M - 6

THE PROPERTIES OF GROUP OF 3×3 MATRICES OVER INTEGERS MODULO PRIME NUMBER

Ibnu Hadi, Yudi Mahatma
ibnu_unj@yahoo.co.id

Universitas Negeri Jakarta, Jl. Pemuda No. 10 Rawamangun Jakarta Timur, 13220 Indonesia

Abstract

This paper discusses about group consists of 3×3 matrices over integers modulo prime number. We will consider the order of the group and some of the subgroups. We also determine the normality of the subgroups.

Key words: integers modulo *p*, group, subgroup

INTRODUCTION

Group is one of the familiar subject in algebra. In this paper, we will discuss about group of 3×3 matrices over integers modulo prime number. This topic came from a problem arose in Herstein book. The problem is about determining the order of the group of 2×2 matrices over integers modulo prime number p. By observing the determinants, Hadi got the result.

In group of 3×3 matrices, the difficulty came due to the complexity of the determinant of 3×3 matrix. Hence, we will use another method based on theorems in linear algebra.

DISCUSSION

The set of all $m\times n$ matrices over real, obviously is an addition group. In order to create a multiplication group of matrices, we need some requirements. First, the matrices should be square. Thus, $m=n$. Next, since the group requires existence of the inverse element, then the matrices should be nonsingular i.e its determinant is not zero. It can be easily shown that the set of all nonsingular matrices over real forms a multiplication group. The group, of course, is infinite.

If we change the entries of the matrices with integers modulo p, where p is prime, then we may construct a finite multiplication group of matrices. In this paper, we only considering 3×3 matrices over integers modulo p, where p is prime number. For example, suppose that

$$G=\left\{\begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix} \middle| a_{ij}\in Z_p \right\}$$

is a set of 3×3 matrices over Z_p. Here, $n(G)=p^9$. Note that G consists of singular and nonsingular matrices. The question is : how many elements of G are nonsingular? To answer this question we need the concept about rank of a matrix.

Definition If $S=\{v_1,v_2,\ldots,v_n\}$ is a nonempty set of vectors, then the equation $k_1v_1+k_2v_2+\ldots+k_rv_r=0$ has at least one (trivial) solution, that is $k_1=k_2=\ldots=k_r=0$. If this is the only solution, then S is called a *linearly independent set*. Otherwise, S is called a *linearly dependent set*.

Theorem A set S with two or more vectors is

a. linearly dependent if and only if there is a vector in S that can be expressed as a linear combination of another vectors in S.
b. linearly independent if and only if no vector in S can be expressed as a linear combination of the other vectors in S.

Definition The common dimension of row space and column space of a matrix A is called the rank of A and is denoted by $rank(A)$.

Theorem An $m\times m$ matrix A is nonsingular if and only if $rank(A)=m$.

So far, we already have the tools we need to determine how many nonsingular element in the set of 3×3 is. Now we recall the basic concept of group.

Definition A nonempty set G is said to form a *group* if there defined a binary operation in G, called the product and denoted by "$\bullet$", such that

1. For every $a,b\in G$, $a\bullet b\in G$ (closed under the operation).
2. For every $a,b,c\in G$, $a\bullet(b\bullet c)=(a\bullet b)\bullet c$ (associative law).
3. There exists an element $e\in G$ such that $a\bullet e=e\bullet a=a$ for all $a\in G$ (the existence of an identity element in G).
4. For every $a\in G$ there exists an element $a^{-1}\in G$ such that $a\bullet a^{-1}=a^{-1}\bullet a=e$ (the existence of inverses in G).

Definition A group G is said to be *Abelian* (or *commutative*) if for every $a,b\in G$, $a\bullet b=b\bullet a$.

A group which is not Abelian is called non-Abelian. For the case of multiplication group of matrices, it is clear that the group is non-Abelian.

For a group G, the number of elements in G is called *the order of* G and denoted by $o(G)$. If $o(G)<\infty$ then we say that G is finite, otherwise it is infinite.

NUMBER OF NONSINGULAR 3×3 MATRICES OVER INTEGERS MODULO P

Now we start deriving the formula that gives the order of group of 3×3 matrices over integers modulo p. Suppose that

$$G=\left\{\begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33}\end{bmatrix} \middle| a_{ij}\in \mathrm{Z}_p \right\}.$$

Here, $n(G)=p^9$. We will count the number of singular elements in G.

Case I For matrices whose rank is zero, there is only one matrix in G, that is

$$\begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0\end{bmatrix}.$$

Case II For matrices whose rank is 1, there are some possibilities.

