

## NOTE ON MAXIMAL GALOIS SUBRINGS OF FINITE LOCAL RINGS

TAKAO SUMIYAMA

Throughout  $R$  will represent a (not necessarily commutative) finite local ring with radical  $M$ . Let  $K$  be the residue field  $R/M$ , and  $R^*$  the unit group of  $R$ . Let  $|K| = p^r$  ( $p$  a prime),  $|R| = p^{nr}$ ,  $|M| = p^{(n-1)r}$ , and  $p^k$  ( $k \leq n$ ) the characteristic of  $R$ .

Let  $Z_{p^k} = Z/p^kZ$ . Given a polynomial  $g(X)$  in  $Z_{p^k}[X]$ ,  $\bar{g}(X)$  will denote the image of  $g(X)$  under the natural homomorphism  $Z_{p^k}[X] \rightarrow Z_0[X]$ . The  $r$ -dimensional Galois extension  $\text{GR}(p^{kr}, p^k)$  of  $Z_{p^k}$  is called a *Galois ring* (of characteristic  $p^k$  and rank  $r$ ), and is characterized as a ring isomorphic to  $Z_{p^k}[X]/(f(X))$  with a monic basic irreducible polynomial  $f(X) \in Z_{p^k}[X]$  of degree  $r$  (see [1]). By [2, Theorem 8 (i)],  $R$  contains a subring isomorphic to  $\text{GR}(p^{kr}, p^k)$ , which will be called a *maximal Galois subring* of  $R$ . If  $R_1$  and  $R_2$  are maximal Galois subrings of  $R$  then, by [2, Theorem 8 (ii)], there exists a unit  $a$  in  $R$  such that  $R_2 = a^{-1}R_1a$ .

The purpose of this note is to prove the following

**Theorem.** *If an inner automorphism of  $R$  maps a maximal Galois subring of  $R$  into (and hence onto) itself, then it induces the identity map on the maximal Galois subring.*

*Proof.* Let  $\bar{u}_0$  be a generator of  $K^*$ , and choose a monic polynomial  $f_0(X)$  in  $Z_{p^k}[X]$  of degree  $r$  such that  $\bar{f}_0(X)$  is the minimal polynomial of  $\bar{u}_0$ . Then, by [2, Theorem 6], we may assume that  $f_0(u_0) = 0$ . Let  $R_0 = Z_{p^k}[u_0]$  be the subring of  $R$  generated by  $u_0$ , and consider the natural homomorphism  $\phi : Z_{p^k}[X]/(f_0(X)) \rightarrow R_0$ . Since the degree of  $\bar{f}_0(X)$  is  $r$ , it is a routine to see that the sum  $Z_{p^k} + Z_{p^k}u_0 + \dots + Z_{p^k}u_0^{r-1}$  is a direct sum. It follows therefore that  $\phi$  is an isomorphism and  $R_0$  is a maximal Galois subring of  $R$ . Since  $K^* \cong R^*/(1+M)$  and  $1+M$  is a  $p$ -group, the order of the unit  $u_0$  is  $p^s(p^r - 1)$  with some  $s$ . Let us set  $u = u_0^{p^s}$ . Then  $\bar{u}$  is still a generating element of  $K^*$ , and we have  $R_0 = Z_{p^k}[u]$  as above. Let  $M_0$  be the radical of  $R_0$ . Notice that  $R_0/M_0 \cong K$  in the natural way. Now, let  $a$  be a unit of  $R$  such that the inner automorphism  $I_a$  effected by  $a$  maps  $R_0$  onto  $R_0$ . Since  $u$  is of order

$p^r - 1$ ,  $R^*$  is a semidirect product of  $\langle u \rangle$  with  $1 + M$ . We set  $a = u^i(1+x)$  with  $x \in M$ . Then, we can easily see that  $I_a(u) - u = I_{1+x}(u) - u \in M$ . Combining this with  $I_a(u) \in R_i$ , we readily obtain  $I_{1+x}(u) - u = y_0 \in M_0$ . By [3, Proposition 2.2],  $R = R_0 \oplus M'$  with some  $R_i$ - $R_0$ -submodule  $M'$  of  $M$ . Let  $x = x_0 + x'$  with  $x_0 \in R_0$  and  $x' \in M'$ . Since  $R_0$  is commutative,  $(1+x)\{I_{1+x}(u) - u\} = (1+x)y_0$  simplifies to  $ux' - x'u - x'y_0 = (1+x_0)y_0$ . Obviously, the last belongs to  $R_0 \cap M' = 0$ , and hence  $(1+x_0)y_0 = 0$ . Since  $x_0$  is in  $M_0$ , it follows  $y_0 = 0$ . We conclude therefore  $I_i(u) = I_{1+x}(u) = u$ , which proves that  $I_i$  induces the identity map on  $R$ . Now, the rest of the proof is immediate by [2, Theorem 8 (ii)].

**Remark.** Let  $R_0$  and  $u$  be as in the proof of Theorem. Then the number of maximal Galois subrings of  $R$  is equal to the index  $|M : N|$ , where  $N = \{x \in M \mid xu = ux\}$ . In fact, by [2, Theorem 8 (ii)], the number of maximal Galois subrings of  $R$  is given by  $|R^* : L|$ , where  $L = \{a \in R^* \mid I_i(R_0) = R_0\}$ . Since  $R^*$  is a semidirect product of  $\langle u \rangle$  with  $1 + M$ , by Theorem we see that  $L = \{a \in R^* \mid I_a(u) = u\} = \{u^i(1+x) \mid xu = ux, x \in M, 1 \leq i \leq p^r - 1\}$ . Hence,  $|L| = (p^r - 1)|N|$ , so that we obtain  $|R^* : L| = (p^r - 1)|M| / (p^r - 1)|N| = |M : N|$ . Furthermore, we can easily see that  $R$  contains a unique maximal Galois subring if and only if  $R^*$  is a nilpotent group.

Now, we consider the ring  $R = \left\{ \begin{pmatrix} a & b \\ 0 & \sigma(a) \end{pmatrix} \mid a, b \in \text{GF}(p^2) \right\}$ , where  $\sigma$  is a nontrivial automorphism of  $\text{GF}(p^2)$ . Then  $R$  is a local ring with radical  $M = \left\{ \begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} \mid b \in \text{GF}(p^2) \right\}$ . Obviously, for any generating element  $c$  of the multiplicative group of  $\text{GF}(p^2)$  the unit  $u = \begin{pmatrix} c & 0 \\ 0 & \sigma(c) \end{pmatrix}$  of order  $p^2 - 1$  generates a maximal Galois subring of  $R$ . If  $x = \begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix}$  satisfies  $xu = ux$ , then  $(c - \sigma(c))b = 0$ . Since  $\sigma$  is nontrivial, we obtain  $b = 0$ , and so  $x = 0$ . Applying the above remark, we readily see that  $R$  contains  $p^2$  maximal Galois subrings.

#### REFERENCES

- [1] B.R. McDONALD: Finite Rings with Identity, Pure & Appl. Math. Ser. **28**, Marcel Dekker, New York, 1974.
- [2] R. RAGHAVENDRAN: Finite associative rings, *Compositio Math.* **21** (1969), 195–229.
- [3] R.S. WILSON: On the structure of finite rings, *Compositio Math.* **26** (1973), 79–93.

AICHI INSTITUTE OF TECHNOLOGY

(Received October 26, 1978)