CHAPTER 1

GROUPS

1 Basix

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

A group consists of a set and a binary relation $\cdot : G \times G \to G$ (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: **AS**sociative, **C**losed, **I**dentity, 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 $\overline{0}$ 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 $\overline{1}$ and the inverse is that $\overline{c}$, which was shown to exist, such that $\overline{a} \cdot \overline{c} = \overline{1}$.

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 $\& : (A \times B) \times (A \times B) \to A \times B$ 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 $a_1 \cdot a_2 \cdot \dots \cdot a_n$ 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 consequetive 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 $u = b$ $\square$

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 $n \not| m$, then $m = qn + r$ where $0 < r < n$. Therefore, $a^r \neq 1$. We have that $a^{qn+r} = a^{qn} \cdot a^r = a^r \neq 0$ which is absurd.

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

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 $\frac{n}{(m.n)}$ and $\frac{m}{(m,n)}$ 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 $mod(1)$

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 $\{\cdot\}$, $frac\{\cdot\}$ and $\underline{\cdot}$ interchangibly. We consider $x \circ (y \circ z) = frac(\underline{x} + [x] + frac(y + z))$=$frac(\underline{x} + [x] + frac(\underline{y} + [y] + \underline{z} + [z])) = frac(\underline{x} + frac(\underline{y} + \underline{z}))$= $frac(\underline{x} + (\underline{y} + \underline{z}) - [\underline{y} + \underline{z}]) = frac(\underline{x} + \underline{y} + \underline{z})$

Now consider $(x \circ y) \circ z = frac(frac(\underline{x} + \underline{y}) + \underline{z} + [z]) = frac(frac(\underline{x} + \underline{y}) + \underline{z}) = frac((\underline{x} + \underline{y}) - [\underline{x} + \underline{y}] + \underline{z} + [z]) = frac(\underline{x} + \underline{y} + \underline{z})$. Hence we see $\circ$ is associative. Trivial to note that the idenity 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 $|z|^n(cis(\theta))^n = 1$. Taking mod gives us $|z| = 1$. We have to solve for, then, $cis(theta)^n = 1$. It is simple computation to see that $cis(\theta)^n = cis(n\theta)$ which gives us $cis(n\theta) = 1$. 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 $z = cis(\frac{2k\pi}{n})$. We assume a modulo 2π structure, i.e, we classify solutions of the kind $\theta + 2k\pi$ in the class of θ. We see then, that for $k \leq n - 1$, each solution is unique. If we let $\omega = cis(\frac{2\pi}{n})$. We see that all the other elements are generated by ω since for $k = 2$, we just have ω^2 (from the way cis powers work). Till $k = n - 1$, we have unique solutions generated by ω given by $1, \omega, \omega^2 \cdots \omega^{n-1}$. We see that when $k = n$ we get $\theta = \frac{2\pi n}{n} = 2\pi \equiv 0 mod(2\pi)$. For $n + j$ where $j < n$, we see that $\theta = \frac{2\pi(n+j)}{n} = 2\pi + \frac{2\pi j}{n} \equiv \frac{2\pi j}{n} mod(2\pi)$. Hence, all the unique solutions are $1, \omega, \omega^2 \cdots \omega^{n-1}$.

To see that this is a group under multiplication, we note that $\omega^x(\omega^y\omega^z) = (\omega^x\omega^y)\omega^z = \omega^{(x+y+z) mod(n)}$. 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:

x	**1**	**a**	**b**	**c**
1	1	a	b	c
a	a	1	c	b
b	b	c	1	a
c	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)

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

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:

x	1	a	b	c
1	1	a	b	c
a	a	b	c	1
b	b	c	1	a
c	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 $< a >$ 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 $\forall n \in \mathbb{Z}$. $< a > := \{a^n : n \in \mathbb{Z}\}$ 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: $< a >$ 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, $< 1 >$ is precisely $\mathbb{Z}/n\mathbb{Z}$.

n-th roots of unity: $1, \omega, \omega^2 \cdots \omega^{n-1}$, is generated by $< \omega >$.

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.

$\Longrightarrow$) 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.

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

The other case, case (2) is that for every finite subcollection of $\{j_1, j_2 \cdots\}$, their gcd is not 1. Does this mean that $gcd(j_1, j_2 \cdots (\text{till } \infty))$ 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 γ 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). Cosider a H subgroup of G, given by elements $a^j : j \in \{n_1, n_2, \cdots\}$ where $n_1, n_2, \cdots$ is a sequence of integers. Note that, since a^{n_1} is in H, $(a^{q(n_1)})$ 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.

Lemma 1.22

A cyclic group is of prime order if and only if it has no non trivial proper subgroups.

Proof for Lemma

$\implies$) if $|G| = p$ where p is a prime, then the only subgroups (which are cyclic from the previous theorems) for this group are itself and identity, for the order of any subgroup divides the order of the group (because it is cyclic).

