

Introduction to Factorial Subsets

Zack Baker

June 2017

1 Introduction

A *group* G is a set of elements together with a binary operation \cdot such that the following properties hold:

1. **Closure** of the set under the binary operation: For any $a, b \in G$, $a \cdot b$ is also an element of G .
2. **Associativity**: for any $a, b, c \in G$, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.
3. There exists an **identity** element $e \in G$ such that for all $a \in G$, $a \cdot e = e \cdot a = a$.
4. Each element $a \in G$ has an **inverse** $b \in G$ such that $a \cdot b = b \cdot a = e$.

When the binary operation is understood, and we are working in a multiplicative group, we will often use concatenation in place of writing the binary operation between two elements. For example, if we want to represent $a \cdot b$ for $a, b \in G$ we may simply write ab .

Group theory aims to understand the relations between elements of a group. This paper aims to further analyze the relationship between elements of a group by extending the concept of the factorial from the integers to any group.

For n a non-negative integer, the *factorial* of n , written $n!$ is defined as $n \times (n-1) \times \dots \times 2 \times 1$, with the special case $0! = 1$. Thus, $1! = 1$, $2! = 2 \times 1 = 2$, $3! = 3 \times 2 \times 1 = 6$, and so on. We seek to extend the factorial by imposing an ordering on the underlying set of the group.

2 Definitions

Let G be a finite group under the binary operator \oplus . To begin, we must define a binary relation \preceq on G , where \preceq is a total ordering. If the group's underlying set is numeric, and if \preceq is the same as the standard \leq ordering on the set, then we call \preceq the *natural ordering* for G .

We define the factorial of g_i , $g_i! = \bigoplus_{k=0}^i g_k = g_0 \oplus g_1 \oplus g_2 \oplus \dots \oplus g_k$, where $g_0 \preceq g_1 \preceq g_2 \preceq \dots \preceq g_{k-1} \preceq g_k$ and there are no elements $g \in G \setminus \{g_0, \dots, g_k\}$ such that $g_0 \preceq g \preceq g_k$.

Definition 1. Given a group G with some total ordering \preceq , we define the factorial subset of G , denoted $F_{\preceq}(G)$, as $\{g_i! | g_i \in G\}$. In other words, the factorial subset of a group is the set of the factorial of each of that group's elements. If $F_{\preceq}(G)$ is a subset of G , then we say it is a factorial subset of G .

Example: The Klein 4-group is a small, common group suitable for demonstrating the concepts established above. The Klein 4-group is defined as $\{e, a, b, c\}$, where e is the identity, $a^2 = b^2 = c^2 = e$, $ab = c$, $ac = b$, and $bc = a$. Define \preceq such that $e \preceq a \preceq b \preceq c$. Then, $e! = e$, $a! = ea = a$, $b! = eab = ab = c$, and $c! = eabc = cc = e$. Then, the factorial subset of the Klein 4-group, $F_{\preceq}(V_4)$, is $\{e!, a!, b!, c!\}$, or $\{e, a, c\}$. Since the factorial subset has 3 elements and V_4 has 4, clearly the subset is not a subgroup of V_4 . In fact, no orderings of V_4 produce a subgroup

Theorem 1. For any ordering \preceq , $F_{\preceq}(V_4)$ is not a subgroup of V_4 .

Proof. Let x, y, z, w be distinct elements of V_4 . Then, $F_{\preceq}(V_4) = \{x!, y!, z!, w!\}$. Let w be the greatest element. Then, $w! = e \cdot a \cdot b \cdot c = e$. We will show that some element is always duplicated in $F_{\preceq}(V_4)$. We have 4 cases:

Case 1: Let $x = e$. Then, $x! = e$, and e is duplicated

Case 2: Let $y = e$. Then, $y! = x! \cdot y = x! \cdot e = x!$. Thus, $x!$ is duplicated

Case 3: Let $z = e$. Then, $z! = y! \cdot z = y! \cdot e = y!$. Thus, $y!$ is duplicated.

Case 4: Let $w = e$. Then, $w! = z! \cdot w = z! \cdot e = z!$. Thus, $z!$ is duplicated

Therefore, in all cases, $F_{\preceq}(V_4) = \{e, x, y\}$, where x, y are distinct elements of V_4 . \square

3 Factorial Subsets of the Additive Group of Integers modulo n

In this section, we will specifically examine the factorial subsets and subgroups of the additive group of integers modulo n , $\mathbb{Z}/n\mathbb{Z}$.

