FACTORIZATION OF FINITE SIMPLE GROUPS

NURLAN GASIMLI

Abstract: A finite group $G$ is factorizable if for any positive integer numbers $a, b$ with $ab = |G|$ there are subsets $A, B \subset G$ of cardinality $|A| = a$ and $|B| = b$ such that $AB = G$. We prove that all Mathieu groups, some linear, and unitary groups are factorizable.

1. Introduction

A finite group $G$ is factorizable if for any positive integer numbers $a, b$ with $ab = |G|$ there are subsets $A, B \subset G$ of cardinality $|A| = a$ and $|B| = b$ such that $AB = G$.

Factoring finite abelian groups into subsets arose as an attractive problem in geometry. In cryptography, this problem became essential after early 20th century. Also, it has a connection with other fields of mathematics, Fourier analysis, Number theory and so on.

It has been proven that all finite solvable groups are factorizable. After the last century, some cryptosystems are based on factorization of finite groups into subsets of cardinalities prime or four. Apart 2-fold factorization above, 3-fold factorization of finite groups is now clear. G. Bergman [1] proved that alternating group $A_4$ can not be factorized into subsets of order (2,3,2). It follows that answer to conjecture of n-fold factorizability of all groups for $n \geq 3$ is negative.

Problem Let $G$ be a finite group of order $n$.

Is it true for every factorization $n = ab$ there exist subsets $A, B$ such that $|A| = a$, $|B| = b$ and $AB = G$?

This paper is a step towards the solution of problem.

A group is factorizable if it can be factorized into subsets of cardinality $a$ and $n/a$ for every $a \leq \sqrt{|G|}$.

2. Strategy of Proof

Let $G$ a finite group of order $n$. If $G$ has a factorization $BC$ and at least one of $B$ and $C$ is a subgroup of $G$ then we can switch $C$ and $B$ and write as below:

\[
G = BC = CB
\]

If $G = A_1A_2 \cdots A_n$ is a factorization of $G$ into subsets and $A_n$ is a subgroup of $G$, we can switch $A_n$ and remaining side of factorization then write as follows:
\( G = A_n A_1 A_2 \cdots A_{n-1} \)

We use this method to solve problem for all Mathieu groups, some linear and unitary groups. Also, if a finite group \( G \) has a subgroup of order \( a \) then it can be factorized into subsets of cardinalities \( a \) and \( n/a \). These two ideas play an important role towards the goal.

3. **Factorization of Mathieu Groups**

**Corollary 3.1** \( A_6 \) - alternating group on 6 elements is factorizable.

Using factorizability of \( A_6 \) we prove that \( M_{10} \) – Mathieu group is factorizable. In following proposition we use switch property.

**Proposition 3.2** \( M_{10} \) is factorizable.

**Proof.** There is an exact factorization of \( M_{10} \) as follows:

\[
M_{10} = A_6 Z_2 = Z_2 A_6
\]

Above switch is allowed since \( A_6 \) and \( Z_2 \) are both subgroups of \( M_{10} \). For convenience, we write factorization of group into subsets as a product of cardinalities of these subsets and we do switch operation. Let us write factorization:

\[
720 = 360 \cdot 2 = 2 \cdot 360
\]

In this factorization, we can factorize \( A_6 \) into two subsets and multiply right subset with cyclic group of order 2. Since \( A_6 \) is factorizable, cardinality of these two subsets can be any factor of 360. Thus in the left side we can write all factors of 360, so these factorizations are done:

\[
720 = 2 \cdot (180 \cdot 2) \\
720 = 3 \cdot (120 \cdot 2) \\
\ldots \ldots \\
720 = 180 \cdot (2 \cdot 2)
\]

Both sides of these factorizations are cardinalities of subsets, actually we have written factorization of \( M_{10} \) into two subsets as a product of cardinalities : \( 2 \cdot 360, 3 \cdot 240, \ldots, 180 \cdot 4 \). However, there are some factors of 720 which are not factors of 360. We do switch operation and same factorization process as above.

\[
720 = (2 \cdot 2) \cdot 180 \\
\ldots \ldots \\
720 = (2 \cdot 8) \cdot 45
\]
It can be easily seen that additional factors are only multiples of 16. Since all factors of 720 is shown in the factorization of 720 as cardinalities of subsets, proof is complete.

**Corollary 3.3** Let $G$ be a finite group of order $n$ and has an exact factorization $BC$ such that $B$ is factorizable and $C$ is of prime order then $G$ is factorizable.

**Proof.** Let us denote order of $B$ and $C$ by $b$ and $c$, respectively. Write $b$ as $b_1 b_2$ then multiply $b_2$ by $c$.

$$n = b_1 \cdot (b_2 \cdot c)$$

Since $b_1$ varies from 1 to $n/c$ as all factors of , remaining factorizations are $(c \cdot b_1) \cdot b_2$, then we immediately obtain all possible factorizations by switching $c$ and $b$.

