16 Cyclic and Dihedral Groups

The integers modulo n

If the current time is 9 o'clock, then 7 hours later the time will be 4 o'clock. This is because $9 + 7 = 16$ and 16 is treated as the same as 4 since these two numbers differ by 12. This is an instance of arithmetic in $\mathbb{Z}_{12}$, the integers modulo 12.

Definition. For every positive integer n we define $\mathbb{Z}_n$ to be the integers $\mathbb{Z}$ with an additional equivalence: We treat a and b as equivalent if a and b differ by a multiple of n. Up to this equivalence, $\mathbb{Z}_n$ has just n distinct numbers $\{0, 1, \ldots, n-1\}$. We call $\mathbb{Z}_n$ the integers *modulo* n and we say that $a \in \mathbb{Z}_n$ is in *standard form* if a is one of $0, 1, \ldots, n-1$.

Note: When doing clock arithmetic we are working with $\mathbb{Z}_{12}$, the integers modulo 12. However, unlike the usual convention in math of using $\{0, 1, \ldots, 11\}$, when working with a 12 hour clock it is common to use $\{1, 2, \ldots, 12\}$ instead.

Addition. If $a, b \in \mathbb{Z}_n$ are represented in standard form then adding them give us another integer that will be at least 0 and at most $2n-2$. If this integer is $\geq n$, then in order to get back to the usual form we need to subtract n.

Example: The integers modulo 5 have addition table (in standard form)

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

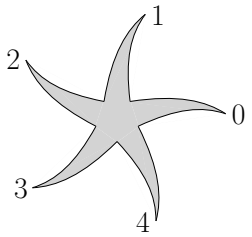
Negation. Our definitions apply equally well to negative numbers. When working in $\mathbb{Z}_n$ a negative integer $-a$ is equivalent to $-a + n$ and $-a + 2n$ and so on.

Example: The following chart shows the negation of the (standard form) elements of $\mathbb{Z}_8$.

number	0	1	2	3	4	5	6	7
negation	0	7	6	5	4	3	2	1

The cyclic group C_n

To see why we introduced the integers modulo n, let's think about symmetries of the figure below, where we have marked the 5 extreme points with the elements of $\mathbb{Z}_5$.



The only symmetries of this object are rotations about the centre point by multiples of $\frac{2\pi}{5}$. Let's think about how the marked points behave under the symmetries. If we rotate (counterclockwise) by $\frac{2\pi}{5}$, then 0 goes to 1, 1 goes to 2, 2 goes to 3, 3 goes to 4, and 4 goes to 1. This is described very compactly by using the arithmetic of $\mathbb{Z}_5$. Namely, working in $\mathbb{Z}_5$, the point with label a goes to the point with label $a+1$.

Definition. If a is an element of $\mathbb{Z}_n$ we define the function $R_a : \mathbb{Z}_n \to \mathbb{Z}_n$ by the rule $R_a(x) = x + a$. We call any such function a *rotation* (of $\mathbb{Z}_n$). It is straightforward to verify that every rotation is a transformation of $\mathbb{Z}_n$.

Definition. $C_n = \{R_a \mid a \in \mathbb{Z}_n\}$. The following lemma shows that C_n is a subgroup of $\mathbb{Z}_n$ and we say that C_n is a *cyclic* group.

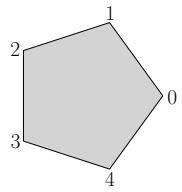
Lemma 16.1. *C_n is a subgroup of* $\mathrm{Trans}(\mathbb{Z}_n)$

Proof. First note that the $R_0 = I$, so C_n does contain the identity. Next let $a, b \in \mathbb{Z}_n$ and consider the product of the functions R_a and R_b. For every $x \in \mathbb{Z}_n$ we have $R_aR_b(x) = R_a(R_b(x)) = R_a(x+b) = x + (a+b) = R_{a+b}(x)$. It follows that C_n is closed under products. It follows from this that every $a \in \mathbb{Z}_n$ satisfies $R_aR_{-a} = R_0 = I$. So, the inverse of R_a is R_{-a} and we have that C_n is also closed under inverses. □

