

## 3. MORE GROUP THEORY

Today we talked about the main properties of the elements of a group (although I didn't define a group yet). I just said that these are all permutations. I changed the format of the class to problem solving, similar to problem sessions, instead of lecturing.

## 3.1. inverse.

**Definition 3.1.** The inverse of a permutation  $\sigma$  is given by

$$\sigma^{-1}(x) = y \quad \text{where} \quad \sigma(y) = x$$

- a) Show that this defines a permutation  $\sigma^{-1}$ .
- b) Find a formula for the inverse of  $\tau = (a_1, a_2, \dots, a_k)$ .
- c) Show that  $(\sigma\tau)^{-1} = \tau^{-1}\sigma^{-1}$ .

Students found Question (a) confusing so we first did (b) and (c).

3.1.1. *inverse of a k-cycle.* The inverse of a cycle is given by writing the cycle backwards:

$$\tau^{-1} = (a_k, a_{k-1}, \dots, a_2, a_1)$$

This is supposed to be obvious, but a proof would go like this:

*Proof.* Let  $x = a_i$ . Then  $\tau(a_{i-1}) = a_i = x$ . So,  $\tau^{-1}(a_i) = a_{i-1}$ . Special care is needed in the case  $i = 1$ . Then the equation  $\tau(a_k) = a_1$  means (by definition) that  $\tau^{-1}(a_1) = a_k$ . If  $x$  is not any of the  $a_i$  then  $\tau(x) = x$ . So,  $\tau^{-1}(x) = x$ . This shows that  $\tau^{-1}(x)$  is given by the cycle above for all  $x$ .  $\square$

3.1.2. *inverse of a product.* The derivation of the formula

$$(\sigma\tau)^{-1} = \tau^{-1}\sigma^{-1}$$

used a lot more stuff than I thought. The concepts that were used by students familiar with groups were the following:

- (1) *associativity:*  $(ab)c = a(bc)$ . This implies that parentheses can be placed arbitrarily.
- (2) *identity:*  $id(x) = x$  is called the *identity* function and it is also called  $e = id$ . This has the property that  $e\sigma = \sigma = \sigma e$  since:

$$e\sigma(x) = e(\sigma(x)) = \sigma(x), \quad \sigma e(x) = \sigma(e(x)) = \sigma(x)$$

- (3) The group theoretic definition of the inverse which is:

$$\sigma^{-1}\sigma = e = \sigma\sigma^{-1}.$$

The proof of the inverse formula that students came up with, using these properties, was:

$$\begin{aligned}
 (\sigma\tau)(\tau^{-1}\sigma^{-1}) &= \sigma \underbrace{(\tau\tau^{-1})}_{e=id} \sigma^{-1} && \text{by associativity} \\
 &= \sigma e \sigma^{-1} && \text{by group theoretic def of inverse} \\
 &= \sigma \sigma^{-1} && \text{by property of } e \\
 &= e && \text{by def of inverse}
 \end{aligned}$$

We needed to know that, when the product of two things is the identity, the two things are inverse to each other:

**Lemma 3.2.** *If  $ab = e$  then  $b = a^{-1}$ .*

*Proof.* Multiply both sides by  $a^{-1}$ :

$$a^{-1}ab = a^{-1}e$$

The left hand side (LHS) is  $a^{-1}ab = eb = b$ , the RHS is  $a^{-1}$ .  $\square$

I actually skipped this lemma. What I verified in class was the group theoretic definition of inverse using my definition.

**Lemma 3.3.** *If  $\sigma^{-1}$  is defined as in Def. 3.1 (the “inverse function” definition) then we get the formulas:*

$$\sigma\sigma^{-1}(x) = x \quad \forall x, \quad \text{i.e., } \sigma\sigma^{-1} = id$$

$$\sigma^{-1}\sigma(y) = y \quad \forall y, \quad \text{i.e., } \sigma^{-1}\sigma = id$$

*Proof.* My definition was that  $\sigma^{-1}(x) = y$  if  $\sigma(y) = x$ . If we insert  $\sigma(y)$  in for  $x$  in the first equation we get:

$$\sigma^{-1}(\sigma(y)) = y$$

Thus  $\sigma^{-1}\sigma = id$ . If we insert the first equation into the second we get:

$$x = \sigma(y) = \sigma(\sigma^{-1}(x))$$

i.e.,  $\sigma\sigma^{-1} = id$ .  $\square$

3.1.3. *definition of a function.* I had to explain the first question because students had no idea even what it was asking.

