8-23-2016

Examples of Groups

In this section, I'll look at some additional examples of groups. Some of these will be discussed in more detail later on.

In many of these examples, I'll assume familiar things like associativity of addition or multiplication. A really careful discussion would often require an extensive discussion of foundations: For instance, associativity of addition for the integers would require a discussion of how the integers are constructed.

Example. (**The integers mod n**) $\mathbb{Z}_n$ (read "Z mod n") denote the set of equivalence classes of integers under equality mod n. It's a group under addition mod n.

If a and b are integers and n is a positive integer (in most cases, $n > 1$), then a and b are **congruent mod n** if n divides $a - b$. In this case, you write $a = b \pmod{n}$.

For example, -6 and 36 are congruent mod 14, since 14 divides $36 - (-6) = 42$.

Equality mod n is an **equivalence relation** on $\mathbb{Z}$, and therefore $\mathbb{Z}$ is **partitioned** into **equivalence classes**. For example, the equivalence classes of integers mod 4 are

$$\{\ldots, -8, -4, 0, 4, 8, \ldots\},$$

$$\{\ldots - 7, -3, 1, 5, 9, \ldots\},$$

$$\{\ldots - 6, -2, 2, 6, 10, \ldots\},$$

$$\{\ldots - 5, -1, 3, 7, 11, \ldots\}.$$

To say that this is a partition of $\mathbb{Z}$ means that every integer is in exactly one of these sets.

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

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

Relative to congruence mod n, there are n equivalence classes: The class containing 0, the class containing 1, ..., the class containing $n-1$. As usual, I'll abuse notation and denote the equivalence classes by 0, 1, ..., $n-1$. Then $\mathbb{Z}_n$ is the set of these n equivalence classes.

Addition mod n gives a binary operation on $\mathbb{Z}_n$. It is associative, and the identity is 0. If $0 \le k < n$, then the inverse of k is $-k = n - k$.

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

I'll take the axioms for granted right now; later, they will follow from the construction of $\mathbb{Z}_n$ as a **quotient group** of $\mathbb{Z}$. □

Example. Find the order of 6 in $\mathbb{Z}_{10}$.

$$\mathbb{Z}_{10} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}.$$

The operation is addition and the identity is 0. To find the order of an element, I find the first positive *multiple* which equals 0.

Thus, 6 has order 5, because

$$1 \cdot 6 = 6 \ne 0, \quad 2 \cdot 6 = 2 \ne 0, \quad 3 \cdot 6 = 8 \ne 0, \quad 4 \cdot 6 = 4 \ne 0, \quad \text{but} \quad 5 \cdot 6 = 0.$$

Example. (**Guessing an identity and inverses**) Define an operation $*$ on the real numbers by

$$a * b = a + b + 2 \quad \text{for all} \quad a, b \in \mathbb{R}.$$

Does this give a group structure on $\mathbb{R}$?

$*$ takes two real numbers and produces a real number, so $*$ is a binary operation on $\mathbb{R}$.

Next, I'll check associativity. Let $a, b, c \in \mathbb{R}$. Then

$$(a * b) * c) = (a + b + 2) * c = (a + b + 2) + c + 2 = a + b + c + 4,$$

$$a * (b * c) = a * (b + c + 2) = a + (b + c + 2) + 2 = a + b + c + 4.$$

Thus, $(a * b) * c) = a * (b * c)$, so $*$ is associative.

Next, I have to determine whether there is an identity for $*$. First, I'll work backwards to *guess* what the identity should be. *This is not a proof!* Once I have my guess, I'll *confirm* my guess (if possible).

Suppose e is the identity. Then in particular, $e * 3 = 3$ (I picked 3 at random). This means that $e + 3 + 2 = 3$, or $e = -2$.

My guess is that the identity is -2. To see if it works, let $a \in \mathbb{R}$. Then

$$a * (-2) = a + (-2) + 2 = a, \quad (-2) * a = (-2) + a + 2 = a.$$

This proves that -2 is the identity for $*$.

Finally, I want to show that every element has an inverse. Since -2 is the identity, this means that for every element a, I must find an element a^{-1} such that $a * a^{-1} = -2$ and $a^{-1} * a = -2$.

As I did in the identity step, I'll *guess* a^{-1} by working backwards, then confirm my guess. Since I want a *formula* for a^{-1} in terms of a, I'll work with an arbitrary $a \in \mathbb{R}$ — in contrast to picking a random element of $\mathbb{R}$, as I did to find the identity.

