A note on absolute Galois subfields of pure extension number fields

Takeo FUNAKURA

Department of General Education, Okayama University of Science
Ridai-cho, Okayama 700, *Japan*

(Received September 21, 1979)

Synopsis: We determine all absolute Galois fields included in pure extension number fields.

A field F is said to be a *pure extension number field*, if F is obtained by adjoining a root of an irreducible polynomial X^n-A ($A\in\mathbf{Z}$) to the rational number field $\mathbf{Q}$. A field F is said to be an *absolute Galois field*, if the extension $F/\mathbf{Q}$ is Galois.

LEMMA 1. *Let p be any odd prime. A polynomial X^q-A ($q=p^e$) is reducible on a field F if and only if A is an pth power of an element in F.*

LEMMA 2. *Suppose that positive integers m and n are relatively prime. A polynomial $X^{mn}-A$ is irreducible on a field F if and only if both X^m-A and X^n-A are irreducible on F.*

See [1] or [2] about proofs of Lemmas 1 and 2.

LEMMA 3. *Let A be a rational integer and p be an odd prime. If X^q-A ($q=p^e$) is irreducible on $\mathbf{Q}$, then it is also irreducible on every abelian extension field of $\mathbf{Q}$.*

PROOF. We shall prove the contraposition of the proposition. Suppose that X^q-A is reducible on a certain abelian extension field F. From Lemma 1, there exists an element γ in F such that $A=\gamma^p$. Thus $\mathbf{Q}(\sqrt[p]{A})=\mathbf{Q}(\gamma)$ is an abelian extension field of $\mathbf{Q}$. If $\mathbf{Q}(\sqrt[p]{A})$ does not equal to $\mathbf{Q}$, then the index $[\mathbf{Q}(\sqrt[p]{A}):\mathbf{Q}]$ is p. Let ζ be a pth primitive root of unity. Since $\zeta\sqrt[p]{A}$ is conjugate to $\sqrt[p]{A}$, the field $\mathbf{Q}(\sqrt[p]{A})$ contains ζ. Therefore $\mathbf{Q}(\sqrt[p]{A})$ includes the cyclotomic field $\mathbf{Q}(\zeta)$, and so $[\mathbf{Q}(\sqrt[p]{A}):\mathbf{Q}]$ is divisible by $[\mathbf{Q}(\zeta):\mathbf{Q}]$ which is even. This contradiction implies $\mathbf{Q}(\sqrt[p]{A})=\mathbf{Q}$, so that there exists a rational integer B with $A=B^p$. Namely by Lemma 1, the polynomial X^q-A is reducible on $\mathbf{Q}$.

LEMMA 4. *If X^n-A is irreducible on a field F, then X^m-A is irreducible on F for every divisor m of n.*

PROOF. Clear.

From now on, let $\sqrt[n]{A}$ be the root of an irreducible polynomial X^n-A ($A\in\mathbf{Z}$) satisfied

$$\arg\sqrt[n]{A}=\begin{cases}0 & \text{if } A>0,\\ \pi/2^s & \text{if } A<0,\end{cases}$$

where n is divisible by 2^s, not by 2^{s+1}.

PROPOSITION 1. *If n is odd, then $\mathbf{Q}(\sqrt[n]{A})$ does not have a non-trivial absolute Galois subfield.*

PROOF. Obviously the Galois closure of the extension $\mathbf{Q}(\sqrt[n]{A})/\mathbf{Q}$ is $\mathbf{Q}(\sqrt[n]{A},\zeta)$, where ζ is an nth primitive root of unity. It follows from Lemma 2 and 3 that

$$[\mathbf{Q}(\sqrt[n]{A},\zeta):\mathbf{Q}]=[\mathbf{Q}(\sqrt[n]{A}):\mathbf{Q}][\mathbf{Q}(\zeta):\mathbf{Q}]$$

