AMERICAN JOURNAL OF MATHEMATICS

FOUNDED BY THE JOHNS HOPKINS UNIVERSITY

Volume 100, 1978

THE JOHNS HOPKINS UNIVERSITY PRESS
BALTIMORE, MARYLAND 21218
U. S. A.

DIOPHANTINE PROPERTIES OF SUBFIELDS OF $\tilde{\mathbf{Q}}$.

By Michael Fried and Moshe Jarden.

Introduction. By the *Galois closure* of a separable algebraic field extension F/E we mean the smallest extension $\hat{F}$ of F which is Galois over E.

A finitely generated field extension F/K of dimension r is said to be *stable* if it has a separating transcendence base $t_1,\dots,t_r$ such that the Galois closure, $\hat{F}$, of the (separable) extension $F/K(\mathbf{t})$ is regular over K. This is equivalent to saying that $\mathcal{G}\left(\hat{F}/K(\mathbf{t})\right)\cong\mathcal{G}\left(\tilde{K}\cdot\hat{F}/\tilde{K}(\mathbf{t})\right)$, where $\tilde{K}$ is the algebraic closure of K (cf. [5, Section 1]). The system $t_1,\dots,t_r$ is said to be a *stablizing* base for F/K.

A field K is said to be *stable* if every finitely generated regular extension F of K is stable.

A field K is said to be *pseudo-algebraically closed* (*PAC*) if every non-void absolutely irreducible variety V defined over K has a K-rational point.

It was proved in [5, Theorem 3.4] that

(A) *Every PAC field is stable.*

A close examination of the proof of this theorem reveals that actually a little more was proven. Indeed, it was proven that given a PAC field K and a regular finitely generated extension F of K, there exists a stabilizing base $(\mathbf{t})$ for F/K such that $\mathcal{G}(\hat{F}/K(\mathbf{t}))$ is isomorphic to a symmetric group S_n, where $n=[F:K(\mathbf{t})]$. It turns out that it is important for the applications also to have this stronger property. We therefore make the following definitions.

A regular finitely generated extension F/K is said to be *symmetrically stable* if it has a stabilizing base $(\mathbf{t})$ such that $\mathcal{G}(F/K(\mathbf{t}))$ is isomorphic to a symmetric group. In particular every symmetrically stable extension is stable. The field K is said to be *symmetrically stable* if every regular finitely generated extension F/K is symmetrically stable.

Having made these definitions we can now restate (A) as follows:

(A′) *Every PAC field is symmetrically stable.*

The aim of this paper is to generalize this result for fields of characteristic

Manuscript received June 25, 1976.

American Journal of Mathematics, Vol. 100, No. 3, pp. 653–666
0002-9327/78/1003-0653 $01.50

0 and to prove that

(B) *Every field of characteristic* 0 *is symmetrically stable.*

The question of the stability of non-zero characteristic fields remains open.

The first step in proving (B) is to show that it suffices to consider only extensions F/K of dimension 1 and to find a transcendental element $t \in F$ such that $\mathcal{G}\left(\tilde{K}\hat{F}/\tilde{K}(t)\right) \cong S_n$, where $n = [F : K(t)]$. This condition is then shown to be satisfied if t is chosen in such a way that every prime divisor $\mathfrak{p}$ of $\tilde{K}(t)/\tilde{K}$ that ramifies in $\tilde{K}\hat{F}$ decomposes in $\tilde{K}\hat{F}$ as $\mathfrak{p} = \mathfrak{P}_1 + \cdots + \mathfrak{P}_{n-2} + 2\mathfrak{P}_{n-1}$, where the $\mathfrak{P}_i$ are distinct prime divisors of $\tilde{K}\hat{F}/\tilde{K}$. In order to show that such a choice of t is possible, we use a well-known theorem which says that F/K has a projective plane model Γ with at most nodes as singularities. Given such a Γ, we show that it is possible to choose a K-rational point $O \in \mathbf{P}^2 - \Gamma$ such that all lines that pass through O cut Γ in at least $n-1$ distinct points, where $n = \deg \Gamma$. The stereographic projection of Γ from O maps a generic point P of Γ over K onto a generic point Q of $\mathbf{P}^1$ over K. The field $K(Q)$ is then a pure transcendental extension of K, and the above decomposition law for the prime divisors of $\tilde{K}(Q)/K$ is satisfied.

In Section 4, the theorem (B) is applied to construct a normal extension N of the field $\mathbf{Q}$ of rational numbers such that N is PAC and hilbertian and $\mathcal{G}(\tilde{\mathbf{Q}}/N)$ is not contained in any finitely generated closed subgroup of $\mathcal{G}(\tilde{\mathbf{Q}}/Q)$. This reanswers a question of Ax and simultaneously answers a question of the first author.

The authors are indebted to P. Roquette, H. Popp and W. D. Geyer for some very useful conversations.

1. Stable Extensions. We begin, as announced in the introduction, by reducing the problem of proving the stability of fields to the problem of proving the stability of finitely generated extensions of dimension 1.