$\impliedby$) Suppose the only subgroups of G are the trivial one and itself. Suppose G is of a non prime order q. Then, if $m|q$, there is an element $a^{q/m}$, and its corresponding generated set, that is a proper subgroup of G. Absurd.nan

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 1.23: Rotation r

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

$$1 \xrightarrow{\text{r}} 2$$

$$2 \xrightarrow{\text{r}} 3$$

$$\vdots$$

$$n - 1 \xrightarrow{\text{r}} n$$

$$n \xrightarrow{\text{r}} 1$$

Whose inverse is, as one can guess:

$$2 \overset{\text{inverse(r)}}{\longrightarrow} 1$$

$$3 \overset{\text{inverse(r)}}{\longrightarrow} 2$$

$$\vdots$$

$$n \overset{\text{inverse(r)}}{\longrightarrow} n - 1$$

$$1 \overset{\text{inverse(r)}}{\longrightarrow} n$$

Definition 1.24: Symmetry, or flipping, or mirror whatever

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

$$1 \overset{s}{\mapsto} 1$$
$$2 \overset{s}{\mapsto} n$$
$$3 \overset{s}{\mapsto} n-1$$
$$\vdots$$
$$n \overset{s}{\mapsto} 2$$

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, $\cdots r^{n-1}$ 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 $1, r, r^2, \cdots r^{n-1}$ constitute the subgroup of rotations, each one corresponding to a rotation of $\frac{2j\pi}{n}$.
7. The elements $s, rs, r^2s \cdots r^{n-1}s$ correspond to "pivoting" the $j-th$ number and flipping about that. These on their own dont 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 $\{1, r, r^2 \cdots r^{n-1}; s; rs, r^2s, \cdots r^{n-1}s\}$ Constitutes a group, of order $2n$. This is stated formally in the next theorem, with proof.

Theorem 1.25

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

Proof for Theorem.

We note that $1, r, r^2, \cdots r^{n-1}$ 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^js. These have inverses as well, for if we compose this with r^{n-j}, we would have $r^{n-j} \circ (r^js) = s$. If we compose this still, with s, we get 1. The total composition on r^js would have been sr^{n-j}. Infact, these elements too are self inverses. Easier way to see this is $(r^is)(r^is) = r^i(sr^i)s = r^i(r^{-i}s)s = 1$. These also, then follow ASCII. ■

1.2 Symmetry group $Sym(A)$

We define the symmetric group of a given set Ω, denoted by sym(Ω) as the set of *all* permutations, or bijections, from Ω to Ω. In this group, $Id(x)$, the identity map, is taken as the identity element. The operation is function composition. By definition, it is closed under operation. Consider $f : \Omega \to \Omega$ a bijection. By definition of a bijection, there exists a two sided inverse: $f^{-1} : \Omega \to \Omega$ such that $f \circ f^{-1} \equiv f^{-1} \circ f \equiv Id$. Hence, inverse exists. It is also trivial to see that if f_1 and f_2 are bijections, $f_1 \circ f_2$ is a bijection too.
In the specific case where $\Omega = \{1, 2, \cdots, n\}$, we denote sym($\Omega$) as S_n. It is easy to see that the size of this group is $n!$.

Theorem 1.26

Given $\Omega := \{1, 2, 3, \cdots\}$, $sym(\Omega)$ is a group of infinite order.

Proof for Theorem.

Let f_1 be the identity, i.e, that which takes everything to itself, specifically 1 to 1. There are obviously more than one functions that take 1 to 1. Let f_2 be the function that takes 1 to 2. There may, again, be multiple ones. But this "set", f_2 is necessarily disjoint from f_1. As such, define f_j as that "set" of functions that take 1 to j. We notice that there are atleast $\mathbb{N}$ many functions. This makes $|\mathbb{N}| \leq |S_\Omega|$. More, though, can be said about this:

Consider $P(\mathbb{N})$. If an element in $P(\mathbb{N})$ is a finite set, say, (1,6,5), order the set and map it to that function whose cycle representation is (1,5,6). Therefore, given any two finite sets, the function we get under this mapping is unique. Suppose $S \in P(\mathbb{N})$ is an infinite set, say of the kind, (1,3,5,6,8,....). In this case, we map the set to pair-wise transposition's product. i.e, (1,3,6,8,....) maps to ((1,3)(6,8)....). Given any two distinct infinite subsets S_1 and S_2, it is clear that one contains an element not in the other, which means that this element is "remapped" whereas in the case of the first set, it stays the same. Therefore, given two infinite sets that are distinct, we get distinct bijections. If suppose S_1 is a finite set, while S_2 is an infinite set. For example, $S_1 = (1, 3, 4)$ and $S_2 = (1, 5, 7, 8, \cdots)$. We note that, beyond a finite point, the function $f(S_1)$ would stay constant, whereas there exists no such point for $f(S_2)$. Hence, this is an injection from $P(\mathbb{N})$ to $symm(\mathbb{N})$. Therefore, $symm(\mathbb{N})$ is uncountable. ■

Theorem 1.27

If σ is an $m-$ cycle $(a_1, a_2 \cdots a_m)$, then $\sigma^i(a_j) = a_{i+j \mod (m)}$

Proof for Theorem.

