Note on H-separable Galois extension

Kozo Sugano

Series ♯181. February 1993

HOKKAIDO UNIVERSITY
PREPRINT SERIES IN MATHEMATICS

♯ 153: Y. Watatani, Lattices of intermediate subfactors, 33 pages. 1992.

♯ 154: T. Ozawa, On critical cases of Sobolev inequalities, 11 pages. 1992.

♯ 155: M. Ohnuma, M. Sato, Singular degenerate parabolic equations with applications to geometric evolutions, 20 pages. 1992.

♯ 156: S. Izumiya, Perestroikas of optical wave fronts and graphlike Legendrian unfoldings, 13 pages. 1992.

♯ 157: A. Arai, Momentum operators with gauge potentials, local quantization of magnetic flux, and representation of canonical commutation relations, 11 pages. 1992.

♯ 158: S. Izumiya, W.L. Marar, The Euler number of a topologically stable singular surface in a 3-manifold, 11 pages. 1992.

♯ 159: T. Hibi, Cohen-Macaulay types of Cohen-Macaulay complexes, 26 pages. 1992.

♯ 160: A. Arai, Properties of the Dirac-Weyl operator with a strongly singular gauge potential, 26 pages. 1992.

♯ 161: A. Arai, Dirac operators in Boson-Fermion Fock spaces and supersymmetric quantum field theory, 30 pages. 1992.

♯ 162: S. Albeverio, K. Iwata, T. Kolsrud, Random parallel transport on surfaces of finite type, and relations to homotopy, 8 pages. 1992.

♯ 163: S. Albeverio, K. Iwata, T. Kolsrud, Moments of random fields over a family of elliptic curves, and modular forms, 9 pages. 1992.

♯ 164: Y. Giga, M. Sato, Neumann problem for singular degenerate parabolic equations, 12 pages. 1992.

♯ 165: J. Wierzbicki, Y. Watatani, Commuting squares and relative entropy for two subfactors, 18 pages. 1992.

♯ 166: Y. Okabe, A new algorithm driven from the view-point of the fluctuation-dissipation theorem in the theory of KM_2O-Langevin equations, 13 pages. 1992.

♯ 167: Y. Okabe, H. Mano and Y. Itoh, Random collision model for interacting populations of two species and its strong law of large numbers, 14 pages. 1992.

♯ 168: A. Inoue, On the equations of stationary precesses with divergent diffusion coefficients, 25 pages. 1992.

♯ 169: T. Ozawa, Remarks on quadratic nonlinear Schrödinger equations, 19 pages. 1992.

♯ 170: T. Fukui, Y. Giga, Motion of a graph by nonsmooth weighted curvature, 11 pages. 1992.

♯ 171: J. Inoue, T. Nakazi, Finite dimensional solution sets of extremal problems in H^1, 10 pages. 1992.

♯ 172: S. Izumiya, A characterization of complete integrability for partial differential equations of first order, 6 pages. 1992.

♯ 173: T. Suwa, Unfoldings of codimension one complex analytic foliation singularities, 49 pages. 1992.

♯ 174: T. Ozawa, Wave propagation in even dimensional spaces, 15 pages. 1992.

♯ 175: S. Izumiya, Systems of Clairaut type, 7 pages. 1992.

♯ 176: A. Hoshiga, The initial value problems for quasi-linear wave equations in two space dimensions with small data, 25 pages. 1992.

♯ 177: K. Sugano, On bicommutators of modules over H-separable extension rings III, 9 pages. 1993.

♯ 178: T. Nakazi, Toeplitz operators and weighted norm inequalities, 17 pages. 1993.

♯ 179: O. Ogurisu, Existence and structure of infinitely degenerate zero-energy ground states of a Wess-Zumino type model in supersymmetric quantum mechanics, 26 pages. 1993.

♯ 180: O. Ogurisu, Ground state of a spin 1/2 charged particle in an even dimensional magnetic field, 9 pages. 1993.

