K. UCHIDA
KODAI MATH. J.
3 (1980), 83—95

SEPARABLY HILBERTIAN FIELDS

By Kôji Uchida

Let t and X be indeterminates. Let $f_i(t, X)$, $i=1, \cdots, m$ be irreducible polynomials over a field k and let $a(t)$ be a non-zero polynomial over k. A field k is called Hilbertian [6] if for any choice of f_i and a there exists an element s of k such that every $f_i(s, X)$ is irreducible and $a(s)\neq 0$. Any Hilbertian field of non-zero characteristic p is non-perfect because it has an element s such that X^p-s is irreducible. But this is not essential in applications of Hilbertian fields, and a slight modification of the definition allows us perfect Hilbertian fields. Let t and X be indeterminates. Let $f(t, X)$ be a polynomial over a field k such that it is separably irreducible over $k(t)$ as a polynomial of X. A field k is called separably Hilbertian if for any choice of such $f(t, X)$ it contains an element s such that $f(s, X)$ is separably irreducible over k. Let k be a Hilbertian field and let $f(t, X)$ be a polynomial over k which is separably irreducible with respect to X. Then the discriminant $D_f(t)$ is not zero. Now there exists an element s of k such that $f(s, X)$ is irreducible and $D_f(s)\neq 0$. Then $f(s, X)$ is separably irreducible, i.e., any Hilbertian field is separably Hilbertian. It has been known and will be shown below that two definitions are equivalent when the characteristic of a field k is zero. In the first section, it will be shown that a field k of non-zero characteristic is Hilbertian if and only if it is separably Hilbertian and non-perfect. In section 2, we will show some extensions of separably Hilbertian fields are also separably Hilbertian. Galois groups of extensions of separably Hilbertian fields of cohomological dimension 1 will be dealt in the last section. We will remark here an important application of Hilbertian fields essentially due to Lang [7] which does not seem to be well known. Let k be a field of characteristic p containing a finite field F_q. Let G be a connected linear algebraic group defined over F_q. Let x be a generic point of G over k. Then $k(x)$ is a finite Galois extension of $k(x^{-1}\cdot x^{(q)})$ with Galois group $G(F_q)$, the rational points of G over F_q. As $x^{-1}\cdot x^{(q)}$ is also a generic point of G over k, $k(x^{-1}\cdot x^{(q)})$ is isomorphic to $k(x)$ over k. This shows that if k is (separably) Hilbertian and if $k(x)$ is purely transcendental over k, k has a Galois extension with Galois group $G(F_q)$. It is known that $k(x)$ is purely transcendental if G splits over k. For example, let $\bar{F}_p$ be the algebraic closure of F_p and let t be an indeterminate. Then $\bar{F}_p(t)$ has a Galois extension with Galois group $G(F_q)$ for any connected linear

Received February 7, 1979

algebraic group G defined over a finite extension F_q of F_p.

1. Hilbertian fields and separably Hilbertian fields.

Let k be a field and let u be an indeterminate. Then it is known that $k(u)$ is Hilbertian. This was first proved by Franz [1] for infinite fields k and by Inaba [3] in the general case. This theorem will be used in the reduction step. A proof of this theorem in the case k is infinite is rather elementary, and we only need this case because every separably Hilbertian field is infinite.

LEMMA 1. *Finite fields are not separably Hilbertian.*

Proof. Let F_q be a finite field with q elements. Let l be a prime number which is not a divisor of q. A polynomial $f(t, X)=X^l-t+t^q$ is separably irreducible, but $f(s, X)=X^l$ is not irreducible for any $s\in F_q$.

LEMMA 2. *Let k be a separably Hilbertian field. Let $t_1, \cdots, t_l$ and X be indeterminates. Let a polynomial $f(t_1, \cdots, t_l; X)$ be separably irreducible over $k(t_1, \cdots, t_l)$ and let $a(t_1, \cdots, t_l)$ be a non-zero polynomial. Then there exist elements $s_1, \cdots, s_l$ of k such that $f(s_1, \cdots, s_l; X)$ is separably irreducible over k and $a(s_1, \cdots, s_l)\neq 0$.*

Proof. We first assume $l=1$ and we put

$$f(t_1, X)=b_0(t_1)X^n+b_1(t_1)X^{n-1}+\cdots+b_n(t_1).$$

If $n=1$, the assertion is easy as k is infinite. We assume $n\geqq 2$. As the polynomial

$$g(t_1, X)=X^n+a(t_1)b_1(t_1)X^{n-1}+\cdots+a(t_1)^n b_0(t_1)^{n-1}b_n(t_1)$$

is separably irreducible, there exists an element s_1 of k such that $g(s_1, X)$ is separably irreducible. Neither $a(s_1)$ nor $b_0(s_1)$ is zero for such s_1, and $f(s_1, X)$ is separably irreducible. We now assume $l\geqq 2$. Then the field $k(t_1, \cdots, t_{l-1})$ is Hilbertian by Franz-Inaba theorem. Let $D_f(t_1, \cdots, t_l)$ be the discriminant of $f(t_1, \cdots, t_l; X)$. Then we can find a rational function $ct_1, \cdots, t_{l-1})$ such that $f(t_1, \cdots, t_{l-1}, c(t_1, \cdots, t_{l-1}); X)$ is irreducible and $a(t_1, \cdots, t_{l-1}, c(t_1, \cdots, t_{l-1}))$ $D_f(t_1, \cdots, t_{l-1}, c(t_1, \cdots, t_{l-1}))\neq 0$. We put

