

---

# CHAPTER 1

---

## GROUPS

### 1 Basix

#### Definition 1.1: A group $(G, \cdot)$

A group consists of a set and a binary relation  $\cdot : G \times G \rightarrow G$  (which makes it closed by definition) such that:

1.  $\forall a, b, c \in G, (a \cdot b) \cdot c = a \cdot (b \cdot c)$  (Associative)
2. There exists an element  $e \in G$  called identity so that for every  $a \in G$  we have  $a \cdot e = e \cdot a = a$
3. For every element  $a$  in  $G$  we have another element  $a^{-1}$  so that  $aa^{-1} = a^{-1}a = e$

A way to remember group axioms is to remember ASCII: **A**Ssociative, **C**losed, **I**ntity, and **I**nverse

#### *Example : Some group examples:*

$\mathbb{Z}$  with the usual addition, with 0 as identity. Inverse being  $-a$ .

$\mathbb{Z}/n\mathbb{Z}$  with the modular addition, with identity being  $\bar{0}$  and inverse being  $\overline{-a}$ .

In fact  $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$  are groups with respective addition, identity being 0 and inverse being  $-a$ .

$\mathbb{R}^+, \mathbb{C} - \{0\}, \mathbb{R} - \{0\}$ , etc. are groups with multiplication as the operation. Here identity is 1, and inverse is  $\frac{1}{a}$ .

$\mathbb{Z}/n\mathbb{Z}^*$ , the set of all congruence classes in  $\mathbb{Z}/n\mathbb{Z}$  which have a multiplicative inverse (or equivalently, those that have gcd with  $n$  as 1) forms a group under multiplication. The identity is  $\bar{1}$  and the inverse is that  $\bar{c}$ , which was shown to exist, such that  $\bar{a} \cdot \bar{c} = \bar{1}$ .

### Definition 1.2: Direct Product

If  $(A, !)$  and  $(B, *)$  are each groups, then we define the **Direct Product** as the group formed by  $A \times B := \{(a, b) : a \in A, b \in B\}$  with the operation  $\& : (A \times B) \times (A \times B) \rightarrow A \times B$  defined by  $(a_1, b_1)\&(a_2, b_2) = (a_1!a_2, b_1 * b_2)$

### Proposition 1.3

If  $G, \cdot$  is a group, then the following hold:

1. The identity element  $e$  is unique.
2. for every  $a \in G$ , the inverse element  $a^{-1}$  is unique
3.  $(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$
4. For any  $a_1, a_2, \dots, a_n \in G$ , the expression  $a_1 \cdot a_2 \cdots a_n$  is independent of how it is bracketed.

**Proof.** (1) Suppose the identity is not unique, i.e, there exists  $e_1$  and  $e_2$  so that it obeys identity axioms. We have  $a \cdot e = e \cdot a = a$ , which means  $(e_1)e_2 = e_2(e_1) = e_2$ , treating  $e_2$  as true identity. But also,  $(e_2)e_1 = e_1(e_2) = e_1 = e_2$ . Hence we see easily that  $e_1 = e_2$ .

(2) Suppose two inverses  $x$  and  $y$  exist.  $ax = e$ , which means  $yax = ye = y$ , but from associativity,  $(ya)x = x = y$ . Hence,  $x = y := a^{-1}$

(3)  $a \cdot b(a \cdot b)^{-1} = e$  which implies  $a^{-1}a \cdot b(a \cdot b)^{-1} = a^{-1} \implies b^{-1}(a^{-1}a) \cdot b(a \cdot b)^{-1} = b^{-1}a^{-1}$  which directly gives  $(a \cdot b)^{-1} = b^{-1}a^{-1}$

(4) (**PEDANTIC PROOF AHEAD, SKIP IF NOT A PEDANT**) For just one element  $a_1$ , there is no need to even check. Assume that the bracketing does not change the meaning for any consecutive  $n$  operations. Consider

$$a_1 \cdot a_2 \cdot a_3 \cdots a_n \cdot a_{n+1}$$

First look at the bracketing

$$\{(a_1 \cdot a_2 \cdot a_3 \cdots a_n)\} \cdot (a_{n+1})$$

From induction hypothesis, no bracketing inside the  $\{\}$  affects the operations. Next, consider the kind

$$\{(a_1 \cdot a_2 \cdot a_3 \cdots)\}(a_n \cdot a_{n+1})$$

Again, from induction, no bracketing affects the operations. By means of reverse induction, we show that no bracketing affects the end result of these operations.  $\square$

### Proposition 1.4

Let  $G$  be a group and let  $a, b$  be elements in the group. Then the equations  $ax = b$  and  $ya = b$  have unique solutions. Explicitly, we have the left and right cancellation laws:

If  $au = av$ , then  $u = v$

If  $ub = vb$ , then  $u = v$

**Proof.** If  $au = av$ , we multiply both sides by  $a^{-1}$  to preserve equality  $u = v$ . Similarly, we multiply  $b^{-1}$  to either side of the equation  $ub = vb$  which gives  $u = v$   $\square$

### Definition 1.5: Order of an element $g$ in a group $G$

We say an element  $g$  in  $G$  is of *order*  $n \in \mathbb{N}$  if  $n$  is the smallest natural number so that  $g^n = g \cdot g \cdots g = e$ , the identity. We denote this as  $O(g)$ .

### Definition 1.6: Order of a Group $G$ , denoted by $|G|$ .

The cardinality of the group.

### Theorem 1.7

If  $G$  is a group and  $a$  an element in  $G$  with  $O(a) = n$ , then  $a^m = 1$  if and only if  $n|m$

**Proof for Theorem.**

$\implies$  ) Given  $O(a) = n$  we have  $n$  to be the smallest natural number so that  $a^n = 1$ . If we have that  $a^m = 1$ , and  $n \nmid m$ , then  $m = qn + r$  where  $0 < r < n$ . Therefore,  $a^r \neq 1$ . We have that  $a^{qn+r} = a^{qn} \cdot a^r = a^r \neq 1$  which is absurd.

$\impliedby$  ) Given  $n|m$ , obviously then  $a^m = 1$ .  $\blacksquare$

### Theorem 1.8

If  $O(a) = n$ , then  $O(a^m) = \frac{n}{\gcd(m,n)}$ .

