powers. This requires modifications of some of the results leading to the estimate of the singular series $\mathcal{S}$.

References

[1] R. Ayoub, *An Introduction to the Analytic Theory of Numbers*, Providence, Rhode Island, 1963.

[2] L. Carlitz, *On the representation of a polynomial in a Galois field as the sum of an even number of squares*, Trans. Amer. Math. Soc. 35 (1933), pp. 397–410.

[3] — *On the representation of a polynomial in a Galois field as the sum of an odd number of squares*, Duke Math. Journ. 1 (1935), pp. 298–315.

[4] — *Sums of squares of polynomials*, Duke Math. Journ. 3 (1937), pp. 1–7.

[5] — *The singular series for sums of squares of polynomials*, Duke Math. Journ. 14 (1947), pp. 1105–1120.

[6] Eckford Cohen, *Sums of an even number of squares in* GF$[p^n, x]$, Duke Math. Journ. 14 (1947), pp. 251–267.

[7] — *Sums of an even number of squares in* GF$[p^n, x]$, *II*, Duke Math. Journ. 14 (1947), pp. 543–557.

[8] D. R. Hayes, *A polynomial analog of the Goldbach conjecture*, Bull. Amer. Math. Soc. 69 (1963), pp. 115–116.

[9] — *The expression of a polynomial as a sum of three irreducibles*, Acta Arith. 11 (1966), pp. 461–488.

[10] R. E. A. C. Paley, *Theorems on polynomials in a Galois field*, Quart. Journ. Math. 4 (1933), pp. 52–63.

[11] Stefan Schwarz, *On Waring's problem for finite fields*, Quart. Journ. Math. 19 (1948), pp. 123–128.

[12] L. Tornheim, *Sums of n^{th} powers in fields of prime characteristic*, Duke Math. Journ. 4 (1938), pp. 359–362.

WASHINGTON STATE UNIVERSITY

Received on 6. 12. 1971 (241)

ACTA ARITHMETICA
XXII (1973)

On a theorem of Bauer and some of its applications II

by

A. Schinzel (Warszawa)

The aim of this paper is to extend to polynomials in many variables the results of papers [1] and [6]. It is convenient to first restate these results in a concise form.

Let K be an algebraic number field, $|K|$ its degree, $\bar{K}$ its normal closure. We denote by $P(K)$ the set of primes which have in K at least one prime ideal factor of the first degree, and by $N_{K/Q}$ the norm from K to the rational field Q. We say that K *has property* (P) if for all but finitely many primes q and for every $\omega \in K$ $\left(\operatorname{ord}_q N_{K/Q}(\omega), |K|\right) = 1$ implies $q \in P(K)$. A field K is called *Bauerian* if for every Ω, $P(\Omega) \leqslant P(K)$ implies that Ω contains one of the conjugates of K ($P(\Omega) \leqslant P(K)$ means that $P(\Omega) \setminus P(K)$ is finite).

Several types of Bauerian fields have been described in [6], it happens so that all those fields have property (P). For some of them (cubic and quartic fields, solvable fields K with $\left(\frac{|\bar{K}|}{|K|}, |K|\right) = 1$) this has been established in the course of proof of Lemma 1 ([6]) for the others (certain solvable fields of degree p^2) it follows from Lemma 3 and Theorem 4 below. For normal fields the fact is obvious and for Bauerian fields of the types described in [4] (fields with property (N), fields $Q(\sqrt[n]{A})$ with $n \not\equiv 0 \bmod 8$) it is also true (see Corollary 2 and p. 230). In Theorem 5 I give a new class of Bauerian fields (normal extensions of quadratic fields) which need not have property (P).

Apart from the description of Bauerian fields, from Theorem 1 of [1] which has been generalized in [5] and various counterexamples the results of papers [1] and [6] can be summarized as follows.

Theorem A. *If K is a cyclic field or a solvable field such that $|K|$ is squarefree and $\left(\frac{|\bar{K}|}{|K|}, |K|\right) = 1$, $f(x) \in Q[x]$ and in every arithmetic progression there is an integer x such that*

$$f(x) = N_{K/Q}(\omega), \qquad \omega \in K,$$

then

$$f(x) = N_{K/Q}\big(\varphi(x)\big), \quad \textit{where} \quad \varphi(x) \in K[x].$$

THEOREM B. *If K is a Bauerian field with property* (P), *$f(x) \in Q[x]$, the multiplicity of each zero of f is relatively prime to $|K|$ and in every arithmetic progression there is an integer x such that*

