ON POLYNOMIAL EXTENSIONS OF SIMPLE RINGS

By

Kazuo KISHIMOTO *)

Introduction. Let S be a simple ring, and A an extension ring of S with the common identity. If $[A:S]_r = n(>1)$ and there exists some $y \in A$ such that $A = \sum_{i=0}^{n-1} y^i S$ and $Sy \subseteq yS + S$, then A/S is called *an n dimensional right polynomial extension* and $\{y^i;\ i=0,1,\cdots,n-1\}$ is called *a right polynomial S-basis for A*. Then, by $sy = ys' + s''$ $(s \in S)$, we can define in S a monomorphism $\rho_y : s \rightarrow s'$ and a $(1, \rho_y)$-derivation[1] $D_y : s \rightarrow s''$. On the other hand, an extension ring A' of S (with the common identity) is called *an m dimensional left polynomial extension* over S if $[A':S]_l = m$ (>1), $A' = \sum_{i=0}^{m-1} Sx^i$ and $xS \subseteq Sx + S$. Finally, a right polynomial extension is called *a polynomial extension* if it is a left polynomial extension at the same time. Any right quadratic extensions and cyclic extensions (Cf. [4]) are right polynomial extensions.

The purpose of the present paper is to give some information to the study of finite dimensional right polynomial simple ring extensions. In **§1**, we shall give a relation between the left dimension and the right dimension of a right polynomial extension and a necessary and sufficient condition for a simple ring to have a finite dimensional right polynomial extension. **§2** is devoted to determine the structure of $V = V_R(S)$, the centralizer of S in R (R is a finite dimensional right polynomial simple ring extension), under the restriction that ρ is inner or D_y is ρ_y-inner[2]. As the result, we can see that V is a commutative semi-simple ring with minimum condition in the most of cases. In **§3**, we shall treat with a right polynomial simple ring extension that is Galois. Finally, in **§4**, a general description of right quadratic extensions of simple rings will be given, and it is closely related to that investigated in [1]. Throughout the present paper, we assume always R will mean an n dimensional right polynomial simple ring extension over S, and that $R = \sum_{i=0}^{n-1} y^i S = (\oplus_{i=0}^{n-1} y^i S$[3]$)$ and $sy = y(s\rho_y) + sD_y$. By C and Z, we denote the respective centers of R and S, and other notations and terminologies used in this paper, we follow [4].

---

*) Domestic Fellow in the Mathematical Institute, Hokkaido University, on leave from Hokkaido Gakugei University.

1) Cf. [3]. P. 170.

2) Unless otherwise stated, a ρ-derivation means $(1, \rho)$-derivation.

3) $\oplus$ means a direct sum.

§ 1. The left dimension and the construction of a right polynomial extension.

Throughout this section, we assume that A is an n dimensional (not necessary simple) right polynomial extension over S such that $A=\sum_{i=0}^{n-1} y^i S$, $sy=y(s\rho_y)+sD_y$ $(s\in S)$. By $P_{k,i}$, we denote the sum of all formally different products of consisting of i ρ_y's and $k-i$ D_y's. (e.g. $P_{3,2}=\rho_y^2 D_y+\rho_y D_y \rho_y+D_y\rho_y^2$, and we set $\rho_y^0=D_k^0=1$). Then,

Lemma 1.1. *$sy^k=\sum_{i=0}^{n-1} y^i sP_{k,i}$ for each $s\in S$.*

Proof. We prove the assertion by the induction on k. Obviously, $sy=y(s\rho_y)+sD_y=ysP_{1,1}+sP_{1,0}$. Assume that $sy^{k-1}=\sum_{i=0}^{k-1} y^i sP_{k-1,i}$. Then $sy^k=(\sum_{i=0}^{k-1} y^i sP_{k-1,i})y=\sum_{i=0}^{k-1} y^{i+1}(sP_{k-1,i})\rho_y+\sum_{i=0}^{k-1} y^i(sP_{k-1,i})D_y=(sP_{k-1,0})D_y+\sum_{i=1}^{k-1} y^i$ $((sP_{k-1,i})D_y+(sP_{k-1,i-1})\rho_y)+y^k(sP_{k-1,k-1}\rho_y)$. Noting here that the number of formally different terms of $P_{j,i}$ is $\binom{j}{i}$, $P_{k-1,i}D_y+P_{k-1,i-1}\rho_y$ coincides with $P_{k,i}$ which completes our induction.

Corollary 1.1. *Let $\{x^i;\ i=0,1,\cdots,n-1\}$ be a right polynomial S-basis with $sx=x(s\rho_x)+sD_x$ $(s\in S)$. Then $\rho_x t_l=\rho_y t_r$ for some $t\in S$ and $0<k<n$. In particular, if ρ_y is an automorphism or S is a division ring, then $\rho_x=\rho_y\widetilde{t^{-1}}$ and $D_x=\sum_{i=0}^{k} P_{i,0}s_{ir}-\rho_y\widetilde{t^{-1}}s_{0l}$ for some $s_i\in S$ where $\widetilde{t^{-1}}$ is the inner automorphism generated by t^{-1}.*

Proof. Let $x=y^k s_k+\sum_{j=0}^{k-1} y^j s_j$ $(k\geqq 1,\ s_i\in S,\ s_k\neq 0)$. Then we have $y^k s_k(s\rho_x)+\sum_{j=0}^{k-1} y^j s_j(s\rho_x)+sD_x=x(s\rho_x)+sD_x=sx=s(y^k s_k+\sum_{j=0}^{k-1} y^j s_j)=y^k(s\rho_y^k)s_k+\sum_{i=0}^{k-1} y^i sP_{k,i}s_k+\sum_{j=0}^{k-1}(\sum_{i=0}^{j} y^j sP_{j,i})s_j$. This show that $\rho_x t_l=\rho_y t_r$ where $t=s_k$ and $D_x=\sum_{i=0}^{k} P_{i,0}s_{ir}-\rho_x s_{0l}$. In particular, if ρ_y is an automorphism (or S is a division ring), $s_k\in S^{\cdot}$ [4] by $Ss_k=S\rho_y^k s_k=s_k S\rho_x$. Hence we have $\rho_x=\rho_y\widetilde{t^{-1}}$ *and* $D_x=\sum_{i=0}^{k} P_{i,0}s_{ir}-\rho_y\widetilde{t^{-1}}s_{0l}$.

