ON THE IMBEDDING PROBLEM OF NORMAL ALGEBRAIC NUMBER FIELDS

EIZI INABA

Let G and H be finite groups. If a group $\bar{G}$ has an invariant subgroup $\bar{H}$, which is isomorphic with H, such that the factor group $\bar{G}/\bar{H}$ is isomorphic with G. then we say that $\bar{G}$ is an extension of H by G. Now let G be the Galois group of a normal extension K over an algebraic number field k of finite degree. The imbedding problem concerns us with the question, under what conditions K can be imbedded in a normal extension L over k such that the Galois group of L over k is isomorphic with $\bar{G}$ and K corresponds to $\bar{H}$. Brauer connected this problem with the structure of algebras over k, whose splitting fields are isomorphic with K. Following his idea, Richter investigated its local aspect using the norm theorem in the class field theory. Considering the case, where G is a p-group and the order of H is p, Scholz, Reichardt, and Tannaka succeeded to construct a normal extension over k, whose Galois group is a given p-group with $p \neq 2$. Scholz also solved the case, where G and H are both abelian. In spite of the efforts of these mathematicians the general case remains in a situation very difficult to approach. In the present paper we shall investigate the case, where G is arbitrary and H abelian of type $(p, \ldots, p)$ for a prime number p. In view of the fact, that every solvable group has a chief series $\{G_i\}$ such that the factor groups G_i/G_{i+1} are abelian of type $(p, \ldots, p)$, the following investigation shall be available for the construction of normal extensions with solvable groups.

In the following we identify $\bar{H}$ with H. Let $g_s \in \bar{G}$ be a representative of the coset, which corresponds to $s \in G$. We denote with sh the element $g_s h g_s^{-1} \in H$, which is uniquely determined for $s \in G$ and $h \in H$ irrespective of the choice of g_s from the coset. H becomes a G-module by this operation and yields a representation Λ of G. If the rank of H is n, then every element in H can be regarded as an n-dimensional vector, whose components are integers mod. p. If it corresponds a matrix $\Lambda(s)$ for $s \in G$ in the representation Λ, then $sh = \Lambda(s)h$. From $g_s g_t = A(s, t) g_{st}$ with $A(s, t) \in H$ it follows

$$(1) \qquad A(s, t) + A(st, u) = A(s, tu) + \Lambda(s) A(t, u),$$

where $A(s, t)$ is called *the factor set of the extension* $\bar{G}$ of H by G. If we take $g_s' = B(s) g_s$ with $B(s) \in H$ in place of g_s, then we have a factor set $A'(s, t)$, which

Received September 19, 1951.

is *equivalent* to $A(s, t)$, and

$$A'(s, t) = A(s, t) + B(s) - B(st) + \Lambda(s)B(t).$$

The transformation of the basis of H gives rise to a representation $D\Lambda D^{-1}$, which is equivalent with Λ. In this case we obtain the factor set $DA(s, t)$ in place of $A(s, t)$. It is well known that the extension of H by G is uniquely determined up to isomorphism by the class of representations and the class of factor sets.

Now let S be a subgroup of G. If there exists $B(\sigma) \in H$ for every $\sigma \in S$ such that

$$A(\sigma, \tau) = B(\sigma) - B(\sigma\tau) + \Lambda(\sigma)B(\tau)$$

for every $\sigma, \tau \in S$, then we say that $A(s, t)$ *splits relative to* S. In this case $A(s, t)$ is equivalent to a factor set $A'(s, t)$ such that $A'(\sigma, \tau) = 0$ for every σ, $\tau \in S$.

LEMMA. *v being any fixed element in G, $\Lambda(v)A(v^{-1}sv, v^{-1}tv)$ is a factor set, which is equivalent to $A(s, t)$.*

This lemma can be easily verified, if we choose $g'_s = g_v g_{v^{-1}sv} g_v^{-1}$ as the representative of the coset g_sH in place of g_s. From this lemma we have readily

THEOREM 1. *If $A(s, t)$ splits relative to S, then it splits also relative to any conjugate subgroup $v^{-1}Sv$ of S.*

THEOREM 2. *Let S be a p-Sylow subgroup of G. If $A(s, t)$ splits relative to S, then it splits relative to G. Two factor sets are equivalent to each other, if their difference splits relative to S.*