**Lemma 3.4** $M_{11}$ is factorizable.

**Proof.** There is an exact factorization of $M_{11}$ [4]:

$$M_{11} = M_{10}Z_{11} = Z_{11}M_{10}$$

Since $M_{10}$ is factorizable and $Z_{11}$ is of prime order, $M_{11}$ is factorizable.

**Theorem 3.5** [3] Let $G$ be a finite group of order $n$. If $a$ or $n/a$ divides the order of any proper subgroup of $G$ then $G$ can be factorized into two subsets of orders $a$ and $n/a$.

In [3], remaining order for $M_{12}$ is 270. Thus if we solve question for 270 it would follow that $M_{12}$ is factorizable.

**Lemma 3.6** $M_{12}$ is factorizable.

**Proof.** There is an exact factorization of $M_{12}$ [4]:

$$M_{12} = PSL_2(11) \cdot Z_2 \rtimes M_9$$

Let us factorize $PSL_2(11)$ into two subsets of cardinalities 30 and 22. Then we switch $M_9$ and $PSL_2(11) \cdot Z_2$, because $M_9$ is a subgroup of $M_{12}$. Now, we write factorization as a product of factors:

$$95040 = 9 \cdot 30 \cdot 22 \cdot 2$$

Product of subgroup and subset makes a subset of order 270. Proof is complete.
To prove $M_{22}$ is factorizable, we first show that $PSL_3(4)$ is factorizable. Following lemma deals with this question.

**Lemma 3.7** $PSL_3(4)$ is factorizable.

*Proof.* There is an exact factorization of $PSL_3(4)$ [2] as a product of Sylow subgroups:

\[(3.4) \quad PSL_3(4) = P_7P_3P_2P_5\]

Orders of Sylow subgroups are 7, 9, 64, and 5. Using Theorem 3.5 and [6], we eliminate most of orders, however, 35, 70, and 140 remain open. We do switch operation for subgroup of order 5 and remaining side of factorization.

\[(3.5) \quad PSL_3(4) = P_5P_7P_3P_2\]

Now, it is obvious that in the left side there is a subset of cardinality 35.

For 70 and 140, we just factorize subgroup of order 64 into subset of cardinality 16 and subgroup of order 4. Then let us factorize subgroup of order 4 into two subgroups of order 2. Lastly, to obtain 70 and 140, we just switch subgroup of order 2 and remaining side of factorization once and two times, respectively. We write factorization as a product of factors:

\[
20160 = 5 \cdot 7 \cdot 9 \cdot 16 \cdot 2 \cdot 2 \\
20160 = 2 \cdot 5 \cdot 7 \cdot 9 \cdot 16 \cdot 2 \\
20160 = 2 \cdot 2 \cdot 5 \cdot 7 \cdot 9 \cdot 16
\]

Now, subsets of cardinalities 70 and 140 are obvious. This completes proof. \[\square\]

**Lemma 3.8** $M_{22}$ is factorizable.

*Proof.* There is an exact factorization of $M_{22}$ [2]:

\[(3.6) \quad M_{22} = PSL_3(4) \cdot Z_2 \cdot Z_{11}\]

Using Theorem 3.5 and [6], we eliminate many cases, however, multiples of order 11 up to square root of 443520 remain open. We switch subgroup of order 11 and remaining side of factorization and factorize $PSL_3(4)$ into two subsets. Then all orders which are multiples of 11 up to square root of 443520 are clear.

\[
443520 = 11 \cdot 2 \cdot .... \\
\cdots \cdots \cdots \cdots \cdots \cdots \cdots \cdots \\
443520 = 11 \cdot 10080 \cdot ...
\]

In the left side, we make all remaining orders. Proof is complete. \[\square\]
Lemma 3.9 $M_{23}$ is factorizable.

Proof. There is an exact factorization of $M_{23}$ [2]:

\[(3.7) \quad M_{23} = M_{22}Z_{23} = Z_{23}M_{22}\]

Since $M_{22}$ is factorizable and $Z_{23}$ is of prime order, result follows immediately from Corollary 3.3.

To show that $M_{24}$ is factorizable, we should apply switch operation a bit more.

Lemma 3.10 $M_{24}$ is factorizable.

