P(\Omega) \leqslant P(K)$ implies that Ω 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 $\left(\frac{|\bar{K}|}{|K|}, |K|\right) = 1$ (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 Ω are algebraic number fields and K has property* (N) *then $P(\Omega) \leqslant P(K)$ implies that Ω 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 | | denote both the degree of the field over Q and the order of the group.