$$f(t_1, \cdots, t_{l-1}, c(t_1, \cdots t_{l-1}); X)=d(t_1, \cdots t_{l-1})^{-1}g(t_1, \cdots, t_{l-1}; X)$$

where $g\in k[t_1, \cdots t_{l-1}; X]$ and d is a power of the denominator of c. By the induction, we can find elements $s_1, \cdots, s_{l-1}$ of k such that $g(s_1, \cdots, s_{l-1}; X)$ is separably irreducible, $d(s_1, \cdots, s_{l-1})\neq 0$, $a(s_1, \cdots, s_{l-1}, c(s_1, \cdots, s_{l-1}))\neq 0$ and $D_f(s_1, \cdots, s_{l-1}, c(s_1, \cdots s_{l-1}))\neq 0$. Then $s_l=c(s_1, \cdots, s_{l-1})$ is an element of k such that $f(s_1, \cdots, s_l; X)$ is separably irreducible and $a(s_1, \cdots, s_l)\neq 0$.

Let k be a field and let $t_1, \cdots t_l$ be indeterminates. We put $R=k[t_1, \cdots t_l]$. Let $f_i(t_1, \cdots t_l; X)$, $i=1, \cdots, m$, be separably irreducible polynomials over R. Let α_i be a root of $f_i(t_1, \cdots, t_l; X)=0$ in the algebraic closure of $k(t_1, \cdots t_l)$.

Any l-tuple $(s_1, \cdots s_l)$ of elements of k determines a maximal ideal $(t-s)=(t_1-s_1, \cdots, t_l-s_l)$ of R. Let R_s be the local ring determined by this maximal ideal. We put $S=R_s[\alpha_1, \cdots \alpha_m]$ and $S_{(j)}=R_s[\alpha_{j_1}, \cdots \alpha_{j_r}]$ for any subset $(j)=(j_1, \cdots j_r)$ of $(1, \cdots m)$. Let β_i be the residue class of α_i in $S/(t-s)S$.

LEMMA 3. *Let $a_i(t_1, \cdots t_l)$ and $D_i(t_1, \cdots, t_l)$ be the leading coefficient and the discriminant of $f_i(t_1, \cdots, t_l; X)$ respectively. If we choose $s_1, \cdots s_l$ as $a_i(s_1, \cdots s_l)D_i(s_1, \cdots s_l)\neq 0$ for every i, $S_{(j)}$ is the integral closure of R_s in the field $k(t_1, \cdots t_l; \alpha_{j_1}, \cdots, \alpha_{j_r})$ for any (j).*

Proof. Our assumption shows every α_i is integral over R_s. We only need to show $S_r=R_s[\alpha_1, \cdots, \alpha_r]$ is integrally closed for any r. It is clear for $r=0$. We assume S_{r-1} is integrally closed. As the defining polynomial of α_r over S_{r-1} divides $f_r(t_1, \cdots, t_l; X)$, our assumption shows the discriminant of that is a unit in S_{r-1}. Let

$$\beta=b_0+b_1\alpha_r+\cdots+b_{q-1}\alpha_r^{q-1}, \qquad b_i\in k(t_1, \cdots, t_l; \alpha_1, \cdots \alpha_{r-1})$$

be integral over S_{r-1}, where q is the degree of α_r over S_{r-1}. We get q equations by replacing α_r to its conjugates. By solving these equations with respect to b_i, we see $b_0, \cdots b_{q-1}\in S_{r-1}$ as every conjugate of β is integral over S_{r-1}. This proves S_r is integrally closed.

LEMMA 4. *Let k be a separably Hilbertian field. Let $f_i(t_1, \cdots t_l; X)$, $i=1, \cdots m$, be separably irreducible with respect to X, and let $a(t_1, \cdots, t_l)$ be a non-zero polynomial. Then there exist elements $s_1, \cdots, s_l$ in k such that every $f_i(s_1, \cdots s_l; X)$ is separably irreducible and $a(s_1, \cdots s_l)\neq 0$.*

Proof. Let α_i and β_i be as above. As every α_i is separable over $k(t_1, \cdots, t_l)$, we can find an element α such that $k(t_1, \cdots t_l; \alpha_1, \cdots, \alpha_m)=k(t_1, \cdots, t_l; \alpha)$. Let $f(t_1, \cdots, t_l; X)$ be the defining polynomial of α. Lemma 2 shows that we can find $s_1, \cdots, s_l$ in k such that $f(s_1, \cdots, s_l; X)$ is irreducible, $a(s_1, \cdots, s_l)\neq 0$ and they satisfy the conditions of Lemma 3 for every f_i and f. Then $S=R_s[\alpha]=R_s[\alpha_1, \cdots, \alpha_m]$ is integrally closed. Let β be a root of $f(s_1, \cdots, s_l; X)=0$. Then $S/(t-s)S\cong k[\beta]$ is a field as $f(s_1, \cdots, s_l; X)$ is irreducible. Hence $(t-s)$ is a maximal ideal of $S_{(j)}$ for all (j). Then $R_s[\alpha_i]/(t-s)R_s[\alpha_i]\cong k(\beta_i)$ is a field and

$$[k(\beta_i): k]=[R_s[\alpha_i]: R_s]=[k(t_1, \cdots, t_l; \alpha_i): k(t_1, \cdots, t_l)].$$

This shows $f_i(s_1, \cdots, s_l; X)$ is irreducible, and it is separable by our chice of $s_1, \cdots, s_l$.

Remark. This lemma shows a field k of characteristic 0 is Hilbertian if and only if it is separably Hilbertian.

