ON MINIMAL SETS OF GENERATORS OF PURELY INSEPARABLE FIELD EXTENSIONS

PAUL T. RYGG[1]

1. Let F be an extension field of K. A *minimal set of generators* of F over K is a subset S of F such that $F=K(S)$ and $S'\subset S$ implies $K(S')\subset K(S)$ where $\subset$ denotes proper inclusion. Pickert [**4**, p. 88] has shown that if F is a finite inseparable extension of K (the characteristic of K is $p\neq 0$) and $S=\{a_1, \cdots, a_n\}$ is a minimal set of generators of F over K, then S is p-independent in F (this concept, due to Teichmüller [**5**], is defined in §2 following) and is a minimal set of generators of F over $F^p(K)$. A *relative p-basis* of F over K, as introduced in [**5**], is a minimal set of generators of F over $F^p(K)$. It is shown by Becker and MacLane [**1**, Theorem 6] that if F is a finite purely inseparable extension of K, then the minimal number of generators of F over K is n, the exponent determined by the degree $[F: F^p(K)]=p^n$. Closely related results are given by Weil [**6**, Chapter I, §5] and by Zariski and Samuel [**7**, Chapter II, §17] in a discussion of derivations on fields.

In this note we assume that F is a purely inseparable extension of K of arbitrary degree but with finite exponent e: $F^{p^e}\subset K$. It is the purpose of this note to prove the following:

THEOREM 1. *If F is a purely inseparable extension of K with finite exponent e, then there exist minimal sets of generators of F over K and any two such sets have the same cardinal number.*

This result for the case of exponent $e=1$ is given by MacLane [**2**, Theorem 12, p. 463].

2. Let ϕ be a mapping of the set of all subsets of a set F into itself. A subset X is *free with respect to* ϕ, or ϕ*-free* (or simply *free*), when $x\notin\phi(X-x)$ for all $x\in X$. (Here $X-x$ denotes the complement of $\{x\}$ in X.) A ϕ*-basis* (or simply a *basis*) of F is a subset X of F that is free and such that $\phi(X)=F$.

The following theorem is well known. (For example see [**7**, Chapter II].)

THEOREM A. *If ϕ satisfies the following dependence axioms*:

(D_1) $X\subseteq\phi(X)$,

Received by the editors December 1, 1961 and, in revised form, August 13, 1962.

[1] The author is indebted to Professor Bernard Vinograde.

(D_2) *if* $x \in \phi(X)$, *then* $x \in \phi(X_0)$ *for some finite subset* X_0 *of* X,

(D_3) *if* $X \subseteq Y$, *then* $\phi(X) \subseteq \phi(Y)$,

(D_4) $\phi(\phi(X)) = \phi(X)$,

(D_5) *if* $y \in \phi(X, x) = \phi(X \cup \{x\})$ *and* $y \notin \phi(X)$, *then* $x \in \phi(X, y)$, *then there exist bases of F and any two bases have the same cardinal number.*

In the case F is an extension field of K we define the mapping ϕ_K by $\phi_K(X) = K(X)$ for $X \subseteq F$. We will say that a subset X of F is *minimal with respect to the subfield* K when X is free with respect to ϕ_K. A subset X is a minimal set of generators of F over K when X is a ϕ_K-basis of F.

That Theorem 1 does not follow directly from Theorem A is seen from the following example. Let Q be a perfect field of characteristic $p \neq 0$ and let u and v be algebraically independent indeterminates over Q. Define $K = Q(u, v)$ and $F = K(x)$ where $x = (y+v)^{p^{-1}}$ and $y = u^{p^{-1}}$. Obviously $y \in K(x)$ and $y \notin K$. But if $x \in K(y)$, then $y \in K$ so ϕ_K in this case does not satisfy (D_5).

In [7, p. 129] it is shown that for any field F with characteristic $p \neq 0$ the mapping ϕ_{F^p} satisfies (D_1) – (D_5). The property exhibited by (D_5) in this case is called the *exchange property*. A ϕ_{F^p}-basis is called a *p-basis* of F. A subset X of F is *p-independent* in F if and only if X is free with respect to ϕ_{F^p}.

3. PROPOSITION 1. *Let* G' *be a subset of* K *that is p-independent in* F *and such that* $F^p(G') = F^p(K)$. *If* G' *is extended to a p-basis* $G' \cup M$ *of* F, *then* M *is a minimal set of generators of* F *over* K.

PROOF. Let $W = G' \cup M$. We have

$$F = F^p(W) = F^{p^e}(W) = F^{p^e}(K, M) = K(M).$$

Assume $a \in M$ and $a \in K(M-a)$. Since $K(M-a) \subset F^p(G', M-a)$, we have $a \in F^p(W-a)$, a contradiction.

COROLLARY. *Every p-basis of* F *contains a subset* M *that is a minimal set of generators of* F *over* K.

PROOF. Let W be a p-basis of F and put $M' = W \cap (F - F^p(K))$. Let G' be as defined above. Since $F = F^p(G', M')$, G' can be extended to a p-basis $G' \cup M$ where $M \subseteq M'$.

PROPOSITION 2. *Let* M' *be a subset of* F *that can be extended to a p-basis* $M' \cup G^*$ *of* F *where* $G^* \subset K$. *Then* M' *is a minimal set of generators of* F *over* K *if and only if* $F^p(G^*) = F^p(K)$.

