MA294 Lecture

Timothy Kohl

Boston University

January 30, 2024

Groups

The integers mod m, $\mathbb{Z}_m$ under addition, and $U(m)$ the units mod m under multiplication, are prototype examples of the concept of a 'group' which is one of the most important ideas in mathematics.

Definition

Given a set G, a binary operation $*$ is a function which assigns to every ordered pair of elements $(a, b) \in G \times G$ another element of G denoted $a * b$.

i.e. If $a, b \in G$ then $a * b \in G$ which is also phrased as 'G is closed with respect to $*$'.

Now, this 'closure' property is sometimes included as part of the definition of group, but we define it separately, in order to focus on the three fundamental aspects of what it means for a set G with a binary operation $*$, sometimes written $(G, *)$, to be a group.

Definition

A set G with a binary operation $*$, denoted $(G, *)$, is a **group** if the following properties hold.

- $(a * b) * c = a * (b * c)$ for all $a, b, c, \in G$. [associativity]
- There exists an element $e \in G$, called (an) identity, such that $a * e = a$ and $e * a = a$ for all $a \in G$. [identity element]
- For every $a \in G$, there exists $b \in G$ such that $a * b = e$ and $b * a = e$. (Such an element b is called an inverse to a.) [inverses]

There are two quick facts we can establish about groups.

Proposition

In a group $(G, *)$ the identity element is unique, and every element has a unique inverse.

Proof

Suppose e, e' are both identity elements in G.

Consider $e * e'$. Since e is an identity

$$e * e' = e'$$

but since e' is *also* an identity, $e * e' = e$, and so

$$e * e' = e'$$
$$e * e' = e$$

So $e = e'$.

Proof continued

Given a in G, let b, c be inverses, and consider $b * a * c$ which can be parenthesized in two ways:

$$(b * a) * c$$

which must equal $e * c$ since b is an inverse of a, but $e * c = c$. Conversely, we can parenthesize it as

$$b * (a * c) = b * e = b$$

again because c is an inverse of a.

Lastly, we invoke associativity to realize that

$$(b * a) * c = c$$
$$b * (a * c) = b$$

so $c = b$. $\square$

We note that the group operation is not always denoted by $*$, (which looks like 'multiplication') so sometimes if the group is related to arithmetic, we use 'additive notation' and use the symbol $+$.

As such, if we use a 'multiplicative' symbol like '$*$' then the inverse of 'a' might be denoted a^{-1}, in particular because inverses have now been proven to be unique!

Similarly, if the group operation is 'additive' we might denote the inverse of 'a' by $-a$ and perhaps use the symbol '0' to denote the identity.

The notation though can vary greatly for different examples of groups.

Indeed arithmetic provides our first source of examples.

Example: $(\mathbb{Z}, +)$ is a group (the integers with addition)
Why?

Well it's certainly closed, i.e. $a, b \in \mathbb{Z}$ implies $a + b \in \mathbb{Z}$.

Also $a + (b + c) = (a + b) + c$ is a familiar fact we're all used to.

And the number 0 is such that $a + 0 = a = 0 + a$, and for every $a \in \mathbb{Z}$.

Morever, for every integer $a \in \mathbb{Z}$, the integer $-a \in \mathbb{Z}$ where now
$a + (-a) = 0 = (-a) + a$.

Before we explore more examples, let's consider some 'non-examples', namely sets with binary operations that turn out not to be groups.

Keep in mind that in order for a set with a given operation to be a group, the operation must be closed, and the associativity, identity, and inverse axioms must hold.

As such, if any property fails, we don't have a group structure.

Non-Example: $(\mathbb{Z}, \cdot)$, namely the integers with multiplication.

What fails?

Well, if $a, b \in \mathbb{Z}$ then clearly $a \cdot b \in \mathbb{Z}$ so closure holds.✓

We also know that $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ so associativity holds.✓

Also, the number 1 acts as the identity since $a \cdot 1 = a = 1 \cdot a$.✓

As to inverses, we observe that, for example there is no integer a such that $2 \cdot a = 1$, and certainly 0 does not have a multiplicative inverse.

