GALOIS EXTENSIONS AND CROSSED PRODUCTS

By

Yôichi MIYASHITA

Introduction.

In this paper we treat Galois extensions, crossed products, (projective) Frobenius extensions and separable extensions. In §1, we state a relation between Galois extensions and (generalized) crossed products. This relation is fundamental. In §2, we consider the separability of crossed products. In §3, we give a relation between Frobenius extensions and separable extensions. In §4, we give a relation between Frobenius extensions and H-separable extensions. In §5, we give several conditions that an extension ring is a finite Galois extension with a free basis of g elements, where g is the order of the automorphism group.

Throughout the present paper, all rings have identities, and modules are unitary. A subring of a ring contains the same identity. By a ring homomorphism, we always mean a ring homomorphism such that the image of 1 is 1. Let ${}_RM$ and ${}_RN$ be R-left modules. We denote by $\mathrm{Hom}_l({}_RM, {}_RN)$ (resp. $\mathrm{Hom}_r({}_RM, {}_RN)$) the module of all R-homomorphisms from M to N acting on the left (resp. right) side. Similarly we define $\mathrm{Hom}_l(M'_R, N'_R)$ and $\mathrm{Hom}_r(M'_R, N'_R)$ for R-right modules M'_R, N'_R. Let f be a mapping from a set S to a set T. For any element s in S, the image of s by f is written as $f(s)={}^fs=(s)f=s^f$, and f is written as $f=(s\to f(s))(s\in S)$, etc.

§ 1. Galois extensions and crossed products.

Let us begin with the definition of crossed products. Let $\Delta\supseteq A^*$ be rings, and G a finite group. Δ is said to be a *crossed product* of A^* with G, if there is a subset $\{u_\sigma;\ \sigma\in G\}$ of inversible elements of Δ such that $\Delta=\sum_{\sigma\in G}\oplus A^*u_\sigma$ (direct sum), $u_1=1$, $A^*u_\sigma=u_\sigma A^*$, and $A^*u_\sigma u_\tau=A^*u_{\sigma\tau}$. Evidently, the last implies that the mapping $\sigma\to A^*u_\sigma$ from G to $\{A^*u_\sigma;\ \sigma\in G\}$ is a group homomorphism. For any σ in G, the mapping $x\to u_\sigma xu_\sigma{}^{-1}$ from A^* to A^* is a ring automorphism. If we write $u_\sigma xu_\sigma{}^{-1}=\sigma(x)$, then $u_\sigma x=\sigma(x)u_\sigma$. To be easily seen, $A^*u_\sigma{}^{-1}=A^*u_\sigma{}^{-1}=u_\sigma{}^{-1}A^*=u_\sigma{}^{-1}A^*$. For σ, τ in G, $u_\sigma u_\tau=a_{\sigma,\tau}u_{\sigma\tau}$ for some $a_{\sigma,\tau}$ in A^*. Let $\sum_\rho x_\rho u_\rho$ $(x_\rho\in A^*)$ be the inverse of $a_{\sigma,\tau}$. Then $a_{\sigma,\tau}x_1=1$. For any x in A^*, $xu_\sigma u_\tau=xa_{\sigma,\tau}u_{\sigma\tau}$. On the other hand, $xu_\sigma u_\tau=u_\sigma\cdot\sigma^{-1}(x)\ u_\tau=u_\sigma u_\tau(\sigma\tau)^{-1}(x)=a_{\sigma,\tau}u_{\sigma\tau}(\sigma\tau)^{-1}(x)=a_{\sigma,\tau}xu_{\sigma\tau}$. Hence each $a_{\sigma,\tau}$ is an inversible element

of C^*, where C^* means the center of A^*. Therefore, $\sum_{\sigma\in G}\oplus C^*u_\sigma$ is a crossed product of C^* with G. $\{a_{\sigma,\tau};\ \sigma, \tau\in G\}$ is called the *factor set* of a crossed product $\Delta=(A^*, G, \{u_\sigma;\ \sigma\in G\})$.

The proof of the following lemma may be omitted.

Lemma 1.1. *Let $M\neq 0$ be a module, and R, S subrings of $T=\mathrm{End}_l(M)$ such that $\mathrm{V}_T(R)=S$ and $\mathrm{V}_T(S)=R$, where $\mathrm{End}_l(M)$ is the endomorphism ring of M acting on the left side, and $\mathrm{V}_T(R)=\{t\in T;\ rt=tr \text{ for all } r \text{ in } R\}$. If c is an inversible element of T such that $cRc^{-1}=R$, then $cSc^{-1}=S$.*

Now, let $\Delta=(A^*, G, \{u_\sigma\})$ be a crossed product, and ${}_\Delta M\sim{}_\Delta\Delta$ (cf. [7]). Then ${}_{A^*}\Delta\sim{}_{A^*}A^*$ implies that ${}_{A^*}M\sim{}_{A^*}A^*$. If we set $T=\mathrm{End}_l(M)$, $\mathrm{V}_T(\Delta)=B$ and $\mathrm{V}_T(A^*)=A$, then ${}_AM\sim{}_AA$, ${}_BM\sim{}_BB$, and B is a subring of A. Therefore ${}_BA\sim{}_BB$. For any σ in G, $\tilde{u}_\sigma$ denotes the inner automorphism $(f\to u_\sigma f u_\sigma^{-1})$ of T, where $f\in T$. Since $\tilde{u}_\sigma$ induces the automorphism $\tilde{u}_\sigma|A^*$ of A^*, $\tilde{u}_\sigma$ induces the automorphism $\tilde{u}_\sigma|A$ of A (Lemma 1.1), and G may be considered as a finite group of automorphisms of A. In this sence, $A^G=B$ holds. Moreover we have the following

Theorem 1.2. *Let $\Delta=(A^*, G, \{u_\sigma\})$ be a crossed product, ${}_\Delta M\sim{}_\Delta\Delta$, $\mathrm{End}_l({}_\Delta M)=B$ and $\mathrm{End}_l({}_{A^*}M)=A$. Then A/B is a finite G-Galois extension* (cf. [7]).

Proof. Since ${}_\Delta M|{}_\Delta\Delta$, there are $f_i\in\mathrm{Hom}({}_\Delta M, {}_\Delta\Delta)$, $m_i\in M$ such that $\sum_i {}^{f_i}m\cdot m_i=m$ for all m in M. Since ${}_\Delta\Delta|{}_\Delta M$, there are $g_k\in\mathrm{Hom}({}_\Delta M, {}_\Delta\Delta)$, $n_k\in M$ such that $\sum_k {}^{g_k}n_k=u_1$ $(=1)$. For τ in G, the mapping $\sum x_\sigma u_\sigma\to x_\tau$ from Δ to A^* is an A^*-left homomorphism. We denote this by p_τ. Evidently, $\sum_{\tau\in G}{}^{p_\tau}\delta\cdot u_\tau=\delta$ for any δ in Δ. Let $\varphi_{\tau,i,k}$ be the A^*-left homomorphism from M to M such that $\varphi_{\tau,i,k}(m)={}^{p_\tau f_i}m\cdot u_\tau n_k$ for any m in M, and let $\psi_{\tau,i,k}$ be the A^*-left homomorphism from M to M such that $\psi_{\tau,i,k}(m)={}^{p_\tau g_k}m\cdot u_\tau m_i$ for any m in M. Then, as is easily seen, $\sum_{\tau,i,k}\psi_{\tau,i,k}u_\sigma\varphi_{\tau,i,k}=\delta_{1,\sigma}$ for all σ in G, or equivalently, $\sum_{\tau,i,k}\psi_{\tau,i,k}\cdot\sigma(\varphi_{\tau,i,k})=\delta_{1,\sigma}$ for all σ in G. Thus A/B is a finite G-Galois extension.