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

then

$$f(x) = N_{K/Q}\big(\varphi(x)\big), \quad \textit{where} \quad \varphi(x) \in K[x].$$

THEOREM C. *If K is any field of degree p or p^2 (p prime), $f(x) \in Q(x)$, the multiplicity of each zero and pole of f is relatively prime to $|K|p^{-1}$ and in every arithmetic progression there is an integer x such that*

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

then

$$f(x) = N_{K/Q}\big(\varphi(x)\big), \quad \textit{where} \quad \varphi(x) \in K(x).$$

The proof of all these theorems passes through the same stage which we formulate below as

LEMMA 1. *Let K and the multiplicities of the factors of f satisfy the assumptions of Theorems* A, B *or* C. *If for every integer x and every prime q there exists $\omega \in K$ such that*

$$\operatorname{ord}_q f(x) = \operatorname{ord}_q N_{K/Q}(\omega)$$

(provided the left hand side is defined) and f_1 is an irreducible factor of f then

$$f_1(x)^e = aN_{K/Q}\big(\varphi(x)\big),$$

where $a \in Q$, $\varphi(x) \in K[x]$ and $e = \operatorname{ord}_{f_1} f$ in case A, B, *$(e, |K|) = (\operatorname{ord}_{f_1} f, |K|)$ in case* C.

We generalize Theorems A, B and C as follows.

THEOREM 1. *If K is a cyclic field or a solvable field such that $|K|$ is squarefree and $\left(|K|, \dfrac{|\overline{K}|}{|K|}\right) = 1$, $f \in Q[x_1, \ldots, x_k]$ and for any arithmetic progressions $P_1, \ldots, P_k$ there are integers $x_1, \ldots, x_k$, such that* for *$x_i \in P_i$ $(1 \leqslant i \leqslant k)$*

$$f(x_1, \ldots, x_k) = N_{K/Q}(\omega), \quad \omega \in K,$$

then

$$f(x_1, \ldots, x_k) = N_{K/Q}\big(\varphi(x_1, \ldots, x_k)\big), \quad \varphi(x_1, \ldots, x_k) \in K[x_1, \ldots, x_k].$$

THEOREM 2. *If K is a Bauerian field with property* (P), *$f \in Q[x_1, \ldots, x_k]$, the multiplicity of each irreducible factor of f is relatively prime to $|K|$ and for any arithmetic progressions $P_1, \ldots, P_k$ there are integers $x_1, \ldots, x_k$ such that $x_i \in P_i$*

$$f(x_1, \ldots, x_k) = N_{K/Q}(\omega), \quad \omega \in K,$$

then

$$f(x_1, \ldots, x_k) = N_{K/Q}\big(\varphi(x_1, \ldots, x_k)\big), \quad \varphi \in K[x_1, \ldots, x_k].$$

THEOREM 3. *If K is any field of degree p or p^2 (p prime), $f \in Q[x_1, \ldots, x_k]$, the multiplicity of each irreducible factor of f is relatively prime to $|K|p^{-1}$ and for any arithmetic progressions $P_1, \ldots, P_k$ there are integers $x_1, \ldots, x_k$, such that $x_i \in P_i$ $(1 \leqslant i \leqslant k)$,*

$$f(x_1, \ldots, x_k) = N_{K/Q}(\omega), \quad \omega \in K,$$

then

$$f(x_1, \ldots, x_k) = N_{K/Q}\big(\varphi(x_1, \ldots, x_k)\big), \quad \varphi \in K(x_1, \ldots, x_k).$$

All the three theorems can be deduced from Lemma 1 by means of Hilbert's Irreducibility Theorem. The idea of using Hilbert's theorem in this connection is due to H. Davenport.

We prove first a generalization of Lemma 1.

LEMMA 2. *Let K and the multiplicities of the factors of f satisfy the assumptions of Theorem* 1, 2 *or* 3. *If for any integers $x_1, \ldots, x_k$ and every prime q there exists $\omega \in K$ such that*

$$\operatorname{ord}_q f(x_1, \ldots, x_k) = \operatorname{ord}_q N(\omega)$$

(provided the left hand side is defined) and f_1 is an irreducible factor of f then

$$f_1(x_1, \ldots, x_k)^e = aN_{K/Q}\big(\varphi(x_1, \ldots, x_k)\big),$$

where $a \in Q$, $\varphi \in K[x_1, \ldots, x_k]$ and $e = \operatorname{ord}_{f_1} f$ in case 1 *and* 2, *$(e, |K|) = (\operatorname{ord}_{f_1} f, |K|)$ in case* 3.