**Proof for Theorem.**

We understand that  $\frac{n}{\gcd(m,n)}$  is atleast a candidate, since we can see clearly that  $(a^m)^{\frac{n}{\gcd(m,n)}} = (a^n)^{\frac{m}{\gcd(m,n)}} = 1$ . Suppose  $k$  is the order, with  $k < \frac{n}{\gcd(m,n)}$  so that  $a^{mk} = 1$ . From the previous theorem, we see that  $n|mk$ . i.e,  $n\delta = mk \implies \frac{n}{\gcd(m,n)}\delta = \frac{m}{\gcd(m,n)}k$ . Note that  $\frac{n}{\gcd(m,n)}$  and  $\frac{m}{\gcd(m,n)}$  share no common divisors, for if they did, then that, multiplied with the

actual gcd would yield a divisor larger than the gcd. Hence,  $\gcd(\frac{n}{(m,n)}, \frac{m}{(m,n)}) = 1$ . This means, from previous lemmas, that  $\frac{n}{(m,n)}$  divides  $k$ . This is, ofcourse, absurd. ■

### Theorem 1.9: Real Numbers $\text{mod}(1)$

Let  $G := \{x \in \mathbb{R} : 0 \leq x < 1\}$ . Define  $x \circ y = \{x + y\}$  where  $\{\cdot\}$  denotes the fractional part (and  $[\cdot]$  denotes the integral part, or the GIF). Then,  $G$  is an abelian group under  $\{\circ\}$

#### *Proof for Theorem.*

Closure of  $x \circ y$  is pretty obvious. We freely use  $\{\cdot\}$ ,  $\text{frac}\{\cdot\}$  and  $\cdot$  interchangeably. We consider  $x \circ (y \circ z) = \text{frac}(\underline{x} + [x] + \text{frac}(y + z)) = \text{frac}(\underline{x} + [x] + \text{frac}(\underline{y} + [y] + \underline{z} + [z])) = \text{frac}(\underline{x} + \text{frac}(\underline{y} + \underline{z})) = \text{frac}(\underline{x} + (\underline{y} + \underline{z}) - [\underline{y} + \underline{z}]) = \text{frac}(\underline{x} + \underline{y} + \underline{z})$

Now consider  $(x \circ y) \circ z = \text{frac}(\text{frac}(\underline{x} + \underline{y}) + \underline{z} + [z]) = \text{frac}(\text{frac}(\underline{x} + \underline{y}) + \underline{z}) = \text{frac}((\underline{x} + \underline{y}) - [\underline{x} + \underline{y}] + \underline{z} + [z]) = \text{frac}(\underline{x} + \underline{y} + \underline{z})$ . Hence we see  $\circ$  is associative. Trivial to note that the identity element is  $\underline{0}$  and the inverse for every  $\underline{x}$  is  $\underline{-x}$ . ■

### Theorem 1.10: Group of the $n$ -th roots of unity

Suppose  $G := \{z \in \mathbb{C} : z^n = 1 : \text{for some } n\}$

#### *Proof for Theorem.*

We want to solve  $z^n = 1$ . Applying polar coordinates we have  $|z|^n(\text{cis}(\theta))^n = 1$ . Taking mod gives us  $|z| = 1$ . We have to solve for, then,  $\text{cis}(\theta)^n = 1$ . It is simple computation to see that  $\text{cis}(\theta)^n = \text{cis}(n\theta)$  which gives us  $\text{cis}(n\theta) = 1$ . The solutions to this are  $\theta = \frac{2\pi k}{n}$  for any integer  $k$ . Therefore, the solutions to  $z^n = 1$  are of the form  $z = \text{cis}(\frac{2\pi k}{n})$ . We assume a modulo  $2\pi$  structure, i.e, we classify solutions of the kind  $\theta + 2k\pi$  in the class of  $\theta$ . We see then, that for  $k \leq n - 1$ , each solution is unique. If we let  $\omega = \text{cis}(\frac{2\pi}{n})$ . We see that all the other elements are generated by  $\omega$  since for  $k = 2$ , we just have  $\omega^2$  (from the way cis powers work). Till  $k = n - 1$ , we have unique solutions generated by  $\omega$  given by  $1, \omega, \omega^2 \dots \omega^{n-1}$ . We see that when  $k = n$  we get  $\theta = \frac{2\pi n}{n} = 2\pi \equiv 0 \text{mod}(2\pi)$ . For  $n + j$  where  $j < n$ , we see that  $\theta = \frac{2\pi(n+j)}{n} = 2\pi + \frac{2\pi j}{n} \equiv \frac{2\pi j}{n} \text{mod}(2\pi)$ . Hence, all the unique solutions are  $1, \omega, \omega^2 \dots \omega^{n-1}$ .

To see that this is a group under multiplication, we note that  $\omega^x(\omega^y\omega^z) = (\omega^x\omega^y)\omega^z = \omega^{(x+y+z) \text{mod}(n)}$ . Every element has an inverse since  $\omega^j \cdot \omega^{n-j} = 1$  (1 is the identity here since  $1\omega^j = \omega^j \cdot 1 = \omega^j$ )

$G$ , though a group under multiplication, is not one under addition. For example, consider  $1 + 0i \in G$ .  $1 + 1 = 2 + 0i$  which is not in  $G$ . ■

**Fact 1.11**

If  $a, b \in G$ , then  $|ab| = |ba|$

**Proof.** We have  $(ab)(ab) \cdots (ab) = (ab)^n = e$ . Rearranging the brackets we get  $a(ba)(ba) \cdots (b) = a(ba)^{n-1}(b) = e$  which gives  $(ba)^{n-1} = a^{-1}b^{-1} = (ba)^{-1}$  which eventually gives  $(ba)^n = e$ . Therefore, if  $m$  was the order of  $ba$ , then  $m|n$ . Similarly we can re-run the argument in the other direction starting with  $(ba)^m = e$  to get  $n|m$ . This gives  $n = m$ .  $\square$

**Fact 1.12**

If  $x^2 = 1$  for every  $x \in G$ , then  $G$  is abelian

**Proof.** Let  $ab \neq ba \implies a^2b = b \neq a(ba)$ . This implies  $b^2 = e \neq (ba)^2 \implies 1 \neq 1$ . Absurd.  $\square$

**Fact 1.13**

Any finite group of even order contains an element  $a$  with order 2.