1. If the first and the second rows are $\begin{bmatrix}0 & 0 & 0\end{bmatrix}$, then the third row can not be $\begin{bmatrix}0 & 0 & 0\end{bmatrix}$. There are p^3-1 possibilities for the row.
2. If the first row is $\begin{bmatrix}0 & 0 & 0\end{bmatrix}$ and the second row is not $\begin{bmatrix}0 & 0 & 0\end{bmatrix}$, then the third row must be a multiplication of the second row, that is if the second row is $\begin{bmatrix}a & b & c\end{bmatrix}$ then the third row must be $\begin{bmatrix}ka & kb & kc\end{bmatrix}$ where $k=0,1,2,\ldots,p-1$. Since there are p^3-1 ways to perform the second row, then the total number of matrices of this type is $\left(p^3-1\right)p=p^4-p$.
3. If the first row is not $\begin{bmatrix}0 & 0 & 0\end{bmatrix}$ then the second and the third row must be a multiplication of the first row. If the first row is $\begin{bmatrix}x & y & z\end{bmatrix}$ then second row must in the form of $\begin{bmatrix}mx & my & mz\end{bmatrix}$ and third row must in the form of $\begin{bmatrix}nx & ny & nz\end{bmatrix}$ where $m,n=0,1,2,\ldots,p-1$. Since there are p^3-1 ways to perform the first row, then the total number of matrices of this type is $\left(p^3-1\right)p^2=p^5-p^2$.

Based on these facts, there are $\left(p^3-1\right)+\left(p^4-p\right)+\left(p^5-p^2\right)=p^5+p^4+p^3-p^2-p-1$ matrices in G whose rank is 1.

Case III For matrices whose rank is 2, there are some possibilities.

1. If the first row is $\begin{bmatrix}0 & 0 & 0\end{bmatrix}$ then the second row can not be $\begin{bmatrix}0 & 0 & 0\end{bmatrix}$ and the second and the third row must linearly independent. It means that the third row must not a multiplication of the second row. So, if the second row is $\begin{bmatrix}p & q & r\end{bmatrix}$ then the third row can be in any form except $\begin{bmatrix}lp & lq & lr\end{bmatrix}$ where $l=0,1,2,\ldots,p-1$. Since there are p^3-1 ways to perform the second row and p^3-p ways to perform the third row then

there are $\left(p^3-1\right)\left(p^3-p\right)=p^6-p^4-p^3+p$ matrices of this type.

2. If the first row is not $\begin{bmatrix}0 & 0 & 0\end{bmatrix}$ and the second row is a multiplication of the first row then the third row must linearly independent from first row. Since there are p^3-1 ways to perform the first row, p ways to perform the second row, and p^3-p ways to perform the third row, then there are $\left(p^3-1\right)p\left(p^3-p\right)=p^7-p^5-p^4+p^2$ matrices of this type.
3. If the first row is not $\begin{bmatrix}0 & 0 & 0\end{bmatrix}$ and the second row is linearly independent from the first row then the third row must be the linear combination of the first and the second rows. Hence, if the first row is $\begin{bmatrix}a_1 & b_1 & c_1\end{bmatrix}$ and the second row is $\begin{bmatrix}a_2 & b_2 & c_2\end{bmatrix}$ then the third row must be in the form of $\begin{bmatrix}\alpha a_1+\beta a_2 & \alpha b_1+\beta b_2 & \alpha c_1+\beta c_2\end{bmatrix}$ where $\alpha,\beta=0,1,2,\ldots,p-1$. Since there are p^3-1 ways to perform the first row, p^3-p ways to perform the second row, and p^2 ways to perform the third row, then there are $\left(p^3-1\right)\left(p^3-p\right)p^2=p^8-p^6-p^5+p^3$ matrices of this type.

Based on these facts, there are $p^8+p^7-2p^5-2p^4+p^2+p$ matrices in G whose rank is 2.

Overall, we have that the total number of singular matrices in G is $p^8+p^7-p^5-p^4+p^3$. Therefore the number of nonsingular matrices in G is $p^9-p^8-p^7+p^5+p^4-p^3=(p-1)^3\,p^3\,(p+1)\left(p^2+p+1\right)$.

For example, the order of group of 3×3 nonsingular matrices over 0 and 1 is then 168.

