

A NOTE ON GALOIS THEORY OF PRIMARY RINGS

HISAO TOMINAGA

1°. A ring R (with 1) will be said to be *primary* [completely primary] if the (Jacobson) radical N of R is nilpotent and R/N is a simple ring with minimum condition (for one-sided ideals) [a division ring]. As is well-known, the centre of a primary ring is completely primary, and the characteristic of a primary ring is zero or a power of a prime (cf. [8, p. 125]). The purpose of this note is to extend the results in [1]¹⁾ to primary rings (Theorems 1, 2).

Now we shall begin our course with several remarks concerning primary rings, which may be more or less known but do not seem to the author to have been explicitly stated in literature.

Lemma 1. *Let $R \ni 1$ be a ring, $S \ni 1$ a primary subring of R with minimum condition. If R is S -right regular²⁾, then R possesses a linearly independent (finite) S -right basis.*

Proof. As is familiar, S may be regarded as a complete matrix ring over a completely primary ring C (with minimum condition): $S = \sum_{i,j=1}^m C e_{ij}$. Then, $S = \sum_{i=1}^m \oplus e_{ii} S$, whence we have $R = \sum_{i=1}^m \oplus e_{ii} R$. Evidently $e_{ii} R (= e_{ii} R)$ and $e_{ii} R (= e_{ii} R)$ are S -isomorphic, and so they are decomposed into directly indecomposable S -submodules in the same number, say k . While each indecomposable direct summand of R is isomorphic to $e_{ii} S (\cong e_{ii} S)$ because of the S -right regularity of R , so that R is S -isomorphic to the direct sum of mk copies of $e_{ii} S$, whence so is to the direct sum of k copies of S . We have proved therefore our assertion.

Lemma 2. *Let $R \supseteq T \supseteq S$ be rings with the same identity element 1, and let S be a primary ring with minimum condition. If R, T possess a linearly independent finite T -right basis $\{r_1, \dots, r_n\}$ and a linearly independent finite S -right basis $\{t_1, \dots, t_m\}$ respectively, then T is a direct summand of R as an S -right submodule.*

Proof. Let M be the radical of S , and let S/M be the direct sum of s irreducible right ideals. Then the following (into) homomorphisms $T/TM \rightarrow T/T \cap RM \leftrightarrow (T + RM)/RM \rightarrow (r_i T + RM)/RM$ yield $u \geq v \geq v_i$ ($i = 1, \dots, n$), where u, v , and v_i are S/M -lengths of $T/TM, T/T \cap RM,$

¹⁾ Cf. also the errata for [1] to appear in the Notices of Amer. Math. Soc.

²⁾ An S -right [left] module m is said to be S -right [left] regular when a direct sum of a certain number of its copies is isomorphic, as S -module, to the direct sum of a certain number of S itself (cf. [3]).

and $(r_i T + RM)/RM$ respectively. Since $(S/M)^{(r,m)} \cong (T/TM)^{(n)} \cong R/RM = \sum_{i=1}^n (r_i T + RM)/RM$ imply $smn = un \leq \sum_{i=1}^n v_i$, where $(*)^{(j)}$ means the direct sum of j copies of $*$, it is clear that $(sm =)u = v = v_i$ ($i = 1, \dots, n$). On the other hand, $R/RM = (T + RM)/RM \oplus U/RM$ with some S -submodule U . Now, noting that the S/M -length of $(T + RM)/RM$ is sm , it follows that U/RM possesses a linearly independent S/M -basis $\{\bar{u}_1, \dots, \bar{u}_{m(n-1)}\}$, where \bar{u}_k is the residue class modulo RM containing u_k , whence $R = T + \sum_{k=1}^{m(n-1)} u_k S + RM$. Then, applying [6, II] to $R/(T + \sum_{k=1}^{m(n-1)} u_k S)$, we obtain $R = T + \sum_{k=1}^{m(n-1)} u_k S$. Comparing the S -lengths of the left and right terms, we readily see that $R = T \oplus \sum_{k=1}^{m(n-1)} u_k S$ (and that $\{u_1, \dots, u_{m(n-1)}\}$ is linearly independent over S).