**Proof.** Suppose that for every non-identity element  $x$  we have  $o(x) = p \neq 2$  with  $p \geq 3$ . We can then notice that for every element,  $x \neq x^{-1}$ . Hence, every element along with its inverses would form an even sized set (due to uniqueness of inverses, none overlap). Hence, adding identity to this would make the group odd.  $\square$

**Example :**  $G = \{1, a, b, c\}$  is  $|G| = 4$  with 1 identity. Say no element has order 4. Then this group has a unique multiplication table

We can immediately fill up the initial parts:

x	1	a	b	c
1	1	a	b	c
a	a	x	x	x
b	b	x	x	x
c	c	x	x	x

Since this is a finite group of order 4, there should be atleast one element with order 2. We WLOG select that element to be  $b$  so that  $b^2 = 1$ . Is  $ab = a$  or  $b$ ? Nope, since that would make either one identity. So  $ab = c$ . Is  $ba = a$  or  $b$ ? In much the same way, we conclude  $ba = ab = c$ .  $b(ba) = bc = a$  and  $(ab)b = ab^2 = cb$ . Hence  $bc = cb = a$ . So far we got: (This is applicable for any group of size 4, since we did not use the property that this group has no element with order 4.)

x	1	a	b	c
1	1	a	b	c
a	a	x	c	x
b	b	c	1	a
c	c	x	a	x

(**The Klein Route**) Is  $a^2 = b$ ? Can't be, because then, since  $b^2 = 1$ , we'd have  $a^4 = 1$  which is against hypothesis. Hence  $a^2 = 1$ , or  $a^2 = c$ . Likewise, we can conclude that  $c^2 = 1$  or  $c^2 = a$  (Ask the same questions, is  $c^2 = b$ ? No). Suppose  $a^2 = 1$  and  $c^2 = a$ . That would make  $c^4 = 1$ , which is against hypothesis. Hence, if  $a^2 = 1$  then  $c^2 = 1$  as well. Likewise, if  $c^2 = 1$ , then  $a^2 = 1$  as well. Suppose neither, i.e,  $c^2 = a$  and  $a^2 = c$ . Then  $c^4 = a^2 = c$  and  $a^4 = c^2 = a$ . We have  $a^3 = 1$  and  $c^3 = 1$ .  $(ba)a^2 = b$  which means  $ca^2 = b \implies c^2 = b$ . But  $c^2 = a$ . Absurd. Hence, this scenario is impossible. Hence, for the Klein route,  $a^2 = c^2 = 1$ .

Question for  $ac$  and  $ca$ , then arises. Is  $ac = 1$ ? That would mean  $a^2c = 1c = a$ , absurd. Hence,  $ac = b$ . Similarly, is  $ca = 1$ ? we would then have  $c = a$  again. Therefore,  $ac = ca = b$ . This completes the Klein Route:

<b>x</b>	<b>1</b>	<b>a</b>	<b>b</b>	<b>c</b>
<b>1</b>	1	a	b	c
<b>a</b>	a	1	c	b
<b>b</b>	b	c	1	a
<b>c</b>	c	b	a	1

(**The  $\mathbb{Z}/4\mathbb{Z}$  Route**) Suppose that  $G$  has an element of order 4. Since the size of the cyclic subgroup of this element is 4 as well, this group is cyclic. WLOG, assume that  $G = \langle a \rangle$ . Then every element is  $1, a = a, a^2 = b, a^3 = c$ . We have (for a general 4 membered group)

<b>x</b>	<b>1</b>	<b>a</b>	<b>b</b>	<b>c</b>
<b>1</b>	1	a	b	c
<b>a</b>	a	x	c	x
<b>b</b>	b	c	1	a
<b>c</b>	c	x	a	x

Since the group is cyclic, we can immediately write  $a^2 = b$ . Since  $a^3 = c$ ,  $a^6 = a^2 = c^2 = b$ . We can write that in as well. All that is left is  $ac$  and  $ca$ . Let us rule out the obvious:  $ac \neq a$ ,  $ca \neq a$ ,  $ac \neq c$ ,  $ca \neq q$ . Is  $ac = b$ ? That would mean  $a^4 = b$ , which makes  $b = 1$ . Same way,  $ca \neq b$ . Hence,  $ac$  and  $ca$  have only one option left, 1. We can fill that in to get the  $\mathbb{Z}/4\mathbb{Z}$  isomorph:

<b>x</b>	<b>1</b>	<b>a</b>	<b>b</b>	<b>c</b>
<b>1</b>	1	a	b	c
<b>a</b>	a	b	c	1
<b>b</b>	b	c	1	a
<b>c</b>	c	1	a	b

Note that Klein is the unique 4 membered group with no element of order 4.  $\mathbb{Z}/4\mathbb{Z}$  isomorph is the unique group with one element with order 4. ■

### Definition 1.14: Subgroup

A set  $H \subseteq G$  of group  $G$  is said to be a subgroup if  $H$  is itself a group, i.e, follows ASCII axioms under the operation inherited from  $G$ . If  $H$  is a proper subgroup of  $G$ , then we denote it by  $H < G$ . Else,  $H \leq G$

### Definition 1.15: Cyclic Subgroup

Suppose  $G, \cdot$  is a group, with an element  $a$ . Suppose  $\langle a \rangle$  is a subgroup of  $G$  that contains  $a$ . Must definitely have  $e$  which is notated to be  $a^0$ . It must then definitely have  $a \cdot a, a \cdot a \cdot a$  and so on till  $a^n$  where  $o(a) = n$ . If no order exists, we take it to be  $\forall n \in \mathbb{Z}. \langle a \rangle := \{a^n : n \in \mathbb{Z}\}$  This is enough for it to be a group:

$e = a^0$  is in the group. For every  $b$ , i.e,  $a^k$  in the group,  $a^{-k}$  is also in the group by definition. It obeys ASCII.

**Fact:**  $\langle a \rangle$  is the smallest subgroup of  $G$  containing  $a$ . Analogous to *span*.

#### *Example : Some groups cyclically generated*

$\mathbb{Z}/n\mathbb{Z}$  as an additive group is generated by 1. That is,  $\langle 1 \rangle$  is precisely  $\mathbb{Z}/n\mathbb{Z}$ .