Remark. Let c, d be inversible elements of Δ. Then, $\tilde{c}|A=\tilde{d}|A$ if and only if $cA^*=dA^*$.

Proposition 1.3. *With the same notations and assumptions as in* Th. 1.2, *the following conditions are equivalent*:

(i) $\mathrm{V}_A(B)=C$, *where C is the center of A.*

(ii) $\mathrm{V}_\Delta(A^*)=C^*$.

(iii) *For any σ in G such that $\sigma\neq 1$, $\{a\in A^*;\ \sigma(x)a=ax$ for all x in $A^*\}=\{0\}$.*

If (iii) *holds and* $\Delta=(A^*, G, \{v_\sigma\})$, *then* $u_\sigma A^*=v_\sigma A^*$ *for all* σ *in* G.

Proof. Since $V_\Delta(A^*)=V_A(B)$ and $C=C^*$, (i)$\Longleftrightarrow$(ii) is evident. For $\delta=\sum a_\sigma u_\sigma$ in Δ, $\delta\in V_\Delta(A^*)$ if and only if $xa_\sigma=a_\sigma\cdot\sigma(x)$ for all σ in G and x in A^*. Thus we have (ii)$\longleftrightarrow$(iii). If (iii) holds, then $\mathrm{Hom}({}_{A^*}A^*u_{\sigma A^*}, {}_{A^*}A^*v_{\tau A^*})=0$ for any σ, τ in G such that $\sigma\neq\tau$ (cf. [6 ; p. 127]). Thus $A^*u_\sigma\subseteq A^*v_\sigma$. Symmetrically we have $A^*v_\sigma\subseteq A^*u_\sigma$. Hence $A^*u_\sigma=A^*v_\sigma$ for all σ in G.

If a corossed product Δ satisfies the condition (ii) in Prop. 1.3, we call Δ an *outer crossed product.*

The following is well known.

Lemma 1.4. *Let* S *be a ring,* σ *an automorphism of* S, *and* ${}_SN$ *a faithful* S*-left module. If, for any* s *in* S *and* x *in* N, *we define* $s*x=\sigma(s)x$, *then we have a new* S*-left module* ${}_S(\sigma, N)$. *Then,* ${}_S(\sigma, N)\simeq{}_SN$ *if and only if* σ *can be extended an inner automorphism of* $\mathrm{End}_l(N)$.

By Lemma 1.4, ${}_A(\sigma, M)\simeq{}_AM(\sigma\in G)$ in Th. 1.2. Next we shall prove the converse of Th. 1.2. Let A/B be a finite G-Galois, ${}_AM\sim{}_AA$, and assume that each $\sigma\in G$ can be extended to an inner automorphism $\tilde{u}_\sigma$ of $\mathrm{End}_l(M)$, that is, $u_\sigma xu_\sigma^{-1}=\sigma(x)$ for all x in A. We take u_1 as $u_1=1$. Put $\Delta=\mathrm{End}_l({}_BM)$ and $A^*=\mathrm{End}_l({}_AM)$. Then A^* is a subring of Δ. Now, there are elements a_s, a_s' in A such that $\sum_s a_s\cdot\sigma(a_s')=\delta_{1,\sigma}$ for all σ in G. Then $\sum_s\tau(a_s)\sigma(a_s')=\delta_{\tau,\sigma}$ for any σ, τ in G, that is, $\sum_s u_\tau a_s u_\tau^{-1}\cdot u_\sigma a_s' u_\sigma^{-1}=\delta_{\tau,\sigma}$ for any τ, σ in G. Therefore, $\sum_s a_s u_\tau^{-1}u_\sigma a_s'=\delta_{\tau,\sigma}$ for any τ, σ in G. Assume that $0=\sum_\sigma u_\sigma x_\sigma$ $(x_\sigma\in A^*)$. Then, for any τ in G, $0=\sum_s a_s u_\tau^{-1}(\sum_\sigma u_\sigma x_\sigma)a_s'=\sum_\sigma(\sum_s a_s u_\tau^{-1}u_\sigma a_s')x_\sigma=x_\tau$. Thus we know $\Delta\supseteq\sum_{\sigma\in G}\oplus u_\sigma A^*\supseteq A^*$. For τ, σ in G, $\tau\sigma=(\tilde{u}_\tau|A)(\tilde{u}_\sigma|A)=\widetilde{u_\tau u_\sigma}|A$. On the other hand, $\tau\sigma=\tilde{u}_{\tau\sigma}|A$. Hence $u_{\tau\sigma}A^*=u_\tau u_\sigma A^*$. Since $\tilde{u}_\sigma$ induces an automorphism of A, $\tilde{u}_\sigma$ induces an automorphism of A^*, that is, $u_\sigma A^*=A^*u_\sigma$. Lastly we shall show that $\Delta\subseteq\sum_{\sigma\in G}A^*u_\sigma$. Since ${}_AM|{}_AA$, there are $f_i\in\mathrm{Hom}({}_AM, {}_AA)$ and $m_i\in M$ such that $\sum_i f_i m\cdot m_i=m$ for all $m\in M$. Since ${}_AA|{}_AM$, there are $g_k\in\mathrm{Hom}({}_AM, {}_AA)$ and $n_k\in M$ such that $\sum_k g_k n_k=1$. For any x in A, $\sum_s t_G(xa_s)a_s'=x$. For any $\delta\in\Delta$, we put $\varphi_{i,s,k}(\delta)=(x\to g_k x\cdot\delta a_s' m_i)$, where $x\in A^*$. Then $\varphi_{i,s,k}: {}_{A^*}\Delta\to{}_{A^*}A^*$. For any x in A^*, we put $\psi_{i,s,k}(x)=(m\to t_G(f_i m\cdot a_s)xn_k)$, where $m\in M$. Then $\psi_{i,s,k}: {}_{A^*}A^*\to{}_{A^*}\Delta$. To be easily seen, there holds $\sum_{i,s,k}\psi_{i,s,k}\varphi_{i,s,k}=1_\Delta$. Thus ${}_{A^*}\Delta$ is generated by $\{(m\to t_G(f_i m\cdot a_s)n_k);$ $i, s, k\}$. Further, $t_G(f_i m\cdot a_s)n_k=\sum_\sigma u_\sigma\cdot f_i m\cdot a_s u_\sigma^{-1}n_k$, and $(m\to f_i m\cdot a_s u_\sigma^{-1}n_k)$ $(m\in M)$ is in A^*. Thus we have proved that $\Delta\subseteq\sum_{\sigma\in G}\oplus A^*u_\sigma$, and hence Δ is a crossed product of A^* with G. Thus we obtain the following

Theorem 1.5. *Let* A/B *be finite* G*-Galois,* ${}_AM\sim{}_AA$, $\Delta=\mathrm{End}_l({}_BM)$, *and* $A^*=\mathrm{End}_l({}_AM)$. *Further, assume that each* σ *in* G *can be extended to*

an inner automorphism $\tilde{u}_\sigma$ *of* $End_t(M)$. *Then* $\Delta=\sum_{\sigma\in G}\oplus A^*u_\sigma=(A^*, G, \{u_\sigma\})$, *which is a caossed product of* A^* *with* G.

