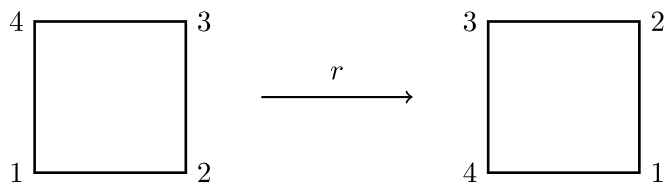
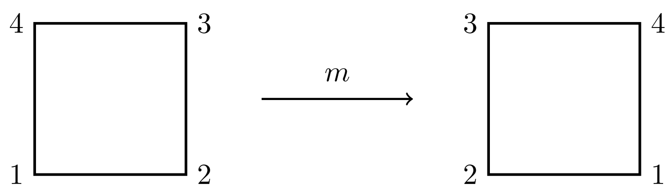
Math 31 - Homework 3 Solutions

1. Let D_4 be the 4th dihedral group, which consists of symmetries of the square. Let $r \in D_4$ denote counterclockwise rotation by $90°$, and let m denote reflection across the vertical axis.



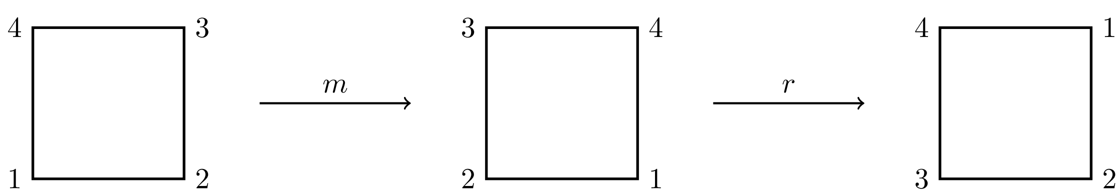


Check that

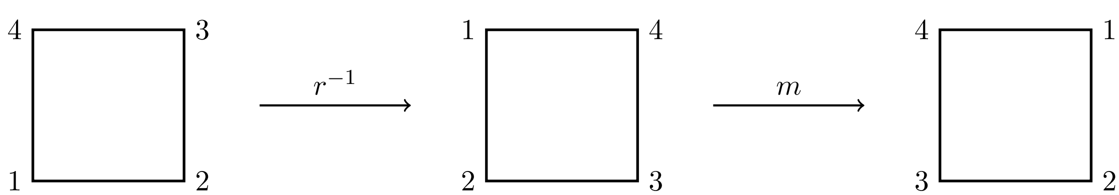
$$rm = mr^{-1}.$$

Conclude that D_4 is a nonabelian group of order 8.

Solution. It is probably simplest to just draw pictures that illustrate the effect of rm and mr^{-1} on the square. First we have:



Thus rm corresponds to reflection across the diagonal through vertices 2 and 4. On the other hand:



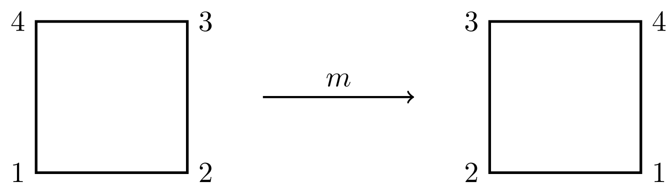
Thus mr^{-1} is the same transformation, and we have shown that $rm = mr^{-1}$. In particular, r and m do not commute, so D_4 is nonabelian. We already saw in class that D_4 is a group and that its order is $2 \cdot 4 = 8$.

2. We mentioned in class that elements of D_n can be thought of as permutations of the vertices of the regular n-gon. For example, the rotation r of the square mentioned in the last problem can be identified with the permutation

$$\rho = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}.$$

Write the reflection m as a permutation $\mu \in S_4$, and compute the product $\rho\mu$ in S_4. Then compute $rm \in D_4$, and write it as a permutation σ. Check that $\sigma = \rho\mu$. (In other words, this identification of symmetries of the square with permutations respects the group operations.)

Solution. In the previous problem we saw that m is given by



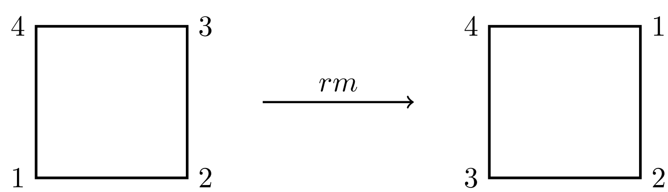
Thus the permutation μ will have to send 1 to 2, 2 to 1, 3 to 4, and 4 to 3. In other words,

$$\mu = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}.$$

As elements of S_4 we then have

$$\rho\mu = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}.$$

Now recall from Problem 2 that if we multiply r and m in D_4, we obtain the reflection across the diagonal through vertices 2 and 4:



The permutation σ corresponding to this transformation will have to send 1 to 3 and leave 2 and 4 unchanged. In other words,

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}.$$

This is precisely the permutation $\rho\mu$, so indeed $\sigma = \rho\mu$. We will see later that we can identify D_4 with a proper subgroup of S_4, and that this identification preserves the group operations. This exercise is a specific example of this phenomenon.