Proof. Let t_iS, $i = 1, \ldots, r$, be all left cosets of S in G. We can assume that $A(\sigma, \tau) = 0$ for every $\sigma, \tau \in S$ and $A(t_i, \sigma) = 0$, $i = 1, \ldots, r$, for every $\sigma \in S$, if we put $g_{t_i\sigma} = g_{t_i} g_\sigma$. Since we have from (1) $A(s, \sigma) = 0$ for every $\sigma \in S$ and $s \in G$, it follows $A(s, t) = A(s, t\sigma)$ from (1). If we put

$$B(u) = \sum_{i=1}^{r} A(u, t_i)$$

for every $u \in G$, then $B(u)$ is determined uniquely irrespective of the choice of the representatives t_i in the cosets t_iS. Then we have from (1)

$$B(u) - B(uv) + \Lambda(u)B(v) = rA(u, v)$$

for every $u, v \in G$. Since the index r of S is prime to p, $A(u, v)$ splits relative to G.

By this theorem we see that the extension $\bar{G}$ is completely determined by the representation Λ and the part of the factor set for a p-Sylow subgroup S. When in particular the order of G is prime to p, then $\bar{G}$ is determined completely by Λ. Next we consider the case, where Λ is irreducible. This means that the

G-module H is irreducible, i.e. H has no proper subgroup, which is an invariant subgroup of $\bar{G}$. In this case the extension $\bar{G}$ is called *irreducible*. When $\bar{G}$ is not irreducible, it can be obtained by repeating irreducible extensions. In fact, choose an irreducible G-submodule H_1 of H. Then $\bar{G}$ becomes an irreducible extension of H_1 by $\bar{G}/H_1$ and $\bar{G}/H_1$ an extension of H/H_1 by G, and so forth. Now let $\bar{S}$ be the subgroup of $\bar{G}$, which corresponds to S in the natural homomorphism $\bar{G}\rightarrow G$. By a theorem on finite groups it follows that the intersection of H and the center of $\bar{S}$ has a vector, which is different from zero, since $\bar{S}$ is a p-group. Consequently there exists $h\neq 0$ in H, such that $\sigma h=h$ for every $\sigma\in S$. The submodule of H, which is generated by t_ih, $i=1,\ldots,r$, is a G-module and hence is identified with H, since H is an irreducible G-module. Then we can assume that $t_1h,\ldots,t_nh$ form a basis of H, where $n\leqq r$. If in particular S is invariant, then H becomes a G/S-module and yields an irreducible representation Λ of the factor group G/S.

Every element $u\in G$ induces a permutation of all left cosets t_iS with $ut_iS=t_{i(u)}S$ and hence a permutation $i\rightarrow i(u)$ of indices i with $i(uv)=i(v)(u)$. Let the matrix $\Lambda_0(u)=(\lambda_{ij}(u))$ be determined such that $\lambda_{ij}(u)=1$, if $i=j(u)$, and $\lambda_{ij}(u)=0$, if $i\neq j(u)$. Then $\Lambda_0(u)$ yields a representation Λ_0 of G, which is induced by the identical representation of S. If in particular S is invariant, then Λ_0 is the regular representation of the factor group G/S. We can assume that t_1 is the identity of G and, putting

$$h_1=\begin{pmatrix}1\\0\\\vdots\\0\end{pmatrix},$$

we have

$$h_i=t_ih_1=\Lambda_0(t_i)h_1=\begin{pmatrix}0\\\vdots\\1\\\vdots\\0\end{pmatrix}.$$

We denote with H_0 the G-module, which is gererated by h_i, $i=1,\ldots,r$. An extension $\bar{G}_0$ of H_0 by G with the representation Λ_0 shall be called *regular*. The following theorem asserts that every irreducible extension can be obtained by means of a certain regular extension, if S is invariant.