For inner Galois extensions we remark the following

Proposition 1.6. *With the same notations and assumptions as in* Th. 1. 5, *the following are equivalent*:

(i) A/B *is finite inner* G-*Galois* (*i.e. each* $\sigma\in G$ *is an inner automorphism of* A).

(ii) *Each* $\tilde{u}_\sigma|A^*$ *is an inner automorphism of* A^*.

(iii) *For a suitable* $\{u_\sigma; \sigma\in G\}$ *there holds that* $xu_\sigma=u_\sigma x$ *for all* x *in* A^*.

Proof. It σ is an inner automorphism of A, then $\tilde{u}_\sigma|A=\tilde{c}_\sigma|A$ for some inversible c_σ of A. Then $c_\sigma^{-1}u_\sigma\in A^*$, which is an inversible element of A^*. If we put $d_\sigma=c_\sigma^{-1}u_\sigma$, then $\tilde{d}_\sigma|A^*=\tilde{u}_\sigma|A^*$, which is an inner automorphism of A^*. Symmetrically, if $\tilde{u}_\sigma|A^*$ is inner, then so is $\tilde{u}_\sigma|A$. Thus the proof is complete.

If a crossed product Δ satisfies the condition (ii) in Prop. 1.6, we call Δ an *inner crossed product*. Thus the outer (resp. inner) corssed products and the outer (resp. inner) Galois extensions correspond to each other;

Let S, T be rings, and ${}_SM_T$. If ${}_SM\sim{}_SS$ and $End_r({}_SM)=T$, then $M_T\sim T_T$ and $End_l(M_T)=S$ (Morita). We call such a module a *Morita module*. If there is a Morita module ${}_SM_T$, then we write $S\sim T$. This is an equivalence relation (Morita).

Theorem 1.7. (1) *Let* A/B *be finite* [*outer, inner*] G-*Galois, and* $B\sim B'$. *Then there is a finite* [*outer, inner*] G-*Galois extension* A'/B' *such that* $A'\sim A$.

(2) *Let* Δ/A^* *be an* [*outer, inner*] *crossed product of* A^* *with* G, *and* $A^*\sim A^{**}$. *Then there is an* [*outer, inner*] *crossed product* Δ^*/A^{**} of A^{**} *with* G *such that* $\Delta^*\sim\Delta$.

Proof. (1) Let ${}_BM_{B'}$ be a Morita module, and $\Delta=End_l(A_B)$. Then ${}_\Delta A\otimes_B M_{B'}$ is a Morita module, and Δ/A is an crossed product of A with G. If we put $A'=End_r({}_AA\otimes_BM)$, then A'/B' is a required one. (2) Let ${}_{A^{**}}N_{A^*}$ be a Morita module, and $End_r({}_{A^*}\Delta)=A$. Then ${}_{A^{**}}N\otimes_{A^*}\Delta_A$ is a Morita module, and A/Δ is a finite [outer, inner] G-Galois extension. If we put $\Delta^*=End_l(N\otimes_{A^*}\Delta_\Delta)$, then Δ^*/A^{**} is a required one.

In the rest of this section, we remark on factor sets. Let $\Delta=(A, G, \{u_\sigma; \sigma\in G\})$ be a crossed product of A with G, $\{a_{\sigma,\tau}; \sigma, \tau\in G\}$ its factor set, and C the center of A. Then, $u_\sigma u_\tau=a_{\sigma,\tau}u_{\sigma\tau}$ and each $a_{\sigma,\tau}$ is a inversible element of C. If we write $u_\sigma a u_\sigma^{-1}=\sigma(a)$ for any $a\in A$, then σ is an automor-

phism of A, and the mapping $\varphi : \sigma \to (a \to \sigma(a))(\sigma \in G, a \in A)$ is a group homomorphism. $(u_\sigma u_\tau)u_\rho = u_\sigma(u_\tau u_\rho)$ implies that $a_{\sigma,\tau}a_{\sigma\tau,\rho} = {}^\sigma a_{\tau,\rho}a_{\sigma,\tau\rho}$ for σ, τ, ρ in G, and $a_{\sigma,1} = a_{1,\sigma} = 1$, because $u_1 = 1$. Conversely, if we give a group homomorphism from G into the automorphism group of A and a factor set $\{a_{\sigma,\tau}; \sigma, \tau \in G\}$ such that $a_{\sigma,\tau}a_{\sigma\tau,\rho} = {}^\sigma a_{\tau,\rho}a_{\sigma,\tau\rho}$ $(\sigma, \tau, \rho \in G)$ $a_{\sigma,1} = a_{1,\sigma} = 1$, then we have a crossed product.

Proposition 1.8. *Let $\Delta = \sum_{\sigma \in G} \oplus Au_\sigma$ and $\Delta' = \sum_{\sigma \in G} \oplus Av_\sigma$ be crossed products of A with G, C the center of A, and let $\{a_{\sigma,\tau}\}$ and $\{b_{\sigma,\tau}\}$ be factor sets of Δ and Δ', respectively. Then the following statements are equivalent:*

(i) *There is an A-ring isomorphism f from Δ to Δ' such that $f(Au_\sigma) = Av_\sigma$ for all σ in G.*

(ii) *For any σ in G, $u_\sigma a u_\sigma^{-1} = v_\sigma a v_\sigma^{-1}$ for all a in A, and there is a subset $\{c_\sigma; \sigma \in G\}$ of inversible elements of C such that $b_{\sigma,\tau} = c_{\sigma\tau}^{-1}c_\sigma \cdot {}^\sigma c_\tau a_{\sigma,\tau}$ for all σ, τ in G, and $c_1 = 1$.*

Proof. (i)$\Rightarrow$(ii) We may assume that $\Delta = \Delta'$. Let $v_\sigma = c_\sigma u_\sigma$. Then, for any x in A, $v_\sigma x = c_\sigma u_\sigma x = c_\sigma \cdot \sigma(x)u_\sigma$. On the other hand, $v_\sigma x = \sigma(x)v_\sigma = \sigma(x)c_\sigma u_\sigma$, and so $\sigma(x)c_\sigma = c_\sigma \cdot \sigma(x)$ for all x in A. Thus $c_\sigma \in C$ for all σ in G. The remainder is rather familiar.

Now, we fix a group homomorphism φ from G into the automorphism group of A, then the set of all factor sets with respect to φ is an abelian group $G(A, \varphi)$: $\{a_{\sigma,\tau}\}\{b_{\sigma,\tau}\} = \{c_{\sigma,\tau}\}$, where $c_{\sigma,\tau} = a_{\sigma,\tau}b_{\sigma,\tau}$. Let $\{c_\sigma; \sigma \in G\}$ be a subset of inversible elements of C such that $c_1 = 1$. If we put $d_{\sigma,\tau} = c_{\sigma\tau}^{-1}c_\sigma \cdot {}^\sigma c_\tau$ for all σ, τ in G, then $\{d_{\sigma,\tau}\}$ is a factor set, and the set of such factor sets forms a subgroup $G_0(A, \varphi)$ of $G(A, \varphi)$. Then Prop. 1.8 yields at once the following

Proposition 1.9. *Let $\Delta = \sum_{\sigma \in G} \oplus Au_\sigma$ and $\Delta' = \sum_{\sigma \in G} \oplus Av_\sigma$ be crossed products of A with G, and let $\{a_{\sigma,\tau}\}$ and $\{b_{\sigma,\tau}\}$ be factor sets of Δ and Δ', respectively. Then the following are equivalent:*

(i) *There is an A-ring isomorphism f from Δ to Δ' such that $f(Au_\sigma) = Av_\sigma$ for all σ in G.*

(ii) *For any σ in G, $u_\sigma a u_\sigma^{-1} = v_\sigma a v_\sigma^{-1}$ for all a in A, and $\{a_{\sigma,\tau}\} \equiv \{b_{\sigma,\tau}\}$* mod $G_0(A)$.