3. Recall that if $*$ is a binary operation on a set S, an element x of S is an **idempotent** if $x * x = x$. Prove that a group has exactly one idempotent element.

Proof. Let G be a group and suppose that $a \in G$ is an idempotent. Then

$$a^2 = a = ae,$$

and the left cancellation law implies that

$$a = e.$$

Therefore, the only idempotent in G is the identity element e, and G has exactly one idempotent. $\square$

4. Consider the group $\langle \mathbb{Z}_{30}, +_{30} \rangle$ under addition.

(a) Find the orders of the elements 3, 4, 6, 7, and 18 in $\mathbb{Z}_{30}$.

(b) Find all the generators of $\langle \mathbb{Z}_{30}, +_{30} \rangle$.

Solution. (a) We saw in class that if $a \in \mathbb{Z}_{30}$, then $o(a) = 30/\gcd(a, 30)$. Therefore,

$$\begin{aligned} o(3) &= 30/3 = 10 \\ o(4) &= 30/2 = 15 \\ o(6) &= 30/6 = 5 \\ o(7) &= 30/1 = 30 \\ o(18) &= 30/6 = 5 \end{aligned}$$

(b) The generators of $\mathbb{Z}_{30}$ are precisely the elements of order 30. These are exactly the elements $a \in \mathbb{Z}_{30}$ for which $\gcd(a, 30) = 1$. Therefore, the generators are

$$1, 7, 11, 13, 17, 19, 23, \text{ and } 29.$$

6. [Saracino, Section 4, #25] Show that if G is a finite group and $|G|$ is even, then there is an element $a \in G$ such that $a \neq e$ and $a^2 = e$.

Proof. Define $S \subseteq G$ by

$$S = \left\{ a \in G : a \neq a^{-1} \right\}.$$

Note that S is a *proper* subset of G, since $e \notin S$. Since $(a^{-1})^{-1} = a$ for all $a \in G$, we can conclude that $a \in S$ if and only if $a^{-1} \in S$. Thus we can pair up the elements of S with their inverses:

$$S = \left\{ a_1, a_1^{-1}, a_2, a_2^{-1}, \ldots, a_n, a_n^{-1} \right\}.$$

We can then see that S has an even number of elements, say $2n$. If $|G| = 2m$, then $n < m$ and the number of elements $a \in G$ with the property that $a = a^{-1}$ is

$$2m - 2n = 2(m - n).$$

In particular, an even number of elements in G are equal to their own inverses. Since $e = e^{-1}$, there must be at least one other element $a \in G$ with $a = a^{-1}$. $\square$

7. [Saracino, Section 4, #21] Let a and b be elements of a group G. Show that if ab has finite order n, then ba also has order n.

Proof. Suppose that ab has order n, so that n is the smallest positive integer for which

$$(ab)^n = e.$$

Note that

$$(ab)^n = \underbrace{abab \cdots ab}_{n \text{ times}} = a(ba)^{n-1}b,$$

so

$$(ba)^{n-1} = a^{-1}(ab)^n b^{-1} = a^{-1}eb^{-1} = a^{-1}b^{-1} = (ba)^{-1}.$$

That is,

$$(ba)^n = (ba)(ba)^{n-1} = (ba)(ba)^{-1} = e.$$

Therefore, we know that $(ba)^n = e$, and we just need to see that n is the smallest such positive integer. Suppose that $0 < m < n$ and $(ba)^m = e$. Then the same computations that we have just done show that

$$(ab)^m = e,$$

which is impossible since $|ab| = n$. Therefore, n must be the smallest positive integer for which $(ba)^n = e$, i.e., $|ba| = n$. $\square$

8. [Saracino, Section 4, #20] Let G be a group and let $a \in G$. An element $b \in G$ is called a *conjugate* of a if there exists an element $x \in G$ such that $b = xax^{-1}$. Show that any conjugate of a has the same order as a.

Proof. Let $a, x \in G$, and put $b = xax^{-1}$. Suppose first that a has finite order n. Then

$$b^n = (xax^{-1})^n = \underbrace{(xax^{-1})(xax^{-1}) \cdots (xax^{-1})}_{n \text{ times}} = xa^n x^{-1} = xex^{-1} = xx^{-1} = e,$$

since a has order n. Thus $b^n = e$, so $o(b) \leq n = o(a)$. On the other hand, let $m = o(b)$. Note that $a = x^{-1}bx$, so

$$a^m = (x^{-1}bx)^m = x^{-1}b^m x = x^{-1}x = e.$$

Thus $o(a) \leq m = o(b)$. We must then have $o(a) = o(b)$.

Now suppose that a has infinite order. Then $a^n \neq e$ for all $n \in \mathbb{Z}$. Suppose that b does not have infinite order, so there is some integer m such that $b^m = e$. Then the computations above show that $a^m = e$ as well, contradicting the fact that a has infinite order. Therefore, b must also have infinite order. $\square$