Lecture 10: Groups

Contents

Group Theory is typically referred to as the mathematical study of symmetry. The puzzles we are studying have exhibited a remarkable amount of symmetry. In this lecture we begin our introduction into group theory by introducing the concept of a *group*. Though, from our experience in exploring puzzle and permutations we already have experience in working with groups. In later lectures, we will see that group theory is the tool required to understand permutation puzzles, in particular their *end-game*.

10.1 Group: Definition

Playing with permutation puzzles has already given us a working definition of a *group*. We have a set of move-sequences, call this set M. We are able to compose two move-sequences together to form a new move-sequence ($m_1, m_2 \in M \implies m_1 m_2 \in M$), there is a "do-nothing" move, and we can "undo" a move sequence (for $m_1 \in M$ there is an $m_1^{-1} \in M$). This is very similar to how permutations behave under composition. Each consist of a set, an operation to combine objects in the set, and a few properties this operation must possess. This is precisely what we will call a group.

Definition 10.1 (Group) *A **group** is a nonempty set G, together with an operation, which can be thought of as a function $* : G \times G \to G$, that assigns to each ordered pair (a, b) of elements in G and element $a * b \in G$, that satisfies the following properties:*

1. Associativity*: The operation is associative: $(a * b) * c = a * (b * c)$ for all $a, b, c \in G$.*
2. Identity*: There is an element e (called the identity) in G, such that $a * e = e * a = a$ for all $a \in G$.*
3. Inverses*: For each element $a \in G$, there is an element b in G (called the inverse of a) such that $a * b = b * a = e$.*

Typically we drop the notation * for the operation and just write the operation by juxtaposition, that is, we simply write $a * b$ as ab. We've already been doing this with permutation composition, and the composition of puzzle moves. In the case were the group operation is addition, then we will use the symbol "+".

Definition 10.2 (Order of a Group) *The number of elements of a group (finite of infinite) is called the **order** of the group. We will use $|G|$ to denote the order of the group, since this is really just the cardinality of the set.*

The power of mathematics resides in abstraction. Mathematicians look for the similarities between objects, then articulate and abstract these similarities. They generally work with these abstract conceptualizations, since as a result, their discoveries hold for *all* objects satisfying the properties of the abstraction.

Consider an analogy from biology. Biologists consider the similarities between spiders, scorpions, harvestmen, ticks, and mites, to be significant enough that they talk about them as being from the same "family": the Arachnid family. Arachnids are a class of joint-legged invertebrate animals, all of which have eight legs. There are over 100,000 named species, five of which we named above. In this sense, a biologist who studies the (abstract) family Arachnida is in effect studying over 100,000 named species, simultaneously.

Looking back at the definition of a group, in particular at the property "inverses", we see that nowhere did it say the inverse has to be unique. However, in our examples of puzzle movements, and permutations, inverses were unique. Should we have added this as a property? Well, it turns out that we don't need to since it is a direct consequence of the properties in the definition. We'll state this as a theorem.

Theorem 10.1 (Uniqueness of Inverses) *For each element a in a group G, there is a unique element $b \in G$ such that $ab = ba = e$.*

Proof: Suppose b and c are both inverses of a. Then, on one hand, we have

$$\begin{aligned} b(ab) &= be && \text{since } ab = e \text{ (property 3)} \\ &= b && \text{since } be = b \text{ (property 2)} \end{aligned}$$

However, on the other hand, since $ab = e = ac$, we have

$$\begin{aligned} b(ab) &= b(ac) \\ &= (ba)c && \text{by associativity (property 1)} \\ &= ec && \text{since } ba = e \text{ (property 3)} \\ &= c. && \text{since } ec = c \text{ (property 2)} \end{aligned}$$

Therefore $b = c$, so inverses are unique. □

Since inverses are unique we can unambiguously denote the inverse of $a \in G$ by a^{-1}.

Previously we observed that permutations under composition satisfied the cancellation property. This is true of any group.

Theorem 10.2 (Cancellation Property) *In a group G, the right- and left- cancellation properties hold: $ba = ca$ implies $b = c$, and $ab = ac$ implies $b = c$.*

Proof: If $ba = ca$ then $(ba)a^{-1} = (ca)a^{-1}$ and by associativity, $b(aa^{-1}) = c(aa^{-1})$. Since $aa^{-1} = e$, then $be = ce$ from which it follows that $b = c$. Left cancellation can be proved in a similar manner. □

10.1.1 Multiplication (Cayley) Table

Since a group is merely a set with a way to combine elements (a sort-of *multiplication*), we can give the operation in terms of a table, provided the set is finite.

The **multiplication table**[1] of a (finite) group G is a tabulation of the values of the operation $*$. Let $G = \{g_1, ..., g_n\}$. The multiplication table of G is:

$*$	g_1	g_2	$\cdots$	g_j	$\cdots$	g_n
g_1						
g_2						
$\vdots$						
g_i				$g_i * g_j$		
$\vdots$						
g_n						

This says the entry of the table on row g_i and column g_j is the element $g_i * g_j$.

This table must satisfy some basic properties, which are immediate consequences of the definition of a group:

Lemma 10.1 *(a) Each element $g_k \in G$ occurs exactly once in each row of the table.*

(b) Each element $g_k \in G$ occurs exactly once in each column of the table.

(c) If the $(i, j)^{th}$ entry of the table is equal to the $(j, i)^{th}$ entry then $g_i * g_j = g_j * g_i$.

(d) If the table is symmetric about the diagonal then $g * h = h * g$ for all $g, h \in G$. (In this case, we call G abelian.)

[1] Also known as a *Cayley table*, after noted English mathematician Arthur Cayley (1821-1895)

The proof is left to the reader as Exercise 29.

In the next section we give a number of examples of groups, most of which should already be familiar to the reader. It is interesting to note that we have just proven, for those examples, and any other example we encounter during the rest of our lives, if the set satisfies the properties of a group then (i) inverses are unique, and (ii) the cancellation property holds. This is the power of abstraction!

10.2 Some Everyday Examples of Groups

Now that we have a formal description of a group, our first job is to notice we already know many examples.

(1) The set of integers $\mathbb{Z}$, the set of rational numbers $\mathbb{Q}$, and the set of real numbers $\mathbb{R}$, are all groups under ordinary addition. The identity is 0 in each case, and the inverse of a is its negative, $-a$.

(2) The set of non-zero rational numbers $\mathbb{Q}^* = \{r \in \mathbb{Q} \mid r \neq 0\}$ is a group under ordinary multiplication. The identity is 1, and the inverse of r is $1/r$.

Similarly, the set of non-zero real numbers $\mathbb{R}^* = \{r \in \mathbb{R} \mid r \neq 0\}$ is a group under ordinary multiplication. The identity is 1, and the inverse of r is $1/r$.

Note, that we had to leave out 0, since it doesn't have a multiplicative inverse, i.e. there is no rational number r such that $r \cdot 0 = 1$. In other words, $\mathbb{Q}$ is not a group under multiplication.