Corollary 1.2. *Let R be an n dimensional right polynomial (simple ring) extension over S.*

(**a**) *If ρ_x is inner, then so is every $\rho_{x'}$, and there exists a right polynomial S-basis $\{y^i;\ i=0,1,\cdots,n-1\}$ such that $\rho_y=1$.*

(**b**) *If D_x is ρ_x-inner, then ρ_x is an automorphism, every $D_{x'}$ is $\rho_{x'}$-inner, and then there exists a right polynomial S-basis $\{y^i;\ i=0,1,\cdots,n-1\}$ such that $D_y=0$ and $\rho_y=\rho_x$.*

Proof. (a) Let $\rho_x=\tilde{u}$ for some $u\in S$. Then $\rho_{x'}=\rho_x\widetilde{t^{-1}}=\widetilde{ut^{-1}}$ for some $t\in S$. Further, $sxu=xus+sE$ $(s\in S)$ where $E=D_x u_r$ is a derivation in S, and $\{(xu)^i;\ i=0,1,\cdots,n-1\}$ is a requested right polynomial S-basis.

4) $S^{\cdot}$ means the multiplicative group consisting of the regular elements of S.

(b) Let D_x be ρ_x-inner generated by $u\in S$. Then $s(x-u)=(x-u)(s\rho_x)$ $(s\in S)$ and $\{(x-u)^i;\ i=0,1,\cdots,n-1\}$ is a requested polynomial S-basis. Further, $D_{x'}=\sum_{i=0}^k P_{i,0}s_{ir}-\rho_{x'}s_{0l}$ where $P_{i,j}$ is defined by ρ_y and D_y $(=0)$ and $y=x-u$. Hence $P_{i,0}=0$ if $i\neq 0$. This means that $D_{x'}$ is an inner ρ_x-derivation generated by s_0. Now, let $\sum_i y^i t_i$ $(t_i\in S)$ be an arbitrary element of R. Then $(\sum_i y^i t_i)y$ $=y(\sum_i y^i t_i\rho_y)$ implies $R=RyR=yR$. Thus y is a regular element of R, and hence $y^{-1}Sy=S\rho_y\subseteqq S$. On the other hand, since $R=\sum_{i=0}^{n-1}y^iS$, $R=y^{-1}Ry=$ $\sum_{i=0}^{n-1}y^i(y^{-1}Sy)$ shows that $\rho_y=\widetilde{y^{-1}}\,|\,S$ is an automorphism. The rest is clear from Corollary 1.1.

Theorem 1.1. $[A:S]_l=\sum_{i=1}^n([S:S\rho_y]_l)^i+1$.

Proof. Let $B_0=\{1\}$, and B_i a left $S\rho_y^i$-basis for S $(i=1,2,\cdots)$. Then one will easily see that $\sharp B_i=(\sharp B_1)^i$. Now, we shall prove that $Y=\{y^iB_i;$ $i=0,1,\cdots,n-1\}$ is a left S-basis for A. Since $y^i(s\rho_y^i)-sy^i\in\sum_{j=0}^{i-1}y^jS$ $(i=1,2,\cdots,n-1)$, we readily see that $y^iS\subseteqq Sy^iB_i+\sum_{j=0}^{i-1}y^jS$, whence it follows $y^iS\subseteqq\sum_{j=0}^{i}Sy^jB_j$, namely, Y is a left generating system of A over S. At the same time, the linear independence of Y over S will easily seen.

Corollary 1.3. *The following conditions are eqnivalent.*

(a) $[A:S]_l=[A:S]_r$.

(b) *There exists an element* $x\in A\backslash S$ *such that* $xs=(s\tau)x+sE$ $(s\in S)$ *where* τ *is a monomorphism in* S, E *a* $(\tau,1)$*-derivation in* S.

(c) ρ_y *is an automorphism.*

Proof. (c)→(a). This is direct consequence of Theorem 1.1.

(a)→(b). By Theorem 1.1, ρ_y is an automorphism, and then, $sy=y(s\rho_y)$ $+sD_y$ $(s\in S)$ implies $ys=(s\rho_y^{-1})y+s(-\rho_y^{-1}D_y)$.

(b)→(c). If $x=y^ks_k+\sum_{j=0}^{k-1}y^js_j$ $(s_i\in S)$, *then* $k\geqq 1$ and $s_k\neq 0$. Hence, for each $u\in S$, $y^ks_ku+\sum_{j=0}^{k-1}y^js_ju=xu=(u\tau)x+uE=(u\tau)(y^ks_k+\sum_{j=0}^{k-1}y^js_j)+uE$. Therefore, we obtain $s_ku=(u\tau)P_{k,k}s_k=(u\tau\rho_y^k)s_k$, whence it follows $S=Ss_kS$ $=Ss_k$, namely, $s_k\in S^{\cdot}$. Hence $\tau\cdot\rho_y^k=\tilde{s}_k$, which means that ρ_y is an automorphism.

Combining Corollary 1.2 (b) with Corollary 1.3, we have

Corollary 1.4. *If* D_y *is* ρ_y*-inner, then* $[R:S]_l=[R:S]_r$ [5].

