Groups

Definition: Let G be a set. A binary operation on G is a function that assigns each ordered pair of elements of G an element of G. This condition is called *closure.*

image

Suppose we remove a square region from a plane, move it in some way, then put the square back into the space it originally occupied. Our goal in this chapter is to describe all possible ways in which this can be done. More specifically, we want to describe the possible relationships between the starting position of the square and its final position in terms of motions. However, we are interested in the net effect of a motion, rather than in the motion itself.

To begin, we can think of the square region as being transparent (glass, say), with the corners marked on one side with the colors blue, white, pink, and green. This makes it easy to distinguish between motions that have different effects.

The eight motions $R\_0, R\_90, R\_180, R\_270, H, V, D$, and D', together with the operation composition, form a mathematical system called the dihedral group of order 8. *Note: Inverse of R_α, L is $R\_360 - \alpha$, L resp. (L is a reflection)*

Cayley Table for D_4 image The analysis carried out above for a square can similarly be done for an equilateral triangle or regular pentagon or, indeed, any regular n-gon ($n \geq 3$). The corresponding group is denoted by D_n and is called the dihedral group of order $2n$. It is often called the group of symmetries of a regular n-gon.

A plane symmetry of a figure F in a plane is a function from the plane to itself that carries F onto F and preserves distances; that is, for any points p and q in the plane, the distance from the image of p to the image of q is the same as the distance from p to q.

The symmetry group of a plane figure is the set of all symmetries of the figure. Obviously, a rotation of a plane about a point in the plane is a symmetry of the plane, and a rotation about a line in three dimensions is a symmetry in three-dimensional space. Similarly, any translation of a plane or of three-dimensional space is a symmetry. A reflection across a line L is that function that leaves every point of L fixed and takes any point q, not on L, to the point q' so that L

is the perpendicular bisector of the line segment joining q and q'. A reflection across a plane in three dimensions is defined analogously.

Just as a reflection across a line is a plane symmetry that cannot be achieved by a physical motion of the plane in two dimensions, a reflection across a plane is a three-dimensional symmetry that cannot be achieved by a physical motion of three-dimensional space.

To be sure that D_4 is indeed a group, we should check this equation for each of the $8^3 = 512$ possible choices of a, b, and c in D_4. In practice, however, this is rarely done! Here, for example, we simply observe that the eight motions are functions and the operation is function composition. Then, since function composition is associative, we do not have to check the equations.

Be sure to verify closure when testing for a group.

Notice that if a is the inverse of b, then b is the inverse of a.

If a group has the property that ab = ba for every pair of elements a and b, we say the group is Abelian. A group is non-Abelian if there is some pair of elements a and b for which ab $\neq$ ba.

Example: The set of integers under ordinary multiplication is not a group. Since the number 1 is the identity, property 3 fails.

Example: The set S of positive irrational numbers together with 1 under multiplication satisfies the three properties given in the definition of a group but is not a group. Indeed, $\sqrt{2} * \sqrt{2} = 2$, so S is not closed under multiplication.

image

Example: By Exercise 11 in Chapter 0, an integer a has a multiplicative inverse modulo n if and only if a and n are relatively prime (easy to prove, and a very important observation is that if integer a has multiplicative inverse b, then we can as well say that a is the multiplicative inverse of b and therefore b and n are relatively prime). So, for each n > 1, we define U(n) to be the set of all positive integers less than n and relatively prime to n. Then U(n) is a group under multiplication modulo n. (We leave it to the reader to check that this set is closed under this operation (Proof: $at\_1 + nt\_2 = 1, bt\_3 + nt\_4 = 1 \Rightarrow abt\_1t\_3 + at\_1nt\_4 + nt\_2bt\_3 + n^2t\_2t\_4 \Rightarrow ab(..) + n(..) = 1$).) For n = 10, we have U(10) = {1, 3, 7, 9}.

Example: The set of integers under subtraction is not a group, since the operation is not associative.

image

image

image

Example: The set {1, 2, . . . , n - 1} is a group under multiplication modulo n if and only if n is prime (as each element must possess an inverse).

image

The following three theorems were very easy to prove for me.

image

image

image

A consequence of the cancellation property is the fact that in a Cayley table for a group, each group element occurs exactly once in each row and column. **Proof:** Each element occurs at least once as suppose M doesn't occur in column of R, its not possible as we have $R^{-1}M =$ something (binary composition). Now to prove at most 1, we have $RM = K$ and $RN = K \Rightarrow RM = RN \Rightarrow M = N$.

image

So we will unambiguously denote the inverse by g^{-1}

image

image

image

Note: $ax = b \Rightarrow x = a^{-1}b$ *which is unique as inverse is unique*

Also, one must be careful with this notation when dealing with a specific group whose binary operation is addition and is denoted by "+"

image

So, g^{-3} means $(-g) + (-g) + (-g)$ and is written as $-3g$.

As is the case for real numbers, we use a - b as an abbreviation for a + (-b).

image

image