147. *Large Subfields and Small Subfields*

By Mikihiko ENDO
Department of Mathematics, Rikkyo University

(Comm. by Kenjiro SHODA, M. J. A., Nov. 13, 1972)

Let L/K be any extension of fields. As in the module theory (Lambek [2], p. 93), a subfield E of L/K (i.e. a subfield of L containing the field K) is called *a small subfield*, if, for any subset A of L, $E(A)=L$ implies $K(A)=L$, where $K(A)$ is the subfield generated by A over K. Further, a subfield F is called *a large subfield* of L/K, if, for any subfield H of L, $F\cap H=K$ implies $H=K$. We shall discuss the existence of a minimal large subfield and a maximal small subfield. The method used here is similar to the one in the group theory (Kurosh [1], p. 217).

A field H is called *a proper subfield* of L/K, if $K\subsetneqq H\subsetneqq L$.

Theorem 1. *Assume that any proper subfield of L/K contains a proper minimal subfield. Then, the subfield F, generated by all the proper minimal subfields of L/K, is a unique minimal large subfield of L/K.*

Proof. We shall show that, for any subfield G of L/K, G is large if and only if $G\supseteqq F$.

If $G\not\supseteq F$, there exists a minimal subfield M such that $G\not\supseteq M$. Then, by the minimality of M, $G\cap M=K$. Since $K\subsetneqq M$, G is not large.

On the other hand, let G be not large. Then, there exists a subfield $H\supsetneqq K$ of L/K, such that $G\cap H=K$. By assumption, there exists a minimal subfield M such that $H\supseteqq M\supsetneqq K$. Then, $M\cap G\subseteqq H\cap G=K$. This shows that $G\not\supseteq M$, and so $G\not\supseteq F$. Q.E.D.

If L/K is an algebraic extension, the assumption of Theorem is always satisfied. Further, if L/K is a Galois extension, the above field F is the Frattini subfield defined by Neukirch ([3], p. 41). On the other hand, by Lüroth's Theorem, any proper subfield of a rational function field $K(X)/K$ is also a rational function field of the type $K(Y)$ ($Y\in K(X)$: transcendental over K). Therefore, a rational function field $L=K(X)$ does not satisfy the assumption of Theorem 1.

As a dual of Theorem 1, we have

Theorem 2. *Assume that any proper subfield of L/K is contained in a proper maximal subfield of L/K. Then, the intersection E of all the proper maximal subfields of L/K is a unique maximal small subfield of L/K.*

Since the proof is also dual to that of Theorem 1, we do not repeat it.

When L/K is a finite separable extension, L is a simple extension over any subfield of L/K. In this case, a subfield H of L/K is called to have the property (P), if $H(\alpha)=L$ always implies $K(\alpha)=L$. In [4], Okuzumi characterized the maximal subfield F having the property (P) as the intersection of all the proper maximal subfields of L/K. It is clear that Theorem 2 covers the result of Okuzumi.

It the assumption of Theorem 2 does not hold, we must modify the result as follows:

Theorem 3. *Let E be the intersection of all the maximal subfields of L/K (if there is no maximal subfield, the vacuous intersection means the whole field L). Then, an element x of L belongs to E, if and only if, for any subset A of L, $K(x, A)=L$ implies $K(A)=L$, namely, x is omissible from any generator system of L over K.*

Proof. First, we assume that x is not contained in E. Then, by the definition of the field E, there exists a maximal subfield M of L/K not containing the element x. Since $M=K(M)\subsetneqq K(x, M)$, $K(x, M)$ must be equal to L. This shows that x cannot be omitted from a generator system $\{x\}\cup M$.

Conversely, assume that $K(A)\neq L$ but $K(x, A)=L$. The system of all the subfields, containing the field $K(A)$ but not containing the element x, constitutes an inductive system with respect to the inclusion. Therefore, there exists a maximal subfield M in the system. If H is a subfield greater than M, H must contain the element x. Since M contains the field $K(A)$, H must be equal to the whole field L. Therefore, the field M is a maximal subfield of L/K. Since x is not contained in M, it is not contained in the field E. Q.E.D.

Let C be the algebraic closure of the rational number field $\boldsymbol{Q}$ and R be the real subfield of C. Then, if M is a proper subfield of R, the degree $[R: M]$ must be infinite, since $[C: M]<\infty$ implies $M\cong R$ (Neukirch [3], p. 23 Satz (4.1)). Since R/M is algebraic, there are infinite many intermediate subfields between R and M. This shows that R has no proper maximal subfields.

As an example of Theorem 3, we give a subfield of the algebraic real field R. Let

$$A=\{\sqrt{2}, \sqrt[4]{2}, \sqrt[8]{2}, \cdots, \sqrt[2^n]{2}, \cdots\}.$$

The field L generated by A over $\boldsymbol{Q}$ is an infinite algebraic extension of $\boldsymbol{Q}$. And each element $\sqrt[2^n]{2}$ can be omissible from the generators A of L, since $\sqrt[2^n]{2}=(\sqrt[2^{n+1}]{2})^2$. But, clearly, it is impossible to omit all the elements of A at a time. This example shows a difference between Theorem 2 and Theorem 3.

References

[1] Kurosh, A. G.: The Theory of Groups, Vol. 2. Chelsa Pub. Co. (1960). (Translated by Hirsch, K. A.)
[2] Lambek, J.: Lectures on Rings and Modules. Blaisdell Pub. Co. (1966).
[3] Neukirch, N.: Über gewisse ausgezeichnete unendliche algebraische Zahlkörper. Bonner Math. Schriften Nr. 25, 1–73 (1965).
[4] Okuzumi, M.: Generating elements in a field. Kōdai Math. Sem. Reports, **16**, 127–128 (1964).