Linear Algebra and its Applications 465 (2015) 296–311

Contents lists available at ScienceDirect

Linear Algebra and its Applications

www.elsevier.com/locate/laa

Several Anzahl theorems of matrices over Galois rings and their applications

Jun Guo[a,*], Fenggao Li[b]

[a] *Math. and Inf. College, Langfang Teachers University, Langfang 065000, China*
[b] *College of Mathematics, Hunan Institute of Science and Technology, Yueyang 414006, China*

A R T I C L E I N F O

Article history:
Received 9 June 2014
Accepted 18 September 2014
Available online 10 October 2014
Submitted by R. Brualdi

MSC:
05B20
05E30
34A30
15A09

Keywords:
Galois ring
Orbit
Association scheme
System of linear equations
Generalized invertible matrix
Idempotent matrix
Involutory matrix

A B S T R A C T

Let R denote the Galois ring of characteristic p^s and cardinality p^{sh}. In this paper, we determine the Smith normal forms of matrices over R, compute the number of the orbits of $m \times n$ matrices under the group $GL_m(R) \times GL_n(R)$ and the length of each orbit. Moreover, we discuss their applications to association schemes, systems of linear equations, generalized invertible matrices, idempotent matrices and involutory matrices.

* Corresponding author.
E-mail addresses: guojun_lf@163.com (J. Guo), fenggaol@163.com (F. Li).

http://dx.doi.org/10.1016/j.laa.2014.09.036

1. Introduction

As a generalization of finite fields and rings of residue class modulo a prime power, the theory of Galois rings was first developed by Krull [3]. A *Galois ring* is defined to be a finite commutative ring with the identity 1 such that the set of its zero divisors with 0 added forms a principal ideal $(p1)$ for some prime number p. It is well known that any two Galois rings of the same characteristic and the same cardinality are isomorphic. In this paper, we always use the notation $R := GR(p^s, p^{sh})$ to denote any Galois ring of characteristic p^s and cardinality p^{sh}, where s, h are positive integers. Note that R is a finite field with p^h elements if $s = 1$, and R is the ring of residue classes of $\mathbb{Z}$ modulo its ideal $p^s\mathbb{Z}$ if $h = 1$. By Theorem 14.8 in [6], any element a of R can be written uniquely as $a = a_0 + a_1 p + \cdots + a_{s-1}p^{s-1}$, where each a_i belongs to $\Omega := \{0, 1, \xi, \ldots, \xi^{p^h-2}\}$ and ξ is a unit of multiplicative order $p^h - 1$. Moreover, a is a unit if and only if $a_0 \neq 0$. Let R^* be the unit group of R. Then R^* has the size $(p^h - 1)p^{h(s-1)}$. By Theorem 14.15 in [6] the principal ideals $(1), (p), (p^2), \ldots, (p^{s-1}), (0)$ are all the ideals of R and (p) is the unique maximal ideal of R. It follows that R is a local principal ideal ring.

Let $a, b \in R$. If there is an element $c \in R$ such that $b = ac$, we say that *a divides b* and denote it by $a|b$. Let $d, b_1, b_2, \ldots, b_r \in R$. If $d|b_i$ for $i = 1, 2, \ldots, r$, then d is called a *common divisor* of $b_1, b_2, \ldots, b_r$. A common divisor d of $b_1, b_2, \ldots, b_r$ is called a *greatest common divisor* of them if any common divisor d' of them divides d. Since the principal ideals $(1), (p), (p^2), \ldots, (p^{s-1}), (0)$ are all the ideals of R, there exists some $i \in \{0, 1, \ldots, s\}$ such that p^i is a greatest common divisor of $b_1, b_2, \ldots, b_r$, denoted by $p^i := \gcd(b_1, b_2, \ldots, b_r)$.

A matrix T in $M_{n\times n}(R)$ is called *invertible* if the determinant, denoted by $\det(T)$, of T is in R^*. The set of $n \times n$ invertible matrices over R forms a group under matrix multiplication, called the *general linear group* of degree n over R and denoted by $GL_n(R)$. Let $A, B \in M_{m\times n}(R)$. The matrices A and B are called *equivalent* if $SAT = B$ for some $S \in GL_m(R)$ and $T \in GL_n(R)$. The direct product $GL_m(R) \times GL_n(R)$ acts on the set $M_{m\times n}(R)$ in the following way:

$$M_{m\times n}(R) \times \big(GL_m(R) \times GL_n(R)\big) \to M_{m\times n}(R)$$
$$\big(A, (S, T)\big) \mapsto S^{-1}AT.$$

Clearly, both A and B belong to the same orbit of $M_{m\times n}(R)$ under $GL_m(R) \times GL_n(R)$ if and only if they are equivalent.

Let $A \in M_{m\times n}(R)$ and $1 \leq t \leq \min\{m, n\}$. By a $t \times t$ *minor* of A we mean the determinant of a $t \times t$ submatrix of A. Then there exists some $i \in \{0, 1, \ldots, s\}$ such that p^i is the greatest common divisor of all $t \times t$ minors of A, denoted by $p^i := \gcd_t(A)$. For any $S \in GL_m(R)$ and $T \in GL_n(R)$, we have $\gcd_t(SAT) = \gcd_t(A)$.

Wan [5], You and Nan [9] studied several Anzahl theorems of $m \times n$ matrices over R for $s = 1$ or $h = 1$, respectively. Their research stimulates us to consider the Anzahl theorems of matrices over the general Galois ring R. The rest of this paper is structured as follows.