ON CYCLIC EXTENSIONS OF SIMPLE RINGS

By

Kazuo KISHIMOTO*)

In his paper [2], Amitsur has given the condition for a division ring to have a cyclic extension, and at the same time he has determined the types of cyclic extensions. Obviously, the earlier works for the commutative case (Artin-Schreier [3], Albert [1], Witt [12]) and for the non-commutative quadratic case (Dieudonné [4]) are contained in Amitsur’s one. The purpose of this paper is to give simple rings an analogue. Concerning the case that the simple ring is of prime characteristic $p$ and the extension dimension is a power of $p$, our attempt will be accomplished in §2. While, §3 is devoted to the study of the case that the simple ring is of characteristic 0 or prime $p$ not dividing the extension dimension. Now, we shall begin our study with the following preliminary section.

§ 1. Notations and prerequisite results.

Throughout the present paper, $R \supseteq S$ represent simple rings1) with the respective centers $C$ and $Z$ such that $R$ is a unital $S$-module, and $V$ the centralizer $V_{R}(S)$ of $S$ in $R$.

I. Let $\rho$ be an automorphism of a ring $A$ and $D$ a $\rho$-derivation2) in $A$. Then $A[X; \rho, D]$ means the ring of all (non-commutative) polynomials in the indeterminate $X$ with the coefficient in $A$ (written on the right side), where the multiplication is defined by the distributive law and the rule $aX=X(a\rho)+aD(a\in A)$. In particular, we set $A[X; D]=A[X; 1, D]$, $A[X; \rho]=A[X; \rho, 0]$ and $A[X]=A[X; 1, 0]$.

(i) Let $g=\sum X^{s}a_{s}$ be an arbitrary element of $A[X; D]$. If $c$ is a non-zero element of $V_{A}(A)$ with $cD=c$ then $gI_{c}^{m}=(g(c_{r}-c_{l})^{m})=m!c^{m}a_{m}$.

In fact, $gI_{c}^{m}=(gc-cg)I_{c}^{m-1}=(X^{m-1}mca_{m}+\cdots)I_{c}^{m-1}=m!c^{m}a_{m}$ by induction.

(ii) If $a$ is an arbitrary element of $A$ then $(X+a)^{n}=\sum_{s=0}^{n}\left(\begin{array}{l}n\vspace{1em}\hline k\end{array}\right)X^{n-k}A_{k}(a)$ in $A[X; D]$, where $A_{k}(a)=1$ and $A_{k}(a)=(A_{k-1}(a))D+(A_{k-1}(a))a^{3}$.

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

1) Throughout the present paper, a simple ring means a (simple) Artinian ring


An easy induction with respect to (abbreviated w.r.t.) $n$ will prove the assertion.

(iii) Let $\tau$ be an endomorphism of $A$, and $a$ an element of $A$. The map $\Phi: \sum X^\alpha a \rightarrow \sum (X+a)^\alpha (a, \tau)$ defines an endomorphism of $A[X; D]$ if and only if $D\tau - \tau D = \tau \cdot I_n$. Moreover, the endomorphism $\Phi$ is an automorphism if and only if $\tau$ is an automorphism. In particular, for any $c \in V_A(A)$, $\Phi: \sum X^\alpha a \rightarrow \sum (X+c)^\alpha a$, defines an $A$-ring automorphism of $A[X; D]$.

Indeed, $\Phi$ is an endomorphism if and only if $b\Phi X\Phi = (Xb + bD)\Phi$ and hence $b\tau \cdot (X+a) = X(b\tau) + (b\tau)D + b\tau \cdot a = (X+a)b\tau + (b\tau)\tau$, consequently, $b(D\tau - \tau D) = (b\tau)a - a(b\tau) = b \cdot \tau I_n$ for each $b \in A$. If $(\sum_{\nu=0}^n X^\alpha a_\alpha)\Phi = \sum_{\nu=0}^n (X+a)^\nu (a, \tau) = \sum_{\nu=0}^n \left( \sum_{\mu=0}^\nu \binom{\nu}{\mu} X^{\nu-\mu} a_\mu (a, \tau) \right)$ then $a_\nu \tau = \Delta_1 (a) a_\nu \tau + a_{\nu-1} \tau = \frac{n}{2} \Delta_1 (a) a_\nu \tau + \binom{n-1}{1} \Delta_1 (a) a_{\nu-1} \tau + a_{\nu-2} \tau = \cdots = \binom{n}{n-1} \Delta_{n-1} (a) a_n \tau + \binom{n-1}{n-2} \Delta_{n-2} (a) a_{n-1} \tau + \cdots + \Delta_1 (a) a_{\nu-1} \tau + a_{\nu-2} \tau = 0$. Thus, $\Phi$ is an automorphism.

(iv) Let $\rho$ be an automorphism, and $\tau$ an endomorphism of $A$ respectively. The map $\Psi: \sum X^\alpha a \rightarrow \sum (Xb)^\alpha (a, \tau)$ where $b$ is an arbitrary regular element of $A$ defines an endomorphism of $A[X; \rho]$ if and only if $\tau \cdot \rho = \rho \cdot \tau \cdot \tilde{a}$ where $\tilde{a} = a_1 \cdot a_1^{-1}$. Moreover, the endomorphism $\Psi$ is an automorphism if and only if $\tau$ is an automorphism.

Indeed, $\Psi$ is an endomorphism if and only if $b\Psi X\Psi = b\tau (Xa) = X(b\rho a)\rho = (Xb\rho)\Psi = Xa(b\rho \tau)$, and hence, $b\tau \rho = b\rho \tau \cdot \tilde{a}$ for each $b \in A$. Since $(\sum X^\alpha a_\alpha)\Psi = \sum X^\alpha (a\rho^{-1} a\rho^{-2} \cdots \rho^{-n} a)(a, \tau)$, an endomorphism $\Psi$ is an automorphism if and only if $\tau$ is an automorphism.