THE SUBGROUPS

Let G be the group of all nonsingular 3×3 matrices over Z_p. Let H be the set of all 3×3 matrices over Z_p whose determinant is 1. It can be easily shown that H is a subgroup of G. In order to determine the order of H, consider that if $A,B\in G$ then $A\equiv B \bmod H$ if and only if $AB^{-1}\in H$ if and only if $\left|AB^{-1}\right|=1$ if and only if $|A|=|B|$. Therefore, there are $p-1$ equivalence classes (corresponds to $p-1$ different determinants of elements of G) of cosets of H in G. Hence $o(H)=o(G)/(p-1)=p^8-p^6-p^5+p^3$. Further, H is normal in G for if $A\in G$ and $K\in H$ then $\left|AKA^{-1}\right|=1$ and hence $AKA^{-1}\in H$ which shows that $AHA^{-1}\subseteq H$.

Now, what is the center of G? Let Z be the center of G. We know that Z is a subgroup of G. Let

$$X=\begin{bmatrix}a & b & c\\ d & e & f\\ g & h & i\end{bmatrix}\in Z\,.$$

Note that the matrices

$$A=\begin{bmatrix}1&1&1\\0&1&1\\0&0&1\end{bmatrix} \text{ and } B=\begin{bmatrix}0&0&1\\0&1&0\\1&0&0\end{bmatrix}$$

both are in G. Then, since $AX = XA$, we have

$$\begin{bmatrix}a+d+g&b+e+h&c+f+i\\d+g&e+h&f+i\\g&h&i\end{bmatrix}=\begin{bmatrix}a&a+b&a+b+c\\d&d+e&d+e+f\\g&g+h&g+h+i\end{bmatrix}$$

that can be concluded that $a=e=i$, $b=f$, and $d=g=h=0$. Next, since $BX = XB$, we have

$$\begin{bmatrix}g&h&i\\d&e&f\\a&b&c\end{bmatrix}=\begin{bmatrix}c&b&a\\f&e&d\\i&h&g\end{bmatrix}$$

which gives us $b=h$. Hence, from the previous result we have $b=f=0$. We have shown that the matrices in Z are in the form

$$\begin{bmatrix}k&0&0\\0&k&0\\0&0&k\end{bmatrix}=kI_3$$

where $k\in Z_p$. Hence $o(Z)=p-1$. Clearly, Z is normal in G.

Now consider the set of all diagonal matrices in G. Denote this set by D. In set notation,

$$D=\left\{\begin{bmatrix}s&0&0\\0&t&0\\0&0&u\end{bmatrix}\middle| s,t,u\in Z_p\right\}.$$

Clearly, D is a subgroup of G with order $(p-1)^3$. This subgroup is not normal in G except if $p=2$. To show this, we can verify that

$$\begin{bmatrix}1&1&1\\0&1&1\\0&0&1\end{bmatrix}\begin{bmatrix}k&0&0\\0&l&0\\0&0&m\end{bmatrix}\begin{bmatrix}1&1&1\\0&1&1\\0&0&1\end{bmatrix}^{-1}=\begin{bmatrix}k&-k+l&-l+m\\0&l&-l+m\\0&0&m\end{bmatrix}.$$

In order to make the matrix in the right side of the equation above belongs to D, it requires $k=l=m$ while if $p>2$ we can choose different values for k, l, and m.

CONCLUSION AND SUGGESTION

Basically, multiplication group of square matrices is easy to verified. But, if this group is related with some other theory, this can be interesting. Many things can be observed, like the order of the group, the center, kind of subgroups, etc. If we expand the order of the matrices, of course the problem will be more complex. It is still possible to make an observation about group of larger order of matrices over integers modulo prime number.

REFERENCES

[1] Anton, Howard dan Chris Rorres, (2005), *Elementary Linear Algebra 9nd ed.*, John Wiley and Sons, New York

[2] Burton, David M, (2002), *Elementary Number Theory*, McGraw Hill

[3] Durbin, John R, (2005), *Modern Algebra An Introduction 6nd ed*, John Wiley and Sons, New York

[4] Herstein, I.N, (1975), *Topics in Algebra*, John Wiley and Sons, New York

[5] Hungerford, Thomas W, (1974), *Algebra*, Springer-Verlag, New York

[6] Hadi, Ibnu, (2013), *Karakteristik Grup yang Dibangun oleh Himpunan Matriks Berukuran 2x2 dengan Entri Bilangan Bulat Modulo P*, Prosiding Seminar Matematika dan Pendidikan Matematika, Malang, 18 Mei 2013

[7] Rosen, Kenneth H, (1984), *Elementary Number Theory and Its Application*, Addison-Wesley Publishing Company

[8] Paley, Hiram dan Paul M Weichsel, (1972), *Elements of Abstract and Linear Algebra*, Holt, Rinehart and Winston Inc., New York

[9] Raisinghania, M.D dan R.S Aggarwal, (1980), *Modern Algebra*, S Chand and Company Ltd., New Delhi