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 prmie 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 rings[1] 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 ρ be an automorphism of a ring A and D *a* ρ*-derivation*[2] 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* $g = \sum X^\nu a_\nu$ *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* $(X+a)^n = \sum_{k=0}^{n} \binom{n}{k} X^{n-k} \Delta_k(a)$ *in* $A[X; D]$, *where* $\Delta_0(a) = 1$ *and* $\Delta_k(a) = (\Delta_{k-1}(a))D + (\Delta_{k-1}(a))a$[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

2) Cf. [6] p. 171.

3) Cf. [5] p. 223.

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

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

Indeed, Φ is an endomorphism if and only if $b\Phi X\Phi = (Xb+bD)\Phi$ and hence $b\tau \cdot (X+a) = X(b\tau) + (b\tau)D + b\tau \cdot a = (X+a)b\tau + (bD)\tau$, consequently, $b(D\tau - \tau D) = (b\tau)a - a(b\tau) = b \cdot \tau I_a$ for each $b \in A$. If $(\sum_{\nu=0}^{n} X^\nu a_\nu)\Phi = \sum_{\nu=0}^{n} (X+a)^\nu (a_\nu \tau) = \sum_\nu (\sum_{\mu=0}^{\nu} \binom{\nu}{\mu} X^{\nu-\mu} \Delta_\mu(a))(a_\nu \tau) = 0$ then $a_n \tau = \Delta_1(a) a_n \tau + a_{n-1}\tau = \binom{n}{2} \Delta_2(a) a_n \tau + \binom{n-1}{1} \Delta_1(a) a_{n-1}\tau + a_{n-2}\tau = \cdots = \binom{n}{n-1} \Delta_{n-1}(a) a_n \tau + \binom{n-1}{n-2} \Delta_{n-2}(a) a_{n-1}\tau + \cdots + \Delta_1(a) a_1 \tau + a_0 \tau = 0$. Thus, Φ is an automorphism.

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

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

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

Let $\mathfrak{S} = S[X; \rho, D]$ such that ρ 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 *w-irreducible*. If g is central (i. e. $g \in V_{\mathfrak{S}}(\mathfrak{S})$) and irreducible then it is w-irreducible while the converse is not true[4], and if S is a field[5]

4) Let S be the ring of 2×2 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 $X^2 + X + 1 = (X + e_{12} + e_{21} + e_{22})(X + e_{11} + e_{12} + e_{12})$. 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 $s \in V_S(S) = GF(2)$. Thus, $X^2 + X + 1$ is central and w-irreducible, but not irreducible.

5) Throughout the present paper, "field" means a commutative field.

and $\mathfrak{S}=S[X]$ then the notion of w-irreducibility coincides with that of irreducibility.

(v) *A non-zero ideal I of $\mathfrak{S}$ 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 $[R:S]\leqq\sharp\mathfrak{G}$ (order of $\mathfrak{G}$)* [9, Lemma 2].

If $\mathfrak{G}$ is an F-group and $[R:J(\mathfrak{G}, R)]=\sharp\mathfrak{G}$, $R/J(\mathfrak{G}, R)$ 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 $\mathfrak{G}=(\sigma)$, 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 than $R=C$. If γ is the order or $\sigma|C$[6] then $\sigma^{\gamma}=\tilde{v}$ with some v. Since $c'=v\sigma\cdot v^{-1}\in C$ by $\sigma\tilde{v}=\tilde{v}\sigma$ and there holds $N_{C/C\cap S}(c')=\prod_0^{\gamma-1}c'\sigma^i=1$, it is well known that there exists an element $c\in C$ such that $c'^{-1}=c^{-1}\cdot c\sigma$. Setting here $z=vc$, we see that $\tilde{\sigma}=\tilde{z}$ 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 $\frac{1}{p}\mathfrak{G}$ and V coincides with the field $C[Z]$* [7, Theorem 5].

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

(ix) *If $\sigma\to s_\sigma$ 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 σ in $\mathfrak{G}$* [10, Corollary 3].