This last point echoes that discussion of units mod m as we saw earlier, which led to the development of $U(m)$.

Indeed, $\mathbb{Z}_m$ is not a group under multiplication since not every element has an inverse under multiplication, especially 0.

More on this later.

Here is another non-example based on the integers, namely $(\mathbb{Z}, -)$.

This is not a group even though it is closed.

What fails is associativity, and the existence of an identity, and therefore inverses.

i.e. Generally $(a - b) - c \neq a - (b - c)$ and while $a - 0 = a$, $0 - a = -a$.

Note also, that if one property fails, one doesn't need to check whether any others *do* hold since the group definition requires all 3 (or 4 if you include closure) properties to hold.

Other examples of groups.

$(\mathbb{Q}, +)$ - The rational numbers $\frac{a}{b}$ with addition.

closure and associativity are clear, and 0 is the identity as it is for $\mathbb{Z}$, and for $\frac{a}{b} \in \mathbb{Q}$, one has $-\frac{a}{b} \in \mathbb{Q}$ too.

If $\mathbb{Q}^*$ is the set of non-zero rationals, and $\cdot$ is multiplication, then $(\mathbb{Q}^*, \cdot)$ is a group,again, closure and associativity are clear,and certainly $\frac{a}{b} \cdot 1 = \frac{a}{b}$.

The omission of 0 gives rise to the existence of inverses for every element,since if $\frac{a}{b} \in \mathbb{Q}^*$ then $\frac{b}{a} \in \mathbb{Q}^*$ and obviously $\frac{a}{b} \cdot \frac{b}{a} = 1$.

Recall that $U(m)$ is constructed from $\mathbb{Z}_m$ by omitting those elements of $\mathbb{Z}_m$ that don't have inverses.

Is there a subset of $\mathbb{Z}$ which is a group under multiplication?

Yes, but it's kind of small, namely $\{\pm 1\}$ since any integer $a < -1$ or $a > 1$ will not have an inverse, but $(-1)(-1) = 1$ and also $(-1) \cdot 1 = (-1$ and $1 \cdot (-1) = -1$ and of course, $1 \cdot 1 = 1$.

Two really simple (dare I say trivial) examples of groups.

$(\{0\}, +)$ - literally the number zero by itself under addition

$(\{1\}, \cdot)$ - literally the number 1 under multiplication.

The verification of these is not too difficult.

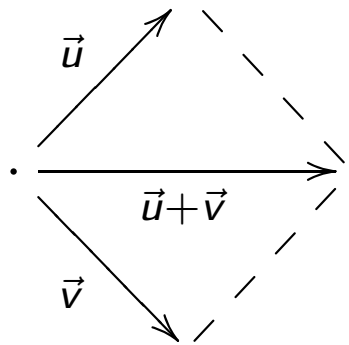
And, of course, as explored earlier, $(\mathbb{Z}_m, +)$ and $(U(m), \cdot)$ are both groups, where in $\mathbb{Z}_m$ it's addition mod m and in $U(m)$ it's multiplication mod m.

We noted in the development of $\mathbb{Z}_m$ and $U(m)$ that they do indeed form groups under the different operations.

We should also note that we consider the addition and multiplication operations on $\mathbb{Z}_m$, in particular how they interact via the distibutive law $a \cdot (b + c) = a \cdot b + a \cdot c$.

Sets which are closed with respect to *two* operations like this are called rings, which is a different class of mathematical objects we'll explore later in the course.

Another example of a group is the set of vectors in the plane, where the addition is by the so-called 'parallelogram rule' to add two vectors $\vec{u}$ and $\vec{v}$ to get $\vec{u} + \vec{v}$.



And one can see that this operation is closed and associative.

Moreover, there exists $\vec{0}$ which has zero length and has the property that $\vec{0} + \vec{u} = \vec{u}$.

Also, for every vector $\vec{u}$, the vector pointing in the *opposite direction* may be denoted $-\vec{u}$ and the sum of them is the zero vector $\vec{0}$.