M - 5

CHARACTERISTIC OF GROUP OF MATRIX 3X3 MODULO P, P A PRIME NUMBER

Ibnu Hadi, Yudi Mahatma

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

Abstract

This paper discussed about group based on a set consists of matrix 3x3 with elements integers modulo p, p a prime number. It begin with determine the number of matrix which hold in set matrix. Using combination of element of integer modulo p, p prime number, we get the total element in matrix set is finite. By group theory, we characterisation this set such that the properties of group theory is hold

Key words: group theory, integers modulo p

INTRODUCTION

Concept of group is one of the familiar things in algebra. Problems in group usually depends on which concept are used. In this paper, we will discussed about one example of group of matrix 3x3 with element integer modulo p, p is prime number. This problem is expand from the original problem in Herstein book. First problem arose in problem in Herstein book for matrix 2x2. The difficulties of this problem is to determine the number of matrix in this group because element-element in this matrix depends on how many integers can be used. Using combination of element in matrix 2x2, Hadi got the result.

In matrix 3x3, we cannot using same concept to determine how many matrix can be formed where the elements of matrix is integers modulo p, p prime number. So, the first characteristic of this group is how to find number of elements in this group. After that, we can construct a group with this matrix set. Our goal is to generated a group using this matrix and apply some concept of group to establish this example of group. The benefit in this paper is to rich examples of group especially group of matrix such that we can more curious about group of matrix. In addition, we will know the general form of group of matrix with elements integers modulo p, p prime number.

DISCUSSION

Before we enter far, we need some concept related to matrix 3x3 and concept of group. Afetr that, we can characterize group of matrix using this concept.

Definition. A matrix 3x3 is matrix with form

$$\begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix}$$

where $a_{11}, a_{12}, \ldots, a_{33}$ are entries of matrix.

Definition. A matrix is called singular if determinant of matrix is equal zero. On the other hand, nonsingular matrix has determinant not zero.

In this paper, we use entries of matrix are integers modulo p, p prime number. For example, if

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

is a set of matrix 3x3, let $p = 2$, we get the number of elements of G is 2^9. Note that, all matrix in G consists of singular and nonsingular matrix. So, if we construct some set with p prime number, we have the elements of this set is p^9. This paper will construct group of matrix using this set and because of that, we have to make the matrix set must consist only nonsingular matrix. To solve that, we use concept of rank of matrix.

Definition. If $S = \{v_1, v_2, \ldots, v_n\}$ is a nonempty set of vectors, then the vector equation $k_1 v_1 + k_2 v_2 + \ldots + k_r v_r = 0$ has at least one solution, namely $k_1 = 0, k_2 = 0, \ldots, k_r = 0$. If this is the only solution, then S is called a linearly independent set. If there are other solutions, then S is called a linearly dependent set.

Theorem. A set S with two or more vectors is
a. linearly dependent if and only if at least one of the vevtors in S is expressible as a linear combination of the other vectors in S.
b. linearly independent if and only if no vector in S is expressible as a linear combination of the vectors in S.

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

So far, we already have definition to determine how many element in set of matrix 3x3. Now we define basic concept of group.

Definition. A nonempty set of elements G is said to form a group if in G there is defined a binary operation, called the product and denote by $\bullet$, such that
1. $a, b \in G$ implies that $a \bullet b \in G$ (closed).
2. $a, b, c \in G$ implies that $a \bullet (b \bullet c) = (a \bullet b) \bullet c$ (assosiatif 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, naturally enough, non-Abelian. In this cases, because we evaluate set of matrix to be a group, it is clear that group of matrix is non-Abelian group.

NUMBER OF ELEMENT OF MATRIX 3X3 MODULO P, P PRIME NUMBER

Before we construct group from this set, we must determine the number of this matrix. It is important to know because can be influence the characteristic of group whis is formed. Let

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

Let $p=2$. Then all element $a_{11}, a_{12}, \ldots, a_{33}$ of G only 0 and 1. So total element of G, denoted with $n(G)$, is $2^9 = 512$. If we write

$$I_3 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix},$$

then $I_3 \in G$. It is clear that this set is nonempty and I become identity element in group of this matrix. Remember that group of matrix must be consists of nonsingular to ensure that each matrix have invers element. So, for arbitrary p prime number, it is clear that $n(G) = p^9$. Fortunately, this set is finite for some p. So we determine nonsingular matrix using how many singular matrix in this set. Now we evaluate how many singular matrix in G.

