Linear Algebra and its Applications 474 (2015) 169–183

Contents lists available at ScienceDirect

Linear Algebra and its Applications

www.elsevier.com/locate/laa

Several Anzahl theorems of alternate matrices over Galois rings

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*

ARTICLE INFO

Article history:
Received 27 October 2014
Accepted 10 February 2015
Available online 3 March 2015
Submitted by R. Brualdi

MSC:
05B20
05B25
94A62
05E30

Keywords:
Galois ring
Alternate matrix
Orbit
Authentication code
Association scheme

ABSTRACT

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

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

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

http://dx.doi.org/10.1016/j.laa.2015.02.016
0024-3795/

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 $a = a_0 + a_1p + \cdots + a_{s-1}p^{s-1}$, where each a_i belongs to $\Omega := \{0, 1, \xi, \ldots, \xi^{p^h-2}\}$ and ξ is a unit of multiplicative order $p^h - 1$. It follows that the unit group $R^* := \{a \in R \mid a_0 \neq 0\}$ of 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 $p^i := \gcd(b_1, b_2, \ldots, b_r)$.

Let $M_{m\times n}(R)$ denote the set of all $m \times n$ matrices over R. When $m = n$, we write simply $M_n(R)$ for $M_{n\times n}(R)$. A matrix T in $M_n(R)$ 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 $GL_n(R)$. A matrix $A = (a_{ij})$ in $M_n(R)$ is called *alternate* if $a_{ij} = -a_{ji}$ for $1 \leq i \neq j \leq n$, and $a_{ii} = 0$ for $i = 1, 2, \ldots, n$. Let $Alt_n(R)$ be the set of all $n \times n$ alternate matrices over R. The matrices A and B in $Alt_n(R)$ are called *cogredient* if $TAT^{\mathrm{T}} = B$ for some $T \in GL_n(R)$, where T^{T} is the transpose of T. The group $GL_n(R)$ acts on the set $Alt_n(R)$ in the following way:

$$\begin{aligned} Alt_n(R) \times GL_n(R) &\to Alt_n(R) \\ (A, T) &\mapsto TAT^{\mathrm{T}}. \end{aligned}$$

Let $1 \leq t \leq n$ and $A \in M_n(R)$. 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 $T \in GL_n(R)$, we have $\gcd_t(TAT^{\mathrm{T}}) = \gcd_t(A)$.

Wan [5], Wu and Nan [9] studied several Anzahl theorems of $n \times n$ alternate matrices over R for $s = 1$ or $h = 1$, respectively. In this paper, we focus on Anzahl theorems of alternate matrices over the general Galois ring R. The rest of this paper is structured as follows. In Section 2, we give some useful lemmas, which are included for later reference. In Section 3, we determine the Smith normal forms and compute the number of the orbits of $n \times n$ alternate matrices under the group $GL_n(R)$. In Section 4, we compute the length of each orbit of $n \times n$ alternate matrices under $GL_n(R)$. In Section 5, we