Note on H-separable Galois extension

Kozo Sugano

Throughout this paper A is a ring with the identity 1, B is a subring of A containing 1, C is the center of A and $D = V_A(B)$, the centralizer of B in A. We will denote the group of ring automorphisms of A which fix all elements of B by $\mathrm{Aut}(A/B)$. In addition when we write $\{A/B, S/T\}$ we always mean that S is a ring containing A as a subring with the common identity, and T is a subring of S containing B. In this case we denote the center of S and the centralizer of T in S by $\tilde{C}$ and $\tilde{D}$, respectively. In this paper we will use the same notation as the author's previous papers [9] and [10]. In particular we say that $\{A/B, S/T\}$ satisfy the centralizer property in the case where $V_S(A) = \tilde{C}$ and $V_S(B) = \tilde{D}$. As for the definition and the fundamental properties of the H-separable extension of a non-commutative ring see [1] and [4]. The aim of this paper is to show that, if A is an H-separable Galois extension of B relative to a group G, A^* is also an H-separable Galois extension of B^* relative to the same group G, where $A^* = \mathrm{Bic}({}_AM)$ and $B^* = \mathrm{Bic}({}_BM)$ with M an arbitrary left A-module. In this case $\{A^*/A, B^*/B\}$ satisfy the centralizer property (See [8]). Therefore we will consider the general case where $\{A/B, S/T\}$ satisfy the centralizer property. To begin with we have

Proposition 1. Let $\{A/B, S/T\}$ satisfy the centralizer property, and assumme that A is an H-separable extension of B, and $S = AT = TA$. Then for each σ in $\mathrm{Aut}(A/B)$ there exists the unique ring endomorphism $\tilde{\sigma}$ of S such that $\tilde{\sigma} \mid A = \sigma$ and $\tilde{\sigma} \mid T = 1_T$. If furthermore S is an H-separable extension of T, then $\tilde{\sigma} \in \mathrm{Aut}(S/T)$.

Proof. Since $\sigma \in \mathrm{End}({}_BA_B) \cong D\otimes_C D$, there exists $\Sigma u_i \otimes v_i \in D\otimes_C D$ such that $\sigma(a) = \Sigma u_i a v_i$ for each $a \in A$. On the other hand by Theorem 1 (2) [10] we have $\tilde{D} = D\tilde{C} = D\otimes_C \tilde{C}$. Therefore if we define $\tilde{\sigma}$ by $\tilde{\sigma}(s) = \Sigma u_i s v_i$ for any $s \in S$, $\tilde{\sigma}$ is a T-T-endomorphism of S. If there exists another $\tilde{f} \in \mathrm{End}({}_TS_T)$ such that $\tilde{f} \mid A = \tilde{\sigma} \mid A = \sigma$, then $(\tilde{\sigma} - \tilde{f})(S) = (\tilde{\sigma} - \tilde{f})(TS) =$

$T(\tilde{\sigma} - \tilde{f})(A) = 0$, and we have $\tilde{\sigma} = \tilde{f}$. Thus such $\tilde{\sigma}$ exists uniquely. We will show that $\tilde{\sigma}$ is a ring endomorphism. First let $a \varepsilon A$, and define the map ϕ by $\phi(x) = \tilde{\sigma}(ax) - \tilde{\sigma}(a)\tilde{\sigma}(x)$. Obviously ϕ is a right T-endomorphism of S with $\phi(A) = 0$. Then $\phi(S) = \phi(AT) = \phi(A)T = 0$, which means that $\tilde{\sigma}(ax) = \tilde{\sigma}(a)\tilde{\sigma}(x)$ for each $a \varepsilon A$ and $x \varepsilon S$. Next let $s \varepsilon S$, and define the map ϕ by $\phi(x) = \tilde{\sigma}(xs) - \tilde{\sigma}(x)\tilde{\sigma}(s)$ for each $x \varepsilon S$. Then $\phi \varepsilon \mathrm{End}({}_T S)$, and we have $\phi(A) = 0$, since $\tilde{\sigma}(as) = \tilde{\sigma}(a)\tilde{\sigma}(s)$ for each $a \varepsilon A$ by the above argument. Then we have $\phi(S) = \phi(TS) = T\phi(A) = 0$, which means that $\tilde{\sigma}(xs) = \tilde{\sigma}(x)\tilde{\sigma}(s)$ for each s, $x \varepsilon S$. Thus $\tilde{\sigma}$ is a ring endomorphism of S. That $\tilde{\sigma} \mid T = 1_T$ is obvious. If S is an H-separable extension of T, then by Theorem 1 [6] we have that $\tilde{\sigma} \varepsilon \mathrm{Aut}(S/T)$.