$n$ -th roots of unity:  $1, \omega, \omega^2 \dots \omega^{n-1}$ , is generated by  $\langle \omega \rangle$ . ■

### Fact 1.16

If  $O(a) = n < \infty$  for  $a \in G$  and  $G = \langle a \rangle$ , then  $|G| = n$

### Theorem 1.17

Suppose  $G = \langle a \rangle$  with  $O(a) = n < \infty$ , then  $\langle a^j \rangle = G$  if and only if  $\gcd(j, n) = 1$

#### *Proof for Theorem.*

$\Rightarrow$  ) Since  $O(a) = n$ , the order of  $a^j$  is given by  $n/\gcd(j, n)$ . If  $\gcd(j, n) \neq 1$ , then clearly the orders are different, implying the groups they generate will be of different cardinality.

$\Leftarrow$  ) Suppose  $\gcd(j, n) = 1$  with  $O(a) = n$  and  $G = \langle a \rangle$ . Then  $O(a^j) = n$ . Note that  $\langle a^j \rangle \leq \langle a \rangle$  since every element of the former is in the latter. But the order of each is the same, whilst being finite. Therefore,  $\langle a^j \rangle = \langle a \rangle$  ■

#### *Example : An application of the previous theorem to $\mathbb{Z}/n\mathbb{Z}$*

We know that  $\langle 1 \rangle = \mathbb{Z}/n\mathbb{Z}$  under addition. Order of 1 is  $n$  here. Consider another element  $j \in \mathbb{Z}/n\mathbb{Z}$  so that  $\gcd(j, n) = 1$ . Then order of  $j$  is  $n$ . As such,  $\langle j \rangle = \mathbb{Z}/n\mathbb{Z}$ . All the elements of  $\mathbb{Z}/n\mathbb{Z}$  that generate  $\mathbb{Z}/n\mathbb{Z}$  belong to the multiplicative  $\mathbb{Z}/n\mathbb{Z}^*$  group. ■

### Corollary 1.18

The number of generators for a cyclic group of order  $n$  is  $\phi(n)$ .

### Theorem 1.19

Subgroup of a cyclic group is cyclic.

#### *Proof for Theorem.*

Let  $G = \langle a \rangle$ . Suppose  $H \leq G = \langle a \rangle$  is the subgroup of  $G$ .

Say  $e, a^{j_1}, a^{j_2} \dots a^{j_n} \dots$  are in  $H$ . Case (1), if there exists a finite subcollection of these indices so that their  $\gcd$  is 1. Let them be  $j_1, j_2 \dots j_n$ . This means  $\gcd(j_1, j_2 \dots j_n) = 1$  and from generalised bezout, we have  $x_1 j_1 + x_2 j_2 \dots x_n j_n = 1$  whence we see that  $H$  has to be  $G$  necessarily.

The other case, case (2) is that for every finite subcollection of  $\{j_1, j_2 \dots\}$ , their  $\gcd$  is not 1. Does this mean that  $\gcd(j_1, j_2 \dots (\text{till } \infty))$  is not 1? i.e, do they all share one common factor? Suppose there exists  $j'_1$  and  $j'_2$  so that they do not share a common factor. This would mean that  $\gcd(j'_1, j'_2) = 1$ , which contradicts the hypothesis of case (2). Hence, in this case, every  $j$  is a multiple of some number  $\gamma$  which makes  $H = \langle a^\gamma \rangle$ .

**Alt Proof:(Similar)** Let  $m$  be the smallest index so that  $a^m \in H$ . We claim  $a^m$  is the cyclic generator of  $H$ . Suppose  $a^n$  where  $n > m$  is in the group  $H$ . Then  $a^n = a^{mq+r}$  where  $0 \leq r < m$ . This means  $a^n \cdot (a^m)^{-q} = a^r$ . By virtue of being a group which is closed, we see that  $a^r \in H$ . If  $r \neq 0$ , we get a contradiction. Hence,  $r = 0$ . Therefore, every element is  $(a^m)^{\text{something}}$ . ■

### Corollary 1.20

If  $G$  is a cyclic group generated by  $a$  and a subgroup has two elements  $a^j$  and  $a^k$ , then this subgroup would necessarily have to be the bigger group  $G$  if  $(j, k) = 1$ .

#### *Proof for Corollary.*

Let  $G = \langle a \rangle := \{a^n : n \in \mathbb{Z}\}$  where  $a \in G$  (the generator of  $G$ ). Consider a  $H$  subgroup of  $G$ , given by elements  $a^j : j \in \{n_1, n_2, \dots\}$  where  $n_1, n_2, \dots$  is a sequence of integers. Note that, since  $a^{n_1}$  is in  $H$ ,  $(a^{n_1})^q$  for  $q \in \mathbb{Z}$  is also in  $H$ . Suppose that there exists  $n_j$  and  $n_k$  indices so that  $\gcd(n_j, n_k) = 1$ . This means that  $xn_j + yn_k = 1$ . Hence,  $(a^{n_j})^x (a^{n_k})^y = a$  Which would make  $a^{xn_j + yn_k}$  the cyclic generator of  $G$  itself, which would force  $H$  to become  $G$ . ■

#### *Example :*

Consider  $G = \mathbb{Z}/n\mathbb{Z} = \langle 1 \rangle$ . Consider a subgroup that is known to contain 2 and 3. In notation,  $3 = 1^3$  and  $2 = 1^2$ , and  $\gcd(3, 2) = 1$ . This means that This subgroup must be



$\mathbb{Z}/n\mathbb{Z}$  itself. ■

**Example :**

Consider  $\mathbb{Z}/n\mathbb{Z} = \langle 1 \rangle$ . Let a subgroup be such that it contains 2, 4 and 3, 6. The  $\gcd(2, 4) = 2 \neq 1$  and the  $\gcd(3, 6) = 3 \neq 1$ , but  $\gcd(2, 1) = 1$ . This means that this subgroup must necessarily be the main group. ■

**Lemma 1.21**

If a cyclic group is infinite, then every subgroup is infinite (except the trivial subgroup)

**Proof for Lemma**

Suppose  $G = \langle a \rangle$  that is infinite. i.e,  $a$  has no order. Consider a subgroup that is non trivial, i.e, has an element  $a^j, j \neq 0$ . If this group is of finite order, then  $a^j$  must be of finite order, obviously.  $O(a^j) = q$  which means  $a^{qj} = 1$  which is absurd. ■

## 1.1 The Dihedral Group $D_{2n}$

Given an  $n$  – gon that is regular, we define the symmetries on it by permutation maps or bijective maps from  $\{1, 2, 3 \cdots, n\}$  into itself.