(x) *If $\sigma\to s_\sigma$ is an anti-homomorphism of $\mathfrak{G}$ into $S^{\cdot}$*[7], *then there exists an element x in $R^{\cdot}$ such that $s_\sigma=x^{-1}x\sigma$ for all σ 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 σ to C.

7) Let $A(\ni 1)$ be a ring. Then, $A^{\cdot}$ 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, $R=S\otimes_Z C$. 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 $S[C]=S\otimes_Z C$ 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 $\sharp\mathfrak{G}=p^e$. 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, $R=S[C]=S\otimes_Z C$. The converse is obviously true.

Let R/S be $\mathfrak{G}$-regular, and an intermediate ring T of R/S is $\mathfrak{H}$-regular. If $\mathfrak{H}=\mathfrak{G}|T$, 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^e.

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 w-irreducible in $\mathfrak{S}=S[X;D]$. More precisely, if there exist D, s satisfying* (1), (2) *then $M=(X^p-X-s)\mathfrak{S}$ is a maximal ideal, $R^*=S[y]=\mathfrak{S}/M$ is a p dimensional cyclic extension of S with a generating automorphism σ^* 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. $\mathfrak{G}=(\sigma)$, 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 $X^p-X-s\in V_{\mathfrak{S}}(\mathfrak{S})$, and so (2) implies the maximality of M (§1, (v)). Hence, $R^*=\sum_0^{p-1}y^iS$ is a simple ring and $\{1, y, \cdots, y^{p-1}\}$ forms a linearly indpendent S-basis of R^*. Noting that X^p-X-s is left invariant by $\Phi: \sum X^\nu s_\nu \to \sum (X+1)^\nu s_\nu$, we see that Φ induces in R^* an S-automorphism σ^* of order p such that $y\sigma^*=y+1$. If $(\sum_0^{p-1}y^is_i)\cdot\sigma^*=\sum_0^{p-1}y^is_i$ then $\sum_0^{p-1}(y+1)^is_i=\sum_0^{p-1}y^is_i$ yields $\binom{p-1}{p-2}s_{p-1}+s_{p-2}=s_{p-2}$, 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, (σ^*) is inner or outer. If σ^* 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 $C^*[z]$ is a subfield of Z. Moreover, one may remark that $y\tilde{z}=y+1$ implies $zD=z\neq 0$, and so $D|Z\neq 0$. While, if σ^* is outer then (σ^*) 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. $\mathfrak{G}=(\sigma)$. Then, in virtue of (ix) of §1, there exists an element $x\in R$ such that $x\sigma=x+1$, and then it is easy to see that $R=S[x]=\sum_0^{p-1}x^iS$, $s=x^p-x\in S$, and $D=I_x|S$ is a derivation in S. To be easily seen, X^p-X-s is contained in the center of $\mathfrak{S}$. Since $\varphi: \sum X^\nu s_\nu \to \sum x^\nu s_\nu$ is an S (-ring) homomorphism of $\mathfrak{S}$ onto R whose kernel contains M and $[\mathfrak{S}/M: S]=p$, $\varphi^*: \sum y^is_i \to \sum x^is_i$ 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 $gI_z^m=m!z\neq 0$ (§1, (i)), which proves $(g)=\mathfrak{S}$, 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)→(2). If R is a p dimensional trivial cyclic extension of S w.r.t. (σ), 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)→(3). If we set $D=0$, our implication is trivial.

(3)→(1). If $D=I_{s'}$ for some $s'\in S$, then $c=y-s'$ is contained in the center C^* of R^*, and $c\sigma^*=c+1$. Hence, $R^*=\sum_0^{p-1}c^iS=S\otimes_Z C^*$.