LEMMA 1.1. *A sufficient (and obviously necessary) condition for an infinite field K to be stable (respectively, symmetrically stable) is that for every extension L of K, every finitely generated regular extension F/L of dimension* 1 *is stable (symmetrically stable).*

Proof. Let L be an extension of K, and let F/K be a finitely generated regular extension of dimension r. We prove, by induction on r, that F/L is stable (symmetrically stable). If $r = 0$, then $F = L$ and there is nothing to prove. The case $r = 1$ has been assumed in the lemma. Suppose therefore that $r \geqslant 2$ and that the statement is valid for $r-1$. Let $t_1, \ldots, t_r$ be a separating transcendence base for F/L. Then there exists at least one derivation D of F over L such that

$Dt_r \neq 0$ (cf. Lang [9, p. 186]); hence $t_r \notin LF^p$, where $p = \mathrm{char}(L)$ (cf. [9, p. 185]). A lemma of Zariski and Matsusaka implies therefore that there exists an element c of L such that F is regular over $L_1 = L(t_{r-1} + ct_r)$ (see [9, p. 213]). The element $u_1 = t_{r-1} + ct_r$ is transcendental over L, since t_{r-1}, t_r are algebraically independent over L, and hence $\dim F/L_1 = r-1$. F/L_1 has therefore, by the induction hypothesis, a stabilizing (symmetrically stabilizing) base $u_2, \ldots, u_r$. The system $u_1, u_2, \ldots, u_r$ is a stabilizing (symmetrically stabilizing) base for F/L.

Q.E.D.

We must therefore consider only finitely generated regular extensions of dimension 1. We have already mentioned that if F/K is such an extension and if t is a separable transcendence element for F/K, then t is also a stable element for F/K if and only if $\mathcal{G}(\hat{F}/K(t)) \cong \mathcal{G}(\tilde{K}\hat{F}/\tilde{K}(t))$, since $\hat{F}/K$ is regular if and only if $\hat{F}$ is linearly disjoint from $\hat{K}$ over K. This Galois theoretic condition is automatically fullfilled if $\mathcal{G}(\tilde{K}\hat{F}/\tilde{K}(t))$ is a symmetric group. Indeed we have the following Lemma (see [5, Lemma 1.2]):

LEMMA 1.2. *Let t be a separating transcendence element of a finitely generated regular extension F/K of dimension 1, and let $n = [F:K(t)]$. If $\mathcal{G}(\tilde{K}\hat{F}/\tilde{K}(t))$ is isomorphic to the symmetric group S_n, then $\mathcal{G}(\hat{F}/K(t)) \cong S_n$ and hence F/K is symmetrically stable.*

The Galois-theoretic condition that appears in Lemma 1.2 is satisfied if the prime divisors of $\tilde{K}(t)$ decompose in a certain way, as described in Lemma 1.5 below. In order to prove Lemma 1.5 we use the following two well-known lemmas.

LEMMA 1.3. *Let L be an algebraically closed field, let t be a transcendental element over L, and let E be a finite Galois extension of $L(t)$. Then $\mathcal{G}(E/L(t))$ is generated by the inertia groups of the prime divisors of E/L.*

Proof. Let $\mathfrak{P}$ be a prime divisor of E/L, and let

$$I(\mathfrak{P}) = \{\sigma \in \mathcal{G}(E/L(t)) \mid \mathfrak{P}(\sigma x - x) = 0 \ \forall x \in E\}$$

be the inertia group of $\mathfrak{P}$. Denote by $T(\mathfrak{P})$ the fixed field of $I(\mathfrak{P})$ in E; this is the inertia field of $\mathfrak{P}$. $T(\mathfrak{P})$ is the maximal subfield of E that contains $L(t)$ such that the restriction of $\mathfrak{P}$ to $T(\mathfrak{P})$ is unramified over $L(t)$. The fixed field, T, of the subgroup G generated by all the inertia groups $I(\mathfrak{P})$ is unramified over $L(t)$. It follows that the different of T over $L(t)$ is the zero divisor. Furthermore, the genus of $L(t)$ is zero. Hence, if we denote by g the genus of T/L, we obtain from Hurwitz genus formula (cf. Chevalley [3, p. 106, Corollary 2]) that

$2g-2=-2[T:L(t)]$. It follows that $[T:L(t)]=1$; hence $T=L(t)$; hence $G=\mathcal{G}(E/L(t))$. Q.E.D.

LEMMA 1.4. *If G is a transitive subgroup of S_n and if G is generated by cycles of length 2, then $G=S_n$.*

Proof (Z. Janko). We consider G as operating on a set X of n elements. For every subset Y of X we denote by $S(Y)$ the group of all permutations of X which leave $X-Y$ elementwise fixed. G is not empty, since it is transitive; hence it contains $S(\{x\})$ for every $x\in X$. Suppose that G contains $S(Y)$, where Y is a proper subset of X. Then there exists a transposition (xy) in G such that $x\in X-Y$ and $y\in Y$, since otherwise G would transfer Y into itself, contradicting the transitivity. It follows that G contains $S(Y\cup\{x\})$, since $S(Y\cup\{x\})$ is generated by $S(Y)$ and (xy). By repeating this argument at most n times, we conclude that $G=S(X)$. Q.E.D.

LEMMA 1.5. *Let L be an algebraically closed field, let t be a transcendental element over L, let F be a separable extension of $L(t)$ of degree n, and let F be the Galois closure of $F/L(t)$. If every prime divisor $\mathfrak{p}$ of $L(t)$ that ramifies in F decomposes in F in the form*

$$\mathfrak{p}=\mathfrak{P}_1+\cdots+\mathfrak{P}_{n-2}+2\mathfrak{P},$$

where $\mathfrak{P}_1,\ldots,\mathfrak{P}_{n-2},\mathfrak{P}$ are distinct prime divisors of F/L, then $\mathcal{G}(\hat{F}/L(t))\cong S_n$.