### Definition 1.22: Rotation $r$

$r : \{1, 2, 3 \cdots n\} \rightarrow \{1, 2, \cdots, n\}$  is defined as

$$\begin{aligned} 1 &\xrightarrow{r} 2 \\ 2 &\xrightarrow{r} 3 \\ &\vdots \\ n-1 &\xrightarrow{r} n \\ n &\xrightarrow{r} 1 \end{aligned}$$

Whose inverse is, as one can guess:

$$\begin{aligned} 2 &\xrightarrow{\text{inverse}(r)} 1 \\ 3 &\xrightarrow{\text{inverse}(r)} 2 \\ &\vdots \\ n &\xrightarrow{\text{inverse}(r)} n-1 \\ 1 &\xrightarrow{\text{inverse}(r)} n \end{aligned}$$

**Definition 1.23: Symmetry, or flipping, or mirror whatever**

$s$  is defined as  $s : \{1 \cdots n\} \rightarrow \{1 \cdots n\}$  as follows:

$$\begin{aligned} 1 &\xrightarrow{s} 1 \\ 2 &\xrightarrow{s} n \\ 3 &\xrightarrow{s} n-1 \\ &\vdots \\ n &\xrightarrow{s} 2 \end{aligned}$$

Note that,  $s^2 = 1$

**Some Properties of  $D_{2n}$**  The symmetries of  $D_{2n}$  are the functions listed above. Note the following:

1.  $1, r, \dots, r^{n-1}$  form distinct elements.  $|r| = n$  since  $r^n = 1$
2.  $r$  follows  $\mathbb{Z}/n\mathbb{Z}$  structure in that,  $r^j$  has, as its inverse,  $r^{n-j}$ . It obeys similar modular structure.
3.  $s^2 = 1$
4.  $rs = sr^{-1}$ . Note that  $rs$  amounts to "Pivoting" about 2 and flipping the dihedron, which can be achieved by reverse rotating, i.e,  $r^{-1}$  first, and then flipping, i.e  $sr^{-1}$ . Hence,  $rs = sr^{-1}$ .
5. Since the inverse elements of  $r^i$  are  $r^{-1}$ , the previous result can be more generally written as  $(r^i)s = sr^{-i}$ . In a spoon feedy way we see that  $rs = sr^{-1} \implies r(rs) = r^2s = r(sr^{-1}) = (rs)(r^{-1}) = (sr^{-1}r^{-1}) = sr^{-2}$ . Keep going as such.
6. The elements  $1, r, r^2, \dots, r^{n-1}$  constitute the subgroup of rotations, each one corresponding to a rotation of  $\frac{2j\pi}{n}$ .
7. The elements  $s, rs, r^2s, \dots, r^{n-1}s$  correspond to "pivoting" the  $j$ -th number and flipping about that. These on their own don't constitute a group for,  $(r^ns)(r^ms) = r^n(sr^m)s = r^n(r^{-m})$  which falls into the rotation group.
8. Note that  $s \neq r^i$  for any  $i$ . This ought to be intuitively clear.
9.  $sr^i \neq sr^j$  since flipping about different pivots achieves a different structure, one that is different by rotations alone (obviously).
10. The set  $\{1, r, r^2, \dots, r^{n-1}; s, rs, r^2s, \dots, r^{n-1}s\}$  Constitutes a group, of order  $2n$ . This is stated formally in the next theorem, with proof.

**Theorem 1.24**

The set  $\{1, r, r^2 \dots r^{n-1}; s; rs, r^2s, \dots r^{n-1}s\}$  Constitutes a group, of order  $2n$ .

*Proof for Theorem.*

We note that  $1, r, r^2, \dots r^{n-1}$  all obey ASCII. So does  $s$ , since it is self inverse (The identity here is the identity function). Consider the permutations of the kind  $r^j s$ . These have inverses as well, for if we compose this with  $r^{n-j}$ , we would have  $r^{n-j} \circ (r^j s) = s$ . If we compose this still, with  $s$ , we get 1. The total composition on  $r^j s$  would have been  $sr^{n-j}$ . Infact, these elements too are self inverses. Easier way to see this is  $(r^i s)(r^i s) = r^i (sr^i) s = r^i (r^{-i} s) s = 1$ . These also, then follow ASCII. ■

**1.2 More basix, Homomorphisms, isomorphisms, centers****Definition 1.25: Homomorphism**

Let  $\langle G, \cdot \rangle$  and  $\langle H, * \rangle$  be two groups. We say a function  $\phi : G \rightarrow H$  is a **homomorphism** if  $\forall x, y \in G, \phi(x \cdot y) = \phi(x) * \phi(y)$ .

Some notable features of a homomorphism are:

1.  $\phi(e_G) = e_H$
2.  $\phi(a^{-1}) = \phi(a)^{-1}$

**Definition 1.26: Group Isomorphism**

A homomorphism from  $\langle G, \cdot \rangle$  to  $\langle H, * \rangle$  is a group isomorphism if it is bijective.

**Theorem 1.27**

Let  $\langle G, \cdot \rangle$  be a group. Consider  $*$  :  $G \times G \rightarrow G$  a binary operation defined as

$$a * b = b \cdot a$$

. Then this is a group isomorphism from  $G \cdot$  to  $G, *$ .

*Proof for Theorem.*

Consider  $\phi : G \rightarrow G$  given by  $\phi(a) = a^{-1}$ . This is a bijection since every  $a$  maps to a unique  $a^{-1}$ , and vice versa. Consider  $\phi(a \cdot b) = b^{-1} \cdot a^{-1} = \phi(b) \cdot \phi(a) = \phi(a) * \phi(b)$ , which makes  $\phi$  a homomorphism, hence, an isomorphism. ■

**Definition 1.28: Centralizer of  $a \in G$** 

**Centralizer** of an element  $a$  in group  $G$  is defined as

$$H_a := \{x \in G : xa = ax\}$$

or, the set of all elements in  $G$  that commute with  $a$ .