For each automorphism $\rho$ of $A$, we set $RN_\rho (a; \rho) = a \cdot a\rho \cdots a\rho^{-1}$ and $LN_\rho (a; \rho) = a\rho^{-1} a\rho^{-2} \cdots a\rho \cdot a (a \in A)$, and it will be called the right (resp. left) $\rho$-norm of $a$ if $\rho$ is of order $\nu$.

Let $\mathfrak{S} = S[X; \rho, D]$ such that $\rho$ is an automorphism. If $I$ is an arbitrary non-zero ideal of $\mathfrak{S}$, there exists a uniquely determined monic polynomial $f$ such that $I = f\mathfrak{S} = \mathfrak{S}f$. In fact, $f$ is the monic polynomial in $I$ of the lowest degree, and called the monic generator of $I$. Now, let $g$ be a monic polynomial in $\mathfrak{S}$. If $g$ does not generate $\mathfrak{S}$ but any proper monic left divisor of $g$ does $\mathfrak{S}$, $g$ is defined to be $\rho$-irreducible. If $g$ is central (i.e. $g \in V_S(\mathfrak{S})$) and irreducible then it is $\rho$-irreducible while the converse is not true, and if $\mathfrak{S}$ is a field.

4) Let $S$ be the ring of $2 \times 2$ matrices over $GF(2)$ with a system of matrix units $\{e_{ij}; i,j = 1, 2\}$ and $\mathfrak{S} = S[X]$. Then $X^2 + X + 1$ is contained in the center of $\mathfrak{S}$ and $X^2 + X + 1 = (X+e_{12}+e_{21}+e_{22}) (X+e_{11}+e_{12}+e_{13})$. On the other hand, as is easily seen, a monic divisor $X+s$ of $X^2 + X + 1$ does not generate $\mathfrak{S}$ if and only if $s \in V_S(\mathfrak{S}) = GF(2)$. Thus, $X^2 + X + 1$ is central and $\rho$-irreducible, but not irreducible.

5) Throughout the present paper, "field" means a commutative field.
and $\mathfrak{G}=S[X]$ then the notion of $w$-irreducibility coincides with that of irreducibility.

(v) A non-zero ideal $I$ of $\mathfrak{G}$ is maximal if and only if the monic generator of $I$ is $w$-irreducible.

II. An automorphism group $\mathfrak{G}$ of $R$ is called an $F$-group if $\mathfrak{G}$ is of finite order and the subring $I(\mathfrak{G})$ of $R$ generated by all the regular element $v$ inducing inner automorphism $\tilde{v}$ contained in $\mathfrak{G}$ is a simple ring. Needles to say, if $R$ is a division ring, any finite automorphism group is an $F$-group.

(vi) If $\mathfrak{G}$ is an $F$-group then $S=J(\mathfrak{G}, R)$ (the fixsubring of $\mathfrak{G}$) is simple, $V=I(\mathfrak{G})$ and $[R:S]\leq\#\mathfrak{G}$ (order of $\mathfrak{G}$) [9, Lemma 2].

If $\mathfrak{G}$ is an $F$-group and $[R:J(\mathfrak{G}, R)]=\#\mathfrak{G}$, $R/J(\mathfrak{G}, R)$ is said to be $\mathfrak{G}$-regular (or strictly Galois w.r.t. $\mathfrak{G}$ [9]).

(vii) If $R$ is Galois and finite over $S$ with a cyclic Galois group $\mathfrak{G}=\langle \sigma \rangle$, then $V$ is a field, and hence, by [8, Lemma 1.4], each intermediate ring of $R/S$ is simple.

For the sake of completeness, we shall give here a short proof. Since $V$ is Galois and finite over $Z$ contained in the center of $V$, it suffices to prove that if $R$ is Galois and finite over a subfield $S$ of $C$ then $R=C$. If $\widetilde{\mathfrak{G}}$ is the order of $\sigma/C^6$ then $\widetilde{\mathfrak{G}}=\tilde{\sigma}$ with some $\tilde{\sigma}$. Since $\tilde{\sigma}^{-1}=\tilde{\sigma}^{-1}\in C$ by $\alpha\tilde{\sigma}^{-1}=\tilde{\sigma}$ and there holds $N_{C,C^{6}}(c^\prime)\equiv \Pi_{0}^{\gamma-1}c^\prime=1$, it is well known that there exists an element $c\in C$ such that $c^{-1}=c^{-1}$. Setting here $z=v\sigma$, we see that $\tilde{\tau}=\tilde{z}$ and $z$ is contained in $Z$. Hence, $C[z]$ is a subfield of the center of $V$, and so $R=V=C[z]=C$.

(viii) If $\mathfrak{G}$ is an $F$-group of order $p^e$ such that $J(\mathfrak{G}, R)=S$ and $Z$ contains no primitive $p$-th roots of 1, then $[R:S]$ is a divisor of $\#\mathfrak{G}$ and $V$ coincides with the field $C[Z]$ [7, Theorem 5].

Let $R/S$ be $\mathfrak{G}$-regular.

(ix) If $\sigma\rightarrow s_\sigma$ is a homomorphism of $\mathfrak{G}$ into the additive group of $S$, then there exists an element $x$ in $R$ such that $s_\sigma = -x + x\sigma$ for all $\sigma$ in $\mathfrak{G}$ [10, Corollary 3].

(x) If $\sigma\rightarrow s_\sigma$ is an anti-homomorphism of $\mathfrak{G}$ into $S^*$, then there exists an element $x$ in $R^*$ such that $s_\sigma = x^{-1} x \sigma$ for all $\sigma$ in $\mathfrak{G}$ [10, Corollary 2].