and

$$\mathbf{Q}(\sqrt[n]{A})\cap\mathbf{Q}(\zeta)=\mathbf{Q}.$$

The extension $\mathbf{Q}(\sqrt[n]{A},\zeta)/\mathbf{Q}(\zeta)$ is cyclic and every its intermediate field is given by $\mathbf{Q}(\sqrt[m]{A},\zeta)$, where m is a divisor of n. Thus every intermediate field of $\mathbf{Q}(\sqrt[n]{A})/\mathbf{Q}$ is given by $\mathbf{Q}(\sqrt[m]{A})$, where m is a divisor of n. Suppose now that $\mathbf{Q}(\sqrt[n]{A})$ is an absolute Galois field. By Lemma 4, it is an extension field of $\mathbf{Q}$ of degree m. Therefore $\mathbf{Q}(\sqrt[m]{A})$ has an mth primitive root of unity. If m is more than 1, then similarly to Proof of Lemma 3, we obtain a contradiction. Hence we have $m=1$.

PROPOSITION 2. *If n is even and A is positive, then the maximal absolute Galois subfield of $\mathbf{Q}(\sqrt[n]{A})$ is $\mathbf{Q}(\sqrt{A})$.*

PROOF. From the way of taking the argument of $\sqrt[n]{A}$, the field $\mathbf{Q}(\sqrt[n]{A})$ is real. Let F be the maximal absolute Galois subfield of $\mathbf{Q}(\sqrt[n]{A})$. Similarly to Proof of Proposition 1, the field $\mathbf{Q}(\sqrt[n]{A})$ must have an mth primitive root of unity, where m equals $[F:\mathbf{Q}]$. Hence we get $[F:\mathbf{Q}]=2$, so that it holds $F=\mathbf{Q}(\sqrt{A})$.

We complete the note by considering the case that n is even and A is negative. Then we can put $A=-B^a$ ($a=2^s$) or $A=-B^bC^{b/2}$ ($b=2^m$, $0<m\leqq s$), where B, C are positive integers and further C is a square free except for 1.

PROPOSITION 3. *If n is even and A is negative, then the maximal absolute Galois subfield M of $\mathbf{Q}(\sqrt[n]{A})$ is given by the following;*

$$M=\begin{cases}\mathbf{Q}(\sqrt[a]{A})=\mathbf{Q}(\zeta_{2a}) & \text{if } A=-B^a \ (a=2^s),\\ \mathbf{Q}(\sqrt[2b]{A})=\mathbf{Q}(\zeta_{4b}\sqrt{B}\cdot\sqrt[4]{2}) & \text{if } A=-B^b2^{b/2} \ (b=2^m,\ 3\leqq m<s),\\ \mathbf{Q}(\sqrt[6]{A})=\mathbf{Q}(\zeta_{12}\sqrt[3]{B}\cdot\sqrt[6]{3}) & \text{if } A=-B^23 \text{ and } 3\mid n,\\ \mathbf{Q}(\sqrt[b]{A})=\mathbf{Q}(\zeta_{2b}\sqrt{C}) & \text{otherwise.}\end{cases}$$

where ζ_i is an ith primitive root of nuity.

PROOF. Put $n=2^st$, and so t is odd. Using Lemmas 1 and 2 as often as we wish, we obtain

$$[\mathbf{Q}(\sqrt[t]{A},\ \zeta_{2^n}):\mathbf{Q}(\zeta_{2^n})]=t.$$

Further from Lemma 2, we have $(a=2^s)$

$$[\mathbf{Q}(\sqrt[n]{A},\ \zeta_{2^n}):\mathbf{Q}(\zeta_{2^n})]=[\mathbf{Q}(\sqrt[a]{A},\ \zeta_{2^n}):\mathbf{Q}(\zeta_{2^n})]\cdot t.$$