THEOREM 1. *Let k be a separably Hilbertian field and let $t_1, \cdots, t_l$ be indeterminates. We put $K=k(t_1, \cdots, t_l)$. Let $K(\alpha_1, \cdots, \alpha_m)$ be a Galois extension*

of K with Galois group G and let $f_i(t_1, \cdots, t_l; X)$ be the defining polynomial of α_i. Then we can find $s_1, \cdots, s_l$ in k and roots β_i of $f_i(s_1, \cdots, s_l; X)=0$ such that $k(\beta_1, \cdots, \beta_m)$ is a Galois extension whose Galois group is isomorphic to G and intermediate fields $K(\alpha_{j_1}, \cdots, \alpha_{j_r})$ correspond to $k(\beta_{j_1}, \cdots, \beta_{j_r})$ through this isomorphism for all (j).

Proof. We can find an element α such that $K(\alpha)=K(\alpha_1, \cdots, \alpha_m)$. Let $f(t_1, \cdots, t_l; X)$ be the defining polynomial of α. We can find $s_1, \cdots, s_l$ in k as in the proof of Lemma 4. Then $S=R_s[\alpha]=R_s[\alpha_1, \cdots, \alpha_m]$ is integrally closed and $f(s_1, \cdots, s_l; X)$ is separably irreducible. The Galois group G operates on S and on $(t-s)S$. Hence G operates on $S/(t-s)S \cong k(\beta)$ where β is a root of $f(s_1, \cdots, s_l; X)=0$. As G operates faithfully on $S/(t-s)S$, $k(\beta)$ is a Galois extension of k whose Galois group is isomorphic to G. The proof of Lemma 4 shows

$$R_s[\alpha_{j_1}, \cdots, \alpha_{j_r}]/(t-s)R_s[\alpha_{j_1}, \cdots, \alpha_{j_r}] \cong k(\beta_{j_1}, \cdots, \beta_{j_r}).$$

Hence $K(\alpha_{j_1}, \cdots, \alpha_{j_r})$ and $k(\beta_{j_1}, \cdots, \beta_{j_r})$ are fixed fields of corresponding subgroups.

LEMMA 5. *Let k be a field of non-zero characteristic p. Let $f(X)$ be a separably irreducible polynomial over k whose leading coefficient is 1 and which has a coefficient not contained in k^p. Then $f(X^q)$ is irreducible over k for any power q of p.*

Proof. Let α be a root of $f(X^q)=0$. Then $\beta=\alpha^q$ is a root of $f(X)=0$. We have to show $[k(\alpha): k(\beta)]=q$. As $[k(\alpha): k(\beta)]$ is a power of p and is not greater than q, $\alpha^{q/p}$ should be contained in $k(\beta)$ if $[k(\alpha): k(\beta)]<q$. Then $k(\alpha^{q/p})=k(\beta)$ and $\alpha^{q/p}$ satisfies an equation

$$X^n+a_1X^{n-1}+\cdots+a_n=0, \qquad a_i \in k, \qquad n=[k(\beta): k].$$

Then β satisfies

$$X^n+a_1{}^pX^{n-1}+\cdots+a_n{}^p=0,$$

which is impossible by our assumption.

LEMMA 6. *Let k be a non-perfect field of characteristic p. Let $h(t)$ be a polynomial over k which is not contained in $k^p[t^p]$. If there exist elements a of k such that $h(t+a) \in k^p[t]$, they are contained in a unique residue class of the additive group k mod k^p. Let b be an element of k such that $h(t+b) \notin k^p[t]$. Then the number of elements c of k such that $h(b+c^p) \in k^p$ is at most finite.*

Proof. Let $g(t)=h(t+a) \in k^p[t]$. Let b be an element of k such that $c=b-a$ is not in k^p. We put

$$g(t)=g_1(t^p)+g_2(t), \qquad g_1(t^p) \in k^p[t^p], \qquad g_2(t) \in k^p[t].$$

Then $g_2(t)$ is not zero and whose degree m is not a multiple of p. As

$$h(t+b)=g(t+c)=g_1(t^p+c^p)+g_2(t+c)$$

and as $g_1(t^p+c^p)\in k^p[t^p]$, the coefficient of degree $m-1$ of $h(t+b)$ is not contained in k^p. Now let $h(t+b)\notin k^p[t]$. Then there exist elements $1, u_2, \cdots, u_r$ of k which are linearly independent over k^p such that

$$h(t+b)=\phi_1(t)+\phi_2(t)u_2+\cdots+\phi_r(t)u_r, \qquad \phi_i(t)\in k^p[t].$$

Our assumption asserts at least one of $\phi_2(t), \cdots \phi_r(t)$ is not zero. If

$$h(b+c^p)=\phi_1(c^p)+\phi_2(c^p)u_2+\cdots+\phi_r(c^p)u_r\in k^p,$$

it must be $\phi_2(c^p)=\cdots=\phi_r(c^p)=0$. Hence such elements are at most finite.

