数理解析研究所講究録
第 701 巻 1989 年 72-77

On algebraic extensions of the nonstandard rational number field

MASAHIRO YASUMOTO (NAGOYA UNIVERSITY)

Let $^*\mathbf{Q}$ and $^*\mathbf{Z}$ denote enlargements of the rational number field $\mathbf{Q}$ and the integer ring $\mathbf{Z}$ respectively where by an enlargement, we mean an elementary extension which satisfies ω_1-saturation property. Let H be the height function of $^*\mathbf{Q}$; i.e. $H(\alpha/\beta) = \max(|\alpha|, |\beta|)$ where α and β are mutually prime nonstandard integers. A subfield Q_1 of $^*\mathbf{Q}$ is called H-convex if $x \in Q_1$ and $H(x) > H(y)$ imply $y \in Q_1$. In the rest of this paper, Q_1 always denotes an H-convex subfield of $^*\mathbf{Q}$. Let x be a nonstandard integer not contained in Q_1. Then x is transcendental over Q_1([4, Lemma 1]) Let F be a finite algebraic extension of $Q_1(x)$. (F is not necessary included in $^*\mathbf{Q}$.) Since $^*\mathbf{Q}F$ is a finite algebraic extension of $^*\mathbf{Q}$, $^*\mathbf{Q}F$ is internal. Let $\mathcal{O}$ be the ring of all algebraic integers in $^*\mathbf{Q}F$. Let K_1 denote the algebraic closure of Q_1 in $^*\mathbf{Q}F$. Then F is an algebraic function field of one variable over K_1. By a functional prime of F, we mean an equivalence class of nontrivial valuations of F which are trivial on K_1. Let $|x|_1, \ldots, |x|_s$ be all internal archimedean absolute values of $^*\mathbf{Q}F$ which induce in $^*\mathbf{Q}$ the ordinary absolute value. Since $s \leq [\,^*\mathbf{Q}F : {}^*\mathbf{Q}\,]$, s is finite.

LEMMA 1. *Let $z \notin K_1$ and $z\mathcal{O} = J_1/J_2$ where J_1 and J_2 are coprime ideals of $\mathcal{O}$. If for all $i \leq s$, there is $\gamma \in Z_1$ such that $|z|_i < \gamma$, then $J_2 \cap Z_1 = \{0\}$.*

PROOF: Assume there exists a nonzero $t \in J_2 \cap Z_1$. Then $tz \in \mathcal{O}$. Since $|tz|_i < |t|\gamma$ for all $i \leq s$, tz is algebraic over Z_1, so $tz \in \mathcal{O} \cap K_1$, hence $z \in K_1$, a contradiction.

For each $i \leq s$, let $R_i = \{z \in {}^*\mathbf{Q}F \mid |z|_i < \gamma \ \text{ for some } \ \gamma \in Z_1\}$, then R_i is a valuation ring whose maximal ideal is $\{z \in {}^*\mathbf{Q}F \mid |z|_i < 1/|\gamma| \ \text{ for all } \ \gamma \in Z_1\}$. If $F \cap R_i$ is not trivial, namely $F \not\subset R_i$, then $F \cap R_i$ is a valuation ring. Since $F \cap R_i \supset K_1$, this valuation ring yields a functional prime P of F. We say that P is induced by an archimedean absolute value.

Let $R = \{z \in {}^*\mathbf{Q}F \mid \gamma z \ \text{ is an algebraic integer for some } \ \gamma \in Z_1\}$ and I a maximal ideal of R. Let R_I denote the local ring of R by I. If $F \cap R_I$ is not trivial, then $F \cap R_I$ is a valuation ring, hence it also yields a functional prime P of F. We say that P is induced by I.

THEOREM 1. (cf. [4, Lemma 2],[2, Lemma 4.1]) Every functional prime P of F is induced by an archimedean prime or a maximal ideal I of R.

