Finite Groups and Subgroups

Scribe: Yoseph Mak

Date: 23 Apr 2019

1 Quotient Groups

Define $\mathbb{Z}/4\mathbb{Z}$ or "$\mathbb{Z} \mod 4\mathbb{Z}$" as the group of cosets of the latter in the former. These are obviously $\{4\mathbb{Z}, 4\mathbb{Z}+1, 4\mathbb{Z}+2, 4\mathbb{Z}+3\}$. We'll refer to these as $\{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}$. The four is implied in context. This is called a **quotient group**.

We can prove that this is a group under addition modulo 4, or $+_4$:

1. **Closure:** Let's make a **Cayley Table** for this group:

$+_4$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{0}$	$\overline{1}$	$\overline{2}$

   This is a relatively ludicrous way of proving closure, but it works since every two elements under our operator give another element in the set.

2. **Associativity:** Addition is closed, so $+_4$ inherits this property. We can prove this more formally, but it's not really necessary.

3. **Identity:** The zero element, $\overline{0}$. Trivial.

4. **Inverse:** We can look at the table and find that every element has an inverse.

There's nothing special about the 4, really; $\mathbb{Z}/\ltimes\mathbb{Z}$ is a group (for $n \geq 2$) by the same reasoning. This group is surprisingly common, so we'll call it $\mathbb{Z}_n$ in general. (Note that $\mathbb{Z}_1 = \mathbb{Z}$.

What if we try to make a 4-element group under multiplication? The quotient group clearly doesn't work under multiplication since we have a 0 in $\overline{0}$. Even if we get rid of the $\overline{0}$, $\overline{2}$ doesn't have an inverse.

Observe that this is the case because. If we take $\mathbb{Z}_5$ on the other hand, we can fill out a Cayley table:

$\times_5$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{2}$	$\overline{2}$	$\overline{4}$	$\overline{1}$	$\overline{3}$
$\overline{3}$	$\overline{3}$	$\overline{1}$	$\overline{4}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

So this is closed. Alternatively, we can simply look at two arbitrary elements of the group $\overline{a} = \overline{5k+a}$ and $\overline{b} = \overline{5l+b}$ which gives

$$\overline{a} \times_5 \overline{b} = (\overline{5k+a}) \times_5 (\overline{5l+b}) = 25kl + 5kb + 5la + ab$$

$$= 5(5kl + kb + la) + ab = 5t + ab \text{ where } t = 5kl + kb + la$$

for some t so $\overline{a} \times_5 \overline{b}$ is in the set.

2 Group isomorphism

We define two groups as **isomorphic** if we can map the elements from one to the other such that every possibility remains the same.

Can we map our two groups so far to each other? Well, we can try. Define the function f to go from our first group to our second group. Then, if we set $f(\overline{0}) = \overline{1}, f(\overline{1}) = \overline{2}, f(\overline{2}) = \overline{4}, f(\overline{3}) = \overline{3}$, things are equivalent. (We can also set $\overline{1}, \overline{3}, \overline{4}, \overline{2}$ for the four elements of $\ntrianglerighteq$ in order and get an isomorphism.)

To prove that this works, we can simply construct a Cayley table, but with the elements in a different order. There's nothing stopping us from doing this.

$\times_5$	$\overline{1}$	$\overline{2}$	$\overline{4}$	$\overline{3}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{4}$	$\overline{3}$
$\overline{2}$	$\overline{2}$	$\overline{4}$	$\overline{3}$	$\overline{1}$
$\overline{4}$	$\overline{4}$	$\overline{3}$	$\overline{1}$	$\overline{2}$
$\overline{3}$	$\overline{3}$	$\overline{1}$	$\overline{2}$	$\overline{4}$

This table is equivalent to the first one.

3 More Subgroups

Does $(\mathbb{Z}_4, +_4)$ have subgroups? Yes, it has three: the trivial subgroup, the entire group, and $\{\overline{0}, \overline{2}\}$.

There's an easy way to get this from the table, though. Obviously, all we really need to prove is closure because other properties are basically inherited besides inverses. If we take $\overline{0}$ and $\overline{2}$ in the table...

