28. A Note on the Hilbert Irreducibility Theorem

The Irreducibility Theorem and the Strong Approximation Theorem*),**)

By Yasuo MORITA
Mathematical Institute, Tohoku University

(Communicated by Shokichi IYANAGA, M. J. A., April 12, 1990)

Introduction. Let k be a finite algebraic number field. For any irreducible polynomial $f(t, x) \in k(t)[x]$, let $U_{f,k}$ denote the set consisting of all $s \in k$ such that $f(s, x)$ is defined and irreducible in $k[x]$. A subset of k of this form is called a *basic Hilbert subset* of k. Further, an intersection of a non-empty Zariski open subset of k and a finite number of basic Hilbert subsets of k is called a *Hilbert subset* of k.

In this paper, we obtain the following theorem:

Main theorem. *Let Ω be the set of all primes of a finite algebraic number field k, let $\mathfrak{q}$ be an element of Ω, and let S be a finite subset of $\Omega-\{\mathfrak{q}\}$ such that $\Omega-S-\{\mathfrak{q}\}$ contains only non-archimedean primes of k. We choose an element $\alpha_{\mathfrak{p}}$ of k for each $\mathfrak{p} \in S$. Then, for any positive number ε and for any Hilbert subset H of k, there exists an element $\alpha \in H$ such that*

$$\begin{cases} |\alpha-\alpha_{\mathfrak{p}}|_{\mathfrak{p}} < \varepsilon & \text{for any } \mathfrak{p} \in S, \\ |\alpha|_{\mathfrak{p}} \leq 1 & \text{for any } \mathfrak{p} \in \Omega-S-\{\mathfrak{q}\}. \end{cases}$$

Clearly, this theorem shows that the Hilbert irreducibility theorem and the strong approximation theorem for k are compatible. It is easy to reduce this theorem to the Hilbert irreducibility theorem if S contains only non-archimedean primes, but it seems nontrivial if S contains archimedean primes.

We prove the theorem by modifying an argument in S. Lang [1], VIII, § 1.

The author would like to thank Professor Peter Roquette for valuable comments.

§ 1. Hilbert sets and rational points of algebraic curves. Let k be a finite algebraic number field, and let H be a Hilbert subset of k. Then, for some non-empty Zariski open subset O of k, we can write $O \cap H = O \cap (\bigcap_{i=1}^{m} U_{f_i,k})$, where $f_i(t, x)$ is an irreducible polynomial in $k(t)[x]$ and $U_{f_i,k}$ is the basic Hilbert subset corresponding to f_i. Here, by multiplying an element of $k[t]$ and changing O if necessary, we may assume $f_i(t, x) \in k[t, x]$.

Let $f(t, x)$ be one of the $f_i(t, x)$. Let $\overline{k(t)}$ be the algebraic closure of $k(t)$, and write $f(t, x) = a(t) \prod_{h=1}^{l} (x-\alpha_h)$ $(a(t) \in k[t], \alpha_h \in \overline{k(t)})$. Let $f(t, x) =$

*) Dedicated to Professor Ichiro SATAKE on his sixtieth birthday.

**) This result was obtained when the author was a member of the Sonderforschungsbereich 170, Geometrie und Analysis in Göttingen.

$g(x)h(x)$ be a factorization of $f(t, x)$ in $\overline{k(t)}[x]$. Since $f(t, x)$ is irreducible in $k(t)[x]$, $g(x)$ does not belong to $k(t)[x]$. Hence, at least one coefficient y of $g(x) \in \overline{k(t)}[t]$ does no belong to $k(t)$. Let C denote the affine algebraic curve $\mathrm{Spec}\, k[t, y]$. Then the function field $k(C)=k(t, y)$ of C is a nontrivial extension of $k(t)$.

Let s be an element of the Zariski open subset O, and let $\mathfrak{p}(s)$ be the specialization $t \to s$. We extend $\mathfrak{p}(s)$ to a $\bar{k}$-valued place of $\overline{k(t)}$, and denote it by the same symbol. Let $f(t, x)=g(x)h(x)$ in $\overline{k(t)}[x]$, and let $b(t)$ and $c(t)$ be the leading coefficients of $g(x)$ and $h(x)$, respectively. Then $g(x)$ and $h(x)$ are $\mathfrak{p}(s)$-finite if $b(t)$, $c(t)$ and the α_h are $\mathfrak{p}(s)$-finite. Since this assumption excludes only a finite number of elements of O, by changing O if necessary, we may assume that $g(x)$ and $h(x)$ are $\mathfrak{p}(s)$-finite. Then we have a factorization $f(s, x)=p(x)q(x)$ in $\bar{k}[x]$. Put $\eta=y \bmod \mathfrak{p}(s)$. If $f(s, x)=p(x)q(x)$ holds in $k[x]$, then $\eta \in k$. Hence (s, η) is a k-rational point of C.