**Lemma 1.29**

Centralizer of  $a \in G$  is a subgroup of  $G$

***Proof for Lemma***

$e$  is obviously in  $H_a$ . Suppose some  $b \in H_a$ , i.e,  $ab = ba$ . Consider  $abb^{-1} = a = bab^{-1} \implies b^{-1}a = ab^{-1}$  which means that if  $b \in H_a$ ,  $b^{-1}$  is also in  $H_a$ . That it is closed and associative is also obvious (since  $ba = ab$  and  $ca = ac$  would mean  $bca = abc$ ). ■

**Definition 1.30: Centralizer of a subset  $S \subset G$** 

**Centralizer of a set  $S$**  in  $G$  is defined as

$$H_S := \{x \in G : xz = zx \forall z \in S\}$$

**Lemma 1.31**

Centralizer of a set  $S \subset G$  is a subgroup of  $G$

***Proof for Lemma***

Again, obviously  $e$  is in  $H_S$ . Let  $b \in H_S$ , i.e,  $bx = xb, \forall x \in S$ .  $b^{-1}bx = x = b^{-1}xb \implies xb^{-1} = b^{-1}xb$  which gives  $xb^{-1} = b^{-1}x, \forall x \in S$ . Hence,  $b^{-1} \in H_S$ . Suppose  $a, b \in H_S$ , i.e,  $ax = xa, \forall x \in S$  and  $bx = xb, \forall x \in S$ .  $a(bx) = a(xb) = (ax)b = x(ab)$  which makes  $ab \in H_S$ . ■

**Definition 1.32: Center of a group  $G$** 

**The center of a group  $G$**  is defined as the centralizer of  $G$ , i.e

$$H_G := \{x \in G : xz = zx, \forall z \in G\}$$

by the previous lemma, this is also a group.

**Lemma 1.33**

Center of a group  $G$  is an abelian subgroup.

*Proof for Lemma*

$H_G := \{x \in G : xz = zx, \forall z \in G\}$  is easily seen to be a group. Consider  $k_1, k_2 \in H_G$ , and consider  $k_1 \cdot k_2 \in H_G$  (which exists in  $H_G$  due to closure). Treating  $k_1$  as an element in  $H_G$  and  $k_2$  as an element in  $G$ , we note that by definition,  $k_1(k_2) = k_2k_1$ . Hence, the group is abelian. ■

**Definition 1.34: Normal Subgroup**

A subgroup  $H \leq G$  is said to be *normal* if for every element  $h \in H$  and for every element  $g \in G$ ,  $ghg^{-1} \in H$ . This essentially says (see next notation) that  $\forall g \in G$ ,  $gHg^{-1} \subseteq H$ . But we can also say equivalently that  $\forall g \in G$ ,  $gHg^{-1} = H$  by the following argument:

Let  $g$  be arbitrary. We ask the question, given any  $h \in H$ , can it be written in the form  $gh'g^{-1}$  for some  $h' \in H$ ? For that would guarantee the back inclusion.  $h \in H$  implies  $h^{-1} \in H$  which implies  $gh^{-1}g^{-1} \in H$  which implies  $g^{-1}hg \in H$  for any  $h \in H$ . This means  $g^{-1}hg = h'$  for some  $h'$  which gives  $h = gh'g^{-1}$  which gives us the back inclusion.

**Definition 1.35: Notation:  $gH$ ,  $Hg$  and  $gHg^{-1}$  for a set  $H$** 

1.  $gH := \{gh : h \in H\}$
2.  $Hg := \{hg : h \in H\}$
3.  $gHg^{-1} := \{ghg^{-1} : h \in H\}$

**Definition 1.36: Normalizer**

The normalizer  $N_G(S) := \{z \in G : zSz^{-1} = S\}$  which is subtle, as it means not only that for every  $z \in N_G(S)$  it is that for every  $s \in S$ ,  $zsz^{-1} \in S$ , but also another condition that for every  $s \in S$ , there exists  $s' \in S$  so that  $s = zs'z^{-1}$ .

We denote the normalizer of a set  $S$  as  $N_G(S)$  which tells us with respect to what group we are normalizing  $S$ .

**Remark.**

Note that instead of stating the back inclusion as " $\forall s \in S, \exists s'$  so that  $s = xs'x^{-1}$ " we can also equivalently say  $\forall s \in S, x^{-1}sx \in S$ .

**Theorem 1.37**

Normalizer  $N_G(S)$  of a set  $S$  is a group

**Proof for Theorem.**

Consider  $N_G(S) := \{g \in G : gSg^{-1} = S\}$ .  $e$  clearly belongs in  $N_G$  since  $ese^{-1} = s$  and for every  $s \in S, \exists s$  such that  $s = ese^{-1}$ . Let  $x$  and  $y$  be in  $N_G(S)$ . This means that for any  $s \in S, xsx^{-1} \in S$  and  $ysy^{-1} \in S$ . Does  $x(ysy^{-1})x^{-1} \in S$ ? Yes, obvious from the bracketing. We know that (since  $x, y \in N_G(S)$ ) if  $s \in S, \exists s', s'' \in S$  so that  $s = xs'x^{-1}$  and  $s = ys''y^{-1}$ . Now we ask, for any given  $s \in S$ , does there exist a  $t \in S$  so that  $s = x(yty^{-1})x^{-1}$ ? For the given arbitrary  $s$ , there exists  $s'$  so that  $s = xs'x^{-1}$ , and for  $s'$ , there exists  $s''$  so that  $s' = ys''y^{-1}$  which means  $s = xys''y^{-1}x^{-1}$  which means  $xy$  is also in  $N_G(S)$ . All that is left is the inverse. Let  $x \in N_G(S)$  which means that  $\forall s, xsx^{-1} \in S$  and for all  $s, \exists s'$  so that  $s = xs'x^{-1}$ . For every  $s$ , there exists  $s' \in S$  so that  $s = xs'x^{-1}$  which means  $x^{-1}sx = s' \in S$  which means for all  $s, x^{-1}sx \in S$ . If  $s \in S$ , does there exist  $s' \in S$  so that  $s = x^{-1}s'x$ ? Or rephrased, does there exist  $s'$  so that  $s' = xsx^{-1}$ ? Obviously, if  $s$  is in  $S$ , there exists  $xsx^{-1}$  so that  $xsx^{-1} = s' \in S$  which means  $s = x^{-1}s'x$  which completes the proof. ■

**Theorem 1.38**

$\langle S \rangle \triangleleft N_G(S)$

And  $N_G(H)$  is the largest subgroup of  $G$  which  $H$  is *normal* to.