The set of non-zero integers $\mathbb{Z}^* = \{n \in \mathbb{Z} \mid n \neq 0\}$ is *not* a group under ordinary multiplication, since it is not closed under taking inverses. For example, the inverse of 2 is $\frac{1}{2}$, but $\frac{1}{2}$ is not in $\mathbb{Z}^*$.

(3) The set $\mathbb{R}^3 = \{(a_1, a_2, a_3) \mid a_1, a_2, a_3 \in \mathbb{R}\}$ is a group under componentwise addition:

$$(a_1, a_2, a_3) + (b_1, b_2, b_3) = (a_1 + b_1, a_2 + b_2, a_3 + b_3).$$

The identity is $(0, 0, 0)$ and the inverse of (a_1, a_2, a_3) is $(-a_1, -a_2, -a_3)$.

In general, the set of all n-tuples of real numbers $\mathbb{R}^n = \{(a_1, a_2, \ldots, a_n) \mid a_1, a_2, \ldots, a_n \in \mathbb{R}\}$ is a group under componentwise addition:

$$(a_1, a_2, a_3, \ldots, a_n) + (b_1, b_2, b_3, \ldots, b_n) = (a_1 + b_1, a_2 + b_2, a_3 + b_3, \ldots, a_n + b_n).$$

The identity is $(0, 0, 0, \ldots, 0)$.

(4) A rectangular array of the form $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$, where $a, b, c, d \in \mathbb{R}$, is called a 2×2 (real) matrix. The set of all 2×2 matrices is denoted by $M_{2,2}(\mathbb{R})$:

$$M_{2,2}(\mathbb{R}) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \mid a, b, c, d \in \mathbb{R} \right\}.$$

If we define the addition of two matrices to be componentwise:

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} + \begin{bmatrix} w & x \\ y & z \end{bmatrix} = \begin{bmatrix} a+w & b+x \\ c+y & d+z \end{bmatrix},$$

then $M_{2,2}(\mathbb{R})$ is a group under this addition. The identity is $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$ and the inverse of $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ is $\begin{bmatrix} -a & -b \\ -c & -d \end{bmatrix}$.

In general, for positive integers n and m, the set of all matrices with n rows and m columns, the so-called $n \times m$ matrices, $M_{n\times m}(\mathbb{R})$ is a group under componentwise addition.

$$M_{n,m}(\mathbb{R}) = \left\{ \begin{bmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,m} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,m} \\ a_{n,1} & a_{n,2} & \cdots & a_{n,m} \end{bmatrix} \mid a_{i,j} \in \mathbb{R} \right\}.$$

(5) **General Linear Group.** The *determinant* of a 2×2 matrix $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ is the number $\det(A) = ad - bc$. The set of all 2×2 matrices with non-zero determinant,

$$GL(2, \mathbb{R}) = \{A \in M_{2,2}(\mathbb{R}) \mid \det(A) \neq 0\}.$$

under matrix multiplication:

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} w & x \\ y & z \end{bmatrix} = \begin{bmatrix} aw + by & ax + bz \\ cw + dy & cx + dz \end{bmatrix}$$

is a group. The identity is $I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, and the inverse of $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ is $\begin{bmatrix} \frac{d}{ad-bc} & \frac{-b}{ad-bc} \\ \frac{-c}{ad-bc} & \frac{a}{ad-bc} \end{bmatrix}$.

In general, the set of invertible $n \times n$ matrices $GL(n, \mathbb{R})$, under matrix multiplication, is a group. It is called the *general linear group of* $n \times n$ *matrices over* $\mathbb{R}$. This follows from the properties that $\det(AB) = \det(A)\det(B)$ and A is invertible if and only if $\det(A) \neq 0$. These statements are proved in any elementary course in linear algebra.

(6) **Special Linear Group.** The set of $n \times n$ matrices with determinant 1 is a group under matrix multiplication. This group is denoted by $SL(n, \mathbb{R})$ and is called the *special linear group of* $n \times n$ *matrices over* $\mathbb{R}$.

$$SL(n, \mathbb{R}) = \{A \in GL(n, \mathbb{R}) \mid \det(A) = 1\}.$$

To see why it is closed under multiplication, suppose $A, B \in SL(n, \mathbb{R})$. Then $\det(A) = 1$ and $\det(B) = 1$, but then $\det(AB) = \det(A)\det(B) = 1 \cdot 1 = 1$, by the property of determinants. Therefore, $AB \in SL(n, \mathbb{R})$. Moreover, since $\det(A^{-1}) = \frac{1}{\det(A)} = \frac{1}{1} = 1$ then $A^{-1} \in SL(n.\mathbb{R})$.

(7) **Differentiable functions.** The set of all differentiable functions $\mathbb{R} \to \mathbb{R}$ is a group under the operation of addition: $(f + g)(x) = f(x) + g(x)$. The reason that the sum of two differentiable functions is differentiable follows from the fact that $\frac{d}{dx}(f + g) = \frac{d}{dx}f + \frac{d}{dx}g$. The reason the (additive) inverse of f is differentiable follows from the fact that $\frac{d}{dx}(-f) = -\frac{d}{dx}f$.

(8) **Translations.** For each $(a, b) \in \mathbb{R}^2$, define $T_{a,b} : \mathbb{R}^2 \to \mathbb{R}^2$ by

$$(x, y) \mapsto (x + a, y + b).$$

The set of all such functions $T_{a,b}$:

$$\mathcal{T}(\mathbb{R}^2) = \{T_{a,b} \mid a, b \in \mathbb{R}\}$$

is a group under function composition. To see this, notice that

$$(T_{a,b} \circ T_{c,d})(x, y) = T_{a,b}(T_{c,d}(x, y)) = T_{a,b}(x + c, y + d) = (x + a + c, y + b + d) = T_{a+c,b+d}(x + y)$$

for all $(a, y) \in \mathbb{R}^2$. Therefore, $T_{a,b} \circ T_{c,d} = T_{a+c,b+d}$, so $\mathcal{T}(\mathbb{R}^2)$ is closed under composition. Moreover, $T_{0,0}$ is the identity, and the inverse of $T_{a,b}$ is $T_{-a,-b}$. Function composition is always associative. The elements in $\mathcal{T}(\mathbb{R}^2)$ are called *translations* of $\mathbb{R}^2$.

Similarly we could define the group of translations of $\mathbb{R}^n$, for any positive integer n, as

$$\mathcal{T}(\mathbb{R}^n) = \{T_{a_1,\ldots,a_n} : \mathbb{R}^n \to \mathbb{R}^n \mid a_i \in \mathbb{R}\}$$

where $T_{a_1,\ldots,a_n}(x_1, \ldots, x_n) = (x_1 + a_1, \ldots, x_n + a_n)$.