Let ρ be a monomorphism in S and D a ρ-derivation in S. We consider the ring $\mathfrak{S}=S[X;\ \rho,D]=\{\sum_i X^is_i;\ s_i\in S\}$, where the multiplication is defined by $sX=X(s\rho)+sD$. If S is a division ring or a simple ring (of the capacity

5) The converse is not true. For, as is shown in Theorem 4.2, a right quadratic extension R/S is Galois (and hence $[R:S]_l=[R:S]_r$) if and only if D_y is ρ_y-inner provided $\chi(S)\neq 2$. On the other hand, as was constructed in [2], there exists a non Galois quadratic extension R/S $(\chi(S)\neq 2)$ such that $[R:S]_l=[R:S]_r$.

>1) and ρ is an automorphism, then $\mathfrak{S}$ is a right principal ideal ring, that is, each right ideal of $\mathfrak{S}$ is generated by some monic polynomial f (i.e. the leading coefficient of f is 1). Let f be a monic polynomial of $\mathfrak{S}$. Then f is called w-irreducible if f does not generate $\mathfrak{S}$ but any monic proper left factor of f does $\mathfrak{S}$. By easy computations, we can see that an ideal M of $\mathfrak{S}$ is maximal if and only if *the monic generator*[6] of M is w-irreducible.

Now, we shall give a necessary and sufficient condition for S to have an n dimensional right polynomial extension.

Theorem 1.2. (**a**) *In order that S have an n dimensional right polynomial extension, it is necessary and sufficient that there exist a monomorphism ρ in S, a ρ-derivation D in S and a $1\times n$ matrix $(u_0, u, \cdots, u_{n-1})$ with entries in S such that*

(1) $u_{i-1}-u_{i-1}\rho=u_iD+u_i(u_{n-1}-u_{n-1}\rho)$ $(i=0,1,\cdots,n-1$ *where we set* $u_{-1}=1)$.

(2) $P_{n,j}+\sum_{i=0}^{n-1}P_{i,j}u_{ir}$ *is a* (ρ^j,ρ^n)*-inner derivation generated by* $-u_j$ *for each* $j=0,1,\cdots,n-1$.

(**b**) *In order that S have an n dimensional polynomial extension, it is necessary and sufficient that there exist an automorphism ρ in S, a ρ-derivation D in S and a $1\times n$ matrix $(u_0, u, \cdots, u_{n-1})$ with entries in S satisfying* (1), (2) *stated above.*

(**c**) *In order that S have an n dimensional polynomial simple ring extension, it is necessary and sufficient that there exist an automorphism ρ in S, a ρ-derivation D in S and a $1\times n$ matrix $(u_0, u_1, \cdots, u_{n-1})$ with entries in S satisfying* (1), (2) *stated above and*

(3) $X^n+\sum_{i=0}^{n-1}X^iu_i$ *is w-irreducible in* $S[X;\rho,D]$.

Proof. (a) The conditions (1) and (2) are equivalent with the statment that the right ideal M of $S[X;\rho,D]$ generated by $f(X)=X^n+\sum_{i=0}^{n-1}X^iu_i$ is a two-sided ideal. In fact, M is a two-sided ideal if and only if $Xf(X)=f(X)(X+t)$ $(t\in S)$ and $sf(X)=f(X)s'$ $(s'\in S)$ for every $s\in S$. The former implies $X^{n+1}+\sum_{i=0}^{n-1}X^{i+1}u_i=(X^n+\sum_{i=0}^{n-1}X^iu_i)(X+t)=X^{n+1}+\sum_{i=0}^{n-1}X^{i+1}u_i\rho+X^nt+\sum_{i=0}^{n-1}X^i(u_iD+u_it)=X^{n+1}+X^n(u_{n-1}\rho+t)+\sum_{i=1}^{n-1}X^i(u_{i-1}\rho+u_iD+u_it)+u_0D+u_0t$ which means $t=u_{n-1}-u_{n-1}\rho$, $u_{i-1}=u_{i-1}\rho+u_iD+u_it$, $i=1,2,\cdots,n$ and $u_0D+u_0t=0$. Thus, we have $u_{i-1}-u_{i-1}\rho=u_iD+u_i(u_{n-1}-u_{n-1}\rho)$ for each $i=0,1,\cdots,n-1$. Next, the latter implies $s(X^n+\sum_{i=0}^{n-1}X^iu_i)=\sum_{i=0}^{n}X^isP_{n,i}+\sum_{j=0}^{n-1}(\sum_{i=j}^{n}X^jsP_{j,i})u_i$ $=X^ns\rho^n+\sum_{i=0}^{n-1}X^isP_{n,i}+\sum_{j=0}^{n-1}(\sum_{i=j}^{n}X^jsP_{i,j})u_i=X^ns'+\sum_{i=0}^{n-1}X^iu_is'$. Hence $s\rho^n=s'$, $sP_{n,j}+\sum_{i=j}^{n}sP_{i,j}u_i=sP_{n,j}+\sum_{i=j}^{n}sP_{i,j}u_i=sP_{n,j}+\sum_{i=j+1}^{n}sP_{i,i}u_i+sP_{j,j}u_j$ $=u_js'$, and this means that $P_{n,j}+\sum_{i=j+1}^{n}P_{i,j}u_{ir}$ is a (ρ^j,ρ^n)-inner derivation

6) Cf. [4]. P. 75.

generated by $-u_j$ for each $j=0,1,\cdots,n-1$. Thus $S[X;\rho,D]/M=A\cong\oplus_{i=0}^{n-1}y^iS$ where $sy=y(s\rho)+sD$ $(s\in S)$, y is the residue class of X modulo M, is a requested one. Conversely, let $A=\oplus_{i=0}^{n-1}y^iS$ be an n dimensional right polynomial extension with $sy=y(s\rho_y)+sD_y$ for each $s\in S$. Then the mapping φ: $\sum_i X^is_i\to\sum_i y^is_i$ is an S (ring) epimorphism of $S[X;\rho_y,D_y]$ *to* A. Let $y^n+\sum_{i=0}^{n-1}y^iu_i=0$ for some $u_i\in S$. Then N, the kernel of φ, contains $M=(X^n+\sum_{i=0}^{n-1}X^iu_i)S[X;\rho_y,D_y]$. Now, we conclude that M coincides with N. For, if $g(X)=\sum_{i=0}^m X^is_i$ $(s_i\in S)$ is a polynomial of N with $m<n$, then $\sum_{i=0}^m y^is_i=0$ in A, and hence $g(X)=0$. Thus, each polynomial of N has $X^n+\sum_{i=0}^{n-1}X^iu_i$ as its left factor. This means that $N=M$. Consequently, ρ_y, D_y and $(u_0,u_1,\cdots,u_{n-1})$ satisfy conditions (1) and (2).