Start with $a * a^{-1} = -2$. This means that $a + a^{-1} + 2 = -2$, so $a^{-1} = -4 - a$.

(Be sure you understand why I'm not finished yet! Finding $a^{-1} = -4 - a$ *does not prove that inverses exist*. Think about the reasoning: I started with $a * a^{-1} = -2$, which *assumes* that a^{-1} is defined. I need to *confirm* that $-4 - a$ is the inverse of a under $*$, which I do by direct computation.)

I have

$$a * (-4 - a) = a + (-4 - a) + 2 = -2 \quad \text{and} \quad (-4 - a) * a = (-4 - a) + a + 2 = -2.$$

Therefore, $-4 - a$ is the inverse of a.

I've verified all the axioms, so $\mathbb{R}$ is a group under the operation $*$. $\square$

Example. (**A left identity and right inverses**) 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.)

Show that the operation is associative, has a left identity but not a right identity, and has right inverses but not left inverses. If a and b are nonzero real numbers, so is $a \cdot b = |a| b$. Therefore, the set is closed under the operation.

Let $a, b, c \in \mathbb{R}^*$. Then

$$(a \cdot b) \cdot c = (|a| b) \cdot c = ||a| b| c = |a||b| c, \qquad \text{while} \qquad a \cdot (b \cdot c) = a \cdot (|b| c) = |a||b| c.$$

Therefore, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$, and $\cdot$ is associative.

1 is a **left identity**, in the sense that $1 \cdot a = a$ for all $a \in \mathbb{R}^*$. But (for example)

$$(-3) \cdot 1 = |-3| 1 = 3, \qquad \text{so} \qquad (-3) \cdot 1 \neq -3.$$

In other words, 1 is not a two-sided identity, as required by the group definition.

There are also **right inverses**: $a \cdot \dfrac{1}{|a|} = 1$ for all $a \in \mathbb{R}^*$. But (for instance) there is no $x \in \mathbb{R}^*$ such that $x \cdot (-3) = 1$, since

$$x \cdot (-3) = |x|(-3) \le 0 \quad \text{for all} \quad x.$$

$\mathbb{R}^*$ with $\cdot$ is not a group. This example shows why you have to be careful to check the identity and inverse properties on "both sides" (unless you know the operation is commutative).

Note: It *is* true that if an associative operation has a **left identity** and every element has a **left inverse**, then the set is a group. □

Example. (**A group which is a subset of the integers**) Let

$$G = \{8a + 14b \mid a, b \in \mathbb{Z}\}.$$

Is G a group under integer addition? (Assume that integer addition is associative.)

First, I'll check whether integer addition actually gives a binary operation on G. To do this, I need to check whether the set is closed under the operation. I'll take two arbitrary elements of G, add them, and see if the sum is an element of G.

Let $8a + 14b, 8a' + 14b' \in G$. Then

$$(8a + 14b) + (8a' + 14b') = 8(a + a') + 14(b + b') \in G.$$

To show that the sum is in G, I have to write it in the form of a typical element of G, namely

$$8(\text{stuff}) + 14(\text{junk}).$$

Note that I didn't pick two *specific* elements of G (like "22" and "0"): I used two *general* elements.

I also didn't use "$8a + 14b$" and "$8a + 14b$", since that would be using the same element twice.

Now I know that addition gives a binary operation on G.

I'm assuming that addition is associative.

Next, I must show that G has an identity element. 0 is an identity element for addition of integers, so it will work for elements of G:

$$0 + (8a + 14b) = 8a + 14b, \quad (8a + 14b) + 0 = 8a + 14b.$$

However, I also have to show that 0 is in G! To do this, write it as $8(\text{stuff}) + 14(\text{junk})$:

$$0 = 8 \cdot 0 + 14 \cdot 0 \in G.$$

Therefore, 0 is the identity element of G.

Finally, let $8a + 14b \in G$. I must show that it has an inverse under addition. The ordinary additive inverse works:

$$(8a + 14) + (-8a - 14b) = 0, \quad (-8a - 14b) + (8a + 14b) = 0.$$

However, as with the identity 0, I have to show that $-8a - 14b$ is in G. To do this, just rewrite it so it has the correct form:

$$-8a - 14b = 8(-a) + 14(-b) \in G.$$

This shows that every element of G has an inverse.