(9) **Linear Transformations.** A *linear transformation* of $\mathbb{R}^n$ is a function $T : \mathbb{R}^n \to \mathbb{R}^n$ such that $T(a\vec{v}+\vec{w}) = aT(\vec{v})+T(\vec{w})$ for all $\vec{v}, \vec{w} \in \mathbb{R}^n$ and $a \in \mathbb{R}$. The set of all linear transformations $L(\mathbb{R}^n)$ of $\mathbb{R}^n$, for a positive integer n:

$$L(\mathbb{R}^n) = \{T : \mathbb{R}^n \to \mathbb{R}^n \mid T \text{ is a linear transformation}\}$$

is a group under function addition: for $T, U \in L(\mathbb{R}^n)$ define $T + U$ by

$$(T + U)(\vec{v}) = T(\vec{v}) + U(\vec{v}).$$

To see why, first we note that $T + U$ is a linear transformation since

$$\begin{aligned}(T + U)(a\vec{v} + \vec{w}) &= T(a\vec{v} + \vec{w}) + U(a\vec{v} + \vec{w}) = aT(\vec{v}) + T(\vec{w}) + aU(\vec{v}) + U(\vec{w}) \\ &= a(T(\vec{v}) + U(\vec{v})) + (T(\vec{w} + U(\vec{w})) \\ &= a(T + U)(\vec{v}) + (T + U)(\vec{w}).\end{aligned}$$

So $L(\mathbb{R}^n)$ is closed under addition. Moreover, the linear transformation $\vec{v} \mapsto \vec{0}$ is the identity, and for any T the inverse is $-T$. Since addition in $\mathbb{R}$ is associative, so is addition in $L(\mathbb{R}^n)$.

Some of the previous examples have the property that the group operation is commutative, that is $ab = ba$ for all $a, b \in G$. Groups with this property are called **abelian**. Named after Niel Abel, a noted Norwegian mathematician who studied such groups in the 1820's. Groups where there exist elements that do not commute are called **non-abelian**.

10.3 Further Examples of Groups

Now we'll present a few more examples of groups. These are the examples that will be important to us in this course, since we will use them quite frequently.

10.3.1 Symmetric and Alternating Groups

A *permutation* of a set X is a bijection $X \to X$. The set of *all* permutations of a set X, is a group under composition. This set is denoted by S_X and called it the **symmetric group of X**.

$$S_X = \{\alpha : X \to X \quad | \ \alpha \text{ is a bijection}\}.$$

In the case where X is the set $\mathbb{Z}_n = \{1, 2, 3, \ldots, n\}$ then we denoted $S_{\mathbb{Z}_n}$ simply by S_n, and called it the *symmetric group of degree* n.

The set of even permutations A_n in S_n is a also a group. Since it is a subset of S_n we call it a *subgroup* of S_n.

For example, consider A_4: the set of even permutations of degree 4. We know $|A_4| = \frac{4!}{2} = 12$ and we can list all the permutations in A_4 as follows:

$\varepsilon = (1)$, $\sigma_1 = (1,2)(3,4)$, $\sigma_2 = (1,3)(2,4)$, $\sigma_3 = (1,4)(2,3)$, $\sigma_4 = (1,2,3)$, $\sigma_5 = (1,3,2)$, $\sigma_6 = (1,2,4)$, $\sigma_7 = (1,4,2)$, $\sigma_8 = (1,3,4)$, $\sigma_9 = (1,4,3)$, $\sigma_{10} = (2,3,4)$, $\sigma_{11} = (2,4,3)$.

We can compute all possible products of two elements of the group and tabulate them in a multiplication table. This table contains all the information of the group A_4. For example, the inverse of σ_6 is σ_7 since ε appears as table entry $\sigma_6\sigma_7$. Also, A_4 is not abelian, since the table is not symmetric about the diagonal line.

	ε	σ_1	σ_2	σ_3	σ_4	σ_5	σ_6	σ_7	σ_8	σ_9	σ_{10}	σ_{11}
ε	ε	σ_1	σ_2	σ_3	σ_4	σ_5	σ_6	σ_7	σ_8	σ_9	σ_{10}	σ_{11}
$(1,2)(3,4) = \sigma_1$	σ_1	ε	σ_3	σ_2	σ_8	σ_{10}	σ_9	σ_{11}	σ_4	σ_6	σ_5	σ_7
$(1,3)(2,4) = \sigma_2$	σ_2	σ_3	ε	σ_1	σ_{11}	σ_6	σ_5	σ_8	σ_7	σ_{10}	σ_9	σ_4
$(1,4)(2,3) = \sigma_3$	σ_3	σ_2	σ_1	ε	σ_7	σ_9	σ_{10}	σ_4	σ_{11}	σ_5	σ_6	σ_8
$(1,2,3) = \sigma_4$	σ_4	σ_{11}	σ_7	σ_8	σ_5	ε	σ_3	σ_{10}	σ_6	σ_1	σ_2	σ_9
$(1,3,2) = \sigma_5$	σ_5	σ_9	σ_{10}	σ_6	ε	σ_4	σ_8	σ_2	σ_3	σ_{11}	σ_7	σ_1
$(1,2,4) = \sigma_6$	σ_6	σ_{10}	σ_9	σ_5	σ_2	σ_{11}	σ_7	ε	σ_1	σ_4	σ_8	σ_3
$(1,4,2) = \sigma_7$	σ_7	σ_8	σ_4	σ_{11}	σ_9	σ_3	ε	σ_6	σ_{10}	σ_2	σ_1	σ_5
$(1,3,4) = \sigma_8$	σ_8	σ_7	σ_{11}	σ_4	σ_{10}	σ_1	σ_2	σ_5	σ_9	ε	σ_3	σ_6
$(1,4,3) = \sigma_9$	σ_9	σ_5	σ_6	σ_{10}	σ_3	σ_7	σ_{11}	σ_1	ε	σ_8	σ_4	σ_2
$(2,3,4) = \sigma_{10}$	σ_{10}	σ_6	σ_5	σ_9	σ_1	σ_8	σ_4	σ_3	σ_2	σ_7	σ_{11}	ε
$(2,4,3) = \sigma_{11}$	σ_{11}	σ_4	σ_8	σ_7	σ_6	σ_2	σ_1	σ_9	σ_5	σ_3	ε	σ_{10}

We can use SAGE to construct multiplication tables. The command to use is `cayley_table()`.

SAGE

```
sage: A4=AlternatingGroup(4)
sage: A4.cayley_table()
 *  a b c d e f g h i j k l
 +----------------------
a| a b c d e f g h i j k l
b| b c a f d e h i g l j k
c| c a b e f d i g h k l j
d| d g j a h k b e l c f i
e| e i k c g l a f j b d h
f| f h l b i j c d k a e g
g| g j d k a h e l b i c f
```

```
h| h l f j b i d k c g a e
i| i k e l c g f j a h b d
j| j d g h k a l b e f i c
k| k e i g l c j a f d h b
l| l f h i j b k c d e g a
```

Notice that we have no idea which element of A_4 each letter represents. We can use the command `column_keys()` to find out.

SAGE

```
sage: A4.cayley_table().column_keys()
((), (2,3,4), (2,4,3), (1,2)(3,4), (1,2,3), (1,2,4), (1,3,2), (1,3,4),
(1,3)(2,4), (1,4,2), (1,4,3), (1,4)(2,3))
```

This tells us the order the elements appear in the column and row headings. In other words, $a = ()$, $b = (2,3,4)$, etc. We can change the order of the elements in the table by creating a list with the order we want, then passing the list to `cayley_table()` using the optional argument `elements=`.