Case I. For matrix with rank zero, we have only one matrix in G i.e

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

Case II. For matrix with rank 1, there is some possibilities.

1. If first row and second row of matrix is $\begin{bmatrix} 0 & 0 & 0 \end{bmatrix}$, then third row must not equal $\begin{bmatrix} 0 & 0 & 0 \end{bmatrix}$. Then we have $p^3 - 1$ possibilities.

2. If first row of matrix is $\begin{bmatrix} 0 & 0 & 0 \end{bmatrix}$ and second row is not equal $\begin{bmatrix} 0 & 0 & 0 \end{bmatrix}$, then third row must be multiplication of second row which is if second row has form $\begin{bmatrix} a & b & c \end{bmatrix}$ then third row has form $\begin{bmatrix} ka & kb & kc \end{bmatrix}$ where $k = 0,1,2,\ldots,p-1$. The possibility of second row is $p^3 - 1$. So, the total matrix for this type is $\left(p^3 - 1\right)p = p^4 - p$.

3. If first row of matrix is not $\begin{bmatrix} 0 & 0 & 0 \end{bmatrix}$ then second row and third row must be multiplication of first row. Let first row is $\begin{bmatrix} x & y & z \end{bmatrix}$. Then second row must has form $\begin{bmatrix} mx & my & mz \end{bmatrix}$ and

third row must has form $\begin{bmatrix} nx & ny & nz \end{bmatrix}$ where $m,n = 0,1,2,\ldots, p-1$. The possibilities of first row is p^3-1. So, the total matrix of this form is $\left(p^3-1\right)p^2 = p^5 - p^2$.

Based on these fact, we have totally for matrix with rank one is

$$\left(p^3-1\right)+\left(p^4-p\right)+\left(p^5-p^2\right) = p^5+p^4+p^3-p^2-p-1.$$

Case III. For matrix with rank 2, there is some possibilities.

1. Let assume that first row has form $\begin{bmatrix} 0 & 0 & 0 \end{bmatrix}$. Then second row not equal $\begin{bmatrix} 0 & 0 & 0 \end{bmatrix}$ and second and third row must linearly independent. It means that third row must be not multiplication of second row. So, if second row has form $\begin{bmatrix} p & q & r \end{bmatrix}$ then third row must not has form $\begin{bmatrix} lp & lq & lr \end{bmatrix}$ where $l = 0,1,2,\ldots, p-1$. The possibilities for second row is p^3-1 and for third row is p^3-p. So the total matrix of this type is

$$\left(p^3-1\right)\left(p^3-p\right) = p^6-p^4-p^3+p$$

2. Let assume that first row is not equal $\begin{bmatrix} 0 & 0 & 0 \end{bmatrix}$ and second row is multiplication of first row. Then third row must linearly independent from first row. Note that the possibilities of first row is p^3-1, second row is p, and third row is p^3-p, then we have total matrix for this type is $\left(p^3-1\right)p\left(p^3-p\right) = p^7-p^5-p^4+p^2$.

3. Let assume that first row not equal $\begin{bmatrix} 0 & 0 & 0 \end{bmatrix}$ and third row is not multiplication of first row. Then third row must be linear combination of first row and second row. So, if first row is $\begin{bmatrix} a_1 & b_1 & c_1 \end{bmatrix}$ and second row is $\begin{bmatrix} a_2 & b_2 & c_2 \end{bmatrix}$ then third row must be $\begin{bmatrix} \alpha a_1+\beta a_2 & \alpha b_1+\beta b_2 & \alpha c_1+\beta c_2 \end{bmatrix}$ where $\alpha,\beta = 0,1,2,\ldots, p-1$. Because the possibilities of first row is p^3-1, second row is p^3-p, third row is p^2, then total matrix in this form is

$$\left(p^3-1\right)\left(p^3-p\right)p^2 = p^8-p^6-p^5+p3.$$

So, total matrix with rank 2 is $p^8+p^7-2p^5-2p^4+p^2+p$.