Corollary 2.2. *If R/S is an abelian extension w.r.t. $\mathfrak{G}$[8] of dimension p^e, 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 $\mathfrak{H}$ of order p (§1, (viii)) and $T=J(\mathfrak{H},R)$ 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 §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 statment 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 $\mathfrak{S}$, 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 $WD\subseteqq W$ 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 $WD\subsetneqq W$ 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 $\sum_0^{p-1}y^is_i$ 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. (σ), then $T/T\cap S$ is a p dimensional cyclic extension w.r.t. $(\sigma|T)$. Hence, there exists $t\in T$ with $t\sigma=t+1$ (§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 refered 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. $\mathfrak{H}=(\tau)$ 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) $\tau^{-1}\cdot D\cdot\tau-D=I_b$, (4) $T_{\mathfrak{H}}(b)\neq 0$, *and* (5) $\Delta_p(b)-b=a(\tau-1)$.

Proof. By (iii) of §1, (3) means that $\Phi:\sum X^\nu t_\nu\to\sum(X+b)^\nu(t_\nu\tau)$ 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 §1, we can see that X^p-X-a is left invariant by Φ, and hence Φ induces in R^* an S-automorphism σ^* 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 $\sum y^it_i=(\sum y^it_i)\tau^{*p^2}$ then $\sum y^it_i=\sum(y+T_{\mathfrak{H}}(b))^it_i=\sum_i(\sum_{k=0}^i\binom{i}{k}y^{i-k}\Delta_k(T_{\mathfrak{H}}(b))t_i$ (§1, (ii)), whence it follows $t_{p-2}=\binom{p-1}{1}\Delta_1(T_{\mathfrak{H}}(b))t_{p-1}+t_{p-2}$, namely, $\binom{p-1}{1}\Delta_1(T_{\mathfrak{H}}(b))t_{p-1}=0$. Since $sT_{\mathfrak{H}}(b)-T_{\mathfrak{H}}(b)s=T_{\mathfrak{H}}(sb-bs)=T_{\mathfrak{H}}(s(\tau^{-1}\cdot D\cdot\tau-D))=T_{\mathfrak{H}}(sD\tau-sD)=0$ for each $s\in S$, $T_{\mathfrak{H}}(b)$ 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 $J(\sigma^{*p^e},R^*)=T$. Hence, R^*/T is a cyclic extension w.r.t. (σ^{*p^e}) and $J(\sigma^*,R^*)=J(\sigma^*|T,T)=S$. If R^*/T is outer, the unique minimal subgroup (σ^{*p^e}) of $\mathfrak{G}=(\sigma^*)$ is outer, and hence so is $\mathfrak{G}$ 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 $\sigma^{*p^g}=\tilde{v}$, $v\in V^*=V_{R^*}(S)$ and $\sigma^{*i}\notin\tilde{V}^*$ for each positive $i<p^g$. Obviously, v is contained in $J(\tilde{v}^{e-g},R^*)\cap V^*=J(\sigma^{*p^e},R^*)\cap V^*=T\cap$

$V^* = V_T(S)$. Since $V_T(S)$ is a field (§1, (vii)), $C^*[v]$ is its subfield. Hence, in either case, $\mathfrak{G}$ is an F-group. Conversely, assume that T is regularly embedded in a cyclic extension R/S w. r. t. $\mathfrak{G}=(\sigma)$ of order $p^{e+1}(\sigma|T=\tau)$. Since V is a field (§1, (vii)) and $[R:T]=p$, R/T is cyclic w. r. t. $\mathfrak{G}(T)=(\sigma^{p^e})$. Then, there exists an element $x\in R$ such that $x\sigma^{p^e}-x=1$ (§1, (ix)). Evidently, $b=x\sigma-x$ is contained in T and $T_{\mathfrak{G}}(b)=1$. Moreover, one will easily see that I_x induces a derivation D in T. If we set $a=x^p-x$ then, patterning after the proof of Theorem 2.1, one will easily complete the proof.