Corollary 1. *Let $R \supseteq T \supseteq S$ be rings with the same identity element 1, and let S be a primary ring with minimum condition. If R possesses a linearly independent finite T -right basis and S -right basis as well, then the R -module $\text{Hom}_{S_r}(T, R)$ consisting of all the S_r -homomorphisms of T into R coincides with $(\text{Hom}_{S_r}(R, R))_T$, the restriction of $\text{Hom}_{S_r}(R, R)$ onto T^3 .*

Proof. As is well-known, T is S -right regular (cf. [3, p. 206]) and so, by Lemma 1, possesses a linearly independent finite S -right basis. Thus, $R = T \oplus U$ by Lemma 2, whence each $\alpha \in \text{Hom}_{S_r}(T, R)$ can be extended to an element of $\text{Hom}_{S_r}(R, R)$.

Remark 1. Of course, Lemmas 1, 2 and Corollary 1 are valid symmetrically if “right” and “left” are exchanged each other.

We shall conclude this section with the following lemma and its corollary.

Lemma 3. *Let S be a completely primary ring, and \mathfrak{G} a group of finite order $n > 1$. Then the following conditions are equivalent to each other :*

(1) $\mathfrak{G}S$ is completely primary, where $\mathfrak{G}S$ is the group ring (defined as usual) of \mathfrak{G} over S .

(2) S is of characteristic p^e (p ; prime) and $n = p^e$.

And, when one of the above conditions is fulfilled, the radical of $\mathfrak{G}S$ is $\sum_{1 \neq \sigma \in \mathfrak{G}} (1 - \sigma)S + \mathfrak{G}M$, where M is the radical of S .

Proof. One will readily see that the mapping $\lambda : \sum_{\sigma \in \mathfrak{G}} \sigma x_\sigma \rightarrow \sum_{\sigma \in \mathfrak{G}} \bar{x}_\sigma$,

³⁾ For $x \in R$, x_r and x_l mean the right and left multiplications induced by x respectively. Similarly, for $X \subseteq R$, $X_r = \{x_r | x \in X\}$ and $X_l = \{x_l | x \in X\}$.

where \bar{x}_σ means the residue class modulo M containing x_σ , defines a ring homomorphism of $\mathbb{G}S$ onto $\bar{S} = S/M$. And then $\lambda^{-1}\{0\} = \sum_{1 \neq \sigma \in \mathbb{G}} (1 - \sigma)S + M = \sum_{1 \neq \sigma \in \mathbb{G}} (1 - \sigma)S + \mathbb{G}M$.

(1) \Rightarrow (2). Naturally, $\lambda^{-1}\{0\}$ is the radical of $\mathbb{G}S$ and nilpotent. If S is of characteristic zero, then $\lambda(\sum_{\sigma \in \mathbb{G}} \sigma 1) = n \cdot \bar{1} \neq 0$, but on the other hand, $(\sum_{\sigma \in \mathbb{G}} \sigma 1)(1 - \tau) = 0$ for any $\tau \neq 1$ of \mathbb{G} . This contradiction shows that S is of characteristic $p^e \neq 0$. Now, let $n = p^e n'$ with $(n', p) = 1$, and suppose that $n' > 1$. Then for any prime divisor q of n' , we can find a q -Sylow group \mathfrak{Q} of \mathbb{G} . We set here $x_\sigma = 1$ and 0 according as σ is in \mathfrak{Q} or not. Then $\lambda(\sum_{\sigma \in \mathbb{G}} \sigma x_\sigma)$ is a power of q , and so it is not zero (in \bar{S}). While, $(\sum_{\sigma \in \mathbb{G}} \sigma x_\sigma)(1 - \tau) = 0$ for any $\tau \neq 1$ of \mathfrak{Q} , which is a contradiction.

