

# 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]:<sup>1)</sup>

(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  $n = p^e$ .

On the other hand, in [1], A. S. Amitsur considered cyclic division ring extensions,<sup>2)</sup> 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  $n = p^e$ . 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.<sup>3)</sup>

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  $u_\sigma u_\tau = u_{\sigma\tau}$ ,  $du_\sigma = u_\sigma d$  ( $d \in D$ ) and  $R = \sum_{\sigma \in \mathfrak{G}} \oplus u_\sigma D$ . 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  $\sum_{\sigma \in \mathfrak{G}} \oplus u_\sigma D$  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  $\mathfrak{G}D = \sum_{\sigma \in \mathfrak{G}} \oplus \sigma D$  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.

$\mathfrak{G}$  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  $\{(\sum_{\sigma \in \mathfrak{G}} \sigma d_\sigma)\tau \mid \tau \in \mathfrak{G}\}$  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  $\{(\sum_{\sigma \in \mathfrak{G}} \sigma d_\sigma)\tau \mid \tau \in \mathfrak{G}\}$  is linearly dependent, being contradictory to the assumption. Thus  $\chi(D) = p \neq 0$ . Now we set  $n = p^e n'$ , where  $(p, n') = 1$ . If  $n' > 1$  then, for any prime factor  $q$  of  $n'$ , there exists a  $q$ -Sylow group  $\mathfrak{H}$  of  $\mathfrak{G}$ . We set here  $d_\sigma = 1$  and  $0$  according as  $\sigma$  is in  $\mathfrak{H}$  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,  $\{(\sum_{\sigma \in \mathfrak{G}} \sigma d_\sigma)\tau \mid \tau \in \mathfrak{G}\}$  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  $A_0 \subset A_1 \subset \dots \subset A_{p-1} \subset A_p = \mathfrak{G}D$ . Recalling the well-known formula  $\binom{p-1}{r} \equiv (-1)^r \pmod{p}$ , 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  $A_{p-j}$  but not in  $A_{p-j-1}$  ( $j = 0, \dots, p-1$ ). Hence  $\{(\sum_{i=0}^{p-1} \sigma^i d_i)(1 - \sigma)^j \mid j = 0, \dots, p-1\}$  forms an independent  $D$ -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  $(\sum_{i=0}^{p-1} \sigma^i d_i) \cdot (1 + \sigma + \dots + \sigma^{p-1}) = \sum_{i=0}^{p-1} d_i \cdot \sum_{j=0}^{p-1} \sigma^j$  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  $\mathfrak{U}D$  is completely primary then the totality of non-regular elements is  $N = \{ \sum_{\sigma \in \mathfrak{U}} \sigma d_\sigma \mid \sum_{\sigma \in \mathfrak{U}} d_\sigma = 0 \} = \sum_{1 \neq \sigma \in \mathfrak{U}} (1 - \sigma) D$ .

*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 1. 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,  $\psi^*(\sum_{\sigma \in \mathfrak{U}} \sigma d_\sigma) = \sum_{\sigma \in \mathfrak{U}} d_\sigma$  defines a ring homomorphism  $\psi^*$  of  $\mathfrak{U}D$  onto  $D$  with  $N$  as the kernel. Accordingly the maximal ideal  $N$  coincides with the totality of non-regular elements. Noting that  $\sum_{\sigma \in \mathfrak{U}} \sigma d_\sigma$  is regular if and only if the set  $\{ (\sum_{\sigma \in \mathfrak{U}} \sigma d_\sigma) \tau \mid \tau \in \mathfrak{U} \}$  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  $\mathfrak{U}$  is a  $p$ -group, we can find a normal subgroup  $\mathfrak{H}$  of order  $p$ . Let  $S^*$  be a (fixed) complete representative system of  $\mathfrak{U} = \mathfrak{U}/\mathfrak{H}$ , and  $\bar{\sigma}$  be the residue class of  $\sigma \in \mathfrak{U}$  modulo  $\mathfrak{H}$ . Then  $\psi^*(\sum_{\sigma \in \mathfrak{U}} \sigma d_\sigma) = \sum_{\sigma \in \mathfrak{U}} \bar{\sigma} d_\sigma$  defines a ring homomorphism  $\psi^*$  of  $\mathfrak{U}D$  onto  $\bar{\mathfrak{U}}D$  with the kernel  $M = \{ \sum_{\sigma \in \mathfrak{U}} \sigma d_\sigma \mid \sum_{\eta \in \mathfrak{H}} d_{\sigma^* \eta} = 0 \text{ for all } \sigma^* \in S^* \}$ . At first we shall prove that  $M$  is a nil-ideal. To this end, consider an arbitrary finite set  $\{ \sigma_i \sum_{\eta \in \mathfrak{H}} \eta d_\eta^{(i)} \mid i = 1, \dots, m \}$  with  $\sum_{\eta \in \mathfrak{H}} d_\eta^{(i)} = 0$  where  $\sigma_i$ 's are in  $\mathfrak{U}$ . As is easily verified, then there holds the following :