...we clearly see that only these two elements come up in the ”mini-table”, and every element has an inverse since there's one $\overline{0}$ in every row and column.

As expected, the sizes of these groups are factors of 4.

4 Another Group

Can we make another different size-4 group that's not isomorphic to our first group? Remember that both groups we found so far are isomorphic.

Well, recall that each group we found so far has our first element, which we'll call a, multiply to one of the other two elements b and c (excluding the identity). However, both of these were proven to be equal, and because every row and column must contain the entire set (think about why: if this weren't the case, we could have two inverses of element), we can't do this.

Thus, we set $a \times a = e$. The only way to continue from here without contradiction is to set $a \times b = c$ and $a \times c = b$ since we can't multiply the identity by itself. Now, we have the choice between $b \times b$ equals e or a. As it turns out, the latter is isomorphic to both of the previous groups, so we go with the former and obtain the following table:

$+_2$	[0, 0]	[0, 1]	[1, 0]	[1, 1]
[0, 0]	[0, 0]	[0, 1]	[1, 0]	[1, 1]
[0, 1]	[0, 1]	[0, 0]	[1, 1]	[1, 0]
[1, 0]	[1, 0]	[1, 1]	[0, 0]	[0, 1]
[1, 1]	[1, 1]	[1, 0]	[0, 1]	[0, 0]

This is the $\mathbb{Z}_2 \times \mathbb{Z}_2$ group.

Next question: What's the symmetry group of a rectangle? Well, there are four things that we can obviously do that aren't unique: nothing (e), horizontal and vertical reflection (H and V), and rotation by 180 degrees (R), which we'll set clockwise WLOG.

We have $H \times V = V \times H = R$, $V \times R = H$, and so on, so this happens to be the same as $\mathbb{Z}_2 \times \mathbb{Z}_2$:

$+_2$	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 can prove that there are only two groups of order four. Proving that there are at most 2 is not possible for the scope of this course, but proving that there are at least 2 is easy because $x^2 = e$ for all x in the rectangle group, but not all such x are covered by one group based on our work earlier. (Plus, we've already found two groups anyway.)

5 *

Consider $\mathbb{Z}_5^*$. This is the official definition of our second group; it's the quotient group without the zero. In general, the $*$ means that we take out everything without an inverse to make it an actual group for obvious reasons.

For example, think of $\mathbb{Z}_6^*$. The inverse under multiplication modulo 6 is still $\overline{1}$, but the only two numbers modulo 6 that can have an inverse mod 6 are 1 and 5, so our group would just be $\{\overline{1}, \overline{5}\}$. Specifically, **every number relatively prime to n** where we're looking for $\mathbb{Z}_n^*$ is in the group.

The number of numbers less than a number relatively prime to the number can be found with **Euler's totient function** $\phi(n)$. For example, $\phi(p) = p - 1$ for any prime p since every number less than a prime is relatively prime to it.

6 Cyclic Groups

A **cyclic group** with generator g is simply $g = \{g^0, g^1, g^2, \dots, g^{n-1}\}$.

Examples of cyclic groups include $(\mathbb{Z}_{13}^*, \times_{13})$ and $(\mathbb{Z}_{12}, +_{12})$.

$(\mathbb{Z}_4, +_4)$ is also cyclic with generator $\overline{1}$, giving $\overline{1} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}$. We can also use $\overline{3}$ to get $\overline{3} = \{\overline{0}, \overline{3}, \overline{2}, \overline{1}\}$.

The rectangle group (aka $\mathbb{Z}_2 \times \mathbb{Z}_2$) isn't cyclic since every number is its own inverse. In light of this, we can define the **order** of any element a, or $\text{ord}(a)$, to be the smallest number n such that $a^n = e$. For example, the order of any element of the rectangle group besides the identity is 2 while the order of the identity is 1 (in general).

Similarly, we can develop a **cyclic subgroup** of a group G based on an element $h \in G$. For example, $\{e, V\}$ is a cyclic subgroup since $V^2 = e$.

We also have a corollary of Lagrange's Theorem as a result: $|G| \mid \text{ord}(h)$, aka the order of any element in the group is a factor of the cardinality of the group.