ON THE EXISTENCE OF EXCEPTIONAL FIELD EXTENSIONS

BY ROBERT GILMER[1] AND WILLIAM HEINZER

Communicated by G. D. Mostow, January 15, 1968

Let F be a field of characteristic $p \neq 0$ and let K be an algebraic field extension of F. Let K_i denote the subfield of K of elements purely inseparable over F, K_s the subfield of separable elements, and K^n the normal closure of K/F. We say that K/F splits if $K = K_iK_s$ and following Reid's terminology in [2], K is called an *exceptional* extension of F provided $K_i = F$ and $K_s \neq K$.

LEMMA 1. *K/F splits if and only if $K_i = (K^n)_i$.*

PROOF. If K/F splits it follows easily that $K_i = (K^n)_i$. Conversely assume that $K_i = (K^n)_i$. Then K^n/K is separable normal and hence a Galois extension. Since a normal extension splits we have $K^n = (K^n)_i(K^n)_s$ and if $a \in K$, $a = \sum a_\alpha e_\alpha$ with $a_\alpha \in (K^n)_s$ and $\{e_\alpha\}$ a linearly independent set of elements of $(K^n)_i = K_i$ over F. If σ is an automorphism of K^n/K then $\sigma(a) = a$ implies that $\sum(\sigma(a_\alpha) - a_\alpha)e_\alpha = 0$. But K_i and $(K^n)_s$ are linearly disjoint over F so that $\{e_\alpha\}$ is linearly independent over $(K^n)_s$. Hence $\sigma(a_\alpha) = a_\alpha$ and we have $a_\alpha \in K \cap (K^n)_s = K_s$. Thus $K = K_sK_i$.

THEOREM 2. *If K/F is a simple extension then K/F splits if and only if K^n/F is simple.*

PROOF. If K/F splits then by Lemma 1, $K_i = (K^n)_i$ and it is clear that K^n/F is also simple.

If K^n/F is simple then K/F and $(K^n)_i/F$ are simple. Let $f(X)$ be the minimum polynomial of t over F, where t is chosen such that $K = F(t)$. Then K^n is the splitting field of $f(X)$ and we have

(a) $\exp f(X) = \exp (K^n)_i$,

(b) $p^{\exp f(X)} = [K: K_s]$.

Since $(K^n)_i/F$ is simple it follows that $p^{\exp (K^n)_i} = [(K^n)_i: F]$ [3, pp. 120–123]. Hence $[K: K_s] = [(K^n)_iK_s: K_s]$ and since $K \subseteq (K^n)_iK_s$ we have $(K^n)_iK_s = K$ and $(K^n)_i = K_i$. By Lemma 1, K/F splits.

Our next lemma gives a method for constructing exceptional field extensions.

[1] The first author received partial support from the National Science Foundation while this research was being done.

LEMMA 3. *Let a, b, and s be elements of an algebraic extension field of F with a and b purely inseparable over F, s separable over F and not in F. Let $t=a+bs$ and $K=F(t)$. Then $F(a, b)=(K^n)_i$ and $F(a, b)/F$ is generated by the coefficients of the minimum polynomial for t over $F(a, b)$.*

PROOF.[2] Let $s=s_1, s_2, \cdots, s_n$ be a complete set of conjugates of s over F and let $t_i=a+bs_i$. If e is a nonnegative integer such that a^{p^e}, $b^{p^e}\in F$, then $F(t_i^{p^e})=F(s_i^{p^e})=F(s_i)$. Hence $F(s_1, \cdots, s_n) \subseteq F(t_1, \cdots, t_n)$. Also $b=(t_1-t_2)(s_1-s_2)^{-1}$ so that b, and hence a, are in $F(t_1, \cdots, t_n)$. It follows that $F(t_1, \cdots, t_n)=F(a, b)\otimes F(s_1, \cdots, s_n)$. And since the t_i are con'ugates over F, we have $F(t_1, \cdots, t_n)=K^n$ and $F(a, b)=(K^n)_i$ [1, p. 50]. The minimum polynomial for t over $F(a, b)$ is $g=\prod_{i=1}^n(X-t_i)$. If F_0 is the subfield of $F(a, b)$ obtained by adjoining the coefficients of g to F, then F_0/F is purely inseparable and K^n/F_0 is separable. Therefore, $F_0=(K^n)_i=F(a, b)$.