If $i = 1$, then $\sigma(a_j) = a_{j+1}$ if $j < m$ and 1 if $j = m$, which can be written as $\sigma(a_j) = a_{j+1 \mod (m)}$. Assume it to be true for all $i \leq n$. Consider $n+1$, i.e $\sigma^{n+1}(a_j) = \sigma(\sigma^n(a_j)) = \sigma(a_{j+i \mod (m)}) = a_{(j+i \mod m+1) \mod m} = a_{i+j+1 \mod m}$ ■

Corollary 1.28

Suppose σ is an $m-$cycle- $(a_1, a_2 \cdots a_m)$. Then $|\sigma| = m$.

Proof for Corollary.

We are looking for the smallest $n \in \mathbb{N}$ so that $\sigma^n \equiv Id$, or rather, for every $x \in A$, $\sigma^n(x) = x$. Note that σ acts only on $a_1, a_2 \cdots a_m$, and every other element is kept the same. This means that σ^k for any k can only possibly change these $a_1, a_2 \cdots a_m$ elements, and no other. From the previous theorem, we found that $\sigma^i(a_j) = a_{i+j \mod m}$. We want smallest n so that $\sigma^n(a_j) = a_{n+j \mod m} = a_{j \mod m}$ which means $n + j \mod m = j \mod m$, which means $n \equiv 0 modm$, or $n = km$ for some k. Smallest non 0 k is 1. So $n = m$. Hence, order is m. ■

Theorem 1.29

Let σ be an m cycle. Then σ^i is also an m cycle if and only if $(i, m) = 1$

Proof for Theorem.

$\implies$) Suppose σ^i is an m cycle. Recall the theorem that if $|a| = k$, then $|a^j| = k/gcd(j, k)$. Same applies here, where $|\sigma| = m$, we have $|\sigma^i| = m/gcd(i, m) = m$ which means $gcd(i, m) = 1$.

$\impliedby$) Suppose $gcd(i, m) = 1$. $|\sigma^i| = |\sigma|/gcd(i, |\sigma|) = m/gcd(1, m) = m$. Order of σ^i is therefore m. If σ was, say, $(a_1, a_2 \cdots, a_m)$, we can rewrite it as $(a, \sigma(a), \sigma^2(a) \cdots, \sigma^{m-1}(a))$. Can $\sigma^i(a) = a_{i+1 \mod (m)} = a_{1 \mod (m)}$? This would imply that $i + 1 \equiv 1 \mod (m)$, which makes $i \equiv 0 \mod m$. But we know that there exists x such that $xi \equiv 1 \mod (m)$. This contradicts the previous assertion, since that would make $x(i) \equiv x(0) \equiv 0 \mod (m)$. Is $\sigma^{ri}(a) = \sigma^{qi}(a)$ for any $q < r$? That would mean $a_{1+ri \mod (m)} = a_{1+qi \mod (m)}$ or $1+ri \equiv qi+1 \mod (m)$. That means $(r-q)i \equiv 0 \mod (m)$ where $(r-q) \in \mathbb{N}$. Also note that, we want $r - q < m$, since if it is greater than m, one of r or q would be greater than m, but we as a whole want ri and or qi to be less than m (since we are taking modulo m anyways). Therefore, $(r-q)(xi) \equiv (r-q)(1) \mod (m) = ((r-q)i)x \equiv 0 \mod (m)$ which would mean that $r = q + \delta m$. If we take that $r < m$, this would be absurd. Therefore, for any $0 < r < m$, $\sigma^{ri}(a) \neq \sigma^{qi}(a)$ for any $q < r$. Therefore, $a, \sigma^i(a), \sigma^{2i}(a) \cdots \sigma^{(m-1)i}(a)$ are all necessarily distinct. We have $m-$distinct members of the cycle, therefore they should all necessarily be from the set $(a_1, a_2 \cdots a_m)$, which makes σ^i an $m-$cycle.

Theorem 1.30

Given an m-cycle, $\sigma = (a_1, a_2, \cdots, a_m)$ or $\{a, \sigma(a), \sigma^2(a) \cdots, \sigma^{m-1}(a)\}$ and an integer i, the permutation σ^i "splits" into $gcd(i, m)$ cycles, each of size $m/gcd(i, m)$

Proof for Theorem.

Consider r to be the smallest integer such that $\sigma^{ri}(a) = a$, or rather, $a_{ri+1 \mod (m)} = a_{1 \mod (m)}$ which gives $ri \equiv 0 \mod (m)$. We have to find the least such r. Note that, $m/gcd(i, m)$ is a candidate, since $mi/gcd(i, m) \equiv 0 \mod (m)$. Let $q = gcd(i, m)$ for notation.

