MATH 3311, FALL 2025: LECTURE 5, SEPTEMBER 5

Video: `https://youtu.be/OqjiXmOBktw`

Definition 1. A **group** is a triple $(G, *, e)$, where:

- G is a set;
- $*$ is a (binary) operation

$$G \times G \to G$$
$$(g_1, g_2) \mapsto g_1 * g_2$$

- $e \in G$ is an element

that satisfy the following properties:

(1) (Identity) For all $g \in G$, we have

$$e * g = g * e = g.$$

We call e the **identity** element of G.

(2) (Associativity) For all $g_1, g_2, g_3 \in G$, we have[1]

$$g_1 * (g_2 * g_3) = (g_1 * g_2) * g_3.$$

(3) (Inverse) For every $g \in G$, there exists $h \in H$ such that

$$g * h = e.$$

Fact 1. Given $g \in G$, there is a *unique* element $g^{-1} \in G$ such that $g * g^{-1} = g^{-1} * g = e$.

Note that there are two things new here:

- The *uniqueness* of the element g^{-1} such that $g * g^{-1} = e$. Condition (3) only gives you the *existence* of such an element.
- The unique right inverse g^{-1} is *also* a left inverse.

You will prove these facts rigorously on Homework 2.

Fact 2. Set[2]

$$g^n = \begin{cases} \underbrace{g * \cdots * g}_{n\text{-times}} & \text{if } n > 0 \\ \underbrace{g^{-1} * \cdots * g^{-1}}_{|n|\text{-times}} & \text{if } n < 0 \\ e & \text{if } n = 0. \end{cases}$$

Then, for any $n_1, n_2 \in \mathbb{Z}$, we have

$$g^{n_1} * g^{n_2} = g^{n_1 + n_2}.$$

Proof. The case where $n_1, n_2 \geq 0$ or both $n_1, n_2 \leq 0$ is easy (why?). What requires a bit of proof is the case where n_1 and n_2 are of different signs. This can be done using induction on both simultaneously. Consider

[1] The main motivation for what at first glance may seem non-intuitive is that function composition is *always* associative. This is very important.

[2] Note that this multiple self-product makes sense by associativity: it doesn't matter how you bracket the various successive products.

the example $g^2 * g^{-3}$:

$$\begin{aligned} g^2 * g^3 &\overset{Definition}{=} (g*g)*(g^{-1}*g^{-1}*g^{-1}) \\ &\overset{Assoc.}{=} g*(g*(g^{-1}*g^{-1}*g^{-1})) \\ &\overset{Assoc.}{=} g*((g*g^{-1})*(g^{-1}*g^{-1})) \\ &\overset{Inv.}{=} g*(e*(g^{-1}*g^{-1})) \\ &\overset{Ident.}{=} g*(g^{-1}*g^{-1}) \\ &\overset{Definition}{=} g*g^{-2} \end{aligned}$$

This process has reduced both exponents by 1 in magnitude. The same process works for any two exponents of opposite signs and lets us run the induction argument.

In particular, it applies to $g*g^{-2}$ to tell us that it is equal to $g^0*g^{-1} = e*g^{-1} = g^{-1}$. That is, we have found that $g^2 * g^{-3} = g^{-1}$. □

Remark 1. Why should $g^0 = e$? If we want $g^0 * g^m = g^m$, then this forces $g^0 = e$ by the next fact.

Fact 3. The identity element is *unique*. In fact, if $e', g \in G$ are such that $e' * g = g$ then $e' = e$.

Proof. Since we know by Fact 1 that we have the element g^{-1}, we can multiply $e' * g = g$ on the right by g^{-1} and obtain $(e' * g) * g^{-1} = g * g^{-1}$. The left hand side is equal to

$$e' * (g * g^{-1}) = e' * e = e',$$

while the right hand side is $g * g^{-1} = e$. Therefore, we conclude that $e' = e$. Note that all we did here was 'cancel' g from both sides using its inverse. □

Example 1. The first example is the **group with one element** or **trivial group**: We have $G = \{e\}$, the element e is the identity and the operation is given by $e * e = e$.