(b) By Corollary 1.3, a finite dimensional right polynomial extension is a polynomial extension if and only if ρ is an automorphism. Hence the statment is clear from (a).

(c) Recalling that (3) is equivalent with the maximality of $M=(X^n+\sum_{i=0}^{n-1}X^iu_i)S[X;\rho_y\, D_y]$ by the remark stated just before our theorem the statment is clear from (a) and (b).

§2. The centralizer of S in R.

Let $V=V_R(S)$ be the centralizer of S in R. In this section, we shall investigate the relations between $\{\rho_y,D_y\}$ and V.

Lemma 2.1. *If $V\neq Z$, then ρ_y is an automorphism and $m=((\rho_y):(\rho_y)\cap\tilde{S})<n$ where $\tilde{S}$ is the set of all inner automorphisms determined by the elements of $S^{\cdot}$.*

Proof. Since $V\neq Z$, there exists an element $v=y^ks_k+\sum_{j=0}^{k-1}y^js_j$ $(s_i\in S)$ of V such that $s_k\neq 0$ $(0<k<n)$. Then $\sum_{i=0}^k y^isP_{k,i}s_k+\sum_{j=0}^{k-1}(\sum_{i=0}^j y^isP_{j,i})s_j=sv=vs=y^ks_ks+\sum_{j=0}^{k-1}y^js_js$ $(s\in S)$, which implies that $sP_{k,k}s_k=s\rho_y^ks_k=s_ks$, in particular, $S=Ss_kS=Ss_k$. Hence $s_k\in S^{\cdot}$, and $\rho_y^k=\tilde{s}_k$.

Theorem 2.1. *Let D_y be an inner ρ_y-derivation.*

(**a**) *$V\neq Z$ if and only if ρ_y is an automorphism and $m=((\rho_y):(\rho_y)\cap\tilde{S})<n$, and when this is the case, m is a divisor of n.*

(**b**) *V is a finite dimensional commutative algebra over Z. Moreover, if $\chi(S)$, the characteristic of S, is 0 or relatively prime to n, then V is a finite direct sum of fields.*

Proof. Since D_y is ρ_y-inner, we may choose a right polynomial S-basis $\{w^i;\ i=0,1,\cdots,n-1\}$ with $D_w=0$ by Corollary 1.2 (b). Therefore we may assume from the beginning $sy=y(s\rho_y)$. Thus as was shown in the proof of Corollary 1.2 (b), $y\in R^{\cdot}$ and $\tilde{y}^{-1}|S=\rho_y$. For the sake of simplicity, we set $\rho=\rho_y$.

(a) The only if part is shown in Lemma 2.1. Conversely, let ρ be an automorphism and $m=((\rho):(\rho)_\cap\tilde{S})<n$. Then $\widetilde{y^{-m}}|S=\tilde{s}$ for some $s\in S$. Therefore $y^m s$ is not contained in Z but in V. Let $y^n+\sum_{i=0}^{n-1}y^i u_i=0$ $(u_i\in S)$. Then $s(y^n+\sum_{i=0}^{n-1}y^i u_i)-(y^n+\sum_{i=0}^{n-1}y^i u_i)(s\rho^n)=0$ $(s\in S)$ yields at once $su_0=u_0(s\rho^n)$. Since $u_0\neq 0$ by the regularlity of y, the last means that u_0 is a regular element. Consequently we have $\rho^n=\widetilde{u_0^{-1}}$, equivalently, m is a divisor of n.

(b) It suffices to prove the case $V\neq Z$. By (a), ρ is an automorphism and $m=((\rho):(\rho)_\cap\tilde{S})$ is a proper divisor of n: $m'=n/m$. Let $v=\sum_{i=0}^{n-1}y^i s_i$ $(s_i\in S)$ be an element of V. Since $\sum_{i=0}^{n-1}y^i(t\rho^i)s_i=tv=vt=\sum_{i=0}^{n-1}y^i s_i t$ for each $t\in S$, we see that $ty^i s_i=y^i(t\rho^i)s^i=y^i s_i t$, namely, each $y^i s_i\in V$. Moreover, if $s_i\neq 0$, then $t\rho^i s_i=s_i t$ proves $s_i\in S^{\cdot}$ and $\rho^i=\tilde{s}_i$. Thus $V=\{\sum_{k=0}^{m'}y^{mk}s^k z_k;\ z_k\in Z\}$, where $\tilde{s}=\rho^m$. The commutativity of V follows from the fact that $y^{mk}s^k z_k$ commutes with every element of V. Thus V is an m' dimensional commutative algebra over Z. Next, let us assume that $\chi(S)=0$ or $(\chi(S), n)=1$. We shall denote the extension $\widetilde{y^{-1}}$ of ρ again by ρ. Let v an element of V. Then $T_m(v;\rho)=\sum_{i=0}^{m-1}v\rho^i$ is contained in C, for $T_m(v;\rho)=T_m(v;\rho)\rho$. If v is nilpotent, then so is $v\rho$ $(v\rho\in V)$ and hence $T_m(v;\rho)$ is nilpotent, and so 0. (Recall that ρ is an automorphism in S and $T_m(v;\rho)$ is in C). Thus we have proved that if $T_m(v;\rho)\neq 0$ then v is non nilpotent. Now we shall show that each (non-zero) non regular element of V is non nilpotent. If $v=\sum_{i=0}^{n-1}y^i s_i\in V\backslash Z$ $(s_i\in S)$, $s_0=1$ (is non regular), then $T_m(v;\rho)=T_m(v-1;\rho)+m\neq 0$. For $T_m(v-1;\rho)$ is either 0 or not contained in Z. (Note that m is a divisor of n). In general, if $v=y^{mj}s^j z_j+\sum_{k>j}y^{mk}s^k z_k\in V\backslash Z$ $(z_j\neq 0)$ is non regular, $u=(y^{mj}s^j z_j)^{-1}v$ $(\in V)$ is non regular and its constant term is 1, and so, u is non nilpotent by the last remark. Hence u is non nilpotent in either case, which means the semi-simplicity of V.