(2) \Rightarrow (1). We shall prove that $\lambda^{-1}\{0\}$ is nilpotent (and so that $\lambda^{-1}\{0\}$ is the radical of $\mathbb{G}S$). In case $e = 1$, noting that $(1 - \sigma)^{p^m} = 0$ for each $\sigma \in \mathbb{G}$, it will be easy to see that $(\lambda^{-1}\{0\})^{p-1)p^e+m} = 0$, where m is the nilpotency index of M . Thus we shall proceed with induction for e . Let $e > 1$ and \mathfrak{H} be a normal subgroup of \mathbb{G} of order p . Then $\mu(\sum_{\sigma \in \mathbb{G}} \sigma x_\sigma) = \sum_{\sigma \in \mathbb{G}} \bar{\sigma} \bar{x}_\sigma$ defines a ring homomorphism of $\mathbb{G}S$ onto $\bar{\mathbb{G}}\bar{S}$, where $\bar{\mathbb{G}} = \mathbb{G}/\mathfrak{H}$, and $\mu^{-1}\{0\}$ is the ideal generated by $\{1 - \eta \mid \eta \in \mathfrak{H}\}$ and M . Accordingly, noting that $\sigma'(1 - \eta)\sigma = \sigma' \sigma(1 - \sigma^{-1}\eta \sigma)$ for $\sigma', \sigma \in \mathbb{G}$ and $\eta \in \mathfrak{H}$, we readily obtain $(\mu^{-1}\{0\})^{h+m} = 0$, where h is the nilpotency index of the radical of $\mathfrak{H}S$. Since $\mu(\sum_{1 \neq \sigma \in \mathbb{G}} (1 - \sigma)S + \mathbb{G}M)$ is contained in the radical of $\bar{\mathbb{G}}\bar{S}$ by our induction hypothesis, there holds $\mu((\lambda^{-1}\{0\})^l) = 0$, where l is the nilpotency index of the radical of $\bar{\mathbb{G}}\bar{S}$. Hence we have our assertion $(\lambda^{-1}\{0\})^{l \cdot h+m} = 0$.

Corollary 2. *Let S be a primary ring with minimum condition, \mathbb{G} a group of finite order, and \mathfrak{H} a normal subgroup of order $n > 1$. Then the following conditions are equivalent to each other :*

(I') $\sum_{\sigma \in \mathbb{G}} \sigma x_\sigma \in \mathbb{G}S$ is regular if and only if $\sum_{\sigma \in \mathbb{G}} \bar{\sigma} x_\sigma \in \bar{\mathbb{G}}S$ is so, where $\bar{\mathbb{G}} = \mathbb{G}/\mathfrak{H}$ and $\bar{\sigma}$ means the residue class of σ modulo \mathfrak{H} .

(II) S is of characteristic p^e (p ; prime) and $n = p^e$.

Proof. $\psi(\sum_{\sigma \in \mathbb{G}} \sigma x_\sigma) = \sum_{\sigma \in \mathbb{G}} \bar{\sigma} x_\sigma$ defines a ring homomorphism ψ of the group ring $\mathbb{G}S$ onto $\bar{\mathbb{G}}S$, and $\psi^{-1}\{0\}$ is the ideal generated by $\{1 - \eta \mid \eta \in \mathfrak{H}\}$.

(I') \Rightarrow (II). Given any $\alpha \in \psi^{-1}\{0\}$, (I') implies that $1 - \alpha \in \psi^{-1}\{\bar{1}\}$ is regular, that is, $\psi^{-1}\{0\}$ is a quasi-regular ideal. Thus, as $\mathbb{G}S$ satisfies minimum condition, $\psi^{-1}\{0\}$ is nilpotent. Accordingly, nilpotent is the

subring $\sum_{1 \neq \gamma \in \mathfrak{G}} (1 - \gamma) V_S(S)$ which may be considered as an ideal of the group ring $\mathfrak{G} V_S(S)$. From this fact, one readily sees that $\mathfrak{G} V_S(S)$ is completely primary. Hence the completely primary ring $V_S(S)$ is of characteristic $p^c(p; \text{prime})$ and n is a power of p by Lemma 3.

(II) \Rightarrow (I'). $\mathfrak{G} V_S(S)$ is completely primary by Lemma 3 again, and so $\sum_{1 \neq \gamma \in \mathfrak{G}} (1 - \gamma) V_S(S)$ is nilpotent. From this we can readily see that $\psi^{-1}\{0\}$ is nilpotent. Hence (I') holds good.