THEOREM 3. *Let $\bar{G}$ be an irreducible extension of H by G. If the p-Sylow subgroup S of G is invariant, then there exists a regular extension $\bar{G}_0$ of H_0 by G and a submodule $\bar{H}$ of H_0, such that $\bar{G}$ is isomorphic with $\bar{G}_0/\bar{H}$ and H corresponds to $H_0/\bar{H}$.*

Proof. Since the order of G/S is prime to p, its regular representation Λ_0

is completely reducible. There exists a submodule H_1 of H_0 with $H_0 = H_1 + H_2$, such that H is operator-isomorphic with H_1. If Λ is the irreducible representation of G by H, then we have

$$D\Lambda_0 D^{-1} = \begin{pmatrix} \Lambda & 0 \\ 0 & X \end{pmatrix}.$$

Let $A(s, t)$ be the factor set of the extension $\bar{G}$. Putting

$$A(s, t) = \begin{pmatrix} a_1(s, t) \\ \vdots \\ a_n(s, t) \end{pmatrix},$$

we consider the r-dimensional vector

$$\bar{A}(s, t) = \begin{pmatrix} a_1(s, t) \\ \vdots \\ a_n(s, t) \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

Then this becomes a factor set for the representation $D\Lambda_0 D^{-1}$ and yields a regular extension $\bar{G}_0$ of H_0 *by* G. The factor group $\bar{G}_0/H_2$ is now an extension of H_0/H_2 by G, where H_0/H_2 is isomorphic with H. Its factor set can be identified with $A(s, t)$, the representation being Λ. Hence $\bar{G}$ is isomorphic with $\bar{G}_0/H_2$ and H corresponds to H_0/H_2.

If S is invariant, then $\Lambda(\sigma)$ is the unit matrix for every $\sigma \in S$. Hence every component $a(\sigma, \tau)$ of the factor set $A(\sigma, \tau)$ for an irreducible extension satisfies the relation

$$a(\sigma, \tau) + a(\sigma\tau, \varphi) = a(\sigma, \tau\varphi) + a(\tau, \varphi) \tag{2}$$

for $\sigma, \tau, \varphi \in S$. This is also satisfied by every component of the factor set for a regular extension, since $\Lambda_0(\sigma)$ is the unit matrix for $\sigma \in S$. From the preceding lemma we have

$$\Lambda_0(t_i) A(t_i^{-1}\sigma t_i, t_i^{-1}\tau t_i) = A(\sigma, \tau) + B(\sigma, i) - B(\sigma\tau, i) + \Lambda_0(\sigma) B(\tau, i) .$$

If we consider only the i-th components, then this implies

$$a_1(t_i^{-1}\sigma t_i, t_i^{-1}\tau t_i) = a_i(\sigma, \tau) + b_i(\sigma, i) - b_i(\sigma\tau, i) + b_i(\tau, i) .$$

Now, putting

$$A'(\sigma, \tau) = \begin{pmatrix} a_1(t_1^{-1}\sigma t_1, t_1^{-1}\tau t_1) \\ \vdots \\ a_1(t_r^{-1}\sigma t_r, t_r^{-1}\tau t_r) \end{pmatrix}, \quad B'(\sigma) = \begin{pmatrix} b_1(\sigma, 1) \\ \vdots \\ b_r(\sigma, r) \end{pmatrix},$$

we have

$$A'(\sigma, \tau) = A(\sigma, \tau) + B'(\sigma) - B'(\sigma\tau) + A_0(\sigma)B'(\tau)$$

for $\sigma, \tau \in S$. If we choose $B'(s)$ arbitrarily, when s does not belong to S, then we can extend $A'(\sigma, \tau)$ to a factor set $A'(s, t)$, which is equivalent to $A(s, t)$ by theorem 2, such that

$$A'(s, t) = A(s, t) + B'(s) - B'(st) + A_0(s)B'(t).$$

The vectors $A'(\sigma, \tau)$ can be determined only by the values of the first components $a_1(\sigma, \tau)$ of $A(\sigma, \tau)$ for all $\sigma, \tau \in S$. The set of values $a_1(\sigma, \tau)$ is called *the fundamental component* of the factor set for the regular extension and denoted with $a(\sigma, \tau)$ in place of $a_1(\sigma, \tau)$. We say that two fundamental components $a(\sigma, \tau)$ and $a'(\sigma, \tau)$ are *equivalent*, if there exist integers $b(\sigma)$ mod. p such that