Theorem 2.2. *Let ρ_y be an inner automorphism.*

If $\chi(S)=0$ or $\chi(S)>n$, then V coincides with either C or Z, more precisely, if $V\neq Z$, $R=S[C]$.

Proof. Since ρ_y is an inner automorphism, we may choose a right polynomial S-basis $\{w^i;\ i=0,1,\cdots,n-1\}$ with $sw=ws+sD_w$ $(s\in S)$ by Corollary 1.2 (a). Therefore we may assume that from the beginning that $sy=ys+sD_y$ $(s\in S)$. Assume $V\neq Z$, and write $D=D_y$. Then there exists an element $v=y^k s_k+y^{k-1}s_{k-1}+\cdots+s_0$ $(k\geqq 1,\ s_i\in S,\ s_k\neq 0)$ of V, and $\sum_{i=0}^{k}(y^i sP_{k,i})s_k+\sum_{i=0}^{k-1}(y^i sP_{k-1,i})s_{k-1}+\cdots+ss_0=sv=vs=y^k s_k s+y_{k-1}s_{k-1}s+\cdots+s_0 s$ implies $s_k\in Z$. Since $\binom{k}{k-1}sDs_k+ss_{k-1}=sP_{k,k-1}s_k+sP_{k-1,k-1}s_{k-1}=s_{k-1}s$, D is an inner derivation generated by $-(1/k)s_{k-1}s_k^{-1}$. Thus, by Corollary 1.2 (b), we can choose an S-basis $\{c^i;\ i=0,1,\cdots,n-1\}$ such that $c\in C$.

Corollary 2.1. If $[S:Z]$ is finite, then $[R:S]_l=[R:S]_r$.

Proof. By [5. Lemma], $[R:C]$ is finite. If $V=Z$, then $Z\supseteq C$, and hence $[R:S]_l[S:C]_l=[R:C]_l=[R:C]_r=[R:S]_r[S:C]_r$ shows that $[R:S]_l=[R:S]_r$. On the other hand, if $V\neq Z$, ρ_y is an automorphism by Lemma 2.1. Hence the assertion is a direct consequence of Corollary 1.3.

§ 3. Polynomial Galois extensions.

Throughout the present section, by $\mathfrak{G}$, we denote the set of all S-automorphisms of R.

If σ is an arbitrary element of $\mathfrak{G}$, and $u_\sigma=y\sigma-y$ then $su_\sigma=u_\sigma(s\rho_y)$ $(s\in S)$. For, $s(y\sigma)=(sy)\sigma=(y\,(s\rho_y)+sD_y)\sigma=(y\sigma)s\rho_y+sD_y$ $(s\in S)$, we have $s(y\sigma-y)=(y\sigma-y)(s\rho_y)$.

Lemma 3.1. *Let $\mathfrak{G}\neq 1$ and $\sigma\neq 1$ be an arbitrary element of $\mathfrak{G}$. Then, there exists a right polynomial S-basis $\{y^i;\ i=0,1,\cdots,\mathrm{n}-1\}$ such that $y\sigma-y\in V$ if and only if some (and so every) ρ_x is inner.*

Proof. Let $v_\sigma=y\sigma-y$ be in V. Then $v_\sigma s=sv_\sigma=v_\sigma s\rho_y$. Hence $v_\sigma(s-s\rho_y)=0$. If we note that the right annihilator of $v_\sigma(\neq 0)\in V$ in S is a two-sided ideal, we can readily obtain $s\rho_y=s$, namely, $\rho_y=1$. Thus each ρ_x is inner by Corollary 1.2 (a). Conversely, if each ρ_x is inner, there exists a right polynomial S-basis $\{y^i;\ i=0,1,\cdots,n-1\}$ with $\rho_y=1$ by Corollary 1.2 (a). Then $y\sigma-y$ is in V.

Corollary 3.1. *Let R be an n dimensional right polynomial division ring extension over S. If $\mathfrak{G}\neq 1$, then $[R:S]_l=[R:S]_r$.*

Proof. For any $\sigma(\neq 1)\in\mathfrak{G}$, there exists a non zero $u_\sigma\in R$ such that $su_\sigma=u_\sigma(s\rho_y)$ for every right polynomial S-basis $\{y^i;\ i=0,1,\cdots,n-1\}$. Hence $\widetilde{u_\sigma^{-1}}|S=\rho_y$, $R=R\widetilde{u_\sigma^{-1}}=\sum_{i=0}^{n-1}y^i\widetilde{u_\sigma^{-1}}(S\widetilde{u_\sigma^{-1}})=\sum_{i=0}^{n-1}y^i\widetilde{u_\sigma^{-1}}(S\rho_y)$ and $\{y^i\widetilde{u_\sigma^{-1}};\ i=0,1,\cdots,n-1\}$ is right linearly independent over $S\rho_y$. This means that $n=[R:S]_r=[R:S\rho_y]_r$. Thus ρ_y is an automorphism in S, and then $[R:S]_l=[R:S]_r$ by Corollary 1.3.

