

## GENERATING ELEMENTS IN A FIELD

BY MOTOICHI OKUZUMI

It is well known that, when  $F$  is a finite separable extension of a field  $k$ , there is an element  $\alpha$  in  $F$  such that  $F=k(\alpha)$ . Let  $L$  be an intermediate field between  $F$  and  $k$ , then every generating element of  $F$  over  $k$  is a generating element over  $L$ . But the converse is not true.

We shall say that an intermediate field  $M$  in  $F/k$  has property (P), when every generating element over  $M$  is a generating element over  $k$ . In the present note we shall prove the existence of the maximal intermediate field with property (P) in  $F/k$  and characterize this field.

In the case when  $k$  is a finite field, the above subfield may be given by the following theorem.

**THEOREM 1.** *When  $k$  is a finite field and  $F/k$  is an extension of degree  $n=p_1^{e_1}p_2^{e_2}\cdots p_s^{e_s}$ , then the maximal subfield with property (P) is the subfield of degree  $p_1^{e_1-1}p_2^{e_2-1}\cdots p_s^{e_s-1}$ .*

*Proof.*  $F/k$  is a cyclic extension field and for any divisor  $d$  of  $n$ , there is a unique subfield of degree  $d$ . Let  $\Delta$  be the subfield of degree  $p_1^{e_1-1}p_2^{e_2-1}\cdots p_s^{e_s-1}$ , then  $\Delta$  has property (P). For, let  $\Delta(\alpha)=F$  and  $k(\alpha)$  has degree  $p_1^{f_1}p_2^{f_2}\cdots p_s^{f_s}$  over  $k$ . If for some  $i$ ,  $f_i < e_i$ , then there is a unique proper subfield  $\Delta'$  of degree  $p_1^{m_1}p_2^{m_2}\cdots p_s^{m_s}$ , where  $m_i = \max(f_i, e_i - 1)$  ( $i=1, 2, \dots, s$ ). But  $\Delta'$  contains  $\alpha$  and  $\Delta$ , so  $\Delta'=F$ . This contradicts the hypothesis that  $\Delta'$  is a proper subfield of  $F$ .

Conversely, let  $L$  be a subfield with property (P) and its degree be  $p_1^{l_1}p_2^{l_2}\cdots p_s^{l_s}$ , then  $L$  is contained in  $\Delta$ . For, if for some  $i$ ,  $e_i - 1 < l_i$ , then  $L$  contains the subfield  $F_i$  of degree  $p_i^{e_i}$ . As  $F$  is direct product of  $F_i$  and  $F'_i$  whose degree is  $\prod_{j \neq i} p_j^{e_j}$ , there is a generating element  $\xi$  in  $F'_i$  over  $F_i$ . So  $\xi$  is a generating element over  $L$  and from property (P),  $k(\xi)=F$ . This contradicts with the assumption  $k(\xi) \subset F'_i$ .

In the following, we assume that  $k$  has an infinite number of elements.

**LEMMA.** *If two intermediate fields  $L_1, L_2$  in  $F/k$  have property (P), so the composite field  $L=(L_1, L_2)$ .*

*Proof.* We denote generating elements as follows:

$$F=L(\alpha), \quad L=L_1(\beta_2)=L_2(\beta_1) \quad (\beta_i \in L_i, i=1, 2).$$

---

Received January 30, 1964.