Proof. Let $G=\mathcal{G}(\hat{F}/L(t))$, and let $H=\mathcal{G}(\hat{F}/F)$. Then the only subgroup of H that is normal in G is the trivial one. Let $X=\{\sigma H|\sigma\in G\}$ be the set of the left cosets of G modulo H. X contains exactly n elements, since $(G:H)=[F:L(t)]=n$. G operates transitively on X by multiplication from the left: $\tau\cdot\sigma H=\tau\sigma H$. Thus we get a homomorphism of G into the symmetric group $S(X)$ of all permutations of X. The kernel of this homomorphism is clearly contained in H and is normal in G: hence it is trivial. It follows that G can be identified with a subgroup of $S(X)$. We show that $G=S(X)$.

By Lemma 1.3, G is generated by the inertia subgroups $I(\mathfrak{q})$ of the prime divisors $\mathfrak{q}$ of $\hat{F}/L$. Every prime divisor of $\hat{F}/L$ lies over a certain prime divisor of $L(t)/L$. Let $\mathfrak{p}$ be a prime divisor of $L(t)/L$. If $\mathfrak{p}$ is unramified in F, then $I(\mathfrak{q})\subseteq H$ for every prime divisor $\mathfrak{q}$ of $\hat{F}/L$ that lies over $\mathfrak{p}$. The subgroup J generated by all these $I(\mathfrak{q})$ is thus contained in H. J is also normal in G; hence $J=1$.

It follows that G is generated by all the inertia groups $I(\mathfrak{q})$ such that the prime divisors $\mathfrak{p}$ of $L(t)/L$ that lie under $\mathfrak{q}$ ramify in F. By Lemma 1.4, it suffices to show that for such $\mathfrak{q}$'s $I(\mathfrak{q})$ is a cyclic group generated by a transposition.

Suppose therefore that $\mathfrak{p}$ is a prime divisor of $L(t)/L$ that ramifies in F. Then we have, by assumption, that $\mathfrak{p}=\mathfrak{P}_1+\cdots+\mathfrak{P}_{n-2}+2\mathfrak{P}$, where $\mathfrak{P}_1,\ldots,\mathfrak{P}_{n-2},\mathfrak{P}$ are distinct prime divisors of F/L. Let $\mathfrak{q}$ be a prime divisor of $\hat{F}/L$ that lies over $\mathfrak{P}$. If $\mathfrak{q}'$ is another prime divisor of $\hat{F}/L$ that lies over $\mathfrak{p}$, then $I(\mathfrak{q}')$ is conjugated to $I(\mathfrak{q})$. It suffices therefore to prove that $I(\mathfrak{q})$ is a cyclic group generated by a transposition.

For each $1\leqslant i\leqslant n-2$, consider an extension $\mathfrak{q}_i$ of $\mathfrak{P}_i$ to $\hat{F}$. $\mathfrak{P}_i$ is unramified over $L(t)$; hence $I(\mathfrak{q}_i)\subseteq H$. Furthermore, there exists a $\sigma_i\in G$ such that $\mathfrak{q}_i=\mathfrak{q}\sigma_i$. If $1\leqslant j\leqslant n-2$ and $j\neq i$, then $\sigma_i|F\neq\sigma_j|F$, since $\mathfrak{P}_i\neq\mathfrak{P}_j$; hence $\{\sigma_1H,\ldots,\sigma_{n-2}H\}$ contains exactly $n-2$ elements of X. Let $\sigma_{n-1}H$ and σ_nH be the remaining two elements of X. If $\tau\in I(\mathfrak{q})$, then

$$\sigma_i^{-1}\tau\sigma_i\in I(\mathfrak{q}\sigma_i)=I(\mathfrak{q}_i)\subseteq H;$$

hence $\tau(\sigma_iH)=\sigma_iH$ for $i=1,\ldots,n-2$. It follows that τ can permute only $\sigma_{n-1}H$ with σ_nH. Furthermore, $I(\mathfrak{q})\neq 1$, since $\mathfrak{q}$ is ramified over $L(t)$. Hence there exsits an element $\tau\in I(\mathfrak{q})$ such that $\tau\neq 1$. This element generates $I(\mathfrak{q})$, and its image in $S(X)$ is exactly the cycle $(\sigma_{n-1}H,\sigma_nH)$. Q.E.D.

If we combine Lemma 1.2 with Lemma 1.5 we get

LEMMA 1.6. *Let t be a separating transcendence element of a finitely generated regular extension F/K of dimension 1, and let $n=[F:K(t)]$. If every prime divisor $\mathfrak{p}$ of $\tilde{K}(t)$ that ramifies in $\tilde{K}F$ decomposes in $\tilde{K}\hat{F}$ in the form*

$$\mathfrak{p}=\mathfrak{P}_1+\cdots+\mathfrak{P}_{n-2}+2\mathfrak{P},$$

where $\mathfrak{P}_1,\ldots,\mathfrak{P}_{n-2}$ are distinct prime divisors of $F\cdot\tilde{K}/\tilde{K}$, then $\mathcal{G}\left(\hat{F}/K(t)\right)\cong\mathcal{G}\left(\tilde{K}\hat{F}/\tilde{K}(T)\right)\cong S_n$ and hence F/K is symmetrically stable.

