On strictly Galois extensions of degree $p^e$ over a division ring of characteristic $p$

Takesi Onodera*  Hisao Tominaga†

*Hokkaido University
†Okayama University

Copyright ©1957 by the authors. Mathematical Journal of Okayama University is produced by The Berkeley Electronic Press (bepress). http://escholarship.lib.okayama-u.ac.jp/mjou
ON STRICTLY GALOIS EXTENSIONS OF DEGREE $P^e$
OVER A DIVISION RING OF CHARACTERISTIC $P$

TAKESI ONODERA and HISAO TOMINAGA

Let $K$ be a field and $\mathfrak{G}$ be an automorphism group of finite order $n > 1$ with $D$ as the fixed subring. Recently C. C. Faith announced the equivalence of the following two propositions [2]:

1) If $T_\mathfrak{G}(k) = \sum_{\sigma \in \mathfrak{G}} k^\sigma$ is non-zero then $\{k^\sigma \mid \sigma \in \mathfrak{G}\}$ is a basis of $K/D$.

2) $D$ has prime characteristic $p$ and $n = p^t$.

On the other hand, in [1], A. S. Amitsur considered cyclic division ring extensions, and proved in this case that (2) implies (1) [1, Theorem 1]. In this note, we shall prove that Amitsur’s result can be extended to the case that $D$ has prime characteristic $p$ and $n = p^t$. More precisely: if $K/D$ is strictly Galois with respect to $\mathfrak{G}$ of order $n > 1$, then (1) and (2) are equivalent to each other.

Of course, our result contains Faith’s completely. And we suppose that the essential tools in our proof are similar to those in [2], nevertheless the details of Faith’s discussion do not appear so far.

1. Group ring defined by $\mathfrak{G}$ and $D$

Let $D$ be a division ring, and $\mathfrak{G}$ be a finite group. A ring $R$ containing $D$ (with the common identity) is called a group ring defined by $\mathfrak{G}$ and $D$ if there exist regular elements $u_\sigma (\sigma \in \mathfrak{G})$ such that $u_\sigma u_\tau = u_{\sigma \tau}$, $d u_\sigma = u_\sigma d (d \in D)$ and $R = \sum_{\sigma \in \mathfrak{G}} u_\sigma D$. In what follows, for the sake of brevity, we shall write $\mathfrak{G}D$ and $\sum_{\sigma \in \mathfrak{G}} \sigma d_\sigma$ instead of $\sum_{\sigma \in \mathfrak{G}} u_\sigma D$ and $\sum_{\sigma \in \mathfrak{G}} u_\sigma d_\sigma$ respectively. Needless to say, given $\mathfrak{G}$ and $D$, we can construct a group ring defined by $\mathfrak{G}$ and $D$ in an obvious way.

Lemma 1. Let $\mathfrak{G}D = \sum_{\sigma \in \mathfrak{G}} \sigma D$ be a group ring defined by a group

1) Numbers in brackets refer to the references cited at the end of this paper.
2) He called $K$ a cyclic extension of $D$ if $K$ possesses a cyclic group $\mathfrak{G}$ of $n$ automorphisms with $D$ as the fixed subring, and $K$ has a right (and so left) $D$-dimension $n$. The last requirement is superfluous for outer automorphism groups, but it is essential in our present consideration as well as in [1].
3) For the terminology “strictly Galois”, see the definition given in §2.
TAKESI ONODERA and HISAO TOMINAGA

$\mathfrak{G}$ of order $n > 1$ and a division ring $D$. If $\sum_{\sigma \in \mathfrak{G}} d_{\sigma} \neq 0$ ($d_{\sigma} \in D$) implies that the set $\{(\sum_{\sigma \in \mathfrak{G}} d_{\sigma})^\tau \mid \tau \in \mathfrak{G}\}$ is linearly independent over $D$, then $\chi(D)$ (the characteristic of $D$) is a prime $p$ and $n = p^e$.

Proof. If $\chi(D) = 0$ then, setting all $d_{\sigma} = 1$, $\sum_{\sigma \in \mathfrak{G}} d_{\sigma} = n \neq 0$ but evidently the set $\{(\sum_{\sigma \in \mathfrak{G}} d_{\sigma})^\tau \mid \tau \in \mathfrak{G}\}$ is linearly dependent, being contradictory to the assumption. Thus $\chi(D) = p \neq 0$. Now we set $n = p^n$, where $(p, n') = 1$. If $n' > 1$ then, for any prime factor $q$ of $n'$, there exists a $q$-Sylow group $\mathfrak{G}$ of $\mathfrak{G}$. We set here $d_{\sigma} = 1$ and 0 according as $\sigma$ is in $\mathfrak{G}$ or not. Then $\sum_{\sigma \in \mathfrak{G}} d_{\sigma}$ is a power of $q$ and so it is not zero.