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

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

Lemma 3.1 *Let ρ be an automorphism of S. If there exists $z_0\in Z^*$ with $z_0\rho=z_0\zeta$, 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 $f=X^k s_k+\cdots+s_0\in S[X;\rho]$ $(0\leqq k<m,\ s_0\neq 0)$. Since the constant term of $z_0 f-fz_0\zeta^k$ is $s_0 z_0(1-\zeta^k)\neq 0$ and $deg\ (z_0 f-fz_0\zeta^k)<k$, 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 ρ of S and $s_0\in S^*$ such that* (1) $\rho^m=\tilde{s}_0^{-1}$, $s_0\rho=s_0$, $\zeta\rho=\zeta$, *and* (2) X^k-s_0 *is w-irreducible in $\mathfrak{S}_k=S[X;\rho^{k'}]$, where k ranges over all the positive divisor of m and $k'=m/k$. More precisely, if there exist ρ, s_0 satisfying* (1), (2), *then $M=(X^m-s_0)\mathfrak{S}$ is maximal ideal of $\mathfrak{S}=S[X;\rho]$ and $R^*=S[y]=\mathfrak{S}/M$ is a cyclic extension of S with a generating automorphism σ^* of order m defined by $y\sigma^*=y\zeta$, where y is the residue class of X modulo M. Conversely, if R/S is an m-dimensional cyclic extension w. r. t. $\mathfrak{G}=(\sigma)$, then we can find ρ, 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 ρ and s_0 satisfying* (1), (2) *and* (3) *if $\rho^i=\tilde{s}$ then $s\rho=s$.*

(c) *In order that S has an m dimensional inner cyclic extension, it is necessary and sufficient that there exist ρ and s_0 satisfying* (1) *and* (4) *$z_0\rho=z_0\zeta$ for some $z_0\in Z^*$.*

Proof. (a) and (b). Let k be an arbitrary positive divisor of m, and $k'=m/k$. To be easily seen, $\rho^m=\tilde{s}_0^{-1}$ and $s_0\rho=s_0$ imply that $X^k s_0^{-1}-1$ is contained in the center of $\mathfrak{S}_k=S[X;\rho^{k'}]$, and conversely. Hence, by (2), $M_k=(X^k s_0^{-1}-1)\mathfrak{S}_k=(X^k-s_0)\mathfrak{S}_k$ is maximal, and so $R_k^*=S[y_k]=\mathfrak{S}_k/M_k$ 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 $X^k-s_0\in\mathfrak{S}_k$ is left invariant by the automorphism $\Psi_k:\sum X^i s_i\to\sum(X\zeta^{k'})^i s_i$ (§1, (iv)), Ψ_k induces in R_k^* an S-automorphism σ_k^* of order k such that $y_k\cdot\sigma_k^*=y_k\zeta^{k'}$ and $J(\sigma_k^*,R_k^*)=S$. Now, let k be especially the least positive integer such that σ_m^{*k} is inner: $\sigma_m^{*k}=\tilde{v}$. If $\sigma^*=\sigma_m^*$, $y=y_m$ and $R^*=R_m^*$, then $T^*=J(\sigma^{*k},R^*)=\sum y^{k'}S$. Noting here that R_k^* is a simple ring, we see that $\varphi_k^*:\sum y_k^i s_i\to\sum y^{k'i}s_i$ defines an S-isomorphism of R_k^* onto T^*. Since v is contained in $J(\tilde{v},R^*)\cap V_{R^*}(T^*)=V_{T^*}(T^*)$ and $v^{k'}\in C^*=V_{R^*}(R^*)$, $C^*[v]$ is a subfield of the center of the simple ring T^*, which proves that (σ^*) is an F-group. Needless to say, $\zeta y=y(\zeta\rho)=y\zeta$, namely, ζ is contained in C^*. Now, let $s=\sum y^i u_i$ $(u_i\in S)$ be an arbitrary non-zero element of $V^*=V_{R^*}(S)$. Since $y^iS=Sy^i$, every y^iu_i is contained in V^*. Hence, if u_i is non-zero then $(y^iu_i)S=S(y^iu_i)S=y^i(S\rho^i)u_iS=y^iS$, 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. $\mathfrak{G}=(\sigma)$. Then, there exists $x\in R^*$ such that $x\sigma=x\zeta$ and $R=\sum_0^{m-1}x^iS$ is a direct sum by §1, (x) and [10, Corollary 1]. If we set $\rho=\tilde{x}^{-1}|S$ and $s_0=x^m$, one will easily see that ρ 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 $\mathfrak{S}_k$ and R_k is isomorphic to the simple ring $J(\sigma^k,R)=\sum x^{k'i}S$, which proves (2). Finally, assume that R/S is outer and $\rho^i=\tilde{s}$. By the validity of (1), we may assume that $0\leq i<m$. Since $\rho^i=\tilde{x}^{-i}|S$, it follows $x^is\in V=C$, and so $x^{i+1}s\rho=x^isx=x^{i+1}s$, namely $s\rho=s$.