2. Reformulation of the Problem in Geometric Terms. In Lemma 1.6 we gave a certain algebraic condition for a regular extension of dimension 1 to be symmetrically stable. In this section we translate the algebraic condition into a geometric one which is easier to handle. Extensions of dimension 1 are strongly connected with curves. Our geometric condition is therefore on finite morphisms of curves.

LEMMA 2.1. *Let Γ be an absolutely irreducible projective plane curve of degree n defined over a field K, and let O be a K-rational point of $\mathbf{P}^2-\Gamma$ satisfying the following condition*:

(*) *Every line that passes through O cuts Γ in at least $n-1$ points; almost every line that passes through O cuts Γ in n points.*

Then the function field, $K(\Gamma)$, of Γ over K is a symmetrically stable extension of K.

Proof. The assumption that O does not lie on Γ and that Γ is a projective curve implies that λ, a projection from O, is a finite morphism and that $\lambda(\Gamma)=\mathbf{P}^1$ (see e.g. Shafarevich [14, p. 50]). Further, λ is defined over K, since O is K-rational.

Let Q' be a point of $\mathbf{P}^1$, and let P' be a point of Γ which is mapped onto Q' by λ. The set of all points of Γ that are mapped onto Q' by λ is exactly the set of points of Γ that lie on the line L through O and P'. The condition (*) therefore implies that there are at least $n-1$ points and at most n points of Γ lying over Q'; the number $n-1$ is obtained only for finitely many points Q'. It follows, by standard arguments, that if P is a generic point of Γ over K and $Q=\lambda(P)$, then $[K(P):K(Q)]_s=n$. On the other hand $[K(P):K(Q)]\leqslant n$, since $\deg\Gamma=n$ and since O is K-rational. Hence $K(P)$ is a separable extension of $K(Q)$ of degree n. We also know that $K(P)$ is a regular extension of K, since Γ is absolutely irreducible; hence also $[\tilde{K}(P):\tilde{K}(Q)]=n$. Moreover, Q is a generic point of P^1 over K. This means that there exists a transcendental element t over K such that $K(Q)=K(t)$.

Let $\mathfrak{p}$ be a prime divisor of $\tilde{K}(t)/\tilde{K}$ that ramifies in $\tilde{K}(P)$. By what was said above, there are at least $n-1$ points $P_1',\dots,P_{n-1}'$ of Γ that lie over $Q'=\mathfrak{p}(Q)$. Each one of the $\tilde{K}$-specializations $P\to P_1'$ can be extended to a prime divisor $\mathfrak{P}_i$ of $\tilde{K}(P)/\tilde{K}$, and we have

$$\mathfrak{P}_i(Q)=\mathfrak{P}_i(\lambda(P))=\lambda(P_i')=Q'=\mathfrak{p}(Q).$$

This means that $\mathfrak{P}_i$ lies over $\mathfrak{p}$. There cannot be any more prime divisors of $\tilde{K}(P)/\tilde{K}$ that lie over $\mathfrak{p}$, since $\mathfrak{p}$ is ramified and since the sum of the multiplicities of $\mathfrak{p}$ in the $\mathfrak{P}_i$ must be equal to n. Hence $\mathfrak{p}$ decomposes in $\tilde{K}(P)$ in the form

$$\mathfrak{p}=\mathfrak{P}_1+\cdots+\mathfrak{P}_{n-2}+2\mathfrak{P}_{n-1},$$

and the $\mathfrak{P}_i'$'s are distinct.

It follows from Lemma 1.6 that $K(P)/K$ is a symmetrically stable extension. Q.E.D.

3. **Realizing the Geometric Conditions over Fields of Characteristic 0.** Consider a projective plane curve Γ of degree n and a point O in $\mathbf{P}^2-\Gamma$. Let L be a line through O, and let $P_1,\dots,P_m$ be the intersection points of L with Γ. One assigns to each of the points P_i a positive intersection multiplicity $i(\Gamma,L;P_i)$ (cf. Seidenberg [13, p. 33]) and one has, by Bezout's theorem, that $\sum_{i=1}^{m} i(\Gamma,L;P_i)=n$ (cf. [13, p. 44]). It follows that $m\leqslant n$ and that a necessary condition for M to be $\geqslant n-1$ is that $i(\Gamma,L;P_i)\leqslant 2$ for $i=1,\dots,m$. One also knows that $i(\Gamma,L;P_i)$ is not less than the multiplicity of P_i on Γ. Thus a necessary condition for the inequality $i(\Gamma,L;P_i)\leqslant 2$ to hold is that the multiplicity of P_i on Γ is at most 2. Since every point P of Γ occurs as a point of intersection of Γ with a certain line through O, all the singular points of Γ must be of multiplicity 2. If $\mathrm{char}(K)=0$, then Γ can be birationally transferred onto a curve Γ' that satisfies this condition. Indeed, we have the following lemma:

LEMMA 3.1. *If K is a field of characteristic 0 and if F is a finitely generated regular extension of K of dimension 1, then there exists a projective plane curve Γ which is defined over K and has only singular points of multiplicity 2 such that $K(\Gamma)=F$.*

A proof of this lemma can be found in Lefschetz [10, p. 130] for the case where K is algebraically closed (and of characteristic 0). It consists of two main steps. In the first one it is shown that F/K has a projective space model without singularities. In the second step the space model is projected on the plane and one obtains a projective plane model for F/K with only nodes as singularities, and hence with singularities of multiplicity 2 only. The method of the proof of both steps is to show that starting from a projective smooth model Γ' for F/K in $\mathbf{P}^k$ (that always exists), one can find a proper algebraic subset A of $\mathbf{P}^k$ such that the projection of Γ' into $\mathbf{P}^{k-1}$ from any point $O\in\mathbf{P}^k-A$ is a "good" one. Hence, even if K is not algebraically closed, one can choose O to be rational over K and in this way to obtain the desired model for F/K.

