# The Lecture Title

Scribe: Your Name

**Date**: Day, Mon, Date Year

## 1 Finite Groups and Subgroups

Recall that

$$\mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, \ldots\}, \quad 4\mathbb{Z} = \{0, \pm 4, \pm 8, \pm 12, \ldots\}$$

Now, define $\mathbb{Z}1/4\mathbb{Z}$ ("$\mathbb{Z}$ mod $4\mathbb{Z}$"), the quotient group of cosets of $4\mathbb{Z} \subseteq \mathbb{Z}$. This is the set $\{0 + 4\mathbb{Z}, 1 + 4\mathbb{Z}, 2 + 4\mathbb{Z}, 3 + 4\mathbb{Z}\} = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$ for convenience. These are not numbers

We claim that this set is a group under set addition ($+_4$). Let's go through and prove each of the necessary properties one by one.

First, we prove closure. This can be done exhaustively using a *Cayley table*:

| $+_4$ | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ | $\bar{3}$ |
|---|---|---|---|---|
| $\bar{0}$ | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ | $\bar{3}$ |
| $\bar{1}$ | $\bar{1}$ | $\bar{2}$ | $\bar{3}$ | $\bar{0}$ |
| $\bar{2}$ | $\bar{2}$ | $\bar{3}$ | $\bar{0}$ | $\bar{1}$ |
| $\bar{3}$ | $\bar{3}$ | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ |

Associativity here is inherited from the addition operation, so clearly associativity holds here (as the operation in question is essentially addition mod 4).

There is clearly an identity here, the element $\bar{0}$. There is also an inverse for every element, as we can find a $\bar{0}$ in every row and column of the table. This shows that this set is a group.

Well, the number 4 is not very special, so we can generalize this to the broader set $\mathbb{Z}/n\mathbb{Z}$ for $n \geq 2$. This is in general true and this grou pappears so often that we just abbreviate this as $\mathbb{Z}_n$.

What if we now wanted a group with four elements, under a multiplication operation? Naively changing + to $\times$ gives problems - $\bar{0}$ doesn't have an inverse, and in fact neither does $\bar{2}$. We should consider instead $\mathbb{Z}/5\mathbb{Z}$ without $\bar{0}$. Here is a Cayley table under the multiplication operation with this set:

| $\times_5$ | $\bar{1}$ | $\bar{2}$ | $\bar{3}$ | $\bar{4}$ |
|---|---|---|---|---|
| $\bar{1}$ | $\bar{1}$ | $\bar{2}$ | $\bar{3}$ | $\bar{4}$ |
| $\bar{2}$ | $\bar{2}$ | $\bar{4}$ | $\bar{1}$ | $\bar{3}$ |
| $\bar{3}$ | $\bar{3}$ | $\bar{1}$ | $\bar{4}$ | $\bar{2}$ |
| $\bar{4}$ | $\bar{4}$ | $\bar{3}$ | $\bar{2}$ | $\bar{1}$ |

This can essentially be filled in by noting that $\bar{a} \times_5 \bar{b} \equiv \overline{ab} \bmod 5$. The proof of this fact is essentially an explicit computation of these sets in mod 5, and this is in fact true in general. tly see that this is a group, and furthermore, it's an abelian group by the symmetry in the table.

Are these groups the same? By that, we are asking whether or not there exists a mapping between the elements of these groups that preserves all the relations between these elements. This property is called an *isomorphism*. Notice that we can find two such mappings:

| $x$ | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ | $\bar{3}$ |
|---|---|---|---|---|
| $f_1(x)$ | $\bar{1}$ | $\bar{3}$ | $\bar{4}$ | $\bar{2}$ |
| $f_2(x)$ | $\bar{1}$ | $\bar{2}$ | $\bar{4}$ | $\bar{3}$ |

and if we arrange these elements, we can see the same relations are preserved:

| $\times_5$ | $\bar{1}$ | $\bar{2}$ | $\bar{4}$ | $\bar{3}$ |
|---|---|---|---|---|
| $\bar{1}$ | $\bar{1}$ | $\bar{2}$ | $\bar{4}$ | $\bar{3}$ |
| $\bar{2}$ | $\bar{2}$ | $\bar{4}$ | $\bar{3}$ | $\bar{1}$ |
| $\bar{4}$ | $\bar{4}$ | $\bar{3}$ | $\bar{1}$ | $\bar{2}$ |
| $\bar{3}$ | $\bar{3}$ | $\bar{1}$ | $\bar{2}$ | $\bar{4}$ |

