A NOTE ON AN EQUIVALENCE RELATION ON A PURELY INSEPARABLE FIELD EXTENSION

P. Rygg and B. Lehman*

(received June 28, 1968)

1. We assume F is a purely inseparable field extension of the field K. The characteristic of K is $p \neq 0$, and we assume F and K are not perfect. For $x \in F$, the exponent of x over K is the smallest non-negative integer e such that $x^{p^e} \in K$ and will be denoted by $e(x)$; $\underline{x}$ will denote $x^{p^{e(x)}}$. For any subset S of F, $e(x;S)$ will denote the exponent of x over $K(S)$; in case $S = \{y\}$ we will write $e(x;y)$ for $e(x;S)$.

For subsets A and B of F, $A \subset B$, we write $x \in B \setminus A$ in case $x \in B$ and $x \notin A$.

For $x, y \in F \setminus K$ we define $x \sim y$ if and only if $K^p(\underline{x}) = K^p(\underline{y})$, i.e., if and only if $\underline{x}$ and $\underline{y}$ are p-dependent in K. It is immediate that "$\sim$" is an equivalence relation on $F \setminus K$. It is the purpose of this note to establish a one-to-one correspondence between the equivalence classes so determined and the subfields of K of the form $K^p(a)$ where $a \in (K \cap F^p) \setminus K^p$. For $x \in F \setminus K$, the equivalence class containing x will be denoted by $[x]$ and $[\underline{x}]$ will denote the set $\{\underline{y} \mid y \in [x]\}$. It is apparent that for $a \in F \setminus K$, $K^p(\underline{a}) = K^p([\underline{a}])$.

For definitions and relevant theorems the reader is referred to Chapter II of [1].

LEMMA 1. *Let* $x, y \in F$. *If* $y \in K(x) \setminus K$, *then* $x \in K(y)$ *or* $y \in K(x^p)$.

Proof. We assume $y = \sum_{i=0}^{n} a_i x^i$ where $a_i \in K$, $a_n \neq 0$, $n \geqslant 1$. Let $i = q_i p + r_i$, $0 \leqslant r_i < p$, $i = 0, 1, \ldots, n$.

*The authors are indebted to the referee.

Then

$$y = \sum_{i=0}^{n} a_i x^i = \sum_{i=0}^{n} a_i (x^p)^{q_i} x^{r_i} = \sum_{j=0}^{p-1} B_j x^j \quad \text{where}$$

$B_j = \sum a_t (x^p)^{q_t}$ and the summation is over t such that $0 \leqslant t \leqslant n$ and $t \equiv j \pmod p$. Let $f(Z) = (B_o - y) + \sum_{j=1}^{p-1} B_j Z^j$, $f(Z) \in K(x^p, y)[Z]$. Suppose $f(Z)$ is not the zero polynomial. Then the minimal polynomial of x over $K(x^p, y)$ has degree not exceeding $p-1$, hence x is separable over $K(x^p, y)$. But x is purely inseparable over $K(x^p, y)$ so $x \in K(x^p, y)$. Hence $K(y)(x) = K(y)(x^p)$ and so x is separable over $K(y)$. Since x is also purely inseparable over $K(y)$, we have $x \in K(y)$. If $x \notin K(y)$, then $f(Z)$ is the zero polynomial and $y = B_o$ is an element of $K(x^p)$.

THEOREM 1. *Let* $y, x \in F$. $y \in K(x) \setminus K(x^p)$ *if and only if* $x \in K(y) \setminus K(y^p)$.

Proof. Assume $y \in K(x) \setminus K(x^p)$. By Lemma 1, $x \in K(y)$. Suppose $x \in K(y^p)$, then $K(x) \subseteq K(y^p)$ and so $y \in K(y^p)$. But then $K(y) = K(y^p)$ and y is separable over K. It follows that $y \in K$, since y is also purely inseparable over K. This is a contradiction so $x \in K(y) \setminus K(y^p)$. The converse follows by symmetry.

COROLLARY 1. *Let* L *be a subfield of* F, $S \subseteq F$, $x, y \in F$, $x^p \in L^p(S)$. *If* $y \in L^p(S, x)$ *and* $y \notin L^p(S)$, *then* $x \in L^p(S, y)$.

THEOREM 2. *Let* $y, x \in F$. *If* $y \in K(x) \setminus K$, *then* $y \in K(x^{p^g}) \setminus K(x^{p^{g+1}})$ *where* $g = e(x; y)$.