On the other hand, as one will readily see, $\{(\sum_{\sigma \in \mathfrak{G}} d_{\sigma})^\tau \mid \tau \in \mathfrak{G}\}$ is linearly dependent. This contradiction proves $n' = 1$.

Lemma 2. Let $\mathfrak{G}D$ be a group ring defined by $\mathfrak{G}$ of order $p$ and $D$ of characteristic $p \neq 0$. Then $\mathfrak{G}D$ is completely primary, that is, all the non-regular elements form an ideal.

Proof. Let $\sigma$ be a generating element of $\mathfrak{G}$. Evidently $1 - \sigma$ is a central nilpotent element of $\mathfrak{G}D$ of nilpotency index $p$, accordingly $A_i = \{x \in \mathfrak{G}D \mid x(1 - \sigma)^i = 0\}$ is an ideal and there holds $A_0 \subset A_1 \subset \cdots \subset A_{p-1} \subset A_p = \mathfrak{G}D$. Recalling the well-known formula $\binom{p-1}{r} = (-1)^r \mod p$, we obtain

$(1 - \sigma)^{p-1} = \sum_{r=0}^{p-1} (-1)^r \binom{p-1}{r} \sigma^r = \sum_{r=0}^{p-1} \sigma^r$. We shall prove that $N = \{\sum_{i=0}^{p-1} \sigma^i d_i \mid \sum_{i=0}^{p-1} d_i = 0\}$ is the ideal consisting of all the non-regular elements. If $\sum_{i=0}^{p-1} d_i \neq 0$ then $(\sum_{i=0}^{p-1} \sigma^i d_i) \cdot (1 - \sigma)^{p-1} = \sum_{i=0}^{p-1} d_i \cdot \sum_{j=0}^{p-1} \sigma^j \neq 0$, whence $\sum_{i=0}^{p-1} \sigma^i d_i$ is not in $A_{p-1}$. Moreover this fact implies that $\sum_{i=0}^{p-1} \sigma^i d_i \cdot (1 - \sigma)^j$ is contained in $A_{p-1}$ but not in $A_{p-1-j}$ ($j = 0, \ldots, p-1$). Hence $\{\sum_{i=0}^{p-1} \sigma^i d_i (1 - \sigma)^j \mid j = 0, \ldots, p-1\}$ forms a basis of $\mathfrak{G}D$, that is, $\sum_{i=0}^{p-1} \sigma^i d_i$ is a regular element. Conversely, if $\sum_{i=0}^{p-1} \sigma^i d_i$ is regular in $\mathfrak{G}D$ then $\sum_{i=0}^{p-1} \sigma^i d_i \cdot (1 + \sigma + \cdots + \sigma^{p-1}) = \sum_{i=0}^{p-1} d_i \cdot \sum_{j=0}^{p-1} \sigma^j$ is non-zero, whence $\sum_{i=0}^{p-1} d_i \neq 0$. As evidently $N$ is an ideal, our proof is complete.

The above lemma is still valid for $\mathfrak{G}$ of order $p^e$, but moreover we shall prove the following theorem.

Theorem 1. A group ring $\mathfrak{G}D$ defined by $\mathfrak{G}$ of order $n > 1$ and
D is completely primary if and only if $\chi(D)$ is a prime $p$ and $n = p^e$. And if $\mathfrak{O}D$ is completely primary then the totality of non-regular elements is $N = \{\sum_{\sigma \in \mathfrak{O}} \sigma d_{\sigma} | \sum_{\sigma \in \mathfrak{O}} d_{\sigma} = 0\} = \sum_{\sigma \in \mathfrak{O}} (1 - \sigma) D$.

Proof. In any completely primary ring, all the non-regular elements form a unique maximal one-sided ideal, which coincides with the (Jacobson) radical by [3, Theorem I. 6.1]. And, as is well-known, the radical of a ring with minimum condition is nilpotent. These remarks will be required in the sequel.

Necessity. To be easily verified, $\psi^* (\sum_{\sigma \in \mathfrak{O}} \sigma d^\tau) = \sum_{\sigma \in \mathfrak{O}} \sigma d^\tau$ defines a ring homomorphism $\psi^*$ of $\mathfrak{O}D$ onto $D$ with $N$ as the kernel. Accordingly the maximal ideal $N$ coincides with the totality of non-regular elements. Noting that $\sum_{\sigma \in \mathfrak{O}} \sigma d_{\sigma}$ is regular if and only if the set $\{\sum_{\sigma \in \mathfrak{O}} \sigma d_{\sigma} \tau | \tau \in \mathfrak{O}\}$ is linearly independent over $D$, our assertion is clear from Lemma 1.