Proof. Let

$$f = cf_1^{e_1} f_2^{e_2} \ldots f_m^{e_m} \tag{1}$$

and

$$f_1 = c_1 \varphi_1^{\varepsilon_1} \varphi_2^{\varepsilon_2} \ldots \varphi_n^{\varepsilon_n} \tag{2}$$

be the factorization of f and f_1 into irreducible factors in Q and K respectively. We have

$$N_{K/Q}\varphi_l(x_1, \ldots, x_k) = \gamma_l f_1(x_1, \ldots, x_k)^{\delta_l}. \tag{3}$$

We may assume without loss of generality that x_k really occurs in f_1. Denote the coefficient of the highest power of x_k in f_1 by $h(x_1, \ldots, x_{k-1}) \neq 0$ and the discriminant of $f_1 f_2 \ldots f_m$ with respect to x_k by $D(x_1, \ldots, x_{k-1})$. By Hilbert's Irreducibility Theorem there exist integers x_i' $(1 \leqslant i < k)$ such that $h(x_1', \ldots, x_{k-1}')\,D(x_1', \ldots, x_{k-1}') \neq 0$, $f_j(x_1', \ldots, x_{k-1}', x_k)$ are irreducible in Q and $\varphi_l(x_1', \ldots, x_{k-1}', x_k)$ are irreducible in K as polynomials in x_k $(1 \leqslant j \leqslant m,\ 1 \leqslant l \leqslant n)$. Therefore by (1), in case 2 or 3 the multiplicity of each factor of $f(x_1', \ldots, x_{k-1}', x_k)$ is relatively prime to $|K|$ or $|K|p^{-1}$, respectively. On the other hand, for every integer x_k and every prime q there exists $\omega \in K$ such that

$$\operatorname{ord}_q f(x_1', \ldots, x_{k-1}', x_k) = \operatorname{ord}_q N_{K/Q}(\omega)$$

(provided the left hand side is defined). By Lemma 1 we infer

$$f_1(x_1', \ldots, x_{k-1}', x_k)^e = \alpha' N_{K/Q}\big(\varphi'(x_k)\big), \tag{4}$$

where $\alpha' \in Q$, $\varphi' \in K[x_k]$ and $e = \operatorname{ord}_{f_1} f$ in case 1, and 2, $(e, |K|) = (\operatorname{ord}_{f_1} f, |K|)$ in case 3. In virtue of (2) and of the choice of x_i' $(1 \leqslant i < k)$ we have for some nonnegative integers $\eta_1, \ldots, \eta_n$ and some $\beta \in K$

$$\varphi'(x_k) = \beta \prod_{l=1}^{n} \varphi_l(x_1', \ldots, x_{k-1}', x_k)^{\eta_l}. \tag{5}$$

It follows from (3), (4) and (5) that

$$f_1(x_1', \ldots, x_{k-1}', x_k)^e = \alpha' N_{K/Q}(\beta) \prod_{l=1}^{n} \gamma_l^{\eta_l} f_1(x_1', \ldots, x_{k-1}', x_k)^{\delta_l \eta_l}. \tag{6}$$

Since $h(x_1', \ldots, x_{k-1}') \neq 0$, $f_1(x_1', \ldots, x_{k-1}', x_k)$ is not constant and (6) implies $\sum_{l=1}^{n} \delta_l \eta_l = e$, which proves the lemma with $\varphi = \prod_{l=1}^{n} \varphi_l^{\eta_l}$.

Proof of Theorems 1, 2 and 3. Let

$$f(x_1, \ldots, x_k) = \frac{g(x_1, \ldots, x_k)}{h(x_1, \ldots, x_k)},$$

where the polynomials g and h have integer coefficients and $(g, h) = 1$. Take any k integers $x_1, \ldots, x_k$ such that $h(x_1, \ldots, x_k) \neq 0$. If

$$g(x_1, \ldots, x_k) = 0$$

we have for any prime q

$$\operatorname{ord}_q f(x_1, \ldots, x_k) = \infty = \operatorname{ord}_q N_{K/Q}(0).$$

If $g(x_1, \ldots, x_k) \neq 0$ set

$$\operatorname{ord}_q g(x_1, \ldots, x_k) = \mu, \qquad \operatorname{ord}_q h(x_1, \ldots, x_k) = \nu.$$

By the assumptions there exist integers $t_1, \ldots, t_k$ such that

$$f(x_1 + q^{\mu+\nu+1} t_1, \ldots, x_k + q^{\mu+\nu+1} t_k) = N_{K/Q}(\omega), \qquad \omega \in K.$$

