PROOF OF SOME CONJECTURES ON COHOMOLOGICAL DIMENSION[1]

JAMES AX

Introduction. Let k be a field of characteristic q ($=$ prime or 0) and let r be a non-negative integer. Then k is said to be C_r if and only if every (homogeneous) form of degree d in n variables over k has a nontrivial zero over k if $n>d^r$. In Serre [3, Chap. II, Corollary to Proposition 8] the following result is obtained: If k is C_1 then $\dim(k) \leqq 1$ and $[k:k^q]=1$ or q. Here $\dim(k)$ is defined cohomologically; $\dim(k) \leqq 1$ is equivalent to the nonexistence of noncommutative finite dimensional division algebras over k. Serre then remarks:

"On ignore si la réciproque du corollaire précédente est vrai—c'est peu probable."

Approximately this same problem had been previously raised by Nagata [5, Problem 6]. Namely Nagata noted that if k is C_1 then $N_{L/k}$: $L \to k$ is surjective for all finite extensions L/k. Nagata then asked if the converse is true. The approximate equivalence of these problems follows from Serre [Chap. II, Prop. 5], and the fact that the surjectivity of the norm implies $[k:k^q]=1$ or q.

In §1 we answer both these questions in the negative by exhibiting a field R of characteristic zero of dimension 1 which is not C_1. This implies, for all $r \geqq 1$, the existence of fields of dimension r which are not C_r. But the situation is worse than that: R is quasifinite in the sense of Serre [2, Chap. XIII, §2], and for all r, R is not C_r. The interest in these considerations stemmed from a possible relation with Artin's conjecture which states: If k_1 is the maximal abelian extension of the rationals then k_1 is C_1; if k_2 is a totally imaginary number field or a p-adic field then k_2 is C_2. Indeed, $\dim(k_1)=1$ and $\dim(k_2)=2$ as follows from Serre [Cor. to Prop. 9, Cor. to Prop. 12, Prop. 13].

We denote by G_k, the galois group of an algebraic closure $\bar{k}$ of k over k. We also denote the cohomological p-dimension of G_k by $cd_p(G_k)$. In §2 we solve the problem raised in the following remark of Serre [3, Chap. II, §4.2]:

"Supposons que $cd_p(G_k)=\infty$. Il est probable que l'on a alors $cd_p(G_{k'})=\infty$ pour toute extension *transcendante pure* k' of k, mais je ne vois pas comment le démontrer."

Serre then raises the corresponding problem for a field complete

Received by the editors January 13, 1965.

[1] Partially supported by NSF Grant GP-3665.

under a discrete valuation with residue class field k. It is this problem we solve first in the Corollary to Theorem 2; the desired fact about purely transcendental extensions is then deduced in the Corollary to Theorem 3.

1. **The field** R. We first introduce some simple devices involved in the construction of R. Let n be a positive integer and let A be a field of characteristic zero, containing all of 1. Set $B=A((s))(s^{1/m}: (m, n)=1)$, the field obtained from the field of formal power series $A((s))$ over A by the adjunction of the mth root $s^{1/m}$ of s for all positive integers m prime to n. Then the galois groups of $\tilde{B}/B$ and $\tilde{A}/A$ are related by

$$G_B = \bigoplus_{p|n} Z_p \oplus G_A$$

where Z_p is the p-adic integers. We omit the proof of this which is similar to, but simpler than, the considerations of §2. Let Z_{-n} be the additive subgroup of the rationals consisting of the fractions e/f with $(f, n)=1$. Let ord: $B \to Z_{-n} \cup \{\infty\}$ be the natural valuation of B with residue class field A. Suppose that $H(U_1, \cdots, U_v)$ is a form of degree d over A with no nontrivial zero over A. Then H has no nontrivial zero over B; in fact if $b_i \in B$, $i=1, \cdots, v$, and if not all the b_i are zero then

$$\operatorname{ord}(H(b_1, \cdots, b_v)) \in dZ_{-n}.$$

To see this, let $b \in B$ be such that

$$\operatorname{ord}(b) = \min_i(\operatorname{ord}(b_i)).$$

Letting $a_i=b_i/b$, we have

$$\begin{aligned}\operatorname{ord}(H(b_1, \cdots, b_v)) &= \operatorname{ord}(b^d H(a_1, \cdots, a_v)) \\ &= d \operatorname{ord}(b) + \operatorname{ord}(H(a_1, \cdots, a_v)).\end{aligned}$$

Denoting passage to the residue class field $A \subset B$ of B by a bar we have, since $\operatorname{ord}(a_i) \geq 0$ for $i=1, \cdots, v$ and $\operatorname{ord}(a_i)=0$ for some i,

$$H(\bar{a}_1, \cdots, \bar{a}_v) \neq 0 \text{ in } A.$$

Thus $\operatorname{ord}(H(b_1, \cdots, b_v))=d \operatorname{ord}(b) \in dZ_{-n}$.