Based on three cases, we have all singular matrix is sum of matrix with rank zero, rank 1, and rank 2 and we get

$$p^8+p^7-p^5-p^4+p^3.$$

For $p=2$, we have singular matrix is 344 matrix. On the other hand, we get number of non singular matrix is 168. It is very amazing. Here, we do not interest to find all matrix with this property. We only want to know the characteristic of group from this set.

GROUP OF MATRIX 3X3 MODULO P, P PRIME NUMBER

Again, let G is all nonsingular matrix with property

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

From previous section, G is nonempty set with $n(G)=p^9-p^8-p^7+p^5+p^4-p^3<\infty$. Now we define multiplication matrix as binary operation in this set. We will prove that G under this operation form a group. Let

$$A=\begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix} \text{ and } B=\begin{bmatrix} b_{11} & b_{12} & b_{13} \\ b_{21} & b_{22} & b_{23} \\ b_{31} & b_{32} & b_{33} \end{bmatrix}$$

two elements of G. Then we have

$$AB=\begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix}\begin{bmatrix} b_{11} & b_{12} & b_{13} \\ b_{21} & b_{22} & b_{23} \\ b_{31} & b_{32} & b_{33} \end{bmatrix}$$

$$=\begin{bmatrix} a_{11}b_{11}+a_{12}b_{21}+a_{13}b_{31} & a_{11}b_{12}+a_{12}b_{22}+a_{13}b_{32} & a_{11}b_{13}+a_{12}b_{23}+a_{13}b_{33} \\ a_{21}b_{11}+a_{22}b_{21}+a_{23}b_{31} & a_{21}b_{12}+a_{22}b_{22}+a_{23}b_{32} & a_{21}b_{13}+a_{22}b_{23}+a_{23}b_{33} \\ a_{31}b_{11}+a_{32}b_{21}+a_{33}b_{31} & a_{31}b_{12}+a_{32}b_{22}+a_{33}b_{32} & a_{31}b_{13}+a_{32}b_{23}+a_{33}b_{33} \end{bmatrix}.$$

For each entry in AB, it can be proved that belongs to integer modulo p, p prime number. Because A, B is nonsingular matrix, we get AB is nonsingular. So, closed property of group hold. Furthermore, it is clear that assosiative law hold for G. For identity element of G, we choose I_3 because $I_3 \bullet A = A \bullet I_3 = A$ for all $A \in G$. Therefore, for all $A \in G$, we can define $A^{-1} \in G$ because A is nonsingular matrix. So we have a finite group of matrix 3x3 with element integer modulo p, p prime. We usually write number elements of G is order of G ($o(G)$). Note that this group is non-Abelian because properties of matrix under multiplication is not always commutative.

Definition. A nonempty subset H of group G is said to be a subgroup of G if, under the product of G, H itself forms a group.

It is clear that G always has subgroup. Let $H_1=\{I_3\}$. Then H_1 and G forms trivial subgroups. The problems is to find nontrivial subgroup for G. But, by Lagrange theorem below,

Theorem. If G is a finite group and H is a subgroup of G, $o(H)$ is a divisor of $o(G)$.

Based on this theorem, G must have nontrivial subgroup.

CONCLUSION AND SUGGESTION

Basicly, group from matrix under multiplication is easy to prove. But, if this group is related with some theory of group, this can be interesting. The first difficult to construct group of matrix is we must ensure the number of element of matrix. If we expand order of matrix, it may more complex. There is no standard procedure to solve that. Fortunately, many concept of group holds in this group.

This paper only evaluate for matrix with order 3x3 using concept of rank matrix. This discussion is very possible to expand to matrix with order nxn where elements of matrix is integers modulo p, p prime. It may get some general example of finite group especially group of matrix.

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