3.1 Factorial Subsets with the natural ordering of $\mathbb{Z}/n\mathbb{Z}$

Let $\mathbb{Z}/n\mathbb{Z}$ be the additive group of integers modulo n , and let $\mathbb{Z}/n\mathbb{Z}$ be ordered by the natural ordering. The following table describes $F_{\preceq}(\mathbb{Z}/n\mathbb{Z})$ for small n .

| n | $F_{\preceq}(\mathbb{Z}/n\mathbb{Z})$ | Is $F_{\preceq}(\mathbb{Z}/n\mathbb{Z})$ a subgroup of $\mathbb{Z}/n\mathbb{Z}$? |
|-----|---------------------------------------|---|
| 2 | $\{0, 1\}$ | ✓ |
| 3 | $\{0, 1\}$ | X |
| 4 | $\{0, 1, 2, 3\}$ | ✓ |
| 5 | $\{0, 1, 3\}$ | X |
| 6 | $\{0, 1, 3, 4\}$ | X |
| 7 | $\{0, 1, 3, 6\}$ | X |
| 8 | $\{0, 1, 2, 3, 4, 5, 6, 7\}$ | ✓ |
| 9 | $\{0, 1, 3, 6\}$ | X |
| 10 | $\{0, 1, 3, 5, 6, 8\}$ | X |

As we can see, $F_{\preceq}(\mathbb{Z}/n\mathbb{Z})$ is only a subgroup of $\mathbb{Z}/n\mathbb{Z}$ if n is 2, 4 or 8. Continuing these calculations up to $n = 10000$, $F_{\preceq}(\mathbb{Z}/n\mathbb{Z})$ is only a subgroup if $n = 2^k$, for some positive integer k , and for all $n = 2^k$, $F_{\preceq}(\mathbb{Z}/n\mathbb{Z}) = \mathbb{Z}/n\mathbb{Z}$

Conjecture 1. *For \preceq the natural ordering, $F_{\preceq}(\mathbb{Z}/n\mathbb{Z})$ is equivalent to $\mathbb{Z}/n\mathbb{Z}$ if and only if $n = 2^k$ for some positive integer k .*

3.2 All Factorial Subgroups of $\mathbb{Z}/n\mathbb{Z}$

In the previous section we examined a single ordering for many values of n . Conversely in this section, we will look at many orderings for few n . We ask for some n , how many orderings of $\mathbb{Z}/n\mathbb{Z}$ produce factorial subgroups? Since there are $n!$ ways of ordering n elements, there will be many different orderings to check. The following table describes the number of factorial subgroups produced by $\mathbb{Z}/n\mathbb{Z}$

| n | Number of orderings for which $F_{\preceq}(\mathbb{Z}/n\mathbb{Z})$ is a subgroup of $\mathbb{Z}/n\mathbb{Z}$ |
|-----|---|
| 2 | 1 |
| 3 | 0 |
| 4 | 2 |
| 5 | 0 |
| 6 | 4 |
| 7 | 0 |
| 8 | 24 |
| 9 | 0 |
| 10 | 288 |
| 11 | 0 |
| 12 | 3856 |

Curiously, taking the non-zero entries as a sequence replicates the known integer sequence A14159.

Since for $\mathbb{Z}/n\mathbb{Z}$ there are $n!$ possible orderings, this quickly makes computation impossible for larger values of n . There are several observations which reduce the total number of orderings needed to check.

Theorem 2. *$F_{\preceq}(\mathbb{Z}/n\mathbb{Z})$ is a subgroup of $\mathbb{Z}/n\mathbb{Z}$ if and only if $F_{\preceq}(\mathbb{Z}/n\mathbb{Z}) = \mathbb{Z}/n\mathbb{Z}$*

Proof. For some n , let a_i be the factors of n . Then, $\langle a_i \rangle$ generates a subgroup of $\mathbb{Z}/n\mathbb{Z}$. All elements of all subgroups are of the form $n \cdot a_i$, where a_i is the generating element. Assume for all elements $g_i \preceq 1$, $g_i = n \cdot a_i$, and let g_k directly precede 1. Then, $1! = g_k! \cdot a_i + 1$. If $a_i \neq 1$, then $g_k! \cdot a_i + 1$ is not a multiple of a_i , so $g_k! \cdot a_i + 1$ isn't in $\langle a_i \rangle$. The only a_i for which $g_k! \cdot a_i + 1$ is a multiple of is 1. Since the subgroup generated by 1, $\langle 1 \rangle$, is the entire group, $F_{\preceq}(\mathbb{Z}/n\mathbb{Z})$ must be equal to $\mathbb{Z}/n\mathbb{Z}$ to be a subgroup of $\mathbb{Z}/n\mathbb{Z}$. \square

Lemma 1. *For any n , if 0 is not the smallest element in $\mathbb{Z}/n\mathbb{Z}$, then $F_{\preceq}(\mathbb{Z}/n\mathbb{Z}) \neq \mathbb{Z}/n\mathbb{Z}$.*