III. Let $R/S$ be $\mathfrak{G}$-regular. $R$ is called a cyclic extension of $S$ w.r.t. $\mathfrak{G}$ if $\mathfrak{G}$ is cyclic. In particular, if $R/S$ is a cyclic extension w.r.t. inner (resp. outer) $\mathfrak{G}$, we say that $R/S$ is an inner (resp. outer) cyclic extension. $R/S$ is defined to be a parallel extension of $S$ w.r.t. $\mathfrak{G}$ if there exists a $\mathfrak{G}$-invariant

---

6) $\sigma|C$ means the contraction of $\sigma$ to $C$.

7) Let $A(\mathfrak{G}1)$ be a ring. Then, $A^*$ means the multiplicative group consisting of the regular elements of $A$. 

---
simple subring $T$ of $R$ such that $R = S[T]$ and $T/T \cap S$ is $\mathfrak{G}|T$-regular. Obviously, if $R/S$ is a parallel extension then $\mathfrak{G}$ is isomorphic to $\mathfrak{G}|T$, and hence $[R : S] = [T : T \cap S]$. A parallel extension $R = S[T]$ of $S$ w.r.t. $\mathfrak{G}$ is called a $d$-parallel (resp. $f$-parallel), if $T$ can be a division ring (resp. field). In particular, an $f$-parallel extension $R = S[T]$ is called a trivial extension if $T = C$, namely, $R = S \otimes \mathbb{F} C$. If $R/S$ is a trivial extension, it is obviously outer Galois and each $\mathfrak{G}$-invariant (simple) intermediate ring of $R/S$ is a trivial extension of $S$. The following facts are pointed out by H. Tominaga.

(xi) If $R/S$ is outer Galois and finite and $[S : Z] < \infty$ then $R/S$ is trivial. In particular, if $R$ is outer Galois and finite over a field then $R$ is a field.

In fact, noting that $[R : C] < \infty$ by [11, Lemma], $V_{R}(S[C]) = V = C$, and that $S[C] = S \otimes \mathbb{F} C$ is simple, the principal theorem of simple rings yields at once $R = S[C]$.

(xii) Assume that $R/S$ is $\mathfrak{G}$-regular, $S$ is of characteristic $p$, and $\mathfrak{G} = \mathfrak{G}^{p}$. In order that $R/S$ is a trivial extension, it is necessary and sufficient that $C$ contains an element $c$ with $T_{\mathfrak{G}}(c) = \sum_{\sigma \in \mathfrak{G}} c \sigma \neq 0$.

If $c$ is an element of $C$ with $T_{\mathfrak{G}}(c) \neq 0$ then $\{c \sigma ; \sigma \in \mathfrak{G}\}$ is an $S$-basis of $R$ contained in $C$ [9, Corollary 1], and so, $R = S[C] = S \otimes \mathbb{F} C$. The converse is obviously true.

Let $R/S$ be $\mathfrak{G}$-regular, and an intermediate ring $T$ of $R/S$ is $\mathfrak{G}$-regular. If $\mathfrak{G} = \mathfrak{G}|T$, $T/S$ is said to be regularly embedded in $R/S$.

§ 2. Cyclic extension of characteristic $p$ with respect to $\mathfrak{G}$ of order $p^{\mathfrak{s}}$.

Throughout the present section, we assume that $S$ is of characteristic $p$. One of the principal theorem of this section is the following.

Theorem 2.1. (a) In order that $S$ has a $p$ dimensional cyclic extension, it is necessary and sufficient that there exist a derivation $D$ of $S$ and an element $s \in S$ such that (1) $D^{p} - D = I_{s}$, $sD = 0$, and (2) $X^{p} - X - s$ is irreducible in $\mathfrak{G} = S[X; D]$. More precisely, if there exist $D$, $s$ satisfying (1), (2) then $M = (X^{p} - X - s)\mathfrak{G}$ is a maximal ideal, $R^{*} = S[y] = \mathfrak{G}/M$ is a $p$ dimensional cyclic extension of $S$ with a generating automorphism $\sigma^{*}$ defined by $y\sigma^{*} = y + 1$, and $D = I_{y}S$, where $y$ is the residue class of $X$ modulo $M$. Conversely, if $R$ is a $p$ dimensional cyclic extension of $S$ w.r.t. $\mathfrak{G} = \langle \sigma \rangle$, then we can find such $D$, $s$ satisfying (1), (2) that there holds an $S$-isomorphism $\varphi^{*} : R^{*} \cong R$ with $\varphi^{*} \cdot \sigma = \sigma^{*} \cdot \varphi^{*}$.

(b) In order that $S$ has a $p$ dimensional outer cyclic extension, it is necessary and sufficient that there exist $D$ and $s$ satisfying (1), (2) and (3) $D|Z = 0$. 

(c) In order that S has a p dimensional inner cyclic extension, it is necessary and sufficient that there exist D and s satisfying (1) and (4) $zD=z$ for some $z\in Z$.