**Proof for Theorem.**

First we tackle whether  $\langle S \rangle \triangleleft N_G(S)$ . If  $S$  is itself a group, then our job is easier.  $\langle S \rangle = S$  in that case.  $N_G(S) := \{g \in G : gSg^{-1} \subseteq S \iff gSg^{-1} = S\}$  which means that for every element in  $N_G(S)$ , and for every element  $h$  in group  $S$ , we have  $ghg^{-1} \in S$  which makes  $S$  a normal subgroup of  $N_G(S)$ . Say  $S \triangleleft K$  for some subgroup  $K$ , which means for every element  $k \in K, kSk^{-1} \subseteq S \iff kSk^{-1} = S$  (since  $S$  is a group). This means that every point  $k$  of  $K$  is actually a point of  $N_G(S)$  which makes  $N_G(S)$  the largest subgroup  $S$  is normal to.

If  $S$  is just a set,  $\langle S \rangle := \{a_1^{e_1}a_2^{e_2} \cdots a_k^{e_k} : \{a_1, a_2 \cdots a_k\} \in S, e_1, e_2 \cdots e_k \in \{-1, 1\}\}$ . Let  $s$  be an arbitrary element in  $\langle S \rangle$  of the form  $a_1^{e_1}a_2^{e_2} \cdots a_k^{e_k}$ . Let  $z$  be an arbitrary element in  $N_G(S)$ . This means that for every element  $s \in S$ , we have  $zsz^{-1} \in S$  and for every  $s \in S$ , there exists  $s' \in S$  so that  $s = zs'z^{-1}$  (this needn't be said since, if  $zsz^{-1} \in S$ ,  $z^{-1}sz \in S$  too, this comes straight from the remark). We want to show that  $\langle S \rangle \triangleleft N_G(S)$  which means that for every element  $z$  of  $N_G(S)$ , and for every element  $x$  of  $\langle S \rangle$ ,  $zxz^{-1} \in \langle S \rangle$  (or  $x\langle S \rangle x^{-1} = \langle S \rangle$ ). If  $a_j$  (with positive exponent) is in  $S$ , then  $za_jz^{-1}$  is also in  $S$ . If  $a_j$  is in  $S$  but has a negative exponent, then  $za_jz^{-1} \in S$  (from normalizer condition, it also means  $z^{-1}a_jz \in S$ ) which means  $z(a_j)^{-1}z^{-1} \in \langle S \rangle$ . So, if given arbitrary  $s = a_1^{e_1}a_2^{e_2} \cdots a_k^{e_k} \in \langle S \rangle$ , and an element  $z \in N_G(S)$ , We can decompose the product as

$a_1^{e_1} z^{-1} z a_2^{e_2} z^{-2} \dots a_{k-1}^{e_{k-1}} z^{-1} z a_k^{e_k} \in \langle S \rangle$ . If we premultiply and post multiply the previous expression with  $z$  and its inverse, we get  $z(a_1^{e_1} z^{-1} z a_2^{e_2} z^{-2} \dots a_{k-1}^{e_{k-1}} z^{-1} z a_k^{e_k})z^{-1}$  which will then be a product of terms of the kind  $z a_j z^{-1}$  which are in  $\langle S \rangle$ , which means finally that  $z s z^{-1} \in \langle S \rangle$ . Hence, we are done with showing that  $\langle S \rangle \triangleleft N_G(S)$ . Suppose  $\langle S \rangle \triangleleft K$  for some subgroup  $K$ . This means that for every element  $k \in K$  and every  $s \in \langle S \rangle$ ,  $k s k^{-1} \in \langle S \rangle$ .

Also note that  $N_G(S) \leq N_G(\langle S \rangle)$  since if  $g$  is such that  $\forall s \in S$   $g s g^{-1} \in S$  and  $g^{-1} s g \in S$ , then  $g^{-1} s^{-1} g \in \langle S \rangle$  so  $g$  would be an element in  $N_G(\langle S \rangle)$ . ■

### Theorem 1.39

A subgroup  $H$  is normal to  $G$  (denoted  $H \triangleleft G$ ) if and only if  $N_G(H) = G$ .

*Proof for Theorem.*

### Something on Cosets and Lagrange's Theorem

Let  $G$  be a group and  $H$  be a subgroup of  $G$ . Define the equivalence relation  $\equiv$  on  $G$  as follows:  $a \equiv b$  if and only if  $ab^{-1} \in H$ . This is clearly an equivalence relation since  $a \equiv a$ , and  $a \equiv b$  gives us  $ab^{-1} = h \in H$  which gives us  $h^{-1} = ba^{-1} \in H$  which means  $b \equiv a$ . Similarly easy to see that if  $a \equiv b$ ,  $b \equiv c$ , then  $a \equiv c$ .

The equivalence classes of this equivalence relation are denoted  $[b]$  which constitutes the set of all  $x \in G$  so that  $x \equiv b$  or  $xb^{-1} \in H$  (or  $bx^{-1} \in H$ ).

