All Cyclic Subgroups In Group $(\mathbf{Z}_m \times \mathbf{Z}_n, +)$ Using Python

Bobbi Rahman, Samsul Arifin, Indrabayu Muktyas

Abstract— $(\mathbf{Z}_m \times \mathbf{Z}_n, +)$ is a group under addition modulo m,n. Cyclic subgroup is a subgroup that generated by one of in a group. Python is a multipurpose programming language, easy to study, and can run on various operating system platforms. Python also can calculate the modulo operations on groups $(\mathbf{Z}_m \times \mathbf{Z}_n, +)$. In this paper, we will determine all cyclic subgroup of group $(\mathbf{Z}_m \times \mathbf{Z}_n, +)$ using Python.

Index Terms— Group $(\mathbf{Z}_m \times \mathbf{Z}_n, +)$, cyclic subgroup, generator, order of element, Python

1 Introduction

A group is a set G with a binary operations *, so that closed, associative, there is an identity element and each element has an inverse. If a group G has properties a*b=b*a, for any a and b in G, then we said that group G is commutative. The basic properties of groups can be studied in [6], [9] and [11]. A cyclic group G is a group in which any element g in G can be written as gn for $n = 1, 2, \ldots$ Furthermore, the characteristics of cyclic groups can be seen in [16], [7] and [12]. Subgroup is a subset of H on a G which is also a group with the same binary operation in G. For an element group $a \in G$, we can form a subset S that containing all elements of G which contains all forms $a^n, n = 1, 2, \ldots$. This subset forms a subgroup in G, and called a cyclic subgroup that generate by a. Recall that any cyclic group is commutative and subgroups of a cyclic group are also cyclic. The set of all integers modulo n, denoted by $\mathbf{Z}_n$, is a group of modulo addition operations. This group is very important in studying a group, because many concepts in group theory use it as an example. The group $(\mathbf{Z}_n, +)$ are constructed using the division algorithm on the set of all integers. This process can be studied in [11] and [1]. Furthermore, the formation process of the group $(\mathbf{Z}_m \times \mathbf{Z}_n, +)$ can be studied in [3] and [7]. Python is a multipurpose programming language and easy to study (see [15]). Python can also run on various operating system platforms, such as Windows, Linux, Mac OS, Android (see [8]), and the others. In this paper we study about determination of all cyclic subgroups of group $(\mathbf{Z}_m \times \mathbf{Z}_n, +)$ using Python. Review about the notion of group and cyclic subgroup will be discussed in Session 2. The construction of group $(\mathbf{Z}_m \times \mathbf{Z}_n, +)$ will be given in Session 3. Furthermore, a study of the Python program which is the main result of this paper and its output will be discussed in Session 4.

- [1,3]*Mathematics Education Department, STKIP Surya, Tangerang, Indonesia 15115. E-mail: bobbi.rahman@stkipsurya.ac.id, indrabayu.muktyas@stkipsurya.ac.id*
- [2]*Faculty of Science and Technology, Universitas Binawan, Jakarta, Indonesia 13630. E-mail: arifin@binawan.ac.id*

2 The Notion Of Group And Cyclic Subgroup

In this session, we will discussed about groups and cyclic subgroups. The following are the definitions of a groups.

Definition 2.1. Gallian [7]. Group

Let G be a set together with a binary operation (usually called multiplication) that assigns to each ordered pair (a, b) of elements of G an element in G denoted by ab. We say G is a group under this operation if the following three properties are satisfied.

a) **Associativity**. The operation is associative; that is, $(ab)c = a(bc)$ for all a, b, c in G.
b) **Identity**. There is an element e (called the identity) in G such that $ae = ea = a$ for all a in G.
c) **Inverses**. For each element a in G, there is an element b in G (called an inverse of a) such that $ab = ba = e$.