$$a'(\sigma, \tau) = a(\sigma, \tau) + b(\sigma) - b(\sigma\tau) + b(\tau)$$

for all $\sigma, \tau \in S$. Two fundamental components yield a same regular extension up to isomorphism, if and only if they are equivalent. We suppose that it holds

$$DA_0D^{-1} = \begin{pmatrix} A_1 & 0 & \cdots & 0 \\ 0 & A_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & A_m \end{pmatrix},$$

where A_i are irreducible. Then the factor set $DA'(\sigma, \tau)$ decomposes into $A_i(\sigma, \tau)$, $i = 1, \ldots, m$, where $A_i(\sigma, \tau)$ is referred to A_i respectively. We observe that the fundamental component $a(\sigma, \tau)$ of a regular extension is a linear combination of components of factor sets of all irreducible extensions, which can be obtained from the regular extension. Conversely every such irreducible extension is completely determined by A_i and $a(\sigma, \tau)$. We say that each irreducible extension, which can be obtained by $a(\sigma, \tau)$, is referred to $a(\sigma, \tau)$.

We shall now pass to the imbedding of a normal extension K over k, whose Galois group is G. Let Ω be the subfield of K, which corresponds to the p-Sylow subgroup S of G. We assume that k contains a primitive p-th root ζ of unity. If $a(\sigma, \tau)$ is a fundamental component of the factor set for a regular extension, then the $a(\sigma, \tau)$-th powers of ζ become a factor set with respect to S and K by virtue of (2). If $a(\sigma, \tau)$ and $a'(\sigma, \tau)$ are equivalent, then they yield associated factor sets with respect to S and K. If there exists $\xi_\sigma \in K$ such that the $a(\sigma, \tau)$-th power of ζ is equal to $\sigma(\xi_\tau)\xi_{\sigma\tau}^{-1}\xi_\sigma$ for all σ, τ from S, then we say that it splits.

THEOREM 4. *Suppose that k contains a primitive p-th root ζ of unity and the p-Sylow subgroup S of G is invariant. The necessary and sufficient condition, under which the imbedding of K for every irreducible extension by G referred to a fundamental component $a(\sigma, \tau)$ is possible, is that the factor set $\zeta^{a(\sigma,\tau)}$ with respect to S and K splits.*

First we shall prove that the condition is necessary. Let $\bar{G}$ be an irreducible extension of H by G with the fundamental component $a(\sigma, \tau)$ and the Galois group of L over k be $\bar{G}$, where K corresponds to H. We choose $h \in H$ such that $t_1h, \dots, t_nh$ constitute a basis of H, where $\sigma h = h$ for all $\sigma \in S$. To the subgroup H_i of H, which is generated by all elements of the basis except t_ih, corresponds a subfield $L_i = K(\sqrt[p]{\alpha_i})$ of L with $\alpha_i \in K$. We can assume that t_ih induces the automorphism of L_i with $\sqrt[p]{\alpha_i} \to \zeta\sqrt[p]{\alpha_i}$. An automorphism g_σ of L over k induces $\beta \to \sigma(\beta)$ for $\beta \in K$. Since H_i is an invariant subgroup of $\bar{S}$, the field L_i is normal over Ω. Hence we have $g_\sigma(\sqrt[p]{\alpha_i}) = \sqrt[p]{\alpha_i}\xi_\sigma$ with $\xi_\sigma \in K$. Now let $g_\sigma g_\tau = A(\sigma, \tau)g_{\sigma\tau}$ with $A(\sigma, \tau) \in H$ and $a_i(\sigma, \tau)$ be the i-th component of $A(\sigma, \tau)$. Then the automorphism $A(\sigma, \tau)$ induces

$$\sqrt[p]{\alpha_i} \to \zeta^{a_i(\sigma,\tau)}\sqrt[p]{\alpha_i}.$$

It follows then from $g_\sigma g_\tau(\sqrt[p]{\alpha_i}) = A(\sigma, \tau)g_{\sigma\tau}(\sqrt[p]{\alpha_i})$ the relation

$$\sqrt[p]{\alpha_i}\,\xi_\sigma\cdot\sigma(\xi_\tau) = \zeta^{a_i(\sigma,\tau)}\sqrt[p]{\alpha_i}\,\xi_{\sigma\tau}.$$

Hence the $a_i(\sigma, \tau)$-th power of ζ splits. Since $a(\sigma, \tau)$ is a linear combination of all components $a_i(\sigma, \tau)$ for all irreducible extensions, which are referred to $a(\sigma, \tau)$, we can readily see that the $a(\sigma, \tau)$-th power of ζ splits.