Proof. This will be a proof by contradiction. Assume there exists some element g_i directly preceding 0. Then, $0! = g_i! + 0 = g_i!$. Since $g_i!$ is repeated, the size of $F_{\preceq}(\mathbb{Z}/n\mathbb{Z})$ must be smaller than $\mathbb{Z}/n\mathbb{Z}$, so $F_{\preceq}(\mathbb{Z}/n\mathbb{Z}) \neq \mathbb{Z}/n\mathbb{Z}$. \square

Lemma 2. *If n is odd, $F_{\preceq}(\mathbb{Z}/n\mathbb{Z}) \neq \mathbb{Z}/n\mathbb{Z}$.*

Proof. Let g_n be the largest element of $\mathbb{Z}/n\mathbb{Z}$. Then, $g_n! = \sum_{k=0}^{n-1} k = T_{n-1} \equiv T_n - n \equiv T_n \pmod{n}$, where T_n is the n th triangular number. If n is odd, then $T_n \pmod{n}$ is 0. The triangular numbers are defined as $T_n = \sum_{i=0}^n 0+1+2+\dots+n-1+n$. If n is odd, the center of this sum looks like $\dots + \frac{n-1}{2} + \frac{n+1}{2} + \dots$. In $\mathbb{Z}/n\mathbb{Z}$, each element can be paired with its inverse, as there are an even number of terms in the sum, excluding 0. Thus, $T_n \pmod{n} \equiv 0$ for odd n . Then, 0 is duplicated in $F_{\preceq}(\mathbb{Z}/n\mathbb{Z})$, so $F_{\preceq}(\mathbb{Z}/n\mathbb{Z}) \neq \mathbb{Z}/n\mathbb{Z}$. \square

Lemma 3. *For even n , $n > 2$, $\frac{n}{2}$ cannot be the greatest element.*

Proof. This will be a proof by contradiction. Assume $\frac{n}{2}$ is the greatest element of $\mathbb{Z}/n\mathbb{Z}$. Then, since the factorial of the largest element of $\mathbb{Z}/n\mathbb{Z}$ is T_n , $\frac{n}{2}! = T_n$. For even n , $T_n = \frac{n}{2}$. The n th triangular number is defined as $0+1+2+\dots+(n-1)+n$. For even n , the center of this sum looks like $\dots + \frac{n}{2} - 1 + \frac{n}{2} + \frac{n}{2} + 1 + \dots$. Every element in this sum can be paired with its inverse \pmod{n} , except for $\frac{n}{2}$. Thus, the sum equals $\frac{n}{2}$. Since $T_n = \frac{n}{2}$, $\frac{n}{2}! = \frac{n}{2}$. Let g directly precede $\frac{n}{2}$. Then, $g! = \frac{n}{2}! - \frac{n}{2} = \frac{n}{2} - \frac{n}{2} = 0$. Thus, 0 is duplicated, so $F_{\preceq}(\mathbb{Z}/n\mathbb{Z}) \neq \mathbb{Z}/n\mathbb{Z}$. \square

Lemma 4. *For even n , $\frac{n}{2}$ cannot be the second smallest element.*

Proof. If $\frac{n}{2}$ is the second least element, then $\frac{n}{2}! = 0 + \frac{n}{2} = \frac{n}{2}$. However, we know by Lemma 2 that the factorial of the greatest element of $\mathbb{Z}/n\mathbb{Z}$ is $\frac{n}{2}$. Thus, if the second least element is $\frac{n}{2}$, then $\frac{n}{2}$ is duplicated, so $F_{\preceq}(\mathbb{Z}/n\mathbb{Z}) \neq \mathbb{Z}/n\mathbb{Z}$. \square

4 Description of the Algorithm

To begin, the value for n is determined. If n is determined to be odd, the algorithm terminates, by means of Lemma 3.2. If not present, the list of valid beginning subsets of size $\frac{n}{2}$ are calculated. For each possible subset of $\mathbb{Z}/n\mathbb{Z}$ of size $\frac{n}{2}$, it is checked to see if it potentially produces $\mathbb{Z}/n\mathbb{Z}$. If it does, it is stored in a list. Once the subsets have been loaded or calculated, all possible orderings

of $\mathbb{Z}/n\mathbb{Z}$ are calculated. These permutations are then iterated through. First, the first element of each ordering is checked. If it is not 0, the ordering is discarded, by Lemma 3.1. Then, the first half of the ordering is checked against the list of potentially valid subsets calculated above. If the subset of the ordering is not in the list, the ordering is discarded. Next, each element of the ordering is added together mod n . If the resulting sum has already been produced, the ordering is discarded, as it will be impossible to reproduce all of $\mathbb{Z}/n\mathbb{Z}$. If the ordering hasn't been discarded at this point, it will reproduce $\mathbb{Z}/n\mathbb{Z}$.