Gallian [7] has shown that the identity and inverse of any elements on a group are unique, and also there's a cancellation and Socks-Shoes property on a group. We will given a notion of special group which is very important in learning of group, because many concepts in group theory use it as an example. The group is constructed using the division algorithm on the set of all integers. The binary operations addition modulo n and multiplication modulo n on the set {0, 1, 2, . . . , n-1}, which we denote by $\mathbf{Z}_n$, play an extremely important role in abstract algebra. In certain situations we will want to combine the elements of $\mathbf{Z}_n$ by addition modulo n only. The group $\mathbf{Z}_n$ under addition modulo n will denote by $(\mathbf{Z}_n, +)$. Next is a discussion of cyclic subgroups. Following are the definitions of cyclic groups and the generator of a group.

Definition 2.2. Gallian [7]. Subgroup

A group G is called **cyclic** if there is an element a in G such that $G = \left\{ a^n \middle| n \in \mathbf{Z}^+ \right\}$. Such an element a is called a **generator** of G. We may indicate that G is a cyclic group generated by a

by writing $G = \langle a \rangle$. Let $(G,*)$ is a group and $H \subseteq G$ is a subset not empty. Recall that the set H is called a subgroup of G if H is also a group of with same "binary operations" in group G, denoted by $H \subseteq G$ (see [9]). Rotman [16] explained about subgroup test that a subset of a group can be tested whether a subgroup or not, ie, if H is a subset of group G, then H is a subgroup of G if and only if $(\forall a,b \in H)(a * b^{-1} \in H)$. Furthermore, Dummit [5] show us that for an element $g \in G$, we can forms a subgroup in G by g.

Theorem 2.3. Dummit [5]. Cyclic Subgroup

Let G is a group and $g \in G$, then $\langle g \rangle = \{ g^n \mid n \in \mathbf{Z}^+ \}$ is a subgroup of G. Furthermore, $\langle g \rangle$ is called the **cyclic subgroup** of G which is generate by g. Recall that the order of a subgroup is the number of elements of the subgroup. The notion of order of a group element is as follows.

Definition 2.4. Gallian [7]. Order of an Element

The **order** of an element g in a group G is the smallest positive integer n such that $g^n = e$. (In additive notation, this would be $ng = 0$.) If no such integer exists, we say that g has **infinite order**. The order of an element g is denoted by |g|. The following is example of a group which will closed this session. Consider a group $(\mathbf{Z}_{10},+)$ under addition modulo 10. Since $1.2 = 2$, $2.2 = 4$, $3.2 = 6$, $4.2 = 8$, $5.2 = 0$, we will get that $|2| = 5$. Similar computations show that |0| = 1, |7| = 10, |5| = 2, |6| = 5. Here 2.2 is an abbreviation for 2 + 2, 3.2 is an abbreviation for 2 + 2 + 2, etc. (Gallian [7])

3 THE GROUP $(\mathbf{Z}_m \times \mathbf{Z}_n, +)$

In this session, we will study about the construction of group $(\mathbf{Z}_m \times \mathbf{Z}_n, +)$. In this paper we assumed that all groups are commutative. The following is definition of direct product of some groups.

Definition 3.1. Gallian [7]. Direct Product

a) Let $G_1, G_2, ..., G_n$ be a finite collection of groups. The **external direct product** of $G_1, G_2, ..., G_n$, written as $G_1 \oplus G_2 \oplus ... \oplus G_n$, is the set of all n-tuples for which the i-th component is an element of G_i, $i = 1, ..., n$, and the operation is componentwise.Moreover, in symbols,

$$G_1 \oplus G_2 \oplus ... \oplus G_n = \{(g_1, g_2, ..., g_n) \mid g_i \in G_i, i = 1, ..., n\}$$

b) We say that G is **the internal direct** product of H and K and write $G = H \times K$ if H and K are normal subgroups of G and $G = HK$ and $H \cap K = \{e\}$.

Direct product of two groups is a group with identity. Here is a construction of a new group from two given groups.

