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 ω and 1. $(1 + \omega)^n = 1 + \binom{n}{1}\omega + \binom{n}{2}\omega^2 \cdots + 1$ (**TO BE FILLED IN LATER**)

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. 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 a so that $a^2 = q$. Question: Is $ab = a$, or b? Neither, because that would imply a or b is identity. So $ab = c$. We then have that $a^2b = b = ac$. Is $ba = c$? It can't be identity obviously, so yes. Same way, $ac = b$ and likewise $ca = b$ (cuz what else is there?). Same way, $bc = cb = a$. So far we got:

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

Suppose $c^2 = a$. Then $c(ca) = a^2$ which would mean $cb = 1$. Is it then that $c^2 = b$? $(ac)(c) = ab = c$ but $ac = b$ which means $bc = c$. Again, absurd. So $c^2 = 1$. In a similar vein, $b^2 = 1$. Finally we got

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

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 $< \omega >$.

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 1.16: 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 1.17: 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, $(r^n s)(r^m s) = r^n(sr^m)s = r^n(r^{-m})$ 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 1.18

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 $r^j s$. 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. ∎