Proof. (a) and (b). To be easily verified, (1) is equivalent with $X^p - X - s \in V(S)$, and so (2) implies the maximality of $M$ (§1, (v)). Hence, $R^* = \sum y^i S$ is a simple ring and $\{1, y, \ldots, y^{p-1}\}$ forms a linearly independent $S$-basis of $R^*$. Noting that $X^p - X - s$ is left invariant by $\Phi : \sum Xs_r \rightarrow \sum (X + 1)s_r$, we see that $\Phi$ induces in $R^*$ an $S$-automorphism $\sigma^*$ of order $p$ such that $ys^* = y + 1$. If $(\sum y^i s_i) \cdot \sigma^* = \sum y^i s_i$, then $\sum (y + 1)^i s_i = \sum y^i s_i$ yields $\left(\frac{p-1}{p-2}\right)s_{p-1} + s_{p-2} = s_{p-1}$, and hence $s_{p-1} = 0$. Repeating the same procedure, we readily obtain $s_{p-1} = \cdots = s_1 = 0$, namely, $J(\sigma^*, R^*) = S$. Obviously, $\sigma^*$ is inner or outer. If $\sigma^*$ is inner: $\sigma^* = \tilde{z}$, then $z$ is contained $V_R(S) \cap S = Z$ and $z^p \in C^* = V_R(R^*)$, whence we see that $C^*[x]$ is a subfield of $Z$. Moreover, one may remark that $yz = y + 1$ implies $zD = z \neq 0$, and so $D|Z \neq 0$. While, if $\sigma^*$ is outer then $\sigma^*$ is obviously an $F$-group and $D|Z = I_y | S \cap C^* = 0$. Conversely, assume that $R/S$ be a $p$ dimensional cyclic extension w.r.t. $\mathfrak{S} = (\sigma)$. Then, in virtue of (ix) of §1, there exists an element $\in R$ such $x = x + 1$, and then it is easy to see that $R = S[X] = \sum y^i s_i S$, $s = x^p - x \in S$, and $D = I_y | S$ is a derivation in $S$. To be easily seen, $X^p - X - s$ is contained in the center of $\mathfrak{S}$. Since $\varphi : \sum Xs_r \rightarrow \sum x^i s_r$ is an $S$-ring homomorphism of $\mathfrak{S}$ onto $R$ whose kernel contains $M$ and $[\mathfrak{S}/M : S] = p$, $\varphi^* : y^j s_i \rightarrow x^i s_i$ is an $S$-isomorphism of $R^*$ onto $R$ such that $\varphi^* \cdot \sigma = \sigma^* \cdot \varphi^*$. Hence, $M$ is maximal, and so $X^p - X - s$ is $w$-irreducible, completing the proof of (a). Now, (b) is obvious by the above proof.

(c) By the above proof, it suffices to prove that $X^p - X - s$ is $w$-irreducible. If $g$ is a proper monic left divisor of the central monic polynomial $X^p - X - s$, then $\deg g = m < p$ and $gI_z = m! z \neq 0$ (§1, (i)), which proves $g = e$, namely, $X^p - X - s$ is $w$-irreducible.

Corollary 2.1. The following conditions are equivalent to each other:

1. $S$ has a $p$ dimensional trivial cyclic extension.
2. There exists an element $s \in Z$ such that $X^p - X - s$ is irreducible in $Z[X]$.
3. There exist an inner derivation $D$ and $s$ satisfying (1), (2) in Theorem 2.1.

Proof. (1)$\rightarrow$(2). If $R$ is a $p$ dimensional trivial cyclic extension of $S$ w.r.t. $(a)$, then $C$ is a $p$ dimensional cyclic extension field of $Z$. Hence, there exists an element $s \in Z$ such that $X^p - X - s$ is irreducible in $Z[X]$.

(2)$\rightarrow$(3). If we set $D = 0$, our implication is trivial.
(3) → (1). If $D = I_x$, for some $s' \in S$, then $c = y - s'$ is contained in the center $C^*$ of $R^*$, and $\sigma^*c = c + 1$. Hence, $R^* = \sum_{i=0}^{p-1} c_i S = S \otimes x C^*$.

**Corollary 2.2.** If $R/S$ is an abelian extension w.r.t. $\mathfrak{G}^9$ of dimension $p^r$, and $Z$ is perfect, then it is outer. If moreover, $[S:Z]<\infty$ then it is trivial, in particular, if $S = Z$ then $R = C$.

**Proof.** Since any derivation in the perfect field $Z$ is 0, the case $e = 1$ is obvious by Theorem 2.1. Assume now $e > 1$ and the validity of our assertion for $e - 1$. If $\mathfrak{G}$ contains an inner automorphism different from 1, then $\mathfrak{G}$ contains an inner $F$-group $\mathfrak{G}$ of order $p$ ($\S 1$, (viii)) and $T = J(\mathfrak{G}, R)$ is abelian w.r.t. $\mathfrak{G}(T)^9$. Noting here that $T/S$ is outer Galois by induction hypothesis, we see that the center of $T$ is perfect, and hence $R/T$ is outer, which is a contradiction. The second one is a direct consequence of the former and (xi) of $\S 1$.

**Corollary 2.3.** Assume that $S$ is a division ring. In order that $S$ has a $p$ dimensional cyclic division ring extension, it is necessary and sufficient that there exist $D$ and $s$ satisfying (1) in Theorem 2.1 and (2') $X^p - X - s$ is irreducible. The precise statement corresponding to that in Theorem 2.1 is valid.

**Proof.** Since (1) and (2') imply that $M$ is a maximal ideal of an integral domain $\mathfrak{G}$, $R^*$ is a division ring.

**Corollary 2.4.** (a) $S$ has a $p$ dimensional parallel cyclic extension if and only if there exist $D$, $s$ satisfying (1), (2) in Theorem 2.1 and (3) there exists a simple subring $W$ of $S$ containing $s$ such that $WD \subseteq W$ and $X^p - X - s$ is $w$-irreducible in $W[X; D]$.

(b) $S$ has a $p$ dimensional $d$-parallel cyclic extension if and only if there exist $D$, $s$ satisfying (1), (2) in Theorem 2.1 and (3') there exists a division subring $W$ of $S$ containing $s$ such that $WD \subseteq W$ and $X^p - X - s$ is irreducible in $W[X; D]$.

