Cyclic group, C_n

In this article, we will explore a type of group called "cyclic group." As a prerequisite, we need to learn a new type of number: Integers modulo n.

Remember what we learned in our earlier article "Equivalence relation." If we consider integers modulo 3, there are only three equivalence classes: [0], [1], [2]. Let's denote each element of this class by $\bar{0}_3$, $\bar{1}_3$, $\bar{2}_3$. Then, we have the following addition rules.

$$\bar{0}_3 + \bar{0}_3 = \bar{0}_3, \quad \bar{0}_3 + \bar{1}_3 = \bar{1}_3, \quad \bar{0}_3 + \bar{2}_3 = \bar{2}_3 \tag{1}$$

$$\bar{1}_3 + \bar{0}_3 = \bar{1}_3, \quad \bar{1}_3 + \bar{1}_3 = \bar{2}_3, \quad \bar{1}_3 + \bar{2}_3 = \bar{0}_3 \tag{2}$$

$$\bar{2}_3 + \bar{0}_3 = \bar{2}_3, \quad \bar{2}_3 + \bar{1}_3 = \bar{0}_3, \quad \bar{2}_3 + \bar{2}_3 = \bar{1}_3 \tag{3}$$

It is easy to check that

$$\{\bar{0}_3, \bar{1}_3, \bar{2}_3\} \tag{4}$$

with "+" as the group multiplication form a group. This group is called "cyclic group" of order 3, and is denoted as "C_3."

Problem 1. What is the identity element of this group?

Problem 2. What is the inverse element of $\bar{1}_3$?

Problem 3. Is C_3 Abelian or non-Abelian?

Another way of looking at the cyclic group is regarding it as rotation. Consider the following group of order 3.

$$\{e, c_{120}, c_{240}\} \tag{5}$$

where e is the identity element (i.e. no rotation), c_{120} is a clockwise rotation of 120°, and c_{240} is a clockwise rotation of 240°. Then, for example,

$$c_{240} \bullet c_{120} = e \tag{6}$$

means that, if you rotate an object by clockwise direction in 120° followed by another clockwise rotation of 240°, the object comes to the original point, as it is rotated by 360°.

Given this, it is very easy to find a one-to-one correspondence between this group and C_3. The correspondence is following:

$$\bar{0}_3 \leftrightarrow e, \qquad \bar{1}_3 \leftrightarrow c_{120}, \qquad \bar{2}_3 \leftrightarrow c_{240} \tag{7}$$

Two groups can be regarded as the same group, if there is a one-to-one correspondence between the two groups, and this correspondence preserves the group multiplication. Let me clarify what I mean here. Suppose we have

$$a \bullet b = c \tag{8}$$

where a, b, c, and d are some elements of group G_1. Suppose you found the following one to one correspondence between group G_1 and group G_2, whose elements include A, B, C and D.

$$a \leftrightarrow A, \qquad b \leftrightarrow B, \qquad c \leftrightarrow C, \qquad d \leftrightarrow D \tag{9}$$

Then, if this one-to-one correspondence preserves the group multiplication, the following group multiplication must be satisfied

$$A \bullet B = C \tag{10}$$

because C corresponds to c, which is $a \bullet b$. If $A \bullet B = D$ were satisfied instead of (10), group G_2 and G_1 can *not* be regarded as the same group, even though they have the *same* order. In our case, C_3 and (5) have one-to-one correspondence, which preserves the group multiplication. For example, (6) corresponds to

$$\bar{2}_3 + \bar{1}_3 = \bar{0}_3 \tag{11}$$

Therefore, (5) is the same group as C_3.

Still another way of looking at C_3 is the following:

$$C_3 = \{e, a, a^2; a^3 = e\} \tag{12}$$

where the expression after semicolon denotes the additional condition ($a^3 = e$) we impose. This additional condition determines the group multiplication. For example, if we multiply a^2 and a^2, we get

$$a^2 \bullet a^2 = aaaa = a^3 a = ea = a \tag{13}$$

If $\bar{1}_3$ corresponds to a, this multiplication corresponds to $\bar{2}_3 + \bar{2}_3 = \bar{1}_3$. You can also think of a as a clockwise rotation of $120°$. a^3 is the identity because it corresponds to $360°$ rotation.

I leave what cyclic groups of other orders look like as an imagination to the readers.

Problem 4. Consider C_5, i.e.,

$$\{\bar{0}_5, \bar{1}_5, \bar{2}_5, \bar{3}_5, \bar{4}_5\} \tag{14}$$

with "+" as group multiplication. What is the inverse element of $\bar{3}_5$?

Problem 5. If you regard C_5 as rotation, how much degrees of rotation does $\bar{1}_5$ correspond to? (There are several possible answers, but just find one. Of course, if you want to challenge yourself, you can find all the answers.)

Summary

- Cyclic group C_n is defined by addition of integer modulo n.
- It can also be expressed as

$$C_n = \{e, a, a^2, \cdots, a^{n-1}; a^n = e\}$$