GENERATING ELFMENTS 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 α 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 Δ be the subfield of degree $p_1^{e_1-1}p_2^{e_2-1}\cdots p_s^{e_s-1}$, then Δ 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 Δ' of degree $p_1^{m_1}p_2^{m_2}\cdots p_s^{m_s}$, where $m_i=\max(f_i, e_i-1)$ $(i=1, 2, \cdots, s)$. But Δ' contains α and Δ, so $\Delta'=F$. This contradicts the hypothesis that Δ' 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 Δ. 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 $\Pi_{j\neq i}p_j^{e_j}$, there is a generating element ξ in F_i' over F_i. So ξ 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:

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

Received January 30, 1964.

Then

$$F=L(\alpha)=L_1(\alpha,\ \beta_2).$$

We consider the system of fields $L_1(\alpha+\gamma_n\beta_2)$, $n=1, 2, \cdots$, $\gamma_n \in k$. Then from the finiteness of number of intermediate fields in F/k, there must be a pair, $L_1(\alpha+\gamma_n\beta_2)=L_1(\alpha+\gamma_m\beta_2)$. As the field contains α and β_2, this field is F. So, from property (P), $F=k(\alpha+\beta_2')=L_2(\alpha)=k(\alpha)$.

We denote this maximal subfield with property (P) by $\varDelta$, then we can characterize $\varDelta$ as follows:

THEOREM 2. *$\varDelta$ is the intersection of all maximal subfields of F/k.*

Proof. Let $\varDelta'$ be the intersection of all maximal subfields of F/k and α be a generating element of F over $\varDelta'$: $F=\varDelta'(\alpha)$.

If $k(\alpha)$ is not F, then there is a maximal subfield M containing $k(\alpha)$. From $M\supset\varDelta'$, $M=M(\alpha)=F$. This contradicts with the assumption, $M\subsetneqq F$.

Conversely, a subfield L has property (P) and if there is a maximal subfield M such that $M\not\supset L$, the composite field (M, L) is F. Let $M=k(m)$, then $L(m)=F$ and from property (P), $k(m)=F$. So this contradicts $M\subsetneqq F$.

When F/k is a Galois extension field. every maximal subfield corresponds to a minimal subgroup in the Galois group G of F/k. So $\varDelta=\varDelta_1$ corresponds to the subgroup D_1 generated by all elements of prime order.

The corresponding subgroup D_1 is a normal subgroup, so $\varDelta_1$ is also a Galois extension field of k. And the Galois group is isomorphic with the factor group G/D_1.

Similarly, we can define $\varDelta_2$ as the intersection of all maximal intermediate fields between $\varDelta_1$ and k, and so on.

Thus we obtain a series of normal subfields and correspondingly the principal series $G\supset D_1\supset\cdots\supset E$. And each $\varDelta_{i-1}/\varDelta_i$ is a Galois extension and corresponds to a factor group D_i/D_{i-1} generated by all elements of prime orders in G/D_{i-1}.

REFERENCES

[1] ALBERT, A. A., Modern higher algebra. Chicago, Univ. of Chicago Press (1937).

[2] ARTIN, E., Galois theory. Notre Dame Mathematical Lectures, No. 2. Notre Dame (1942).

[3] VAN DER WAERDEN, B. L., Moderne Algebra. 2 vol. (1930), (1931).

DEPARTMENT OF MATHEMATICS,
TOKYO INSTITUTE OF TECHNOLOGY.