We note that the second step of the proof is carried out by Abhyankar [1, p. 23 and p. 75]. Abhyankar's proof is however valid over every infinite field, and the model obtained in this proof is one with only nodes as singularities and without strange points (i.e., points through which there pass infinitely many tangents to the curve).

We also note that Popp proves in his Thesis and states in [12, p. 510] that if K is an infinite field and F is a conservative regular function field of one variable over K, then F/K has a projective plane model with only nodes as singularities.

Given a plane curve Γ with only double points as singularities, one can

find a K-rational point O satisfying the conditions of Lemma 2.1. This follows from the following lemma.

LEMMA 3.2. *If Γ is an absolutely irreducible projective plane curve defined over a field K of characteristic 0, then there exists a K-rational point O such that:*

(a) *No line through O is tangent to Γ in two distinct points;*
(b) *O does not lie on the tangents to Γ through the points of inflection of Γ;*
(c) *O does not lie on any of the lines that pass through two singular points of Γ;*
(d) *No tangent to Γ that passes through a singular point passes also through O;*
(e) *Only finitely many lines through O are tangent to Γ.*

Proof. The lemma is obviously valid if Γ is a line. Suppose therefore that Γ is not a line, and consider its dual curve Γ^*. Geometrically speaking Γ^* consists of all the tangents to Γ considered as points in the dual plane. A tangent to Γ in two points corresponds to a singular point of Γ^* (see van der Waerden [15, p. 77]). Since Γ^* has only finitely many singular points, we have:

(i) Only finitely many lines are tangent to Γ in two points.

A point P of Γ is a point of inflection if it is simple and if the tangent to Γ at P cuts Γ with multiplicity $\geqslant 3$. The point of Γ^* that corresponds to this tangent has multiplicity $\geqslant 2$ (see [15, p. 76]); hence it is singular. Therefore

(ii) only finitely many lines are tangent to Γ in inflection points.

Γ itself has only finitely many singular points. Hence

(iii) only finitely many lines pass through two singular points of Γ.

There are at most a finite number of tangents to Γ passing through a given point of $\mathbf{P}^2$ (see Lefschetz [10, p. 127]). It follows that

(iv) there are at most a finite number of tangents to Γ that pass through singular points.

There are therefore only finitely many "bad" lines satisfying (i), (ii), (iii), or (iv). Since K is an infinite field, there exists a K-rational point $O \in \mathbf{P}^2 - \Gamma$ that does not lie on any of these lines. O certainly satisfies the conditions (a), (b), (c), and (d). It satisfies also condition (e), since every point does. Q.E.D.

LEMMA 3.3. *Let Γ be an absolutely irreducible projective plane curve of degree n defined over a field K of characteristic 0. Suppose that the multiplicity of the singular points of Γ is 2. Then there exists a K-rational point through $O \in \mathbf{P}^2 - \Gamma$ such that:*

(*) *every line that passes through O cuts Γ in at least $n-1$ points, and almost every line that passes through O cuts Γ in n points.*

Proof. Let O be a K-rational point of $\mathbf{P}^2 - \Gamma$ that satisfies conditions (a)–(e) of Lemma 3.2. We prove that O satisfies (*).

Let L be a line in $\mathbf{P}^2$ that passes through O, and denote by $P_1, \ldots, P_m$ its intersection points with Γ. By Bezout's theorem

$$n = \sum_{i=1}^{m} i(\Gamma, L; P_i). \tag{1}$$

Suppose first that L is not a tangent to Γ and does not pass through singular points of Γ. By (e), there are at most finitely many lines that fail to satisfy this condition. In this case we have that $i(\Gamma, L; P_i) = 1$ for $i = 1, \ldots, m$. It follows from (1) that $m = n$.

Suppose now that L is tangent to Γ, say in P_1. Then P_1 is a simple point of Γ which is not an inflection point, as follows from (b) and (d). Hence $i(\Gamma, L; P_1) = 2$. If $2 \leqslant i \leqslant m$, then P_i is simple and L is not a tangent to Γ at P_i, as follows from (a) and (d); hence $i(\Gamma, L; P_i) = 1$. It follows from (1) that $m = n - 1$.

The last possibility is that L passes through a singular point, say P_1, which is, by assumption, of multiplicity 2. L is not a tangent to Γ, by (d); hence $i(\Gamma, L; P_1) = 2$. If $2 \leqslant i \leqslant m$, then P_i is simple, as follows from (c), hence $i(\Gamma, L; P_1) = 1$. It follows from (1) that $m = n - 1$. Q.E.D.

We come now to our main theorem.