It is relatively simple to construct a field Y such that $\dim(Y)=1$ while Y is not C_1. We carry this out first since it involves the essential idea behind the construction of R; it turns out that Y is C_2. In this section F denotes a fixed algebraically closed field of characteristic zero. Set $C=F((s))(s^{1/m}: (m, 6)=1)$ and then set

$$Y = C((t))(t^{1/n}\colon (n, 5) = 1).$$

Thus $G_Y = \mathbf{Z}_2 \oplus \mathbf{Z}_3 \oplus \mathbf{Z}_5$ so that by Serre [3, Chap. II, Prop. 5], $\dim(Y) = 1$. We will show that Y is not C_1 by constructing a form $H(Z_1, \cdots, Z_{10}) \in Y[Z]$ of degree 5 with no nontrivial zero over Y. Let $J(U_1, U_2)$ (resp.: $K(U_1, U_2, U_3)$) be a form of degree 2 (resp.: 3) over C with no nontrivial zero over C, e.g. take J (resp.: K) to be a norm form of $C(s^{1/2})/C$ (resp.: $C(s^{1/3})/C$). Then $L(U_1, U_2) = J(U_1, U_2)K(U_1, U_2, 0)$ is a form of degree 5 over C with no nontrivial zero over C. It follows from the introductory remarks of this section that

$$\operatorname{ord}(L(u_1, u_2)) \in 5\mathbf{Z}_{-5} \text{ if } (u_1, u_2) \in Y^2 - 0,$$

where ord: $Y \to \mathbf{Z}_{-5}\ U\{\infty\}$ is the natural valuation with residue class field C. We define

$$\begin{aligned} H(Z) &= H(Z_1, \cdots, Z_{10}) \\ &= L(Z_1, Z_2) + tL(Z_3, Z_4) + t^2L(Z_5, Z_6) + t^3L(Z_7, Z_8) \\ &\quad + t^4L(Z_9, Z_{10}). \end{aligned} \tag{1}$$

If we substitute $z \in Y^{10} - 0$ for Z in (1) then some summand is nonzero and each nonzero summand has a different ord in $\mathbf{Z}_{-5}$, different even modulo $5\mathbf{Z}_{-5}$. Thus H has no nontrivial zero over Y.

We now define R. We define F_p inductively for p a prime. Let $F_2 = F((t_2))(t_2^{1/n}\colon (n, 2) = 1)$. If q is the largest prime less than p we set $F_p = F_q((t_p))(t_p^{1/n}\colon (n, p) = 1)$. Finally, we set $R = \operatorname{inj} \lim_p F_p$. Thus $G_R = \prod_p \mathbf{Z}_p$, i.e. R is quasi-finite.

THEOREM 1. *R is not C_r for any r.*

PROOF. We fix r and show R is not C_r. We pick $n > r$ and then α such that $0 < \alpha < 1$ and $\sum_{i=0}^{n-1} \alpha^i \geq r$. We are going to make use of some known results in analytic number theory; it is possible to avoid their use at the expense of complicating the argument with unpleasant details.

Let m be a non-negative integer. We shall say a prime p is m-representable if $m = 0$ or if $p = p_1 + p_2 + p_3$, $p^\alpha < p_1 < p_2 < p_3$ where the p_i are $(m-1)$-representable primes. To complete the proof of Theorem 1, it suffices to establish the following two lemmas.

LEMMA 1. *If p is m-representable there exists a form H of degree p in at least p^λ variables, $\lambda = \sum_{i=0}^{m-1} \alpha^i$, over F_p with no nontrivial zero over F_p and hence over R.*

LEMMA 2. *For all m there exists c such that if $p > c$ then p is m-representable.*