SAGE

```
sage: A4list=["()", "(1,2)(3,4)", "(1,3)(2,4)", "(1,4)(2,3)", "(1,2,3)", "(1,3,2)",
"(1,2,4)", "(1,4,2)", "(1,3,4)", "(1,4,3)", "(2,3,4)", "(2,4,3)"]
sage: A4.cayley_table(elements=A4list)
*  a b c d e f g h i j k l
 +------------------------
a| a b c d e f g h i j k l
b| b a d c i k j l e g f h
c| c d a b l g f i h k j e
d| d c b a h j k e l f g i
e| e l h i f a d k g b c j
f| f j k g a e i c d l h b
g| g k j f c l h a b e i d
h| h i e l j d a g k c b f
i| i h l e k b c f j a d g
j| j f g k d h l b a i e c
k| k g f j b i e d c h l a
l| l e i h g c b j f d a k
```

We can also change the names it uses to represent the elements. We first create a list of "names", in precisely the same order as our elements are listed in `A4list`, then pass this to `cayley_table()` using the optional argument `names=`.

SAGE

```
sage: A4names=["1", "s1", "s2", "s3", "s4", "s5", "s6", "s7", "s8", "s9",
 "s10", "s11"]
sage: A4.cayley_table(names=A4names,elements=A4list)
 *    1  s1  s2  s3  s4  s5  s6  s7  s8  s9 s10 s11
   +-----------------------------------------------
  1|   1  s1  s2  s3  s4  s5  s6  s7  s8  s9 s10 s11
 s1|  s1   1  s3  s2  s8 s10  s9 s11  s4  s6  s5  s7
 s2|  s2  s3   1  s1 s11  s6  s5  s8  s7 s10  s9  s4
 s3|  s3  s2  s1   1  s7  s9 s10  s4 s11  s5  s6  s8
 s4|  s4 s11  s7  s8  s5   1  s3 s10  s6  s1  s2  s9
```

```
 s5|  s5  s9 s10  s6   1  s4  s8  s2  s3 s11  s7  s1
 s6|  s6 s10  s9  s5  s2 s11  s7   1  s1  s4  s8  s3
 s7|  s7  s8  s4 s11  s9  s3   1  s6 s10  s2  s1  s5
 s8|  s8  s7 s11  s4 s10  s1  s2  s5  s9   1  s3  s6
 s9|  s9  s5  s6 s10  s3  s7 s11  s1   1  s8  s4  s2
s10| s10  s6  s5  s9  s1  s8  s4  s3  s2  s7 s11   1
s11| s11  s4  s8  s7  s6  s2  s1  s9  s5  s3   1 s10
```

And there is our multiplication table, labeled exactly how we wanted!

Exercise 10.1 *Construct a multiplication table for S_3. First list the elements of S_3 then work out the table. Check your resulting table by using* SAGE.

10.3.2 Finite Cyclic Groups

Consider the set of Rubik's cube moves $G = \{\varepsilon, \mathrm{R}, \mathrm{R}^2, \mathrm{R}^3\}$. Notice that the composition of any moves in this set is still in this set. For example, move R followed by move R^2 is move R^3, similarly move R^3 followed by move R^2 is move R. In other words,

$$\mathrm{R}\mathrm{R}^2 = \mathrm{R}^3, \quad \text{and} \quad \mathrm{R}^3\mathrm{R}^2 = \mathrm{R}.$$

Each element has an inverse, $\mathrm{R}^{-1} = \mathrm{R}^3$ and $(\mathrm{R}^2)^{-1} = \mathrm{R}^2$.

It follows that this set G is a group. It has the particular property that every element in G is some power of R (even the identity is a power of R: $\varepsilon = \mathrm{R}^0 = \mathrm{R}^4$). A group with this property is called a *cyclic group*.

Definition 10.3 (Cyclic Group) *A group G is called **cyclic** if there is one element in G, say g, so that every other element of G is a power[2] of g:*

$$G = \{g^k \mid k \in \mathbb{Z}\}.$$

*In this case we write $G = \langle g \rangle$, and say g is a **generator** for G.*

*If g has order n then $G = \{e, g, g^2, g^3, \ldots, g^{n-1}\}$ and we say G is a **cyclic group of order** n.*

In our example, G is a cyclic group of order 4, since it has four elements, and it is generated by R.

The multiplication table for G is

G	ε	R	R^2	R^3
ε	ε	R	R^2	R^3
R	R	R^2	R^3	ε
R^2	R^2	R^3	ε	R
R^3	R^3	ε	R	R^2

[2] In the case when the group operation is addition then $G = \{kg \mid k \in \mathbb{Z}\}$.

As another example consider the move sequence $\alpha = \mathrm{R}^2\mathrm{U}^2$ of the Rubik's cube. This move has order 6, and if we consider the set of all powers of this move, we get a cyclic group of order 6:

$$H = \langle \alpha \rangle = \{\varepsilon, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5\}.$$

The multiplication table for H is

H	ε	α	α^2	α^3	α^4	α^5
ε	ε	α	α^2	α^3	α^4	α^5
α	α	α^2	α^3	α^4	α^5	ε
α^2	α^2	α^3	α^4	α^5	ε	α
α^3	α^3	α^4	α^5	ε	α	α^2
α^4	α^4	α^5	ε	α	α^2	α^3
α^5	α^5	ε	α	α^2	α^3	α^4

You may have noticed that in each of our examples all elements commute under the operation. In other words, the group is abelian. This is true for any cyclic group.

Definition 10.4 (Cyclic Groups are Abelian) *Let G be a cycle group. For any $a, b \in G$, $ab = ba$.*

Proof: Let $G = \langle g \rangle$. For $a, b \in G$ there exist r and s such that $a = g^r$ and $b = g^s$, and so $ab = g^r g^s = g^{r+s} = g^{s+r} = g^s g^r = ba$.

□

In the examples above each element is determined precisely by the power of R (or α), so let's write out the multiplication table where we just write i, in place of R^i (or α^i).

G	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

H	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

These tables represent the way we "multiply" in G and H. If we look closely we see that to multiply α^2 and α^4 we just add the exponents, and if the sum is larger than 5 then we take the remainder when divided by 6. So in this case $2 + 4 = 6$ which has remainder 0 when divided by 6.

In the next section, we investigate this "remainder" operation on the set of integers.

10.3.3 Group of Integers Modulo n: C_n

Consider the set $C_{12} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$. We define the operation $+_{12}$ to be *addition modulo* 12. By this we mean $a +_{12} b$ is the remainder of $a + b$ when divided by 12. This type of addition is familiar to anyone who adds time on a clock. For example, if it is 8-o'clock, then 6 hours later is $8 +_{12} 6 = 2$, or 2-o'clock.

