数理解析研究所講究録
第 658 巻 1988 年 8-16

A Note on the Hilbert Irreducibility Theorem, the Irreducibility Theorem and the Strong Approximation Theorem

By Yasuo Morita

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 elements $t^0 \in k$ such that $f(t^0,x)$ 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 finite number of basic Hilbert subsets of k with a non-empty Zariski open subset of k is called a *Hilbert subset* of k.

In this paper, we shall prove the following theorem:

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

$$|\alpha-\alpha_p|_p < \varepsilon \qquad \text{for any } p \in S, \text{ and}$$
$$|\alpha|_p \leq 1 \qquad \text{for any } p \in \Omega-S-\{q\} .$$

Clearly, this theorem shows that the Hilbert irreducibility theorem and the strong approximation theorem for k is compatible. It is easy to reduce this theorem to the well-known Hilbert irreducibility theorem if S contains only non-archimedean primes (in particular, in the function field case), but it seems non-trivial if S contains archimedean primes. It should be also noted that this theorem does not follow from the usual Hilbert irreducibility theorem with the density condition (cf. *e.g.* Inaba [1]), because

$$\lim_{t\to\infty} \frac{\{ \alpha \in \mathcal{O}_k \; ; \; |\alpha|_{1,\infty} \le t \; , \; |\alpha-\alpha_{i,\infty}|_{i,\infty} \le \varepsilon \; (i\ne 1)\}}{\{ \alpha \in \mathcal{O}_k \; ; \; |\alpha|_{i,\infty} \le t \; (i\ge 1) \}} = 0$$

for a fixed $\varepsilon > 0$ if $[k:\mathbb{Q}] > 1$, where $\mathcal{O}_k$ denotes the ring of integers of k , and the $|\;|_{i,\infty}$ denote the archimedean primes of k . We shall prove the main theorem by modifying an argument in S. Lang [2], VIII, §1.

§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 . We assume that there exists a Zariski open subset O of k such that $O \cap H$ is an intersection $O \cap (\bigcap_{i=1}^{m} U_{f_i,k})$ of a Zariski open subset O of k and sets of the form $U_{f_i,k}$, where $f_i(t,x)$ are irreducible polynomials in $k(t)[x]$. Here, by changing the above Zariski open subset O if necessary, we may assume that the polynomials $f_i(t,x)$ belong to $k[t][x]$, and they are irreducible in $k[t,x]$.

Let $f(t,x)$ be one of the $f_i(t,x)$ $(i=1,2,\ldots,m)$. Let

$\overline{k(t)}$ be the algebraic closure of $k(t)$, and write

$$f(t,x) = a(t) \prod_{h=1}^{l} (x-\alpha_h) \quad (a(t) \in k[t] , \quad \alpha_h \in \overline{k(t)}) .$$

Let $f(t,x) = g(x)h(x)$ be a factorization of $f(t,x) \in k(t)[x]$ in $\overline{k(t)}[x]$. Since $f(t,x)$ is irreducible in $k(t)[x]$, $g(x)$ does not belong to $k(t)[x]$ for any such factorization. In other words, for any such factorization $f(t,x) = g(x)h(x)$ in $\overline{k(t)}[x]$, there exists at least one coefficient y of $g(x)$ such that $y \in \overline{k(t)}$ but $y \notin k(t)$. Let $C = C(f,g,h,y)$ denote the plane algebraic curve Spec $k[t,y]$. Then the function field $k(C) = k(t,y)$ of C is a non-trivial extension of $k(t)$.

Let t^0 be an element of the above Zariski open subset O, and let $\mathfrak{P}(t^0)$ be the specialization $t \longrightarrow t^0$. We extend this specialization to a $\bar{k}$-valued place of $\overline{k(t)}$, and denote it by the same symbol $\mathfrak{P}(t^0)$. Let $f(t,x) = g(x)h(x)$ in $\overline{k(t)}[x]$, let $p = \deg g(x)$, $q = \deg h(x)$, and let $b(t)$ and $c(t)$ be the coefficient of x^p of $g(x)$ and the coefficient of x^q of $h(x)$, respectively. Then $g(x)$ and $h(x)$ are $\mathfrak{P}(t^0)$-finite if $b(t)$, $c(t)$ and the α_h are $\mathfrak{P}(t^0)$-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 $\mathfrak{P}(t^0)$-finite. Then this factorization induces another factorization $f(t^0,x) = g^0(x)h^0(x)$ in $\bar{k}[x]$.