$q\gamma_i = i$ and $q\gamma_m = m$. Suppose there exists $r < m/q$ such that $ri \equiv 0 \mod (m)$. That means $ri = \delta m$ for some δ. $rq\gamma_i = \delta q\gamma_m \implies r\gamma_i = \delta\gamma_m$. We note here that r has to divide $\delta(\gamma_m)$. But also note that $r(i/q) = \delta(m/q)$ which yields $r(i/q)/(m/q) = \delta$ but m/q and i/q share no common factors (if a and b are given numbers, then $a/gcd(a, b)$ and $b/gcd(a, b)$ share no common factors for if they did, say $ep = a/gcd(a, b)$ and $ep' = b/gcd(a, b)$, then this would yield $(e \cdot gcd(a, n))p = a$ and $(e \cdot gcd(a, b))p' = b$ which makes $e \cdot gcd(a, b)$ a bigger divisor of a, b, which is absurd). Moreover, if $e|ab$, but $gcd(e, a) = 1$, then $e|b$ (To see this, from bezout, $xe + ya = 1$ which gives $xeb + yab = b$, which implies $xb + y(ab/e) = b/e$, which tells us $e|b$). With this, we can conclude that, $m/q|r$, contrary to assumption. Hence, m/q is the least r such that $ri \equiv 0 \mod (m)$. Hence, it is the least integer such that $\sigma^{ri}(a) = a$. This means that $\{a, \sigma^i(a), \sigma^{2i}(a) \cdots \sigma^{(r-1)i}(a)\}$ forms a sub-cycle in the main cycle σ^i, and all elements here are distinct from our proof. Keeping other elements, other than a as our starting point to constructing the cycle, we note that each cycle must be of size $r = m/gcd(i, m)$. Two subcycles are either the same, or are completely disjoint (for obvious reasons), which means that, if there are g cycles, each of stipulated size $m/gcd(i, m)$, then we would have "covered" $g \cdot m/gcd(i, m)$ elements of the original permutation. We require this number to be m, i.e $g \cdot m/gcd(i, m) = m$, which yields $g = gcd(i, m)$. Hence, proved.

Example :
Suppose that $\tau = (1, 2)(3, 4)(5, 6)(7, 8)(9, 10)$. We need to find a $\sigma = (a_1, a_2, \cdots a_m)$, an $m-$cycle, and a k so that $\sigma^k = \tau$.

We start by noting that $\tau^2 = e$, or $|\tau| = 2$. We therefore require, for whatever σ, that $|\sigma^i| = m/gcd(i, m) = 2$ or $gcd(i, m) = m/2$ (m must therefore be even). We can solve this equation for i, which has to be $m/2$ (It cant be larger than $m/2$ whilst being smaller than m and still being a multiple of $m/2$). Can m be anything other than 10? It can't, since $\sigma^{m/2}$ would split into $m/2$ cycles of size 2. Since τ is a product of 5 cycles of size 2, this immediately selects for us, the choice of m, which is

10. Therefore, we have boiled down to σ being an $10-$ cycle, and i to be 5. We require a choice of $a_1, a_2 \cdots a_m$ arrangement so that $\sigma^5 = \tau$. Keeping things abstract, let $\sigma = (a_1, a_2, \cdots a_{10})$. $\sigma^5 = (a_1, a_6)(a_2, a_7)(a_3, a_8)(a_4, a_9)(a_5, a_10)$. With the choices $a_1 = 1, a_2 = 3, a_3 = 5, a_4 = 7, a_5 = 9, a_6 = 2, a_7 = 4, a_8 = 6, a_9 = 8, a_{10} = 10$, we will have fulfilled the requirements for $\sigma^5 \equiv \tau$ ■

1.3 More basix, Homomorphisms, isomorphisms, centers

Definition 1.31: Homomorphism

Let $\langle G, \cdot \rangle$ and $\langle H, * \rangle$ be two groups. We say a function $\phi : G \to H$ 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 1.32: Group Isomorphism

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

Theorem 1.33

Let $\langle G, \cdot \rangle$ be a group. Consider $* : G \times G \to G$ 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 $\phi : G \to G$ 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 ϕ a homomorphism, hence, an isomorphism. ■

Definition 1.34: 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 1.35

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 $ca = cb$ would mean $bca = abc$). ■

Definition 1.36: 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 1.37

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, $bx = xb, \forall x \in S$. $b^{-1}bx = x = b^{-1}xb \implies xb^{-1} = b^{-1}xbb^{-1}$ 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 1.38: 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 1.39

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 $k_1, l_2 \in H_G$, 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 1.40: 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 guarentee 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 1.41: 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 1.42: 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 $s = gs'g^{-1}$.

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 1.43

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

Proof for Theorem.

> Consider $N_G(S) := \{g \in G : gSg^{-1} = G\}$. 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 exists $s' \in S$ 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 1.44

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

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

Proof for Theorem.

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

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

Theorem 1.45

Ω is bijective to Δ if and only if $S_\Omega \cong S_\Delta$

Proof for Theorem.

