Recall:

You found that there are 8 motions on the square that leave the square seemingly unmoved:

$$\{R_0, R_{90}, R_{180}, R_{270}, H, V, D, D'\}.$$

We called these motions the *symmetries of the square*.
Notation:

$$H \circ R_{90} \quad \Longleftrightarrow \quad \text{first rotating counter-clockwise by } 90^\circ$$
$$\text{then reflecting across a horizontal axis.}$$

The 8 motions on the square

$$\{R_0, R_{90}, R_{180}, R_{270}, H, D, V, D'\}$$

and the operation $\circ$ of combining the motions form a system called the **dihedral group of order 8**, denoted D_4.

The 8 motions on the square

$$\{R_0, R_{90}, R_{180}, R_{270}, H, D, V, D'\}$$

and the operation $\circ$ of combining the motions form a system called the **dihedral group of order 8**, denoted D_4.

Why is it called D_4?

1. $D \Longleftrightarrow$ **dihedral** (two faces): that means the square has not only rotations but also reflections.

The 8 motions on the square

$$\{R_0, R_{90}, R_{180}, R_{270}, H, D, V, D'\}$$

and the operation $\circ$ of combining the motions form a system called the **dihedral group of order 8**, denoted D_4.

Why is it called D_4?

1. $D \iff$ **dihedral** (two faces): that means the square has not only rotations but also reflections.
2. $4 \iff$ the number of rotations. The reason you only need the 4 is that if an object has any reflections (which would mean we're using the letter "D"), it has the same number of reflections as it does rotations.

The 8 motions on the square

$$\{R_0, R_{90}, R_{180}, R_{270}, H, D, V, D'\}$$

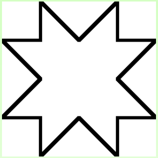
and the operation $\circ$ of combining the motions form a system called the **dihedral group of order 8**, denoted D_4.

Why is it called D_4?

1. $D \iff$ **dihedral** (two faces): that means the square has not only rotations but also reflections.
2. $4 \iff$ the number of rotations. The reason you only need the 4 is that if an object has any reflections (which would mean we're using the letter "D"), it has the same number of reflections as it does rotations.

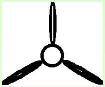
The set of symmetries of an equilateral triangle (3 rotations, 3 reflections) is called D_3, and in general, the set of symmetries of a regular n-gon (n rotations, n reflections) is called D_n.

Consider the following figure:

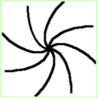


How can we move this and leave it (seemingly) unchanged?

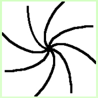
What sort of symmetries does this figure have?



What about this figure?

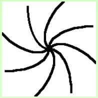


What about this figure?



This figure has no reflection symmetry.

What about this figure?



This figure has no reflection symmetry.

It does have 8 rotations: R_{45}, R_{90}, etc. We say this figure has symmetry group $< R_{45} >$.

Below is the *Cayley* table showing the result of applying the operation to any 2 elements.

$\circ$	R_0	R_{90}	R_{180}	R_{270}	H	D	V	D'
R_0	R_0	R_{90}	R_{180}	R_{270}	H	D	V	D'
R_{90}	R_{90}	R_{180}	R_{270}	R_0	D'	H	D	V
R_{180}	R_{180}	R_{270}	R_0	R_{90}	V	D'	H	D
R_{270}	R_{270}	R_0	R_{90}	R_{180}	D	V	D'	H
H	H	$\boxed{D^*}$	V	D'	R_0	R_{90}	R_{180}	R_{270}
D	D	V	D'	H	R_{270}	R_0	R_{90}	R_{180}
V	V	D'	H	D	R_{180}	R_{270}	R_0	R_{90}
D'	D'	H	D	V	R_{90}	R_{180}	R_{270}	R_0

* Remember that the D in row H and column R_{90} comes from $H \circ R_{90}$.

Properties of D_4 to focus on:

1. *Closure:* No new motions are introduced. If $A, B \in D_4$, then $A \circ B \in D_4$.
2. *Identity:* R_0 acts as an identity motion — $R_0 \circ A = A \circ R_0 = A$ for all $A \in D_4$.
3. *Inverses:* Every element has an inverse motion that "undoes" what the motion does. For example, $R_{90} \circ R_{270} = R_{270} \circ R_{90} = R_0$.
4. *Associativity:* $(A \circ B) \circ C = A \circ (B \circ C)$ for all $A, B, C \in D_4$.

A few examples of sets, *together with operations*, which are closed, associative, have an identity, and have all necessary inverses are:

- Integers ($\mathbb{Z}$) under $+$
- Rational numbers ($\mathbb{Q}$) under addition
- $\mathbb{Q}$ under multiplication is not a group, as 0 has no inverse –even though every other element does.
- The set of all invertible 2x2 matrices with real entries, under matrix multiplication.

Well Ordering Principle:

Every non-empty set of positive *integers* contains a smallest member.

Well Ordering Principle:

Every non-empty set of positive *integers* contains a smallest member.

Notice that this is **not** true for $\mathbb{R}$ or $\mathbb{Q}$, or even if we allow negative integers.

Well Ordering Principle:

Every non-empty set of positive *integers* contains a smallest member.

> **Notice** that this is **not** true for $\mathbb{R}$ or $\mathbb{Q}$, or even if we allow negative integers.

Examples:

1. $\{x \in \mathbb{Z}^+ | x \leq 200\}$ has a smallest element, by the well-ordering principle.
2. $\{x \in \mathbb{Q}^+ | x \leq 200\}$ doesn't have a smallest element. For any rational number between 0 and 200, you can always find another, smaller, one, by taking half of the one you have. It will of course still be rational.