Proof of Lemma 1. We may assume $m \geqq 1$, the lemma true for $m-1$, and that

$$(2) \qquad p = p_1 + p_2 + p_3, \qquad p^\alpha < p_1 < p_2 < p_3,$$

with p_i an $(m-1)$-representable prime. By induction, there exists a form $H_i(U_1, \cdots, U_{v_i})$ of degree p_i over F_{p_i} with no nontrivial zero over F_{p_i}, where

$$v_i \geqq p_i^\mu \geqq p_1^\mu, \qquad \mu = \sum_{i=0}^{m-2} \alpha^i.$$

By setting extra variables equal to zero, we may assume that $v_1 = v_2 = v_3$ $(= v$, say). Thus

$$(3) \qquad v \geqq p_1^\mu, \qquad \mu = \sum_{i=0}^{m-2} \alpha^i.$$

Set $K(U_1, \cdots, U_v) = H_1(U_1, \cdots, U_v) \cdot H_2(U_1, \cdots, U_v) \cdot H_3(U_1, \cdots, U_v) \in F_{p_3}[U_1, \cdots, U_v]$. Then set

$$\begin{aligned} H(Z_1, \cdots, Z_{pv}) = {} & K(Z_1, \cdots, Z_v) + t_p K(Z_{v+1}, \cdots, Z_{2v}) \\ & + \cdots + t_p^{p-1} K(Z_{(p-1)v}, \cdots, Z_{pv}) \\ & \in F_p[Z_1, \cdots, Z_{pv}]. \end{aligned}$$

H is a form of degree $p_1 + p_2 + p_3 = p$ in pv variables over F_p. It follows as before that H has no nontrivial zero over F_p. But by (2) and (3),

$$pv \geqq pp_1^\mu \geqq p^{1+\alpha\mu} = p^\lambda.$$

This proves Lemma 1.

Proof of Lemma 2. By induction, it suffices to prove the lemma when $m = 1$. It follows from Vinogradov [4, Chap. X, Theorem] that there exists $b > 0$ such that the number of representations of an odd integer $N > b$ as $N = p_1 + p_2 + p_3$ with $p_1 \leqq p_2 \leqq p_3$, p_i prime, exceeds $N^2/(\log N)^4$. Now the number of representations of N as $2n_1 + n_2$ with n_i a positive integer is at most N. Also the number of representations of N as $N = n_1 + n_2 + n_3$, $n_1 \leqq N^\alpha$, n_i a positive integer is at most $N^{1+\alpha}$. Thus, if N is an odd integer, $N > b$, then the number of representations of N as

$$N = p_1 + p_2 + p_3, \quad N^\alpha < p_1 < p_2 < p_3, \qquad p_i \text{ prime}$$

exceeds

$$(4) \qquad N^2/(\log N)^4 - N - N^{1+\alpha}.$$

Since $\alpha<1$ there exists $c>b$ such that if $N>c$ then the expression (4) is positive. This completes the proof of Lemma 2.

This concludes the proof of Theorem 1.

It is equally possible to provide similar examples in any characteristic.

We note that if we neglect the prime 2 in the construction of R, then, in the notation of Serre [3, Chap. II, §4.5], the resulting field R' is C_2' but not C_2. To see this, observe that

$$G_{R'} \approx \prod_{p\neq 2} Z_p$$

so that R' has no quadratic extensions. Thus every quadratic form (in 5 variables) over R' has a nontrivial solution over R'. Also $\dim(R')=1$ so that by Serre [3, Chap. II, Prop. 5], the condition on the finite dimensional division algebras over R' is vacuously satisfied. Finally, the proof that for all r, R is not C_r works equally well for R'.

2. **On transcendental extensions.** By a *Hensel field* W, we mean a field W with an additive valuation ord into an ordered abelian group, $\operatorname{ord}(W)$, such that Hensel's lemma holds.

LEMMA 3. *Let W be a Hensel field such that the residue class field $\overline{W}$ of W is algebraically closed and* $\operatorname{ord}(W)$ *is divisible. If $q=\operatorname{char}(\overline{W})$, then G_W is a pro-q-group. If $q=0$, the last statement is understood to mean that $G_W=1$, i.e. W is algebraically closed.*

PROOF. For the "complete" case (W algebraic over a complete field valued in the integers Z) this follows from Hilbert theory as in Serre [2, Chap. IV, §2, Cor. 3 to Prop. 7]. We give a direct argument, similar to the standard proof that the field of formal Puiseaux expansions over an algebraically closed field of characteristic zero is algebraically closed. We may assume W is perfect. Let H be a q-Sylow subgroup of G_W. Let $\alpha\in W$ be fixed by H. Then $q\nmid m=[W(\alpha):W]$, and it suffices to show $m=1$. Let $F(X)=\sum_{i=0}^{m} f_iX^i$ be the monic irreducible polynomial for α over W. Since $m\neq 0$ in W, we may assume $f_{m-1}=0$ by replacing α by $\alpha-f_{m-1}/m$. Since W is a Hensel field, each root of W has the same ord value γ [1, Chap. VII, (43.2) (2)]. Since $\operatorname{ord}(W)$ is divisible, there exists $a\in W$ such that $\operatorname{ord}(a)=\gamma$. Thus we may assume $\gamma=0$ by replacing α by α/a. We now claim that $\bar{f}(X)$ factors into two relatively prime factors in $\overline{W}[X]$ if $m>1$. Indeed, otherwise the fact that $\overline{W}$ is algebraically closed implies there exists $b\in W$ such that $\operatorname{ord}(b)=0$ and $\bar{f}(X)=(X-\bar{b})^m$. But this is impossible since the coefficient of X^{m-1} on the right is not zero in $\overline{W}$