Hence

$$\begin{aligned} N_{K/Q}(\omega) &= \operatorname{ord}_q g(x_1 + q^{\mu+\nu+1} t_1, \ldots, x_k + q^{\mu+\nu+1} t_k) - \\ &\qquad\qquad - \operatorname{ord}_q h(x_1 + q^{\mu+\nu+1} t_1, \ldots, x_k + q^{\mu+\nu+1} t_k) \\ &= \operatorname{ord}_q g(x_1, \ldots, x_k) - \operatorname{ord}_q h(x_1, \ldots, x_k) = \operatorname{ord}_q f(x_1, \ldots, x_k). \end{aligned}$$

Let (1) be the factorization of f into irreducible factors in Q. By Lemma 2 we have for each $j \leqslant m$

$$f_j(x_1, \ldots, x_k)^{e'_j} = \alpha_j N_{K/Q}\big(\varphi_j(x_1, \ldots, x_k)\big),$$

where $a_j \in Q$, $\varphi_j \in K[x_1, \ldots, x_k]$ and $e_j' = e_j$ in case 1 and 2, $(e_j', |K|) = (e_j, |K|)$ in case 3. In the last case there exist integers a_j and b_j such that

$$e_j' a_j - |K| b_j = e_j.$$

It follows

$$f_j(x_1, \ldots, x_k)^{e_j} = a_j^{a_j} N_{K/Q}\big(\varphi_j(x_1, \ldots, x_k)^{a_j} f_j(x_1, \ldots, x_k)^{-b_j}\big)$$

and we obtain from (1)

$$f(x_1, \ldots, x_k) = \begin{cases} c \prod_{j=1}^{m} a_j N_{K/Q}\Big(\prod_{j=1}^{m} \varphi_j(x_1, \ldots, x_k)\Big) & \text{in case 1 and 2,} \\ c \prod_{j=1}^{m} a_j^{a_j} N_{K/Q}\Big(\prod_{j=1}^{m} \varphi_j(x_1, \ldots, x_k)^{a_j} f_j(x_1, \ldots, x_k)^{-b_j}\Big) & \text{in case 3.} \end{cases}$$

Choosing $x_1, \ldots, x_k$ so that $f(x_1, \ldots, x_k) = N_{K/Q}(\omega) \neq 0$ we infer that $c\prod_{j=1}^{m} a_j$ or $c\prod_{j=1}^{m} a_j^{a_j}$ in case 1 and 2 or 3 respectively, is a norm of an element of K and the theorems follow.

It seems more difficult to generalize to polynomials in many variables the results of [2]. In particular I do not know, whether the solubility in rationals x, y of an equation

$$a(t, u)x^2 + b(t, u)y^2 = 1$$

for all integer values of t, u implies the existence of rational functions $\varphi(t, u)$, $\psi(t, u)$ such that identically

$$a(t, u)\varphi^2(t, u) + b(t, u)\psi^2(t, u) = 1.$$

Now we shall prove a result on fields of degree p^2 announced in the introduction. We show first

LEMMA 3. *Let the Galois group $\mathfrak{G}$ of $\overline{K}$ be represented as permutation group on the conjugates of K. The field K has property* (P) *if and only if every permutation of $\mathfrak{G}$ for which the lengths of cycles are relatively prime fixes at least one element.*

Proof. Necessity. Suppose that a permutation σ of $\mathfrak{G}$ has the cycles of lengths $f_1, \ldots, f_k$ and $(f_1, \ldots, f_k) = 1$. By Čebotarev's density theorem there exist infinitely many primes q not dividing the discriminant of K such that $\left(\frac{\overline{K}}{q}\right)$ is the class of σ. By the well known Artin's result (see [3], p. 126) these primes factorize in K into prime ideals of degrees $f_1, \ldots, f_k$. Let $q = \mathfrak{q}_1 \ldots \mathfrak{q}_k$, where $\mathfrak{q}_i$ is of degree f_i. Since $(f_1, \ldots, f_k) = 1$ there exist integers $\alpha_1, \ldots, \alpha_k$ such that

$$\alpha_1 f_1 + \ldots + \alpha_k f_k = 1,$$

there exists also an ideal $\mathfrak{a}$ relatively prime to q such that the ideal $\mathfrak{q}_1^{a_1}\cdot\ldots\cdot\mathfrak{q}_k^{a_k}\mathfrak{a}$ is principal equal (ω), say. Then

$$\operatorname{ord}_q N_{K/Q}(\omega) = 1$$

and by the assumption at least one of the numbers $f_1, \ldots, f_k$ is 1.