**Definition:(Left Coset)** We digress to define what is called a **left coset** of  $H \leq G$  given an element  $b \in G$  (denoted  $bH$ ).

$$bH := \{z \in G : \exists h \in H : z = bh\}$$

or equivalently

$$bH := \{bh : h \in H\}$$

**Definition:(Right Coset)** Similarly, a **Right Coset** of  $H \leq G$  given an element  $a \in G$  (denoted  $Ha$ ) is defined as

$$Ha := \{z \in G : \exists h \in H : z = ha\}$$

or equivalently

$$Ha := \{ha : h \in H\}$$

From this definition, it is clear that the set of all equivalence classes are precisely the left



cosets of  $H$ . i.e,  $[b]$  is the set of all  $x \in G$  so that  $x \equiv b$  which means  $xb^{-1} = h \in H$  or equivalently  $x = bh, h \in H$  which means  $x \in bH$ . Every element in  $[b]$  is an element in  $bH$ , and conversely, consider an element  $z \in bH$  which means  $z = bh, h \in H$  which means immediately that  $z \equiv b$  or  $z \in [b]$ . Consider two elements in the set of all distinct equivalence classes,  $[a]$  and  $[b]$ . Note that  $[a] = aH$  and  $[b] = bH$ . Note here that there exists a bijective map from  $[a]$  to  $[b]$ , given by  $\psi : aH \rightarrow bH$  defined by  $ah \mapsto bh$ .  $\psi(ah_1) = \psi(ah_2) \implies bh_1 = bh_2$  or  $h_1 = h_2 \implies ah_1 = ah_2$ , whence injectivity is clear. Consider  $bh \in bH$ . There exists  $ah$  so that  $\psi(ah) = bh$  which means that  $\psi$  is bijective. This means that  $|[a]| = |[b]|$  i.e, the cardinality of  $[a]$  is the same as the cardinality of  $[b]$ .

Note that, if we look at  $[e]$ , i.e, the set  $eH := \{eh = h : h \in H\} = H$ , we see from the previous result that for whatever  $a \in G$ ,  $|[a]| = |aH| = |H|$ . The size of any equivalence class is the size of the subgroup itself.

Note that the collection of distinct equivalence classes form a partition of the entire group  $G$ . If  $G$  is finite, say, of order  $n$ , then the sum of the cardinalities of all the equivalence classes ought to give us  $n$ . Formally this means, suppose  $X = \{[a] : a \in G\}$  be the collection of all (distinct) equivalence classes. Then

$$\sum_{[a] \in X} |[a]| = |G|$$

But since  $|[a]| = |aH| = |H|$ , we can rewrite the above as:

$$\sum_{i=1}^{|\{[a]: a \in G\}|} |H| = |G|$$

which implies

$$|\{[a] : a \in G\}| \cdot |H| = |G|$$

This is Lagrange's theorem:

### Theorem 1.40: Lagrange's Theorem

Suppose  $G$  is a given finite group, and  $H$  a subgroup of  $G$ . Then,  $|H| \mid |G|$

*Proof for Theorem.*

We saw from the previous analysis that for some integer  $k$ ,  $k|H| = |G|$ . This means that for any subgroup  $H$  of finite group  $G$ ,  $|H|$  divides  $|G|$ . ■

### Corollary 1.41

(Euler's Theorem) Let  $\gcd(a, n) = 1$ , then  $a^{\phi(n)} \equiv 1 \pmod{n}$  where  $\phi(n)$  is the totient function.

*Proof for Corollary.*

Consider  $(\mathbb{Z}/n\mathbb{Z})^*$ , the multiplicative group. This has, as we know,  $\phi(n)$  elements (i.e, all numbers  $q$  smaller than  $n$  such that  $\gcd(q, n) = 1$ ). Consider a given  $a$  so that  $(a, n) = 1$ , which means  $a \in \mathbb{Z}/n\mathbb{Z}^*$ . Consider  $\langle a \rangle \leq (\mathbb{Z}/n\mathbb{Z})^*$ . Since the main group is of finite order, this cyclic subgroup also has to have finite order  $k$ . i.e,  $a^k = 1$ . Moreover, from Lagrange's theorem, we note that any subgroup's cardinality divides the main group's cardinality, which means  $k|\phi(n)$ . This means  $k\gamma = \phi(n)$  which gives us  $(a^k)^\gamma = a^{\phi(n)} = 1$ , which proves the result.

**Alt proof:** work in progress....

### Corollary 1.42

**Fermat's Little Theorem** Let  $a, p \in \mathbb{Z}$ ,  $p$  being a prime, with  $\gcd(a, p) = 1$ , then  $a^{p-1} \equiv 1 \pmod{p}$

*Proof for Corollary.*

Simply plug  $n = p$  and  $\phi(n) = \phi(p) = p - 1$  into Euler's Theorem. We are done.

**Alt proof:** work in progress....

## 1.3 Even more basix, Generators etc.

### Definition 1.43: Generator

Let  $G$  be a group and  $S$  a subset of  $G$ . We say  $G$  is **generated by**  $S$ , denoted by  $G = \langle S \rangle$  if every element of  $G$  can be written as a finite sequence of products of elements in  $S$ . More specifically, for every  $x \in G$ , there exists  $q_1, q_2, \dots, q_{n_x}$  (needn't all be distinct) and indices  $p_1, p_2, \dots, p_{n_x}$  so that  $x = q_1^{p_1} q_2^{p_2} \dots q_{n_x}^{p_{n_x}}$ .

$$\langle S \rangle := \{a_1^{e_1} a_2^{e_2} \dots a_n^{e_n} : \text{for any } a_1, a_2 \dots a_n \text{ in } S, \text{ and any } e_1, e_2 \dots e_n \in \mathbb{Z}\}$$

### Theorem 1.44

Let  $G$  be a cyclic group  $\langle a \rangle$  of order  $n$ . Suppose  $m|n$ , then there exists a cyclic subgroup of order  $m$  in  $G$ . Moreover, this group is the unique subgroup of order  $m$ .

*Proof for Theorem.*

Consider  $\langle a^{n/m} \rangle$ .  $O(a^{n/m}) = n/(\gcd(n/m, n)) = n/(n/m) = m$ . So existence is clear. Now onto uniqueness:

We found  $\langle a^{n/m} \rangle$  to be one such group. Suppose another subgroup  $\langle a^j \rangle$  also is  $m$  order.  $O(a^j) = n/\gcd(j, n)$  which is the order of the group. Hence  $n/(j, n) = m \implies n/m = \gcd(j, n)$  which means  $n/m|j$  or  $\delta(n/m) = j$  which puts  $a^j$  inside  $\langle a^{n/m} \rangle$  which makes  $\langle a^j \rangle$  a subgroup of  $\langle a^{n/m} \rangle$ . But since order is the same, the two groups must be

■ same. ■