(c) $S$ has a $p$ dimensional $f$-parallel cyclic extension if and only if there exist $D$, $s$ satisfying (1), (2) in Theorem 2.1 and (3'') there exists a subfield $W$ of $S$ containing $s$ such that $WD = 0$ and $X^p - X - s$ is $w$-irreducible in $W[X; D]$.

**Proof.** (a) If $T^*$ is the subring of $R^*$ consisting of all the elements $\sum_{i=0}^{p-1} y_i s_i$ with $s_i \in W$, then $R^* = S[T^*]$ and $T^*$ is $W$-isomorphic to the simple ring $W[X; D]/M_w$, where $M_w = (X^p - X - s)W[X; D]$ (Theorem 2.1). Since $\sigma^*[T^*]$ is an automorphism of $T^*$ with $J(\sigma^*[T^*, T^*]) = T^* \cap S = W$, $T^*/T^* \cap S$

---

8) $R/S$ is called an abelian extension w.r.t. $\mathfrak{G}$ if $R/S$ is $\mathfrak{G}$-regular and $\mathfrak{G}$ is abelian.
9) $\mathfrak{G}(T) = \{ \sigma \in \mathfrak{G}; t \sigma = t \text{ for all } t \in T \}.$
is $(\sigma^*|T^*)$-regular again by Theorem 2.1. Conversely, if $R=S[T]$ is a $p$ dimensional parallel cyclic extension of $S$ w.r.t. $(\sigma)$, then $T/T\cap S$ is a $p$ dimensional cyclic extension w.r.t. $(\sigma|T)$. Hence, there exists $t \in T$ with $t\sigma=t+1$ ($\S$ 1, (ix)). If $D=I_t|S$, $s=t^p-t$ and $W=T\cap S$, then our assertion is easy by the proof of Theorem 2.1.

(b) Combining (a) with Corollary 2.3, we readily obtain (b).

(c) Noting that $W[X;D]=W[X]$ by $WD=0$, the proof is obvious by the proof of (a).

If $S$ is a field and has a $p$ dimensional cyclic extension field, then, as is well known, $S$ has a $p^e$ dimensional cyclic extension field for each positive integer $e$. However, as was referred to in [2], the same will be seemed no longer valid for simple rings. Concerning the regular embedding of a $p^e$ dimensional cyclic extension, we can prove following theorem.

**Theorem 2.2.** Let $T/S$ be a cyclic extension w.r.t. $\phi=(\tau)$ of order $p^e$. In order that $T$ is regularly embedded in some $p^{e+1}$ dimensional cyclic extension $R/S$, it is necessary and sufficient that there exist a derivation $D$ in $T$ and elements $a, b \in T$ such that (1) $D^p-D=I_a$, $aD=0$, (2) $X^p-X-a$ is w-irreducible in $T[X;D]$, (3) $\tau^{-1}D\cdot\tau-D=I_b$, (4) $T\psi(b)\neq 0$, and (5) $A_p(b)-b=a(\tau-1)$.

**Proof.** By (iii) of $\S$ 1, (3) means that $\phi: \sum X^\nu t_{\nu} \rightarrow \sum (X+b)^\nu(t, \tau)$ defines in $\mathfrak{T}=T[X;D]$ an automorphism, whose order is $p^{e+1}$ by (4). Next, (1) and (2) shows that $M=(X^p-X-a)\mathfrak{T}$ is a maximal ideal and $R^*=\mathfrak{T}/M$ is a $p$ dimensional simple ring extension of $T$ (Theorem 2.1). By a brief computation with (5) and (ii) of $\S$ 1, we can see that $X^p-X-a$ is left invariant by $\phi$, and hence $\phi$ induces in $R^*$ an $S$-automorphism $\sigma^*$ of order $p^{e+1}$ such that $y\sigma^*=y+b$ and $\sigma^*|T=\tau$, where $y$ is the residue class of $X$ modulo $M$. If $\sum y^i t_i=(\sum y^i t_i)\tau^p$ then $\sum y^i t_i=\sum (y+T_\phi(b))^i (t_i)=\sum s\Delta(A^p(b))(t_i)$, whence it follows $t_{p-2}=\cdots=t_{p-1}=0$. Since $sT_\phi(b)-T_\phi(b)=T_\phi(s\bar{b}-bs)=T_\phi(s(\tau^{-1}D\cdot\tau-D))=T_\psi(sD\tau-sD)=0$ for each $s \in S$, $T_\phi(b)$ is an element of $Z^*$, and so we obtain $t_{p-1}=0$. Repeating the same arguments, we readily obtain $t_{p-1}=\cdots=t_{1}=0$, which proves evidently $J(\sigma^*|R^*)=T$. Hence, $R^*/T$ is a cyclic extension w.r.t. $(\sigma^*|R^*)$ and $J(\sigma^*, R^*)=J(\sigma^*|T, T)=S$. If $R^*/T$ is outer, the unique minimal subgroup $(\sigma^*|R^*)$ of $\phi=(\sigma^*)$ is outer, and hence so is $\phi$ itself. On the other hand, if $R^*/T$ is inner then $T$ contains the center $C^*$ of $R^*$ and there exists a divisor $p^g$ of $p^e$ such that $\sigma^*|C^*\cong\mathfrak{G}$, $\nu \in V^*=V_{R^*}(S)$ and $\sigma^*|C^*=\nu^*$ for each positive $i<p^g$. Obviously, $\nu$ is contained in $J(\tilde{\sigma}^{e-q}, R^*) \cap V^*=J(\sigma^*|R^*) \cap V^*=T \cap
V^* = V_T(S). Since V_T(S) is a field (§1, (viii)), C^*[v] is its subfield. Hence, in either case, G is an F-group. Conversely, assume that T is regularly embedded in a cyclic extension R/S w. r. t. G = <a> of order \rho^{r+1}|s|T = \tau. Since V is a field (§1, (vii)) and [R : T] = \rho, R/T is cyclic w. r. t. G(T) = \langle a^r \rangle. Then, there exists an element \epsilon \in R such that x \rho^{r+1} - x = 1 (§1, (ix)). Evidently, b = x \sigma - x is contained in T and T_\varphi(b) = 1. Moreover, one will easily see that I_\epsilon induces a derivation D in T. If we set a = x^p - x then, pattern the proof after the proof of Theorem 2.1, one will easily complete the proof.

