ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 22, Number 2, Spring 1992

A NOTE ON FINITE LOCAL RINGS

E.A. WHELAN

1. The aim of this short note is to correct an error concerning finite rings which has found its way into the literature and, so far as can be discovered, has not yet been corrected. Throughout, all rings are associative with unity (preserved by homomorphisms and inherited by subrings and overrings), and all unexplained terminology is standard.

2. The problem concerns an extension $R \subseteq S$ of commutative rings, in the case where S is a *separable* or a *Galois* extension of R. Suppose that S and R are commutative local finite rings; then it is stated at [**3**, Theorem 5.3] that S is a *separable* extension of R (see Paragraph 4) if and only if S is a *Galois* extension (see Paragraph 4 again) of R. Since a Galois extension is always a separable extension for any extension of commutative rings (Paragraph 4), the effect of this statement is that, for any separable extension $R \subseteq S$ of finite commutative local rings, S is free as an R-module (see [**3**, p. 532] and Paragraph 4 below). We give a counter-example to this statement in Paragraph 6 below and examine the reasons for the error in Paragraphs 7, 8.

3. A differently formulated—but equivalent—incorrect statement is given in [**4**, Theorem XIV], and, consequently, the implication "separable implies Galois" is false in [**4**, Corollary XV.3 and Theorem XV.11].

4. The basic facts about *separable* and *Galois* extensions of (general) commutative rings can be found in [**2**]; we note that S is *separable over* R if S is a projective (right) module over the enveloping algebra $S^e = S^{\mathrm{op}} \otimes_R S$ [**2**, p. 40], and that S is a *Galois* extension of R if it is a separable extension of R and if extra conditions identified at [**2**, pp. 80–81] are also satisfied. When S, R are finite and local (so that 0, 1 are the only idempotents of S, and their residue fields are Galois

Received by the editors on December 26, 1988.

field) these conditions reduce to the requirement that S is projective (i.e., free) as R-module [**3**, Theorem 5.2(a)].

5. It is well known that, for any rational prime p and any integers $e, n \in \mathbf{N}$, there exists (up to ring isomorphism) a unique ring $R = \mathrm{GR}\,(p, e, n)$ with the following properties:

(i) R is a commutative local ring with maximal ideal pR;

(ii) $|R| = p^{en}$ and $|R/pR| = p^e$;

(iii) the characteristic of R is p^n.

These rings are known as *Galois rings*, and a fuller discussion of them can be found in [**6**, Section 3] or [**4**, Chapter XVI]. But note that the claim at [**6**; Proposition 1, p. 213] that subrings (with unity) of Galois rings are themselves Galois is *false*: see [**5**, p. 367] and the later [**1**]. If $n = 1$, then $\mathrm{GR}\,(p, e, n)$ is simply the Galois field of order p^e.

6. Let p, e, n be as in the previous paragraph, and suppose that $n > 1$. Let T be the Galois ring $\mathrm{GR}\,(p, e, n)$ of order p^{en} and S be the Galois ring $\mathrm{GR}\,(p, 2e, n)$ of order p^{2en}, with common characteristic p^n. Then S contains a unique subring isomorphic to T; identifying T with this subring, let R be the ring $T + pS$. Since $n > 1$, $pS \neq 0$, and R is a local ring with maximal ideal, $m = pT + pS = pS \neq pT$. One checks easily that $|R| = p^{en} \times p^{e(n-1)}$. Since $(pS)^n = p^n S = 0$, it is clear that $m^n = 0$ and that $pS = mS$. Now S/pS contains R/m as a subfield and is separable as a field extension of R/m since S/pS is finite. It follows by [**2**; Theorem 7.1, p. 72] that S is a (finitely generated) separable extension of R. But, evidently, S is not a free extension of R since $p^{e(2n-1)} = |R| < |S| = p^{2en} < |R|^2 = p^{2e(2n-1)}$.

7. The errors in the attempted proof of [**3**, Theorem 5.2] (and in the virtually identical argument for [**4**, Theorem XIV] are to be found in a complicated series of calculations using tensor products (see [**3**, p. 533] and [**4**, pp. 287-289]). To highlight the flaw, we add to the conventions in Paragraph 6 the assumptions $n = 2$ (for ease of calculation) and $M = pS$, $k = R/m$, $K = S/M$ (to bring our notation fully into line with that of [**3**]). Then in these terms it is claimed at [**3**; p. 533, line 14] that $|M/M^2| = |m/m^2|^{\dim_k K} = |m/m^2|^2$. But in the given situation $m = M$, $|m| = p^{2e(n-1)} \neq 1$, and $m^2 = M^2 = 0$, so the previous equality is impossible.

8. Backtracking through the argument supporting the equality just discussed, the error can be found in the passage from line 9 to line 10 on [**3**, p. 533]. In the context of Paragraph 7, this step asserts an isomorphism of abelian groups: $M/M^2 \simeq (S \otimes_R M)/(S \otimes_R M^2)$. But $M^2 = 0$, so the claimed isomorphism reduces to $M \simeq S \otimes_R M$. Now M is a k-vector space of dimension 2, while the facts that $M^2 = 0$ and $M \subseteq R$ imply that $S \otimes_R M \simeq K \otimes_k M$, a k-vector space of dimension 4; this yields two distinct values for $|M|$, so the original claim of an isomorphism must be false.

9. The counter-example in Paragraph 6 can be extended, albeit at the expense of making detailed calculations much more difficult. Suppose $T \subset S$ are finite, commutative local rings, that the maximal ideal of S is M, and that $T \subset R = T + M$. Then R is a finite commutative local ring, and S is a separable extension of R (because their maximal ideals coincide), but S is not free, and therefore not Galois, over R. This construction is sufficiently general to demonstrate that there can be no partial result which would "save" [**3**, Theorem 5.3], at least in selected special cases.

REFERENCES

1. Y. Al-Khamees, *The intersection of distinct Galois subrings is not necessarily Galois*, Comp. Math. **40** (1980), 283–286.

2. F. DeMeyer and E. Ingraham, *Separable algebras over commutative rings*, Lecture Notes in Mathematics, vol. **181**, Springer, Berlin, 1971.

3. G. Ganske and B.R. McDonald, *Finite local rings*, Rocky Mountain J. Math. **3** (1973), 521–540.

4. B.R. McDonald, *Finite rings with unity*, Marcel Dekker, New York, 1974.

5. A.A. Nečaev, *Finite principal ideal rings*, Math. USSR Sbornik **20** (1973), 364–382, trans. of Mat. Sbornik **91** (1973), 350–366.

6. R. Raghavendran, *Finite associative rings*, Comp. Math. **21** (1969), 195–229.

72 Moray Road, London N4 3LG, England