2°. Throughout this section, R be a primary ring with minimum condition, N and Z be the radical and the centre of R respectively, and \mathfrak{G} be a finite group of automorphisms of R . $V(\mathfrak{G})$ will mean the subring of R generated by Z and all regular elements v with $v_i v_r^{-1} \in \mathfrak{G}$ ⁴⁾. We consider here the following conditions:

- (1) $((V(\mathfrak{G}) + N)/N) \cdot V_{R/N}(R/N)$ is simple, (whence $V(\mathfrak{G})$ is primary.)⁵⁾
- (2) If $\{\rho(\bar{1}) = 1, \rho(\bar{\sigma}), \dots, \rho(\bar{\tau})\}$ is a complete representative system of $\mathfrak{G}/\mathfrak{G}_0 = \{\bar{1}, \bar{\sigma}, \dots, \bar{\tau}\}$, where \mathfrak{G}_0 is the totality of inner automorphisms contained in \mathfrak{G} , then the R_i - R_i -modules R_i and $\rho(\bar{\sigma})R_i$ ($\bar{\sigma} \neq \bar{1}$) have no isomorphic composition residue modules.
- (3_i) $V(\mathfrak{G})$ possesses a linearly independent Z -basis $\{v_i\}$ such that $\{v_{i,r}\}$ is linearly independent over R_i .
- (3_r) $V(\mathfrak{G})$ possesses a linearly independent Z -basis $\{u_r\}$ such that $\{u_{r,i}\}$ is linearly independent over R_r .

In case \mathfrak{G} satisfies (1), (2), and (3_i) [(1), (2), and (3_r)], \mathfrak{G} is called an F_i -group [F_r -group]. And if \mathfrak{G} is an F_i -group as well as an F_r -group, then it is an F -group.

The following remarks will be readily seen from Nakayama's papers [4] and [5] (and of course the corresponding remarks are true for F_r -groups): Let \mathfrak{G} be an F_i -group then $\mathfrak{G}R_i = \mathfrak{G}V(\mathfrak{G})_r R_i = \sum \rho(\bar{\sigma}) V(\mathfrak{G})_r R_i$ yields that the independent basis $\{v_i\}$ in (3_i) is finite. And $\mathfrak{G} \widetilde{V(\mathfrak{G})}$ ⁶⁾ is evidently a regular group in Nakayama's sense [5], and so, setting $S = J(\mathfrak{G}, R) = \{x \in R \mid x\sigma = x \text{ for all } \sigma \in \mathfrak{G}\}$ ⁷⁾, S is a primary ring with minimum condition, moreover $(S + N)/N$ is simple. Further $V(\mathfrak{G}) = V_R(S)$, $\mathfrak{G}R_i = \text{Hom}_{S_r}(R, R)$, R possesses a linearly independent S -right basis, and $[R : S]_r = (\mathfrak{G} : \mathfrak{G}_0) \cdot [V(\mathfrak{G}) : Z] \leq \#\mathfrak{G}$ (the order of \mathfrak{G}).

4) In case R is a simple ring (with minimum condition), $V(\mathfrak{G})$ is the subring of R generated by all the regular elements v with $v_i v_r^{-1} \in \mathfrak{G}$.

5) In general, for any non-empty subset X of a ring A , $V_A(X)$ will signify the centralizer of X in A .

6) $\widetilde{V(\mathfrak{G})}$ denotes the totality of inner automorphisms induced by regular elements contained in $V(\mathfrak{G})$.

7) $x\sigma$ means the image of x by σ .

If \mathfrak{G} is an F -group then $[R : S]_l = [R : S]_r$, where $S = J(\mathfrak{G}, R)$. In particular, when $[R : S]^{(8)}$ coincides with $\#\mathfrak{G}$, we say that R is *strictly Galois* with respect to the F -group \mathfrak{G} .

Remark 2. If \mathfrak{G} is outer then the conditions (3_l) and (3_r) are superfluous, and so the notion of F_l -group coincides with that of F -group. On the other hand, in case R is a simple ring, it will be easy to see that \mathfrak{G} is an F -group if and only if $V(\mathfrak{G})$ is two-sided simple. Moreover, in case R is a division ring, the notion of F group is trivial, and R is strictly Galois with respect to \mathfrak{G} if and only if \mathfrak{G} is a finite group with $[R : J(\mathfrak{G}, R)] = \#\mathfrak{G}$.