Sufficiency. Suppose that q does not divide the discriminant of K and

$$(7) \qquad \left(\operatorname{ord}_q N_{K/Q}(\omega),\, |K|\right) = 1.$$

Let $\mathfrak{q}_1, \mathfrak{q}_2, \ldots, \mathfrak{q}_l$ be all the prime ideal factors of q in K and let

$$(\omega) = \mathfrak{q}_1^{a_1}\ldots\mathfrak{q}_l^{a_l}\mathfrak{a}\mathfrak{b}^{-1},$$

where $(\mathfrak{a}\mathfrak{b}, q) = 1$. If $\mathfrak{q}_i$ is of degree f_i we have

$$\operatorname{ord}_q N_{K/Q}(\omega) = a_1 f_1 + \ldots + a_l f_l$$

and since $f_1 + \ldots + f_l = |K|$, by (7)

$$(8) \qquad (f_1, \ldots, f_l) = 1.$$

By Artin's theorem quoted above, any permutation σ of $\mathfrak{G}$ belonging to $\left(\dfrac{\overline{K}}{q}\right)$ factorizes into cycles of the lengths $f_1, \ldots, f_l$. By (8) and the assumption one of these lengths is 1, thus $q \in P(K)$.

COROLLARY 1. *Every field K with the Galois group of $\overline{K}$ being a p-group has property* (P).

Proof. It is clear that the lengths of cycles of the permutations in question can only be powers of p.

COROLLARY 2. *Every pure field $K = Q(\sqrt[m]{A})$ has property* (P).

Proof. The Galois group of $\overline{K}$ can be represented by permutations of residue classes mod m given by $\sigma(x) \equiv ax + b \pmod{m}$. Suppose that for some f: $\sigma^f(x) = x$. Then

$$\frac{a^f - 1}{a - 1}\left((a-1)x + b\right) \equiv 0 \bmod m$$

and

$$(a-1, m) \mid b\,\frac{a^f - 1}{a - 1}.$$

If the lengths of the cycles of σ: $f_1, \ldots, f_k$ are relatively prime then

$$(a-1, m) \mid b\,\frac{a^{f_i} - 1}{a - 1} \qquad (i = 1, \ldots, k)$$

implies

$$(a-1, m) \mid b,$$

and $\sigma(x) = x$ is soluble.

Corollary 1 establishes property (P) for one class of Bauerian fields of degree p^2 found by P. Roquette and mentioned in [6]. For the other class found by L. Alperin (primitive solvable fields of degree p^2, $p > 3$) the same holds in virtue of

THEOREM 4. *Let K be a field of degree p^k (p prime) and assume that the Galois group $\mathfrak{G}$ of $\overline{K}$ represented as a permutation group on the points of* $\mathrm{GF}[p]^k$ *consists of affine transformations. Then K has property* (P) *and if $k \leqslant 2$ or $k = 3$, $p = 2$ it is Bauerian. For $k \geqslant 3$, $p \geqslant 3$ or $k \geqslant 4$ there are non-Bauerian fields of this type.*

Proof. Let σ be a permutation of the points of $\mathrm{GF}[p]^k$ given by an affine transformation. If the lengths of cycles of σ are relatively prime, one of them is not divisible by p. Let the relevant cycle be $(p_1, \ldots, p_l)$. Then

$$(9) \qquad \sigma\Big(l^{-1}\sum_{i=1}^{l} p_i\Big) = l^{-1}\sum_{i=1}^{l}\sigma(p_i) = l^{-1}\sum_{i=1}^{l} p_i,$$

thus σ has a fixed point.

Assume now that $k \leqslant 2$ and $\mathfrak{J}$ is a subgroup of $\mathfrak{G}$ contained in the union of stability subgroups. If the lengths of orbits of $\mathfrak{J}$ were not coprime then by Lemma 3 of [6] there would exist in $\mathfrak{J}$ a permutation with the lengths of cycles non coprime, against the assumption. Therefore the lengths of orbits are coprime and one of them is not divisible by p. Let the relevant orbit be $(p_1, \ldots, p_l)$. Then for any σ from $\mathfrak{J}$ the formula (9) holds and $\mathfrak{J}$ is contained in the stabilizer of $l^{-1}\sum_{i=1}^{l} p_i$. It follows by Theorem 1 of [6] that K is a Bauerian field.