For any algebraic curve C defined over k, let $C(k)$ denote the set of all k-rational points on C. For any k-rational function t on C, and for any subring R of k, put

$$U_{t,R}(C)=\{s \in R;\ \text{no } P \in C(k) \text{ satisfies } t(P)=s\}.$$

Then we have the following theorem (cf. [1], VIII, § 1):

Theorem 1. *Let t be a variable over k, and let H be a Hilbert subset of k. Then there exist a non-empty Zariski open subset O of k and a finite number of elements $y^{(i)} \in \overline{k(t)}$ $(i=1, 2, \cdots, M)$ such that $y^{(i)} \notin k(t)$ and $O \cap H = O \cap (\bigcap_{i=1}^{M} U_{t,k}(\mathrm{Spec}\, k[t, y^{(i)}]))$.*

§ 2. Proof of the main theorem. Let k, Ω, $\mathfrak{q}$, S, $\alpha_{\mathfrak{p}}$ $(\mathfrak{p} \in S)$, ε, H be as in the main theorem. Then

$$R=\{\alpha \in k;\ |\alpha|_{\mathfrak{p}} \leq 1 \text{ for any } \mathfrak{p} \in \Omega - S - \{\mathfrak{q}\}\}$$

is a subring of k. Let t be a variable over k, let y be one of the $y^{(i)}$ in Theorem 1, let $C=C^{(i)}=\mathrm{Spec}\, k[t, y^{(i)}]$, and define $U_{t,k}(C)$ and $U_{t,R}(C)$ as in § 1.

If C is not absolutely irreducible, then there is an absolutely irreducible algebraic curve C_1 defined over an extension k_1 of k such that, for some conjugate C_1^{σ} of C_1 $(C_1^{\sigma} \neq C_1)$, $C(k)$ is contained in $C_1(k_1) \cap C_1^{\sigma}(k_1^{\sigma})$. Since $C_1(\bar{k}_1) \cap C_1^{\sigma}(\bar{k}_1)$ is a finite set, $C(k)$ is a finite set. Hence the complements of $U_{t,k}(C)$ and $U_{t,R}(C)$ are finite sets. Therefore, to study R-valued points of H and to prove the main theorem, (by replacing O if necessary,) we may assume that C is absolutely irreducible.

If the genus $g(C)$ of $k(C)$ is not 0, then by Siegel's theorem (cf. [1], p. 127, Theorem 3), the complement of $U_{t,R}(C)$ is a finite set. Hence we may assume $g(C)=0$.

If C has no k-rational points, then $U_{t,k}(C)=k$. Since such curves make no trouble, we may assume that $k(C)$ is a rational function field.

Now we use *Néron's trick* (cf. [1], p. 144).

Let t, y, C be as above, and let β be an element of k. Let U be a variable over $k(C)=k(t, y)$, let l be an integer ≥ 3, and put $F(U)=U^l+\beta$, $C'=$

Spec $k[t, y, U]/(F(U)-t)$, $u=U \bmod (F(U)-t)$. Let $C^{\sharp}$ and $C'^{\sharp}$ be the complete nonsingular models of C and C'. Then there is a covering map

$$\pi: C' \ni P'=(t, y, u) \longmapsto (t, y)=P \in C,$$

and $P' \in C'(k)$ if and only if $P \in C(k)$ and $u(P') \in k$. Hence

$$F(k) \cap U_{t,R}(C)=F(k) \cap U_{t,R}(C').$$

Hereafter we study this set.

Now we assume that there exist at least three $\bar{k}$-rational points P on $C^{\sharp}$ such that $t(P)=\beta$ or ∞. Let $P_1, \cdots, P_r$ be all such points. We choose an integer $l \geq 3$ such that, for any $C=C^{(t)}$ which satisfies our assumption, l is prime to the degree $[k(C): k(t)]$ and the ramification indices of these points. We claim that the genus $g(C')$ of $k(C')$ is greater than 1, and hence, by Siegel's theorem, the complement of $U_{t,R}(C')$ is a finite set.