THEOREM 2. *Let k be a field of non-zero characteristic p. It is Hilbertian if and only if it is separably Hilbertian and non-perfect.*

Proof. If k is Hilbertian, it has been shown that it is separably Hilbertian and non-perfect. We now assume that k is separably Hilbertian and non-perfect. Let $f_i(t, X)$, $i=1, \cdots, m$, be any irreducible polynomials and let $a(t)$ be any non-zero polynomial. We can assume that the leading coefficient of every $f_i(t, X)$ is 1. Let $f_1, \cdots, f_l$ be inseparable, and let $f_{l+1}, \cdots, f_m$ be separable. We can find a separably irreducible polynomial $g_i(t, X)$ for any $i=1, \cdots, l$ such that $f_i(t, X)=g_i(t, X^{q_i})$ for some power q_i of p. Then g_i has the leading coefficient 1 and has a coefficient $h_i(t)$ which is not in $k^p[t^p]$ as f_i is irreducible. As the additive group k/k^p has infinitely many residue classes, there exists an element b of k such that

$$h_i(t+b)\notin k^p[t], \qquad i=1, \cdots, l.$$

We put $g_i=f_i$ for $i=l+1, \cdots, m$. As $g_i(t+b, X)$ are separably irreducible with respect to X, $g_i(t^p+b, X)$ are also separably irreducible. There exist only a finite c_j in k such that $h_i(b+c_j{}^p)\in k^p$ for some $i=1, \cdots, l$. Let $d(t)$ be the product of $a(b+t^p)$ and all $t-c_j$ for such c_j. Then Lemma 4 shows there exists an element r of k such that $g_i(b+r^p, X)$, $i=1, \cdots m$, are separably irreducible and $d(r)\neq 0$. We put $s=b+r^p$. As $h_i(s)\notin k^p$ for $i=1, \cdots, l$, $g_i(s, X)$ has a coefficient which is not contained in k^p for every $i=1, \cdots, l$. Then every $f_i(s, X)$ is irreducible and $a(s)\neq 0$. This shows k is Hilbertian.

2. Extensions of separably Hilbertian fields.

LEMMA 7. *Finitely generated extensions of a separably Hilbertian (resp. Hilbertian) field k are also separably Hilbertian (resp. Hilbertian).*

Proof. If k is non-perfect, every finitely generated extension of k is also non-perfect. Hence we only need to prove the separably Hilbertian case. We can divide the proof into three steps, i. e., purely transcendental extensions, separably algebraic extensions and purely inseparable extensions. First step

comes from Franz-Inaba theorem. For the second step, see [6]. Let K be a purely inseparable extension of k. In this case K does not need to be finitely generated. Let $f(t, X)$ be a separably irreducible polynomial over $K[t]$. We put

$$f(t, X)=a_0(t)X^n+a_1(t)X^{n-1}+\cdots+a_n(t).$$

Then we can find a power q of the characteristic such that

$$g(t, X)=a_0(t)^qX^n+a_1(t)^qX^{n-1}+\cdots+a_n(t)^q$$

is a polynomial over $k[t]$. Let α be a root of $f(t, X)=0$. Then α^q is a root of $g(t, X)=0$. As α is separable over $K(t)$, it must be $K(t, \alpha)=K(t, \alpha^q)$. This shows $g(t, X)$ is separably irreducible over $K(t)$, hence also over $k(t)$. Then we can find s in k such that $a_0(s)\neq 0$ and $g(s, X)$ is separably irreducible over k. Let β be a root of $g(s, X)=0$. As β is separable over k, it must be

$$n=[k(\beta): k]=[K(\beta): K]\leqq[K(\beta^{1/q}): K].$$

As $f(s, \beta^{1/q})=0$, $[K(\beta^{1/q}): K]\leqq n$. This shows $\beta^{1/q}$ is separable of degree n over K, i. e., $f(s, X)$ is separably irreducible over K.

We now show examples of infinite algebraic extensions of a separably Hilbertian field which are separably Hilbertian. These are generalizations of [5].

THEOREM 3. *Let k be a separably Hilbertian (resp. Hilbertian) field. Then*

i) *Every abelian extension of k is separably Hilbertian (resp. Hilbertian).*

ii) *Let K be contained in a nilpotent extension of k. If K contains a subfield E finite over k such that $[E: k]$ is divisible by at least two prime numbers, K is separably Hilbertian (resp. Hilbertian).*

Proof. If k is non-perfect, every separable extension is also non-perfect. Hence we only need to show the separably Hilbertian cases. Let K be an extension of k as in i) or ii). Let t be an indeterminate and let $f(t, X)$ be a separably irreducible polynomial over $K[t]$. Let α be a root of $f(t, X)=0$ and we choose an element β such that $K(t, \alpha)\subset K(t, \beta)$ and $K(t, \beta)$ is a Galois extension of $K(t)$. We can find a finite subextension E of K such that every coefficient of $f(t, X)$ is in E, $E(t, \beta)$ is a Galois extension of $E(t)$ whose Galois group is isomorphic to that of $K(t, \beta)$ over $K(t)$, and $[E: k]$ is divisible by at least two primes in case ii). Then there exists a field F such that $E\supset F\supset k$, E is a cyclic extension of F of degree $n>1$, and n is divisible by at least two primes in case ii). Let σ be a generator of $G(E/F)$. Let $t=t_1, \cdots, t_n$ be indeterminates and let σ operate as $\sigma(t_i)=t_{i+1}$, $i=1, \cdots, n-1$, and $\sigma(t_n)=t_1$. Then σ determines an automorphism of $E(t_1, \cdots, t_n)$ of order n. Let σ also denote an extension to an automorphism of the algebraic closure of $E(t_1, \cdots, t_n)$. We put $\alpha=\alpha_1$, $\beta=\beta_1$, and we define $\alpha_1, \cdots, \alpha_n, \beta_1, \cdots, \beta_n$ by $\sigma(\alpha_i)=\alpha_{i+1}$ and $\sigma(\beta_i)=\beta_{i+1}$, $i=1, \cdots, n-1$. Though $\sigma(\beta_n)$ may not be β_1, σ causes an automorphism of $E(t_1, \cdots, t_n, \beta_1, \cdots, \beta_n)$ because $\sigma(\beta_n)=\sigma^n(\beta_1)$ is in $E(t_1, \beta_1)$. Let

