<table>
<thead>
<tr>
<th>Title</th>
<th>ON A SIMPLE RING WITH A GALOIS GROUP OF ORDER $p^e$</th>
</tr>
</thead>
<tbody>
<tr>
<td>Author(s)</td>
<td>Takazawa, Takao; Tominaga, Hisao</td>
</tr>
<tr>
<td>Citation</td>
<td>Journal of the Faculty of Science Hokkaido University. Ser. 1 Mathematics = 北海道大学理学部紀要 北海道大学理学部紀要</td>
</tr>
<tr>
<td>Issue Date</td>
<td>1961</td>
</tr>
<tr>
<td>Doc URL</td>
<td><a href="http://hdl.handle.net/2115/56016">http://hdl.handle.net/2115/56016</a></td>
</tr>
<tr>
<td>Type</td>
<td>bulletin (article)</td>
</tr>
</tbody>
</table>
ON A SIMPLE RING WITH A GALOIS GROUP
OF ORDER $p^e$

By

Takao TAKAZAWA and Hisao TOMINAGA

Recently in [2, §3],1) the next was obtained: Let $R$ be a simple ring (with minimum condition) of characteristic $p \neq 0$, and $\mathfrak{G}$ a DF-group of order $p^e$. If $S=J(\mathfrak{G}, R)$, then $[R:S]$ divides $p^e$, and $V_R(S)$ coincides with the composite of the center of $R$ and that of $S$. More recently, in [1], M. Moriya has proved the following: Let $R$ be a division ring, $\mathfrak{G}$ an automorphism group2) of order $p^e$ ($p$ a prime), and $S=J(\mathfrak{G}, R)$. If the center of $S$ contains no primitive $p$-th roots of 1, then $[R:S]$ divides $p^e$, and $V_R(S)$ coincides with the composite of the center of $R$ and that of $S$. And moreover, $[R:S]$ is equal to $p^e$ provided $R$ is not of characteristic $p$.

The purpose of this note is to extend these facts to simple rings in such a way that our extension contains also the fact cited at the beginning.

In what follows, we shall use the following conventions: $R$ is a simple ring with the center $C$, and $\mathfrak{G}$ a DF-group of order $p^e$ where $p$ is a prime number. We set $S=J(\mathfrak{G}, R)$, which is a simple ring by [2, Lemma 2]. And by $Z$ and $V$ we shall denote the center of $S$ and the centralizer $V_R(S)$ of $S$ in $R$ respectively. Finally, as to notations and terminologies used here, we follow [2].

Now, we shall begin our study with the following theorem.

**Theorem 1.** If $Z$ contains no primitive $p$-th roots of 1, then $[R:S]$ divides $p^e$.

**Proof.** Firstly, in case $e=1$, $\mathfrak{G}$ is either outer or inner. If $\mathfrak{G}$ is outer, then it is well-known that there holds $[R:S]=p$. Thus, we may, and shall, assume that $\mathfrak{G}$ is inner, and set $\mathfrak{G} = \{1, \bar{v}, \ldots, \bar{v}^{p-1}\}$. Then, to be easily seen, $v$ is contained in $Z(\supseteq C)$, and $v^p = c$ for some $c \in C$. If the polynomial $X^p - c \in C[X]$ is reducible, then it possesses a linear factor, that is, there exists an element $c_0 \in C$ such that $c_0^p = c$, whence it follows that

---

1) Numbers in brackets refer to the references cited at the end of this note.

2) One may remark here that in case $R$ is a division ring any automorphism group of finite order becomes naturally a $DF$-group.
On a Simple Ring with a Galois Group of Order $p^e$

$(w^{-1})^p = 1$. Recalling here $w^{-1} = 1$, we obtain $(w^{-1})^e = 1$. But this contradicts $\varnothing \equiv 1$. Consequently, we see that $X^p - c$ is irreducible in $C[X]$, and so $V = C[v]$ yields at once $p = [V : C] = [R : S]$. Now we proceed with induction for $e$, and assume $e > 1$. Take a subgroup $\mathfrak{B}$ of order $p$ which is contained in the center of $\mathfrak{G}$, and set $P = J(\mathfrak{B}, R)$. Then, by [2, Lemma 3], $\mathfrak{B}$ is also a DF-group and $V_p(S)$ is a division ring of finite dimension over $V_p(P)$. Hence, $\mathfrak{G} | P (= the restriction of $\mathfrak{G}$ to $P$) is a DF-group whose order is a divisor of $p^e - 1$. And so, by our induction hypothesis, $[P : S]$ is a divisor of $p^e - 1$. Further, noting that $J(\mathfrak{G} | V_p(S), V_p(S)) = Z$ and the order of $\mathfrak{G} | V_p(S)$ is a divisor of $p^e - 1$, we see that $[V_p(S) : Z]$ is a divisor of $p^e - 1$ again by our induction hypothesis. Accordingly, it follows that $V_p(S)$, so that $V_p(P)$ contains no primitive $p$-th roots of 1. Combining this with the fact that $\mathfrak{B}$ is a DF-group of order $p$, we obtain $[R : P] = p$. Hence, $[R : S] = [R : P] . [P : S]$ is a divisor of $p^e$.

**Lemma 1.** If $Z$ contains no primitive $p$-th roots of 1, then $S \cong C$ provided $e > 0$.

**Proof.** If, on the contrary, $S = C$ then $R$ is a division ring necessarily and $\mathfrak{G}$ is inner. Now, choose a subgroup $\mathfrak{B} = \{1, \tilde{v}, \ldots, \tilde{v}^{p - 1}\}$ of order $p$ contained in the center of $\mathfrak{G}$. Then, for each $\sigma = \tilde{u} \in \mathfrak{G}$, $\tilde{v}\sigma = \sigma \tilde{v}$ implies $\sigma \in C \subseteq Z$. And $v^p = u\tilde{v}u^{-1} = (u\tilde{v})^p = v^p c_2^p$ yields $c_2 = 1$, i.e. $c_2 = 1$. This means evidently $v \in S = C$. But this is a contradiction.