PROOF. Assume M' is a minimal set of generators of F over K. If

$F^p(G^*) \neq F^p(K)$, then there is an element $x \in K$ such that $x \notin F^p(G^*)$ and $x \in F^p(G^*, M')$. This implies that there is a finite subset M_0 of M' and an element $a \in M_0$ such that $x \in F^p(G^*, M_0)$ and

$$x \notin F^p(G^*, M_0 - a).$$

By the exchange property we obtain $a \in F^p(G^*, M_0 - a, x)$. Since $F^p(G^*, M_0 - a, x) \subseteq K(M' - a, a^p)$, we have $a \in K(M' - a, a^p)$. This implies that a is separable over $K(M' - a)$ and, since a is purely inseparable over K, it follows that $a \in K(M' - a)$. This is a contradiction so $F^p(G^*) = F^p(K)$.

If $F^p(G^*) = F^p(K)$, then M' is a minimal set of generators of F over K by Proposition 1.

PROPOSITION 3. *If M is a minimal set of generators of F over K, then M is p-independent in F and $F^p(M) \cap F^p(K) = F^p$.*

PROOF. If M is not p-independent in F there is an element $a \in M$ such that $a \in F^p(M - a)$. Since $F^p = K^p(M^p)$, this implies that $a \in K(M - a, a^p)$. From this it follows, as in the preceding proof, that $a \in K(M - a)$ which is a contradiction.

Since $F = F^p(M, K)$, M can be extended to a p-basis $M \cup G'$ of F, where $G' \subset K$. From Proposition 2 we have $F^p(G') = F^p(K)$. If $y \notin F^p$ and $y \in F^p(M) \cap F^p(K)$, then there exists a finite subset M_0 of M containing an element a such that $y \in F^p(M_0)$ and $y \notin F^p(M_0 - a)$. By the exchange property we have $a \in F^p(M_0 - a, y)$. Since $y \in F^p(G')$, we obtain the contradiction $a \in F^p(M - a, G')$.

COROLLARY. *If M is a minimal set of generators of F over K, then $M \cap F^p(K) = \varnothing$.*

PROOF. Since M is p-independent in F, $M \cap F^p = \varnothing$.

PROPOSITION 4. *The following assertions are equivalent:*

(a) $F = K$.

(b) $F = F^p(K)$.

(c) *K contains a p-basis of F.*

(d) *There exists no nonempty minimal set of generators of F over K.*

PROOF. It is easily seen that (a), (b) and (c) are equivalent. If M is a nonempty minimal set of generators of F over K, then by the corollary to Proposition 3 we have $M \subseteq (F - F^p(K))$ and $F \neq F^p(K)$. If $F \neq F^p(K)$, then there exists a nonempty minimal set of generators of F over K by Proposition 1.

In the following let $L = F^p(K)$. That ϕ_L satisfies the dependence axioms (D_1–D_5) follows immediately from the fact that ϕ_{F^p} satisfies these axioms. An application of Theorem A gives the following:

PROPOSITION 5. *There exist minimal sets of generators of F over L and any two such sets have the same cardinal number.* (*See MacLane* [3, §4, *p.* 376].)

The proof of the following lemma is easily obtained using the exchange property.

LEMMA. *If C is a subset of F that is p-independent in F and if B is a subset of F that is minimal with respect to $F^p(C)$, then $B\cup C$ is p-independent in F.*

Theorem 1 follows immediately from Proposition 5 and the following:

PROPOSITION 6. *Let M be a subset of F. M is a minimal set of generators of F over L if and only if M is a mininal set of generators of F over K.*

PROOF. Assume M is a minimal set of generators of F over L. Clearly M is minimal with respect to K. Let G' be as defined in Proposition 1. By the lemma, $G'\cup M$ is p-independent in F and is a p-basis of F since $F=L(M)=F^p(G', M)$. By Proposition 1, M is a minimal set of generators of F over K.

Assume M is a minimal set of generators of F over K. Clearly $L(M)=F$. M may be extended to a p-basis $M\cup G'$ of F, where $G'\subset K$ and, by Proposition 2, $F^p(G')=L$. Since $M\cup G'$ is p-independent in F, M is minimal with respect to L and so is a minimal set of generators of F over L.

REFERENCES

1. M. F. Becker and S. MacLane, *The minimum number of generators for inseparable extensions*, Bull. Amer. Math. Soc. **46** (1940), 182–186.

2. S. MacLane, *A lattice formulation for transcendence degrees and p-bases*, Duke Math. J. **4** (1938), 455–468.

3. ———, *Modular fields*. I, Duke Math. J. **5** (1939), 372–393.

4. G. Pickert, *Inseparable körpererweiterungen*, Math. Z. **52** (1949), 81–136.

5. O. Teichmüller, *p-Algebren*, Deutsche Math. **1** (1936), 362–388.

6. A. Weil, *Foundations of algebraic geometry*, Amer. Math. Soc. Colloq. Publ. Vol. 29, Amer. Math. Soc., Providence, R. I., 1946.

7. O. Zariski and P. Samuel, *Commutative algebra*, Vol. I, Van Nostrand, Princeton, N. J., 1958.

WESTERN WASHINGTON STATE COLLEGE