($\implies$) Suppose $f : \Omega \to \Delta$ is a bijection. Consider $\sigma \in S_\Omega$. Define $\lambda : \Delta \to \Delta$ as $\gamma \in \Delta \mapsto f\sigma f^{-1}(\gamma)$. $\lambda(\gamma_1) = \lambda(\gamma_2) \implies f\sigma f^{-1}(\gamma_1) = f\sigma f^{-1}(\gamma_2)$ which gives (due to bijectivity) $\gamma_1 = \gamma_2$. Let $\delta \in \Delta$, does there exist $\gamma \in \Delta$ such that $\lambda(\gamma) = f\sigma f^{-1}(\gamma) = \delta$? Answer is yes, obviously, $\gamma = f^{-1}\sigma^{-1}f(\delta)$. Hence, λ is a permutation of Δ. Consider a mapping (call it $Y : S_\Omega \to S_\Delta$) $\sigma \mapsto Y(\sigma) = \lambda = f\sigma f^{-1}$. Is this a homomorphism? Consider σ_1 and σ_2, $Y(\sigma_1 \circ \sigma_2) = \lambda_{12} = f(\sigma_1)f^{-1}f(\sigma_2)f^{-1} = Y(\sigma_1) \circ Y(\sigma_2)$ which makes Y a homomorphism. $Y(\sigma) = f\sigma f^{-1} = Id_\Delta$ means $\sigma = Id_\Omega$, which makes Y an injection. Let $\lambda \in S_\Delta$ be a permutation of Δ. Does there exist $\sigma \in S_\Omega$ such that $Y(\sigma) = f\sigma f^{-1} = \lambda$? $\sigma = f^{-1}\lambda f$ does the trick. Hence, Y is an isomorphism from S_Ω to S_Δ.

($\impliedby$) Suppose $S_\Omega \cong S_\Delta$ for two underlying sets Ω and Δ. ∎

$$\begin{tikzcd}
\Omega \arrow[r, "\sigma"] \arrow[d, "f"] & \Omega \arrow[d, "f"] \\
\Delta \arrow[r, "\lambda"] & \Delta
\end{tikzcd}$$

Theorem 1.46

If two groups G and H are isomorphic, then

1. $|H| = |G|$
2. $|x \in H| = |\phi(x)|$
3. G is abelian if and only if H is abelian

Proof for Theorem.

1)Is pretty obvious. Bijection, pal.

2) Suppose x is of infinite order, i.e $x, x^2 \cdots$ are all distinct. $\phi(x^j) = \phi(x)^j$. Suppose $\phi(x)^j = \phi(x)^k$, this gives us $\phi(x)^{j-k} = e$, or $x^j = x^k$ which is absurd. Suppose x is of finite order n. Then $x, x^2, \cdots x^{n-1}$ are distinct and $x^n = 1$. Consider $\varphi(x)$. $\varphi(x)^j = \varphi(x)^k$ would yield us $x^j = x^k$, which shall never happen if $j, k < n$. So $\phi(x), \phi(x)^2 \cdots \phi(x)^{n-1}$ are all distinct, and of course, $\phi(x)^n = e$. Hence $|\phi(x)| = n$.

Let $\phi : G \to H$ be an isomorphism. Suppose G is abelian, i.e, $\forall a, b \in G$ $ab = ba$. Consider $c, d \in H$. We have some $a, b \in G$ so that $\phi(a) = c, \phi(b) = d$. Consider $cd = \phi(a)\phi(b) = \phi(ab) = \phi(ba) = \phi(b)\phi(a) = dc$ which makes H abelian. The back direction follows in a similar fashion. ∎

Theorem 1.47

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

Proof for Theorem.

$\implies$) Suppose $H \triangleleft G$ which means that for every $q \in G$, $\forall h \in H$, $qhq^{-1} \in H$. The normalizer of H, $N_G(H) := \{x \in G : \forall h \in H, xhx^{-1} \in H\}$, which is easily seen to be the whole set.

$\impliedby$) Suppose $N_G(H) = G$ which means for every element g of G, every element h is so that $ghg^{-1} \in H$ which makes H normal in G. ■

Definition 1.48: $G//H$

This is called as the "quotient" of G over H. We define the equivalce relation $\equiv mod(H)$ as follows:

$a \equiv bmod(H)$ if and only if $a^{-1}b \in H$ or $b \in aH$. We denote the set of all equivalence classes of this relation as $G//H$. The notation for a particular equivalence class of, say, $a \in G$, looks like aH, the left coset of H wrt a.

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 $a^{-1}b \in H$ (which is equivalent to saying $\exists h \in H$ so that $b = ah$). We digress to define the following:

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

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

Note that, the relation "$\equiv$" is an equivalence one, and that the equivalence classes formed are precisely the left cosets of H.