Example 2. The integers $(\mathbb{Z}, +, 0)$ under addition with 0 as the additive identity. Note that the natural numbers do *not* form a group under addition, because they don't contain inverses for the operation.

Definition 2. A group G has **finite order** if the underlying set is finite. In this case, its order $|G|$ is the size of the finite set.

Example 3. The set $\mathbb{Z}/n\mathbb{Z}$ of equivalence classes of integers mod-n equipped with *addition*: the identity is the equivalence class of 0, the bin containing all multiples of n. This is a finite group of order n.

The multiplicative group $(\mathbb{Z}/n\mathbb{Z})^\times$

In Homework 1, you checked using Bezout's lemma that, when p is a prime, the set $(\mathbb{Z}/p\mathbb{Z})^\times = (\mathbb{Z}/p\mathbb{Z})\backslash\{0\}$ of non-zero bins mod-p is a group under multiplication. The main point is that every non-zero bin admits a multiplicative inverse, which is a translation of the fact that, for $p \nmid a$, we can find integers s and t such that

$$1 = \gcd(a, p) = sa + tp.$$

This ensures that sa is in the same bin as 1 mod-p and so s functions as the multiplicative inverse for a mod-p.

Suppose that we replace p with any integer n (not necessarily prime). Then the same reasoning works *as long as* $\gcd(a, n) = 1$. In other words:

Fact 4. When $\gcd(a, n) = 1$, the bin of a mod-n admits a multiplicative inverse. Therefore, the set

$$(\mathbb{Z}/n\mathbb{Z})^\times = \{a \in \mathbb{Z}/n\mathbb{Z} : \ \gcd(a, n) = 1\}$$

forms a group under multiplication.

Example 4. One really has to discard all the elements *not* relatively prime to n to get multiplicative invertibility. If, for instance, we work with $n = 4$, then the non-zero entries in $\mathbb{Z}/4\mathbb{Z}$ are represented by $1, 2, 3$. Recall the multiplication table for these elements:

$\cdot$	1	2	3
1	1	2	3
2	2	0	2
3	3	2	1

Note that the second row and column have two features you wouldn't want in a group: Repetitions and an entry from *outside* the set being considered, in this case, the element 0. If we threw away 2 however (note that 2 is not relatively prime to 4), the remaining elements $1, 3$ do give a multiplicative group of order 2.

Example 5. Consider the group $(\mathbb{Z}/8\mathbb{Z})^\times$. This is a group of order 4. However, note that we have

$$3^2 = 5^2 = 7^2 = 1 \in (\mathbb{Z}/8\mathbb{Z})^\times.$$

It turns out that we can set up an isomorphism of groups

$$\begin{aligned} \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} &\xrightarrow{\simeq} (\mathbb{Z}/8\mathbb{Z})^\times \\ (1,1) &\mapsto 1 \\ (1,0) &\mapsto 3 \\ (0,1) &\mapsto 5 \\ (1,0) &\mapsto 7 \end{aligned}$$

Here, the left hand side is a *direct product*, which will be introduced in the next lecture.

Definition 3. Given groups $(G, *_G, e_G), (H, *_H, e_H)$, a **group homomorphism** $f : (G, *_G, e_G) \to (H, *_H, e_H)$ (or more simply $f : G \to H$) is a function

$$f : G \to H$$

such that, for all $g_1, g_2 \in G_1$, we have

$$f(g_1 *_G g_2) = f(g_1) *_H f(g_2) \in G_2.$$

Fact 5. For any group homomorphism $f : G \to H$, we have $f(e_G) = e_H$.

Proof. Note that we have equalities

$$f(g) = f(e_G *_G g) = f(e_G) *_H f(g)$$

Therefore, by Fact 3 applied in H we conclude that $f(e_G) = e_H$. □