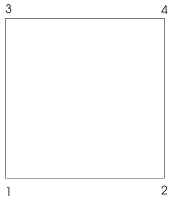
Therefore, G is a group. □

Example. (**Symmetry groups**) 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 preserves 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.)

Construct D_4, the dihedral group of order 8 (the group of symmetrices of a square).

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



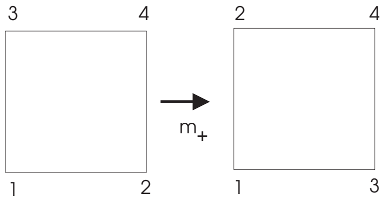
Consider vertex 1. A rigid motion can map it to any of the 4 vertices. Once I know where 1 goes, 3 must go to the vertex opposite it, since distance are preserved. Now there are only two possibilities for vertices 2 and 4. All together, I have $4 \cdot 2 = 8$ choices, so there at most 8 symmetries. I'll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

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

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_+:

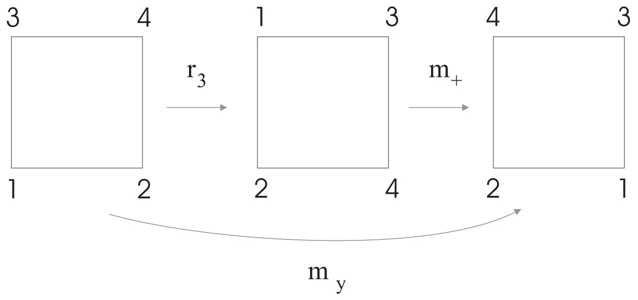


The operation on D_4 is function composition — do one rigid motion after another. It's clear that this is a binary operation, but I need to establish a convention concerning how I will write the operation. I will write

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

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.

From the table, it is apparent that D_4 is *not* abelian. For example, $m_+ r_3 = m_y$, but $r_3 m_+ = m_x$. □

The next proposition contains the result I mentioned about rows and columns of finite group tables.

Proposition. In a finite group operation table, each row or column contains each element of the group exactly once.

Proof. 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}:

$$\begin{aligned} a^{-1} \cdot ab &= a^{-1} \cdot ac \\ b &= c \end{aligned}$$

That is, the b and c-columns are actually the same column. 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. □

Example. (**Products of groups**) Consider the following set:

$$\mathbb{Z}^2 = \mathbb{Z} \times \mathbb{Z} = \{(a, b) \mid a, b \in \mathbb{Z}\}.$$

Is this a group under componentwise-addition ("vector addition")?
What about componentwise-multiplication?

$\mathbb{Z} \times \mathbb{Z}$ is a group under componentwise-addition. This is really just addition of two-dimensional (integer) vectors: For example,

$$(3, -8) + (10, 15) = (3 + 10, -8 + 15) = (13, 7).$$

It's associative, the identity is $(0, 0)$, and the inverse of (a, b) is $-(a, b) = (-a, -b)$.

$\mathbb{Z} \times \mathbb{Z}$ is not a group under componentwise-multiplication. Here the operation would look like this:

$$(3, -8) \cdot (10, 15) = (3 \cdot 10, (-8) \cdot 15) = (30, -120).$$

It's associative, and the identity is $(1, 1)$. However, many pairs don't have multiplicative inverses. For example, suppose

$$(3, 0) \cdot (a, b) = (1, 1).$$

Then

$$3a = 1 \quad \text{and} \quad 0 \cdot b = 1.$$

The first equation has no integer solutions, and the second says "$0 = 1$", so I have two contradictions!

□

Notes: If you use the notation "$\mathbb{Z}^2$" for this group, don't confuse it with "$\mathbb{Z}_2$".

You can replace $\mathbb{Z}$ with $\mathbb{Q}$ or $\mathbb{R}$ or $\mathbb{C}$. Thus, $\mathbb{Q} \times \mathbb{Q}$, $\mathbb{R} \times \mathbb{R}$, and $\mathbb{C} \times \mathbb{C}$ are all groups under componentwise-addition (and not under componentwise-multiplication). And you can extend this to more than two factors: For example $\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$ is a group under componentwise-addition.

