36. On the Normal Basis Theorem of the Galois Theory for Finite Factors

By Zirô TAKEDA
Ibaraki University

(Comm. by K. KUNUGI, M.J.A., March 13, 1961)

This paper is a continuation of [3], [4] and [5]. In these preceding papers we have shown that the fundamental principles of the Galois theory remain true for finite factors as same as for rings with minimum condition. In this paper we shall show the existence of a normal basis for a Galois extension of a finite factor and a theorem concerning to normal subgroups of a Galois group corresponding to the well-known theorems of the classical theory.

1. Employing the terminology of J. Dixmier [1], we denote by A a continuous finite factor standardly acting on a separable Hilbert space H and by G a finite group of outer automorphisms of A. Then G permits a unitary representation $\{u_g\}$ on H such that $x^g=u_g^*xu_g$ for $x\in A$.[1] Putting $x'^g=u_g^*x'u_g$ for $x'\in A'$, every $g\in G$ $(g\neq 1)$ induces an outer automorphism to the commutor A' of A. Hence G may be considered as a group of outer automorphisms of A' as well as of A (cf. [4]). We put B and $\hat{B}$ the subfactors of A and A' consisting of all invariant elements by G respectively.

Next we construct the crossed product $G\otimes A$ of the factor A by the group G (cf. [2]). By the outer property of G, $G\otimes A$ is a finite factor. To say more precisely, let us denote by $G\otimes H$ the Hilbert space of all functions defined on G taking values in H. Let $\sum_g g\otimes\varphi_g$ be a function belonging to $G\otimes H$ which takes value $\varphi_g\in H$ at $g\in G$, then every $a\in A$ and $g_0\in G$ defines an operator a^* and g_0^* on $G\otimes H$ such that

$$(\sum_g g\otimes\varphi_g)a^*=\sum_g g\otimes\varphi_g a,\quad (\sum_g g\otimes\varphi_g)g_0^*=\sum_g gg_0\otimes\varphi u_{g_0}$$

respectively. The crossed product $G\otimes A$ can be understand as a von Neumann algebra generated by $\{a^*, g_0^* \mid a\in A, g_0\in G\}$. We put $A^*=\{a^* \mid a\in A\}$, then by the construction of the Hilbert space $G\otimes H$ and the definition of a^*, we can easily understand that A^* is an n-fold copy of A acting on H. Since the order n of G is finite, both A^* and its commutor $A^{*\prime}$ are finite factors.

As discussed in [4], there exists a subspace K of $G\otimes H$ invariant by $G\otimes A$, on which the restriction of $G\otimes A$ is unitarily isomorphic to $\hat{B}'$ acting on H. In fact, let $1^g\in H$ be a trace element of A sat-

1) x^g is the image of x due to an automorphism g.

isfying $1^{\varrho}u_g=1^{\varrho}$ for every $g\in G$,[2] then $\xi=\sum_g g\otimes 1^{\varrho}/\sqrt{n}\in G\otimes H$ is a trace element of A and the subspace K spanned by $\{\xi a^{\#}\mid a\in A\}$ has the desired property (cf. [4: Lemma 6]).

LEMMA 1. *K has the relative dimension $1/n$ with respect to $(G\otimes A)'$.*

Proof. Since the subspace K reduces every element of $G\otimes A$, it belongs to $(G\otimes A)'$ and also to $A^{\#\prime}$. Hence the relative dimension of K with respect to $(G\otimes A)'$ is equal to that of K with respect to $A^{\#\prime}$. On the other hand K and $1\otimes H$[3] are subspaces of $G\otimes H$ spanned by $\{\xi a^{\#}\}$ and $\{(1\otimes 1^{\varrho})a^{\#}\}$[4] respectively, where ξ and $1\otimes 1^{\varrho}$ are trace elements of $A^{\#}$. Hence they are mutually equivalent with respect to $A^{\#\prime}$ and so they have the same relative dimension. Since $A^{\#}$ acting on $G\otimes H$ is an n-fold copy of A standardly acting on H, $1\otimes H$ has the relative dimension $1/n$ with respect to $A^{\#\prime}$. Hence the relative dimension of K with respect to $(G\otimes A)'$ is $1/n$ too.