§ 2. Separability of crossed products.

Throughout this section, we assume that R/S is a (projective) Frobenius extension. Then there are h: ${}_SR_S \to {}_SS_S$, and $r_i, l_i \in R$ $(i = 1, \cdots, n)$ such that $x = \sum_i r_i \cdot h(l_i x) = \sum_i h(x r_i)l_i$ for all x in R (cf. [9]).

Lemma 2.1. *Let ${}_RM_T$ be an R-left, T-right module. Then φ: $\mathrm{Hom}_t({}_SM_T, {}_SM_T) \simeq \mathrm{Hom}_t({}_RM_T, {}_RR \otimes {}_SM_T)$, where $\varphi(f) = (m \to \sum_i r_i \otimes f(l_i m))$*

($f \in \mathrm{Hom}_t({}_SM_T, {}_SM_T)$, $m \in M$). *For any* g *in* $\mathrm{Hom}_t({}_RM_T, {}_RR\otimes_S M_T)$, $\varphi^{-1}(g) = (h\otimes 1)g$, *where* $(h\otimes 1)(r\otimes m) = h(r)m$ ($r\in R$, $m\in M$).

Proof. $\mathrm{Hom}({}_SM_T, {}_SM_T) \simeq \mathrm{Hom}({}_SR\otimes_R M_T, {}_SM_T) \simeq \mathrm{Hom}({}_RM_T, {}_R(\mathrm{Hom}({}_SR, {}_SM)_T) \simeq \mathrm{Hom}({}_RM_T, {}_R\mathrm{Hom}({}_SR, {}_SS)\otimes_S \mathrm{Hom}({}_SS, {}_SM)_T) \simeq \mathrm{Hom}({}_RM_T, {}_RR\otimes_S M_T)$. If we follow the above sequence of isomorphisms, we obtain the required isomorphism.

Corollary. *For any* ${}_RM_T$, *the following are equivalent*:

(i) *The R-T-homomorphism* $r\otimes m \to rm$ *from* $R\otimes_S M$ *to* M *splits.*

(ii) *There is a homomorphism* f *in* $\mathrm{Hom}_t({}_SM_T, {}_SM_T)$ *such that* $\sum_i r_i \cdot f(l_i m) = m$ *for all* m *in* M.

The following proposition is an easy consequence of Cor. to Lemma 2.1.

Proposition 2.2. *For an extension ring* T *of* R, *the following are equivalent*:

(i) *The R-T-homomorphism* $r\otimes t \to rt$ *from* $R\otimes_S T$ *to* T *splits.*

(ii) *There is an element* c *in* $\mathrm{V}_T(S)$ *such that* $\sum_i r_i c l_i = 1$.

In this case, the mapping $r \to \sum_i r_i \otimes c l_i r$ ($r\in R$) *is an R-T-homomorphism from* R *to* $R\otimes_S T$.

Corollary (Hirata and Sugano [2]). *The following are equivalent*:

(i) R/S *is a separable extension.*

(ii) *There is an element* c *in* $\mathrm{V}_R(S)$ *such that* $\sum_i r_i c l_i = 1$.

Proposition 2.3. *Let* $\Delta = (A, G, \{u_\sigma\})$ *be a crossed product of* A *with* G, H *a subgroup of* G, $\Delta_H = \sum_{\tau\in H}\oplus A u_\tau$, *and* $u_\sigma u_\tau = a_{\sigma,\tau}u_{\sigma\tau}$ ($\sigma, \tau \in G$). *Then* Δ/Δ_H *is a free Frobenius extension. In fact, if* $G = \sigma_1 H \cup \cdots \cup \sigma_r H$ *is the coset decomposition of* G *and* h *is the* Δ_H-Δ_H-*homomorphism from* Δ *to* Δ_H *such that* $h(\sum_{\sigma\in G} a_\sigma u_\sigma) = \sum_{\tau\in H} a_\tau u_\tau$, *then* $\delta = \sum_i h(\delta u_{\sigma_i}) a_{\sigma_i^{-1}, \sigma_i}{}^{-1} u_{\sigma_i^{-1}} = \sum_i u_{\sigma_i} \cdot h(a_{\sigma_i^{-1}, \sigma_i}{}^{-1} u_{\sigma_i^{-1}}\delta)$ *for all* δ *in* Δ.

Proof. That h is a Δ_H-Δ_H-homomorphism will be easily seen. Let $\delta = \sum_{\eta\in H}\sum_i x_{\sigma_i\eta} u_{\sigma_i\eta}$ be in Δ. Then $h(a_{\sigma_i^{-1}, \sigma_i}{}^{-1} u_{\sigma_i^{-1}}\delta) = a_{\sigma_i^{-1}, \sigma_i}{}^{-1} \cdot \sigma_i^{-1}(x_{\sigma_i\eta}) a_{\sigma_i^{-1}, \sigma_i\eta} u_\eta$. Now, $a_{\sigma,\tau}a_{\sigma\tau,\rho} = \sigma(a_{\tau,\rho})a_{\sigma,\tau\rho}$ for all σ, τ, ρ in G. If we put $\rho = \sigma$ and $\tau = \sigma^{-1}$, then $a_{\sigma,\sigma^{-1}}a_{1,\sigma} = \sigma(a_{\sigma^{-1},\sigma})a_{\sigma,1}$. Since $1 = a_{1,\sigma} = a_{\sigma,1}$, we have $a_{\sigma,\sigma^{-1}} = \sigma(a_{\sigma^{-1},\sigma})$ for all σ in G. Further we see that $a_{\sigma_i,\sigma_i^{-1}} = a_{\sigma_i,\sigma_i^{-1}}a_{1,\sigma_i\eta} = \sigma_i(a_{\sigma_i^{-1},\sigma_i\eta})a_{\sigma_i,\eta}$, where $\eta\in H$. Noting these facts we can see that $\sum_i u_{\sigma_i} \cdot h(a_{\sigma_i^{-1}, \sigma_i}{}^{-1} u_{\sigma_i^{-1}}\delta) = \delta$. Next we write δ as $\delta = \sum_{\eta\in H}\sum_j y_{\eta\sigma_j^{-1}} u_{\eta\sigma_j^{-1}}$. Then $h(\delta u_{\sigma_i}) = y_{\eta\sigma_i^{-1}} a_{\eta\sigma_i^{-1}} u_\eta$. Noting that $\eta(a_{\sigma_i^{-1},\sigma_i}) = \eta\sigma_i^{-1}(a_{\sigma_i,\sigma_i^{-1}})a_{\eta\sigma_i^{-1},1} = a_{\eta\sigma_i^{-1},\sigma_i}a_{\eta,\sigma_i^{-1}}$, we can see that $\sum_i h(\delta u_{\sigma_i}) a_{\sigma_i^{-1},\sigma_i}{}^{-1} u_{\sigma_i^{-1}} = \delta$. This completes the proof.