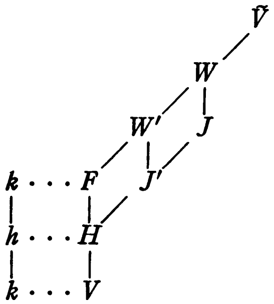
because $q\nmid m$. This completes the proof since if $\bar{f}(X)$ factors into two relatively prime factors in $\overline{W}[X]$, then by Hensel's lemma, $f(X)$ factors in $W[X]$, contradicting the irreducibility of $f(X)$.

THEOREM 2. *Let V be a Hensel field valued in the integers $\boldsymbol{Z}$, such that $\overline{V}=k$ is perfect. Let S be a p-Sylow subgroup of G_k, $p\neq\mathrm{char}(k)$. Then there exists a p-Sylow subgroup T of G_V and a split exact sequence*

$$(5)\qquad 0\to\boldsymbol{Z}_p\to T\xrightarrow{\mu}S\to 1$$

where μ is the restriction to T of the natural epimorphism $\nu\colon G_V\to G_k$.

PROOF. Let $h\subseteq k$ the fixed field of S. Let H be the unique unramified extension of V with $\overline{H}=h$. Set $J=H(\pi^{1/n}\colon n=1,2,\cdots)$ where π is a prime element of V; we assume these nth roots picked consistently so that $(\pi^{1/n})^j=\pi^{1/m}$ if $n=jm$. This is possible since the inverse limit of finite nonempty sets is nonempty. We then obtain the following Hasse diagram.



Here F is the maximal unramified extension of V, $J'=H(\pi^{1/n}\colon p\nmid n)$, $W'=FJ'$, and $W=FJ$. We denote the galois group of an algebraic extension L/K by $G(L/K)$. W' is an unramified extension of J'. J is a purely ramified extension of J' by our consistent choice of the roots of π. It follows that W' and J are linearly disjoint over J'. Therefore there exists a natural split exact sequence

$$(6)\qquad 1\to G(W/W')\to G(W/J')\to G(W'/J')\to 1.$$

We have $G(W/J)\approx S$ by the natural epimorphism. Also $G(W/W')\approx\boldsymbol{Z}_p$. Let T be a p-Sylow subgroup of $G(\tilde{V}/J')$. We claim T is a p-Sylow subgroup of G_V. It follows from Serre [3, Chap. I, Prop. 2] that

$$(G_V\colon 1)=(G(\tilde{V}/\overline{H})\colon 1)(G(\overline{H}/V)\colon 1).$$

Since $G(H/V)\approx G(h/k)$, $p\nmid(G(H/V)\colon 1)$. Hence it suffices to show that T is a p-Sylow subgroup of $G(\tilde{V}/H)$. If this is false there exist fields K and L such that

$$H \subset K \subset L \subset J', \quad [L\colon K] < \infty, \quad p \mid [L\colon K].$$

We may assume $[K\colon H] < \infty$ by replacing K by the field generated over H by the coefficients of a defining polynomial for L/K. The consistency of our choice of the roots of π guarantees that there exists n such $p \nmid n$ and $L \subset H(\pi^{1/n})$. But then $[L\colon K] \mid n$. This contradiction establishes our claim. Now the restriction epimorphism of $G(\tilde{V}/J')$ onto $G(W/J')$ induces an epimorphism $\rho\colon T \rightarrow G(W/J')$ by [3, Chap. I, Prop. 4(b)]. The kernel of ρ is $T \cap G(\tilde{V}/W) = 1$ since $p \neq \mathrm{char}(k)$ and W satisfies the hypothesis of Lemma 1. Thus (6) induces (5).

Corollary.

$$cd_p(G_V) = cd_p(G_k) + 1.$$

Proof. If $cd_p(G_k) < \infty$ this follows from the exactness of (5) by a spectral sequence argument as in [3, Chap. I, Prop. 2(i)]. If $cd_p(G_k) = \infty$ the equality follows from the splitting of (5).