We denote by $B^{\#}$ and $G\otimes B$ the subalgebras of $G\otimes A$ generated by $\{b^{\#}\mid b\in B\}$ and $\{b^{\#}, g_0^{\#}\mid b\in B, g_0\in G\}$ respectively. Then clearly $G\otimes A\supset G\otimes B\supset B^{\#}$ and so $(G\otimes A)'\subset(G\otimes B)'\subset B^{\#\prime}$. Because $B^{\#}$ is an n-fold copy of the finite factor B acting on H, both $B^{\#}$ and its commutor $B^{\#\prime}$ are finite factors. Hence the relative dimension of K with respect to $(G\otimes B)'$ is meaningful and is equal to $1/n$. On the other hand, let B^{ϱ} be a subspace of H spanned by $\{1^{\varrho}b\mid b\in B\}$. Clearly B^{ϱ} is invariant by B and, as we have shown in [5: Lemma 1], its relative dimension with respect to B' is $1/n$. Now we denote by $G\otimes B^{\varrho}$ the subspace of $G\otimes H$ spanned by functions $\sum_g g\otimes\varphi_g$ satisfying $\varphi_g\in B^{\varrho}$. $G\otimes B^{\varrho}$ is invariant by $G\otimes B$ and it has the relative dimension $1/n$ with respect to $(G\otimes B)'$. Thus $G\otimes B^{\varrho}$ and K has the same relative dimension with respect to $(G\otimes B)'$, hence there is a partial isometric operator q in $(G\otimes B)'$ having the initial domain $G\otimes B^{\varrho}$ and the range K.

Now $1\otimes 1^{\varrho}, g\otimes 1^{\varrho}, \cdots, k\otimes 1^{\varrho}$ are trace elements of $B^{\#}$ belonging to $G\otimes B^{\varrho}$ and satisfying $(1\otimes 1^{\varrho})g^{\#}=g\otimes 1^{\varrho}$ for every $g\in G$. Let $[(g\otimes 1^{\varrho})B^{\#}]$ be the subspace of $G\otimes H$ spanned by $\{(g\otimes 1^{\varrho})b^{\#}\mid b\in B\}$. Then $G\otimes B^{\varrho}$ are the direct sum of such spaces, that is,

(1) $\quad G\otimes B^{\varrho}=[(1\otimes 1^{\varrho})B^{\#}]\oplus[(g\otimes 1^{\varrho})B^{\#}]\oplus\cdots\oplus[(k\otimes 1^{\varrho})B^{\#}]$.

We put $\psi=(1\otimes 1^{\varrho})q$ and $\psi^{\varrho}=(g\otimes 1^{\varrho})q$, then ψ and ψ^{ϱ} are elements in K and we get

(2) $\quad \psi^{\varrho}=(g\otimes 1^{\varrho})q=(1\otimes 1^{\varrho})g^{\#}q=(1\otimes 1^{\varrho})qg^{\#}=\psi g^{\#}$.

---

2) Cf. [4:§1] and [5:§2].

3) $1\otimes H$ is the subspace of $G\otimes H$ consisting of functions such that $\varphi_g=0$ for every $g\neq 1$.

4) By $h\otimes 1^{\varrho}$ we mean the function belonging to $G\otimes H$ such that $\varphi_h=1^{\varrho}$ and $\varphi_g=0$ if $g\neq h$.