(c) Under the above notations, the monic polynomial X^m-s_0 is w-irreducible by Lemma 3.1. Since $z_0yz_0^{-1}=y(z_0\rho)\cdot z_0^{-1}=y\zeta$, we obtain $\sigma^*=\tilde{z}_0$. Accordingly, $V=J(\tilde{z}_0|V,V)$ coincides with the field Z. Hence $(\sigma^*)=(\tilde{z}_0)$ is an F-group. Conversely, assume that R/S is an m dimensional inner cyclic extension w.r.t. $\mathfrak{G}=(\tilde{z}_0)$. Noting here that $V=Z$, z_0 is in Z and $z_0\rho=x^{-1}z_0x=x^{-1}(x\tilde{z}_0)z_0=x^{-1}(x\zeta)z_0=z_0\zeta$.

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 $z_0^{1/m}$ is not contained in Z.*

(3) *There exist an inner automorphism* ρ *of* S *and* z_0 *in* S^* *satisfying* (1), (2) *in Theorem* 3.1.

Proof. The implication (1)→(2)→(3) are obvious. (Note that ζ is contained in Z).

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

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* ρ, s_0 *satisfying* (1) *in Theorem* 3.1 *and* (2′) X^m-s_0 *is irreducible in* $S[X;\rho]$. *The precise statment 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* ρ, s_0 *satisfying* (1), (2) *in Theorem* 3.1 *and* (3) *there exists a simple subring* W *of* S *containing* s_0 *such that* $W\rho\subseteqq W$, $V_W(W)\ni\zeta$ *and* X^k-s_0 *is* w*-irreducible in* $\mathfrak{W}_k=W[X;\rho^{k'}]$, *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* ρ, s_0 *satisfying* (1), (2) *in Theorem* 3.1 *and* (3′) *there exists a division subring* W *of* S *containing* s_0 *such that* $W\rho\subseteqq W$, $V_W(W)\ni\zeta$ *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* ρ, s_0 *satisfying* (1), (2) *in Theorem* 3.1 *and* (3″) *there exists a subfield* $W\ni\zeta$ *of* S *containing* s_0 *such that* $\rho|W=1$ *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.* $\mathfrak{G}=(\tau)$ *such that* $V_T(T)\ni\zeta$. *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* ρ *of* T *and regular elements* 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 w-irreducible in $T[X;\rho]$, (3) $\tau^{-1}\cdot\rho^{-1}\cdot\tau\cdot\rho=\tilde{t}_1$, (4)$RN_{m'}(t_1;\tau)=\zeta$, (5) $t_0\tau=t_0LN_m(t_1,\rho)$, and (6) if $(u_0,u_1,\cdots,u_{m-1})$ is a non-zero $1\times m$ matrix with entries in T and $s\rho^i u_i=u_i s$ for all $s\in S$ $(i=0,1,\cdots,m-1)$,

then the simultaneous equations $\sum_0^k u_{k-i}\rho^i w_i + \sum_{i=k+1}^{m-1} t_0 u_{m+k-i}\rho^i w_i = \delta_{0k}$ $(k = 0, 1, \cdots, m-1)$ have a solution in T.