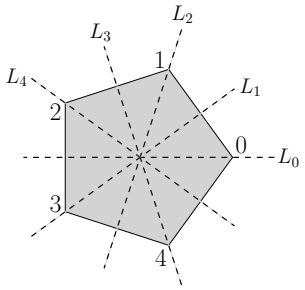
Example: The group C_5 is a subgroup of $\mathrm{Trans}(\mathbb{Z}_5)$ consisting of the five functions R_0 (add 0), R_1 (add 1), R_2 (add 2), R_3 (add 3), and R_4 (add 4). The function R_0 is the identity, R_1, R_4 are inverses, and R_2, R_3 are inverses. To combine the elements we use the rule $R_aR_b = R_{a+b}$ using addition modulo 5 for the indices.

The dihedral group D_n

Next we consider symmetries of a regular pentagon, where the vertices have been marked with elements of $\mathbb{Z}_5$ as shown below.



As before, we consider how the marked points behave under symmetries of the pentagon. Rotating the pentagon around its centre by a multiple of $\frac{2\pi}{5}$ is a symmetry. These symmetries align with the rotations of $\mathbb{Z}_5$ above. However, we also have some additional symmetries. The figure below shows lines, $L_0, \ldots, L_4$ and each of these lines indicates a mirror symmetry.



The mirror symmetry for line L_0 takes the point 0 to itself, interchanges 1 and 4, and interchanges 2 and 3. This is precisely the function $F : \mathbb{Z}_5 \to \mathbb{Z}_5$ given by the rule $F(x) = -x$. More generally, as you can easily verify, the mirror symmetry for line L_i is given by the transformation of $\mathbb{Z}_5$ given by $x \to -x + i$. Next we introduce a definition to generalize this example.

Definition. If a is an element of $\mathbb{Z}_n$, we define the function $M_a : \mathbb{Z}_n \to \mathbb{Z}_n$ by the rule $M_a(x) = -x + a$. We call any such function a *mirror* of $\mathbb{Z}_n$. It is straightforward to verify that every mirror is a transformation of $\mathbb{Z}_n$.

Definition. $D_n = \{R_a \mid a \in \mathbb{Z}_n\} \cup \{M_a \mid a \in \mathbb{Z}_n\}$. So, D_n is the set of all transformations of $\mathbb{Z}_n$ of the form $F(x) = \pm x + a$. The following lemma shows that D_n is a subgroup of $\mathrm{Trans}(\mathbb{Z}_5)$ and we say that D_n is a *dihedral* group.

Lemma 16.2. *D_n is a subgroup of* $\mathrm{Trans}(\mathbb{Z}_n)$

Proof. We have $I = R_0$ so D_n contains the identity. To check for closure under products, let $F, G \in D_n$ and note that we may write F, G as $F(x) = ax + b$ and $G(x) = cx + d$ where $a, c = \pm 1$. Now the function FG satisfies

$$FG(x) = F(G(x)) = F(cx + d) = a(cx + d) + b = (ac)x + (ad + b).$$

Therefore, $FG = R_{ad+b}$ if $ac = 1$ and $FG = M_{ad+b}$ if $ac = -1$. In either case we find that $FG \in D_n$ and thus D_n is closed under products. To verify that D_n is closed under inverses, first note that every rotation R_a has inverse R_{-a}. We claim that every mirror M_a is its own inverse. To check this, we compute

$$M_a M_a(x) = M_a(-x + a) = -(-x + a) + a = x$$

So, every mirror is its own inverse, and we conclude that D_n is closed under inverses. □

At this point we have studied $\mathrm{Trans}(X)$ in three special cases. When $X = \{1, 2, \ldots, n\}$ this is the group of all permutations S_n, and we have shown that A_n (the even permutations) form a subgroup. When $X = \mathbb{Z}_n$ the set X has a simple structure under addition, and we have shown the existence of two subgroups based on this structure: D_n and C_n. Finally we have looked at this when $X = \mathbb{R}^n$ where we introduced several specially structured subgroups.