Division Algorithm:

Let $a, b \in \mathbb{Z}$ where $b > 0$. Then there exist unique integers q, r such that

$$a = qb + r \qquad \text{with} \qquad 0 \leq r < b.$$

Division Algorithm:

Let $a, b \in \mathbb{Z}$ where $b > 0$. Then there exist unique integers q, r such that

$$a = qb + r \qquad \text{with} \qquad 0 \leq r < b.$$

i.e. Let $a, b \in \mathbb{Z}$, where $b > 0$. Then $\exists\,!\ q, r\ \in\ \mathbb{Z}\ \ni$

$$a = qb + r \qquad \text{with} \qquad 0 \leq r < b.$$

Division Algorithm:

Let $a, b \in \mathbb{Z}$ where $b > 0$. Then there exist unique integers q, r such that

$$a = qb + r \qquad \text{with} \qquad 0 \leq r < b.$$

i.e. Let $a, b \in \mathbb{Z}$, where $b > 0$. Then $\exists\ !\ q, r\ \in\ \mathbb{Z}\ \ni$

$$a = qb + r \qquad \text{with} \qquad 0 \leq r < b.$$

Examples:

If $a = 13$ *and* $b = 5$, *then* $a = 2b + 3$.

Remember, there's nothing in the statement of the division algorithm requiring that you choose a to be the larger of the two integers.

If $a = 5$ *and* $b = 13$, *then* $a = 0 \cdot 13 + 5$.

Theorem: (GCD is a Linear Combination)

For any non-zero $a, b \in \mathbb{Z}$, there exist s and t such that $gcd(a, b) = as + bt$. That is, the $gcd(a, b)$ is a linear combination of a and b. Moreover, $gcd(a, b)$ is the smallest positive integer of the form $as + bt$.

Theorem: (GCD is a Linear Combination)

For any non-zero $a, b \in \mathbb{Z}$, there exist s and t such that $gcd(a, b) = as + bt$. That is, the $gcd(a, b)$ is a linear combination of a and b. Moreover, $gcd(a, b)$ is the smallest positive integer of the form $as + bt$.

Outline of Proof:

1. Let $S = \{am + bn \mid m, n \in \mathbb{Z} \text{ and } am + bn > 0\}$. Show $S \neq \emptyset$.

Theorem: (GCD is a Linear Combination)

For any non-zero $a, b \in \mathbb{Z}$, there exist s and t such that $gcd(a, b) = as + bt$. That is, the $gcd(a, b)$ is a linear combination of a and b. Moreover, $gcd(a, b)$ is the smallest positive integer of the form $as + bt$.

Outline of Proof:

1. Let $S = \{am + bn \mid m, n \in \mathbb{Z} \text{ and } am + bn > 0\}$. Show $S \neq \emptyset$.

   NTS $gcd(a, b) \in S$.

Theorem: (GCD is a Linear Combination)

For any non-zero $a, b \in \mathbb{Z}$, there exist s and t such that $gcd(a, b) = as + bt$. That is, the $gcd(a, b)$ is a linear combination of a and b. Moreover, $gcd(a, b)$ is the smallest positive integer of the form $as + bt$.

Outline of Proof:

1. Let $S = \{am + bn \,|m, n \in \mathbb{Z} \text{ and } am + bn > 0\}$. Show $S \neq \emptyset$.

   NTS $gcd(a, b) \in S$.

2. Well-Ordering Principle $\Longrightarrow$ S has a smallest element.
   Let $d =$ smallest elt of S. Since $d \in S$, $\exists\ M,\ N \in \mathbb{Z} \ni d = aM + bN$.

Theorem: (GCD is a Linear Combination)

For any non-zero $a, b \in \mathbb{Z}$, there exist s and t such that $gcd(a, b) = as + bt$. That is, the $gcd(a, b)$ is a linear combination of a and b. Moreover, $gcd(a, b)$ is the smallest positive integer of the form $as + bt$.

Outline of Proof:

1. Let $S = \{am + bn \mid m, n \in \mathbb{Z} \text{ and } am + bn > 0\}$. Show $S \neq \emptyset$.

   NTS $gcd(a, b) \in S$.

2. Well-Ordering Principle $\Longrightarrow$ S has a smallest element.
   Let $d =$ smallest elt of S. Since $d \in S$, $\exists\ M,\ N \in \mathbb{Z} \ni d = aM + bN$.

3. Show $d|a$, $d|b$, so d is a common divisor of a and b.

Theorem: (GCD is a Linear Combination)

For any non-zero $a, b \in \mathbb{Z}$, there exist s and t such that $gcd(a, b) = as + bt$. That is, the $gcd(a, b)$ is a linear combination of a and b. Moreover, $gcd(a, b)$ is the smallest positive integer of the form $as + bt$.

Outline of Proof:

1. Let $S = \{am + bn \,|m, n \in \mathbb{Z} \text{ and } am + bn > 0\}$. Show $S \neq \emptyset$.

   NTS $gcd(a, b) \in S$.

2. Well-Ordering Principle $\Longrightarrow$ S has a smallest element.
   Let $d =$ smallest elt of S. Since $d \in S$, $\exists\ M,\ N \in \mathbb{Z} \ni d = aM + bN$.

3. Show $d|a$, $d|b$, so d is a common divisor of a and b.

4. Show $d = gcd(a, b)$, that is, d is the largest of all the common divisors.