Corollary. *Let* $\Delta = \sum_{\sigma\in G}\oplus A u_\sigma$ *be a crossed product. Then* Δ/A *is a free Frobenius extension. In fact,* $h = (\sum_\sigma a_\sigma u_\sigma \to a_1)$ *is a Frobenius homo-*

morphism, and $\delta=\sum_{\sigma\in G}h(\delta u_\sigma)a_{\sigma^{-1},\sigma}{}^{-1}u_{\sigma^{-1}}=\sum_{\sigma\in G}u_\sigma\cdot h(a_{\sigma^{-1},\sigma}{}^{-1}u_{\sigma^{-1}}\delta)$ *for all* δ *in* Δ.

Theorem 2.4. *With the same notations and assumptions as in* Prop. 2.3, *the following statements are equivalent*:

(i) Δ/Δ_H *is a separable extension.*

(ii) *There is an element* c *in* C (=*the center of* A) *such that* $\sum_i\sigma_i(c)=1$ *and* $\tau(c)=c$ *for all* τ *in* H. (*Remark. Since* $c\in C^H$, $\sum_i\sigma_i(c)$ *is independent of the choice of* $\{\sigma_i\}$.)

Proof. By Prop. 2.3 and Cor. to Th. 2.2, (i) is equivalent to that there is a δ in $V_\Delta(\Delta_H)$ such that $\sum_i u_{\sigma_i}\delta a_{\sigma_i^{-1},\sigma_i}{}^{-1}u_{\sigma_i^{-1}}=u_1$. Now, for any $\delta=\sum_\sigma a_\sigma u_\sigma$ in $V_\Delta(\Delta_H)$, the coefficient of u_1 of $\sum_i u_{\sigma_i}\delta a_{\sigma_i^{-1},\sigma_i}{}^{-1}u_{\sigma_i^{-1}}$ is $\sum_i\sigma_i(a_1)$, and $\delta\in V_\Delta(\Delta_H)$ implies that $a_1\in C$. Since $\delta u_\tau=u_\tau\delta$ for all τ in H, we obtain that $a_\sigma a_{\sigma,\tau}=\tau(a_{\tau^{-1}\sigma\tau})a_{\tau,\tau^{-1}\sigma\tau}$ for τ in H, σ in G. Put $\sigma=1$. Then $a_1=\tau(a_1)$ for all τ in H. Thus, if $\sum_i u_{\sigma_i}\delta a_{\sigma_i^{-1},\sigma_i}{}^{-1}u_{\sigma_i^{-1}}=1$ for some δ in $V_\Delta(\Delta_H)$, then $\sum_i\sigma_i(a_1)=1$ for some a_1 in C^H. Conversely, if there is an element a_1 in C^H such that $\sum_i\sigma_i(a_1)=1$, then $a_1u_1\in V_\Delta(\Delta_H)$ and $\sum_i u_{\sigma_i}a_1u_1a_{\sigma_i^{-1},\sigma_i}{}^{-1}u_{\sigma_i^{-1}}=u_1$. Hence (i) and (ii) are equivalent.

Corollary 1. *When* $\sigma(x)=x$ *for any* $\sigma\in G$ *and any* $x\in C$, Δ/Δ_H *is separable if and only if* $(G:H)$ 1 *is inversible in* A.

Corollary 2. Δ/A *is separable if and only if* $\sum_{\sigma\in G}\sigma(c)=1$ *for some* c *in* C.

Corollary 3. *If* Δ/A *is separable then* Δ_H/A *is separable.*

Proof. If $\sum_{\sigma\in G}\sigma(c)=1$ for c in C, then $1=\sum_{\tau\in H}\tau(\sum_i\sigma_i^{-1}(c))$. By Cor. 2, Δ_H/A is separable.

Remark. As Δ_H is an Δ_H-Δ_H-direct summand of Δ, Δ is (A,Δ_H)-projective (cf. [6]) if and only if Δ_H/A is separable (cf. [7; Lemma 2.10]).

In the rest of this section, $\Omega=\sum_{\sigma\in G}\oplus Au_\sigma$ means a crossed product of A with G such that $u_\sigma u_\tau=u_{\sigma\tau}$ for any σ,τ in G. Then A may be considered an Ω-left module: $\sum_\sigma a_\sigma u_\sigma(x)=\sum_\sigma a_\sigma\cdot\sigma(x)$ for $\sum_\sigma a_\sigma u_\sigma$ in Ω and x in A.

Lemma 2.5. ${}_\Omega A$ *is* (*finitely generated and*) *projective if and only if* $\sum_{\sigma\in G}\sigma(a)=1$ *for some* a *in* A.

Proof. $\mathrm{Hom}({}_\Omega A,{}_\Omega\Omega)\subseteq\mathrm{Hom}({}_A A,{}_A\Omega)\simeq\Omega$, canonically. To be easily seen, $\mathrm{Hom}({}_\Omega A,{}_\Omega\Omega)\simeq(\sum_\sigma u_\sigma)A$ under the isomorphism. Therefore, ${}_\Omega A$ is finitely generated and projective if and only if there are $a_1,\cdots,a_n$; $b_1,\cdots,b_n$ in A such $x\sum_\sigma\sum_i\sigma(b_ia_i)=x$ for all x in A, or equivalently, $\sum_\sigma\sigma(a)=1$ for some a in A.

Remark. ${}_\Omega A\sim{}_\Omega\Omega$ if and only if A/B *is* finite G-Galois, where $B=A^G$.

Combining Lemma 2.5 with Cor. 2 to Th. 2.4, we obtain the following

Proposition 2.6. *If A is a commutative ring, then the following are equivalent*:

(i) Ω/A *is separable.*

(ii) ${}_{\Omega}A$ *is projective.*

(iii) $\sum_{\sigma\in G}\sigma(c)=1$ *for some* c *in* A.

Corollary. *If A is commutative and ${}_AA$ is completely reducible* (i.e. *A is a direct sum of fields*), *then the following are equivalent*:

(i) Ω/A *is separable.*

(ii) ${}_{\Omega}\Omega$ *is completely reducible.*

(iii) ${}_{\Omega}A$ *is projective.*

(iv) $\sum_{\sigma\in G}\sigma(c)=1$ *for some* c *in* A.

§ 3. On Frobenius extensions and separable extensions.

The proof of the following may be omitted.

Lemma 3.1. *Let M be an R-left, R^*-right module,* $\mathrm{End}_r({}_RM)=R^*$, *and* $\mathrm{End}_l(M_{R^*})=R$. *Then* $\mathrm{Hom}_l(M_{R^*}, R^*_{R^*})\simeq\mathrm{Hom}_r({}_RM, {}_RR)$ *by the correspondence* $g\mapsto(x\to(y\to x\cdot{}^gy))$, *where* $g\in\mathrm{Hom}_l(M_{R^*}, R^*_{R^*})$, $x, y\in M$. *Assume that, further,* $M_{R^*}|R^*_{R^*}$. *Then* $M\simeq\mathrm{Hom}_r({}_{R^*}\mathrm{Hom}_l(M_{R^*}, R^*_{R^*}), {}_{R^*}R^*)\simeq\mathrm{Hom}_r({}_{R^*}\mathrm{Hom}({}_RM, {}_RR), {}_{R^*}R^*)$ *by the correspondence* $x\mapsto(g\to{}^gx)\mapsto(f\to(y\to y^f\cdot x))$, *where* $x, y\in M$, $g\in\mathrm{Hom}_l(M_{R^*}, R^*_{R^*})$, $f\in\mathrm{Hom}_r({}_RM, {}_RR)$.

