9-6-1993

Groups.

Definition. A **binary operation** on a set X is a function $f : X \times X \to X$.

Binary operations are usually denoted by **infix operators**:

$$x \cdot y \text{ or } x * y \text{ or even } xy \text{ rather than } f(x, y).$$

Examples. 1. Addition, subtraction, and multiplication are binary operations on $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$. Division is not. $\square$

2. If X is a set and $\mathrm{Hom}(X, X)$ is the set of functions $x \to X$, then function composition is a binary operation on $\mathrm{Hom}(X, X)$. $\square$

Definition. A **group** is a set G with a binary operation $*$ such that:

1. (**Associativity**) $a * (b * c) = (a * b) * c$ for all $a, b, c \in G$.
2. (**Identity**) There is an element $1 \in G$ such that $1 * a = a = a * 1$ for all $a \in G$.
3. (**Inverses**) For each $a \in G$, there is an element $a^{-1} \in G$ (the **inverse** of a) such that $a*a^{-1} = 1 = a^{-1}*a$.

Examples. 1. $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ are groups with addition as the operation. $\square$

2. $\mathbb{Q}^{\geq 0} = \{q \in \mathbb{Q} \mid q \geq 0\}$ is not a group under addition (no inverses). $\square$

3. Let $\mathbb{Z}_n$ (read "Z mod n") denote the set of equivalence classes of integers under equality mod n. There are n equivalence classes: The class containing 0, the class containing 1, ..., the class containing $n - 1$. I will abuse notation and denote the equivalence classes by 0, 1, ..., $n - 1$.

For example, if $n = 4$, $\mathbb{Z}_4 = \{0, 1, 2, 3\}$. Add elements of $\mathbb{Z}_n$ by adding and reducing mod n. Thus, in $\mathbb{Z}_4$,

$$2 + 2 = 0, \quad 3 + 2 = 1, \quad \text{and so on.}$$

With these definitions, $\mathbb{Z}_n$ is a group. It is called the **cyclic group of order** n.

(In general, the **order** of a group is the number of elements in the group, if it is finite. Otherwise, the group is **infinite.**) $\square$

4. $\mathbb{Q}$ is not a group under multiplication. But $\mathbb{Q}^*$, the nonzero rationals, is a group under multiplication. $\square$

5. If X is a set, let $\mathrm{Aut}\, X$ denote the set of bijections $X \to X$. $\mathrm{Aut}\, X$ is a group with the operation of function composition. $\square$

6. $GL(n, \mathbb{R})$ denotes the set of invertible $n \times n$ matrices with real entries, the **general linear group**. $GL(n, \mathbb{R})$ is a group under matrix multiplication. $\square$

7. Let $\mathbb{R}^*$ denote the nonzero reals. Define a binary operation on $\mathbb{R}^*$ by

$$a \cdot b = |a| b.$$

(The operation is $\cdot$, and I multiply as usual on the right side.) This is an associative binary operation. 1 is a **left identity**, in the sense that $1 \cdot a = a$ for all $a \in \mathbb{R}^*$. There are also **right inverses**: $a \cdot \dfrac{1}{a} = 1$ for all $a \in \mathbb{R}^*$. $\mathbb{R}^*$ with $\cdot$ is not a group. $\square$

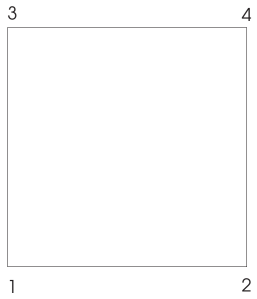
8. A **regular** n**-gon** is a closed, convex polygon in the plane with n equal sides. For example, a regular 3-gon is an equilateral triangle, and a regular 4-gon is a square.

A **rigid motion** of the plane is a map $\mathbb{R}^2 \to \mathbb{R}^2$ which preserve distances. D_n, the **dihedral group** of order $2n$, is the group of rigid motions of the plane which carry a given regular n-gon onto itself. (Such a rigid motion is said to **preserve** the figure. It is also called a **symmetry** of the figure.)

If you wish, you may think of D_n as the set of rigid motions of the plane which carry the set n complex n-th roots of 1 onto itself. For example, the 4-th roots of 1 are $\{1, -1, i, -i\}$, and D_4 is the set of rigid motions of the plane which map the set of 4-th roots to itself.

I will look at D_4, the dihedral group of order 8. First, I will show that the square has 8 symmetries.

A map which carries the square onto itself must map vertices to vertices. Here is a picture of a square with the vertices labelled.



