Journal of Mathematical Research & Exposition
Vol. 18, No. 4, 507-512, November 1998

Orders of Classical Groups over Finite Rings*

Feng Hong
(Dept. of Appl. Math., Dalian University of Technology, Dalian 116024)

Abstract It is observed that a classical group over a finite ring R with identity can be reduced to that over finite fields after the procedures of taking "modulo the radical", "direct sum" and "tensor products". Basing on that fact, we calculate the orders of classical groups over R and the number of k-dimensional free submodules of an n-dimensional free module over R.

Keywords Finite ring, Nilpotent radical, Classifical group, Free module.

Classification AMS(1991) 20H25, 05E15/CCL O152.1

1. Introduction

Let R denote a finite ring with identity and J its nilpotent radical. From the theory of Wedderburn-Artin, we have

$$R/J \cong \bigoplus_{i=1}^{t} M_{m_i}(F_{q_i}) \tag{1}$$

where F_{q_i} is the finite field with q_i elements, and $M_{m_i}(F_{q_i})$, $m_i \times m_i$ the total matrix ring over F_{q_i}. The orders of classical groups over a finite field are well-known, and a parallel result has been given in [6] for finite commutative rings. In this paper, we generalize these results to arbitrary finite rings. The necessary concepts and terminologies on finite rings are referred to [3].

Let R be a finite ring as in (1), $GL_n(R)$ the group of units in $M_n(R)$, and $SL_n(R)$ the subgroup of $GL_n(R)$ generated by the matrices $T_{ij}(\lambda) = I_n + \lambda e_{ij}$, $i \neq j$, $\lambda \in R$. Here I_n is the $n \times n$ identity matrix and e_{ij} is the matrix whose only non-zero entry is a 1 in the (i, j)-position. $GL_n(R)$ and $SL_n(R)$ are called the general linear group and the special linear group, respectively. To define the unitary groups, we suppose that there is an anti-isomorphism $a \to \bar{a}$ in R such that $\bar{\bar{a}} = a$ for any $a \in R$. Two kinds of the unitary groups are defined as follows:

$$U_{2n}(R, H_2) = \left\{ T \in GL_{2n}(R) \mid T H_1 \bar{T}' = H_1 \right\}, \text{where } H_1 = \begin{bmatrix} 0 & I_n \\ -I_n & 0 \end{bmatrix},$$

* Received October 13, 1995. Supported by the National Natural Science Foundation of China and the Natural Science Foundation of Liaoning Province.

$$U_{2n}(R, H_1) = \left\{ T \in \mathrm{GL}_{2n}(R) \mid TH_2\overline{T}' = H_2 \right\}, \text{where } H_2 = \begin{bmatrix} 0 & I_n \\ I_n & 0 \end{bmatrix},$$

Here T' denotes the transpose of T. The main results of this paper are the following four theorems:

Theorem 1 *Let R be a finite ring as in* (1). *Then*

$$|\mathrm{GL}_n(R)| = |J|^{n^2} \prod_{i=1}^{t} |\mathrm{GL}_{nm_i}(F_{q_i})|,$$

Theorem 2 *Let R be as in Theorem* 1. *Then*

$$|SL_n(R)| = |\mathrm{GL}_n(R)| |\Delta| / |R^*|,$$

where R^* denotes the group of units in R, and Δ, the subgroup of R^* generated by $(abc+a+c)(cba+a+c)^{-1}$, $abc+a+c \in R^*$.

Theorem 3 *Let R be as in Theorems* 1 *and* 2, *and suppose that* 2 *is a unit of R. Then*

$$|U_{2n}(R, H_1)| = |J|^{n(2n-1)} |K|^{2n} \prod_{i=1}^{t} |Sp_{2nm_i}(F_{q_i})|,$$

and

$$|U_{2n}(R, H_2)| = |J|^{n(2n-1)} |L|^{2n} \prod_{i=1}^{t} |O_{2nm_i}(F_{q_i})|,$$

where $K = \{a \in J \mid \overline{a} = a\}$, $L = \{a \in J \mid \overline{a} = -a\}$, and $Sp_{2nm_i}(F_{q_i}), O_{2nm_i}(F_{q_i})$ are the symplectic group, orthogonal group over the finite field F_{q_i} respectively.