Now, let $k = 3$, $p = 2$ and let $\mathfrak{J}$ have its former meaning. If the lengths of orbits of $\mathfrak{J}$ are coprime the former argument applies. Otherwise all lengths are even and by Theorem 3.4 of [8], a Sylow 2-subgroup S of $\mathfrak{J}$ has also all orbits of even length. Since S is contained in the union of stability subgroups it is not cyclic and does not contain any translation. It follows that S is of order 4 or 8. The computation shows that all groups of order 8 of affine transformations of $\mathrm{GF}[2]^3$ without translations are of the form $\sigma\langle\sigma_1, \sigma_2\rangle\sigma^{-1}$, where

$$\sigma_1(\boldsymbol{x}) = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}\boldsymbol{x} + \begin{bmatrix} 0 \\ 0 \\ a \end{bmatrix}, \qquad \sigma_2(\boldsymbol{x}) = \begin{bmatrix} 1 & 0 & b \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}\boldsymbol{x} + \begin{bmatrix} c \\ (b+1)a \\ 0 \end{bmatrix}.$$

If $\sigma^{-1}S\sigma$ contains σ_1^2 and σ_2 then the existence of fixed points of these transformations implies that $a = c = 0$ and S has the fixed point $\sigma(0, 0, 0)$. Otherwise $\sigma^{-1}S\sigma$ is the group of order 4 generated by σ_1^2 and $\sigma_2\sigma_1$, where

$$\sigma_2\sigma_1(\boldsymbol{x}) = \begin{bmatrix} 1 & 1 & b+1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}\boldsymbol{x} + \begin{bmatrix} ba + c \\ ba \\ a \end{bmatrix}.$$

We infer again that $a = 0$ and S has the fixed point $\sigma(0, c, 0)$. The contradiction obtained shows that K is a Bauerian field.

If $k \geqslant 3$, $p \geqslant 3$ consider the group $\mathfrak{J} = \{\sigma_{i,j}\}$, where

$$\sigma_{i,j}\colon\ y_1 = x_1 + jx_2 + \left(\binom{j}{2} + i\right)x_3 + i,\ y_2 = x_2 + jx_3,\ y_i = x_i\ (3 \leqslant i \leqslant k).$$

(We have $\sigma_{i_1,j_1}\sigma_{i_2,j_2} = \sigma_{i_1+i_2,j_1+j_2}$.) All fixed points of $\sigma_{i,j}$ are given by $x_2 = -ij^{-1}$, $x_3 = 0$ if $j \neq 0$ and $x_3 = -1$ if $j = 0$, thus $\mathfrak{J}$ has no fixed point. Taking for $\mathfrak{G}$ the group generated by $\mathfrak{J}$ and all the translations we get corresponding to a stability subgroup of $\mathfrak{G}$ a solvable field of degree p^k which is not Bauerian.

If $k \geqslant 4$ consider the group $\mathfrak{J} = \{1, \sigma_1, \sigma_2, \sigma_3\}$, where σ_i are the following affine transformations of $\mathrm{GF}[2]^k$:

$$\sigma_1\colon\ y_1 = x_1 + x_2 + x_3 + 1,\ y_i = x_i\ (2 \leqslant i \leqslant k),$$
$$\sigma_2\colon\ y_1 = x_1 + x_4,\ y_2 = x_3,\ y_3 = x_2,\ y_i = x_i\ (4 \leqslant i \leqslant k),$$
$$\sigma_3\colon\ y_1 = x_1 + x_2 + x_3 + x_4 + 1,\ \ y_2 = x_3,\ y_3 = x_2,\ y_i = x_i\ (4 \leqslant i \leqslant k).$$

Each σ_i has fixed points but there is none in common.

Taking for $\mathfrak{G}$ the group generated by $\mathfrak{J}$ and all the translations, we get corresponding to a stability subgroup of $\mathfrak{G}$ a solvable field of degree 2^k which is not Bauerian.

Remark. The assertion of Theorem 4 concerning property (P) is a special case of the following theorem due to Professor H. Wielandt (written communication). *If a permutation group $\mathfrak{G}$ of prime power degree p^k has a regular normal subgroup (regular means that it is transitive and stabilizer of any point is trivial) then every element of $\mathfrak{G}$ whose cycle lengths are coprime has a fixed point.*

COROLLARY 3. *Every primitive solvable field of degree p^k (p prime) has property* (P) *and if $k \leqslant 2$ or $k = 3$, $p = 2$ it is Bauerian.*

Proof. If K is a primitive solvable field of degree p^k then the Galois group of $\overline{K}$ represented as permutation group on $\mathrm{GF}[p]^k$ consists of affine transformations (see [7], p. 364).

Imprimitive solvable fields of degree p^2 need neither be Bauerian nor have property (P). It is shown by the example of a field K of degree 9 with the Galois group of $\overline{K}$ being the wreath product of S_3 acting on three isomorphic copies of S_3. It remains unsettled whether every primitive solvable field is Bauerian.