Proof. By (iv) of §1, (3) means that $\Psi : \sum X^i t_i' \to \sum (Xt_1)^i (t_i'\tau)$ defines in $\mathfrak{T} = T[X; \rho]$ an automorphism, whose order is $m'm$ by (4). Next, (1) and (2) show that $M = (X^m - t_0)\mathfrak{T}$ is a maximal ideal of $\mathfrak{T}$, $R^* = \mathfrak{T}/M$ is a simple ring with $\{1, y, \cdots, y^{m-1}\}$ 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 Ψ, Ψ induces in R^* an S-automorphism σ^* of order $m'm$ such that $y\sigma^* = yt_1$ and $\sigma^*|T = \tau$. To be easily seen, $J(\sigma^{*m'}, R^*) = T$, and so $J(\sigma^*, R^*) = S$. Finally, if $v = \sum y^i u_i$ is a non-zero element of $V_{R^*}(S)$ then $t\rho^i u_i = u_i t$ 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 $m'm$ dimensional cyclic extension R/S w.r.t. $\mathfrak{G} = (\sigma)$, and set $\tau = \sigma|T$. Since V is a field (§1, (vii)) and $[R : T] = m$, R/T is cyclic extension w.r.t. $\mathfrak{G}(T) = (\sigma^m)$. Then, there exists an element $x \in R^\cdot$ such that $x\sigma^{m'} = x\zeta$ (§1, (x)). Evidently, $t_1 = x^{-1} \cdot x\sigma$ is contained in T and $RN_{m'}(t_1; \tau) = x^{-1}x\sigma^{m'} = \zeta$. Moreover, $\tilde{x}^{-1}$ induces an automorphism ρ of T. If we set $t_0 = x^m$ 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' dimensional cyclic division ring extension w.r.t. $\mathfrak{H} = (\tau)$ such that $V_T(T) \ni \zeta$. In order that T/S is regularly embedded in some $m'm$ dimensional cyclic division ring extension, it is necessary and sufficient that there exist an automorphism ρ 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) $\tau^{-1} \cdot \rho^{-1} \cdot \tau \cdot \rho = \tilde{t}_1$, (4) $RN_{m'}(t_1; \tau) = \zeta$, *and* (5) $t_0\tau = t_0 LN_m(t_1; \rho)$.

References

[1] A. A. ALBERT: Cyclic fields of degree p^e over F of characteristic p, Bull. of Amer. Math. Soc., Vol. 40 (1943).

[2] A. S. AMITSUR: Non-commutative cyclic fields, Duke Math. J., Vol. 21 (1952).

[3] E. ARTIN and O. SCHREIER: Über eine Kennzeichung der reel algebraische Körper, Abh. aus der Math. Sem. der Hamburigischen Univ., Vol. 5 (1927).

[4] J. DIEUDONNÉ: Les extensions quadratiques des corps non-commutatifs et leurs applications, Acta Math., Vol. 87 (1952).

[5] N. JACOBSON: Abstract derivation and Lie algebras, Trans. Amer. Math. Soc., Vol. 42 (1937).

[6] N. JACOBSON: Structure of rings, Providence (1956).

[7] K. KISHIMOTO, T. ONODERA and H. TOMINAGA: On the normal basis theorems and the extension dimension, J. of Fac. Sci. Hokkaido Univ., Ser. I, Vol. 19 (1964).

[8] T. NAGAHARA and H. TOMINAGA: On Galois and locally Galois extensions of simple rings, Math. J. of Okayama Univ., Vol. 10 (1961).

[9] T. NAGAHARA, T. ONODERA and H. TOMINAGA: On normal basis theorem and strictly Galois extensions, Math. J. of Okayama Univ., Vol. 8 (1958).

[10] N. NOBUSAWA and H. TOMINAGA: Some remarks on strictly Galois extensions of simple rings, Math. J. of Okayama Univ., Vol. 9 (1955).

[11] H. TOMINAGA: On a theorem of N. Jacobson, Proc. of Japan Acad., Vol. 9 (1955).

[12] E. WITT: Zyklische Körper und Algebren der Charakteristik p vom Grad p^n, J. für reine und ang. Math., Vol. 176 (1936).

Hokkaido Gakugei University

(Received November 15, 1965)