Since R is noetherian, it has IBN (invariant basis number), namely, for every free R-module A, every two bases of A have the same cardinal Moreover, if A is an n-dimensional free module (with an n-element basis), then any generating set with n elements is a basis (cf. [5], p. 111, Theorem 4. 9).

Let $\begin{bmatrix} n \\ k \end{bmatrix}_R$ denote the number of all k-dimensional free submodules of an n-dimensional free module. If $R = F_q$ is the finite field with q elements, then $\begin{bmatrix} n \\ k \end{bmatrix}_R$ is just the well-known Gauss binomial coefficient $\begin{bmatrix} n \\ k \end{bmatrix}_q$ whose value is given by

$$\begin{bmatrix} n \\ k \end{bmatrix}_q = \frac{(q^n - 1)(q^{n-1} - 1) \cdots (q^{n-k+1} - 1)}{(q^k - 1)(q^{k-1} - 1) \cdots (q - 1)}.$$

In general, we have

Theorem 4 *Let R be as in Theorems 1, 2 and 3. Then*

$$\begin{bmatrix} n \\ k \end{bmatrix}_R = |J|^{k(n-k)} \prod_{i=1}^{t} \begin{bmatrix} nm_i \\ km_i \end{bmatrix}_{q_i}.$$

The proofs of these theorems which will be given in the following four sections are based on the observation that a classical group over a finite ring defined as above can be reduced to that over finite fields after the procedures of taking "modulo the radical", "direct sum" and "tensor products."

2 Proof of Theorem 1

The proof is given in three steps

(i) Since each element of $GL_n(R)$ corresponds to a basis of the n-dimensional free left R-module $R^n = \{(a_1, a_2, \ldots, a_n) \mid a_i \in R\}$, and $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ is a basis of R^n if and only if $\{\alpha_1 \pmod J, \alpha_2 \pmod J, \ldots, \alpha_n \pmod J\}$ is a basis of $(R/J)^n$ (see [3], p. 87), $A \in GL_n(R)$ if and only if $A \pmod J \in GL_n(R/J)$. So we have a surjective group morphism

$$\varphi_1: GL_n(R) \to GL_n(R/J), \quad A \to A \pmod J$$

with the kernel, denoted by $GL_n(J)$, consisting of matrices of the form

$$I_n + (a_{ij})_{n\times n}, \quad a_{ij} \in J.$$

Obviously, $|GL_n(J)| = |J|^{n^2}$.

(ii) Let $R = \oplus_{i=1}^{t} R_i$. Then $M_n(R) \cong \oplus_{i=1}^{t} M_n(R_i)$. So we have a group isomorphism (see [3], p. 398)

$$\varphi_2: \quad GL_n(R) \to \prod_{i=1}^{t} GL_n(R_i),$$

from which it follows that $|GL_n(R)| = \prod_{i=1}^{t} |GL_n(R_i)|$.

(iii) Let $R = M_m(F_q)$. From the structure of "block" matrices, we may view any matrix in $GL_n(R)$ as an invertible matrix in $M_{nm}(F_q)$, and any matrix in $GL_{nm}(F_q)$ can also be considered as an element of $GL_n(R)$. So we have a group isomorphism

$$\varphi_3: \quad GL_n(R) \to GL_{nm}(F_q).$$

To sum up, we have proved the theorem.