Lemma 3.2. *Let R/S be a Frobenius extension. Then there are* h: ${}_SR_S\to{}_SS_S$, $a_i, b_i\in R$ *such that* $x=\sum_i(xa_i)^h\cdot b_i=\sum_i a_i(b_ix)^h$ *for all* x *in* A. *Then there hold the following*:

(1) ${}_RR_S\simeq{}_R\mathrm{Hom}({}_SR, {}_SS)_S$ *by the mapping* $(x\to xh)(x\in R)$. *The inverse of this mapping is* $(g\to\sum_i a_i\cdot b_i^g)(g\in\mathrm{Hom}_r({}_SR, {}_SS))$.

(2) *For any* ${}_RM_{R^*}$, $\mathrm{Hom}_r({}_RM, {}_RR)\simeq\mathrm{Hom}_r({}_SM, {}_SS)$ *as R^*-left, Sright modules, by the mapping* $(f\to fh)(f\in\mathrm{Hom}_r({}_RM, {}_RR))$. *The inverse of this mapping is* $(g\to(x\to\sum_i a_i(b_ix)^g))$, *where* $g\in\mathrm{Hom}_r({}_SM, {}_SS)$, $x\in M$. *From this fact,* $M\simeq\mathrm{Hom}_r({}_{R^*}\mathrm{Hom}_r({}_RM, {}_RR), {}_{R^*}R^*)\simeq\mathrm{Hom}_r({}_{R^*}\mathrm{Hom}_r({}_SM, {}_SS), {}_{R^*}R^*)$ *as S-R^*-modules, by the correspondence* $m\mapsto(f\to fm_r)\mapsto(fh\to fm_r)$, *where* $f\in\mathrm{Hom}_r({}_RM, {}_RR)$, $m\in M$, $m=(r\to rm)(r\in R)$.

Proof. The proof of (1) is found in [9]. (2) We use (1). Then, $\mathrm{Hom}_r({}_RM, {}_RR)\simeq\mathrm{Hom}_r({}_RM, {}_R\mathrm{Hom}_r({}_SR, {}_SS))\simeq\mathrm{Hom}_r({}_SR\otimes_RM, {}_SS)\simeq\mathrm{Hom}_r({}_SM, {}_SS)$. Thus we obtain the required isomorphism.

Now, with the same notations and assumptions as in Lemma 3.2, we set $\mathrm{End}_r({}_RM)=R^*$ and $\mathrm{End}_r({}_SM)=S^*$, and assume that ${}_RR|{}_RM$ and that ${}_SM|{}_SS$. Then $M_{R^*}|R^*_{R^*}, S^*_{S^*}|M_{S^*}$, and R^* is a subring of S^*. Since $S^*=\mathrm{Hom}_r({}_SM, {}_SM)$

$\simeq \mathrm{Hom}_r({}_sM, {}_sS)\otimes_S M \simeq \mathrm{Hom}_r({}_RM, {}_RR)\otimes_S M \simeq \mathrm{Hom}_l(M_{R^*}, R^*_{R^*})\otimes_S M$ as R^*-left modules, we have ${}_{R^*}S^*|_{R^*}R^*$, because ${}_{R^*}\mathrm{Hom}_l(M_{R^*}, R^*_{R^*})|_{R^*}R^*$ and ${}_sM|_sS$. There hold $\mathrm{Hom}_r({}_{R^*}S^*, {}_{R^*}R^*) = \mathrm{Hom}_r({}_{R^*}\mathrm{Hom}_r({}_sM, {}_sM), {}_{R^*}R^*) \simeq \mathrm{Hom}_r({}_{R^*}\mathrm{Hom}_r({}_sM, {}_sS)\otimes_S M, {}_{R^*}R^*) \simeq \mathrm{Hom}_r({}_sM, {}_s\mathrm{Hom}_r({}_{R^*}\mathrm{Hom}_r({}_sM, {}_sS), {}_{R^*}R^*)) \simeq \mathrm{Hom}_r({}_sM, {}_sM) = S^*$ as S^*-R^*-modules (Lemma 3.2). Put $H=(fhm_r \to fm_r)$, where $f\in \mathrm{Hom}_r({}_RM, {}_RR)$, $m\in M$, and $m_r=(r\to rm)(r\in R)$ (Lemma 2.3). Then, under the above isomorphisms, $H \mapsto (fh\otimes m \to fm_r) \mapsto (m\to (fh\to fm_r)) \to (m\to m) = 1_M$ (Lemma 3.2 (2)). Hence S^*/R^* is a Frobenius extension with a Frobenius homomorphism H. Since ${}_sM|_sS$, there are $f_j\in \mathrm{Hom}({}_sM, {}_sS)$, $m_j\in M$ such that $\sum_j x^{f_j}\cdot m = x$ for all $x\in M$. Since ${}_RR|_RM$, there are $g_k\in \mathrm{Hom}_r({}_RM, {}_RR)$, $n_k\in M$ such that $\sum_k n_k^{g_k}=1$. Put $\varphi_{j,i,k}=f_j a_{ir} h m_{kr}$, where $a_{ir}=(x\to xa_i)(x\in R)$, and $n_{kr}=(y\to yn_k)(y\in R)$. Put $\psi_{k,i,j}=g_k h b_{ir} m_{jr}$. Then $\varphi_{j,i,k}, \psi_{k,i,j}\in S^*$, and $s^*=\sum_{j,i,k}\varphi_{j,i,k}\cdot H(\psi_{k,i,j}s^*)=\sum_{j,i,k}H(s^*\varphi_{j,i,k})\psi_{k,i,j}$ for all s^* in S^*. Now, for any a^* in $\mathrm{V}_{S^*}(R^*)$, $(m)\sum_{j,i,k}\varphi_{j,i,k}a^*\psi_{k,i,j}=a^n\cdot m$ for all m in M, where $am=ma^*$ for all $m\in M$. Hence $\sum_{j,i,k}\varphi_{j,i,k}a^*\psi_{k,i,j}=1$ for some a^* in $\mathrm{V}_{S^*}(R^*)$ if and only if $a^n=1$ for some $a\in \mathrm{V}_R(S)$. The former is equivalent to that S^*/R^* is separable, and the latter is equivalent to that ${}_sS_S$ is a direct summand of ${}_sR_S$. Thus we have the following

Theorem 3.3. *Let R/S be a Frobenius extension, and M an R-left module such that ${}_RR|_RM$ and ${}_sM|_sS$. Put $\mathrm{End}_r({}_RM)=R^*$ and $\mathrm{End}_r({}_sM)=S^*$. Then S^*/R^* is a Frobenius extension. With a Frobenius homomorphism h of R/S, a Frobenius homomorphism of S^*/R^* is written as $(fhm_r\to fm_r)$, where $f\in \mathrm{Hom}_r({}_RM, {}_RR)$, $m\in M$, and $m_r=(x\to xm)(x\in R)$. S^*/R^* is separable if and only if ${}_sS_S$ is a direct summand of ${}_sR_S$.*

