MATH 2001
MODULAR ARITHMETIC AND GROUPS

Last time, we proved that for any integers a and b, we have the following relationship between equivalence classes:

$$[a] + [b] = [a + b],$$

where the sum of equivalence classes is defined as follows:

$$[a] + [b] = \{x + y : x \in [a], y \in [b]\}. \tag{1}$$

⋆ **Exercise 1.** Write out the addition table for the integers modulo 4 and modulo 5.

+	[0]	[1]	[2]	[3]
[0]				
[1]				
[2]				
[3]				

+	[0]	[1]	[2]	[3]	[4]
[0]					
[1]					
[2]					
[3]					
[4]					

Definition 2. A *group* is a set A equipped with an operation $*$ (not to be confused with multiplication) that satisfies the following properties.

a.) **Closed.** The group is closed under the operation, meaning: $a * b \in A$ for every pair of elements $a, b \in A$.

b.) **Associative.** The operation is associative, meaning: $a * (b * c) = (a * b) * c$ for every triple $a, b, c \in A$.

c.) **Identity.** The group contains a unique identity element e, meaning: there exists exactly one element $e \in A$ for which $a * e = e * a = a$ for every $a \in A$.

d.) **Inverse.** Every element of the group is invertible, meaning: for each $a \in A$, there exists exactly one element $b \in A$ for which $a * b = b * a = e$.

We denote the group by $G = (A, *)$, or simply G if the set and operation are understood.

Remark 3. The group operation $*$ need not be commutative, meaning that $a * b$ is *not necessarily equal* to $b*a$ for all elements of the group. Matrix multiplication is an example of a non-commutative action. If G is a group with a commutative operation, then G is a *commutative group*.

⋆ **Exercise 4.** Let E be the set of equivalence classes of $\mathbb{Z}$ modulo n, that is

$$E = \{[0], [1], \ldots, [n-1]\}, \quad \text{where} \quad [a] = \{b \in \mathbb{Z} : b \equiv a \bmod n\}.$$

Prove that $(E, +)$ is a group, where $+$ is the operation defined in equation (1).

Homework (Due Friday, November 20)**.** Let $[0], [1], \ldots, [n-1]$ denote the equivalence classes of $\mathbb{Z}$ modulo n, and define the product of equivalence classes by

$$[a] \cdot [b] = [ab]. \tag{2}$$

1.) Note that the product in equation (2) is defined by picking a specific representatives from the classes $[a]$ and $[b]$ (namely, the integers a and b, respectively). However, these classes contain infinitely many elements, and so it would be problematic if the product depended on our choice of representative. That is, it would be terribly inconsistent if we could choose other elements $a' \in [a]$ and $b' \in [b]$ for which $[a'b'] \neq [ab]$. Prove that this does not happen. That is, prove that $[a'b'] = [ab]$ for every $a' \in [a]$ and $b' \in [b]$.

2.) Write out the multiplication tables for the integers modulo 4 and modulo 5. (You do not have to turn these in.)

3.) Let E_n denote the set of non-zero equivalence classes modulo n (i.e. all the equivalence classes except $[0]$). Is $(E_4, \cdot)$ or $(E_5, \cdot)$ a group (where $\cdot$ is the operation defined in equation (2))? If yes, prove that it is a group. If no, explain why it is not.

4.) Define $[a]^m = [a^m]$. (In other words, $[a]^m$ is the product of m copies of $[a]$.) Prove that $\#\{[a]^m : m \in \mathbb{N}\} \leq n$ (i.e. the cardinality of this set is at most n).

Hint: prove that there exist positive integers m_1 and m_2 (where $m_1 \neq m_2$) for which $[a]^{m_1} = [a]^{m_2}$.

5.) Prove that if a and n share no common factors, then $[a]^m = [1]$ for some $m \in \mathbb{Z}$.

Hint: Prove that if a and n share no common factors, then a^k shares no common factors with n for any $k \in \mathbb{N}$.

6.) Make a conjecture: for what positive integers n is $(E_n, \cdot)$ a group. All? Some (which)? None? Prove your claim.