Thus $\mathbf{Q}(\sqrt[n]{A})\cap\mathbf{Q}(\zeta_{2^n})=\mathbf{Q}(\sqrt[a]{A})\cap\mathbf{Q}(\zeta_{2^n})$ $(a=2^s)$, which is denoted by K. In case of $A=-B^a$ $(a=2^s)$, it obviously follows $K=\mathbf{Q}(\sqrt[a]{A})=\mathbf{Q}(\zeta_{2a})=M$ $(a=2^s)$. Hereafter suppose that $A=-B^bC^{b/2}$ $(b=2^m,\ 0<m\leqq s)$. The order of A mod $(\mathbf{Q}(\zeta_{2^n})^\times)^a$ $(a=2^s)$ in the multipule group $\mathbf{Q}(\zeta_{2^n})^\times/(\mathbf{Q}(\zeta_{2^n})^\times)^a$ $(a=2^s)$ is 2^{s-m} if C divides $n/2$, 2^{s-m+1} if C does not divide $n/2$. For $\sqrt{C}$ is in $\mathbf{Q}(\zeta_{2^n})^\times$ if and only if C divides $n/2$, since $2n$ is a multiple of 4. By the theory of Kummer extensions, its order equals $[\mathbf{Q}(\sqrt[a]{A},\ \zeta_{2n}):\mathbf{Q}(\zeta_{2n})]$ $(a=2^s)$, so that

$$[K:\mathbf{Q}]=\begin{cases}2^m & \text{if } C \text{ divides } n/2,\\ 2^{m-1} & \text{if } C \text{ does not divides } n/2.\end{cases}$$

Since K contains $\mathbf{Q}(\zeta_b)$ $(b=2^m)$, we obtain

$$K=\begin{cases}\mathbf{Q}(\zeta_{2b}\sqrt{C}) \ (b=2^m) & \text{if } C \text{ divides } n/2,\\ \mathbf{Q}(\zeta_b) \ \ (b=2^m) & \text{if } C \text{ does not divides } n/2.\end{cases}$$

Now the maximal cyclotomic field F included in K is given by the following;

$$F=\begin{cases}\mathbf{Q}(\zeta_{2a}) & \text{if } A=-B^a \ (a=2^s)\\ \mathbf{Q}(\zeta_{2b}) & \text{if } A=-B^b2^{b/2} \ (b=2^m,\ s\geqq m\geqq 3)\\ \mathbf{Q}(\zeta_6) & \text{if } A=-B^23\\ \mathbf{Q}(\zeta_b) & \text{otherwise.}\end{cases}$$

The extension $\mathbf{Q}(\sqrt[n]{A},\ \zeta_{2n})/\mathbf{Q}(\zeta_{2n})$ is cyclic and its intermediate field is given by $\mathbf{Q}(\sqrt[d]{A},\ \zeta_{2n})$, where d is divisor of n. Therefore any intermediate field of $K(\sqrt[n]{A})/K$ is given by $K(\sqrt[d]{A})$, where d is a divisor of n. Since M is maximal, it holds $K(\sqrt[n]{A})\supset M\supset K$, so that $M=K(\sqrt[d]{A})$ for some divisor d of n. In order that $K(\sqrt[d]{A})/\mathbf{Q}$ is Galois, it is necessary and sufficient that $K(\sqrt[d]{A})$ contains a dth primitve root ζ_d of unity. Since $\mathbf{Q}(\zeta_{2n})$ contains ζ_d, we see $\zeta_d\in K(\sqrt[d]{A})$ implies $\zeta_d\in K$ and further we have $\zeta_d\in F$. Hence $K(\sqrt[d]{A})/F$ is a Kummer extension, so

we can easily complete to prove the proposition.

References

1) G. Fujisaki, Fields and Galois Theory (Japanese), Iwanami, Tokyo, 1978.
2) B. L. van der Waerden, Algebra I/II, Springer Verlag, Berlin-Heidelberg-New York, 1966/67.

Takeo FUNAKURA

Department of General Education
Okayama University of Science
Ridai-cho, Okayama
Japan