Some examples are: $2 +_{12} 3 = 5$, $7 +_{12} 5 = 0$, since $7 + 5 = 12$ which is divisible by 12, and $11 +_{12} 10 = 9$, since $11 + 10 = 21$ which has remainder 9 when divided by 12..

SAGE

```
sage: (2+3)%12
5
sage: (7+5)%12
0
sage: (11+10)%12
9
```

Is C_{12} a group under this "new" addition $+_{12}$?

Lets check the properties one-by-one.

closed: Since the remainder will always be a number between 0 and 11 then C_{12} is certainly closed under $+_{12}$.

associative: This addition is associative, since it is built from regular addition of integers which is associative.

identity: The identity is 0, since $0 +_{12} b = b$ for all $b \in C_{12}$.

inverses: What is the inverse of an element? For example, what is the inverse of 3? This would be a number b such that 12 divides $3 + b$. The number $12 - 3 = 9$ has this property. So the inverse of 3 is 9. In general, the inverse of a is $12 - a$.

It follows that C_{12} is a group.

There was nothing special about 12 in this example, other than it being familiar to us from our experience dealing with clocks. We can really do this for any positive integer n.

Definition 10.5 *Let $n > 1$ be and integer. Define an operation on the set $C_n = \{0, 1, 2, 3, \ldots, n-1\}$, called* addition modulo n*, as follows. For $a, b \in C_n$, let $a +_n b$ be the remainder of $a + b$ when divided by n. C_n is a group under addition modulo n, and is called the (additive)* ***group of integers modulo n****. Since this group is cyclic it is often called the (additive)* ***cyclic group of order*** *n.* [3]

Why is C_n cyclic? Each element of C_n can be obtained from 1 by repeatedly adding 1 to itself. Note, our group operation is addition so the analogy of a "power" is a multiple. Since every element of C_n is a suitable multiple of 1 then $C_n = \langle 1 \rangle$.

Notation & Terminology:

If a, b, and n are integers we say a **is congruent to** b **modulo** n if $n \mid b - a$ and we write $a \equiv b \pmod{n}$. For example, $15 \equiv 3 \pmod{12}$, and $8 \equiv 2 \pmod{4}$, but $7 \not\equiv 3 \pmod{5}$ since $5 \nmid 7 - 3$.

Addition of two integers, a and b, modulo n, which we denoted as $a +_n b$ is often denoted by

$$a + b \pmod{n}.$$

For example, $11 +_{12} 10 = 9$ could also be written as $11 + 10 \equiv 9 \pmod{12}$.

[3] This group is also usually denoted by $\mathbb{Z}/n\mathbb{Z}$.

In section 10.3.2 we saw the multiplication tables for G and H, written only using the exponents, are precisely the groups C_4 and C_6. This observation, is true in general, in the sense that *every finite cycle group is essentially C_n for some integer n.* The only difference it just how the elements were named, which is superficial.

Finite cyclic groups are built into SAGE with the command `CyclicPermutationGroup()`. As the name suggests, cyclic groups are constructed using permutations. Lets look at an example.

SAGE
```
sage: C5=CyclicPermutationGroup(5)
sage: C5.list()
[(), (1,2,3,4,5), (1,3,5,2,4), (1,4,2,5,3), (1,5,4,3,2)]
```

Here, C_5 is represented by using the 5-cycle $(1,2,3,4,5)$ as a generator. We can compute the multiplication table by first telling SAGE how to name the elements.

SAGE
```
sage: C5list=["()", "(1,2,3,4,5)", "(1,3,5,2,4)", "(1,4,2,5,3)", "(1,5,4,3,2)"]
sage: C5names=["0","1","2","3","4"]
sage: C5.cayley_table(names=C5names,elements=C5list])
*  0 1 2 3 4
 +----------
0| 0 1 2 3 4
1| 1 2 3 4 0
2| 2 3 4 0 1
3| 3 4 0 1 2
4| 4 0 1 2 3
```

If one wants to work with C_n where the elements are $\{0,1,\ldots,n-1\}$, rather than permutations, then this can be done using `IntegerModRing()`. Though, for just doing calculations we would use the modulo operator `%`, as in the clock example above.

SAGE
```
sage: C5=IntegerModRing(5)
sage: C5.list()
[0, 1, 2, 3, 4]
sage: C5(3)+C5(4)
2
```

Exercise 10.2 *Construct a Cayley table for $C_7 = \{0,1,2,3,4,5,6\}$, under addition modulo 7. Check your results using* SAGE.

Example 10.1 *We determine the order of each element in $C_{12} = \{0,1,2,3,4,5,6,7,8,9,10,11\}$. 1 has order 12. Since $6 \cdot 2 = 2 +_{12} 2 +_{12} 2 +_{12} 2 +_{12} 2 +_{12} 2 = 0$ then 2 has order 6. Similarly $4 \cdot 3 = 0$ so 3 has order 4. Continuing in this way we find:*

k	***elements of order*** k
1	0
2	6
3	4, 8
4	3, 9
6	2, 10
12	1, 5, 7, 11

It follows that $1, 5, 7,$ *and* 11 *are all generators of* C_{12}*. That is,*

$$C_{12} = \langle 1 \rangle = \langle 5 \rangle = \langle 7 \rangle = \langle 11 \rangle.$$

A few curious things to note: (i) the only orders that show up are divisors of 12*, and (ii) the generators of* C_{12} *are the elements relatively prime to* 12*. Are these coincidences?*

10.3.4 Group of Units Modulo n: $U(n)$

You may wonder if we can do the same thing with multiplication, instead of addition, on C_n. That is, does C_n form a group under *multiplication modulo n*, $\cdot_n$?

First we notice that the identity would be 1, but of course, 0 doesn't have a (multiplicative) inverse. So lets take 0 out of consideration, and just focus on the set $C_n^* = \{1, 2, 3, \ldots, n-1\}$.

As an example consider $C_6^* = \{1, 2, 3, 4, 5\}$. Lets check to see if this set is closed under multiplication modulo 6. Well, $3 \cdot_6 5 = 3 \in C_6^*$, so far so good. But $2 \cdot_6 3 = 0 \notin C_6^*$. Therefore, C_6^* is definitely not closed under multiplication, so it is *not a group*.

But all is not lost. It just seems that some elements in C_6^* are just trouble-makers. Their presence prevents it from being closed under multiplication. Who are these trouble makers? Lets find out.

$$\begin{array}{llll} 1 \cdot_6 2 = 2 & 1 \cdot_6 3 = 3 & 1 \cdot_6 4 = 4 & 1 \cdot_6 5 = 5 \\ 2 \cdot_6 2 = 4 & 2 \cdot_6 3 = 0 \notin C_6^* & 2 \cdot_6 4 = 2 & 2 \cdot_6 5 = 4 \\ 3 \cdot_6 3 = 3 & 3 \cdot_6 4 = 0 \notin C_6^* & 3 \cdot_6 5 = 3 & 4 \cdot_6 4 = 4 \\ 4 \cdot_6 5 = 2 & 5 \cdot_6 5 = 1 & & \end{array}$$

The elements 2, 3 and 4 seem to be causing the problems. These are precisely the elements that have a factor in common with 6. Is this a coincidence? Not at all, the remainder of division by 6 will always be between 0 and 5, and since C_6^* does not contain 0, the trouble makers are the numbers whose products are divisible by 6. For two numbers $a, b \in C_6^*$ to have a product divisible by 6, they each must have a factor in common with 6.

