J. Chosun Natural Sci.
Vol. 8, No. 4 (2015) pp. 313 – 316
http://dx.doi.org/10.13160/ricns.2015.8.4.313

Order of a General Linear Group *GLₙ*(*A*) over a Finite Ring *A*

Kisuk Lee†

Abstract

In this article, we compute the order of a general linear group $GL_n(A)$ over a finite ring A.

Key words : Cryptosystem, Abstract Key Exchange System, Matrix Ring, General Linear Group

1. Backgrounds

Some of the contents of the introduction in the article[1] will be quoted in this section for the readers' convenience due to the difficulty of the access to the article[1].

Various fields have been influenced by mathematics to develop and generalize their theories, and Cryptology is one of such fields. Especially, Mathematics has been playing an increasingly important role in cryptology since the invention of public key cryptography. In 1976, Diffie and Hellman proposed a new type of cryptosystem, called public key cryptosystem[2]: they gave the key exchange system whose security is based on the discrete logarithm problem[3] that is believed to be hard in mathematics. Since then, many public key systems have been invented using algebraic theories. The most widely used system is RSA (created by Rivest, Shamir, and Adlelman[4]) whose security is based on the factoring problem that is also believed to be hard in mathematics. The RSA algorithm is very simple because it uses the Euler's theorem which is known to be the easy and simple theorem in number theory.

While RSA uses a simple theorem in number theory, we gradually need more complicated knowledge of algebra, or number theory to understand ECC (Elliptic curve cryptosystem)[5], or XTR[6]. We need deeper theories in mathematics is to protect our systems from the attacks because they become more powerful due to the rapidly growing technology.

In 1999, J. Koh attempted to generalize further cryptosystems by using algebraic structures. He first used a new concept of public keys, which he called the abstract keys. All cryptosystems proposed so far have finite key spaces, and so it is possible to use exhaustive key search to break some cryptosystems, e.g., DES with 64-bit key size. However, an abstract key has an advantage that its key space has an infinite number of elements. As an example of abstract key space, we may take the set of all polynomials with integer coefficients. In the paper[1], we generalize the ElGamal type key exchange protocols using one of algebraic terminology, so called a group action as follows: The ElGamal-type cryptosystem based on discrete logarithm problem can be generalized in terms of group action.

• **Key generation**: Let φ be a group homomorphism from G to $G^{'}$. Suppose that $G^{'}$ is a group acting on a set M. Alice chooses $g \in G$ and a random exponent a. She computes $A = \varphi(g)^a$ in $G^{'}$. The public key of Alice is $(\varphi(g), A)$.

• **Encryption**: To encrypt a plaintext $m \in M$, Bob gets the public key $(\varphi(g), A)$ of Alice. He chooses a random exponent b, and he computes $B = A^b$ and $C = B \cdot m$. He sends (B, C) to Alice.

• **Decryption**: Alice computes the inverse of B in $G^{'}$, i.e., B^{-1}. She recovers m by computing $B^{-1}C$. In fact,

$$\begin{aligned} B^{-1}C &= \varphi(g)^{-ab} \cdot (\varphi(g)^{ab} \cdot m) \\ &= (\varphi(g)^{-ab}\varphi(g)^{ab}) \cdot m = 1 \cdot m = 1. \end{aligned}$$

In the paper[5], we study the key exchange system

Department of Mathematics, Sookmyung Women's University, Chungpa-dong, Yongsan-ku, Seoul, Korea

†Corresponding author : kilee@sookmyung.ac.kr

(Received: November 1, 2015, Accepted: December 25, 2015)

using the theories in commutative algebra, in which the public keys are Ext-modules defined by cohomologies of modules as follows:

(Abstract-key Exchange System using Ext-modules)[1,7]: Let R be a commutative ring, and $Mod(R)$ denote the category of finitely generated R-modules. For each integer $t \geq 1$, let $X = \{M \in Mod(R) : M$ satisfies Serre's S_t condition$\}$. Let $M \in X$Suppose t and M are publicly known.

(1) Alice chooses an ideal I of height t.

(2) Alice computes $Ext_R^t(R/J, M)$, and sends it to Bob.

(3) Bob chooses an ideal J of height t.

(4) Bob computes $Ext_R^t(R/I, M)$, and sends it to Alice.

(5) Alice computes $Hom_R(R/J, Ext_R^t(R/I, M))$, and Bob computes $Hom_R(R/I, Ext_R^t(R/J, M))$. The common key is $Ext_R^t(R/(I+J), M)$.

In this article, we compute the order of a general linear group $GL_n(A)$ over a finite ring A for the abstract key system using the theories in commutative algebra, especially matrices over commutative rings.