In what follows, S will mean $J(\mathfrak{G}, R)$. For any $r \in R$, $T_{\mathfrak{G}}(r) = \sum_{\sigma \in \mathfrak{G}} r\sigma$ ($\in S$) is called the \mathfrak{G} -trace of r . And if $\{r\sigma \mid \sigma \in \mathfrak{G}\}$ forms an independent S -(right) basis of R then r is called a \mathfrak{G} -normal basis element (abr. \mathfrak{G} -n. b. e.) of R . In general, R may be regarded as a right $\mathfrak{G}S$ -module, where $\mathfrak{G}S$ is the group ring of \mathfrak{G} over S . And R possesses a \mathfrak{G} -n. b. e. when and only when R is $\mathfrak{G}S$ -isomorphic to $\mathfrak{G}S$. Particularly, if S satisfies minimum condition, it is well-known that each element of $\mathfrak{G}S$ is either a regular element or a zero divisor. Thus we obtain the following lemma at once.

Lemma 4. *Let S satisfy minimum condition, and r be a \mathfrak{G} -n. b. e. of R . Then for $\alpha \in \mathfrak{G}S$, $r\alpha$ is also a \mathfrak{G} -n. b. e. if and only if α is regular in $\mathfrak{G}S$.*

Our first theorem is the following (cf. [1], [3] and [7]).

Theorem 1. *Let R be a primary ring with minimum condition. If R is strictly Galois with respect to $\mathfrak{G} = \{\sigma_1, \dots, \sigma_n\}$ then R contains a \mathfrak{G} -n. b. e.*

Proof. By the remark stated previously, $\text{Hom}_{S_l}(R, R) = \mathfrak{G}R_r$ ($S = J(\mathfrak{G}, R)$). Since $[R : S] = [\text{Hom}_{S_l}(R, R) : R_r]_r$, $\mathfrak{G}R_r = \sum_{i=1}^n \oplus R_r \sigma_i$. Evidently $\mathfrak{G}S_r = \sum_{i=1}^n \oplus S_r \sigma_i (\cong \mathfrak{G}S)$ is a ring with minimum (whence maximum) condition. Now let $\{r_1, \dots, r_n\}$ be an independent S -right basis of R . Then it is clear that $\{r_1 r, \dots, r_n r\}$ forms a linearly independent $\mathfrak{G}S_r$ -basis of $\text{Hom}_{S_l}(R, R)$, and so R is $\mathfrak{G}S_r$ -isomorphic to $\mathfrak{G}S_r$ by [2, Satz 4], which completes our proof.

Lemma 5. *Under the same assumption as in Theorem 1, if \mathfrak{G} is a*

⁸⁾ In case the left dimension $[R : S]_l$ coincides with the right one $[R : S]_r$, they are denoted as $[R : S]$.

subgroup of \mathfrak{G} which is an F -group then $\mathfrak{G}(J(\mathfrak{H}, R)) = \mathfrak{H}^9$.

Proof. $T = J(\mathfrak{H}, R)$ is a primary ring with minimum condition, and S -left regular [3, p. 206], accordingly T possesses a linearly independent S -left basis by Lemma 1. Thus, by Corollary 1, we have $\text{Hom}_{S_l}(T, R) = \mathfrak{G}_r R_r$. Further, as $\text{Hom}_{T_l}(R, R) = \mathfrak{H}R_r$, it follows that $\#\mathfrak{G} = \#\mathfrak{H} \cdot (\mathfrak{G} : \mathfrak{H}) \geq [\mathfrak{H}R_r : R_r]_r \cdot [\mathfrak{G}_r R_r : R_r]_r = [R : T] \cdot [T : S] = \#\mathfrak{G}$, whence we have $\#\mathfrak{H} = [R : T]$ and $(\mathfrak{G} : \mathfrak{H}) = [T : S]$. Now, our assertion $\mathfrak{G}(J(\mathfrak{H}, R)) = \mathfrak{H}$ is an easy consequence of the last fact $(\mathfrak{G} : \mathfrak{H})(= [T : S]) = [\mathfrak{G}_r R_r : R_r]_r$.