Definition 3.2. Rotman [16]. Group of Direct Product

If H and K are groups, then their direct product, denoted by $H \oplus K$, is the set of all ordered pairs (h,k) with $h \in H$ and $k \in K$ equipped with the operation (h,k)(h',k') = (hh',kk'). It is easy to check that the direct product $H \oplus K$ is a **group** with the identity is (1,1) and $(h\ k)^{-1} = (h^{-1},k^{-1})$.

The following is an example of a group which is the direct product of two groups. Let

$$\mathbf{Z}_2 \oplus \mathbf{Z}_3 = \{(0,0),(0,1),(0,2),(1,0),(1,1),(1,2)\}.$$

Clearly, this is an Abelian group of order 6. Consider the subgroup of $(\mathbf{Z}_2 \oplus \mathbf{Z}_3, +)$ generated by (1,1). Since the operation in each component is addition, we have (1,1) = (1,1), 2(1,1) = (0,2), 3(1,1) = (1,0), 4(1,1) = (0,1), 5(1,1) = (1,2), and 6(1, 1) = (0, 0), so $\mathbf{Z}_2 \oplus \mathbf{Z}_3 = \langle (1,1) \rangle$. Hence $(\mathbf{Z}_2 \oplus \mathbf{Z}_3, +)$ is cyclic. It follows that $\mathbf{Z}_2 \oplus \mathbf{Z}_3 \cong \mathbf{Z}_6$ (Gallian [7].)

Here is the definition of cartesian product.

Definition 3.3. Huang [10]. Cartesian Product

The **Cartesian Product** of sets $S_1, S_2, ..., S_n$ is the set of all pairwise of n-tupesl $(a_1, a_2, ..., a_n)$ where $a_i \in S_i$ for $i = 1, 2, ..., n$, i.e

$$\prod_{i=1}^{n} S_i = S_1 \times S_2 \times ... \times S_n = \{(a_1, a_2, ..., a_n) \mid a_i \in S_i, i = 1, 2, ..., n\}.$$

As the next theorem shows, the conditions in the definition of internal direct product were chosen to ensure that the two products are isomorphic.

Theorem 3.4. Gallian [7].

If a group G is the internal direct product of a finite number of subgroups $G_1, G_2, ..., G_n$, then G is isomorphic to the external direct product of $G_1, G_2, ..., G_n$, i.e. $G_1 \times G_2 \times ... \times G_n \cong G_1 \oplus G_2 \oplus ... \oplus G_n$.

Here is a properties of direct products of two groups.

Lemma 3.5. Huang [10].

The following statements are true:

1. Let m and n be positive integers. If $\gcd(m,n) = 1$ (i.e. m and n are relative prime), then $\mathbf{Z}_m \times \mathbf{Z}_n$ is cyclic and is isomorphic to $\mathbf{Z}_{mn}$, and $(1,1)$ is a generator of $\mathbf{Z}_m \times \mathbf{Z}_n$. If $\gcd(m,n) \neq 1$ then $\mathbf{Z}_m \times \mathbf{Z}_n$ is not cyclic.
2. The group $\prod_{i=1}^{n} \mathbf{Z}_{m_i}$ is cyclic and is isomorphic to $\mathbf{Z}_{m_1 \cdots m_n}$ if and only if the numbers m_i for $i = 1, ..., n$ are pairwise relative prime, that is, the gcd of any two of them is 1.
3. If a positive integer n is factorized as a product of powers

of distinct prime numbers: $n = p_1^{n_1} \dots p_r^{n_r}$ then $Z_n \cong Z_{p_1^{n_1}} \times \dots \times Z_{p_r^{n_r}}$.

Here is the sufficient and necessary conditions for a direct sum of two groups, $G \oplus H$, to be cyclic.