Proposition 3.4. *With the same notations and assumptions as in* Th. 3.3, *the Frobenius homomorphism H yields h, symmetrically. Therefore, if we set $S'=\mathrm{End}_l(M_{S^*})$, then h is an S'-S'-homomorphism from R into S'.*

Proof. Any f in $\mathrm{Hom}_r({}_RM, {}_RM)$ is written as $f=(x\to(y\to x\cdot {}^g y))(x, y\in M)$ with a suitable g in $\mathrm{Hom}_l(M_{R^*}, R^*_{R^*})$. Therefore $H=((x\to(y\to x\cdot {}^g y)^h\cdot m)\to {}^g m)$, where $x, y, m\in M$, $g\in \mathrm{Hom}_l(M_{R^*}, R^*_{R^*})$. Let $H\to h'$. Then $h'=((y\to m\cdot {}^{h'}(x\to x^f\cdot y))\to m^f)$, where $m, x, y\in M$, $f\in \mathrm{Hom}_r({}_sM, {}_sS)$. Since $x^f=(\sum_i a_i(b_i x)^f)^h$ (Lemma 3.2), we know that $h'=(\sum_i a_i(b_i m)^f\to m^f)$, where $m\in M$, $f\in \mathrm{Hom}_r({}_sM, {}_sS)$. Let $f=f'h$ $(f'\in \mathrm{Hom}_r({}_RM, {}_RR))$. Then $h'=(m^{f'}\to m^{f'h})=h$. (Note that $(M)\mathrm{Hom}({}_RM, {}_RR)=R$.) This completes the proof.

Corollary 1. *Let R/S be a Frobenius extension with a Frobenius homomorphism h, and $S'=\mathrm{End}_l(R_{S'})$, where $S^*=\mathrm{End}_r({}_sR)$. Then R/S' is a Frobenius extension with a Frobenius homomorphism h.*

Remark. Assume that ${}_{S'}S'$ is a direct summand of ${}_{S'}R$. Then $h(c)=1$

for some c in R. Then, for any x in S', $S \ni h(cx) = h(c)x = x$, and so $S = S'$.

Corollary 2. *Let R/S be a Frobenius extension, and R a division ring. Then S is also a division ring.*

Proof. In this case, S' is a division ring. Hence ${}_{S'}S'$ is a direct summand of ${}_{S'}R$, and so $S' = S$ (cf. the above remark).

Proposition 3.5. *Let R/S be a Frobenius extension, and ${}_SS_S$ is a direct summand of ${}_SR_S$. If ${}_RR$ is completely reducible, then so is ${}_SS$.*

Proof. $\mathrm{End}_r({}_SR)/R_r$ is separable. Then, by [7; Lemma 2.10], $\mathrm{End}_r({}_SR)$ is $\mathrm{End}_r({}_SR)$-left completely reducible, and so R is $\mathrm{End}_r({}_SR)$-right completely reducible. Hence ${}_SS$ is completely reducible.

Corollary. *Let R/S be Frobenius and separable, and assume that ${}_SS_S$ is a direct summand of ${}_SR_S$. Then ${}_RR$ is completely reducible if and only if so is ${}_SS$.*

§ 4. On Frobenius extensions and H-separable extensions.

Throughout this section, R/S is a Frobenius extension, h an S-S-homomorphism from R to S, and r_i, l_i elements of R such that $x = \sum_i (xr_i)^h \cdot l_i = \sum_i r_i (l_i x)^h$ for all x in R.

Lemma 4.1. $V_R(S) \simeq \mathrm{Hom}({}_RR_R, {}_RR \otimes {}_SR_R)$ *by the mapping* $a \mapsto (x \to \sum_i r_i \otimes a l_i x)$ $(x \in R)$.

Proof. $V_R(S) \simeq \mathrm{Hom}({}_SR_R, {}_SR_R) \simeq \mathrm{Hom}({}_SR \otimes {}_RR_R, {}_SR_R) \simeq \mathrm{Hom}({}_RR_R, {}_R\mathrm{Hom}({}_SR, {}_SR)_R) \simeq \mathrm{Hom}({}_RR_R, {}_RR \otimes {}_SR_R)$ (cf. Lemma 3.2).

Proposition 4.2. *The following are equivalent:*

(i) ${}_RR \otimes {}_SR_R | {}_RR_R$ (cf. Hirata [3]).

(ii) *There are elements a_j, b_j in $V_R(S)$ such that $\sum_j a_j x b_j = x^h$ for all x in R.*

Proof. To be easily seen, $V_R(S) \simeq \mathrm{Hom}({}_RR \otimes {}_SR_R, {}_RR_R)$ by the mapping $a \mapsto (x \otimes y \to xay)$ $(x, y \in R)$. From this fact, as is easily seen, ${}_RR \otimes {}_SR_R | {}_RR_R$ if and only if there are a_j, b_j in $V_R(S)$ such that $(R \otimes {}_SR \ni)\ y \otimes 1 = \sum_{i,j} r_i \otimes a_j l_i y b_j$ for all y in R. As $R \otimes {}_SR \simeq \mathrm{Hom}({}_SR, {}_SR)$ by the mapping $x \otimes y \to xhy$, $y \otimes 1 = \sum_{i,j} r_i \otimes a_j l_i y b_j$ for all y in R if and only if $yh = \sum_{i,j} r_i h a_j l_i y b_j$ for all y in R. Noting that $a_j \in V_R(S)$, we have $\sum_{i,j} (xr_i)^h \cdot a_j l_i y b_j = \sum_j a_j x y b_j$ $(x \in R)$. Thus the proof is complete.

Remark. If R/S is G-Galois, and each $\sigma \in G$ is an inner automorphism of A, then ${}_RR \otimes {}_SR_R | {}_RR_R$.

Let A/B be rings, and ${}_AA \otimes {}_BA_A | {}_AA_A$. Such an extension was introduced by Hirata [3]. By [3; Th. 2.2], A/B is separable. Sugano [11] call such

an extension an H-*separable extension*.

The proof of the following is similar to [9; Cor. 1.1], and may be omitted.

Lemma 4.3. *If* ${}_SR_S|_{S^*}S_S$ *then we can take* r_i, l_i *in* $V_R(S)$, *and conversely.*

Theorem 4.4. *Let* M *be an* R*-left module such that* ${}_RR|_RM$ *and* ${}_SM|_{S^*}S$, *and let* $R^*=\mathrm{End}_{r}({}_RM)$, *and* $S^*=\mathrm{End}_{r}({}_SM)$. *Then the following are equivalent*:

(i) ${}_SR_S|_{S^*}S_{S^*}$.

(ii) ${}_{S^*}S^*\otimes_{R^*}S^*{}_{S^*}|_{S^*}S^*{}_{S^*}$.

Proof. By Th. 3.3, S^*/R^* is a Frobenius extension with a Frobenius homomorphism $H=(fhm_r\to fm_r)$, where $f\in\mathrm{Hom}_r({}_RM, {}_RR)$, $m\in M$. Let a_i, b_i $(i=1,\cdots,n)$ be in $V_R(S)$, and $a_im=ma_i^*$, $b_im=mb_i^*$ for all m in M. Then, for any y in S^*, $(y)\sum_i a_i^*fhm_rb_i^*=\sum_i b_i(a_i\cdot y^f)^h\cdot m$. Therefore, $\sum_i a_i^*fhm_rb_i^*=fm_r$ for all f, m if and only if $\sum_i b_i(a_i\cdot y^f)^h=y^f$ for all f, y. Now, since ${}_RR|_RM$, there holds $(M)\mathrm{Hom}({}_RM, {}_RR)=R$, and hence the latter is equivalent to that $\sum_i b_i(a_ix)^h=x$ for all x in R. Then, by Lemma 4.3, the proof is evident.