Next we prove that the condition is sufficient. By Speiser's theorem we have $\xi_\sigma^p = \alpha^{\sigma-1}$ with $\alpha \in K$ for all $\sigma \in S$. We choose a prime ideal q in Ω with degree one, such that q is prime to all conjugates of α and does not ramify in K. Choose a number c in Ω under following conditions: (1) c is divisible by q and not divisible by the square of q, (2) c is prime to all conjugate prime ideals of q except q. Putting $\alpha c = \beta$ we have $\beta^{\sigma-1} = \xi_\sigma^p$. We put $\beta_i = t_i(\beta)$ and $\gamma = \prod \beta_i^{c_i}$, where c_i are rational integers. Then γ becomes a p-th power of a number in K, if and only if all c_i are divisible by p. Now let L be a field generated over K by adjoining all numbers $\sqrt[p]{\beta_i}$, $i = 1, \dots, r$. The extension L is normal over k and abelian over K with the Galois group H_0, which is abelian of type $(p, \dots, p)$ and of rank r. H_0 has a basis $h_1, \dots, h_r$, where h_i induces the automorphism $\sqrt[p]{\beta_i} \to \zeta\sqrt[p]{\beta_i}$ and makes invariant all $\sqrt[p]{\beta_j}$ for $j \neq i$. If $ut_i = t_{i(u)}\varphi$ for $u \in G$ with $\varphi \in S$, we choose the automorphism g_u of L/k with

$$\sqrt[p]{\beta_i} \to t_{i(u)}(\xi_\varphi)\sqrt[p]{\beta_{i(u)}}.$$

Then we can readily see that it holds $g_u h_i g_u^{-1} = h_{i(u)}$ and hence H_0 yields the representation Λ_0. Also it is easily verified that we obtain $g_\sigma g_\tau = A(\sigma, \tau) g_{\sigma\tau}$, where $A(\sigma, \tau)$ is a product of $a(t_i^{-1}\sigma t_i, t_i^{-1}\tau t_i)$-th powers of h_i, $i = 1, \dots, r$. Therefore the Galois group of L over k is the regular extension of H_0 by G with the fundamental component $a(\sigma, \tau)$. The imbedding is now possible for every irreducible extension referred to $a(\sigma, \tau)$ by Galois theory and theorem 3.

COROLLARY. *If the order of G is prime to p and k contains a primitive p-th root ζ of unity, then the imbedding of K is possible for every irreducible extension of H by G.*

The case, where a p-Sylow subgroup of G is not invariant, is rather complicated and seems difficult to obtain a simple condition, under which the imbedding is possible.

REFERENCES

[1] R. Brauer, Über die Konstruktion der Schiefkörper, die von endlichem Rang in bezug auf ein gegebenes Zentrum sind. J. reine angew. Math. **168** (1932).

[2] H. Reichardt, Konstruktion von Zahlkörpern mit gegebener Galoisgruppe von Primzahlpotenzordnung. J. reine angew. Math. **177** (1937).

[3] H. Richter, Über die Lösbarkeit einiger nicht-abelscher Einbettungsprobleme, Math. Ann. **112** (1936).

[4] A. Scholz, Über die Bildung algebraischer Zahlkörper mit auflösbarer Galoisscher Gruppe, Math. Z. **30** (1929).

[5] A. Scholz, Reduktion der Konstruktion von Körpern mit zweistufiger metabelscher Gruppe, Heidelberger Akad. Sitzungsber. (1929).

[6] A. Scholz, Konstruktion algebraischer Zahlkörper beliebiger Gruppe von Primzahlpotenzordnung I, Math. Z. **42** (1937).

[7] T. Tannaka, Über die Konstruktion der galoischen Körper mit vorgegebener p-Gruppe, Tôhoku Math. J. **43** (1937).

[8] H. Zassenhaus, Lehrbuch der Gruppentheorie.

Mathematical Institute,
Ochanomizu University