REMARK 4. Reid calls a separable field extension E/F *realizable* if there exists an exceptional extension K/F with $E=K_s$ [2]. Using Lemma 3 we can show that when F/F^p is not simple then any proper separable extension of F is realizable.

THEOREM 5. *Let K/F be normal and inseparable, but not purely inseparable. Then K/F is simple if and only if every subextension of K/F splits.*

PROOF. If K/F is simple and E is an intermediate field then we can take $E^n\subseteq K$. Hence E^n/F is simple and by Theorem 2, E/F splits. Conversely if K/F is not simple then K_i/F is not simple. Hence there exist $a, b\in K_i$ such that $F(a, b)/F$ is not simple. We choose $s\in K_s-F$ and set $t=a+bs$. If $E=F(t)$ then by Lemma 3, $F(a, b)\subseteq E^n$ so that E^n/F is not simple. Hence by Theorem 2, E/F does not split.

Our next result gives necessary and sufficient conditions that a given normal inseparable extension K/F contain intermediate fields which are exceptional over F.

THEOREM 6. *Let K/F be normal and inseparable but not purely inseparable. Let E be the maximal purely inseparable subfield of K/F of exponent one. Then E/F is simple if and only if K/F contains no exceptional subextensions.*

PROOF. If K/F contains an exceptional subextension then K contains an element t such that $F(t)/F$ is exceptional of exponent one.

[2] The proof of Lemma 3 indicated here is that of H. F. Kreimer; it simplifies an earlier proof due to the authors.

Thus $F(t)/F$ does not split and $F(t)^n$ is not simple by Theorem 2. Hence $(F(t)^n)_i$ is purely inseparable of exponent one and not simple. Thus E/F is not simple.

To prove the converse we assume that E/F is not simple and choose $a, b\in E$ such that $F(a, b)/F$ is not simple. Let $s\in K_s - F$ and, as in Lemma 3, set $t=a+bs$. Then $F(t)/F$ does not split and $F(a, b) = (F(t)^n)_i$. Moreover, $F(t^p)=F(s)$ is separable over F. Thus if $F(t)\cap F(a, b)$ properly contained F then $F(t)/F$ would necessarily split. Hence $F(t)_i=F$ and $F(t)/F$ is exceptional.

COROLLARY 7. *If $F(t)/F$ is inseparable but not purely inseparable and if $f=\sum_{i=0}^r a_i X^{ip^e}$ is the minimum polynomial for t over F, where $e=\exp f$, then $F(t)/F$ is exceptional if and only if $F(\{a_i^{1/p}\}_0^r)/F$ is not simple.*

PROOF. Sufficiency follows as in Theorem 2. Necessity follows from Theorem 6 and the fact that $F(\{a_i^{1/p}\}_0^r)$ is the maximal purely inseparable subfield of exponent one of $F(t)^n/F$.

In view of Theorem 6, if there exists a purely inseparable extension L of F such that L/F is not simple and such that E/F is simple where E is the maximal subfield of L/F of exponent one, then there exists a normal extension K of F such that K/F is not simple, but there are no intermediate exceptional extensions. If we take $F=P(X, Y, Z)$ where P is a perfect field and where $\{X, Y, Z\}$ is algebraically independent over P, and if $L=F(X^{1/p}, X^{1/p^2}+Y^{1/p}, X^{1/p^2}Z^{1/p})$, then it can be shown that $E=F(X^{1/p})$, providing the desired example.

REFERENCES

1. N. Jacobson, *Lectures in abstract algebra*. Vol. 3, Van Nostrand, Princeton, N. J., 1964.

2. J. D. Reid, *A note on inseparability*, Michigan Math. J. 13 (1966), 219–223.

3. B. L. van der Waerden, *Modern algebra*. Vol. 1, Ungar, New York, 1953.

FLORIDA STATE UNIVERSITY AND
LOUISIANA STATE UNIVERSITY, BATON ROUGE