3 Proof of Theorem 2

Since a finite ring R is "stable", i.e., R possesses the property that for any left ideal N of R and $r \in R$, $N + r$ contains a unit of R if $N + Rr = R$, (see [3], p. 399). So the discussions about the special linear groups over a division ring (cf. [1]) can be copied for the case over a finite ring. The processes are as follows:

(a) Each element A in $GL_n(R)$ can be decomposed as $A = BD(u)$, where $B \in SL_n(R)$, $D(u) = \mathrm{diag}\{1, \ldots, 1, u\}$ is a diagonal matrix, and $u \in R^*$. So it can be shown that $SL_n(R)$ is a normal subgroup of $GL_n(R)$.

(b) $GL_n(R)/SL_n(R) \cong R^*/\Delta$,

where Δ is the subgroup of R^* generated by $(abc+a+c)(cba+a+c)^{-1}$, $abc+a+c \in R^*$.

Let φ be the natural morphism of R^* onto R^*/Δ_n, where $\Delta_n = \{u \in R^* \mid D(u) \in SL_n(R)\}$. Then

$$\begin{aligned} \det: \quad GL_n(R) &\to R^*/\Delta_n \\ A &\to \varphi(u) \text{ if } A = BD(u) \end{aligned}$$

is a surjective morphism with the kernel $SL_n(R)$. So

$$GL_n(R)/SL_n(R) \cong R^*/\Delta_n.$$

If $n = 2$, we have $\Delta_2 = \Delta$ (see [4]).

If $n \geq 3$, observing that

$$SL_n(R) \cap GL_{n-1}(R) = SL_{n-1}[7],$$

we have that $\Delta_n = \Delta$

Therefore

$$GL_n(R)/SL_n(R) \cong R^*/\Delta,$$

which completes the proof of the theorem.

4 Proof of Theorem 3

The proof of Theorem 3 can be completed as follows

(I) Restricted to $U_{2n}(R, H_1)$, φ_1 (as defined in §2) is a surjective morphism of $U_{2n}(R, H_1)$ onto $Sp_{2n}(R/J)$, which we denote by $\varphi_1|_{U_{2n}(R,H_1)}$.

(II) Let $U_{2n}(J)$ denote the kernel of $\varphi_1|_{U_{2n}(R,H_1)}$. Then by a similar argument in [1], we may show that $|U_{2n}(J)| = |J|^{n(2n-1)}|K|^{2n}$.

(III) If $R = \oplus_{i=1}^{t} R_i$, then $\varphi_2|_{U_{2n}(R,H_1)}$, the restriction on $U_{2n}(R, H_1)$ of φ_2 defined in §2, is an isomorphism of $U_{2n}(R, H_1)$ to $\prod_{i=1}^{t} U_{2n}(R_i, H_1)$.

(IV) Let $R = M_m(F_q)$. We have $M_n(R) \cong M_{nm}(F_q)$. Let $I_n(R)$ denote an identity matrix in $M_n(R)$. By the isomorphism of $M_n(R) \cong M_{nm}(F_q)$, we consider $I_n(R)$ as the same as $I_{nm}(F_q)$ in $M_{nm}(F_q)$. Moreover, we identify the matrix

$$\begin{bmatrix} 0 & I_n(R) \\ -I_n(R) & 0 \end{bmatrix} \text{ with } \begin{bmatrix} 0 & I_{nm}(F_q) \\ -I_{nm}(F_q) & 0 \end{bmatrix}.$$

So we can get an isomorphism between $U_{2n}(R, H_1)$ and $Sp_{2nm}(F_q)$, the symplectic group over the finite field F_q. Therefore,

$$|U_{2n}(R, H_1)| = |Sp_{2nm}(F_q)|$$

To sum up, we have

$$|U_{2n}(R, H_1)| = |J|^{n(2n-1)} |K|^{2n} \prod_{i=1}^{t} |Sp_{2nm_i} f(F_{q_i})|$$

if R is as in (1).

