J. Math. Soc. Japan
Vol. 20, Nos. 1-2, 1968

A type of integral extetsions

To Professor Iyanaga for celebration of his 60th birthday

By Masayoshi NAGATA

(Received Aug. 23, 1967)

The purpose of the present paper is to prove the following

THEOREM. *Let $S \subsetneqq R$ be integral domains with fields of quotients $Q(S) \subsetneqq Q(R)$. Assume that for each element r of R, there is a natural number n (depending on r) such that r^n is in $Q(S)$. Then either* (1) *$Q(R)$ is purely inseparable over $Q(S)$ or* (2) *R and S are algebraic over a finite field.*

The proof is given as follows. Assume that $Q(R)$ is not purely inseparable over $Q(S)$. Then there is an element a of R which is not in $Q(S)$ and which is separable over $Q(S)$. We fix this element a. Let $a = a_1, a_2, \cdots, a_c$ be all of the conjugates of a over $Q(S)$ in an algebraically closed field K containing $Q(R)$. If S contains only a finite number of elements, then (2) holds good obviously. Therefore we assume that S contains infinitely many elements. For each element s of S, there is a natural number $n(s)$ such that $(a+s)^{n(s)} \in Q(S)$ and such that $(a+s)^m \notin Q(S)$ for every natural number m which is less than $n(s)$.

Case 1. Assume that there is an infinite subset S^* of S such that $\{n(s) \mid s \in S^*\}$ is bounded. In this case, there is a natural number N such that $n(s) = N$ for an infinite subset S^{**} of S^*. Take mutually distinct elements, $s_0, s_1, \cdots, s_N$ from S^{**} and consider the relations

$$a^N + \binom{N}{1} s_i a^{N-1} + \cdots + \binom{N}{\alpha} s_i^\alpha a^{N-\alpha} + \cdots + s_i^N = b_i \in Q(S) \qquad (i = 0, 1, \cdots, N).$$

Since the matrix

$$A = \begin{pmatrix} 1 & s_0 & \cdots & s_0^N \\ 1 & s_1 & \cdots & s_1^N \\ & \cdots\cdots\cdots\cdots & & \\ & \cdots\cdots\cdots\cdots & & \\ 1 & s_N & \cdots & s_N^N \end{pmatrix}$$

is non-singular, we see that the non-zero columns in

$$A'=\begin{pmatrix} 1 & \binom{N}{1}s_0 & \cdots & \binom{N}{\alpha}s_0^\alpha & \cdots & s_0^N \\ 1 & \binom{N}{1}s_1 & \cdots & \binom{N}{\alpha}s_1^\alpha & \cdots & s_1^N \\ \multicolumn{6}{c}{\cdots\cdots\cdots\cdots\cdots\cdots\cdots} \\ \multicolumn{6}{c}{\cdots\cdots\cdots\cdots\cdots\cdots\cdots} \\ 1 & \binom{N}{1}s_N & \cdots & \binom{N}{\alpha}s_N^\alpha & \cdots & s_N^N \end{pmatrix}$$

are linearly independent. Set $I=\{i\mid 0\leqq i\leqq N, \binom{N}{i}\neq 0\}$ and let M be the number of elements of I. Then the above fact shows that for a choice of M elements from these s_i, say $s_1, \cdots, s_M$, the determinant of the matrix of the coefficients of the following linear equation on $\{a^{N-\alpha}\mid \alpha\in I\}$ is not zero:

$$\sum_{\alpha\in I}\binom{N}{\alpha}s_i^\alpha a^{N-\alpha}=b_i \qquad (i\in I).$$

Therefore we see that $a^i\in Q(S)$ for every $i\in I$, and a is purely inseparable over $Q(S)$. This contradicts to our choice of a.

Case 2. Assume now that for every infinite subset S^* of S, $\{n(s)\mid s\in S^*\}$ is not bounded. Take an arbitrary infinite subset S^*. For each $s\in S^*$, $a+s$ is a root of a polynomial $f_s(X)$ of the form $X^{n(s)}-s^*$ ($s^*\in Q(S)$). Then $f_s(X)=\prod_{i=1}^{n(s)}(X-\zeta_{si}(a+s))$, where ζ_{si} ranges over all roots of $X^{n(s)}-1$ in the algebraically closed field K. a_i+s is a conjugate of $a+s$ over $Q(S)$, and therefore it is a root of $f_s(X)$. This shows that $a_i+s=\zeta_{sj(i)}(a+s)$ with a suitable $j(i)$ (depending not only on i but also on s). Then $Q(S)$ contains $\prod_i(a_i+s)$ which is equal to $(a+s)^c\prod_i\zeta_{sj(i)}$. If all of $\zeta_{sj(i)}$ are roots of $X^{m(s)}-1$, then we see that $(a+s)^{m(s)c}$ is in $Q(S)$. Therefore the set of $m(s)$ ($s\in S^*$) cannot be bounded. Since each $\zeta_{sj(i)}$ is equal to $(a_i+s)/(a+s)$, we see that the subfield T of $Q(R)$ generated by $a_1, \cdots, a_c$ and S^* contains infinitely many roots of unity. (i) Assume first that S is of characteristic zero. Then we can choose S^* to be the ring of rational integers. Then the above conclusion means that a finitely generated extension of the field of rational numbers contains infinitely many roots of unity. This is impossible. (ii) Assume now that S is of characteristic $p>0$ and that S contains a transcendental element t over the prime field P. Then we can choose S^* to be $\{t^m\mid m=1, 2, \cdots\}$. Then the conclusion given above means that a finitely generated extension of P contains infinitely many roots of unity. This is impossible, too. Thus the proof of our theorem is complete.

Department of Mathematics
Kyoto University