$$(*) \quad \sigma_1 \sum_{\eta \in \mathfrak{H}} \eta d_\eta^{(1)} \cdots \sigma_m \sum_{\eta \in \mathfrak{H}} \eta d_\eta^{(m)} = \sigma_1 \cdots \sigma_m \sum_{\eta \in \mathfrak{H}} \eta^{(1)} d_\eta^{(1)} \cdots \sum_{\eta \in \mathfrak{H}} \eta^{(m)} d_\eta^{(m)},$$

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

## 2. Principal theorem

Throughout this section, let  $K$  be a division ring, and  $\mathfrak{G}$  be a finite group of automorphisms in  $K$  with  $D$  as the fixed subring. In general, as is well-known,  $[K : D]_r = [K : D]_l = [K : D]$  is bounded by the order of  $\mathfrak{G}$  (see, for example, [5]). If in particular  $[K : D]$  coincides with the order of  $\mathfrak{G}$  then we say that  $K/D$  is *strictly Galois* with respect to  $\mathfrak{G}$ . For any  $k \in K$ , we set  $T_{\mathfrak{G}}(k) = \sum_{\sigma \in \mathfrak{G}} k^\sigma$  ( $\mathfrak{G}$ -trace of  $k$ ). In case  $\{k^\sigma \mid \sigma \in \mathfrak{G}\}$  is an independent right  $D$ -basis of  $K$ ,  $k$  is called a  $\mathfrak{G}$ -normal basis element (abbreviated,  $\mathfrak{G}$ -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  $\mathfrak{G} = \{\sigma_1, \dots, \sigma_n\}$  then  $K$  is isomorphic to  $\mathfrak{S} = \mathfrak{G}D_R$  as a right  $\mathfrak{S}$ -module, where  $D_R$  means the totality of right multiplications by elements of  $D$ .<sup>4)</sup>*

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

If  $K/D$  is strictly Galois with respect to  $\mathfrak{G}$  then, as  $\mathfrak{G}D_R = \sum_{\sigma \in \mathfrak{G}} \oplus \sigma D_R$ ,  $\mathfrak{S}D_R$  is canonically isomorphic to a group ring  $\mathfrak{G}D$ , and so  $K$  may be considered as a right  $\mathfrak{S}D$ -module by defining  $k \cdot (\sum_{\sigma \in \mathfrak{G}} \sigma d_\sigma) = \sum_{\sigma \in \mathfrak{G}} k^\sigma d_\sigma$ . Hence, by Lemm 3,  $K$  is  $\mathfrak{G}D$ -isomorphic to  $\mathfrak{G}D$  by an isomorphism  $\varphi$ . Under this situation, there holds the following :

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

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

*Proof.* Since  $\varphi(k^\tau) = (\sum_{\tau \in \mathfrak{G}} \sigma d_\sigma) \tau$ , we have  $\varphi(T_{\mathfrak{G}}(k)) = \sum_{\sigma, \tau \in \mathfrak{G}} \sigma \tau d_\sigma = \sum_{\tau \in \mathfrak{G}} \tau \cdot \sum_{\sigma \in \mathfrak{G}} d_\sigma$ . Accordingly  $T_{\mathfrak{G}}(k) \neq 0$  is equivalent to  $\sum_{\sigma \in \mathfrak{G}} d_\sigma \neq 0$ . 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  $\mathfrak{G}$  of order  $n > 1$  then (1) and (2) are equivalent to each other :*

- (1)  $k \in K$  is a  $\mathfrak{G}$ -n. b. e. if and only if the  $\mathfrak{G}$ -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

- [1] A.S. AMITSUR, Non-commutative cyclic fields, *Duke Math. J.*, 21 (1954) 87—105.
- [2] C.C. FAITH, Normal extensions in which every element with nonzero trace is a normal basis element, *Bull. Amer. Math. Soc.*, 63 (1957) 95—96.
- [3] N. JACOBSON, *Structure of rings*, Amer. Math. Soc. Colloquium Publ., vol. 37 (1956).
- [4] F. KASCH, Über den Endomorphismenring eines Vektorraumes und den Satz von Normalbasis, *Math. Ann.*, 126 (1953) 447—463.
- [5] F. KASCH, Bemerkung zum Hauptsatz der Galoisschen Theorie für Schiefkörper, *Archiv der Math.*, 6 (1955) 420—422.

DEPARTMENTS OF MATHEMATICS,  
HOKKAIDO UNIVERSITY  
OKAYAMA UNIVERSITY

(Received July 10, 1957)