PROOF: By the theorem of Riemann-Roch, there exists $z \in F$ which admits P as its only pole. If there is $i \leq s$ such that $|z|_i > \gamma$ for all $\gamma \in Z_1$, then $z \notin R_i$. Hence $z \notin F \cap R_i$. Then $F \cap R_i$ yields a functional prime which is a pole of z. Since P is the only functional pole of z, P is induced by an archimedean absolute value. Next assume for all $i \leq s$ there is $\gamma \in Z_1$ such that $|z|_i < \gamma$. Let $z\mathcal{O} = J_1/J_2$ where J_1 and J_2 are coprime ideals of $\mathcal{O}$. By Lemma 1, $J_2 \cap Z_1 = \{0\}$. Hence J_2R is a proper ideal. Let I be a maximal ideal of R which includes J_2R. Then the local ring of

I does not contain z, so $z \in R_I - F$. Hence $F \cap R_I$ is not trivial. By the same arguments as above P is induced by I.

Theorem 1 is very useful and it has many applications, so in the following we give one of them. For each irreducible polynomial $f(X,Y) \in R[X,Y]$, we denote by $J(f)$ the set of all $r \in R$ that $f(r,Y)$ is reducible in $R[Y]$.. In case of $R = \mathbf{Z}$, $\mathbf{Z} - J(f)$ (such a set of integers is called a Hilbert subset) is infinite (Hilbert's irreducibility theorem), moreover it is known([1]) that $J(f)$ is very thin. In section 1, we give a sufficient condition that $J(f)$ is finite and give its bound. Let F be a function field over $\mathbf{Q}$ of an algebraic curve Γ defined by the equation $f(X,Y) = 0$, in other words, $F = \mathbf{Q}(x,y)$ where x is transcendental over $\mathbf{Q}$ and $f(x,y) = 0$. By an functional prime divisor of F, we mean an equivalence class of nontrivial valuation of F which is trivial on $\mathbf{Q}$. For a functional prime divisor P, we denote by v_P the normalized valuation(i.e. its valuation group is $\mathbf{Z}$) belonging to P. A functional prime P is called a pole of $z \in \mathbf{Q}[X,Y]$ if $v_P(z) < 0$. For each $f(X,Y) \in \mathbf{Z}[X,Y]$, its height denoted by $H(f)$ is defined to be the maximum of absolute values of coefficients of $f(X,Y)$. We prove

THEOREM 2. *Let $f(X,Y)$ be an irreducible polynomial with integer coefficients and $F = \mathbf{Q}(x,y)$ its function field. Assume there are more than $\deg_Y(f)/2$ poles of x. Then there are only finitely many integers $n \in \mathbf{Z}$ such that $f(n,Y)$ is reducible. Moreover If $f(n,Y)$ is reducible, then*

$$|n| < (H(f)+1)^C$$

where C is a constant determined by the degree of $f(X,Y)$.

PROOF: Suppose Theorem 1 is false. Let $d \in \mathbf{N}$. For any natural number N, there exist an integer α and an irreducible polynomial $f(X,Y) \in \mathbf{Z}[X,Y]$ of degree d which satisfies the assumption of the theorem such that $f(\alpha, Y)$ is reducible and

$$|\alpha| > (H(f)+1)^N \tag{1}$$

By nonstandard principle, the above assertion holds for any enlargement. We take $N \in {}^*\mathbf{N} - \mathbf{N}$. Then $f(X,Y) \in {}^*(\mathbf{Z}[X,Y])$, but since the degree of $f(X,Y)$ is $d \in \mathbf{N}, f(X,Y) \in {}^*\mathbf{Z}[X,Y]$, i.e. $f(X,Y)$ is a polynomial with coefficients in ${}^*\mathbf{Z}$. Let Q_1 be the smallest H-convex subfield of ${}^*\mathbf{Q}$ which contains all coefficients of $f(X,Y)$ i.e.