$E=F(\gamma)$, $\gamma=\gamma_1$ and $\sigma(\gamma_\imath)=\gamma_{\imath+1}$. Then the invariant subfield of σ in $E(t_1, \cdots, t_n)$ is $F(u_1, \cdots, u_n)$, where

$$u_\imath=\gamma_1{}^{\imath-1}t_1+\cdots+\gamma_n{}^{\imath-1}t_n, \qquad \imath=1, \cdots, n.$$

Then $u_1, \cdots, u_n$ are algebraically independent over F, and $E(t_1, \cdots t_n, \beta_1, \cdots, \beta_n)$ is a Galois extension of $F(u_1, \cdots, u_n)$. As F is separably Hilbertian, we can find elements $v_1, \cdots, v_n$ of F such that the specialization $u_i \mapsto v_i$ maps $E[t_1, \cdots, t_n, \beta_1, \cdots, \beta_n]/F[u_1, \cdots, u_n]$ to a Galois extension of F with isomorphic Galois group. Then $E[t_1, \cdots, t_n]$ maps onto E. If we put $t_i \mapsto s_i \in E$, $\alpha_i \mapsto \lambda_i$ and $\beta_i \mapsto \mu_\imath$, we can assume $E(\mu_\imath)/E$ is a Galois extension containing $\lambda_\imath$, and

$$[E(t, \alpha): E(t)]=[E(t_1, \cdots, t_n, \alpha_1): E(t_1, \cdots, t_n)]$$

$$=[E(\lambda_1): E].$$

As λ_1 is a root of $f(s_1, X)=0$, $f(s_1, X)$ is separably irreducible over K if $E(\mu_1)\cap K=E$. Let L be a subextension of $E(t, \beta)$ which consists of the algebraic elements over F. We can assume that L maps identically onto itself by the above specialization. Then

$$E \subset L\cap K \subset E(t_1, \beta_1)\cap K(t_1)\cap K=E(t_1)\cap K=E,$$

i. e., $E=L\cap K$. As $L(t_1, \beta_1)$ is a regular extension of L and as it is free from $L(t_\imath, \beta_\imath)$, $\imath\neq 1$, over L, they are linearly disjoint, i. e.,

$$L(t_1, t_\imath, \beta_1)\cap L(t_1, t_\imath, \beta_\imath)=L(t_1, t_\imath), \qquad \imath\neq 1.$$

Then

$$L(t_1, \cdots, t_n, \beta_1)\cap L(t_1, \cdots, t_n, \beta_\imath)=L(t_1, \cdots, t_n)$$

maps onto $L(\mu_1)\cap L(\mu_\imath)=L$ by the specialization. This shows $E(\mu_1)\cap E(\mu_\imath)\subset L$. When K is abelian, $E(\mu_1)\cap K$ is also abelian. Then it is invariant by σ. As σ maps $E(\mu_1)$ onto $E(\mu_2)$,

$$E(\mu_1)\cap K=E(\mu_1)\cap K\cap E(\mu_2)\subset L\cap K=E.$$

This proves the first case. In the second case $E(\mu_1)\cap K$ is contained in a nilpotent extension of F. Hence it is generated by elements of prime power degrees over F. So we only need to show that $\delta\in E$ for any element $\delta\in E(\mu_1)\cap K$ of the degree l^d for some prime l. By our assumption σ^m for some m has a prime order $r\neq l$ on E. Then there exists an isomorphism which coincides with σ^m on E and is the identity on $F(\delta)$. Such an isomorphism maps $E(\mu_1)$ onto $E(\mu_{m+1})$, $m+1\neq 1$. Hence δ is contained in $E(\mu_1)\cap E(\mu_{m+1})\cap K\subset L\cap K=E$.

Remark. Let k be a separably Hilbertian field and let K be the maximal p-extension of k for some prime p. Then K is not separably Hilbertian because it has no p-extension. Let α be contained in some nilpotent extension

of k, but not in K. Then $K(\alpha)$ is separably Hilbertian by our theorem. This example shows that K is not necessarily separably Hilbertian even if it has a finite extension which is separably Hilbertian.

3. Solvable extensions of separably Hilbertian fields of cohomological dimension 1. Let k be a field and let K be a finite Galois extension with Galois group H. Let

$$1 \to N \to E \xrightarrow{\pi} H \to 1$$

be a group extension of finite groups. We call L a field corresponding to this extension if L is a Galois extension containing K with Galois group isomorphic to E and π coincides with the restriction of the operation of $E=G(L/k)$ on K.

LEMMA 8. *Let k be a field and let Ω be a Galois extension of k with Galois group G. We assume that the cohomological dimension of G is 1. Let K be any finite Galois extension of k with Galois group H contained in Ω. Let*

$$1 \to A \to E \xrightarrow{\pi} H \to 1$$

be any split group extension with a finite abelian kernel A. We assume that there exists a field L in Ω corresponding to this extension. Then for any group extension

$$1 \to N \to F \xrightarrow{\tau} H \to 1$$

with a finite solvable kernel N, there exists a field M in Ω corresponding to this extension.