Sufficiency. In case $e = 1$, our assertion is Lemma 2 itself. Now we suppose $e > 1$, and that our assertion is true for $e - 1$. To prove our assertion, it suffices to show that $N$ is a nil-ideal. As $\mathfrak{O}$ is a $p$-group, we can find a normal subgroup $\mathfrak{O}$ of order $p$. Let $S^*$ be a (fixed) complete representative system of $\mathfrak{O} = \mathfrak{O}/\mathfrak{O}$, and $\tilde{\sigma}$ be the residue class of $\sigma \in \mathfrak{O}$ modulo $\mathfrak{O}$. Then $\psi (\sum_{\sigma \in \mathfrak{O}} \sigma d_{\sigma}) = \sum_{\tilde{\sigma} \in \mathfrak{O}} \tilde{\sigma} d_{\tilde{\sigma}}$ defines a ring homomorphism $\psi$ of $\mathfrak{O}D$ onto $\mathfrak{O}D$ with the kernel $M = \{\sum_{\sigma \in \mathfrak{O}} \sigma d_{\sigma} | \sum_{\sigma \in \mathfrak{O}} d_{\sigma^m} = 0$ for all $\sigma^* \in S^*\}$. At first we shall prove that $M$ is a nil-ideal. To this end, consider an arbitrary finite set $\{\alpha_i, \gamma_{d_{\gamma}}(i) \mid i = 1, \ldots, m\}$ with $\sum_{\gamma \in \mathfrak{O}} d_{\gamma}^{(m)} = 0$ where $\alpha_i$'s are in $\mathfrak{O}$. As is easily verified, then there holds the following:

\[ (*) \quad \alpha_i \sum_{\gamma \in \mathfrak{O}} \gamma d_{\gamma}^{(i)} \cdots d_{\gamma^{(m)}} = \alpha_i \cdots d_{\gamma^{(m)}} \sum_{\gamma \in \mathfrak{O}} \gamma d_{\gamma}^{(i)} \cdots d_{\gamma^{(m)}}, \]

where $\gamma \to \gamma^{(i)}$ is a suitable permutation in $\mathfrak{O}$ ($i = 1, \ldots, m$). Since each $\sum_{\gamma \in \mathfrak{O}} \gamma d_{\gamma}^{(i)}$ is contained in the radical of $\mathfrak{O}D$ by Lemma 2, the product $(*)$ is zero if $m$ exceeds the nilpotency index of the radical of $\mathfrak{O}D$. Making use of this fact, we can readily see that each element in $M$ is nilpotent. Now let $\sum_{\sigma \in \mathfrak{O}} d_{\sigma} = 0$. Then $\psi (\sum_{\sigma \in \mathfrak{O}} \sigma d_{\sigma}) = \sum_{\tilde{\sigma} \in \mathfrak{O}} \tilde{\sigma} d_{\tilde{\sigma}}$ is contained in the radical of $\mathfrak{O}D$ by our induction hypothesis, whence $(\sum_{\sigma \in \mathfrak{O}} \sigma d_{\sigma})^t$ is in $M$ for some positive integer $t$. We obtain therefore, by the last remark, $(\sum_{\sigma \in \mathfrak{O}} \sigma d_{\sigma})^t$ is nilpotent, accordingly so is $\sum_{\sigma \in \mathfrak{O}} \sigma d_{\sigma}$. 

Produced by The Berkeley Electronic Press, 1957

3
2. Principal theorem

Throughout this section, let $K$ be a division ring, and $\mathfrak{O}$ be a finite group of automorphisms in $K$ with $D$ as the fixed subring. In general, as is well-known, $[K : D] = [K : D] = [K : D]$ is bounded by the order of $\mathfrak{O}$ (see, for example, [5]). If in particular $[K : D]$ coincides with the order of $\mathfrak{O}$ then we say that $K/D$ is strictly Galois with respect to $\mathfrak{O}$. For any $k \in K$, we set $T_{\mathfrak{O}}(k) = \sum_{\sigma \in \mathfrak{O}} k^\sigma$ ($\mathfrak{O}$-trace of $k$). In case $\{k^\sigma | \sigma \in \mathfrak{O}\}$ is an independent right $D$-basis of $K$, $k$ is called a $\mathfrak{O}$-normal basis element (abbreviated, $\mathfrak{O}$-n. b. e.).