Theorem 1. Let {A/B, S/T} satisfy the centralizer propety, and assume that A is a left projective H-separable extension of B. If furthermore B is a left B-direct summand of A, or A is right B-projective, then each $\sigma \varepsilon \mathrm{Aut}(A/B)$ is extended to a $\tilde{\sigma} \varepsilon \mathrm{Aut}(S/T)$ uniquely.

Proof. By our assumption and Theorems 1, 2 and 3 [9] S is an H-separable extenios of B, and we have S = AT= TA. Therefore we have the assertion by Theorem 1.

For each $\tilde{\sigma} \varepsilon \mathrm{Aut}(S/T)$ and $\sigma \varepsilon \mathrm{Aut}(A/B)$ we will write

$\tilde{J}_{\tilde{\sigma}} = \{s \varepsilon S : xs = s\sigma(x) \text{ for any } x \varepsilon S\}$

$K_{\tilde{\sigma}} = \{s \varepsilon S : xs = s\sigma(x) \text{ for any } x \varepsilon A\}$

$J_{\sigma} = \{a \varepsilon A : xa = a\sigma(x) \text{ for any } x \varepsilon A\}$

Proposition 2. Let {A/B, S/T} satisfy the centralizer property, and assume that S and T are H-separable extensions of T and B, respectively. Let $\tilde{\sigma} \varepsilon \mathrm{Aut}(S/T)$ such that $\tilde{\sigma}(A) \subset A$, and denote $\sigma = \tilde{\sigma} \mid A$. Then $\sigma \varepsilon \mathrm{Aut}(A/B)$, and we have $\tilde{J}_{\tilde{\sigma}} = K_{\tilde{\sigma}}$, and $J_{\sigma} \otimes_C \tilde{C} = \tilde{J}_{\tilde{\sigma}}$ via $a \otimes \tilde{c} \longrightarrow a\tilde{c}$ for $a \varepsilon J_{\sigma}$, $\tilde{c} \varepsilon \tilde{C}$. Consequently, $\tilde{J}_{\tilde{\sigma}} = J_{\sigma}\tilde{C}$.