THEOREM 3.4. *Every field of characteristic 0 is symmetrically stable.*

Proof. By Lemma 1.1, it suffices to prove that if K is a field of characteristic 0 and F is a finitely generated regular extension of K of dimension 1, then F is symmetrically stable over K. Indeed, by Lemma 3.1, F/K has a projective plane model Γ, and all of its singular points are of multiplicity 2. Thus Γ is an absolutely irreducible curve, since F/K is regular of dimension 1. Let $n = \deg \Gamma$. Then, by Lemma 3.3, there exists a K-rational point $O \in P^2 - \Gamma$ such that (*) is satisfied. It follows from Lemma 2.1 that F is a symmetrically stable extension of K. Q.E.D.

4. **An Application: Construction of a Normal PAC Hilbertian Extension of $\mathbf{Q}$.** The question of the existence of a proper PAC subfield of $\tilde{\mathbf{Q}}$ was raised by Ax in [2, p. 269] and answered positively in [6, p. 76]. Indeed, it was proved in [6] that if K is a denumerable hilbertian field of characteristic 0 (and in particular if $K=\mathbf{Q}$) and e is a positive integer, then for almost all $(\sigma_1,\dots,\sigma_e)\in \mathcal{G}(\tilde{K}/K)^e$, the fixed field, $\tilde{K}(\sigma)$, of $(\sigma_1,\dots,\sigma_e)$ in $\tilde{K}$ is PAC. It is also known that every algebraic separable extension of a PAC field is also a PAC field (see Ax [2, p. 268] or Lemma 4.1 below). Hence if $\tilde{K}(\sigma)$ is a PAC field, then every intermediate field $\tilde{K}(\sigma)\subseteq M\subseteq\tilde{K}$ is also PAC. It is strongly believed that in this situation M cannot be normal over K unless $M=\tilde{K}$ (cf. [7, p. 303, Problem 6]). The stability of K makes it now possible to construct a normal algebraic extension M of K such that M is PAC and in addition does not contain any field of the form $\tilde{K}(\sigma)$. We are thus supplied with "new" PAC fields. In addition, these fields can be explicitly constructed. In contrast, the previous PAC fields were known to exist only by a sophisticated measure theoretic argument.

We also note that in [6] we posed the question of fields which are simultaneously PAC and hilbertian. Examples of such fields were provided in [4]. These examples were however of an infinite transcendence degree over the ground field, and it was asked in [4] whether one can construct subfields of $\mathbf{Q}$ which are both PAC and hilbertian. This is done now. In fact, we construct the above field M in such a way that it is also hilbertian.

We begin by a reduction lemma.

An absolutely irreducible polynomial $f\in K[T_1,\dots,T_r,X]$ is said to be *stable* (*symmetrically stable*) *over* K *with respect to* $T_1,\dots,T_r$ if $\partial f/\partial X\neq 0$ and if there exist elements $t_1,\dots,t_r,x$ such that (i) $f(\mathbf{t},x)=0$; (ii) $t_1,\dots,t_r$ are algebraically independent over K; (iii) $\{t_1,\dots,t_r\}$ is a stabilizing (symmetrically stabilizing) base for $K(\mathbf{t},x)/K$.

LEMMA 4.1. *Let K be a field of characteristic 0, and let M be an algebraic extension K. A sufficient (and obviously necessary) condition for M to be PAC is that for every polynomial $f\in K[T_1,\dots,T_r,X]$ which is symmetrically stable over K with respect to $T_1,\dots,T_r$, such that $\deg_x f\geqslant 2$, and for every non-void K-open subset A of the affine space S^r, there exist $a_1,\dots,a_r,b\in M$ such that $(\mathbf{a})\in A$ and $f(\mathbf{a},b)=0$.*

Proof. Let W be an absolutely irreducible variety defined over K, and let F be its function field over K. Then F is a finitely generated regular extension of K. By Theorem 3.4, F is symmetrically stable over K. Let $t_1,\dots,t_r$ be a symmetrically stabilizing base for F/K. Then F is a finite extension of $K(\mathbf{t})$; hence there exists an $x\in F$ such that $F=K(\mathbf{t},x)$. Let $f\in K[T_1,\dots,T_r,X]$ be an irreducible polynomial such that $f(\mathbf{t},x)=0$. Then f is absolutely irreducible and

symmetrically stable over K with respect to $T_1, \ldots, T_r$. Moreover, there exists a birational map φ of the hypersurface $V(f)$ defined by $f(\mathbf{T}, X)=0$ into W, and there exists a non-void K-open subset A of S^r such that φ is defined in every point of $V(f)\cap(A\times S^1)$. By assumption, $V(f)\cap(A\times S^1)$ contains an M-rational point (a, b) (the case $\deg_x f=1$ being trivial). The point $\varphi(\mathrm{a}, b)$ is an M-rational point of W.

Consider now an absolutely irreducible variety V defined over M. By descent theory there exists an absolutely irreducible variety W defined over K and an epimorphism $\pi: W\to V$ defined over M (see Weil [16, p. 5]). By the first part of the proof, W has an M-rational point P. Its image, $\pi(P)$, is an M-rational point of V.

Thus, M is a PAC field. Q.E.D.

The following Lemma follows from Theorem 1 of Kuyk in [42]. It is also proved in [17].