Hence $\psi, \psi^g, \cdots, \psi^k$ are trace elements of $B^\#$ contained in K and, corresponding to (1), K decomposes into mutually orthogonal subspaces such as

$$K=[\psi B^\#]\oplus[\psi^g B^\#]\oplus\cdots\oplus[\psi^k B^\#]. \tag{3}$$

2. We put $\varphi^g=\varphi u_g$ for $\varphi\in H$, then we get

LEMMA 2. *There exists a trace element $\varphi\in H$ of B which satisfies*

$$H=[\varphi B]\oplus[\varphi^g B]\oplus\cdots\oplus[\varphi^k B].$$

Proof. Let u be a unitary isomorphism between H and K which gives the spatial isomorphism of $\hat{B}'$ acting on H and $G\otimes A$ acting on K. Then especially we get $ua^\#u^*=a$, $ug_0^\#u^*=u_{g_0}$. Hence, putting $\varphi=\psi u^*$, we get $\varphi^g=\varphi u_g=\varphi u g^\# u^*=\psi^g u^*$. Then, corresponding to (3), H decomposes into

$$H=[\varphi B]\oplus[\varphi^g B]\oplus\cdots\oplus[\varphi^k B]. \tag{4}$$

Since ψ^g is a trace element of $B^\#$, φ^g is a trace element of B.

q.e.d.

LEMMA 3. *There is an element $a\in A$ such that $\varphi=a^\varphi$, that is,*

$$H=[a^\varphi B]\oplus[a^{g\varphi}B]\oplus\cdots\oplus[a^{k\varphi}B],$$

where $a^\varphi=1^\varphi a$ for each $a\in A$.

Proof. Putting $(1^\varphi b)v=\varphi b$ for $b\in B$ and $\eta v=0$ for $\eta\in B^{\varphi\perp}$, we get a partially isometric operator v. Clearly v belongs to the commutor B' of B. Hence it permits an expression such that $v=a_1'+u_g a_g'+\cdots+u_k a_k'$ where $a_1', \cdots, a_k'$ are elements of A' (cf. [3: Lemma 4]). Hence

$$\varphi=1^\varphi(a_1'+u_g a_g'+\cdots+u_k a_k')=1^\varphi(a_1'+a_g'+\cdots+a_k')$$

because $1^\varphi u_g=1^\varphi$. By the assumption, A and A' act standardly on H, whence for every $a_g'\in A'$ there exists $a_g\in A$ such that $1^\varphi a_g'=1^\varphi a_g$. Put $a=a_1+\cdots+a_k$, then $a\in A$ and we get $\varphi=1^\varphi(a_1+a_g+\cdots+a_k)=1^\varphi a=a^\varphi$ and so $\varphi^g=a^\varphi u_g=a^{g\varphi}$. q.e.d.

The following theorem corresponds to the so-called normal basis theorem in the classical Galois theory for Noetherian rings (cf. [6]).

THEOREM 1. *Let B be a subfactor of a continuous finite factor A consisting of all invariant elements by a finite group G of outer automorphisms of A, then there exists $a\in A$, by which every $x\in A$ is expressed as*

$$x=ab_1+a^g b_g+\cdots+a^k b_k$$

where $b_1, b_g, \cdots, b_k$ are elements of B.

Proof. We show by $\div$ the conditional expectation of A conditioned by B (cf. [7]). Let $a\in A$ be an element shown in Lemma 3 and put $b_1=(a^*x)^\div$ for $x\in A$, then for every $b\in B$ we get

$$\langle a^\varphi b_1 \mid a^\varphi b\rangle=\tau(bb_1^*)=\tau(b(x^*a)^\div)=\tau(bx^*a)=\tau(abx^*)=\langle x^\varphi \mid a^\varphi b\rangle,$$

where τ means the standard trace of A. This implies that $a^\varphi b_1$ is the projection of x^φ onto the subspace $[a^\varphi B]$. Similarly, put $b_g=(a^{g*}x)^\div$, then $a^{g\varphi}b_g$ is the projection of x^φ to the subspace $[a^{g\varphi}B]$. Hence by Lemma 3 we know

$$x^g=a^gb_1+a^{gg}b_g+\cdots+a^{kg}b_k=(ab_1+a^gb_g+\cdots+a^kb_k)^g.$$

Since the mapping $x\to x^g$ from A into H is one-to-one, we get

$$x=ab_1+a^gb_g+\cdots+a^kb_k. \qquad \text{q.e.d.}$$

3. As same as in § 2, we denote by A a Galois extension of a finite factor B having a Galois group G. Let C be an intermediate subfactor between A and B. Then by the fundamental theorem [3: Theorem 2], A is a Galois extension of C and its Galois group F is a subgroup of G. Now let σ be an isomorphism of C into A fixing every element of B, then by the extension theorem [4], σ can be extended to an automorphism g of A belonging to G. As easily seen, the isomorphic image C^g is an intermediate subfactor between A and B, and $g^{-1}Fg$ is its corresponding Galois group.