In fact, since $u^l=t-\beta$, the prime divisors of $\bar{k}(t)$ corresponding to the points $t=\beta$ and $t=\infty$ ramify fully in $\bar{k}(t)(u)/\bar{k}(t)$. Hence the ramification index of any prime divisor of $\bar{k}(t)(u)$ which is over $t=\beta$ or $t=\infty$ is exactly l. On the other hand, the ramification indices of $P_1, \cdots, P_r$ in $\bar{k}(C)/\bar{k}(t)$ are prime to l. Since $\bar{k}(C')=\bar{k}(C)(u)$, the equality $[\bar{k}(C'): \bar{k}(C)]=l$ holds, and the ramification index of any point of $C'^{\sharp}$ which is over one of the $P_1, \cdots, P_r$ is exactly l. It follows that $C'^{\sharp}$ is absolutely irreducible. Therefore, by the Hurwitz formula, the genus $g(C')$ of $k(C')$ satisfies $g(C') \geq (l+1)/2 \geq 2$.

Since we have proved the claim, we may assume that the number of the points P on $C^{\sharp}$ such that $t(P)=\beta$ or ∞ is at most 2. Since $t-\beta \notin \bar{k}$, it has a pole. Since the degree of the divisor $(t-\beta)$ is zero, there exists exactly one $\bar{k}$-rational point P_∞ (resp. P_β) on $C^{\sharp}$ such that $t(P_\infty)=\infty$ (resp. $t(P_\beta)=\beta$). In particular, P_∞ and P_β are k-rational.

Let z be an element of $k(C)$ such that $k(z)=k(C)$, and such that z has a simple pole at P_∞ and a simple zero at P_β. Then $(t-\beta)z^{-r}$ has no pole on $C^{\sharp}$ for some integer r. It follows $d=(t-\beta)z^{-r} \in k$, $\neq 0$. Hence $t=\beta+dz^r$. Hence, if $P \in C(k)$ satisfies $t(P)=s$, then we can write $s=\beta+dw^r$ with some $w \in k$. Since $[k(C): k(t)]=r$, r is prime to l. Further, since $k(C) \neq k(t)$, $r \geq 2$.

Therefore we have proved the following theorem:

Theorem 2. *Let k, H, and R be as before. Let β be any element of k. Then the Hilbert set H contains, up to a finite number of points, a set of the form*

$$\bigcap_{i=1}^{I} \{s \in R;\ s=\beta+v^l\ (\exists v \in R),\ s \neq \beta+d_i w_i^{r_i} \text{ for any } w_i \in k\},$$

where I, l, $r_i \in N$, $r_i \geq 2$, $(r_i, l)=1$, and $0 \neq d_i \in k$.

By using Theorem 2, we obtain the main theorem.

Let the notation and assumption be as in the main theorem, and let R be as in the beginning of this section. We use the strong approximation theorem for k, and take an element β of R such that $|\beta-\alpha_\mathfrak{p}|_\mathfrak{p} < \varepsilon/2$ holds for all $\mathfrak{p} \in S$. Let I, l, d_i, r_i be as in Theorem 2. Let $\mathfrak{l}$ be an element of $\Omega - S - \{\mathfrak{q}\}$ such that $\mathfrak{l}$ is prime to d_i for all i. Then, if the order $\mathrm{ord}_\mathfrak{l}(s)$ of $s \in k$

at $\mathfrak{l}$ is prime to r_i, s is not contained in $d_i k^{r_i} = \{d_i w_i^{r_i};\ w_i \in k\}$. Since $r_i \geq 2$, it follows from the strong approximation theorem that there exists an element $s_0 \in R$ such that $(\mathrm{ord}_{\mathfrak{l}}(s_0), r_i) = 1$ for all $i \in I$, and $|s_0|_{\mathfrak{p}} < \varepsilon/2$ for all $\mathfrak{p} \in S$. Since $(l, r_i) = 1$ for all i, the l-th power $s = (s_0)^l$ of s_0 belongs to $\bigcap_{i=1}^{I} \{s \in R^l;\ s \notin d_i k^{r_i}\}$. It follows from Theorem 2 that, for a sufficiently small ε, $\alpha = \beta + s \in R$ is an element of H. Since s and β satisfy $|s|_{\mathfrak{p}} < \varepsilon/2$ and $|\beta|_{\mathfrak{p}} < \varepsilon/2$ for any $\mathfrak{p} \in S$, $\alpha \in R$ satisfies $|\alpha|_{\mathfrak{p}} < \varepsilon$ for any $\mathfrak{p} \in S$. This completes the proof of the main theorem.

Reference

[1] S. Lang: Diophantine Geometry. Interscience (1962).