THEOREM 5. *Every normal extension of a quadratic field is Bauerian. There are fields of this type without property* (P).

Proof. Let K be a normal extension of a quadratic field L and $\overline{K}$ the normal closure of K. We can assume that $\overline{K} \neq K$. Let $\mathfrak{G}$ be the Galois group of $\overline{K}$ and $\mathfrak{H}, \mathfrak{N}$ the subgroups of $\mathfrak{G}$ corresponding to K and L, respectively. By the assumption $\mathfrak{H}$ is a normal subgroup of $\mathfrak{N}$, and since $\mathfrak{N}$ is of index two in $\mathfrak{G}$ there is only one subgroup of $\mathfrak{G}$ conjugate to $\mathfrak{H}$ and different from it; let us denote it by $\mathfrak{H}'$. If the field K were not Bauerian then by Theorem 1 of [6] one could find a subgroup $\mathfrak{J}$ of $\mathfrak{G}$ such that

$$\mathfrak{J} \subset \mathfrak{H} \cup \mathfrak{H}', \qquad \mathfrak{J} \not\subset \mathfrak{H}, \qquad \mathfrak{J} \not\subset \mathfrak{H}'. \tag{10}$$

On taking

$$j_1 \in \mathfrak{J} \setminus \mathfrak{H} \subset \mathfrak{H}', \quad j_2 \in \mathfrak{J} \setminus \mathfrak{H}' \subset \mathfrak{H}$$

one obtains

$$j_1 j_2 \in \mathfrak{J} \setminus \mathfrak{H} \setminus \mathfrak{H}'$$

which contradicts (10).

Consider now a group $\mathfrak{G}$ consisting of the following permutations $\sigma_{a,b}$ of residue classes mod12:

$$\sigma_{a,b}(2n) \equiv 2n + a \pmod{12}, \qquad \sigma_{a,b}(2n+1) \equiv 2n + 1 + b \pmod{12}$$
$$(0 \leqslant n \leqslant 5),$$

where (a, b) runs through all pairs of residues mod12 of the same parity. This group is transitive and it has an abelian subgroup of index two namely $\mathfrak{N} = \{\sigma_{a,b}\colon\ a \equiv b \equiv 0 \bmod 2\}$. Therefore there exists an algebraic number field Ω with $\mathfrak{G}$ as its Galois group. The stability subgroups

$$\mathfrak{H} = \{\sigma_{a,0}\colon\ a \equiv 0 \bmod 2\} \quad \text{and} \quad \mathfrak{H}' = \{\sigma_{0,b}\colon\ b \equiv 0 \bmod 2\}$$

are normal subgroups of $\mathfrak{N}$. Thus the subfield K of Ω corresponding to $\mathfrak{H}$ is Bauerian. On the other hand it does not possess property (P) since

$$\sigma_{4,6} = (0, 4, 8)(1, 7)(2, 6, 10)(3, 9)(5, 11);$$

the lengths of cycles are relatively prime but none of them is 1.

Finally we prove that for fields K without property (P) Theorem B and *a fortiori* Theorem 2 does not hold.

THEOREM 6. *If a field K does not possess property* (P) *then there exists an irreducible polynomial $f(x)$ such that for every integer x $f(x) = N_{K/Q}(\omega)$ with $\omega \in K$ but for no polynomial $\varphi(x) \in K[x]$*

$$f(x) = N_{K/Q}\big(\varphi(x)\big). \tag{11}$$

Proof. Let $\mathfrak{G}$ be the Galois group of $\overline{K}$ represented as the permutation group on the conjugates of K and $\mathfrak{H}$ be the subgroup of $\mathfrak{G}$ corresponding to K. Let $\sigma \in \mathfrak{G}$ have the cycles of lengths $f_1, \ldots, f_k$, where $(f_1, \ldots, f_k) = 1$ and $f_i > 1$ $(1 \leqslant i \leqslant k)$. To the group $\mathfrak{J}$ generated by σ there corresponds a field Ω, say.