Put $y^0 = y \pmod{\mathfrak{P}(t^0)}$. If this factorization $f(t^0,x) =$

$g^0(x)h^0(x)$ holds in $k[x]$, y^0 is an element of k . Hence the pair (t^0,y^0) gives 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 of k . For any non-trivial k -rational function on C , and for any subring R of k , we put

$$U_{t,R}(C) = \{ t^0 \in R \text{ ; no } P \in C(k) \text{ satisfies } t(P) = t^0 \}.$$

Then we have proved the following theorem (cf. S. Lang [2], VIII, §1):

Theorem 1. Let H be a Hilbert subset of k , and let t be a transcendental element over k . Then there exist a Zariski open subset O , a finite number of elements $y(i)$ $(i=1,2,...,M)$ of $\overline{k(t)}$ such that $y(i) \notin k(t)$, and the plane algebraic curves $C(i) = \mathrm{Spec}\, k[t,y(i)]$ $(i=1,2,...,M)$ satisfy

$$O \cap H = O \cap (\bigcap_{i=1}^{M} U_{t,k}(C(i))) .$$

§2. Proof of the main theorem

Let k be a finite algebraic number field, let $\Omega = \Omega_k$ be the set of all primes of k , and let $\mathfrak{q}$ be an element of Ω . Let S be a finite subset of $\Omega - \{\mathfrak{q}\}$ such that $\Omega - S - \{\mathfrak{q}\}$ contains only non-archimedean primes of k , and let

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

Then R is a normal ring which is finitely generated over $\mathbb{Z}$. Let ε be a positive number, and let $\alpha_{\mathfrak{p}}$ $(\mathfrak{p} \in S)$ be elements of k . Hence the notation and assumption are as in the main theorem. We use the strong approximation theorem for k , and take an element β of R such that

$$|\beta-\alpha_p| < \varepsilon/2 \qquad \text{for any } p \in S .$$

Let t be a transcendental element over k , and let y be an element of $\overline{k(t)}$ such that $y \notin k(t)$, let C = Spec $k[t,y]$, and let $U_{t,k}(C)$ and $U_{t,R}(C)$ be as in §1. We assume that this plane algebraic curve C is one of the $C(i)$ (i=1,2, ...,M) of Theorem 1.

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

If the genus $g(C)$ of C is not smaller than 1 , then it follows from the Siegel theorem that the set $U_{t,R}(C)$ is a finite set (cf.*e.g.* Lang [2], p.127, Theorem 3). Therefore, to study the Hilbert set H of the main theorem, we replace the Zariski open subset O if necessary, and disregard such curves. Note that, by the Mordell conjecture proved by Faltings, the complement of $U_{t,k}(C)$ is a finite set if $g(C) > 1$.

If C has no k -rational points, then $U_{t,k}(C) = k$. Hence such curves make no trouble to study H . Hence we assume that the genus of C is 0 , and that C has at least one k -rational points. Then $k(C)$ ia a rational function field.

Now we use Néron's trick and study a certain subset of $U_{t,R}(C)$ more closely (cf. Lang [2], p.144).

Let t , y , C , β *etc.* be as above. Let u be a transcendental element over $k(C) = k(t,y)$, let l be an integer ≥ 3 , and put $f(u) = u^l + \beta$, $C' = \mathrm{Spec}\ k[t,y,u]/(f(u)-t)$, $\tilde{u} = u \pmod{f(u)-t} \in k[t,y,u]/(f(u)-t)$. Let $\overline{C}$ and $\overline{C'}$ be the complete non-singular models of C and C' , respectively. Then there is a natural covering map

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

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

$$\begin{aligned} U_{t,R}(C) &= \{ t^0 \in R \ ; \text{ no } P \in C(k) \text{ satisfies } t(P) = t^0 \} \\ &\supset f(k) \cap U_{t,R}(C) \\ &= \{ t^0 \in R \ ; \ t^0 = f(u^0) \text{ with a certain } u^0 \in k \\ &\qquad \text{and no } P \in C(k) \text{ satisfies } t(P) = t^0 \} \\ &= f(k) \cap \{ t^0 \in R \ ; \text{ no } P' \in C'(k) \text{ satisfies } t(P') = t^0 \} \\ &= f(k) \cap U_{t,R}(C') . \end{aligned}$$

Now we assume that there exist at least three $\overline{k}$ -rational points P of $\overline{C}$ such that $t(P) = \beta$ or ∞ . Let P_1 , P_2 , ... be all such points of $\overline{C}$. We assume that l is prime to the degree $[k(C):k(t)]$, and that l is prime to the ramification indeces of these points. It is obvious that this condition can be satisfied with a suitable l for all $C = C(i)$ $(i=1,2,\ldots,M)$ which satisfy our assumption. We claim that the genus $g(C')$ of $k(C')$ is greater than 1 , and hence such curves cause only finitely many exceptions.