Theorem 3.6. Gallian [7].
Let G and H be finite cyclic groups. Then $G \oplus H$ is cyclic if and only if |G| and |H| are relatively prime. Consider the following example. Note that $(Z_5)^2 \not\cong Z_{5^2}$. The group $(Z_5)^2 = Z_5 \times Z_5$ is not cyclic but $Z_{5^2} = Z_{25}$ is cyclic (Huang [10]). Consider example below which is about a cyclic group that direct product of two groups. Also consider another example a direct product of two groups with some generators, which will closed this session.

Example 3.7.

1) Let $(\mathbf{Z}_3 \times \mathbf{Z}_4, +) = \{(0,0),\dots,(0,3),\dots,(2,0),\dots,(2,3)\}$. The set $S = \{(0,0),(0,1),(0,2),(0,3)\}$ is a subgorup of $(\mathbf{Z}_3 \times \mathbf{Z}_4, +)$ which is generated by $(0,1) \in \mathbf{Z}_3 \times \mathbf{Z}_4$ with order 4.
2) Let $\mathbf{Z}_3 \times \mathbf{Z}_3 = \{(0,0),(0,1),(0,2),\dots,(2,0),(2,1),(2,2)\}$. We will get some subgroups of $(\mathbf{Z}_3 \times \mathbf{Z}_3, +)$ with more than one generator:

$a)\ \langle(0,0)\rangle = \{(0,0)\}$ order 1

$b)\ \langle(0,1)\rangle = \langle(0,2)\rangle = \{(0,0),(0,1),(0,2)\}$ order 3

$c)\ \langle(1,0)\rangle = \langle(2,0)\rangle = \{(0,0),(1,0),(2,0)\}$ order 3

$d)\ \langle(1,1)\rangle = \langle(2,2)\rangle = \{(0,0),(1,1),(2,2)\}$ order 3

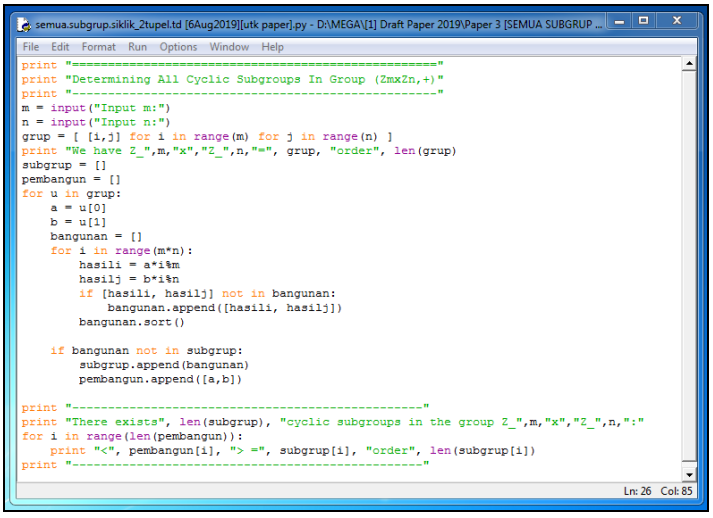
$e)\ \langle(1,2)\rangle = \langle(2,1)\rangle = \{(0,0),(1,2),(2,1)\}$ order 3