We say two numbers are **relatively prime** if they do not have a common prime factor. If two numbers have a common factor then we say they are *not relatively prime*. Note that if two numbers are relatively prime, then they have no common prime factor, and so their greatest common divisor is 1. This means a and b are relatively prime if and only if $\gcd(a, b) = 1$.

We have just determined that the trouble makers are the numbers which are not relatively prime to 6. Namely, 2, 3, and 4.

Therefore, consider just the set of numbers in C_6^* that are relatively prime to 6: This set is denoted by $U(6)$:

$$U(6) = \{1, 5\}.$$

This set is a group! The inverse of 5 is itself. The multiplication table is:

U(6)	1	5
1	1	5
5	5	1

SAGE

```
sage: U6=[m for m in range(0,6) if gcd(m,6)==1]
{1, 5}
```

The previous construction can be done for any integer n in place of 6. This is the next definition.

Definition 10.6 (Group of Units Modulo n) *Let $n > 1$ be and integer, and let*

$$U(n) = \{m \mid 1 \leq m \leq n-1 \textbf{ and } \gcd(m, n) = 1\}.$$

*$U(n)$ is a group under multiplication modulo n, and is called the **group of units modulo** n.*

In the case when p is prime, $U(p) = C_p^* = \{1, 2, 3, \ldots, p-1\}$.

The number of elements in $U(n)$ is precisely the integers between 1 and n which are relatively prime to n. There is an important number-theoretic function, called *Euler's phi function*, denoted by ϕ, which calculates this number.

Definition 10.7 (Euler Phi Function) *For any positive integer n, $\phi(n)$ is the number of integers in $\{1, 2, \ldots, n\}$ which are relatively prime to n. In other words, $\phi(n) = |U(n)|$.*

This function has been implemented in SAGE, under the command `euler_phi()`. For example, here we see $\phi(6) = 2$.

SAGE

```
sage: euler_phi(6)
2
```

Exercise 10.3 *Determine the elements of the set $U(8)$, and construct the multiplication table.*

Example 10.2 *In this example we will investigate the group $U(18)$, which has 6 elements.*

SAGE

```
sage: euler_phi(18)
6
```

Of course, we could have done this by hand (or use SAGE *code similar to the example we did for* $U(6)$*). We would just go through the numbers from* 1 *to* 18 *and omit any that have a factor of* 2 *or* 3*.*

$$U(18) = \{1, 5, 7, 11, 13, 17\}.$$

What is the inverse of 11*? One way is to compute the product of* 11 *with each element of* $U(18)$ *and check when we get* 1*:*

SAGE

```
sage: for m in [1, 5, 7, 11, 13, 17]:
sage:     if 11*m%18==1:
sage:         print m
5
```

Therefore $11^{-1} = 5$ *in* $U(18)$*.*

A more efficient way to find the inverse is to use the Extended Euclidean Algorithm. If a *and* b *are integers and* $gcd(a, b) = d$ *then there must be integers* u *and* v *so that* $ua + vb = d$*. The standard algorithm for finding the* gcd *is called the* Euclidean Algorithm*, and the algorithm for producing numbers* u *and* v *is called the* Extended Euclidean Algorithm*. We won't go into the details of these algorithms, such topics are covered in a course in elementary number theory. However, these algorithms are implemented in* SAGE*, so we can use them.*

SAGE

```
sage:  d,u,v = xgcd(11,18)
sage:  print u,v
5, -3
```

How does this help us find 11^{-1}*? Well, the Extended Euclidean Algorithm has returned three numbers: the first is* 1 *which is the* gcd*, the other two,* 5 *and* -3*, have the property that* $5(11) + (-3)(18) = 1$*. This means* $5(11)$ *has remainder* 1 *when divided by* 18*. Which is exactly what it means for* 5 *to be an inverse of* 11*.*

To find the inverse of 13 *we can do the same thing, and get* $13^{-1} = 7$*.*

SAGE

```
sage:  d,u,v = xgcd(13,18)
sage:  print u,v
7, -5
```

We can write a function called `inverse` *that will return the inverse of* a *in* $U(m)$*.*

SAGE

```
sage: def inverse(a,m):
sage:     d,u,v=xgcd(a,m)
sage:     if d==1:
sage:         return u%m           # return inverse as a number between 1 and m-1
sage:     else:
sage:         return a, "is not in U group"     # just in case a is not in U(m)

sage:  inverse(11,18)
5
sage:  inverse(13,18)
13
```

To compute the order of an element, we can take successive powers until we hit the identity. As an example, we determine the order of 11 *is* 6.

SAGE

```
sage:  for n in (1..6):
sage:      print n, 11^n%18
1 11
2 13
3 17
4 7
5 5
6 1
```

We can also create a function to do this. We'll see next lecture that the order of an element must divide the order of the group so we can limit the exponents we need to check. The function `divisors(m)` *returns a list of the divisors of* m*, arranged from smallest to largest. Recall* $|U(m)| = \phi(m)$*, the Euler phi function.*

SAGE

```
sage:   def order(a,m):
sage:       if gcd(a,m)==1:
sage:           for k in divisors(euler_phi(m)):
sage:               if a^k%m==1:
sage:                   return k
sage:       else:
sage:           return a, "is not in U group"

sage:  order(5,18)
6
sage:  order(13,18)
3
```

It follows that $U(18)$ *is a cyclic group generated by* 5*:*

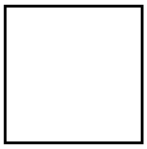
$$U(18) = \langle 5 \rangle.$$

The element 11 *also generates the group.*

$U(18)$ *has subgroups* $\{1\}$*,* $\{1, 17\}$*, and* $\{1, 7, 13\}$.

10.3.5 Dihedral Groups: D_n

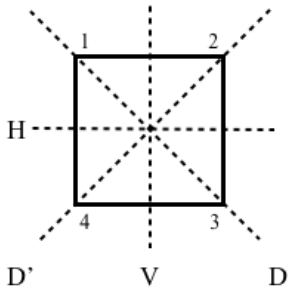
Consider a square as drawn below. We want to determine all the ways we can pick up the square, move it in some way, then put it back in the original space it occupied. If an observer didn't see us pick it up, but only saw it before and after, they shouldn't notice any change. For example, we could rotate it 90 degrees, or we could flip it over a horizontal line. We'd like to determine all possible ways we could have moved the square. In some sense, the number of ways we can do this is related to how "symmetric" a square is.