2. Computation of the order of a general linear group $GL_n(A)$ over a finite ring A

In the paper[7], he introduces various abstract key cryptosytems using matrices over commutative rings. In his signature schemes on matrix rings, it is very important to find the order of a general linear group $GL_n(A)$ over a finite ring A since the units in a matrix ring $Mat_n(A)$ play important roles in those systems. In this paper, we compute the order of a general linear group $GL_n(A)$ over a finite ring A.

The facts in the following Lemma 2.1 are all well-known, but we include the sketch of the proofs for completeness. We denote by $Mat_n(A)$ the set of all n by n matrices over a ring A, and by $GL_n(A)$ the set of all invertible matrices in $Mat_n(A)$.

Lemma 2.1. Let A be a ring with unity.

(1) If $A = \oplus_{i=1}^r A_i$, i.e., the finite direct product of rings A_i with unity, then

$Mat_n(A) \cong \oplus_{i=1}^r Mat(A_i)$ and

$GL_n(A) \cong \oplus_{i=1}^r GL_n(A_i)$

(2) $Mat_n(Mat_m(A)) \cong Mat_{nm}(A)$

(3) $Mat_n(J(A)) = J(Mat_n(A))$, where $J(-)$ denotes the Jacobson radical of a ring.

(4) If A is a field F of order q, then the order of $GL_n(F)$ is

$$|GL_n(F)| = (q^n - 1)(q^n - q)(q^n - q^2) \cdots (q^n - q^{n-1}).$$

Proof. (1) It is easy to show that a map $\varphi : Mat_n(\oplus_{i=1}^r A_i) \rightarrow \oplus_{i=1}^r Mat_n(A_i)$ by $\varphi([\oplus_{i=1}^r a_{kl}^i]) = \oplus_{i=1}^r [a_{kl}^i]$ is a ring isomorphism.

Since the unit group of a direct product of rings is isomorphic to the direct product of the unit group of each ring in general, we have the second part.

(2) Using block addition and multiplication, we can show $Mat_n(Mat_m(A)) \cong Mat_{nm}(A)$.

(3) Note that the Jacobson radical of a ring R is the intersection of all the left annihilators of simple left R-module, and is also the intersection of all maximal left ideals of R. To show one of inequalities $J(Mat_n(A)) \subseteq Mat_n(J(A))$, suppose that $[a_{kl}] \not\subseteq Mat_n(J(A))$. Then there is some entry $a_{kl} \not\subseteq J(A)$. Since $J(A)$ is the intersection of all the left annihilators of simple left A-module, there is a simple left A-module, say T, such that $a_{kl} \not\subseteq ann_A(T)$. Noting that $\oplus_1^n T$ is a simple left $Mat_n(A)$-module and $[a_{kl}] \not\subseteq ann_{Mat_n(A)}(\oplus_1^n T)$, we may conclude $[a_{kl}] \not\subseteq J(Mat_n(A))$.

For the other inequality, let $[a_{kl}] \in Mat_n(J(A))$, but not in $J(Mat_n(A))$. Then there is a maximal left ideal M of $Mat_n(A)$ such that $[a_{kl}] \not\subseteq M$ since $J(Mat_n(A))$ is the intersection of all maximal left ideals of $Mat_n(A)$. Consider the ideal $\langle [a_{kl}], M \rangle$ of $Mat_n(A)$. By the maximality, we have $\langle [a_{kl}], M \rangle = Mat_n(A)$. Thus there are $[b_{kl}] \in Mat_n \ (A)$ and $[c_{kl}] \in M$ such that $[b_{kl}][a_{kl}] + [c_{kl}] = I_n$. Since $[a_{kl}] \in Mat_n(J(A))$, so is $[b_{kl}][a_{kl}]$, which implies that $c_{kl} \in J(A)$ if $k \neq l$, and $c_{kk} - 1 \in J(A)$. Since each c_{kk} is a unit, using the Gaussian Elimination we can show that $[c_{kl}]$ is non-singular. This is a contradiction since $[c_{kl}] \in M$. In all, we have th equality.

(4) We need to find the number of bases of an n -dimensional vector space V over a field F (or, equivalently, the number of matrices such that all rows are linearly independent). Let $(e_1,\cdots,e_n)$ be a basis for V. Then the number of the first choice e_1 is q^n-1, and the second choice e_2 can be taken to be any vector which is not a multiple of e_1, and so there are q^n-q choices for e_2. The third component e_3 can not be of the form ae_1+be_2. Thus the number of e_3 is q^n-q^2. Continuing this process, we finally arrive at

$$|GL_n(F)|=(q^n-1)(q^n-q)(q^n-q^2)\cdots(q^n-q^{n-1}).$$

■

We also need the following facts for the proofs of our main theorems:

Facts 2.2. (1) (Structure Theorem for Artin rings[8]) An Artin ring A is uniquely (up to isomorphism) expressed as a finite direct product of Artin local rings.