Proof. We assume that our assertion is true if the $n-1$-st commutator subgroup is trivial. Let the n-th commutator subgroup of N be trivial. Then the $n-1$-st commutator subgroup A is an abelian normal subgroup of F. By our assumption, there exists a field M' in Ω corresponding to the group extension

$$1 \to N/A \to F/A \xrightarrow{\pi} H \to 1$$

Then we only need to find a field M corresponding to the group extension

$$1 \to A \to F \to F/A \to 1\,.$$

That is, we only need to prove our assertion when N is abelian. We now assume N is abelian. Let $f: G \to H$ be the natural projection. As $\mathrm{cd}\, G=1$, we can find a continuous homomorphism $g: G \to F$ such that $\pi g=f$. Let $H_1=g(G)$ and let K_1 be the field corresponding to the kernel of g. Then K_1 contains K, $H_1=G(K_1/k)$ and $F=H_1 \cdot N$. Let $F_1=H_1 \times N$ be the semi-direct product by the natural action of H_1 on N. Then F is naturally a homomorphic image of F_1. As

$$1\to N\to F_1\to H_1\to 1$$

is a split extension with an abelian kernel N, there exists a field M_1 in Ω corresponding to this extension. Then the field corresponding to the kernel of $F_1\to F$ satisfies our condition.

LEMMA 9. *Let k be a separably Hilbertian field, and let K be a finite Galois extension with Galois group H. Let*

$$1\to A\to E\xrightarrow{\pi} H\to 1$$

be a split group extension with a finite abelian kernel A. Then there exists a field L corresponding to this extension.

Proof. We can assume A is an l-group for some prime l. First we assume l is not the characteristic of k. Let n be the exponent of A. Let K_1 be the field obtained by adjoining a primitive n-th root of unity to K. Let $H_1=G(K_1/k)$. As E is a homomorphic image of a group extension

$$1\to\sum(Z/nZ)H_1\to F\to H_1\to 1$$

where the kernel is a direct sum of finite copies of the group ring of H_1 over Z/nZ, we only need to find a field corresponding to this extension. Let $t_{i\sigma}$, $i=1,\cdots,r$, $\sigma\in H_1$, be indeterminates, where r is the number of copies of $(Z/nZ)H_1$ in the kernel. We define the operation of H_1 by ${}^{\sigma}t_{i\tau}=t_{i,\sigma\tau}$. Then H_1 operates on $K_1(t_{i\sigma}, i=1,\cdots,r, \sigma\in H_1)$. Let $K_1=k(\alpha)$. Then the invariant subfield of H_1 is generated by

$$u_{ij}=\alpha^{j-1}t_{ie}+\alpha^{(j-1)\sigma}t_{i\sigma}+\cdots+\alpha^{(j-1)\tau}t_{i\tau},$$

$H_1=\{e,\sigma,\cdots,\tau\}$, $i=1,\cdots,r$; $j=1,\cdots,m=[K_1: k]=|H_1|$, over k. That is, the invariant subfield M is purely transcendental over k. We note that $K_1(t_{i\sigma})$ $K_1(u_{ij})$. Then the field $K_1(\sqrt[n]{t_{i\sigma}})$ is a Galois extension of M with Galois group isomorphic to F. As k is separably Hilbertian, we get a Galois extension of k corresponding to the above group extension by substituting some values of k for u_{ij}. When l is the characteristic of k, we can find an irreducible polynomial $f(t, X)$ such that a root of $f(t, X)=0$ generates a cyclic extension of degree n over $K(t)$ by using the method of Witt vector. Then we determine indeterminates $t_{i\sigma}$ and the operation of H as above. If we consider a field adjoining all the roots of $f(t_{i\sigma}, X)=0$, the same argument shows the existence of a field corresponding to the given group extension.

Remark. Let k be a separably Hilbertian field of the cohomological dimension 1, i.e., cd $G(k_s/k)=1$, where k_s is the separable closure of k. Then k_s/k satisfies the conditions of Lemma 8. Examples of such fields are function fields of one variable over an algebraically closed field and the maximal abelian extension of the rationals.

We can say a little more for algebraic number fields. Let k be an algebraic number field (not necessarily of a finite degree). Let $G=G(\bar{k}/k)$. We say k or G has the essential cohomological dimension $\operatorname{ess\,cd} k=\operatorname{ess\,cd} G=n<\infty$, if G has an open subgroup H such that $\operatorname{cd} H=n$. It is independent of H and $\operatorname{ess\,cd} k\leqq 2$ for every k [8]. Especially $\operatorname{ess\,cd} k=2$ if k is finite over the rationals. Let k be an algebraic number field and let K be an algebraic extension of k. Then K is called totally real over k if every extension in K of every real prime of k is also real. Then the maximal totally real extension Ω of k is a Galois extension. Let $\tilde{G}$ be the Galois group of this extension.

LEMMA 10. *It holds* $\operatorname{cd}\tilde{G}\leqq\operatorname{ess\,cd} G$ *for any algebraic number field. More precisely,* $\operatorname{cd}_p\tilde{G}\leqq\operatorname{cd}_p G$ *for any odd prime number* p, *and* $\operatorname{cd}_2\tilde{G}\leqq\operatorname{ess\,cd}_2 G$.