Combining Th. 4.4 with Prop. 2.3, we obtain the following

Theorem 4.5. *Let* $\Delta=\sum_{\sigma\in G}\oplus A^*u_\sigma$ *be a crossed product of* A^* *with* G, *and* H *a subgroup of* G. *Then the following are equivalent*:

(i) ${}_\Delta\Delta\otimes_{\Delta_H}\Delta_\Delta|_\Delta\Delta_\Delta$.

(ii) *There are elements* δ_i, δ_i' *in* $V_\Delta(\Delta_H)$ *such that* $\sum_i\delta_iu_\tau\delta_i'=\delta_{H,\tau}u_\tau$ *for all* τ *in* G.

§ 5. On a finite Galois extension with a free basis.

We consider the following condition for a ring R.

(*) If $ab=1$ for a, b in R, then $ba=1$.

Theorem 5.1. *Let* A *be a ring,* G *a finite group of automorphisms of* A, $G=\{\sigma_1,\sigma_2,\cdots,\sigma_g\}$, *and* $B=A^G$. *Let* $(A)_g$ *be the ring of* $n\times n$ *matrices over* A, *and assume that the ring* $(A)_g$ *satisfies the condition* (*). *Then the following are equivalent*:

(i) *For some subset* $\{a_1,\cdots,a_g,b_1,\cdots,b_g\}$ *of* A, *there holds* $\sum_k\sigma_i(a_k)\sigma_j(b_k)=\delta_{i,j}$, *where* $\delta_{i,j}$ *means Kronecker's delta.*

(ii) *For some subset* $\{a_1,\cdots,a_g,b_1,\cdots,b_g\}$ *of* A, *there holds* $\sum_k\sigma_k(b_i)\sigma_k(a_j)=\delta_{i,j}$.

(iii) *For some subset* $\{a_1,\cdots,a_g,b_1,\cdots,b_g\}$ *of* A, $(t_G(b_ia_j))$ *is inversible in* $(B)_g$, *where* $t_G(b_ia_j)$ *is the* (i,j)*-component.*

(iv) A/B *is finite* G*-Galois, and* $A_B=a_1B+\cdots+a_gB$ *for some subset*

$\{a_1, \cdots, a_g\}$ *of* A.

In these cases, $\{a_1, \cdots, a_g\}$ *is a free basis of* ${}_BA$. *For a subset* $S = \{a_1, \cdots, a_g, b_1, \cdots, b_g\}$ *of* A, S *satisfies* (i) *if and only if it satisfies* (ii).

Proof. (i)$\Longleftrightarrow$(ii) If we put $\sigma_i(a_j) = c_{ij}$ and $\sigma_i(b_j) = c^*_{ji}$, then (i) is equivalent to that $(c_{ij})(c^*_{ij}) = E$ (unit matrix). By assumption, the latter is equivalent to that $(c^*_{ij})(c_{ij}) = E$, that is, $\sum_k \sigma_k(b_i)\sigma_k(a_j) = \delta_{i,j}$. (ii)$\Rightarrow$(iii) is trivial. (iii)$\Rightarrow$(ii), (iv) Let (b_{ij}) be the inverse matrix of $(t_G(b_i a_j))$, where $b_{ij} \in B$. Then $\delta_{i,j} = \sum_k b_{ik} \cdot t_G(b_k a_j) = t_G((\sum_k b_{ik} b_k) a_j)$. If we set $b'_i = \sum_k b_{ik} b_k$, then $\delta_{i,j} = \sum_k \sigma_k(b'_i)\sigma_k(a_j)$. Then $\sum_k \sigma_i(a_k)\sigma_j(b'_k) = \delta_{i,j}$, because (i)$\Longleftrightarrow$(ii). Thus A/B is G-Galois. By [9; Cor. 1.1], $\{a_1, \cdots, a_g\}$ is a free basis of A. (iv)$\Rightarrow$(i) There is a subset $\{b_1, \cdots, b_g\}$ of A such that $\sum_i a_i \cdot t_G(b_i x) = x$ for all x in A. Then $\{a_1, \cdots, a_g, b_1, \cdots, b_g\}$ satisfies (i).

Corollary. *Let* A/B *be finite* G*-Galois,* $(G : 1) = g$ *and* A *a semi-primary ring. Further, assume that* ${}_BA$ *or* A_B *is generated by* g *elements. Then* A *has a normal basis.*

Proof. Since A is semi-primary, so is $(A)_g$. Then $(A)_g$ satisfies the condition (*). Hence ${}_BA$ and A_B are free, by Th. 5.1. Consequently, by [6; Th. 1.7], A has a normal basis.

Remark (1) If R is a left Noetherian ring, then R satisfies (*). To see this, let $ab = 1$ for a, b in R. Then, the mapping $x \to xb$ from R to R is an epimorphism. By assumption, this homomorphism must be $1-1$. As $(ba-1)b = 0$, we have $ba - 1 = 0$, that is, $ba = 1$.

(2) If R/I satisfies (*) for an ideal I which is contained in the Jacobson radical of R, then so is R. To see this, let $ab = 1$ for a, b in R. Then $(b+I)(a+I) = 1+I$, and so $ba - 1 \in I$. Therefore $Rba + I = R$. Since I is contained in the Jacobson radical of R, we have $Rba = R$. Hence a has a left inverse. Thus $ba = 1$.

References

[1] G. AZUMAYA: Completely faithful modules and self-injective rings, Nagoya Math. J., 27 (1966), 697-708.

[2] K. HIRATA and K. SUGANO: On Semisimple extensions and separable extensions over non commutative rings, J. Math. Soc. Japan 18 (1966), 360-373.

[3] K. HIRATA: Some types of separable extension of a ring, to appear in Nagoya Math. J.

[4] K. KASCH: Projective Frobenius-Erweiterungen, Sitzungsber. Heidelberger Acad., 1960/1961, 89-109.

[5] H. F. KREIMER: Galois theory for noncommutative rings and normal bases, Trans. Amer. Math. Soc., 127 (1967), 42-49.

[6] Y. MIYASHITA: Finite outer Galois theory of non-commutative rings, J. Fac. Sci. Hokkaido Univ., Ser. I, 19 (1966), 114-134.

[7] ——————: Locally finite outer Galois theory, J. Fac. Sci. Hokkaido Univ., Ser. I, 20 (1967), 1-26.

[8] K. MORITA: Duality for modules and its application to the theory of rings with minimum condition, Sci. Rep. Tokyo Kyoiku Daigaku, 6 (1958), 83-142.

[9] T. ONODERA: Some studies on projective Frobenius extensions, J. Fac. Sci. Hokkaido Univ., Ser. I, 18 (1964), 89-107.

[10] H. TOMINAGA: Some results on normal basis, to appear in Math. J. Okayama Univ.

[11] K. SUGANO: Note on semi-simple extensions and separable extensions, Osaka J. Math., 4 (1967), 265-270.

Department of Mathematics,
Hokkaido University

(Received June 6, 1968)