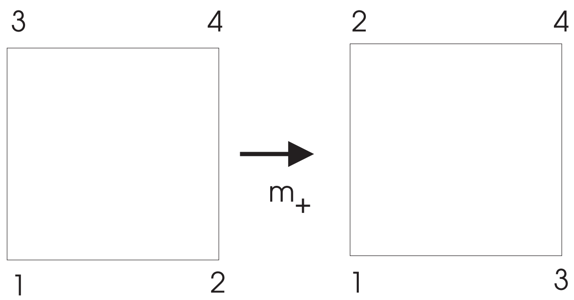
Consider vertex 1. A rigid motion can map it to any of the 4 vertices. Once I know where 1 goes, 3 must go to the vertex opposite it, since distance are preserved. Now there are only two possibilities for vertices 2 and 4. All together, I have $4 \cdot 2 = 8$ choices, so there at most 8 symmetries. I'll show there are exactly 8 by displaying 8 different symmetries.

(Before I do, note that the same argument shows that $|D_n| \leq 2n$.)

I will take my square to be as pictured above. The 8 symmetries are as follows:

1. id, the identity symmetry.
2. r_1, counterclockwise rotation through $\dfrac{\pi}{2}$.
3. r_2, counterclockwise rotation through π.
4. r_3, counterclockwise rotation through $\dfrac{3\pi}{2}$.
5. m_x, reflection across the horizontal line which bisects the square.
6. m_y, reflection across the vertical line which bisects the square.
7. m_+, reflection across the "southwest to northeast" line which bisects the square.
8. m_-, reflection across the "northwest to southeast" line which bisects the square.

For example, here is m_+:

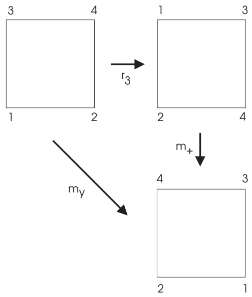


The operation on D_4 is function composition — do one rigid motion after another. It's clear that this is a binary operation, but I need to establish a convention concerning how I will write the operation. I will write

$$m_+ \cdot r_3 \quad \text{to mean} \quad r_3, \text{ then } m_+.$$

In other words, I'll apply the motions from right to left. This is consistent with the usual notation for composing functions: $f(g(x))$ means g first, then f.

The next picture shows the composite $m_+ \cdot r_3$. You can see that $m_+ \cdot r_3 = m_y$.



With a little bit of patience (and perhaps a little cardboard square), you can generate the multiplication table for D_4. Here it is:

	id	r_1	r_2	r_3	m_+	m_-	m_x	m_y
id	id	r_1	r_2	r_3	m_+	m_-	m_x	m_y
r_1	r_1	r_2	r_3	id	m_y	m_x	m_+	m_-
r_2	r_2	r_3	id	r_1	m_-	m_+	m_y	m_x
r_3	r_3	id	r_1	r_2	m_x	m_y	m_-	m_+
m_+	m_+	m_x	m_-	m_y	id	r_2	r_1	r_3
m_-	m_-	m_y	m_+	m_x	r_2	id	r_3	r_1
m_x	m_x	m_-	m_y	m_+	r_3	r_1	id	r_2
m_y	m_y	m_+	m_x	m_-	r_1	r_3	r_2	id

This table illustrates a number of ideas.

A group G is **abelian** if $a \cdot b = b \cdot a$ for all $a, b \in G$. From the table, it is apparent that D_4 is *not* abelian. For example, $m_+ r_3 = m_y$, but $r_3 m_+ = m_x$.

Next, if you examine the table, you will see that each row contains each element of the group exactly once. The same is true for each column. This is true for an arbitrary group G. Here's why.

Consider the row for the element $a \in G$. If x occurs in the b and c columns, this means that $ab = x = ac$. Multiply this equation on the left by a^{-1}:

$$a^{-1} \cdot ab = a^{-1} \cdot ac, \quad \text{so } b = c.$$

That is, the b and c columns are actually the same columns. Hence, each row contains a given element at most once.

On the other hand, consider again the row for $a \in G$. Take $x \in G$; does x occur in this row? Well, $x = a \cdot (a^{-1}x)$, so x occurs in the column for $a^{-1}x$. That is, every element of G occurs in the row for a.

All together, every element of G occurs exactly once in the row for a. A similar argument works for columns.

This fact is of some use if you are constructing group multiplication tables by hand. In fact, why not find *all* groups of a given order by simply writing down multiplication tables?

This is surely a finite process for groups of order (say) 1024, but it isn't very practical. For one thing, the number of possibilities quickly becomes astronomical. (There is no formula known which gives the number of "different" groups of order n in terms of n.) For another thing, there are situations in which two tables represent the "same" group, but this isn't always easy to tell from the group table. $\square$