Example. (**Matrix groups**) Consider the following sets:

$M(n, \mathbb{R})$ - $n \times n$ matrices with real entries

$GL(n, \mathbb{R})$ - $n \times n$ invertible matrices with real entries

Are these groups under matrix addition? Matrix multiplication?

$M(n, \mathbb{R})$ is a group under matrix addition. Matrix addition is associative. The identity for addition is the $n \times n$ zero matrix:

$$\begin{bmatrix} 0 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 0 \end{bmatrix}$$

The inverse of a matrix A is its negative $-A$ (negate all the entries of A).

$M(n, \mathbb{R})$ is not a group under matrix multiplication. Matrix multiplication is associative, and the identity is the $n \times n$ identity matrix:

$$\begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 1 \end{bmatrix}$$

But many matrices don't have inverses under multiplication — for example, the zero matrix above.

With $GL(n, \mathbb{R})$, the situation is reversed. $GL(n, \mathbb{R})$ is a group under matrix multiplication. Matrix multiplication is associative, and the identity is the $n \times n$ identity matrix.

By definition, $GL(n, \mathbb{R})$ consists of invertible matrices, so every element has a multiplicative inverse.

You should know from linear algebra that *matrix multiplication is not commutative*. Thus, $GL(n, \mathbb{R})$ is not an abelian group. (Can you give a particular example of noncommuting 2×2 matrices?)

However, $GL(n, \mathbb{R})$ is not a group under matrix addition. In fact, you can add two invertible matrices and get a non-invertible matrix; for example,

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} + \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}.$$

Thus, addition of matrices is not a binary operation on $GL(n, \mathbb{R})$. □

Note: You can replace "$\mathbb{R}$" in this example with $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{C}$ — in fact, you can even use the integers mod n like $\mathbb{Z}_5$. In the case of $\mathbb{Z}_5$, you add and multiply elements of $\mathbb{Z}_5$ mod 5. And more generally, you can replace "$\mathbb{R}$" with any **commutative ring with identity** (I'll discuss rings later).

Example. (**Groups of order 2**) Suppose G is a group of order 2: $|G| = 2$. Construct the multiplication table for G.

Since G has two elements, $G = \{1, a\}$, where 1 is the identity and $a \neq 1$ is another element. a must have an inverse; since $a \cdot 1 = a$, the inverse of a is not 1. Therefore, the inverse of a is a, and $a \cdot a = 1$. The multiplication table for G looks like this:

$\cdot$	1	a
1	1	a
a	a	1

This group is called $\mathbb{Z}_2$, the cyclic group of order 2. Here is another table for the same group:

+	0	1
0	0	1
1	1	0

In this case, I think of $\mathbb{Z}_2$ as the set $\{0, 1\}$, with addition mod 2.

What do I mean when I say that they're "the same group"?

I mean that I can get the second table from the first this way:

$$1 \to 0, a \to 1, b \to 2.$$

This is an example of an **isomorphism** — a function which "matches up" elements of one group with another, so the group table is preserved. (I'll make this more precise later.) Isomorphic groups are *the same* as groups. In this sense, $\mathbb{Z}_2$ is *the only* group of order 2. □

Example. (**Groups of order 3**) Suppose that G is a group and $|G| = 3$. Construct the multiplication table for G.

Let $G = \{1, a, b\}$, where 1, a, and b are different elements.

If $aa = a$, then $aaa^{-1} = aa^{-1} = 1$, or $a = 1$, contradicting the fact that a and 1 were distinct elements. If $aa = 1$, then $ab = b$ (because $ab = a$ gives $aab = aa = 1$, or $b = 1$, contradicting the fact that b and 1 were distinct elements). But then $abb^{-1} = bb^{-1} = 1$, so $a = 1$, the same contradiction as before. Hence, $aa = b$. Using the principle that each row or column of a multiplication table contains each element exactly once, I can fill in the rest of the table:

$\cdot$	1	a	b
1	1	a	b
a	a	b	1
b	b	1	a

This is $\mathbb{Z}_3$, the cyclic group of order 3. Here is another table for the same group:

$+$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

These two tables give groups which are isomorphic. Up to isomorphism, there is only one group of order 3, namely $\mathbb{Z}_3$.

There are two groups of order 4, one group of order 5, two groups of order 6, and one group of order 7. No one knows a practical formula for determining how many groups of order n there are. And the method of the preceding examples — essentially, trial and error — is untenable once n gets large. □