Let $\Omega = Q(\vartheta)$ and f be the minimal polynomial of ϑ. Assume (11). Then for a certain $\tau \in \mathfrak{G}$ we have $\varphi^{(\tau)}(\vartheta) = 0$ and for a suitable $i \leqslant k$

$$|\mathfrak{J} \cap \tau\mathfrak{H}\tau^{-1}| = \frac{|\mathfrak{J}|}{f_i}.$$

Hence

$$\frac{|\Omega K^{(\tau)}|}{|K^{(\tau)}|} = \frac{|\mathfrak{H}|}{|\mathfrak{J}\cap\tau\mathfrak{H}\tau^{-1}|} = \frac{|\mathfrak{H}|}{|\mathfrak{J}|}f_i = \frac{|\Omega|}{|K|}f_i$$

and it follows that $\varphi^{(\tau)}(x)$ is of degree $\frac{|\Omega|}{|K|}f_i$. By comparison of degrees we get

$$N_{K/Q}(\varphi(x)) = f(x)^{f_i},$$

which contradicts (11) since $f_i > 1$. On the other hand, since $(f_1, \ldots, f_k) = 1$ there exist integers $a_1, \ldots, a_k$ such that

$$a_1f_1 + \ldots + a_kf_k = 1.$$

Hence

$$N_{K/Q}(\varphi_i(x)^{a_i}) = f(x),$$

which proves that for every integer x, $f(x) = N_{K/Q}(\omega)$ for some $\omega \in K$.

It follows by Theorem 3 of [4] that property (N) implies property (P).

Note added in proof. 1. Theorem 4 suggests the following question about the family F_Ω of groups of affine transformations of Ω^2, where Ω is a field: If every element of $\mathfrak{G} \in F_\Omega$ has a fixed point, is there a fixed point for the whole $\mathfrak{G}$? If $\Omega = GF[p]$ the answer is affirmative by the said theorem. If Ω is not simple the answer is negative and a counterexample is given by the abelian group $\mathfrak{G}_0 = \{\sigma_a \colon a \in \Omega\}$, where

$$\sigma_a(\boldsymbol{x}) = \begin{bmatrix}1 & a\\ 0 & 1\end{bmatrix}\boldsymbol{x} + \begin{bmatrix}f(a)\\ 0\end{bmatrix}$$

and where f is a nontrivial solution of the equation $f(x+y) = f(x)+f(y)$ in Ω. In the remaining case $\Omega = Q$ the answer is again negative and a more recondite counterexample is given by

$$\mathfrak{G}_1 = \left\langle \begin{bmatrix}2 & 3\\ 3 & 5\end{bmatrix}\boldsymbol{x},\ \begin{bmatrix}2 & 1\\ 1 & 1\end{bmatrix}\boldsymbol{x} + \begin{bmatrix}1\\ 0\end{bmatrix}\right\rangle.$$

$\mathfrak{G}_1$ clearly has no fixed point. The existence of fixed points for all elements of $\mathfrak{G}_1$ follows from the fact kindly communicated to the writer by Professor R. A. Rankin that the group $\left\langle \begin{bmatrix}2 & 3\\ 3 & 5\end{bmatrix}, \begin{bmatrix}2 & 1\\ 1 & 1\end{bmatrix}\right\rangle$ is free without parabolic elements. On the other hand, J. Browkin has shown that there is no abelian counterexample.

2. It can be verified using the explicit determination of all primitive solvable groups of degree p^4 by G. Bucht (Arkiv f. Mat. 11 (1916)) and of degree p^q (q prime) by D. Suprunenko (*Soluble and nilpotent linear groups*, Providence, R. I. 1963) that all primitive solvable fields of the above degrees are Bauerian.

References

[1] H. Davenport, D. J. Lewis and A. Schinzel, *Polynomial of certain special types*, Acta Arith. 9 (1964), pp. 107–116.

[2] — — — *Quadratic Diophantine equations with a parameter*, Acta Arith. 11 (1966), pp. 353–358.

[3] H. Hasse, *Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper*, Teil II: *Reziprozitätsgesetz*, Würzburg–Wien 1965.

[4] D. J. Lewis, A. Schinzel and H. Zassenhaus, *An extension of the theorem of Bauer and polynomials of certain special types*, Acta Arith. 11 (1966), pp. 345–352.

[5] A. Schinzel, *On Hilbert's Irreducibility Theorem*, Ann. Polon. Math. 16 (1965), pp. 333–340.

[6] — *On a theorem of Bauer and some of its applications*, Acta Arith. 11 (1968), pp. 333–344, *Corrigendum* ibid. 12 (1967), p. 425.

[7] H. Weber, *Lehrbuch der Algebra*, Bd. II, New York 1964.

[8] H. Wielandt, *Finite Permutation Groups*, New York-London 1964.

Corrigenda to [6]

p. 338 line 8 for l divides n read g divides $|\bar{K}|$.
line 10 for n read $|\bar{K}|$.
p. 341 line 6 for $< n/p < p$ read $\leqslant n/p \leqslant p$.

Received on 20. 12. 1971 (242)