(2) If A is a ring, then the quotient ring $A/J(A)$ is semisimple[9].

(3) (Wedderburn-Artin[9]) The following con- ditions on a ring A are equivalent:

(i) A is a non-zero semisimple left Artinian ring;

(ii) There exist division rings $D_1,\cdots,D_t$ and positive integers $n_1,\cdots,n_t$ such that $R\cong\oplus_{i=1}^{t}Mat_{n_i}(D_i)$.

(4) Every finite division ring is a field[9].

Even though Theorem 2.3 below also deals with a commutative ring case as well as a non-commutative case, we state and prove the following commutative case separately. First we compute the order of the general linear group $GL_n(A)$ over a finite local ring A. We define a local ring by a ring with a unique maximal ideal.

Theorem 2.3. Let A be a finite commutative ring with unity. Then

$$|GL_n(A)|=\prod_{i=1}^{r}|GL_n(A_i)|=\prod_{i=1}^{r}|\boldsymbol{m_i}|^{n^2}\cdot|GL_n(A_i/\boldsymbol{m_i})|,$$

where A_i is a local ring with a maximal ideal $\boldsymbol{m_i}$ for $i=1,\cdots,r$.

Proof. Since A is a finite commutative ring, which is Artinian, A is isomorphic to the finite direct product of local rings $(A_i,\boldsymbol{m_i})$, i.e., $A\cong\oplus_{i=1}^{r}A_i$, by Fact 2.2 (1). Since $GL_n(A)\cong\oplus_{i=1}^{r}GL_n(A_i)$ by Lemma 2.1, we know $|GL_n(A)|=\prod_{i=1}^{r}|GL_n(A_i)|$.

Now, to find the order of each $GL_n(A_i)$, consider a map $\varphi_i: GL_n(A_i)\to GL_n(A/\boldsymbol{m_i})$ defined by $\varphi_i([a_{kl}])=[\overline{a_{kl}}]$, where $\overline{a_{kl}}$ is the image of a_{kl} in $A/\boldsymbol{m_i}$. Then φ_i is a well-defined group homomorphism, and moreover is onto. Indeed, if $[\overline{a_{kl}}]\in GL_n(A_i/\boldsymbol{m_i})$, then there is $[\overline{b_{kl}}]\in GL_n(A_i\ /\boldsymbol{m_i})$ such that $[\overline{a_{kl}}][\overline{b_{kl}}]=\overline{I_n}$. Then $[a_{kl}][b_{kl}]=I_n+[m_{kl}]$ for $m_{kl}\in\boldsymbol{m_i}$. Let $[c_{kl}]=[a_{kl}][b_{kl}]$. Then an $n\times n$ matrix $[c_{kl}]$ is invertible since $1+m_{kk}$ is a unit in a local ring A_i, and so we can use the Gaussian elimimination. Thus $[a_{kl}]$ is also invertible, i.e., $[a_{kl}]\in GL_n(A_i)$ and $\varphi_i([a_{kl}])=[\overline{a_{kl}}]$. Let us consider a short exact sequence

$$0\to Ker(\varphi_i)\to GL_n(A_i)\xrightarrow{\varphi_i}GL_n(A_i/\boldsymbol{m_i}).\to 0$$

It is easy to check that $Ker(\varphi_i)=\{I_n+[m_{kl}]: m_{kl}\in\boldsymbol{m_i}\}$, and thus the order of $Ker(\varphi_i)$, $|Ker(\varphi_i)|=|\boldsymbol{m_i}|^{n^2}$\$. Hence

$$\begin{aligned}|GL_n(A_i)|&=|Ker(\varphi_i)||GL_n(A_i/\boldsymbol{m_i})|\\&=|\boldsymbol{m_i}|^{n^2}|GL_n(A_i/\boldsymbol{m_i})|,\end{aligned}$$

and

$$\begin{aligned}|GL_n(A)|&=\prod_{i=1}^{r}|GL_n(A_i)|\\&=\prod_{i=1}^{r}|\boldsymbol{m_i}|^{n^2}\cdot|GL_n(A_i/\boldsymbol{m_i})|.\end{aligned}$$

■

Now, we compute the order of the general linear group $GL_n(A)$ over an arbitrary finite ring A.