LEMMA 4. *If F is a normal subgroup of G, then C is the Galois extension of B having the Galois group isomorphic to G/F.*

Proof. Let C^g be the image of C by g, then the corresponding Galois group of C^g is $g^{-1}Fg$. Since F is normal, $g^{-1}Fg=F$, whence we know $C^g=C$. This implies that every $g\in G$ induces an automorphism of C fixing every element of B. Clearly the induced automorphisms are identity if and only if $g\in F$. Hence the group of automorphisms of C introduced by G is isomorphic to G/F. This group of automorphisms of C is outer. Otherwise it contains a non-identity inner automorphisms σ. Hence there is a unitary element $u\in C$ such that $x^\sigma=u^*xu$ for $x\in C$. Especially for $b\in B$, $b=u^*bu$. That is, $u\in B'$. Thus $u\in C\frown B'\subset A\frown B'$. This is impossible since $A\frown B'$ is the multiples of the identity by [4: Corollary 1].

LEMMA 5. *If C is a Galois extension of B, the group F corresponding to C is a normal subgroup of G.*

Proof. We denote by $\mathfrak{S}$ the Galois group corresponding to the extension C of B. By the extension theorem every $\sigma\in\mathfrak{S}$ can be extended to an automorphism g belonging to G. We put $\mathfrak{G}$ the set of all such possible extensions. If g_1, $g_2\in\mathfrak{G}$, then g_1g_2 and g_1^{-1} induce automorphisms of C belonging to $\mathfrak{S}$, whence $\mathfrak{G}$ is a subgroup of G. Clearly $F\subset\mathfrak{G}$. Hence the elements of A fixed by $\mathfrak{G}$ are included in C. Since $\mathfrak{S}$ is the Galois group of the extension C of B, the set of invariant elements of C by $\mathfrak{S}$ is B itself. Hence the invariant elements of A by $\mathfrak{G}$ coincide with B. This means $\mathfrak{G}=G$. Thus we know that every $g\in G$ induces an automorphism of C. $C^g=C$ implies $g^{-1}Fg=F$. Thus we get the desired conclusion.

By Lemmas 4 and 5 we get

THEOREM 2. *Let A be a Galois extension of a finite factor B, and let C be an intermediate subfactor between A and B. Denote by G and F Galois groups corresponding to A and C respectively. Then C is a Galois extension of B if and only if F is a normal*

subgroup of G; if this is the case, C has a Galois group isomorphic to G/F.

References

[1] J. Dixmier: Les Algèbres d'Opérateurs dans l'Espace Hilbertien, Paris (1957).
[2] M. Nakamura and Z. Takeda: On some elementary properties of the crossed products of von Neumann algebras, Proc. Japan Acad., **34**, 489–494 (1958).
[3] M. Nakamura and Z. Takeda: A Galois theory for finite factors, Proc. Japan Acad., **36**, 258–260 (1960).
[4] M. Nakamura and Z. Takeda: On the fundamental theorem of the Galois theory for finite factors, Proc. Japan Acad., **36**, 313–318 (1960).
[5] Z. Takeda: On the extension theorem of the Galois theory for finite factors, Proc. Japan Acad., **37**, 78–82 (1961).
[6] T. Nakayama: Galois theory for general rings with minimum condition, Jour. Math. Soc. Japan, **1**, 203–216 (1949).
[7] H. Umegaki: Conditional expectation in an operator algebra, Tôhoku Math. Jour., **6**, 177–181 (1954).