Let G denote the set of ways in which we can move the square. To keep track of the motions, we can label the vertices of the squares as $1, 2, 3, 4$, and each motion corresponds to a permutation of the labels on the vertices. In Table 1 we list the elements of G: $G = \{R_0, R_{90}, R_{180}, R_{270}, H, V, D, D'\}$.

notation	**description**	**permutation**
R_0	rotation of $0°$ (i.e. do nothing)	ε
R_{90}	rotation of $90°$ (clockwise)	$(1,2,3,4)$
R_{180}	rotation of $180°$ (clockwise)	$(1,3)(2,4)$
R_{270}	rotation of $270°$ (clockwise)	$(1,4,3,2)$
H	reflection of $180°$ about horizontal axis	$(1,4)(2,3)$
V	reflection of $180°$ about vertical axis	$(1,2)(3,4)$
D	reflection of $180°$ about diagonal axis (see diagram below)	$(2,4)$
D'	reflection of $180°$ about other diagonal axis (see diagram below)	$(1,3)$

Table 1: Symmetries of the square



We can combine elements of G by doing consecutive motions. For example, $R_{90}H$ means first rotate by $90°$, then reflect about the horizontal axis. The resulting motion is equivalent to D'. We can see this by actually doing both motions $R_{90}H$ and D' and observing they do exactly the same thing. Or we could compose their corresponding permutations: $(1,2,3,4)(1,4)(2,3) = (1,3)$.

G is a group under this way of composing moves. It is the *group of symmetries of the square*, or more commonly called **the dihedral group of order 8**, and denoted by D_4. The multiplication table for D_4 is

D_4	R_0	R_{90}	R_{180}	R_{270}	H	V	D	D'
R_0	R_0	R_{90}	R_{180}	R_{270}	H	V	D	D'
R_{90}	R_{90}	R_{180}	R_{270}	R_0	D'	D	H	V
R_{180}	R_{180}	R_{270}	R_0	R_{90}	V	H	D'	D
R_{270}	R_{270}	R_0	R_{90}	R_{180}	D	D'	V	H
H	H	D	V	D'	R_0	R_{180}	R_{90}	R_{270}
V	V	D'	H	D	R_{180}	R_0	R_{270}	R_{90}
D	D	V	D'	H	R_{270}	R_{90}	R_0	R_{180}
D'	D'	H	D	V	R_{90}	R_{270}	R_{180}	R_0

The analysis carried out for a square can similarly be done for any regular n-gon, R_n (where $n \geq 3$). See Figure 1 for some familiar n-gons. If $n = 3$ then R_3 is an equilateral triangle. If $n = 4$ then R_4 is a square as we just considered. If $n = 5$ then R_5 is a regular pentagon, and so on. The corresponding group is denoted by D_n and is called the **dihedral group of order** $2n$.

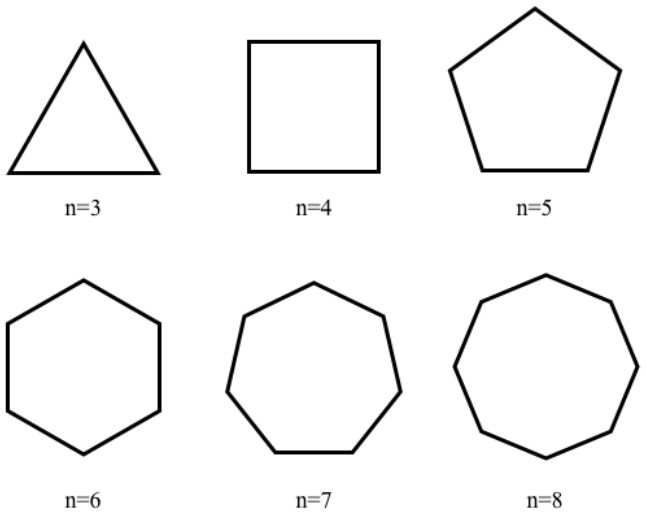


Figure 1: Some regular n-gons.

Dihedral groups are frequently found in art and nature, and they are a very important type of group used by mineralogists to study crystals.

You may wonder where the "2n" comes from in the name. Looking back at the square we see that there are 8 motions preserving the square (we call these the symmetries of the square). Four were rotations, and four were reflections. This is true for any regular n-gon. There will be n rotational symmetries and n reflective symmetries, for a total of $2n$.

Dihedral groups are built into SAGE. Each element is represented as permutations of the vertices of the n-gon. Here is an example with D_4.

SAGE

```
sage: D4=DihedralGroup(4)
sage: D4.list()          #lists the elements of D4 as represented in SAGE
[(), (2,4), (1,2)(3,4), (1,2,3,4), (1,3), (1,3)(2,4), (1,4,3,2),
(1,4)(2,3)]
```

We can assign each element to a name. For example, $(1,2,3,4)$ corresponds to the $90°$ rotation R_{90}.

SAGE

```
sage: R90=D4("(1,2,3,4)")
sage: R180=D4("(1,3)(2,4)")
sage: R270=D4("(1,4,3,2)")
sage: H=D4("(1,4)(2,3)")
sage: V=D4("(1,2)(3,4)")
sage: D=D4("(2,4)")
sage: Dp=D4("(1,3)")         # we use Dp for D'
```

We can now compute products. For example, we see $R_{90}D = H$.

SAGE

```
sage: R90*D
(1,4)(2,3)
```

The full multiplication table for D_4 can be computed in SAGE as follows.

SAGE

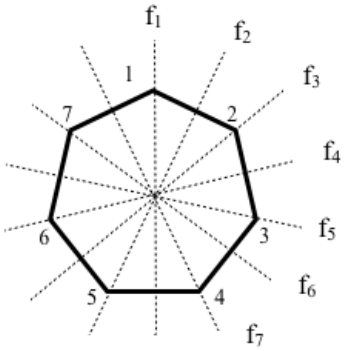
```
sage: D4list=["()", "(1,2,3,4)", "(1,3)(2,4)", "(1,4,3,2)", "(1,4)(2,3)",
"(1,2)(3,4)", "(2,4)", "(1,3)"]
sage: D4names=["R0","R90","R180","R270","H","V","D","D'"]
sage: D4.cayley_table(names=D4names,elements=D4list)

*    R0  R90 R180 R270    H    V    D   D'
    +----------------------------------------
  R0|   R0  R90 R180 R270    H    V    D   D'
 R90|  R90 R180 R270   R0   D'    D    H    V
R180| R180 R270   R0  R90    V    H   D'    D
R270| R270   R0  R90 R180    D   D'    V    H
   H|    H    D    V   D'   R0 R180  R90 R270
   V|    V   D'    H    D R180   R0 R270  R90
   D|    D    V   D'    H R270  R90   R0 R180
  D'|   D'    H    D    V  R90 R270 R180   R0
```

10.3.6 Notation for D_n

For a regular n-gon we typically use r to denote a clockwise rotation through $\frac{360}{n}$ degrees, and more generally, r^k to denote a clockwise rotation through $k\frac{360}{n}$ degrees. A reflection through a line of symmetry is denoted by f_i, for $1 \leq i \leq n$.