Proof. Let p be an odd prime number. Let K be a finite totally real extension of k. Let H and $\tilde{H}$ be corresponding open subgroups of G and $\tilde{G}$, respectively. As $\operatorname{cd}_p\Omega\leqq 1$ and as Ω has no p-extension, we get [8]

$$H^q(\tilde{H}, Z/pZ)\cong H^q(H, Z/pZ), \qquad q=1, 2, \cdots$$

This shows $\operatorname{cd}_p\tilde{G}\leqq\operatorname{cd}_p G$. We now consider the case $p=2$. We first assume that k is of a finite degree. Then $\Omega^{\times 2}$ consists of the totally positive elements, i.e., the elements of $\Omega^\times$ which are positive in any extension of any real prime of k. Let K denote a finite Galois extension of k in Ω, and let $K^\times{}_+$ denote the totally positive elements in $K^\times$. Then

$$\Omega^\times/\Omega^{\times 2}=\varinjlim K^\times/K^\times{}_+ .$$

As K has elements of any signature type, $K^\times/K^\times{}_+$ is isomorphic to the direct sum of r_1 copies of $(Z/2Z)H$, where r_1 is the number of real primes of k and H is the Galois group of K over k. This shows

$$H^q(H, K^\times/K^\times{}_+)=0, \qquad q=1, 2, \cdots$$

and

$$H^q(\tilde{G}, \Omega^\times/\Omega^{\times 2})=0, \qquad q=1, 2, \cdots$$

Then it comes

$$H^q(\tilde{G}, \Omega^{\times 2})=H^q(\tilde{G}, \Omega^\times), \qquad q=2, 3, \cdots$$

This holds also for $q=1$, because $(K^\times/K^\times{}_+)^H=k^\times/k^\times{}_+$, i.e., $(\Omega^\times/\Omega^{\times 2})^{\tilde{G}}=k^\times/k^\times{}_+$. By an exact sequence

$$1\to\mu_2\to\Omega^\times\xrightarrow{2}\Omega^{\times 2}\to 1$$

and by the above equality, the sequence

$$(*)\qquad H^q(\tilde{G}, \Omega^\times)\xrightarrow{2}H^q(\tilde{G}, \Omega^\times)\to H^{q+1}(\tilde{G}, \mu_2)\to H^{q+1}(\tilde{G}, \Omega^\times)$$

$$\xrightarrow{2}H^{q+1}(\tilde{G}, \Omega^\times)$$

is exact for $q=1, 2, \cdots$ The exact sequence

$$1\to\Omega^{\times}\to J_{\Omega}\to C_{\Omega}\to 1$$

induces an exact sequence

$$0\to H^{2}(\tilde{G}, \Omega^{\times})\to H^{2}(\tilde{G}, J_{\Omega})\xrightarrow{\phi} H^{2}(\tilde{G}, C_{\Omega})\to H^{3}(\tilde{G}, \Omega^{\times})$$
$$\to H^{3}(\tilde{G}, J_{\Omega}).$$

As no real prime of k ramifies in Ω, it holds

$$H^{q}(\tilde{G}, J_{\Omega})\cong\sum H^{q}(\tilde{G}_{\mathfrak{P}}, \Omega_{\mathfrak{P}}^{\times}), \qquad q=1, 2, \cdots$$

where the direct sum is taken over all the finite primes of k. As $\Omega_{\mathfrak{P}}$ is algebraically closed for any $\mathfrak{P}$, $\operatorname{cd}\tilde{G}_{\mathfrak{P}}=2$. This shows $H^{3}(\tilde{G}, J_{\Omega})=0$ and $H^{2}(\tilde{G}, J_{\Omega})$ is divisible as local degrees are divisible by p^{∞} for any prime p. Then we see ϕ is surjective, and $H^{3}(\tilde{G}, \Omega^{\times})=0$. We also see the kernel $H^{2}(\tilde{G}, \Omega^{\times})$ of ϕ is divisible. Hence the exact sequence (*) shows $\operatorname{cd}_{2}\tilde{G}\leqq 2$ because (*) and the above argument hold for any finite extension of k in Ω. When k is of infinite degree, $\tilde{G}$ is a projective limit of $G_{n}=G(\Omega_{n}/k_{n})$ where k_{n} are subfields of k of finite degrees and Ω_{n} are maximal totally real extensions of k_{n}. Thus $\operatorname{cd}_{2}\tilde{G}\leqq 2$ also in this case. Then our assertion is true if $\operatorname{ess\,cd}_{2}G=2$. If $\operatorname{ess\,cd}_{2}G=0$, a Sylow 2-subgroup of G is finite. Then a Sylow 2-subgroup of $\tilde{G}$ must be trivial as $\tilde{G}$ has no finite 2-subgroup because $\operatorname{cd}_{2}\tilde{G}\leqq 2$. We now prove the case $\operatorname{ess\,cd}_{2}G=1$. Then every local subgroup $G_{\mathfrak{P}}=\tilde{G}_{\mathfrak{P}}$ has the cohomological 2-dimension at most 1. Then the above shows $H^{2}(\tilde{G}, J_{\Omega})=0$ and $H^{2}(\tilde{G}, \Omega^{\times})=0$. Then $\operatorname{cd}_{2}\tilde{G}\leqq 1$ as above.

Remark. When k is of a finite degree, the above shows $\operatorname{cd}_{p}\tilde{G}=2$ for every prime p.

THEOREM 4. *Let k be a separably Hilbertian algebraic number field with* $\operatorname{ess\,cd} k\leqq 1$. *Let Ω be the maximal totally real extension of k. Let Λ be the maximal solvable extension of k in Ω. Then the Galois group of Λ over k is a free pro-solvable group with countable generators.*

