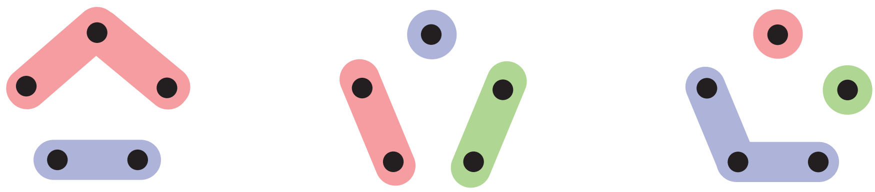
Integers modulo n

In this lecture we discuss some of the most important examples of groups: ones which come from taking certain equivalence classes of integers. To begin, we recall the notion of equivalence relations. Let S be a set, and $R \subset S \times S$ a subset. Write $a \sim b$ if and only if $(a, b) \in R$. Then R is an *equivalence relation* on the set S if the following hold:

1. (Reflexivity) $a \sim a$ for all $a \in S$.
2. (Symmetry) $a \sim b$ implies $b \sim a$.
3. (Transitivity) $a \sim b$ and $b \sim c$ implies $a \sim c$.

Given an equivalence relation on S as above, we write $[a] = \{b \in S : b \sim a\}$ for the *equivalence class of* a, which is a subset of S.

A *partition* of a set S is a collection of non-empty subsets $\{S_i\}_{i \in I}$ of S such that the union of all S_i over $i \in I$ is equal to S, and the subsets are pairwise disjoint: $S_i \cap S_j = \varnothing$ if $i \neq j$. For example, for a set with 5 elements represented by dots, here are depicted a few different partitions of S, where the subsets are encoded by colors:



Equivalence relations on sets and partitions of sets are essentially the same thing. Given an equivalence relation on S, the equivalence classes form a partition of S. Conversely, if we have a partition $\{S_i\}_{i \in I}$ of S, then the relation $a \sim b$ if and only if "a and b belong to some common subset S_i" defines an equivalence relation on S.

The group $\mathbb{Z}_n$

Fix a positive integer n. Define a relation on $\mathbb{Z}$ as follows: $a \sim b$ if and only if $a - b = nk$ for some $k \in \mathbb{Z}$. We check that this is an equivalence relation:

1. (Reflexivity) $a \sim a$ because $a - a = n0$.
2. (Symmetry) $a \sim b$ implies $a - b = nk$. Then $b - a = n(-k)$, implying $b \sim a$.
3. (Transitivity) $a \sim b$ and $b \sim c$ imply $a - b = nk$ and $b - c = nl$. Consequently we have $a - c = (a - b) + (b - c) = nk + nl = n(k + l)$. This implies $a \sim c$.

This equivalence relation partitions the set $\mathbb{Z}$ into n equivalence classes.

$$\mathbb{Z}_n = \{\text{equivalence classes of the relation } \sim \} = \{[0], [1], \ldots, [n-1]\}$$

For example, if $n = 3$, then $\mathbb{Z}_3$ consists of the equivalence classes $[0], [1], [2]$ where

$$[0] = \{0 + 3k : k \in \mathbb{Z}\}$$
$$[1] = \{1 + 3k : k \in \mathbb{Z}\}$$
$$[2] = \{2 + 3k : k \in \mathbb{Z}\}$$

and these partition the integers into 3 subsets. More generally, $[0], [1], \ldots, [n-1]$ are the equivalence classes of this relation. The set $\mathbb{Z}_n$ is called the *integers modulo* n or the *integers mod* n. Another notation for $a \sim b$ is: $a \equiv b \pmod{n}$. In summary we have:

$$[a] = [b] \quad\Longleftrightarrow\quad a - b = nk \text{ for some } k \in \mathbb{Z} \quad\Longleftrightarrow\quad a \equiv b \pmod{n}$$

Next, we define a binary operation "+" on the set $\mathbb{Z}_n$ as follows:

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

We first check this is well-defined. That is, suppose $[a'] = [a]$ and $[b'] = [b]$, i.e. $a' - a = nk$ and $b' - b = nl$. Then $(a' + b') - (a + b) = (a' - a) + (b' - b) = nk + nl = n(k + l)$. We conclude that $[a' + b'] = [a + b]$, and the operation is well-defined.

▸ **The set $\mathbb{Z}_n$ with the operation $+$ is an abelian group.**

To verify this we check the group axioms. First, we have associativity:

$$\begin{aligned}[a] + ([b] + [c]) &= [a] + [b + c] = [a + (b + c)] \\ &= [(a + b) + c] = [a + b] + [c] = ([a] + [b]) + [c].\end{aligned}$$

Note that associativity of $(\mathbb{Z}, +)$ was used from one line to the next. Next, $e = [0]$ is an identity because $[a] + [0] = [a + 0] = [a]$ and similarly $[0] + [a] = [a]$. An inverse for $[a] \in \mathbb{Z}_n$ is $[-a]$ because $[a] + [-a] = [a + (-a)] = [a - a] = [0]$ and similarly $[-a] + [a] = [0]$. Thus $(\mathbb{Z}_n, +)$ is a group. It is abelian because $[a] + [b] = [a + b] = [b + a] = [b] + [a]$.

The group $\mathbb{Z}_n$ is sometimes written $\mathbb{Z}/n$ or $\mathbb{Z}/n\mathbb{Z}$. When working in $\mathbb{Z}_n$ we often drop the brackets from the equivalence classes and write "a" instead of "$[a]$". The context should make it clear that "a" means the equivalence class of a mod n, and not the integer a. Using this convention, the following is the Cayley table for the group $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$:

	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

For example, in $\mathbb{Z}_6$ we have $1 + 1 = 2$, $3 + 3 = 0$ and $4 + 4 = 2$. We can also write these relations as $1 + 1 \equiv 2 \pmod{6}$, $3 + 3 \equiv 0 \pmod{6}$ and $4 + 4 \equiv 2 \pmod{6}$.

Cyclic groups

The group $(\mathbb{Z}_n, +)$ is a finite abelian group of order n. It is also very special because it is a cyclic group. An arbitrary group G is called *cyclic* if there is some $a \in G$ such that

$$G = \{a^k : k \in \mathbb{Z}\}.$$

The element a is called a *generator* of the group G. The group $(\mathbb{Z}, +)$ is cyclic with generator $1 \in \mathbb{Z}$, because any integer $a \in \mathbb{Z}$ can be written as $a = 1 + \cdots + 1$. For a similar reason:

▸ **The group $(\mathbb{Z}_n, +)$ is a cyclic group.**

To spell this out, take $a = [1]$. Then "a^k" in the group $(\mathbb{Z}_n, +)$ is none other than $[1]+\cdots+[1]$, where $[1]$ appears k times, which is equal to $[k]$. Now $\mathbb{Z}_n$ consists exactly of the classes $[k]$ as k runs over the integers; in fact, as we saw above, k need only run over $0, 1, \ldots, n-1$. Thus every element of $\mathbb{Z}_n$ is of the form "a^k" and so $\mathbb{Z}_n$ is cyclic with generator $[1]$.

In turns out the groups $(\mathbb{Z}, +)$ and $(\mathbb{Z}_n, +)$ for positive integers n are essentially the "only" cyclic groups, in a sense that we will make precise later.