Proof. Let g be the largest non-negative integer such that $y \in K(x^{p^g}) \setminus K(x^{p^{g+1}})$. By Theorem 1, $x^{p^g} \in K(y) \setminus K(y^p)$ and so $g \geqslant e(x; y)$. If $g > e(x; y)$ we obtain $x^{p^g} \in K(y^p)$, a contradiction.

https://doi.org/10.4153/CMB-1969-017-3 Published online by Cambridge University Press

THEOREM 3. Let $x, y \in F \setminus K$. Then $e(x) > e(x;y)$ if and only if $K^p(x) = K^p(y)$.

Proof. If $K^p(x) = K^p(y)$, then $x^{p^{-1}} \in K(y^{p^{-1}})$ and so $e(x;y) < e(x)$. Assume $e(x) > e(x;y)$. By Theorem 2,

$$x^{p^{e(x)-1}} \in K(y^{p^t}) \setminus K(y^{p^{t+1}}) \text{ where } t = e(y; x^{p^{e(x)-1}}).$$

Necessarily $t < e(y)$. By Theorem 1, $y^{p^t} \in K(x^{p^{e(x)-1}}) \setminus K$ and so $t + 1 \geq e(y)$. Hence $t = e(y) - 1$ and $x \in K^p(y)$. Corollary 1 of Theorem 1 applies.

THEOREM 4. Let $y, x \in F \setminus K$. Then

(a) $e(y;x) = e(y; x^{p^{e(x;y)}})$ and $e(x;y) = e(x; y^{p^{e(y;x)}})$;

also

(b) $e(y;x) - e(x;y) = e(y) - e(x)$.

Proof. If $e(x) = e(x;y)$, (a) and (b) obviously hold. Assume $e(x) > e(x;y)$. Then $y^{p^{e(y;x)}} \in K(x) \setminus K$ and by Theorem 2 we have $y^{p^{e(y;x)}} \in K(x^{p^f}) \setminus K(x^{p^{f+1}})$ where $f = e(x; y^{p^{e(y;x)}})$. One easily obtains

$$e(y;x) = e(y) - e(x) + e(x; y^{p^{e(y;x)}}), \tag{1}$$

and

$$e(x;y) = e(x) - e(y) + e(y; x^{p^{e(x;y)}}). \tag{2}$$

From equations (1) and (2) we obtain

$$e(x;y) - e(x; y^{p^{e(y;x)}}) = e(y; x^{p^{e(x;y)}}) - e(y;x). \tag{3}$$

The left member of (3) is not negative, the right member of (3) is not positive, hence both are zero and we have part (a). From part (a) and equation (1) we obtain

https://doi.org/10.4153/CMB-1969-017-3 Published online by Cambridge University Press

$$e(y;x) = e(y) - e(x) + e(x;y)$$

and so we have

$$e(y;x) - e(x;y) = e(y) - e(x).$$

THEOREM 5. Let $y, x \in F\backslash K$. Then $K(y^{p^{e(y;x)}}) = K(x^{p^{e(x;y)}})$.

Proof. If $y \not\sim x$, then both fields coincide with K. Suppose $y \sim x$. Then $y^{p^{e(y;x)}} \in K(x)\backslash K$, and by Theorem 2 we have $y^{p^{e(y;x)}} \in K(x^{p^{f}})\backslash K(x^{p^{f+1}})$ where $f = e(x;y^{p^{e(y;x)}})$. But by Theorem 4, $e(x;y^{p^{e(y;x)}}) = e(x;y)$. We therefore have $y^{p^{e(y;x)}} \in K(x^{p^{e(x;y)}})$. Similarly we obtain $x^{p^{e(x;y)}} \in K(y^{p^{e(y;x)}})$. Thus $K(y^{p^{e(y;x)}}) = K(x^{p^{e(x;y)}})$.

THEOREM 6. There is a one-to-one correspondence between the equivalence classes determined by $\sim$ and the subfields of K of the form $K^p(\alpha)$ where $\alpha \in (K \cap F^p)\backslash K^p$.

Proof. Define ψ as follows: $\psi([a]) = K^p(\underline{a})$. ψ is well-defined since $K^p(\underline{a}) = K^p([\underline{a}])$. ψ is one-to-one since $K^p(\underline{a}) = K^p(\underline{b})$ implies $a \sim b$. Let $\alpha \in (K \cap F^p)\backslash K^p$, then $\alpha = b^p$ for some $b \in F$. then $\alpha \in K^p$. Hence $b \in F\backslash K$. $\psi([b]) = K^p(\underline{b}) = K^p(b^p) = K^p(\alpha)$.

It is also easy to show that if the number of equivalence classes $[a]$ of $F\backslash K$ is greater than one, then there are infinitely many of these equivalence classes.

REFERENCE

1. O. Zariski and P. Samuel, Commutative algebra, Vol. I. (D. Van Nostrand Company Inc., Princeton, New Jersey, 1958).

Western Washington State College

Iowa State University

https://doi.org/10.4153/CMB-1969-017-3 Published online by Cambridge University Press