**Theorem 2.** If $Z$ contains no primitive $p$-th roots of 1, then $V$ is the composite $C[Z]$ of $C$ and $Z$.

**Proof.** Since the order of $\mathfrak{G} | V$ is a divisor of $p^e$ and $J(\mathfrak{G} | V, V) = Z$, $[V : Z]$ divides $p^e$ by Theorem 1. We see therefore that $V$ contains no primitive $p$-th roots of 1. For the subgroup $\mathfrak{I} = \tilde{V}$ of $\mathfrak{G}$, the order of $\mathfrak{I} | V$ is a divisor of $p^e$ and $J(\mathfrak{I} | V, V)$ coincides with the center $Z_0$ of $V$. And so, by Lemma 1, $\mathfrak{I} | V = 1$, that is, $V$ is a field. (If $e = 0$, then $V = C$ evidently.) Finally, suppose $V \supseteq C[Z]$. Since $V = V(\mathfrak{G}) (= the subring generated by all regular elements $v \in R$ with $\tilde{v} \in \mathfrak{G}$), $\mathfrak{G}$ contains an inner automorphism determined by an element, $v$ not contained in $C[Z]$. Then evidently $v^d = c$ for some $d > 0$ and $c \in C$. Since $V$ is Galois and finite over $C[Z]$, and so, since the field $V$ is normal and separable over the subfield $C[Z]$, there exists an element $u \in V$ different from $v$ such that $u^d = v^d$, i.e. $(vu^{-1})^d = 1$. Recalling here $V$ does not contain primitive $p$-th roots of 1, we have $vu^{-1} = 1$, i.e. $u = v$. But this is a contradiction. We have proved therefore $V = C[Z]$. 


Now, combining Theorem 2 with [3, Theorem 1.1] and [3, Theorem 3.1], we obtain the next at once.

**Corollary 1.** If \( Z \) contains no primitive \( p \)-th roots of 1, then each intermediate ring \( T \) of \( R/S \) is a simple ring and \( T=S[t] \) with some \( t \).

**Theorem 3.** If \( Z \) contains no primitive \( p \)-th roots of 1, and \( S \) is not of characteristic \( p \), then \([R:S] \) coincides with \( p^e \).

**Proof.** At first, it may be noted that the characteristic of \( S \) is different from 2. If \( e=1 \), then our assertion has been shown in the proof of Theorem 1. We shall proceed again by induction for \( e \). Take a subgroup \( \mathcal{B} \) of order \( p \) which is contained in the center of \( G \), and set \( P=J(\mathcal{B}, R) \). Then, as is cited in the proof of Theorem 1, \( \mathcal{B} \) and \( G|P \) are DF-groups of \( R \) and \( P \) respectively, and \( V_r(P) \) contains no primitive \( p \)-th roots of 1. Thus, by our induction hypothesis, it follows that \([R:S]=\[R:P]\cdot\[P:S]=p\cdot(\text{order of } G|P) \). In what follows, we shall prove that \( \mathcal{B}(P)=\{\sigma \in G; x\sigma = x \text{ for all } x \in P\} \) coincides with \( \mathcal{B} \), which enables us evidently to complete our proof. Since in case \( \mathcal{B} \) is outer there is nothing to prove, we shall restrict our proof to the case where \( \mathcal{B} \) is inner: \( \mathcal{B} =\{1, \tilde{v}, \cdots, \tilde{v}^{p-1}\} \). Since \( R/P \) is evidently inner Galois, each element of \( \mathcal{B}(P) \) is an inner automorphism. If \( \tilde{u}=1 \) is in \( \mathcal{B}(P) \), then \( u^{p^d}=c' \) with some \( d>0 \) and \( c' \in C \). Recalling that the field \( V_{p^d}(P)=C[v] \) is of dimension \( p \) over \( C \), \( u \) possesses a minimal polynomial \( f(x)=X^p+\cdots+c_p \in C[X] \). If \( \zeta \) is a primitive \( p^d \)-th root of 1 (contained in a suitable extension field of \( V \)), then \( \{u\zeta^i; i=0, \cdots, p^d-1\} \) exhausts the roots of \( X^{p^d}-c'=0 \). Hence, noting that \( f(X) \) divides \( X^{p^d}-c' \) in \( C[X] \), we obtain \( -c_p = u^{p^j} \zeta^i \) with some \( j \). Since, as is noted in the proof of Theorem 2, \( V_{r^d}(P) \subseteq \subseteq V_{r^d}(P) \) contains no primitive \( p \)-th roots of 1, \( \zeta^i=-c_p u^{-p} \in V_{r^d}(P) \) yields at once \( u^{-p} = c_p \in C \). Consequently, by [1, Hilfssatz 4], it will be seen that \( u=v^kc \) with some integer \( k \) and \( c \in C \), which shows that \( \tilde{u}=\tilde{v}^e \in \mathcal{B} \).

As a direct consequence of Theorem 3 and [2, Theorem 4], we obtain the following:

**Corollary 2.** If \( Z \) contains no primitive \( p \)-th roots of 1, and \( S \) is not of characteristic \( p \), then \( R/S \) possesses a \( G \)-normal basis element, that is, there exists an element \( r \in R \) such that \( R= \sum_{\sigma \in \mathcal{G}} (r\sigma)S \).
On a Simple Ring with a Galois Group of Order $p^e$

References


Department of Mathematics,
Hokkaido University

(Received September 19, 1960)