4 PYTHON

In this session, we will give a programming by Python 2.7.14 which will be examined in determining all cyclic subgroups of group $(\mathbf{Z}_m \times \mathbf{Z}_n, +)$. This code is main result of this paper. Our main references in making the program are Theorem 2.3. and Definition 3.1. above. It should be noted that the code program below is motivated by the method of determining all cyclic subgroups in the group $(\mathbf{Z}_n, +)$ and its generators (see [13] and [14]), where one of the applications can be studied in [16]. On the other hand, we are also motivated by the method of determining factor groups from all cyclic subgroups in the group $(\mathbf{Z}_n, +)$ which can be studied in [2] where one of the applications can be studied in [4]. The following is the programming code that we used, which is main result of this paper.

```
print "================================================"
print "Determining All Cyclic Subgroups In Group (ZmxZn,+)"
print "------------------------------------------------"
m = input("Input m:")
n = input("Input n:")
grup = [ [i,j] for i in range(m) for j in range(n) ]
print "We have Z_",m,"x","Z_",n,"=", grup, "order", len(grup)
subgrup = []
pembangun = []
for u in grup:
    a = u[0]
    b = u[1]
    bangunan = []
    for i in range(m*n):
        hasili = a*i%m
        hasilj = b*i%n
        if [hasili, hasilj] not in bangunan:
            bangunan.append([hasili, hasilj])
        bangunan.sort()
    if bangunan not in subgrup:
        subgrup.append(bangunan)
        pembangun.append([a,b])
print "------------------------------------------------"
print "There exists", len(subgrup), "cyclic subgroups in the group Z_",m,"x","Z_",n,":"
for i in range(len(pembangun)):
    print "<", pembangun[i], "> =", subgrup[i], "order", len(subgrup[i])
print "------------------------------------------------"
```

The program display of the Python code in Windows OS is as follows.



The following is output display using Python and the example of output from the program above for group $(\mathbf{Z}_3 \times \mathbf{Z}_3, +)$ and $(\mathbf{Z}_5 \times \mathbf{Z}_6, +)$ at Windows OS. The following output display will close this session.

a) For $(\mathbf{Z}_3 \times \mathbf{Z}_3, +)$

```
================================================
Determining All Cyclic Subgroups In Group (ZmxZn,+)
------------------------------------------------
Input m:3
Input n:3
We have Z_ 3 x Z_ 3 = [[0, 0], [0, 1], [0, 2], [1, 0],
[1, 1], [1, 2], [2, 0], [2, 1], [2, 2]] order 9
------------------------------------------------
There exists 5 cyclic subgroups in the group Z_ 3 x Z_
3 :
< [0, 0] > = [[0, 0]] order 1
< [0, 1] > = [[0, 0], [0, 1], [0, 2]] order 3
< [1, 0] > = [[0, 0], [1, 0], [2, 0]] order 3
< [1, 1] > = [[0, 0], [1, 1], [2, 2]] order 3
< [1, 2] > = [[0, 0], [1, 2], [2, 1]] order 3
------------------------------------------------
>>>
```

b) For $(\mathbf{Z}_5 \times \mathbf{Z}_6, +)$

```
================================================
Determining All Cyclic Subgroups In Group (ZmxZn,+)
------------------------------------------------
Input m:5
Input n:6
We have Z_ 5 x Z_ 6 = [[0, 0], [0, 1], [0, 2], [0, 3],
[0, 4], [0, 5], [1, 0], [1, 1], [1, 2], [1, 3], [1,
4], [1, 5], [2, 0], [2, 1], [2, 2], [2, 3], [2, 4],
[2, 5], [3, 0], [3, 1], [3, 2], [3, 3], [3, 4], [3,
5], [4, 0], [4, 1], [4, 2], [4, 3], [4, 4], [4, 5]]
order 30
------------------------------------------------
There exists 8 cyclic subgroups in the group Z  5 x Z
6  yaitu:
< [0, 0] > = [[0, 0]] order 1
< [0, 1] > = [[0, 0], [0, 1], [0, 2], [0, 3], [0, 4],
[0, 5]] order 6
< [0, 2] > = [[0, 0], [0, 2], [0, 4]] order 3
< [0, 3] > = [[0, 0], [0, 3]] order 2
< [1, 0] > = [[0, 0], [1, 0], [2, 0], [3, 0], [4, 0]]
order 5
< [1, 1] > = [[0, 0], [0, 1], [0, 2], [0, 3], [0, 4],
[0, 5], [1, 0], [1, 1], [1, 2], [1, 3], [1, 4], [1,
5], [2, 0], [2, 1], [2, 2], [2, 3], [2, 4], [2, 5],
[3, 0], [3, 1], [3, 2], [3, 3], [3, 4], [3, 5], [4,
0], [4, 1], [4, 2], [4, 3], [4, 4], [4, 5]] order 30
< [1, 2] > = [[0, 0], [0, 2], [0, 4], [1, 0], [1, 2],
[1, 4], [2, 0], [2, 2], [2, 4], [3, 0], [3, 2], [3,
4], [4, 0], [4, 2], [4, 4]] order 15
< [1, 3] > = [[0, 0], [0, 3], [1, 0], [1, 3], [2, 0],
[2, 3], [3, 0], [3, 3], [4, 0], [4, 3]] order 10
------------------------------------------------
>>>
```