Proof. Since $A \cap T \supset B$ by the definition, we have $\tilde{\sigma} \mid B = 1_B$. Then by Theorem 1 [6] we have $\sigma \varepsilon \mathrm{Aut}(A/B)$. It is obvious that $K_{\tilde{\sigma}} \supset \tilde{J}_{\tilde{\sigma}}$ and $K_{\tilde{\sigma}} \supset \tilde{J}_{\tilde{\sigma}}$. Let S_{σ} be the S-S-module shch that $S_{\sigma} = S$ as left S-module and the right S-module structure is defined by $s \cdot x = s\sigma(x)$ for $s \in S_\sigma$, $x \in S$. Then since S and A are H-separable over T and B, respectively, for an S-S and A-A-module S_σ we have the isomorphisms $(S_\sigma)^S \otimes_C \widetilde{D} = (S_\sigma)^T$ via $s \otimes \tilde{d} \longrightarrow s\tilde{d}$ for $s \in (S_\sigma)^S$, $\tilde{d} \in \widetilde{D}$ and $(S_\sigma)^A \otimes_C D \cong (S_\sigma)^B$ defined in the same way. But we have $(S_\sigma)^S = \widetilde{J}_{\tilde\sigma}$, $(S_\sigma)^A = K_{\tilde\sigma}$ and $(S_\sigma)^B = V_S(B) = V_S(T) = (S_\sigma)^T = \widetilde{D}$, while $\widetilde{D} = D \otimes_C \widetilde{C}$. Thus we have $\widetilde{D} = D \otimes_C \widetilde{J}_{\tilde\sigma}$ and $\widetilde{D} = D \otimes_C K_{\tilde\sigma}$ with $K_{\tilde\sigma} \supset \widetilde{J}_{\tilde\sigma}$. Then $D \otimes_C (K_{\tilde\sigma}/\widetilde{J}_{\tilde\sigma}) = 0$, and we have $K_{\tilde\sigma} = \widetilde{J}_{\tilde\sigma}$, since C is a C-direct summand of D. Now we have $\widetilde{J}_{\tilde\sigma} \supset J_\sigma$. Then we can define the map g of $J_\sigma \otimes_C \widetilde{C}$ to $\widetilde{J}_{\tilde\sigma}$ by $g(a \otimes \tilde{c}) = a\tilde{c}$ for $a \in J_\sigma$, $\tilde{c} \in \widetilde{C}$, while $D \otimes_C J_\sigma = D \otimes_C (A_\sigma)^A \cong (A_\sigma)^B = D$ for the same reason as above, where A_σ is defined is the same way as S_σ. Then $D \otimes_C J_\sigma \otimes_C \widetilde{C} = D \otimes_C \widetilde{C} = \widetilde{D}$, and those maps yield the following commutative diagram

$$\begin{tikzcd}
0 \arrow[r] & D \otimes_C (\mathrm{Ker}\, g) \arrow[r] & D \otimes_C (J_\sigma \otimes_C \widetilde{C}) \arrow[r] \arrow[d] & D \otimes_C \widetilde{J}_{\tilde\sigma} \arrow[r] \arrow[d] & D \otimes_C (\widetilde{J}_{\tilde\sigma}/J_\sigma \widetilde{C}) \arrow[r] & 0 \\
 & & \widetilde{D} \arrow[r, "1_{\widetilde{D}}"] & \widetilde{D} & &
\end{tikzcd}$$

where all the column maps are isomorphisms. Then $D \otimes_C (\mathrm{Ker}\, g) = D \otimes_C (\widetilde{J}_{\tilde\sigma}/J_\sigma \widetilde{C}) = 0$, and we have $\mathrm{Ker}\, g = \widetilde{J}_{\tilde\sigma}/J_\sigma \widetilde{C} = 0$. Thus g is an isomorphism.

Let G be a finite subgroup of Aut(A/B), and write $A^G = \{a \in A : \sigma(a) = a$ for each $\sigma \in G\}$. A is said to be a Galois extension of B relative to G, or a G-Galois extension of B, in the case where $B = A^G$ and there exist finite x_i, $y_i \in A$ such that $\Sigma x_i \sigma(y_i) = \delta_{1\sigma}$. If A is a G-Galois extension of B, A is both left and right B-finitely generated projecive, and we have $D = \Sigma \oplus_{\sigma \in G} J_\sigma$ (direct sum) (See [2]). The structure of H-separable Galois extension was researched in [6] and [7] by the same author. Now we have our main theorem

Theorem 2. Let {A/B, S/T} satisfy the centralizer property, and assume that A is an H-separable extension of B. If furthermore A is a Galois extension of B relative to G, then S is an H-separable Galois extension of T relative to the same Galois group G.

Proof. Since A is left and right B-finitely generated projective,

S is a left (as well as right) projective H-separable extension of T by Theorem 1 [10], and each $\sigma \in G$ is extended to a $\tilde{\sigma} \in \mathrm{Aut}(S/T)$ uniquely by Theorem 1. The set $\{\tilde{\sigma} : \sigma \in G\}$ is a group by the uniqueness of the extension of each σ. We can identify this set with G. It is obvious that S is a G-Galois extension of $R = S^G$. On the other hand by Proposition 1 [2] and Proposition 2 we have $V_S(R) = \Sigma \oplus \tilde{J}_{\tilde{\sigma}} \supset \Sigma \oplus J_\sigma = D$. Then, $R \subset V_S(V_S(R)) \subset V_S(D) = T$, where the equality is due to Theorem 2 (1) [10]. Cleary, $T \subset S^G = R$. Hence we have $T = S^G$, and S is a G-Galois extension of T.