Corollary 3.2. *Let ρ_y be an inner automorphism.*

(a) *Assume $V=Z$. If $\chi(S)>n$ or $\chi(S)=0$, then $\mathfrak{G}=1$.*

(b) *Assume $\chi(S)=n$. If $V=Z\neq C$ then R/S is an inner cyclic extension, and conversely.*

Proof. (a) Suppose $\mathfrak{G}$ contains an element $\sigma\neq 1$. Then by Lemma 3.1, there exists a right polynomial S-basis $\{y^i;\ i=0,1,\cdots,n-1\}$ with $sy=ys+sD_y$ $(s\in S)$, and $y\sigma=y+z_\sigma$, $z_\sigma(\neq 0)\in V=Z$. Thus we may assume further $y\sigma=y+1$. Hence if $y^n=\sum_{i=0}^{n-1}y^is_i$ $(s_i\in S)$, we have $y^n\sigma=(y+1)^n=\sum_{i=0}^{n}\binom{n}{i}y^i$

$=y^n+\sum_{i=0}^{n-1}\binom{n}{i}y^i=\sum_{i=1}^{n-1}y^i\left(\binom{n}{i}+s_i\right)$ and $y^n=(\sum_{i=0}^{n-1}y^is_i)\sigma=\sum_{i=0}^{n-1}(y+1)^is_i=\sum_{i=0}^{n-1}\left(\sum_{j=0}^{n-1}\binom{i}{j}y^j\right)s_i$. From those, we see that $\binom{n}{n-1}+s_{n-1}=s_{n-1}$, whence it follows a contradiction $\binom{n}{n-1}=0$.

(b) If R/S is inner Galois, then $V=Z\neq C$ by Theorem 2.2. Next, we shall prove the converse. Let $z_0\in Z\backslash C$. Then $z_0D_y=z_0y-yz_0$ is a non zero element of Z. If $\sum_{i=0}^{n-1}y^it_i$ $(t_i\in S)$ is in $J(\tilde{z}_0, R)$, $\sum_{i=0}^{n-1}y^it_i=(\sum_{i=0}^{n-1}y^iy_i)\tilde{z}_0=\sum_{i=0}^{n-1}z_0y^it_iz_0^{-1}=\sum_{i=0}^{n-1}\left(\sum_{j=0}^{i}\binom{i}{j}y^jz_0D^{i-j}\right)t_iz_0^{-1}$. Hence, we obtain $\binom{n-1}{n-2}z_0Dt_{n-1}z_0^{-1}=0$, and so $t_{n-1}=0$. Repeating the same procedures, we have $t_i=0$, $i=1,2,\cdots,n-1$. Thus $J(\tilde{z}_0, R)=S$. Furthermore, the fact that $C=\{z\in Z;\ zD_y=0\}$ and $z^kD_y=(kz^{k-1})zD_y$ imply the order of $\tilde{z}_0$ is just n.

Theorem 3.1. (a) *Let $\chi(S)=n$. In order that S have an n dimensional polynomial Galois extension $R=\sum_{i=0}^{n-1}y^iS$ with $sy=ys'+s''$ such that $s\to s'$ is an inner automorphism, it is necessary and sufficient that the following condition be satisfied:*

(1) *There exist a derivation D in S and $s\in S$ satisfying $D^n-D=I_s$, $sD=0$ and X^n-X-s is w-irreducible in $S[X;D]$.*

(b) *Let $\chi(S)>n$ or $\chi(S)=0$. In order that S have an n dimensional polynomial Galois extension $R=\sum_{i=0}^{n-1}y^iS$ with $sy=ys'+s''$ such that $s\to s'$ is an inner automorphism, it is necessary and sufficient that the following condition be satisfied:*

(2) *There exists an n dimensional Galois extension field of Z.*

Proof. (a) Let R/S be a Galois extension with the requested property. Then, by Theorem 2.2, V is either Z or C. If $V=C$, then R/S is obviously an n dimensional cyclic extension. On the other hand, if $V=Z\neq C$ then R/S is still an n dimensional cyclic extension by Corollary 3.2 (b). Hence, there holds (1) by [4. Theorem 2.1]. Conversely, if there exist D, S satisfying (1), then, by [4. Theorem 2.1], there exists an n dimensional polynomial Galois extension $R=\sum_{i=0}^{n-1}y^iS$ such that $ty=yt+tD$ $(t\in S)$.

(b) Assume that there exists a Galois extension R/S with the requested property. Then $V=C\supsetneqq Z$ and $R=S[C]$ by Theorem 2.2 and Corollary 3.2 (a). Thus the rest of the proof will be obvious.

Theorem 3.2. *Let ρ be an automorphism in S. In order that S have an n dimensional polynomial inner Galois extension $R=\sum_{i=0}^{n-1}y^iS$ with $sy=y(s\rho)+s''$ such that $s\to s''$ is an inner ρ-derivation, it is necessary and sufficient that there exist $s_0\in S$, $z\in Z$ satisfying the following conditions:*

(1) $\rho^n=\tilde{s}_0$, $s_0\rho=s_0$.

(2) $z\rho^i\neq z$ $(i=1,\cdots,n-1)$.

(3) X^n-s_0 *is w-irreducible in* $S[X;\rho]$.

More precisely, when this is the case, R/S has a cyclic Galois group.

