ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 3, Number 4, Fall 1973

FINITE LOCAL RINGS

G. GANSKE AND B. R. McDONALD

ABSTRACT. In this paper we examine finite local commutative rings which are the building blocks of finite commutative rings. For a finite local ring R our attention centers on the basic structural properties of R, the polynomial ring $R[X]$, the finite local extensions of R and the Galois theory of R. We show that this theory is nearly as complete as that well-known for finite fields.

1. **Introduction.** The purpose of this paper is to examine the structure theory, theory of extensions and Galois theory of finite local commutative rings. The basic approach is to specialize the Chase-Harrison-Rosenberg [3] Galois theory for commutative rings to finite local rings and in this setting sharpen the results to approximately the level of the well-known theory for finite fields.

Since the purpose is to provide a foundation for the theory of finite commutative rings, we work entirely in this context. Thus, though some of the results may be stated more generally we refrain from this and likewise results which we reference we formulate in our setting.

To us the importance of this paper will lie mainly in its applications. Research on finite fields and their applications has been notably extensive, producing rich and deep results in finite geometries, algebraic coding theory, linear groups and other areas. Our work indicates similar results are obtainable over arbitrary finite commutative rings. One of the authors has already utilized portions of this paper on questions in the theory of algebraic cryptography and matrix theory here-to-now formulated only for finite fields and occasionally quotient rings of rational integers. These results appear in [15].

The Galois extensions of Z/Zp^n (called *Galois rings*) are particularly important. Finite noncommutative rings may be considered as algebras over these Galois rings and it now appears that much of the classical theory of algebras over fields may be extended to finite rings with identity ([4], [5], [6], [20], and [22]).

The second author would like to express his deep thanks to E.

Received by the editors March 4, 1971 and, in revised form, February 23, 1972.
AMS (MOS) subject classifications (1970). Primary 12C05, 12C30, 16A44; Secondary 13B05, 13B25.
Key words and phrases. Finite commutative rings, finite local rings, Galois theory, finite fields.