LEMMA 4.2. *Let N be a normal extension of a hilbertian field K, and let $\mathcal{G}(N/K)\cong\prod_{i=1}^{\infty}G_i\times\prod_{j=1}^{\infty}H_j$, where the G_i's and H_j's are finite groups. Denote by $\mathcal{G}$ and $\mathcal{H}$ the families of all simple finite groups that appear as factors in the decomposition sequences of the G_i's and H_j's respectively. If $\mathcal{G}\cap\mathcal{H}=\varnothing$, then N is a hilbertian field.*

We shall also need the following lemma.

LEMMA 4.3. *For every field K there exists a polynomial $g\in K[T_1, \ldots, T_5, Y]$ which is stable with respect to $T_1, \ldots, T_5$ such that $\mathcal{G}(g(\mathbf{T}, Y), K(\mathbf{T}))\cong\mathbf{Z}/5\mathbf{Z}$.*

Proof. Let $\{x_0, x_1, x_2, x_3, x_4\}$ be a set of five algebraically independent elements over K, and consider the action of the group $\mathbf{Z}/5\mathbf{Z}$ on this set given by $n\cdot x_i=x_{i+n(\mathrm{mod}\ 5)}$. Let E be the fixed field of $\mathbf{Z}/5\mathbf{Z}$ in $K(\mathbf{x})$. Then $K(\mathbf{x})$ is Galois over E, and $\mathcal{G}(K(\mathbf{x})/E)\cong\mathbf{Z}/5\mathbf{Z}$. The field E is rational over K, i.e., E contains five algebraically independent elements $t_1, \ldots, t_5$ over K such that $E=K(\mathbf{t})$ (cf. Lenstra [11, p. 321]). If we take a $y\in K(\mathbf{x})$ such that $K(\mathbf{x})=K(t, y)$ and an irreducible polynomial $g\in K[\mathbf{T}, Y]$ such that $g(\mathbf{t}, y)=0$, then g is stable over K with respect to $\mathbf{T}$ and $\mathcal{G}(g(\mathbf{T}, Y), K(\mathbf{T}))\cong\mathbf{Z}/5\mathbf{Z}$. Q.E.D.

THEOREM 4.4. *Let K be a denumerable hilbertian field of characteristic 0. Then there exists a normal extension N of K with the following properties:*

(1) *$\mathcal{G}(N/K)$ is isomorphic to the direct product of infinitely many finite groups.*

(2) *N is a hilbertian field.*
(3) *N contains no field of the form $\tilde{K}(\sigma)$, where $(\sigma)\in\mathcal{G}(\tilde{K}/K)^e$.*

Proof. The set S of all pairs (f,A), where $f\in K[T_1,\dots,T_r,X]$ is absolutely irreducible and symmetrically stable over K with respect to $\mathbf{T}$, $\deg_x f\geqslant 2$, and A is a non-void K-open subset of S^r $(r\geqslant 1)$, is countable. Order S in a sequence $(f_1,A_2),(f_2,A_2),(f_3,A_3),\dots$, and construct by induction a triple sequence of normal extensions of K, $\{K_i,L_i,M_i|i=1,2,3,\dots\}$, which is linearly disjoint over K such that for every $i\geqslant 1$:

(a) $\mathcal{G}(K_i/K)\cong\mathbf{Z}/2\mathbf{Z}$,
(b) $\mathcal{G}(L_i/K)\cong\mathbf{Z}/5\mathbf{Z}$,
(c) $\mathcal{G}(M_i/K)\cong S_{n_i}$,
(d) A_i contains a K-rational point (a) and M_i contains an element b such that $f_i(\mathbf{a},b)=0$.

Indeed, suppose that $\{K_i,L_i,M_i|i=1,\dots,n-1\}$ have already been constructed, and let J be their composition. The polynomial X^2-T is obviously irreducible over J; hence there exists a $c\in K$ such that X^2-c is irreducible over J. Let $c'\in\tilde{K}$ be such that $c'^2-c=0$, and let $K_n=K(c')$. Then $[k_n:K]=2$, and K_n is linearly disjoint from J over K. Consider next the polynomial $g\in K[T_1,\dots,T_5,Y]$ that appears in Lemma 4.3. By [5, Lemma 5.1] there exist $d_1,\dots,d_5\in K$ such that

$$\mathcal{G}(g(\mathbf{d},Y),K)\cong\mathcal{G}(g(\mathbf{d},Y),JK_n)\cong\mathbf{Z}/5\mathbf{Z}.$$

Denote the splitting field of $g(\mathbf{d},Y)$ over K by L_n. Then L_n is a normal extension of K which is linearly disjoint from JK_n over K, and $\mathcal{G}(L_n/K)\cong\mathbf{Z}/5\mathbf{Z}$. At last consider the pair (f_n,A_n). Then polynomial f_n is stable over K and $\mathcal{G}(f(\mathbf{T},X),K(\mathbf{T}))\cong S_k$ for some $k\geqslant 2$. Hence, again by [5, Lemma 5.1], there exists a K-rational point $(\mathbf{a})\in A_n$ such that

$$\mathcal{G}(f_n(\mathbf{a},X),K)\cong\mathcal{G}(f_n(\mathbf{a},X),JK_nL_n)\cong S_k.$$

Denote the splitting field of $f_n(\mathbf{a},X)$ over K by M_n. Then M_n is a finite normal extension of K which is linearly disjoint from JK_nL_n, and there is an element $b\in M_n$ such that $f(\mathbf{a},b)=0$. The induction is now completed.