Proof. Assume that there exists a Galois extension R/S with the requested property. Since V is commutative by Theorem 2.1 (b), V has to coincides with Z. Further, by Corollary 1.2 (b), we may assume $sy=y(s\rho)$ $(s\in S)$. One may remark here $\rho=\widetilde{y^{-1}}|S$ (Cf. the proof of Corollay 1.2 (b).). If $y^n=\sum_{i=0}^{n-1}y^iu_i$ $(u_i\in S)$, then $\widetilde{y^{-n}}|S=\rho^n=\widetilde{u_0^{-1}}$. (By the regularlity of y, $u_0\neq 0$, and hence $u_0\in S^{*}$). Hence $zy^nz^{-1}=y^n(z\rho^n)z^{-1}=y^n$ for each $z\in Z$, which implies $s_0=y^n\in J(\tilde{Z},R)=S$. (Obviously $s_0\rho=s_0$). Further, by the same way as in the proof of Theorem 1.2 (a), $R\cong S[X;\rho]/(X^n-s_0)S[X;\rho]$ and X^n-s_0 is w-irreducible in $S[X;\rho]$. Next, as $[R:S]=[V:C]=[Z:C]$ and $J(\rho|Z,Z)=C$, there exists an element $z\in Z$ such that $z\rho^i\neq z$ for $i=1,\cdots,n-1$. (Take, for instance, a normal basis element of Z/C). Then $J(\tilde{z},R)=S$. In fact, $\sum_{i=0}^{n-1}y^it_i\in J(\tilde{z},R)$ $(t_i\in S)$ shows that $\sum_{i=0}^{n-1}y^it_i=z(\sum_{i=0}^{n-1}y^it_i)z^{-1}=\sum_{i=0}^{n-1}y^it_i(z\rho^i)z^{-1}$ and hence, $t_i=0$ for $i=1,2,\cdots,n-1$. Conversely, assume that there exist $s_0\in S$, $z\in Z$ satisfying (1)–(3). Then (1) is equivalent with $M=(X^n-s_0)S[X;\rho]$ is a two-sided ideal, and hence $R=S[X;\rho]/M=\oplus_{i=0}^{n-1}y^iS$ is an n dimensional polynomial extension with $sy=y(s\rho)$ where y is the residue class of X modulo M. Now (3) is equivalent with the maximality of M. Hence R is simple. Finally by (2), we can use the above argument to prove $J(\tilde{z},R)=S$ and then we have $V=J(\tilde{z}|V,V)=V\cap S=Z$ (a field). Thus R/S is an inner Galois extension with respect to a cyclic Galois group $(\tilde{z})$.

§ 4. Right quadratic extensions.

Let $R=\oplus_{i=0}^{1}y^iS$ be a right quadratic simple ring extension over S. Then, it is clear that $sy=y(s\rho_y)+sD_y$ $(s\in S)$ where ρ_y is a monomorphism in S, D_y is a ρ_y-derivation in S.

Lemma 4.1. *R is $R_l\cdot S_r$-irreducible.*

Proof. It suffices to prove $R=RxS$ for each $x\in R\backslash S$. Since $RxS+S$ is a subring of R properly containing S, $RxS+S=R=S\oplus yS$. Hence there exists $u\in S$ such that $y-u\in RxS$. Noting that $\{1,y-u\}$ is a right S-basis for R, $(R(y-u)S)R=(R(y-u)S)(S+(y-u)S)\subseteq R(y-u)S$, and hence $R=R(y-u)S=RxS$.

Lemma 4.2. *Let ρ be an automorphism in S, and $f(X)=X^2+Xu_1+u_0$ $(u_0,u_1\in S)$ a polynomial of $S[X;\rho,D]$ where D is a ρ-derivation in S. Assume that $f(X)$ generates a proper ideal of $S[X;\rho,D]$. Then $f(X)$ is*

w-irreducible if and only if S has no solution t satisfying the following conditions:

(i) $tD+t(u_1-t\rho)=u_0$.

(ii) $tD=t(t\rho-t)$.

(iii) $sD=t(s\rho)-st$ *for each* $s\in S$.

Moreover, $f(X)$ is irreducible[7] *if and only if S has no solution t satisfying* (i).

Proof. Let t be an element of S. Then $I=(X+t)S[X;\rho,D]$ is a two-sided ideal if and only if $X(X+t)=(X+t)(X+t')$ $(t'\in S)$ and $s(X+t)=(X+t)s'$ $(s'\in S)$ for every $s\in S$. The former imples $t'=t-t\rho$, $tD+tt'=0$. The latter implies $sD=ts'-st$, $s'=s\rho$ for every $s\in S$. Hence I is a two-sided ideal if and only if t satisfies (ii) and (iii).

Let us assume that $f(X)=(X+t)(X+b)=X^2+X(t\rho+b)+tD+tb$. Then $t\rho+b=u_1$, $tD+tb=u_0$, and so, we have $tD+t(u_1-t\rho)=u_0$. Thus $f(X)$ is irreducible if and only if S has no solution t satisfying (i). Next, we assume that $f(X)=(X+t)(X+b)$ is w-irreducible. If we note that the right ideal $I=(X+t)S[X;\rho,D]$ does not coincide with $S[X;\rho,D]$, I can not be a two-sided ideal. Thus t does not satisfy one of the conditions (ii) and (iii) but satisfies (i). Finally, we assume that $f(X)$ is not w-irreducible, then, there exists $t\in S$ such that $f(X)=(X+t)(X+b)$ and the two-sided ideal $(X+t)$ generated by $X+t$ is a proper ideal of $S[X;\rho,D]$. Since the monic generator of $(X+t)$ is $X+t$ itself, $(X+t)=(X+t)S[X;\rho,D]$. Hence t satisfies all the conditions (i)–(iii).

Now, we shall give a necessary and sufficient condition for S to have a right quadratic simple ring extension.

Theorem 4.1. (**a**) *In order that S have a right quadratic simple ring extension, it is necessary and sufficient that there exist a monomorphism ρ in S, a ρ-derivation D in S and a 1×2 matrix (u_0,u_1) with entries in S satisfying* (1), (2) *of Theorem* 1.2 (a) *and the following condition*:

(3) *There exists a finite subset $\{s_i,t_i,v_i\}$ of S satisfyng* $\sum_i(-u_1(s_i\rho)a+s_iDa+s_ib+t_i\rho a)v_i=0$, and $\sum_i(-u_0(s_i\rho)a+t_iDa+s_ib)v_i=1$ for each pair (a,b) of $S\times S$ *such that* $a\neq 0$.