Proof. Let $\tilde{G}=G(\Omega/k)$ and $\bar{G}=G(\Lambda/k)$ be their Galois groups. Lemma 10 shows $\operatorname{cd}\tilde{G}\leqq 1$. First we show that Ω/k satisfies the conditions of Lemma 8. Let K be a totally real finite Galois extension of k with Galois group H. Let

$$1\to A\to E\xrightarrow{\pi} H\to 1$$

be any split group extension with a finite abelian kernel A. We can find an H-module B such that $A\cong B/C$ as an H-module and every element of order 2 in B is contained in C. Let

$$1\to B\to E_{1}\to H\to 1$$

be a split group extension. Lemma 9 shows there exists a field L_1 corresponding to this extension. As E is a homomorphic image of E_1, we can find a subfield L corresponding to E. As K is totally real over k and as C contains the elements of order 2 in B, L must be totally real over k. This argument also shows that $\tilde{G}$ is not trivial, i.e., $\mathrm{cd}\,\tilde{G}=1$. Hence we can apply Lemma 8 to our case. As $\bar{G}$ has countable open subgroups, we can find a basis of neighborhoods of the identity such that

$$\bar{G}=N_0\supset N_1\supset N_2\supset\cdots\supset N_i\supset\cdots,\qquad i=0,\,1,\,2,\,\cdots$$

consisting of open normal subgroups of $\bar{G}$. Let F be a free pro-solvable group with countable generators. Let

$$F=F_0\supset F_1\supset F_2\supset\cdots$$

be a basis of neighborhoods of the identity consisting of open normal subgroups of F. We will prove by the induction that there exist open normal subgroups U_i and V_i of $\bar{G}$ and F respectively such that $U_i\subset N_i\cap U_{i-1}$, $V_i\subset F_i\cap V_{i-1}$ and there exists an isomorphism $f_i\colon \bar{G}/U_i\cong F/V_i$ compatible with f_{i-1}. The case $i=0$ is trivial. We assume that we get U_i, V_i and f_i. Then there exists a natural homomorphism

$$\bar{G}/N_{i+1}\cap U_i\to F/V_i\to 1\,.$$

As F is free with countable generators, there exists a surjective homomorphism $F\to\bar{G}/N_{i+1}\cap U_i$ such that

$$\begin{array}{ccccc} & & F & & \\ & \swarrow & \downarrow & & \\ \bar{G}/N_{i+1}\cap U_i & \longrightarrow & F/V_i & \longrightarrow & 1 \end{array}$$

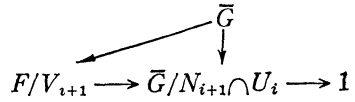
is commutative. Let V_{i+1} be the intersection of F_{i+1} and the kernel of the above homomorphism. Then there exists a surjective homomorphism

$$F/V_{i+1}\to\bar{G}/N_{i+1}\cap U_i\to 1\,.$$

Let K be the Galois extension of k corresponding to $N_{i+1}\cap U_i$. As the kernel of the above homomorphism is solvable, Lemma 8 shows that there exists a field L corresponding to this group extension, i.e., there exists a continuous surjective homomorphism $\tilde{G}\to F/V_{i+1}$ such that

$$\begin{array}{ccccc} & & \tilde{G} & & \\ & \swarrow & \downarrow & & \\ F/V_{i+1} & \longrightarrow & \bar{G}/N_{i+1}\cap U_i & \longrightarrow & 1 \end{array}$$

is commutative. As F/V_{i+1} is solvable, it induces a surjective homomorphism $\bar{G}\to F/V_{i+1}$ such that



is commutative. Let U_{i+1} be the kernel of this homomorphism. Then there exists an isomorphism f_{i+1}: $\bar{G}/U_{i+1}\cong F/V_{i+1}$ compatible with f_i, $U_{i+1}\subset N_{i+1}\cap U_i$ and $V_{i+1}\subset F_{i+1}\cap V_i$. As $U_0\supset U_1\supset U_2\supset\cdots$ and $V_0\supset V_1\supset V_2\supset\cdots$ are bases of neighborhoods of $\bar{G}$ and F respectively, there exists an isomorphism $\bar{G}\cong F$.

EXAMPLES. Let k be the $\hat{Z}$-extension of the rationals. Then it is known that ess cd $k\leqq 1$. As k is separably Hilbertian by Theorem 3, the Galois group of the totally real maximal solvable extension of k is free pro-solvable. Now let k be the maximal abelian extension of an algebraic number field of a finite degree. Then cd $k=1$ and Theorem 4 holds for k. This is a theorem of Iwasawa [4].

Remark. Though we stated our theorem in the case of algebraic number fields, the same is true for every countable separably Hilbertian field with cd $k=1$. For example, let $\bar{F}$ be the algebraic closure of a finite field F of characteristic p. Let t be an indeterminate. Then we can apply our theorem for $\bar{F}(t)$, and its maximal solvable extension has a free pro-solvable Galois group with countable generators as was shown in [4]. Let H be a finite group whose order is not a multiple of p. Then it has been shown that $\bar{F}(t)$ has a Galois extension with Galois group H [2]. These and the remark at the introduction suggest that the Galois group of the separable closure of $\bar{F}(t)$ over $\bar{F}(t)$ be free.

REFERENCES

[1] W. FRANZ, Untersuchungen zum Hilbertschen Irreduzibilitätssatz, Math. Z., 33 (1931).
[2] A. GROTHENDIECK, Géométrie formelle et géométrie algébrique, Sem. Bourbaki, 1959.
[3] E. INABA, Über den Hilbertschen Irreduzibilitätssatz, Japanese J., 19 (1944).
[4] K. IWASAWA, On solvable extensions of algebraic number fields, Ann. Math., 58 (1953).
[5] W. KUYK, Extensions de corps hilbertiens, J. Alg., 14 (1970).
[6] S. LANG, Diophantine geometry, Chap. VIII, Interscience.
[7] S. LANG, Algebraic groups over finite fields, Am. J., 78 (1956).
[8] J.P. SERRE, Cohomologie Galoisienne, Lec. Notes in Math., 5 (1964).

MATHEMATICAL INSTITUTE
TÔHOKU UNIVERSITY
SENDAI, JAPAN.