Theorem 2.4. Let A be a finite ring with identity. Then

$$|GL_n(A)|=|J(A)|^{n^2}\cdot\prod_{i=1}^{r}|GL_{n(i)}(K_i)|,$$

where $J(-)$ denotes the Jacobson radical of a ring, $n(i),\cdots,n(r)$ are positive integers, and each K_i is a finite field.

Proof. Let J_A be the Jacobson radical of A, and consider a map $\varphi : GL_{n(A)} \to GL_n(A/J_A)$ defined by $\varphi([a_{kl}]) = [\overline{a_{kl}}]$, where $\overline{a_{kl}}$ denotes the residue class of a_{kl} modulo J_A. Then φ is a well-defined group homomorphism, and we claim that φ is onto. If $[\overline{a_{kl}}] \in GL_n(A/J_A)$, then there is $[\overline{b_{kl}}] \in GL_n(A/J_A)$ such that $[\overline{a_{kl}}][\overline{b_{kl}}] = \overline{I_n}$. Thus $[a_{kl}][b_{kl}] - I_n \in Mat_n(J_A)$. Since $Mat_n(J_A) = J(Mat_n\ (A))$ by Lemma 2.1, we know that $[a_{kl}][b_{kl}] - I_n$ belongs to the intersection of all maximal left ideals of $Mat_n(A)$. Thus if $[a_{kl}] \not\in GL_{n(A)}$, then $[a_{kl}]$ belongs to M for some maximal left ideal M of $Mat_n(A)$, and so $I_n \in M$, which is a contradiction. Hence $[a_{kl}] \in GL_n(A)$, i.e., φ is onto.

Let us consider the following short exact sequence:

$$0 \to Ker(\varphi) \to GL_n(A) \xrightarrow{\varphi_i} GL_n(A/J(A)) \to 0.$$

It is easy to check that $Ker(\varphi) = \{I_n + [m_{kl}] : m_{kl} \in J_A\}$. Since the order of $Ker(\varphi)$, $|Ker(\varphi)| = |J_A|^{n^2}$, we have

$$\begin{aligned} |GL_n(A)| &= |Ker(\varphi)||GL_n(A/J_A)| \\ &= |J_A|^{n^2}|GL_n(A/J_A)|. \end{aligned}$$

It remains to compute $|GL_n(A/J_A)|$. Since $A/J(A)$ is a finite semi-simple ring (and thus artinian semi-simple) by Facts 2.2 (2), there exist fields $K_1, \cdots, K_r$ and positive integers $n_1, \cdots, n_r$ such that $A/J_A \cong \oplus_{i=1}^{r} Mat_{n_i}(K_i)$ by Facts 2.2 (3) and (4). Thus $|GL_n(A/J_A)| = \prod_{i=1}^{r} |GL_n(Mat_{n_i}(K_i))$. We note that $GL_n(Mat_{n_i}(K_i)) \cong GL_{n(i)}(K_i)$ by Lemma 2.1 , where $n(i) = n \times n_i$. Hence

$$|GL_n(A)| = |J(A)|^{n^2} \cdot \prod_{i=1}^{r} |GL_{n(i)}(K_i)| \qquad \blacksquare$$

Acknowledgments

Kisuk Lee was supported by Sookmyung Women's University Research Grants, 2014.

References

[1] K. Lee, “Use of algebraic theories in cryptography”, Journal of Natural Sciences Sookmyung Women's University, Vol 14, pp. 43-48, 2003.

[2] W. Diffie and M. Hellman, “New directions in cryptography”, IEEE T. Inform. Theory, Vol. 22, pp. 644-654, 1976.

[3] A. Odlyzko, “Discrete logarithms: the past and the future”, Design. Code. Cryptogr., Vol. 19, pp. 129-145, 2000.

[4] R. L. Rievest, A. Shamir, and L. Adleman, “A method for obtaining digital signatures, and public-key cryptosystems”, Commun. ACM, Vol. 21, pp. 120-126, 1978.

[5] N. Koblitz, “A course in number theory and cryptography”, 2nd ed., New York: Springer- Verlag, 1994.

[6] A. K. Lenstra and E. R. Verheul, “The XTR public key system”, in Advances in Cryptology-CRYPTO, New York: Springer-Verlag, pp. 1-19, 2000.

[7] J. Koh, “Commutative algebra and cryp- tography”, 2nd Conference on the Development of Public Key Cryptosystems, KISA, 1999.

[8] M. F. Atiyah and I. G. Macdonald, “Intro- duction to commutative algebra”, Boston: Addison-Wesley, 1969.

[9] T.W. Hungerford, “Algebra”, New York: Springer, 1980.