5 Conclusion

The conclusions that can be obtained from this study are as follows:

a) All subgroups of a cyclic group are also cyclic groups.
b) Using the Python program, we can determine all cyclic subgroups of the group $(\mathbf{Z}_m \times \mathbf{Z}_n, +)$ easily.
c) From the program that has been created, the maximum value of $m, n \in \mathbf{Z}^+$ can be calculated at 1.7×10^{308}. This value corresponds to the upper limit of integers in Python that can be checked by writing the following command.

```
import sys
int(sys.float_info.max)
```

Acknowledgment

The authors wish to thank STKIP Surya. This work was supported with the help of facilities and infrastructure of STKIP Surya. We thank you deeply for your support during this time.

References

[1] Adkins, W.A. and Weintraub, S.H., 2012. Algebra: an approach via module theory (Vol. 136). Springer Science & Business Media.
[2] Arifin, S., 2018. Grup Faktor dari Sebarang Subgrup Siklik dari Grup $(\mathbf{z}_n, +)$. SCIENCE TECH: Jurnal Ilmiah Ilmu Pengetahuan dan Teknologi, Vol 4 No 2, Hal 53-58.
[3] Arifin, S. and Garminia, H. 2018. Valuation Dimension of Ring $\mathbf{z}_n$ Using Python. International Journal of Engineering & Technology, 7 (4), 6351-6356
[4] Arifin, S. and Garminia, H. 2019. Uniserial Dimension Of Module $\mathbf{z}_m \times \mathbf{z}_n$ Over $\mathbf{z}$ Using Python. International Journal of Scientific & Technology Research, 8(7), 194-199
[5] Dummit, D.S. and Foote, R.M., 2004. Abstract algebra (Vol. 3). Hoboken: Wiley.
[6] Fraleigh, J.B. 2000. A First Course in Abstract Algebra, Sixth Edition, Addison-Wesley, New York.
[7] Gallian, J.A. 2017. Contemporary Abstract Algebra, 9th Edition, USA.
[8] Google. (2018, 30 April): available at https://play.google.com/store/apps/details?id=org.qpython.qpy&hl=en
[9] Herstein I. 1996. Abstract Algebra, 3rd Edition, Prentice Hall, New York.
[10] Huang, H. 2018, 28th July. Algebra Lecture Notes, Auburn University Press, available at http://www.auburn.edu/huanghu/math5310/
[11] Isaacs, I.M., 1994. Algebra, a graduate course, Brooks. Cole Publishing Company, Pacific Grove, California.
[12] Malik, D.S., Moderson, J.N., and Sen, M.K. 1997. Fundamentals of Abstract Algebra, USA.
[13] Muktyas, I.B., and Arifin, S. 2018. Sebarang Pembangun Subgrup Siklik Dari Suatu Grup $(\mathbf{z}_n, +)$. Jurnal Matematika" MANTIK", Vol 4 No 2, Hal 116-121.
[14] Muktyas, I.B., and Arifin, S. 2018. Semua Subgrup Siklik dari Grup $(\mathbf{z}_n, +)$. Jurnal Teorema: Teori dan Riset Matematika. Vol 3 No 2, Hal 177-186, September 2018.
[15] Python. 2018, 30 April. available at https://www.python.org/.
[16] Rotman, J. J. 2003. Advanced Modern Algebra, Prentice Hall, New York.