Note the following: every left coset of H is bijective to every other. This is easily seen by the canonical bijection $ah \mapsto bh$. Also note that the equivalence class of $[e]$ is precisely H itself. therefore, the cardinality of every coset is the same, and is equal to the cardinality of H. Owing to the fact that equivalce classes split or partition the set (the set on which the relation is defined) into disjoint subsets whose union gives us back the whole set. Therefore, $\cup_{a\in G} aH = G$. If G is a finite group, then (Let $X := \{[x] : x \in G\}$),

$$\sum_{[a]\in X} [a] = \sum_{[a]\in X} |aH| = k_0|H| = |G|$$

where k_0 counts the number of distinct cosets of H.

This is Lagrange's theorem:

Theorem 1.49: 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 1.50

(**Euler's Theorem**) Let $gcd(a, n) = 1$, then $a^{\phi(n)} \equiv 1 mod(n)$ 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 $gcd(q, n) = 1$). Cosnider a given a so that $(a, n) = 1$, which means $a \in \mathbb{Z}/n\mathbb{Z}^*$. Cosnider $\langle a\rangle \leq (\mathbb{Z}/n\mathbb{Z})^*$. 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 reuslt.

Alt proof: *work in progress....* ∎

Corollary 1.51

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

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....*

On Quotients, and its maps

We define operations on $G//H$ as follows: $[a][b] := [ab]$. Is this well defined? Say $a \equiv a' mod(H)$ and $b \equiv b' mod(H)$, then $a' \in aH$ and $b' \in bH$. $a'b' = ahbh'$. $b^{-1}a^{-1}a'b' = (b^{-1}a^{-1}ahbh') = ?$ Is this back in H? We require that, for this to be back in H, H must be normal in G. Then (and only then) can we say that $b^{-1}hb$ goes back into H (for every element that is). Once this is well defined as an operation, we can see that $G//H$ would have group structure: Consider $[a] \cdot ([b] \cdot [c]) = [a] \cdot [(bc)] = [a(bc)] = [(ab)c] = [ab] \cdot [c] = ([a][b])[c]$. Hence, associative. Closed, obviously. Identity? $[a][e] = [a] = [e][a]$. Hence eH, which is just H, is the idenity element in G/H. $[a] \cdot [a^{-1}] = [e]$, which gives existence of inverse. Hence, G/H is a group when $H \triangleleft G$. Moreover, if $H \not\triangleleft G$, then there exists an element g in G and an element h in H so that $g^{-1}hg$ goes out of H. Hence, if we consider $g^{-1}hg$ and another h' in H, we easily see that $g^{-1}hgh'$ is also not in H. Consider another element $q' = qh$, and let g' be gh'. We then have $g^{-1}q^{-1}qhgh' \notin H$ which gives $(qg)^{-1}q'g' \notin H$. But not that $q' \equiv q$ and $g' \equiv g$ but $q'g' \not\equiv qg$. Hence, the operation won't be well defined.

Theorem 1.52

G/H is a group if and only if $H \triangleleft G$

Definition 1.53: Quotient map

We define a useful map $\pi : G \to G/H$ (where $H \triangleleft G$) given by

$$\pi(a) = [a] = aH$$

Theorem 1.54

Quotient map is a homomorphism, is surjective, and has ker(π)=H

Proof for Theorem.

Consider $\pi(ab) = [ab] = [a][b]$ by definition. Hence, obviously a homomorphism.

Consider $\pi(x) = [x] = [e]$ which means $x \equiv emod(H)$ which means $x \in H$. H is clearly the kernel of π. Consider any $[g] \in G/H$. Obviously, it has (possibly many) inverse images, one such being g itself in G. Hence, clearly surjective. ∎

Definition 1.55: Another interesting map

Let $f : G \to K$ be a surjective group homomorphism (for given arbitrary groups). Define the map

$$\tilde{f} : G/ker(f) \to K$$

as

$$\tilde{f}([x]) = f(x)$$

.

Theorem 1.56

The interesting map $\tilde{f} : G/ker(f) \to K$ is well defined, is a homomorphism that is injective, as well as surjective, i.e, is an isomorphism.

Proof for Theorem.

Consider $x \equiv x' mod(ker(f))$ so that $\tilde{f}([x]) = \tilde{f}([x'])$, which begs the question: Is $f(x) = f(x')$? We hve $x'^{-1}x \in ker(f)$, which gives $f(x')^{-1}f(x) = e$ which means $f(x) = f(x')$. Hence, well defined.

Consider $\tilde{f}([x]) = f(x) = 0$. That means $x \in ker(f)$, which means $[x] = [e]$, which means that the map is injective. Since f is surjective, there exists x so that $f(x) = z$. That is just $\tilde{f}([x]) = z$. Hence, surjective.

This tells us that $\tilde{f}$ is a bijective homomorphism, i.e, an isomorphism, from $G/ker(f)$ to K, where f is a surjective homomorphism from G to K. ■

Theorem 1.57

A subgroup H is normal to G if and only if it is the kernel of some Homomorphism f from G to some other group K

Proof for Theorem.