We continue to denote by $k((t))$ the field of formal power series over k and let k_1 denote the algebraic closure of $k(t)$.

Lemma 4. *If k is perfect, then $k((t))\ k_1$ is algebraically closed.*

Proof. $k((t))\ k_1$ is algebraic over $W = k((t))(t^{1/n}\colon n = 1, 2, \cdots)$. W is perfect and satisfies the hypothesis of Lemma 3. Thus it suffices to show that if N/W is a galois subextension of $\tilde{W}/W$ of degree $n = q^m$, $q = \mathrm{char}(k)$, then there exists a basis $\omega_1, \cdots, \omega_n \in K_1$ for N/W. We do this by induction on m. If $m \geqq 1$, there exists a galois subextension M/W of N/W of degree $j = q^{m-1}$. Assume $\omega_1, \cdots, \omega_j \in k_1$ is a basis for M/W. Then there exist $a_1, \cdots, a_j \in W$ such that $N = M(\alpha)$ where $\alpha^q - \alpha = a = \sum_{i=1}^{j} a_i\omega_i$. Now there exist $b_i \in k_1$ and $c_i \in W$ such that $a_i = b_i + c_i$ and $\mathrm{ord}(c_i\omega_i) \geqq 0$. Let $b = \sum_{i=1}^{j} b_i\omega_i$ and $c = \sum_{i=1}^{j} c_i\omega_i \in M$. Then $b \in k_1$ and $\mathrm{ord}(c) \geqq 0$. Since $\overline{M}$ is algebraically closed there exists $g \in \overline{M}$ such that $\bar{h}(g) = 0$ where $h(X) = X^q - X - c$. g is a simple root of $\bar{h}(X)$ since the derivative of $\bar{h}(X)$ is $-\bar{1}$. Thus by Hensel's lemma for M there exists $\gamma \in M$ such that $h(\gamma) = 0$. Let $\beta \in k_1 \subset \tilde{W}$ be such that $\beta^q - \beta = b$. Then we may take $\alpha = \beta + \gamma \in Mk_1$. This completes the proof.

Theorem 3. *Let $K = k(t)$. Let p be a prime, $p \neq \mathrm{char}(k)$. If S is a p-Sylow subgroup of G_k then there exists a pro-p-subgroup U of G_K and a split exact sequence*

$$0 \rightarrow Z_p, \rightarrow U \rightarrow S \rightarrow 1. \tag{7}$$

Proof. We may assume k is perfect. We then apply Theorem 2 to $V = k((t))$. Thus there exists a pro-p-subgroup T of G_V and a split exact sequence as in (5). It only remains to observe that the restriction homomorphism from G_V into G_K is an injection by Lemma 4, so that T is isomorphic to a closed subgroup U of G_K.

REMARK. Theorem 3 implies that S is (noncanonically) isomorphic to a closed subgroup of G_K. Actually, this is true if K/k is an arbitrary purely transcendental extension. Indeed, if the transcendence degree τ of K/k is finite this follows from Theorem 2 by induction. If τ is infinite, however, the noncanonical nature of the isomorphisms makes it difficult to carry out a limiting argument. One procedure which works is to introduce power series fields in a transcendence basis for K/k. We omit the details since we can establish the Corollary to Theorem 3 without these considerations.

COROLLARY. *If K/k is purely transcendental, then*

$$a + cd_p(k) \leqq cd_p(K), \tag{8}$$

where a = the transcendence degree b of K/k if b is finite and $a = \infty$ if b is an infinite cardinal.

PROOF. If $b=1$ then (8) holds with $a=1$ by Theorem 3. If b is finite, then (8) holds by induction. If b is infinite, then for every positive integer n there exists a subfield L_n of K such that K is a purely transcendental extension of L_n of transcendence degree n. Thus

$$n \leqq n + cd_p(G_{L_n}) \leqq cd_p(G_K)$$

for all n. This completes the proof.

REFERENCES

1. M. Nagata, *Local rings*, Interscience, New York, 1962.

2. J.-P. Serre, *Corps locaux*, Hermann, Paris, 1962.

3. ———, *Cohomologie Galoisienne*, Mimeographed notes, Collège de France, 1963 (also as Lecture Notes in Mathematics, No. 5, Springer-Verlag, 1964).

4. I. M. Vinogradov, *The method of trigonometrical sums in the theory of numbers*, Interscience, New York.

5. M. Nagata, *Note on a paper of Lang concerning quasi algebraic closure*, Mem. Coll. Sci., Univ. Kyoto 30 (1957), 237–241.

CORNELL UNIVERSITY