Now we will study on the problem whether D is a Galois extension of $D \cap B$, when A is an H-separable Galois extension of B. Denote the center of B by Z. Let A be an H-separable Galois extension of B relative to a subgroup G of $\mathrm{Aut}(A/B)$. Then we have $B = V_A(V_A(B))$ by Proposition 3 [6], and consequently, $Z = V_D(D)$, the center of D. It is obvious that $\sigma(D) = D$ for each $\sigma \in \mathrm{Aut}(A/B)$. Let $N = \{\sigma \in G : \sigma \mid D = 1_D\}$ and $R = A^N$. Clearly N is a normal subgroup of G, and $\sigma(R) = R$ for each $\sigma \in G$. For each $\sigma \in G$ let J_σ be the same as in Proposition 2, and let furthermore

$$J_\sigma^{\cdot} = \{r \in R : xr = r\sigma(x) \text{ for each } x \in R\}$$

$$L_\sigma = \{a \in A : xa = a\sigma(x) \text{ for each } x \in R\}$$

$$I_\sigma = \{d \in D : xd = d\sigma(x) \text{ for each } x \in D\}$$

Clearly $J_\sigma^{\cdot} \subset L_\sigma$. But for each $a \in L_\sigma$ we have $a \in D$, since $B \subset R$ and $\sigma \mid B = 1_B$. Then since $D \subset R$, we have $a \in J_\sigma^{\cdot}$ and $a \in I_\sigma$. Thus we have $J_\sigma^{\cdot} = L_\sigma \subset I_\sigma$. We have also $J_\sigma J_\tau = J_{\tau\sigma}$ and in particular $J_\sigma J_{\sigma^{-1}} = C$ for each $\sigma, \tau \in G$ by Theorem 2 [7]. On the other hand, it is well known that A is a Galois extenion of S relative to N. Then by Proposition 1 [2] and Proposition 5 [7] we have $Z \supset \Sigma \oplus_{\rho \in N} J_\rho = V_A(R)$. Since $J_\sigma J_{\sigma^{-1}} = C$ for each $\sigma \in N$ by Theorem 2 [7], we see that A is an H-separable extension of R by the same theorem. Let A_σ be the A-A-module defined in the same way as S_σ in Proposition 2. The H-separability of A over R imlies that $(A_\sigma)^A \otimes_C V_A(R) = (A_\sigma)^R$. But $(A_\sigma)^A = J_\sigma$ and $(A_\sigma)^R = L_\sigma$. Hence we have $L_\sigma = V_A(R) J_\sigma$. As is shown in the proof of Proposition 2 there exists an isomorphism g_σ of $D\otimes_C J_\sigma$ to D such that $g_\sigma(d\otimes a) = da$ for $d\in D$, $a\in J_\sigma$, while we can make D a D-D-module D_σ in the same way as Proposition 2, i.e., $xd\cdot y = xd\sigma(y)$ for $d\in D_\sigma$, $x, y\in D$. Then g_σ is a D-D-isomorphism of $D\otimes_C J_\sigma$ to D_σ, and we have $Z\otimes_C J_\sigma = (D\otimes_C J_\sigma)^D = (D_\sigma)^D = I_\sigma$, since J_σ is C-projective (See Lemma 2.1 [5]). Then we have $I_\sigma = ZJ_\sigma \supset (\Sigma\oplus_{\rho\in N} J_\rho)J_\sigma = \Sigma\oplus_{\rho\in N} J_{\sigma\rho}$. Using these facts we can prove the next theorem

Theorem 3. Let A be an H-separable Galois extension of B relative to G. With the same notation as above we have

(1) $J_\sigma^\cdot = L_\sigma = V_A(R)J_\sigma$, $Z\otimes_C J_\sigma \cong I_\sigma$ via $z\otimes a \longrightarrow za$ for $z\in Z$ and $a\in J_\sigma$, and $I_\sigma = ZJ_\sigma$, for each $\sigma\in G$.