(**b**) *In order that S have a quadratic simple ring extension, it is necessary and sufficient that there exist an automorphism ρ in S, a ρ-derivation D in S and a 1×2 matrix (u_0,u_1) with entries in S satisfying* (1), (2) *of Theorem* 1.2 *(a) and the following condition*:

(3′) *S has no solution t satisfying* (i), (ii) *and* (iii) *of Lemma* 4.2.

---

7) A polynomial $f(X)$ of $S[X;\rho,D]$ is called *irreducible* if $f(X)$ has no left monic factor $g(X)$ such that $\deg g(X)<\deg f(X)$.

Proof. (a) As was shown in the proof of Theorem 1.2 (a), the existence of ρ, D and (u_0, u_1) satisfying (1), (2) are equivalent with the statment that S has a right quadratic (polynomial) extension $R=S[X;\rho,D]/(X^2+Xu_1+u_0)S[X;\rho,D]$. Let $R=S\oplus yS$ where y is the residue class of X modulo $(X^2+Xu_1+u_0)S[X;\rho,D]$. Then (3) yields the simplicity of R. In fact, $\sum_i(ys_i+t_i)(ya+b)v_i=\sum_i y^2s_iav_i+\sum_i y(s_ib+s_iDa+s_ib+t_i\rho a)v_i+\sum_i(t_iDa+t_ib)v_i=\sum_i y(-u_1(s_i\rho)a+s_iDa+s_ib+t_i\rho a)v_i+\sum_i(-u_0(s_i\rho)a+t_iDa+t_ib)v_i=1$ for each $ya+b\in R$ $(a,b\in S)$. Conversely, let R be simple. Then, R is $R_l\text{-}S_r$-irreducible by Lemma 4.1. Hence there exists a finite subset $\{s_i, t_i, v_i\}$ of S satisfying (3).

(b) The assertion is almost evident from the proof of (a) and Lemma 4.2. The proof may be left to readers.

Lemma 4.3. *Let R be a right quadratic simple ring extension over S. Then,*

(**a**) *V is either Z or C.*

(**b**) *If R/S is Galois, then either ρ_y is inner or D_y is ρ_y-inner.*

Proof. (a) Let $V\neq Z$. Then ρ_y is inner by Lemma 2.1, and hence $V=C$ (and $R=S[C]$) by Theorem 2.2.

(b) Let $\sigma(\neq 1)$ be in $\mathfrak{G}$ and $u_\sigma=y\sigma-y$. Then $su_\sigma=u_\sigma(s\rho_y)$ $(s\in S)$. We set $u_\sigma=ya+b$ $(a,b\in S)$. Then $y(s\rho_y)a+sD_ya+sb=su_\sigma=u_\sigma s\rho_y=ya(s\rho_y)+b(s\rho_y)$. Hence, we obtain $(s\rho_y)a=a(s\rho_y)$ and $sD_ya=s(-b)-(-b)(s\rho_y)$. Since ρ_y is an automorphism (Corollary 1.3), the first relation implies $a\in Z$. If $a=0$, then $b\neq 0$ and $sb=b(s\rho_y)$. Hence $b\in S^{\cdot}$ and $\rho_y=\widetilde{b^{-1}}$. On the other hand, if $a\neq 0$, then D_y is ρ_y-inner generated by $(-a^{-1}b)$.

Corollary 4.1. *Let $\chi(S)\neq 2$.* If *$Z\neq C$, then R/S is a Galois extension. If $[S:Z]<\infty$, then R/S is a Galois extension.*

Proof. By the assumption $Z\neq C$ and Lemma 4.3 (a), we have either $V=Z\supsetneqq C$ or $V=C\supsetneqq Z$ and $R=S[C]=S\otimes_Z C$ (Theorem 2.2). The former implies $J(\widetilde{Z},R)=S$ and the latter implies C/Z is Galois, and hence R/S is Galois. The latter assertion is a consequence of the former. In fact, if $[S:Z]<\infty$ and $Z=C$ then $[R:C]<\infty$ and $V=C$ (Lemma 4.3 (a)), we have then a contradiction $R=S$.

Theorem 4.2. *Let $\chi(S)\neq 2$. If R/S is a Galois extension then D_y is ρ_y-inner, and conversely.*

Proof. By Lemma 4.3 (a) and Corollary 4.1, it suffices to prove our theorem for the case $V=Z$. Assume that R/S is Galois. Then ρ_y is an automorphism (Corollary 1.3) and either ρ_y is inner or D_y is ρ_y-inner by Lemma 4.3 (b). If ρ_y is inner, it contradicts Corollary 3.2 (a). Conversely, assume

D_y is ρ_y-inner. Then we may assume $D_y=0$, ρ_y is an automorphism. (Corollary 1.2 (b)). Let $y^2+yu_1+u_0=0$ $(u_i \in S)$. Since $s(y^2+yu_1+u_0)-(y^2+yu_1+u_0)(s\rho_y)=0$ $(s \in S)$, we have $u_1=0$. Otherwise, $\rho_y=u_1^{-1}$ and it contradicts $V=Z$ (Theorem 2.1 (a)). Thus the map $\sigma: s+yt \rightarrow s-yt$ $(s, t \in S)$ is an automorphism of R such that $J(\sigma, R)=S$.

References

[1] P. M. COHN: Quadratic extensions of skew fields, Proc. London Math. Soc., (3) 11 (1961), 531–556.

[2] N. JACOBSON: A note on two dimensional division ring extension, Amer. J. Math., Vol. 77 (1955), 593–599.

[3] N. JACOBSON: Structure of Rings, Providence (1956).

[4] K. KISHIMOTO: On cyclic extensions of simple rings, J. of Fac. Sci. Hakkaido Univ., Ser. I. Vol. 19 (1966), 74–85.

[5] H. TOMINAGA: On a theorem of N. JACOBSON, Proc. Japan Acad., Vol. 31 (1955), 653–654.

Hokkaido Gakugei University

(Received July 22, 1966)