Similarly, we can prove

$$|U_{2n}(R, H_2)| = |J|^{n(2n-1)} |L|^{2n} \prod_{i=1}^{t} |O_{2nm_i}(F_{q_i})|.$$

5. Proof of Theorem 4

1) Let A be any n-dimensional free left R-module, $(n, k)_R$ the set of all ordered k-tuple $\{v_1, v_2, \ldots, v_k\}$ of R-linear independent vectors in A and $[n, k]_R$ the cardinal of $(n, k)_R$. From the definition we know that every ordered k-tuple in $(n, k)_R$ generates a k-dimensional free submodule of A, and every k-dimensional free submodule of A has $[k, k]_R = |GL_k(R)|$ bases, thus we get that $[n, k]_R = \begin{bmatrix} n \\ k \end{bmatrix}_R [k, k]_R$.

2) Let A be an n-dimensional free R-module. Then A/JA is an n-dimensional free R/J-module. The elements of A and A/JA are written as $v = (a_1, a_2, \ldots a_n)$ and $v = (a_1 + J, a_2 + J, \ldots, a_n + J)$ with $a_i \in R$, respectively. As mentioned in §2, $\{v_1, v_2, \ldots, v_n\}$ is a basis of A if and only if $\{v_1, v_2, \ldots, v_n\}$ is a basis of A/JA, so $\{u_1, u_2, \ldots, u_k\} \in (n, k)_R$ if and only if $\{u_1, u_2, \ldots, u_k\} \in (n, k)_{R/J}$ which implies that $[n, k]_R = |J|^{nk} [n, k]_{R/J}$.

3) Let $R = S \oplus W$ be a direct sum of two finite rings. It is easy to establish the bijection from $(n, k)_R$ to $(n, k)_S \times (n, k)_W$. Thus we have

$$\begin{bmatrix} n \\ k \end{bmatrix}_R = \begin{bmatrix} n \\ k \end{bmatrix}_S \begin{bmatrix} n \\ k \end{bmatrix}_W.$$

4) Let $R = M_m(F_q)$, and A an n-dimensional free R-module. Then each element of $(n, k)_R$ can be regarded as $km \times nm$ matrix over F_q of rank km. So, by the theory on Gauss binomial coefficients and 1), we obtain

$$\begin{bmatrix} n \\ k \end{bmatrix}_R = \begin{bmatrix} nm \\ km \end{bmatrix}_q.$$

To sum up, we have

$$\begin{bmatrix} n \\ k \end{bmatrix}_R = |J|^{k(n-k)} \prod_{i=1}^{t} \begin{bmatrix} nm_i \\ km_i \end{bmatrix}_{q_i}.$$

Acknowledgement The author would like to thank Professor H. You for his helpful suggestions

References

1 Hua L K and Wan Z X. *Classical Groups*. Shanghai: Science and Technology Press, Shanghai, 1963.
2 Jacobson N. *Basic Algebra* I, W. H. Freeman and Company, San Francisco, 1974.
3 McDonald B R. *Finite Rings with Identity*. Marcel Dekker, Inc., New York, 1974.
4 Menal P & Moncasi J. *K_1 of Von Neumann regular rings*. J. of Pure and Appl Algebra, 1984, **33**(3): 295- 312
5 Rotman J J. *An Introduction to Homological Algebra*. Academic Press, 1979.
6 You H and Gao Y. *Computation of the orders of calssical groups over finite commutative rings*. Chinese Science Bulletin, 1994, **39**(14): 1150- 1154
7 You H. *Some remarks on decomposition of Steinberg group*. Chinese Science Bulletin, 1992, **37**(24): 2032 - 2037

有限环上典型群的阶

冯 红
(大连理工大学应用数学系, 大连116024)

摘 要

本文通过“取模”,“取值和”,“取积”等方法, 将有单位元的有限环 R 上典型群阶的计算转化为有限域上典型群阶的计算, 并计算了 R 上 n-维自由模 $V_n(R)$ 中 k-维自由子模的个数