Does the group $(\mathbb{Z}_4, +_4)$ have any subgroups? Yes - other than the two trivial ones ($\{\bar{0}\}$, $\{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \}$), there's also $\{\bar{0}, \bar{2}\}$. We can deduce this last nontrivial group from looking mostly at closure and invertibility, starting construction with the identity element. Notice that this shows the validity of Lagrange's Theorem - every subgroup has a size that divides the size of the original group, and in fact each of subgroups have a size that represent every divisor of $4$. (The converse is not true, or true to a limited extent).

Are there other groups of size 4? If we exhaustively search for one, we can find this table that represents a group:

| | e | b | c | d |
|---|---|---|---|---|
| e | e | b | c | d |
| b | b | e | d | c |
| c | c | d | e | b |
| d | d | c | b | e |

Notice that this group is different as every element in this group is its own inverse.

We can apply the notion of groups to the symmetry groups of a rectangle. Notice that we have four basic operations that preserve the shape and orientation of the rectangle: reflection about a horizontal axis (H), reflection about a vertical axis (V), rotation by 180 degrees (R), and the identity (e). Here is the Cayley table for these elements (where our operation is composition).

| | e | H | V | R |
|---|---|---|---|---|
| e | e | H | V | R |
| H | H | e | R | V |
| V | V | R | e | H |
| R | R | V | H | e |

This is the same as the group we just found before! Not only that, we have the theorem for groups of size 4:

**Theorem 1.1.** *This and $Z_4$ are the only groups of size 4 (or order 4).*

The proof that there are less than (or equal) to 2 groups is beyond the scope of the course, but clearly there are at least two by construction.

What would happen if we tried to multiply the group $\mathbb{Z}_2$ by itself, $\mathbb{Z}_2 \times \mathbb{Z}_2$, or adding sets of two elements to themselves mod 2 (taking a Dirac sum)? If we do this operation:

| | e | H | V | R |
|---|---|---|---|---|
| e | e | H | V | R |
| H | H | e | R | V |
| V | V | R | e | H |
| R | R | V | H | e |

we see that this last group that we found is the group $\mathbb{Z}_2 \times \mathbb{Z}_2$.

The notation $\mathbb{Z}_5^*$ is the notation used for the group of units mod 5, or all elements

From this analysis, we define $\mathbb{Z}_n^*$ is the group of integers $x$ relatively prime to $n$, $1 \leq x \leq n$, where the group operation is multiplication mod $n$. The function $\varphi(n)$ counts is the number of integers relatively prime to $n$ less than $n$. show this is $\mathbb{Z}_{\varphi(n)}$,

Is it true that $(\mathbb{Z}_{13}^*, \times) \cong (\mathbb{Z}_{12}, +)$? To show that these are in fact equal, we introduce the idea of a cyclic group of order $n$, where there exists an element $g$ that generates the entire group

$$\{e, g, g^1, g^2, \ldots g^{n-1}\}$$

Notice that $(\mathbb{Z}_4, +_4)$ is cyclic, and in fact $(\mathbb{Z}_n, +_n)$ is always cyclic as we can always generate the entire group with 1 or $n-1$. As a corollary, $\mathbb{Z}_n$ can be generated with $\phi(n)$ generators, all numbers less than $n$ can generate the group.

What about our rectangle group? This is NOT cyclic. Define the order of an element $x$ to be the number $k$ such that $x^k = e$, the identity. In the rectangle subgroup, these are all less than or equal to 2. However, in a cyclic group, a generator must have order $n$. Denote this by $ord(g) = n$.

We can define a cyclic subgroup as the subgroup generated by an element $h \in G$. In our rectangle, the sets $\{R, e\}, \{H, e\}, \{V, e\}$ are all cyclic

subgroups. From Lagrange, the order of $h$ must divide the group size, as this generates a subgroup.

To finish, note that we can construct explicitly an isomorphism between $\mathbb{Z}_{13}^*$ and $\mathbb{Z}_{12}$ as 2 generates the former.