For example, the lines of symmetry for a regular 7-gon are labelled below. Some of the elements are described in Table 2. There are 14 elements in D_7:

$$D_7 = \{1, r, r^2, r^3, r^4, r^5, r^6, r^7, f_1, f_2, f_3, f_4, f_5, f_6, f_7\}.$$



notation	description	permutation
1	rotation of 0° (i.e. do nothing)	ε
r	rotation of $\frac{360}{7}$ degrees (clockwise)	$(1,2,3,4,5,6,7)$
r^k	rotation of $k\frac{360}{n}$ degrees (clockwise) for $1 \leq k \leq 7$	
f_1	reflection of 180° about f_1 line	$(2,7)(3,6)(4,5)$
f_i	reflection of 180° about f_i axis for $1 \leq i \leq 7$	

Table 2: Symmetries of a regular 7-gon

One can check that every element of D_7 can be expressed as a product of the form $r^k f_1^\ell$ for some $0 \leq k \leq 6$, and $0 \leq \ell \leq 1$. For example, $f_5 = r^3 f_1$. We say D_7 is generated by r, f_1 and write

$$D_7 = \langle r, f_1 \rangle.$$

10.4 Exercises

1. Give two reasons why the set of odd integers under addition is not a group.
2. Show that $\begin{bmatrix} 1 & 1 \\ 2 & 2 \end{bmatrix}$ does not have a multiplicative inverse in $GL(2,\mathbb{R})$.
3. Show that the group $GL(2,\mathbb{R})$ is non-abelian by finding two matrices A and B in $GL(2,\mathbb{R})$ where $AB \neq BA$.
4. Find the inverse of $\begin{bmatrix} 1 & 2 \\ 1 & 3 \end{bmatrix}$ in $SL(2,\mathbb{R})$.
5. The group operation $*$ is frequently omitted, for example $a * b$ would just be written as ab. This is due to the fact that we often refer to the operation as "multiplication". However, when the operation is addition we keep the $+$ symbol, and we also use 0 for the identity instead of e. Translate each of the following multiplicative expression into its additive counterpart.
   (a) a^2b
   (b) $b^4a^{-3}b$
   (c) $(ab^3)^{-2}c^3 = e$
6. Let $G = \{a, b, c, d\}$ have an operation $*$ with corresponding multiplication table

$*$	a	b	c	d
a	a	b	c	d
b	b	a	d	c
c	c	d	a	b
d	d	d	b	c

   Is G a group under this operation? Explain.

Dihedral Groups:

Exercises 7 through 13 are on the dihedral groups.

7. (a) With pictures and words, describe each symmetry in D_3 (the set of symmetries of an equilateral triangle).
   (b) Write out a complete multiplication (Cayley) table for D_3.
   (c) Is D_3 abelian (that is, does every element commute with every other element)?
8. With pictures and words, describe each symmetry in D_5 (the set of symmetries of a regular pentagon).
9. For $n \geq 3$ describe the elements of D_n. (You will need to consider two cases, depending on whether n is even or odd.)
10. In D_n, explain geometrically why
    (a) a reflection followed by a reflection must be a rotation.
    (b) a reflection and a rotation taken together in either order must be a reflection.

11. Is D_n a cyclic group? That is, does $D_n = \langle g \rangle$ for some $g \in D_n$?

12. Is D_n abelian?

13. If r_1, r_2, and r_3 represent rotations and f_1, f_2, and f_3 represent reflections from D_n, determine whether $f_1 r_3 r_2 f_2 r_1 f_1$ is a rotation or reflection.

Group of Integers under addition modulo n:

Exercises 14 through 18 are on the group of integers modulo n: C_n.

14. List the element of C_2, and write out a multiplication table for this group.

15. Determine the following in C_{15}

    (a) $7 +_{15} 6$ (c) $12 \cdot 7$ (e) the inverse of 3 (g) ord(7)
    (b) $13 +_{15} 8$ (d) the inverse of 11 (f) ord(10)

16. Determine the order of each element in C_{10}.

17. Determine which elements of C_{10} are generators for C_{10}. That is, find all $g \in C_{10}$ such that $C_{10} = \langle g \rangle$.

18. Find all the elements of $g \in C_{12}$ for which $C_{12} = \langle g \rangle$.

Unit Group modulo n:

Exercises 19 through 22 are on the Unit Groups $U(n)$.

19. Determine the elements of the set $U(5)$, and construct the multiplication table.

20. Determine the elements of the set $U(12)$, and construct the multiplication table.

21. (a) How many elements does $U(37)$ have?
    (b) Find the inverse of 25 in $U(37)$.
    (c) What is the order of 25.
    (d) Is $U(37)$ cyclic? If so, find a generator.

    (Hint: use SAGE to help with calculations.)

22. Is $U(20)$ cyclic?

Groups in General:

Exercises 23 through 30 are on groups in general. Solutions to these exercises should be based on the four properties listed in the definition of a group, and any theorems which were consequences of these properties.

23. For any elements a and b from a group G, and any integer n, prove that $(b^{-1}ab)^n = b^{-1}a^n b$. (We've already shown this for permutations, so this question is asking you to verity this is really just a consequence of group properties.)

24. Let a and b be elements of an abelian group G, and let n be any integer. Show that $(ab)^n = a^n b^n$. Is this true for non-abelian groups? Explain.

25. If $a, b \in G$ such that $\text{ord}(a^2) = \text{ord}(b^2)$, is it necessarily true that $\text{ord}(a) = \text{ord}(b)$?

26. In a group G show that the number of nonidentity elements that satisfy the equation $x^5 = e$ is a multiple of 4.

27. Show that if G is a group and $a \in G$ such that $a^2 = a$ then a must be the identity.

28. Suppose $G = \{e, a, b, c, d\}$ is a group with multiplication table

	e	a	b	c	d
e	e				
a		b			e
b		c	d	e	
c		d		a	b
d					

Fill in the blank entries.

29. Prove Lemma 10.1.
(Hint: The first two parts are really just consequences of the left- and right- cancellation properties.)

30. Prove that if G is a group with the property that the square of every element is the identity (i.e. every element has order 2), then G is abelian.

31. Let G be a group with operation $\cdot$. For which operation $*$ is the set G a group under $*$?

(a) $a * b = b \cdot a$
(b) $a * b = b^{-1} \cdot a \cdot b$
(c) $a * b = b^{-1} \cdot a$
(d) $a * b = (a \cdot b)^2$

A few more examples of groups:

32. The integers 5 and 15 are among a collection of 12 integers that form a group under multiplication modulo 56. List all 12.

33. **Nim Group** Consider the set $G = \{0, 1, 2, 3, 4, 5, 6, 7\}$. Suppose there is a group operation $*$ on G that satisfies the following two conditions:

(a) $a * b \geq a + b$ for all a, b in G,
(b) $a * a = 0$ for all a in G.

Construct the multiplication table for G. This groups is sometimes called the *Nim Group* due to its relationship to the game of Nim.

34. Prove that the set of all 3 matrices with real entries of the form

$$\begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix}$$

is a group under matrix multiplication. (This group, sometimes called the *Heisenberg group* after the Nobel Prize winning physicist Werner Heisenberg, is intimately related to the Heisenberg Uncertainty Principle of Quantum Physics.)