Chapter 10 : Groups

Definition 10.1.1 — 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 an 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 $a*b = b*a = e$.

Definition 10.1.2 — Order of a Group. The number of elements of a group (finite or 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.

Theorem 10.1.1 — 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:

Multiplication (Cayley) Table:

If G is finite then the operation can be given in terms of a "multiplication table":

$G = \{g_1, g_2, \dots, g_n\}$

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

Lemma 10.1.4 (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 $\searrow$ then $g*h = h*g$ for all $g,h \in G$. (In this case, we call G abelian.)

Suppose a occurs twice in row b. This means
$a = bc = bd \Rightarrow$

Examples:

1) $\mathbb{Z}$ under $+$, $\mathbb{Q}$ under $+$, $\mathbb{R}$ under $+$

We write each of these as $(\mathbb{Z},+)$, $(\mathbb{Q},+)$, $(\mathbb{R},+)$.

in each case the identity is ___, inverse of a is ___

2) $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$ under $\cdot$

identity is ___, inverse of a is ___

3) $\mathbb{R}^3 = \{ (a,b,c) : a,b,c \in \mathbb{R} \}$ under componentwise addition.

identity is ___, inverse of (a,b,c) is ___

4) $S_n = \{ \alpha : [n] \to [n] \mid \alpha \text{ is a bijection} \}$

is a group under composition.

$A_n = \{ \alpha \in S_n \mid \alpha \text{ is even} \}$

is a group under composition.

$A_3 = \{ \varepsilon, (1\,2\,3), (1\,3\,2) \}$

	ε	$(1\,2\,3)$	$(1\,3\,2)$
ε			
$(1\,2\,3)$			
$(1\,3\,2)$			

Cayley Table

Cyclic Groups :

Consider the set of cube moves :

$$G = \{ \varepsilon, R, R^2, R^3 \}$$

This set is closed under composition/inverses, and is therefore a group.

Every element of G is a power of R, we call such a group <u>cyclic</u>.

Definition 10.3.1 — 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 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.

(If the operation is addition then $G = \{ kg \mid k \in \mathbb{Z} \}$.)

For $G = \{ \varepsilon, R, R^2, R^3 \}$ the multiplication table is

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

$\xrightarrow{\text{Exponents}}$

	0	1	2	3
0				
1				
2				
3				

Consider $\alpha = R^2 U^2$. This move has order 6 so it generates a group of order 6 :

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

	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

$\xrightarrow{\text{exponents}}$

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

Group of integers mod n:

$\mathbb{Z}_{12} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$

Define the operation $+_{12}$ by

$$a +_{12} b = \underbrace{\text{remainder of } a+b \text{ when divided by } 12}_{a+b \bmod 12}$$

$1 +_{12} 7 =$ ____, $\quad 6 +_{12} 10 =$ ____, $\quad 8 +_{12} 4 =$ ____

$(\mathbb{Z}_{12}, +_{12})$ is a group.

- identity is ____
- inverse of a is ______
- associativity follows from the associativity of $+$ on $\mathbb{Z}$.

Definition 10.3.2 Let $n > 1$ be and integer. Define an operation on the set $\mathbb{Z}_n = \{0, 1, 2, 3, \ldots, n-1\}$, called *addition modulo* n, as follows. For $a, b \in \mathbb{Z}_n$, let $a +_n b$ be the remainder of $a + b$ when divided by n. $\mathbb{Z}_n$ 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.

$(\mathbb{Z}_4, +_4)$

$\mathbb{Z}_4 = \{ \qquad \}$

$+_4$	0	1	2	3
0				
1				
2				
3				

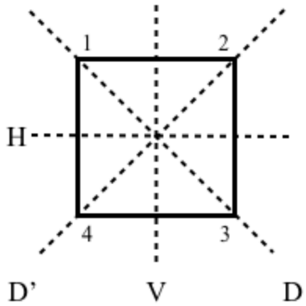
$(\mathbb{Z}_5, +_5)$

$\mathbb{Z}_5 = \{ \qquad \}$

$+_5$	0	1	2	3	4
0					
1					
2					
3					
4					

Dihedral Group D_n :

Consider a square. How many ways can we pick it up move it in some way, then return it back to its original location?



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 Figure 10.1b)	(2 4)
D'	reflection of 180° about other diagonal axis (see Figure 10.1b)	(1 3)

These 8 moves are known as the symmetries of the square.
We can compose moves:

VR_{270} means first reflect across the vertical line then rotate 270°. The result is equivalent to just doing D.

$$VR_{270} =$$

The set

$$D_4 = \{R_0, R_{90}, R_{180}, R_{270}, H, V, D, D'\}$$

under the operation of composition is a group.

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

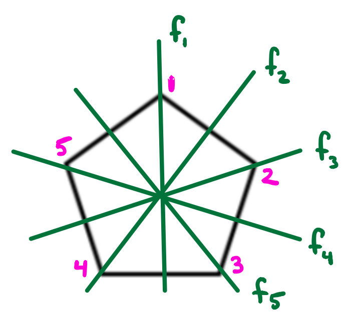
In general, for a regular n-gon the resulting group D_n is called the <u>dihedral group of order $2n$</u>.

An n-gon has n rotational symmetries: for $0 \le k \le n-1$

r^k is a rotation through $k\left(\frac{360}{n}\right)$ degrees

and n reflective symmetries (reflection through n different lines):
$f_1, f_2, \ldots, f_n$

$$D_n = \{e, r, r^2, r^3, \ldots, r^n, f_1, f_2, \ldots, f_n\}$$



Example: In D_5 determine

(a) $(r^3)^{-1}$

(b) $r^2 f_4$

Group of units modulo n:

Consider $\mathbb{Z}_n$ under multiplication modulo n:

$$a \cdot_n b = [\text{remainder of } ab \text{ divided by } n]$$
$$= ab \pmod{n}$$

First off, toss out 0 since it won't have an inverse.

Example: $\mathbb{Z}_6^* = \{ \quad \}$

$\cdot_6$	1	2	3	4	5
1					
2					
3					
4					
5					

$\longrightarrow$

$U(6) =$

$=$

Definition 10.3.3 — Group of Units Modulo n. Let $n > 1$ be and integer, and let

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

$U(n)$ is a group under multiplication modulo n, and is called the **group of units modulo** n.
In the case when p is prime, $U(p) = \mathbb{Z}_p^* = \{1, 2, 3, \ldots, p-1\}$.

Examples: $U(4) = \{ \quad \}$ $\qquad$ $U(5) = \{ \quad \}$

$\cdot_4$	

$\cdot_5$	

$U(8) = \{ \quad \}$

$\cdot_8$	

Algorithm for finding inverses in $U(n)$:

FACT : If $a,b \in \mathbb{Z}$ and $d = \gcd(a,b)$ then there exist $u,v \in \mathbb{Z}$ such that

$$ua + bv = d$$

The usual algorithm for finding d,u,v is called the <u>extended euclidean algorithm</u>.

Example: $1 = \gcd(5,8)$ and

$$5(5) - 3(8) = 1$$

Notice, this means

To find a^{-1} in $U(n)$, first find $u,v \in \mathbb{Z}$ such that

$$ua + vn = 1$$

then

$$a^{-1} \equiv u \pmod{n}$$

Can use sagemath to do this : xgcd(...)