$$Q_1 = \{z \in {}^*\mathbf{Q} \mid H(z) \leq (H(f)+1)^n \quad \text{for some} \quad n \in \mathbf{N}\}$$

By (1), $\alpha \notin Q_1$. Since Q_1 is algebraically closed in ${}^*\mathbf{Q}$, α is transcendental over Q_1. Let $f(\alpha,Y) = f_1(\alpha,Y)f_2(\alpha,Y)$ where $f_1(X,Y), f_2(X,Y) \in {}^*\mathbf{Z}[X,Y]$ and $1 \leq \deg_Y(f_1) \leq \deg_Y(f_2)$. Let $F = Q_1(\alpha,\beta)$ where β satisfies $f_1(\alpha,\beta) = 0$. Then

$$\begin{aligned} s &\leq [{}^*\mathbf{Q}F : {}^*\mathbf{Q}] \leq \deg_Y(f_1) \\ &\leq \frac{1}{2}\deg_Y(f) \end{aligned} \tag{2}$$

Since α is a nonstandard integer, by lemma 2 every functional pole of α in F is induced by an archimedean absolute value in ${}^*\mathbf{Q}F$, so the number of functional pole of α is not more than s, hence by (2) not more than

$\deg_Y(f)/2$. Let x be transcendental over ${}^*\mathbf{Q}$ and y satisfy $f(x, y) = 0$. Then the number of functional poles of x in ${}^*\mathbf{Q}(x, y)$ is, by the assumption of the theorem, larger than $\deg_Y(f)/2$. But there is an embedding

$$\pi : F = Q_1(\alpha, \beta) \longrightarrow {}^*\mathbf{Q}(x, y)$$

where $\pi(\alpha) = x$, $\pi(\beta) = y$ and for all $z \in Q_1$, $\pi(z) = z$. Since Q_1 is algebraically closed in ${}^*\mathbf{Q}$, the number of poles of α and x must be same, this is a contradiction and it completes the proof of theorem1.

In order to prove Theorem 2, we use the fact that ${}^*\mathbf{Q}$ has an unique internal archimedean absolute value, so Theorem 1 cannot be generalized for algebraic number fields of finite degree.

Let us give an example. Let

$$f(X, Y) = X^4 - Y^4 + g(X, Y)$$

be an irreducible polynomial where $\deg(f(X, Y)) \leq 3$. Let $F = \mathbf{Q}(x, y)$ be its function field. There are 3 poles of x corresponding to irreducible factors of $X^4 - Y^4$. Hence the assumption of Theorem 1 is satisfied. So there are only finitely many integers n such that $n^4 - Y^4 + g(n, Y)$ is reducible and there is a constant C such that $n < (H(g) + 1)^C$ for any integer n with $n^4 - Y^4 + g(n, Y)$ reducible.

Let us end this paper with an open problem.

OPEN PROBLEM. *Find a necessary and sufficient condition for an irreducible polynomial $f(X, Y) \in \mathbf{Z}[X, Y]$ that $f(n, Y)$ is reducible for only finitely many integers n and give their bound.*

REFERENCES

1. Cohen, S. D., *The distribution of galois groups and Hilbert's irreducibility theorem*, Proc. London Math. Soc. **(3) 43** (1981), 227-250.
2. Robinson A. and Roquette P., *On the finiteness theorem of Siegel and Mahler concerning diophantine equation*, J. Number Theory **7** (1975), 121-176.
3. Roquette, P., *Nonstandard aspects of Hilbert's irreducibility theorem*, L.N.M. **498** (1975), 231-275.
4. Yasumoto, M., *Nonstandard arithmetic of function fields over H-convex subfields of* $^*Q$, J. Reine Angew. Math. **342** (1983), 1-11.
5. Yasumoto, M., *Algebraic extensions in nonstandard models and Hilbert's irreducibility theorem*, J. Symbolic Logic **53** (1988), 470-480.