Math 322 Lecture 2

rctcwyvrn

Sept 15 2020

1 Quotient sets continued

The quotient set $\mathbb{Z}/n\mathbb{Z}$ has a kind of addition on it

$$[\alpha] + [\beta] = [\alpha + \beta] \tag{1}$$

But is it well defined? (is it consistent for different values of α and β?)

Suppose $\alpha \sim \alpha'$, so $\alpha - \alpha' = kn$, similarly for β and β'. So we can rewrite

$$\alpha + \beta = \alpha' + \beta' + (kn + jn) \tag{2}$$

Which implies that $\alpha' + \beta' \sim \alpha + \beta$, so the addition is well defined.

We can add and subtract in this set, so it's a group

Definition: Group

A **group** is a set G with a binary operation "multiplication" $(\cdot)$ such that

- Associative $(g_1 \cdot g_2) \cdot g_3 = g_1 \cdot (g_2 \cdot g_3)$
- Identity $\exists 1_g : \forall x \in G : 1_g \cdot x = x \cdot 1_g = x$
- Inverse: $\forall x \in G : \exists y \in G : x \cdot y = y \cdot x = 1_g$

A group is a **commutative group** or **abelian group** if

- $\forall x, y \in G : x \cdot y = y \cdot x$
- Notation: use $+$ as the operator for a commutative group

Example: Obvious examples

$\mathbb{Z}, +$

Example:

$(\mathbb{Z}/N\mathbb{Z}, +)$ is a group

- It is also finite and commutative

Example: Matricies

n x n matricies are a group under $+$. The identity matrix is all zero, and the inverse matrix m is $-m$

- What about under multiplication?
- No, because not all matricies have inverses (so you need non-zero determinant matricies)
  - So the set of n by n matricies with non-zero determinant is a group
  - It is also non-commutative (matrix multiplication order matters)

Remark: We didn't actually check associativity (it's usually just trivial or annoying)

Remark: Composition of functions is associative

- ie $x \to y \to z \to w$
- $h \circ (g \circ f) = (h \circ g) \circ f$
- We can use this to check associativity easily

Example:

Let A be a set, and $S(A)$ the set of all bijective maps $f : A \to A$.

- $(S(A), \circ)$ is a group
- The symmetric group on the set A
- You can also thing of each of these functions as a permutation of the order of the elements

Check

- Associativity: $\circ$ is associative
- Identity: The identity function
- Inverse: The inverse function (which is why we require bijection)

Properties (of $S_n = S(\{1, 2, 3, \ldots\})$

- Highly non-commutative
- $n!$ elements

So a group is just a set that we can multiply and divide (multiply by inverse) that satisfies certain rules (depending on the group)

1.1 Cycle decomposition of permutations

Consider the element of S_7

$$1 \to 3 \tag{3}$$
$$3 \to 5 \tag{4}$$
$$\ldots \tag{5}$$

Is there a better way to write it?

$$(1 \to 3 \to 5 \to \ldots) \tag{6}$$

This is called the **cycle representation** (usually written without the arrows)

Example:

$(135)(467)(2)$ each cycle is grouped together, the entire function is

- $1 \to 3 \to 5 \to 1$

- $4 \to 6 \to 7 \to 4$
- $2 \to 2$

Note:

- We see that $\sigma^m = 1$ for some m, namely the LCM of the cycle lengths
- Note that each cycle has separate values, so they are **disjoint**

What about non disjoint cycles? Like $(1,2,3)(3,5,7)$

$$\sigma = \sigma_1 \circ \sigma_2 \tag{7}$$
$$\sigma_1 = (123) \tag{8}$$
$$\sigma_2 = (357) \tag{9}$$

The group operator is composition, so compose them

Note the order matters, $\sigma_2(\sigma_1)$ is

$$\sigma = (12573)(4)(6) \tag{10}$$

The other order is σ_2 first then σ_1, which is the convention for this class($\sigma_1 \circ \sigma_2 = \sigma_1(\sigma_2(x))$

$$\sigma = (12357)(4)(6) \tag{11}$$

So in S_7

$$(123)(357) = (12357) \tag{12}$$

Note: (123) is really just shorthand for $(123)(4)(5)(6)(7)$ in S_7

- They're called **fixed points**
- Note: it does depend on which set you're in ($(1,2,3)$ means different things in S_7 and S_{100})

Remark: Not all cycles are disjoint, but you can rewrite a **disjoint decomposition** for non disjoint cycles, like $(123)(357)$

Remark: Disjoint cycles will always commute with each other, because they don't share any elements. ie $(1,2,3)(4,5,6) = (4,5,6)(1,2,3)$

- Note: Not all commutative elements are disjoint though

Definition: Order

For group G, $g \in G$, the **order of g** is the smallest positive integer m such that $g^m = g \cdot g \cdot g \cdot g \ldots = 1_G$

- If no such m exists, then g has infinite order
- $(1354)(6(2)$ has order 4
- $(123)(45)$ has order 6, because the LCM (the first time they both end up at the start at the same time) is 6

Definition: Group order

The order of a group is the number of elements in G (may be infinite)

Lemma:

Let G be a finite group, then every element of G has finite order

Proof:

Consider $g, g^2, g^3 \ldots$.

Since G is finite $\exists r, s : r \neq s : g^r = g^s$ (by pigeonhole, since G is finite it must repeat at some point).
$\implies g^r g^{-r} = g^s g^{-r}$
$\implies 1_g = g^{s-r}$ and $s \neq r$, so g has order $s - r$

General principle: Commutative groups are simpler and easier to make sense of. Non-commutative groups have weird things and hare harder to deal with

Corresponding reading:

- 1.1, 1.3
- 1.2 next lecture