$\implies$) Consider G/H a group (i.e, $H \triangleleft G$), Cosnider the map $f : G \to G/H$ given by $f(a) = [a] = aH$. Is this a group homomorphism? $f(ab) = [ab] = [a][b] = f(a)f(b)$ which makes it a group homomorphism. Look at $f(x) = [x] = H$. This means that $x \equiv e$ or $x \in H$. Moreover, if $x \in H$, then $f(x) = [e]$. Hence, kernel of f is H.

$\impliedby$) Say H is the kernel of a homomorphism $f : G \to K$. Is H normal in G? Consider any element $h \in \text{kernel}(f)$, so that $f(h) = e_K$. Consider $g \in G$: $f(ghg^{-1}) = f(g)f(h)f(g)^{-1} = e_K$, which makes $ghg^{-1} \in \text{kernel}(f)$. Hence, $ker(f) \triangleleft G$. ∎

Theorem 1.58

A subgroup H is normal in G if and only if any left coset of H is equal to the corresponding right coset.

Proof for Theorem.

$\implies$)Say $H \triangleleft G$, which means for all $h \in H$ and all $g \in G$, we have an $h' \in H$ so that $ghg^{-1} = h'$, or $gh = h'g$. For every element in the left coset, the same is in the right coset. The other direction is also easy to see, whence we get that normal implies left coset=right coset.

Say for every $a \in G$, $aH = Ha$, i.e, for an element $x \in aH$, of the form ah, it is also of the form $h'a$ which means $aha^{-1} = h'$ whence we are done. ∎

1.4 Even more basix, Gnerators etc.

Theorem 1.59

Every homomorphism maps subgroups to subgroups, and inverse maps subgroups to subgroups

Proof for Theorem.

Let $f : G \to K$ be a group homomorphism. Consider $L \leq G$ to be a group. Consider $f(L) \subset K$. Is $f(L)$ a group? Obviously, e is in $f(L)$. Cosider $x \in f(L)$ which means there exists z in L so that $f(z) = x$. Consider z^{-1} in L as well, which maps to $f(z^{-1}) = f(z)^{-1}$. This is the inverse elment of x. Consider x to be in $f(L)$ and y also. This means $f(z_1) = x, f(z_2) = y$. $f(z_1 z_2) = k \in f(L) = f(z_1)f(z_2) = xy$ which ensures closure. Hence, a group.

Let $M \leq K$ be a subgroup of K. Consider $f^{-1}(M)$ which is $\{z \in G : f(z) \in M\}$. Since $e \in M$, and e in G maps to e in K, e is certainly in $f^{-1}(M)$. Let $x \in f^{-1}(M)$. Is $x^{-1} \in G$ also in $f^{-1}(M)$? We have $f(x) = z \in M$, which is a group, which means $f(x)^{-1} = f(x^{-1}) \in M$, which makes $x^{-1} \in f^{-1}(M)$. Hence, inverses exist. Consider $x \in f^{-1}(M)$ and $y \in f^{-1}(M)$. This means $f(x) = z_x$ and $f(y) = z_y$ both in M, a group. This means $f(xy) = f(x)f(y) = z_x \cdot z_y \in M$, which means $xy \in f^{-1}(M)$. Hence, closed. ■

Definition 1.60: 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 $q_1, q_2, \cdots q_{n_x}$ (needn't all be distinct)and indices $p_1, p_2 \cdots p_{n_x}$ so that $x = q_1^{p_1} q_2^{p_2} \cdots q_{n_x}^{p_{n_x}}$.

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

Theorem 1.61

Generated set $\langle S \rangle$ is a group

Proof for Theorem.

Trivial ■

Theorem 1.62

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 $\langle a^{n/m} \rangle$. $O(a^{m/n}) = n/(gcd(n/m, n)) = n/(n/m) = m$. 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. ■

Definition 1.63: Commutator set, commutator group

Let G be a group. Define S, the commutator set, to be

$$S := \{xyx^{-1}y^{-1} : x, y \in G\}$$

. Define $S' := \langle S \rangle$ to be the "commutator group"

Theorem 1.64

Commutator group is normal in G

Proof for Theorem.

Let z be an element in the commutator group of the form $(a_1)^{e_1}(a_2)^{e_2}\cdots(a_k)^{e_k}$, where $a_j = x_jy_jx_j{}^{-1}y_j{}^{-1}$. z is "ultimately" of the form $x_1y_1x_1{}^{-1}y_1^{-1}x_2y_2x_1^{-1}y_1^{-1}\cdots$ (since raising to -1 simply changes the order, where we simply relabel the terms.) So WLOG we say $z = x_1y_1x_1{}^{-1}y_1^{-1}x_2y_2x_1^{-1}y_1^{-1}\cdots$. Let k be any element in the commutator group. Let g be any element of G. Then $gkg^{-1} = gkg^{-1}k^{-1}k$, which is an element again, in the commutator group. Hence, $z = x_1y_1x_1{}^{-1}y_1^{-1}x_2y_2x_1^{-1}y_1^{-1}\cdots$ can be rewritten as $z = x_1y_1x_1{}^{-1}y_1^{-1}g^{-1}gx_2y_2x_1^{-1}y_1^{-1}g^{-1}g\cdots$, which is a sequence of elements of the commutator group multiplied with each other. Hence, commutator group is closed under Conjugation. Hence $\langle S \rangle \triangleleft G$. ■

Lemma 1.65

A homomorphism $f : G \to H$ is injective if and only if its kernel is trivial.