§ 3. Cyclic extension of characteristic 0 or prime \rho not dividing the extension dimension.

Throughout the present section, we assume that Z contains a primitive m-th root \zeta of 1, and a cyclic extension R of S will mean such one that the center C of R contains \zeta. At first, we shall deal with an m dimensional cyclic extension of S.

**Lemma 3.1** Let \rho be an automorphism of S. If there exists \zeta_0 \in Z with \zeta_0 \rho = \zeta_0 \zeta, then any polynomial in S[X; \rho] of degree at most m − 1 with the non-zero constant term generates S[X; \rho].

**Proof.** Let \textit{f} = X^k s_k + \cdots + s_0 \in S[X; \rho] \ (0 \leq k < m, s_0 \neq 0). Since the constant term of \textit{z}_0 \textit{f} - \textit{f} \zeta_0^k is \textit{s}_0 \zeta_0 (1 - \zeta^k) \neq 0 and \textit{deg} \ (\textit{z}_0 \textit{f} - \textit{f} \zeta_0^k) < k, an easy induction will complete the proof.

The next corresponds to Theorem 2.1.

**Theorem 3.1.** (a) In order that S has an m dimensional cyclic extension, it is necessary and sufficient that there exist an automorphism \rho of S and \textit{s}_0 \in S^* such that (1) \rho^m = \textit{z}_0^{-1}, s_0 \rho = \textit{s}_0, \zeta_0 \rho = \zeta_0, and (2) X^k - \textit{s}_0 is \textit{w}-irreducible in S = S[X^k; \rho^k], where \omega ranges over all the positive divisor of m and \omega' = m/k. More precisely, if there exist \rho, \textit{s}_0 satisfying (1), (2), then M = (X^m - \textit{s}_0) S is maximal ideal of E = S[X; \rho] and R* = S[\text{y}] = \mathfrak{S}/M is a cyclic extension of S with a generating automorphism \varphi* of order m defined by \textit{y} \varphi* = \textit{y} \zeta_0, where \textit{y} is the residue class of X modulo M. Conversely, if R/S is an m-dimensional cyclic extension w. r. t. \mathfrak{G} = \langle a \rangle, then we can find \rho, \textit{s}_0 satisfying (1), (2) that there holds an S-isomorphism \varphi*: R* \cong R with \varphi* \cdot \sigma = \sigma^* \cdot \varphi*.

(b) In order that S has an m dimensional outer cyclic extension, it is necessary and sufficient that there exist \rho and \textit{s}_0 satisfying (1), (2) and (3) if \rho^i = \textit{z}_0 \textit{s}_0 then \textit{s}_0 = \textit{s}.

(c) In order that S has an m dimensional inner cyclic extension, it is necessary and sufficient that there exist \rho and \textit{s}_0 satisfying (1) and (4) \textit{z}_0 \rho = \textit{z}_0 \zeta_0 for some \textit{z}_0 \in Z^*.
Proof. (a) and (b). Let $k$ be an arbitrary positive divisor of $m$, and $k' = m/k$. To be easily seen, $\rho'^{m} = \tilde{z}_{0}^{v}$ and $s_{0} \rho = s_{0}$ imply that $X^{k}s_{0}^{-1} - 1$ is contained in the center of $\mathcal{O}_{k} = S[X; \rho^{k}]$, and conversely. Hence, by (2), $M_{k} = (X^{k}s_{0}^{-1} - 1) \mathcal{O}_{k} = (X^{k}-s_{0}) \mathcal{O}_{k}$ is maximal, and so $R_{k}^{*} = S[y_{k}] = \mathcal{O}_{k}/M_{k}$ is simple ring and $\{1, y_{k}, y_{k}^{2}, \cdots, y_{k}^{k-1}\}$ forms an $S$-basis of $R_{k}^{*}$, where (regular) $y_{k}$ is the residue class of $X$ modulo $M_{k}$. Since $X^{k}-s_{0} \in \mathcal{O}_{k}$ is left invariant by the automorphism $\psi_{k} : \sum X^{k}s_{k} \rightarrow \sum (X^{k}s_{k})^{i}s_{i} (\S, (iv))$, $\psi_{k}$ induces in $R_{k}^{*}$ an $S$-automorphism $\sigma_{k}^{*}$ of order $k$ such that $\rho^{i} = y_{k}^{v}$ and $J(\sigma_{k}^{*}, R_{k}^{*}) = S$. Now, let $k$ be especially the least positive integer such that $\sigma_{m}^{*} = \tilde{v}$. If $\sigma = \sigma_{m}^{*}$, $y = y_{m}$ and $R^{*} = R_{m}^{*}$, then $T^{*} = J(\sigma^{*}, R^{*}) = \sum y^{k}S$. Noting here that $R_{k}^{*}$ is a simple ring, we see that $\sigma^{*} : \sum y_{k}s_{k} \rightarrow \sum y_{k}^{k}s_{i}$ defines an $S$-isomorphism of $R_{k}^{*}$ onto $T^{*}$. Since $v$ is contained in $J(\tilde{v}, R^{*}) \cap V_{R^{*}}(T^{*}) = V_{R^{*}}(T^{*})$ and $y^{k'} \in C^{*} = V_{R^{*}}(R^{*})$, $C^{*}[v]$ is a subfield of the center of the simple ring $T^{*}$, which proves that $\sigma^{*}$ is an $F$-group. Needless to say, $\zeta y = y(\zeta \rho) = y \zeta$, namely, $\zeta$ is contained in $C^{*}$. Now, let $s = \sum y^{k}u_{i}$ ($u_{i} \in S$) be an arbitrary non-zero element of $V^{*} = V_{R^{*}}(S)$. Since $y^{k}S = Sy^{k}$, every $y^{k}u_{k}$ is contained in $V^{*}$. Hence, if $u_{i}$ is non-zero then $(y^{k}u_{i})S = S(y^{k}u_{i})S = y^{k}(S \rho^{i})u_{i}S = y^{k}S$, where we see that $u_{i}$ is regular and $\rho^{i} = \tilde{u}_{i}$. Accordingly, if (3) is satisfied then $u_{i} \rho = u_{i}$, which proves obviously $V^{*} = C^{*}$. Conversely, assume that $R/S$ is an $m$ dimensional cyclic extension w.r.t. $G = \langle \sigma \rangle$. Then, there exists $x \in R^{*}$ such that $x \sigma = x \zeta$ and $R = \sum x^{-1}x^{k}S$ is a direct sum by $\S, (x)$ and [10, Corollary 1]. If we set $\rho = \tilde{x}^{-1}|S$ and $s_{0} = x^{n}$, one will easily see that $\rho$ is an automorphism of $S$, $s_{0}$ is in $S$, and (1) is satisfied. Moreover, if $k$ is an arbitrary positive divisor of $m$, then $X^{k}s_{0}^{-1} - 1$ is contained in the center of $\mathcal{O}_{k}$ and $R_{k}$ is isomorphic to the simple ring $J(\sigma_{k}, R) = \sum x^{k}S$, which proves (2). Finally, assume that $R/S$ is outer and $\rho^{k} = \tilde{s}$. By the validity of (1), we may assume that $0 \leq i < m$. Since $\rho^{i} = \tilde{x}^{-1}|S$, it follows $x^{i}s \in V = C$, and so $x^{i+1}s = x^{i+1}s$, namely $s\rho = s$.