In fact, let $\overline{k}$ be the algebraic closure of k . Since $\tilde{u}^l = t - \beta$, the prime divisors of $\overline{k}(t)$ corresponding to the points $t = \beta$ and $t = \infty$ ramify fully in $\overline{k}(t)(\tilde{u})/\overline{k}(t)$. Hence the ramification index in $\overline{k}(t)(\tilde{u})/\overline{k}(t)$ of any prime divisor of $\overline{k}(t)(\tilde{u})$ which is over $t = \beta$ or $t = \infty$ is exactly l . On the other hand, the ramification indeces of P_1 , P_2, ... for $\overline{k}(C)/\overline{k}(t)$ are prime to l . Since $\overline{k}(C') = \overline{k}(C)(\tilde{u})$, the equality $[\overline{k}(C'):\overline{k}(C)] = l$ holds, and the ramification index for $\overline{k}(C')/\overline{k}(C)$ of any point of $\overline{C'}$ which is over one of the points P_1 , P_2 , ... is exactly l . It follows that $\overline{C'}$ is absolutely irreducible. Therefore, by the Hurwitz formula, the genus $g(C')$ of $\overline{C'}$ satisfies $g(C') \geq (l+1)/2 \geq 2$. Hence, by the Siegel theorem, the complement of $U_{f,R}(C)$ is a finite set.

Since we have proved the claim, we may assume that the number of points P on $\overline{C}$ such that $t(P) = \beta$ or ∞ is at most 2. Since $(t-\beta)$ is a principal divisor of the rational function field $k(C)$, the number of the poles of $t-\beta$ is equal to the number of zeros of $t-\beta$. Since t is not a constant, these numbers are both equal to 1 . Hence these two $\overline{k}$ -rational points are both k -rational.

Let z be an element of $k(C)$ such that z generates $k(C)$ over $k(t)$, and such that z has a simple pole at the point of $\bar{C}$ where $t-\beta$ has a pole. Then $(t-\beta)z^{-r}$ has no pole on $\bar{C}$ for a suitable positive integer r. It follows $d = (t-\beta)z^{-r}$ is a non-zero constant in k. Hence we can write $t = \beta + dz^{r}$ ($d \in k$, $z \in k(C)$, $r \in \mathbb{N}$). Since $[k(C):k(t)] = r$, it follows from our assumption on l that r is prime to l. Further, since $k(C) \neq k(t)$, we have $r \geq 2$. 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 an intersection of a Zariski open subset O of k and a set of the form

$$\bigcap_{i=1}^{I} \{ t \in R \; ; \; t = \beta+u^{l} \; (u \in R), \; t \neq \beta+d_i z_i^{r_i} \text{ for any } z_i \in k \} ,$$

where I, l, r_i are positive integers, $r_i \geq 2$, $(r_i, l) = 1$, and d_i are non-zero constants in k.

By using Theorem 2, we can complete the proof of the main theorem.

Let the notation and assumption be as in the main theorem, let R and β be as in the beginning of this section, and let I, l, d_i, r_i *etc.* be as in Theorem 2. Let $\mathfrak{p}_0$ be an element of $\Omega - S - \{\mathfrak{q}\}$ such that $\mathfrak{p}_0$ is prime to d_i for all i. Then it is obvious that, if the order $\mathrm{ord}_{\mathfrak{p}_0}(t)$ of $t \in k$ at

$\mathfrak{p}_0$ is not congruent to 0 (modulo r_i), then t is not contained in $d_i k^{r_i}$. Since all r_i are greater that 1, it follows from the strong approximation theorem for k that there exists an element t_1 of R such that $\mathrm{ord}_{\mathfrak{p}_0}(t_1)$ is prime to r_i for any i, and $|t_1|_{\mathfrak{p}} < \varepsilon/2$ for any $\mathfrak{p} \in S$. Since l is prime to r_i for any i, the l-th power $t = (t_1)^l$ of this element belongs to

$$\bigcap_{i=1}^{I} \{ t \in R^l ; t \notin d_i k^{r_i} \} .$$

It follows from Theorem 2 that $\alpha = \beta + t \in R$ is an element of H. Since t is an element of R satisfying $|t|_{\mathfrak{p}} < \varepsilon/2$ for any $\mathfrak{p} \in S$, and since β satisfies $|\beta|_{\mathfrak{p}} < \varepsilon/2$ 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.

References.

1. E. Inaba, Über den Hilbertschen Irreducibilitatssätz, Jap. J. Math. **19**(1944), 1-25.

2. S. Lang, Diophantine Geometry, Interscience, 1962.

Mathematical Institute
Tohoku University
Aoba, Sendai 980
Japan