Define: When I say that this formula *defines a function* I mean that for every  $x$  there is a unique  $y$  (so that  $\sigma(y) = x$ ).

I used the fact that  $\sigma$  is a permutation  $\Rightarrow$  bijection  $\Rightarrow$  1-1 and onto.

- (1) (existence)  $y$  exists since  $\sigma$  is *onto*: This means for any  $x \in X$  there is a  $y \in X$  so that  $\sigma(y) = x$ . So,  $\sigma^{-1}(x)$  exists.

- (2) (uniqueness) We need to know that for each  $x$  there is only one  $y$ , otherwise we don't have a function. I gave the example of:

$$\sqrt{x} = y \quad \text{if } y^2 = x$$

This formula does not define the square root function since there are two  $y$ 's for each positive  $x$ .

Uniqueness of  $y$  follows from the fact that  $\sigma$  is 1-1: If I had two  $y$ 's say  $y_1$  and  $y_2$  (in other words,  $\sigma^{-1}(x) = y_1$  and  $\sigma^{-1}(x) = y_2$ ) then I would have  $\sigma(y_1) = x = \sigma(y_2)$  which implies  $y_1 = y_2$  since  $\sigma$  cannot send to  $y$ 's to the same thing.

This show that  $\sigma^{-1} : X \rightarrow X$  is a function. To show it is a permutation, we have to show it is 1-1 and onto. We decided in class that both statements are obvious when you write down what they are in equation form:

$$\sigma^{-1}(x_1) = y = \sigma^{-1}(x_2) \Rightarrow \sigma(y) = x_1, \sigma(y) = x_2$$

So,  $\sigma^{-1}$  is 1-1. To show it is onto, we need to take any  $y$  in our set  $X$  and find some  $x$  so that

$$\sigma^{-1}(x) = y, \quad \text{i.e., } \sigma(y) = x.$$

Well, there it is!

**3.2. commutativity.** Students brought up the subject of *commutativity*.

**Definition 3.4.**  $a$  and  $b$  commute if  $ab = ba$ . A group  $G$  is *commutative* if  $ab = ba$  for all  $a, b \in G$ .

I pointed out that “commute” is a *verb* and “commutative” is an *adjective*.

Problem: If  $a, b$  commute, show that  $(ab)^{-1} = a^{-1}b^{-1}$ .

*Proof.* To show this you need to show

$$aba^{-1}b^{-1} = e$$

The proof that students gave is to switch  $a, b$  on the left since they commute:

$$aba^{-1}b^{-1} = baa^{-1}b^{-1} = bb^{-1} = e.$$

□

### 3.3. conjugation.

**Definition 3.5.** We say that  $a$  is *conjugate* to  $b$  if there exists a  $c$  so that

$$a = cbc^{-1}$$

I used the following notation. First,  $a \sim b$  for “ $a$  is conjugate to  $b$ ” and

$$\phi_c(b) := cbc^{-1}$$

The function  $\phi_c$  is a “homomorphism” (a concept that I will explain later).

- (1) Show that conjugation is an equivalence relation, i.e., it is
  - (a) reflective:  $(\forall a)a \sim a$
  - (b) symmetric:  $(\forall a, b)a \sim b \Rightarrow b \sim a$
  - (c) transitive:  $(\forall a, b, c)a \sim b, b \sim c \Rightarrow a \sim c$
- (2) If  $\tau = (a_1, a_2, \dots, a_k)$  then find a formula for  $\sigma\tau\sigma^{-1}$
- (3) Show that every permutation of  $n$  letters is conjugate to its inverse.

This is taking too long. I will write the answers later.