(c) Under the above notations, the monic polynomial $X^{m} - s_{0}$ is irreducible by Lemma 3.1. Since $x_{0}y = y(\zeta x_{0}) \cdot \zeta^{-1} = y \zeta$, we obtain $\sigma^{*} = \tilde{z}_{0}$. Accordingly, $V = J(\tilde{z}_{0}, V, V)$ coincides with the field $Z$. Hence $\langle \sigma^{*} \rangle = \langle \tilde{z}_{0} \rangle$ is an $F$-group. Conversely, assume that $R/S$ is an $m$ dimensional inner cyclic extension w.r.t. $G = \langle \tilde{z}_{0} \rangle$. Noting here that $V = Z$, $z_{0}$ is in $Z$ and $z_{0} \rho = x^{-1}z_{0}x = x^{-1}(x \tilde{z}_{0})z_{0} = x^{-1}(x \zeta)z_{0} = x_{0} \zeta$.

Corollary 3.1. The following conditions are equivalent to each other:

(1) $S$ has an $m$ dimensional trivial cyclic extension.

(2) There exists an element $z_{0}$ in $Z$ such that $z_{0}^{m}$ is not contained in $Z$. 
(3) There exist an inner automorphism $\rho$ of $S$ and $z_0$ in $S^*$ satisfying (1), (2) in Theorem 3.1.

Proof. The implication (1)$\implies$(2)$\implies$(3) are obvious. (Note that $\zeta$ is contained in $Z$).

(3)$\implies$(1). Under the notations in the proof of Theorem 3.1, if $\rho=\frac{s}{t}$ then $c=ys$ is contained in $C^*$ and $c\rho=c\zeta$. Hence, $R=S[c]=S\otimes_sc^*C^*$.

The next corollary will be almost evident and it corresponding to Corollary 2.3.

Corollary 3.2. Let $S$ be a division ring. In order that $S$ has an $m$-dimensional cyclic division ring extension, it is necessary and sufficient that there exist $\rho, s_0$ satisfying (1) in Theorem 3.1 and (2') $X^m-s_0$ irreducible in $S[X; \rho]$. The precise statement corresponding to that in Theorem 3.1 is valid.

Concerning parallel extensions of the present types, we have

Corollary 3.3. (a) $S$ has an $m$ dimensional parallel cyclic extension if and only if there exist $\rho, s_0$ satisfying (1), (2) in Theorem 3.1 and (3) there exists a simple subring $W$ of $S$ containing $s_0$ such that $W\rho \subseteq W$, $V_w(W) \ni \zeta$ and $X^k-s_0$ is $w$-irreducible in $W[X; \rho^k]$, where $k$ ranges over all the positive divisor of $m$ and $k'=m/k$.

(b) $S$ has an $m$ dimensional $d$-parallel cyclic extension if and only if there exist $\rho, s_0$ satisfying (1), (2) in Theorem 3.1 and (3') there exists a division subring $W$ of $S$ containing $s_0$ such that $W\rho \subseteq W$, $V_w(W) \ni \zeta$ and $X^m-s_0$ is irreducible in $W[X; \rho]$.

(c) $S$ has an $m$ dimensional $f$-parallel cyclic extension if and only if there exist $\rho, s_0$ satisfying (1), (2) in Theorem 3.1 and (3'') there exists a subfield $W \ni \zeta$, $S$ contains $s_0$ such that $\rho\mid W=1$ and $X^m-s_0$ is $w$-irreducible in $W[X; \rho]$.