The next lemma is essential in our present consideration, and enables us to reduce our problem to a structure theorem of group rings, Theorem 1.

**Lemma 3.** If $K/D$ is strictly Galois with respect to $\mathfrak{O} = \{\sigma_1, \cdots, \sigma_n\}$ then $K$ is isomorphic to $\mathfrak{O}D_K$ as a right $\mathfrak{O}$-module, where $D_K$ means the totality of right multiplications by elements of $D$.\(^4\)

**Proof.** Let $\mathfrak{G}$ be the $K_R$-$K_R$-module of all linear transformations of the left $D$-module $K$. Since $n = [K : D] = [\mathfrak{G} : K_R]$, we have $\mathfrak{G} = \mathfrak{O}K_R = \sum_{i=1}^n \sigma_i K_R = \sum_{i=1}^n K_R \sigma_i$, by [5, Satz] (or [3, pp. 159 -- 161]). Evidently $\mathfrak{O}D_K = \sum_{i=1}^n \sigma_i D_K$ is a ring with minimum condition. Now let $\{k_1, \cdots, k_n\}$ be an independent right $D$-basis of $K$. Then it is clear that $\mathfrak{G} = \sum_{i=1}^n \sigma_i k_i \mathfrak{O}$, and so $\mathfrak{G}$ is a right scalar ring of $\mathfrak{G}$ in Kasch's sense [4, p. 453]. Hence, by [4, Satz 4], $K$ is $\mathfrak{O}$-isomorphic to $\mathfrak{G}$.

If $K/D$ is strictly Galois with respect to $\mathfrak{O}$ then, as $\mathfrak{O}D_K = \sum_{\sigma \in \mathfrak{O}} \sigma D_K$, $\mathfrak{O}D_K$ is canonically isomorphic to a group ring $\mathfrak{O}D$, and so $K$ may be considered as a right $\mathfrak{O}D$-module by defining $k \cdot (\sum_{\sigma \in \mathfrak{O}} \sigma d) = \sum_{\sigma \in \mathfrak{O}} k^\sigma d$. Hence, by Lemm 3, $K$ is $\mathfrak{O}D$-isomorphic to $\mathfrak{O}D$ by an isomorphism $\varphi$.

Under this situation, there holds the following :

**Corollary 1.** Let $K/D$ be strictly Galois with respect to $\mathfrak{O}$. If $\varphi(k) = \sum_{\sigma \in \mathfrak{O}} \sigma d_{\sigma} (k \in K)$ then $T_{\mathfrak{O}}(k) \neq 0$ is equivalent with $\sum_{\sigma \in \mathfrak{O}} d_{\sigma} \neq 0$, and the fact that $k$ is $\mathfrak{O}$-n. b. e. is nothing but to say that the set $\{\sum_{\sigma \in \mathfrak{O}} \sigma d_{\sigma} \tau \mid \tau \in \mathfrak{O}\}$ is linearly independent over $D$, or what is the same, that $\sum_{\sigma \in \mathfrak{O}} \sigma d_{\sigma}$ is a regular element.

---

4) Similarly, for any $k \in K$, $k_R$ means the right multiplication by $k$.  

http://escholarship.lib.okayama-u.ac.jp/mjou/vol7/iss1/3  

4
ON STRICTLY GALOIS EXTENSIONS OF DEGREE $p^n$ ETC.

Proof. Since $\varphi(k') = (\sum_{\sigma \in \mathcal{G}} \sigma d_{\sigma})$, we have $\varphi(T_{\mathcal{G}}(k)) = \sum_{\sigma \in \mathcal{G}} \sigma d_{\sigma} = \sum_{\tau \in \mathcal{G}} \tau \cdot \sum_{\sigma \in \mathcal{G}} d_{\sigma}$. Accordingly $T_{\mathcal{G}}(k) \neq 0$ is equivalent to $\sum_{\sigma \in \mathcal{G}} d_{\sigma} \neq 0$. The rest of the proof is almost trivial.

We are now at the position to state our principal theorem.

Theorem 2. If $K/D$ is strictly Galois with respect to $\mathcal{G}$ of order $n > 1$ then (1) and (2) are equivalent to each other:

(1) $k \subseteq K$ is a $\mathcal{G}$-n.b.e. if and only if the $\mathcal{G}$-trace of $k$ is non-zero.

(2) $\chi(D)$ is a prime $p$ and $n$ is a power of $p$.

Proof. By Corollary 1, our assertion is an easy consequence of Theorem 1.

REFERENCES


DEPARTMENTS OF MATHEMATICS,
HOKKAIDO UNIVERSITY
OKAYAMA UNIVERSITY

(Received July 10, 1957)