Proof. Using Theorem 3.5 and [6], only multiples of 27 and two other cases remain open. There is an exact factorization of $M_{24}$ [2]:

\[(3.8) \quad M_{24} = M_{23}S_4\]

These two cases are:

$2^8 \cdot 3^2$

$2^9 \cdot 3^2$

We factorize $S_4$ into subset of cardinality 12 and subgroup of order 2. Let us factorize $M_{23}$ into two subsets, since $M_{23}$ is factorizable, cardinalities of subsets would be any factors of $M_{23}$. We take order of left subset as $2^73^2$ and switch subgroup of order 2 and remaining side of factorization. First case is clear.

$$244823040 = 2 \cdot 2^7 \cdot 3^2 \cdot ...$$

Same operation is applied for second case, however, when we factorize $S_4$ into two subsets, cardinality of subset is 6 and order of subgroup is 4. Then process is obvious.

To solve multiples of 27, we take order of subgroups from factorization of $S_4$ as 3,6,12 and switch these and remaining side of factorization with doing above operation. Since $S_4$ has subgroups of these orders, result follows immediately.

4. Factorization of Linear and Unitary Groups

In this section, we prove that $PSL_2(29)$, $PSU_4(2)$, $PSU_3(4)$ are factorizable.

Lemma 4.1 $PSL_2(29)$ is factorizable.

Proof. There is an exact factorization of $PSL_2(29)$ [5]:

\[(4.1) \quad PSL_2(29) = Z_{29} \rtimes Z_7 \cdot A_5\]
Using Theorem 3.5 and [6], 7 cases remain open. These are: 21, 35, 42, 70, 84, 87, 105.

We write above factorization as a product of factors:

\[ 12180 = 29 \cdot 7 \cdot 60 \]

Now, let us factorize subgroup of order 60 into subset and subgroup:

- Subset of cardinality 20 and subgroup of order 3
- Subset of cardinality 12 and subgroup of order 5
- Subset of cardinality 10 and subgroup of order 6
- Subset of cardinality 6 and subgroup of order 10
- Subset of cardinality 5 and subgroup of order 12.

We switch subgroup of order 29 and of order 7 because of semidirect product of subgroups, then switch above subgroups and remaining side of factorization.

\[ 12180 = 3 \cdot 7 \cdot 29 \cdot 20 \]
\[ 12180 = 5 \cdot 7 \cdot 29 \cdot 12 \]
\[ 12180 = 6 \cdot 7 \cdot 29 \cdot 10 \]
\[ 12180 = 10 \cdot 7 \cdot 29 \cdot 6 \]
\[ 12180 = 12 \cdot 7 \cdot 29 \cdot 5 \]

Now, let us factorize subgroup of order 60 into subset of cardinality 20 and subgroup of order 3, then switch subgroup of order 3 and remaining side of factorization.

\[ 12180 = 3 \cdot 29 \cdot 7 \cdot 20 \]

6 cases are clear, however, for the last case we use a trick. We factorize subset of cardinality 15 and subgroup of order 4, then switch 29 and remaining side of factorization.

\[ 12180 = 7 \cdot 15 \cdot 4 \cdot 29 \]

This completes proof. \( \square \)

In the next part of this section, we consider unitary group.

**Lemma 4.2** \( PSU_4(2) \) is factorizable.

**Proof.** There is an exact factorization of \( PSU_4(2) \) [2]:

\[ (4.2) \quad PSU_4(2) = P_3P_2P_5 \]
It is a product of Sylow subgroups and orders are 81, 64, and 5. Using Theorem 3.5 and [6], only 135 remains open. However, we eliminate this order by using switch operation. Let us factorize subgroup of order 81 into subgroup of order 27 and subset of order 3, then switch subgroup of order 5 and remaining side of factorization.

\[ 25920 = 5 \cdot 2^7 \cdot 3 \cdot 64 \]

Now, the last case is clear. Proof is complete.

5. SMALL NOTE ABOUT FACTORIZATION

We note that other small linear and unitary simple groups can be solved by using switch operation. To solve special linear simple groups, some induction methods are required. However, some other techniques are required for other sporadic simple groups.

REFERENCES

[1] G.M.Bergman, A note on factorizations of finite groups, arxiv:2003.12866 (2020).
[2] M.I.Gonzalez Vasco, M.Rötteler, R.Steinwandt, On minimal length factorizations of finite groups, Exp.Math 12 (2003), 1-12.
[3] R. Bildanov, V.Goryachenko, A. Vasil’ev, Factoring nonabelian finite groups into two subsets, arxiv:2005.12003
[4] M. Giudici, Factorisations of sporadic simple groups, Journal of Algebra Volume 304,Issue 1, 1 October 2006, Pages 311-323
[5] C.H.Li, B.Xia, Factorizations of almost simple groups with a solvable factor, and Cayley graphs of solvable factor, arxiv:1408.0350
[6] homepages.ulb.ac.be/~dleemans/atlaslat/
UMass Lowell,
USA.

Email address: Nurlan_Gasimli@student.uml.edu