Proof. (a) is almost evident, and irreducibility (resp. $w$-irreducibility) of only $X^m-s_0$ in (b) (resp. in (c)) is valid from Corollary 3.2.

Corresponding to Theorem 2.2, the regular embedding problem for the present case is solved in the following way.

Theorem 3.2. Let $T/S$ be an $m'$ dimensional cyclic extension w.r.t. $\Phi=\tau$ such that $V_{\tau}(T) \ni \zeta$. In order that $T/S$ is regularly embedded in some $m'm$ dimensional cyclic extension, it is necessary and sufficient that there exist an automorphism $\rho$ of $T$ and regular elements $t_0, t$ of $T$ such that (1) $\rho^m=t_0^{-1}$, $t_0\rho=t_0$, $\zeta\rho=\zeta$, (2) $X^m-t_0$ is $w$-irreducible in $T[X; \rho]$, (3) $\tau^{-1}\cdot \rho^{-1}\cdot \tau\cdot \rho = t_0$, (4) $\iota f N_m(t_0; \tau)=\zeta$, (5) $t\tau=tLN_m(t, \rho)$, and (6) if $(u_0, u_1, \cdots, u_{m-1})$ is a non-zero $1 \times m$ matrix with entries in $T$ and $s\rho^i u_t=u_s$ for all $s\in S$ ($i=0,1,\cdots,m-1$),
then the simultaneous equations \( \sum_{\delta} k_{\delta} u_{k-\delta} \rho^{\delta} \omega_{\delta} + \sum_{i=k+1}^{m-1} t_{0} u_{m+k-\epsilon} \rho^{i} \omega_{i} = \delta_{0k} \) \( (k = 0, 1, \ldots, m-1) \) have a solution in \( T \).

**Proof.** By (iv) of §1, (3) means that \( \psi: \sum X^{i} t_{i}^{' \epsilon} \rightarrow \sum (X t_{i})^{' \epsilon} (t_{i} \sigma) \) defines in \( \mathcal{X} = T[X; \rho] \) an automorphism, whose order is \( m^{\prime}m \) by (4). Next, (1) and (2) show that \( M=(X^{m}-t_{0}) \mathcal{X} \) is a maximal ideal of \( \mathcal{X} \), \( R^{*}=\mathcal{X}/M \) is a simple ring with \( \{1, y, \ldots, y^{m-1}\} \) as an \( S \)-basis, where \( y \) is the residue class of \( X \) modulo \( M \). Since (5) implies that \( X^{m}-t_{0} \) is left invariant by \( \psi \), \( \psi \) induces in \( R^{*} \) an \( S \)-automorphism \( \sigma^{*} \) of order \( m^{\prime}m \) such that \( y \sigma^{*} = y t_{i} \) and \( \sigma^{*}|T = \tau \). To be easily seen, \( J(\sigma^{*}, R^{*}) = T \), and so \( J(\sigma^{*}, R^{*}) = S \). Finally, if \( v = \sum y^{i} u_{i} \) is a non-zero element of \( V_{R^{*}}(S) \) then \( t_{0} u_{i} = u_{i} t \) and (6) secures the existence of the inverse of \( v \), which means that \( V_{R^{*}}(S) \) is a division ring.

Conversely, assume that \( T/S \) is regularly embedded in some \( m^{\prime}m \) dimensional cyclic extension \( R/S \) w. r. t. \( \Theta = (\sigma) \), and set \( \tau = \sigma|T \). Since \( V \) is a field (§1, (vii)) and \( [R: T] = m \), \( R/T \) is cyclic extension w. r. t. \( \Theta(T) = (\sigma^{m}) \). Then, there exists an element \( x \in R^{*} \) such that \( x \sigma^{m} = x \zeta \) (§1, (x)). Evidently, \( t_{1} = \tilde{x}^{-1} \cdot x \sigma \) is contained in \( T \) and \( RN_{m}(t_{1}; \tau) = x^{-1}x \sigma^{m} = \zeta \). Moreover, \( \tilde{x}^{-1} \) induces an automorphism \( \rho \) of \( T \). If we set \( t_{0} = \tilde{x} \zeta \) then, patterning after the proof of Theorem 3.1, we can easily see that the validity of the conditions (1), (2), (3), (5) and (6).

The condition (6) in Theorem 3.2 was needed only to see that the centralizer of \( S \) in the extension considered is simple. Accordingly, combining Theorem 3.2 with Corollary 3.2, we readily obtain the following:

**Corollary 3.4.** Let \( T/S \) be an \( m^{\prime} \) dimensional cyclic division ring extension w. r. t. \( \Theta = (\sigma) \) such that \( V_{R}(T) \ni \zeta \). In order that \( T/S \) is regularly embedded in some \( m^{\prime}m \) dimensional cyclic division ring extension, it is necessary and sufficient that there exist an automorphism \( \rho \) of \( T \) and non zero element \( t_{0}, t_{1} \) of \( T \) such that \( (1) \rho^{m} = \tilde{t}_{0}^{-1}, t_{0} \rho = t_{0}, \zeta \rho = \zeta, (2) X^{m}-t_{0} \) is irreducible in \( T[X; \rho] \), \( (3) \tilde{\sigma^{-1}} \rho^{-1} \cdot \tilde{\sigma} \rho = \tilde{t}_{1}, (4) RN_{m}(t_{1}; \tau) = \zeta \), and \( (5) t_{0} \sigma = t_{0} \rho N_{m}(t_{1}; \rho) \).

**References**


On Cyclic Extensions of Simple Rings


Hokkaido Gakugei University

(Received November 15, 1965)