(2) A is an H-separable Galois extension of R relative to N

(3) D is a Galois extesion of Z relative to G/N if and only if D is a separable Z-algebra and $Z = \Sigma\oplus_{\rho\in N} J_\rho$, that is, D is an Azumaya $V_A(R)$-algebra

(4) If the condition of (3) is satisfied, then R is an H-separable Galois extension of B relative to G/N, and R = DB.

Proof. We have already proved (1) and (2). Let $\{N\sigma_i\}$ be the set of cosets of N in G. Suppose that D is separable over Z and $Z = \Sigma\oplus_{\rho\in N} J_\rho$ ($= V_A(R)$). Then $I_{\sigma_i} = ZJ_{\sigma_i} = (\Sigma\oplus_{\rho\in N} J_\rho)J_{\sigma_i} = \Sigma\oplus_{\rho\in N} J_{\sigma_i\rho}$, while $D = \Sigma\oplus_{\sigma\in G} J_\sigma = \Sigma\oplus_{i,\rho\in N} J_{\sigma_i\rho} = \Sigma\oplus_i I_{\sigma_i}$. Then since D is H-separable over Z, D is a G/N-Galois extension of Z by Theorem 2 [7]. Conversely suppose that D is G/N-Galois over Z. Then D is separable over Z, and we have $D = \Sigma\oplus I_{\sigma_i} \supset \Sigma\oplus_{i,\rho\in N} J_{\sigma_i\rho} = \Sigma\oplus_{\sigma\in G} J_\sigma = D$. Then we have $Z = \Sigma\oplus_{\rho\in N} J_\rho$, since $\Sigma\oplus_{\rho\in N} J_{\sigma_i\rho} \subset I_{\sigma_i}$. Thus we have proved (3). Suppose that the condition of (3) is satisfied. Then there exist $a_j, b_j\in D$ such $\Sigma a_j\sigma_i(b_j) = \delta_{i1}$ for each i, since $\{\sigma_i\}$ is the set of the representatives of G/N. But $a_j, b_j\in R$ and G/N acts on R. Hence R is a G/N-Galois extension of $B = R^{G/N}$. For each $x\in R$ we have $x = \Sigma_j a_j \Sigma_i \sigma_i(b_j x) \in DB$. Thus we have R = DB, which is H-separable over B, since D is Z-Azumaya.

References

[1] K. Hirata: Separable extensions and centralizers of rings, Nagoya Math. J., 35 (1969), 31-45.

[2] T. Kanzaki: Note on Galois algebra over a commutative ring, Osaka J. Math., 2 (1965), 309-317.

[3] A. Rosenberg and D. Zelinsky: Automorphisms of separable algebras, Pacific J. Math., 11 (1961), 1109-1118.

[4] K. Sugano: Note on semisimple extensions and separable extensions, Osaka J. Math., 4 (1967), 265-270.

[5] K. Sugano: On projective H-separable extensions, Hokkaido Math. J., 5 (1976), 44-54.

[6] K. Sugano: Note on automorphisms in separable extension of non commutative ring, Hokkaido Math. J., 9 (1980), 268-274.

[7] K. Sugano: On a special type of Galois extensions, Hokkaido Math. J., 9 (1980), 123-128.

[8] K. Sugano: On bicommutators of modules over H-separable extension rings, Hokkaido Math. J., 20 (1991), 497-502.

[9] K. Sugano: On bicommutators of modules over H-separable extension rings II, Hokkaido Math. J., 20 (1991), 601-608

[10] K. Sugano: On bicommutators of modules over H-separable extension rings III, submitted to Hokkaido Math. J..

Hokkaido University