Proof for Lemma

$\implies$) If f is injective, then $f(x) = f(y)$ means $x = y$. Suppose $f(x) = f(e) = e_H$ which gives $x = e$, and hence kernel is trivial.

$\impliedby$) If kernel(f) is trivial, that means $f(x^{-1}y) = e \iff x^{-1}y = e$ which means $f(x) = f(y) \iff f(xy^{-1}) = e$ which means $x = y$. Hence injective. ■

Theorem 1.66: 1st Isomorphism theorem

Suppose f is a surjective group homomorphism from $G \to H$. Then $G/ker(f) \cong H$

Proof for Theorem.

Suppose f is a surjective group homomorphism from G to H. Define $i : ker(f) \to G$ as the inclusion map, i.e, $i(x) = x$ for all $x \in ker(f)$. Let φ be another surjective group homomorphism from G to K such that $ker(f) \subseteq ker(\varphi)$, or in other words, $\varphi \circ i = 0$ function. We clain that there exists a group homomorphism $\lambda : H \to K$ that is surjective. Let us define λ as follows:

$\lambda(x \in H) := \varphi($ one of the $g \in G$ such that $f(g) = x)$. Is this well defined? There could be many g-s as such. We want to make sure that if g, g' are so that $f(g) = f(g') = w$, then $\varphi(g) = \varphi(g')$. Since $f(g) = f(g') = w$, we have $g^{-1}g' \in ker(f)$, which means automatically that $g^{-1}g' \in ker(\varphi)$. Hence, $\varphi(g) = \varphi(g')$ and the function is well defined. Is this a homomorphism? Consider $\lambda(pq) = \varphi($ one of the $g \in G$ such that $f(g) = pq)$. Since f is surjective, we have for p and q, a non empty inverse image, say g_p and g_q so that $f(g_p) = p$ and $f(g_q) = q$, which gives us $f(g_p g_q) = pq$. Hence, $\lambda(pq) = \varphi(g_p g_q) = \varphi(g_p)\varphi(g_q) = \lambda(p)\lambda(q)$, which makes it a homomorphism. Is this surjective? i.e, for any $k \in K$, do we have $x \in H$ so that $\lambda(x) = k$? Given $k \in K$, we can find a $g \in G$ so that $\varphi(g) = k$. Simply look at $f(g) = w$. What is $\lambda(w)$? it is $\varphi(g) = k$. Hence, we can see that λ is surjective. Suppose that $ker(f) = ker(\varphi)$. Is λ injective? Consider $\lambda(x) = \lambda(y)$. We have that $\varphi($ one of the $g_x \in G$ so that $f(g_x) = x) = \varphi($ one of the $g_y \in G$ so that $f(g_y) = y)$, this means that $\varphi(g_x g_y^{-1}) = e$ which puts $g_x g_y^{-1} \in ker(f) = ker(\varphi)$. This implies $f(g_x) = x = g(g_y) = y$, which makes λ injective, atop of being surjective. Hence, λ is a bijective homomorphism from H to K. $\blacksquare$

$$
\begin{tikzcd}
ker(f) \arrow[r, hook, "i"] & G \arrow[r, "f"] \arrow[d, "\varphi"] & H \arrow[dl, dotted, "\lambda"] \\
 & K &
\end{tikzcd}
$$

Proof. (**Alt**) Since $ker(f)$ is the kernel of a group homomorphism, it is normal in G and is $G/ker(f)$ well defined. Consider the map $g : G/ker(f) \to H$ given by $g([x]) = f(x)$. Is this well defined? If $x \equiv y$, then $x^{-1}y \in ker(f)$ which means $f(x) = f(y)$, and the map is well defined. Is g a homomorphism? $g([x][y]) = g([xy]) = f(xy) = f(x)f(y) = g([x])g([y])$, so yes. Is this map injective? $g([x]) = f(x) = e$ means $x \in ker(f)$ which means $x \equiv eker(f)$, i.e, $[x] = [e]$, which makes g an injection. Is g a surjection? Consider $h \in H$. Since f is a surjection, $\exists q$ so that $f(q) = h$. This means $g([q]) = h$, which makes it a surjection. Hence

$$G/ker(f) \cong range(f)$$

for surjective homomrophism f. $\square$

Fact 1.67

If $H \triangleleft K$ where $H, K \leq G$, that amounts to saying $K \leq N_G(H)$