Let K', L and M be the fields generated by all the K_n's, L_n's and M_n's respectively, and let $N=LM$. Then:

(e) K', L and M are linearly disjoint normal extensions of K. In particular K' is linearly disjoint from N over K.
(f) $\mathcal{G}(K'/K)\cong\prod_{n=1}^{\infty}\mathcal{G}(K_n/K)\cong\prod_{n=1}^{\infty}\mathbf{Z}/2\mathbf{Z}$. In particular $\mathcal{G}(K'/K)$ is not finitely generated (in the topological sense).

(g) We have

$$\mathcal{G}(N/K)\cong\mathcal{G}(L/K)\times\mathcal{G}(M/K),$$

$$\mathcal{G}(L/K)\cong\prod_{n=1}^{\infty}\mathcal{G}(L_n/K)\cong\prod_{n=1}^{\infty}\mathbf{Z}/5\mathbf{Z},$$

$$\mathcal{G}(M/K)\cong\prod_{n=1}^{\infty}\mathcal{G}(M_n/K)\cong\prod_{n=1}^{\infty}S_{r_n}.$$

We see only one group appears in the decomposition sequences of the $\mathcal{G}(L_n/K)$'s, namely $\mathbf{Z}/5\mathbf{Z}$. The groups which can appear in the decomposition sequences of the $\mathcal{G}(M_n/K)$'s are only the A_{r_n}'s and $\mathbf{Z}/2\mathbf{Z}$, and none of them is equal to $\mathbf{Z}/5\mathbf{Z}$. By Lemma 4.2, N is hilbertian.

(h) N is a PAC field, by Lemma 4.1, since every pair (f,A) in S appears as a certain (f_n,A_n), and for the latter there exists an M_n-rational point $(\mathbf{a},b)$ which is obviously also an N-rational point, such that $(\mathbf{a})\in A$ and $f(\mathbf{a},b)=0$.

(i) N satisfies condition (4). Indeed, suppose that there were a positive integer e and $\sigma_1,\ldots,\sigma_e\in\mathcal{G}(\tilde{K}/K)$ such that $\tilde{K}(\boldsymbol{\sigma})\subseteq N$. Then $\tilde{K}(\boldsymbol{\sigma})$ would be linearly disjoint from K' over K, by (d). It would follow that $\mathcal{G}(K'/K)\cong\mathcal{G}(\tilde{K}(\boldsymbol{\sigma})K'/\tilde{K}(\boldsymbol{\sigma}))$, hence $\mathcal{G}(K'/K)$ would be generated by e elements, which is a contradiction to (f).

Remark. The author's original construction was of a field N having properties (1) and (3) above. W. D. Geyer showed then that the construction can be strengthened in such a way that N would also be hilbertian.

QUESTION. Does a PAC hilbertian F have the property that each finite group can be realized as a Galois group of a Galois extension L over F?

UNIVERSITY OF CALIFORNIA, IRVINE.
TEL-AVIV UNIVERSITY.

REFERENCES.

[1] S. S. Abhyankar, *Algebraic Space Curves*, Montréal U. P., Montréal, 1971.
[2] J. Ax, The elementary theory of finite fields, *Ann. of Math.* 88 (1968), pp. 239–271.
[3] C. Chevalley, *Introduction to the Theory of Algebraic Functions of One Variable*, Amer. Math. Soc., 1951.

[4] M. Fried, A review to Jarden's paper "Elementary statements over large algebraic fields," *Math. Reviews* **46** (1973), #1795.
[5] M. Fried and M. Jarden, Stable extensions and fields with the global density property, *Canad. J. Math.*, No. 4, August 1976, pp. 774–787.
[6] M. Jarden, Elementary statements over large algebraic fields, *Trans. Amer. Math. Soc.* **164** (1972), pp. 67–91.
[7] ———, Algebraic extensions of finite corank of hilbertian fields, *Israel J. Math.* **18** (1974), pp. 279–307.
[8] W. Kuyk, Extensions de corps hilbertiens, *J. Algebra* **14** (1970), pp. 112–124.
[9] S. Lang, *Introduction to Algebraic Geometry*, Interscience, New York, 1958.
[10] S. Lefschetz, *Algebraic Geometry*, Princeton U. P., Princeton, 1953.
[11] H. W. Lenstra, Jr., Rational function invariant under a finite abelian group, *Invent. Math.* **25** (1974), pp. 299–325.
[12] H. Popp, Zur Reductionstheorie algebraischer Funktionenkörper vom Transzendenzgrad 1: Existenz einer regularen Reduktion zu vorgegebenen Funktionenkörper als Restklassenkörper, *Arch. Math. (Basel)* **17** (1966), pp. 510–522.
[13] A. Seidenberg, *Elements of the Theory of Algebraic Curves*, Addison-Wesley, 1968.
[14] I. R. Shafarevich, *Basic Algebraic Geometry*, Springer, Berlin, 1974.
[15] B. L. van der Waerden, *Einführung in die algebraische Geometrie*, Springer, Berlin, 1939.
[16] A. Weil, *Adeles and Algebraic Groups*, Institute for Advanced Studies, Princeton, N.J., 1961.
[17] P. Zorn, Der hilbertsche Irreduzibilitatssatz, Staatsexamenarbeit, Erlangen, 1975.