Corollary 3. *Under the same assumption as in Theorem 1, if \mathfrak{H} is a normal subgroup of \mathfrak{G} which is an F -group, then $\overline{\mathfrak{G}} = \mathfrak{G}/\mathfrak{H}$ may be regarded as a group of $T = J(\mathfrak{H}, R)$, and $[T : S] = \#\overline{\mathfrak{G}}$ (and of course $J(\overline{\mathfrak{G}}, T) = S$).*

Now we are at the position to prove our principal theorem which contains the result in [1].

Theorem 2. *Let R be a primary ring with minimum condition. If R is strictly Galois with respect to \mathfrak{G} , \mathfrak{H} an F -group of order $n > 1$ that is a normal subgroup of \mathfrak{G} , and if $T = J(\mathfrak{H}, R)$, then the following conditions are equivalent to each other :*

(I) $r \in R$ is a \mathfrak{G} -n. b. e. if and only if the \mathfrak{H} -trace of r is a $\overline{\mathfrak{G}}$ -n. b. e., where $\overline{\mathfrak{G}} = \mathfrak{G}/\mathfrak{H}$.

(II) S is of characteristic p^e (p ; prime) and $n = p^e$.

Proof. R possesses a \mathfrak{G} -n. b. e. r by Theorem 1. Then, in virtue of Corollary 3, $T_{\mathfrak{H}}(r)$ is a $\overline{\mathfrak{G}}$ -n. b. e. of T , that is, T is $\overline{\mathfrak{G}}$ - S -isomorphic to $\overline{\mathfrak{G}}S$. Noting that $T_{\mathfrak{H}}(r\alpha) = T_{\mathfrak{H}}(r)(\psi(\alpha))$ for each $\alpha \in \mathfrak{G}S$, Lemma 4 yields the equivalence of (I) and (I'), where ψ_r means the ring homomorphism defined in the proof of Corollary 2. The rest of the proof is contained in Corollary 2.

Corollary 4. *Let a division ring R be strictly Galois with respect to \mathfrak{G} , and \mathfrak{H} a subgroup of \mathfrak{G} of order $n > 1$. If \mathfrak{N} signifies the normalizer of \mathfrak{H} in \mathfrak{G} , $N = J(\mathfrak{N}, R)$ and $T = J(\mathfrak{H}, R)$, then the following conditions are equivalent to each other :*

(I₀) $r \in R$ is an \mathfrak{N} -n. b. e. (of R/N) if and only if the \mathfrak{H} -trace of r is an $\mathfrak{N}/\mathfrak{H}$ -n. b. e. (of T/N).

(II₀) S is of characteristic $p \neq 0$ and $n = p^e$.

⁹⁾ $\mathfrak{G}(J(\mathfrak{H}, R))$ is defined to be the set $\{\sigma \in \mathfrak{G} \mid x\sigma = x \text{ for all } x \in J(\mathfrak{H}, R)\}$.

REFERENCES

- [1] C.C. FAITH, Galois extensions in which every element with regular trace is a normal basis element, Proc. Amer. Math. Soc., 9 (1958) 222—229.
- [2] F. KASCH, Über den Endomorphismenring eines Vektorraumes und den Satz von der Normalbasis, Math. Ann., 126 (1953) 447—463.
- [3] T. NAKAYAMA, Galois theory for general rings with minimum condition, J. Math. Soc. Japan, 1 (1949) 203—216.
- [4] T. NAKAYAMA, Generalized Galois theory of rings with minimum condition, Amer. J. Math., 73 (1951) 1—12.
- [5] T. NAKAYAMA, Generalized Galois theory of rings with minimum condition II, Amer. J. Math., 77 (1955) 1—16.
- [6] T. NAKAYAMA, A remark on finitely generated modules, Nagoya Math. J., 3 (1951) 139—140.
- [7] T. ONODERA, and H. TOMINAGA, On strictly Galois extensions of degree p^e over a division ring of characteristic p , Math. J. Okayama Univ., 7 (1957) 77—81.
- [8] E. SNAPPER, Completely primary rings II. Algebraic and transcendental extensions, Ann. Math., 53 (1951) 125—142.

DEPARTMENT OF MATHEMATICS,
OKAYAMA UNIVERSITY

(Received July 18, 1958)