Groups and Rings

Notes

IISER TVM

CONTENTS

Part I

Groups and Rings

CHAPTER 1

PRELIMNARIES

1 Sets, functions and all that

Definition 1.1: Prelimnary definitions

1. (Cartesian Product): if A and B are non empty sets, the *Cartesian Product* $A \times B$ is defined as the set of ordered pairs a, b wherein $a \in A, b \in B$. i.e, $A \times B := \{(a, b) : a \in A, b \in B\}$
2. (Function): A function from A to B is a set $f \subseteq A \times B$ such that, $a, b \in f$ and $a, c \in f \implies b = c$. A is called the **Domain of** f. $Range(f) := f(A)$ (see next definition)
3. (Direct Image): Direct image $f(A) := \{y \in B : \exists x \in A$ such that $f(x) = y\}$
4. (Inverse Image):$f^{-1}(S \subseteq B) := \{x \in A : f(x) \in S\}$
5. (Relation): Any subset $R \subseteq A \times B$ is a relation from A to B.
   We say $x \in X$ is "related to" $y \in Y$ under the relation R, or simply xRy or $R(x) = y$ if $(x, y) \in R \subseteq X \times Y$.
6. (Injection): $f : A \to B$ is injective if $\forall x_1, x_2 \in A, (x_1, b) \in f$ and $(x_2, b) \in f \iff x_1 = x_2$
7. (Surjection): $f : A \to B$ is surjective if $\forall b \in B, \exists a \in A$ such that $f(a) = b$
8. (Bijection): $f : A \to B$ is bijective if its both surjective and injective.
9. (Identity function on a set): $I_A : A \to A$ defined by $\forall x \in A, I_A(x) = x$
10. (Permutation): Simply a bijection from A to itself is called a permutation.

Definition 1.2: (Left Inverse)

We say $f : A \to B$ has a left inverse if there is a function $g : B \to A$ such that $g \circ f = I_A$

Theorem 1.3

$f : A \to B$ has a left inverse if and only if it is injective.

Proof for Theorem.

$\Longrightarrow$) If f has a left inverse g, Consider $x, y \in A$ such that $f(x) = f(y) = p$.
We have $g \circ f(x) = g(p) = x = g \circ f(y) = y$. Hence, $x = y$, Injective.
$\Longleftarrow$) Given that $f : A \to B$ is injective, define $g : B \to A$ as:

$$g(z \in B) = \begin{cases} a, \text{ where } f(a) = z, & \text{if } z \in f(A) \\ \text{whatever}, & \text{if } z \notin f(A) \end{cases}$$

consider $g \circ f(x \in A) = g \circ (f(x))$.
Obviously, $f(x) \in f(A)$, therefore, $g(f(x)) =$ that a such that $f(a) = f(x)$.
That a is x. Hence, $g(f(x)) = x$ ■

Definition 1.4: (Right Inverse)

$f : A \to B$ is said to have a right inverse if there is a function $g : B \to A$ such that $f \circ g = I_B$

Theorem 1.5

$f : A \to B$ has a right inverse if and only if f is Surjective.

Proof for Theorem.

$\Longrightarrow$) If f has a right inverse g, such that $f \circ g = I_B : B \to B$, then it is evident that the range of f is B, for if not, range of $f \circ g$ wouldn't be B either.
$\Longleftarrow$) If f is surjective, then for all $b \in B$, there exists atleast one $a \in A$ such that $f(a) = b$ define g as:

$$g(x \in B) = \text{one of those a} \in A \text{ such that} f(a) = b$$

Consider $f \circ g(x \in B) = f(\text{ one of the } a \text{ such that } f(a) = b) = b, \forall b \in B$
Hence, $f \circ g = I_B$ ■

Theorem 1.6

If f has left inverse g_1 and right inverse g_2, then $g_1 = g_2$. *(True for anything that is Associative, and function composition is associative.)*

Proof for Theorem.

$g_1 \circ f = I_A$ and $f \circ g_2 = I_B$
$g_1 \circ (f \circ g_2) = g_1 \circ I_B = g$
$= (g_1 \circ f) \circ g_2 = I_A \circ g_2 = g_2$
Hence $g_1 = g_2$

Corollary 1.7

f is invertible (i.e, both left and right inverse exist) if and only if it is bijective.

Proof for Corollary.

Obvious

1.1 Operations on Relations

If R and S are binary relations over $X \times Y$:

1. $R \bigcup U := \{(x, y)|xRy \text{ or } xSy\}$
2. $R \bigcap S := \{(x, y)|xRy \text{ and } xSy\}$
3. Given $S : Y \to Z$ and $R : X \to Y$, $S \circ R := \{(x, z)|\exists y \text{ such that } ySz \ \& \ xRy\}$
4. If R is binary over $X \times Y$, $\bar{R} := \{(x, y)|\neg(xRy)\}$

1.2 Homogeneous Relations

If R is a binary relation over $X \times X$, it is Homogeneous.

Definition 1.8: Definitions Regarding Relations

1. (Reflexive): $\forall x \in X, xRx$
2. (Symmetric): $\forall x, y \in X, xRy \implies yRx$
3. (Transitive): $\forall x, y, z \in X,$ if xRy & $yRz \implies xRz$
4. (Dense): $\forall x, y \in X,$ if $xRy,$ then there is some $z \in X$ such that xRz & zRy
5. (**Equivalence Relation**): R is an equivalence relation if it is Reflexive, Symmetric and Transitive.
6. (Equivalence class of $a \in A$(where there is an equivalence relation defined)): Set of all $b \in A$ such that bRa.
7. (Partition of A): Any collection of sets $\{A_i : i \in I\}$ (where I is some indexing set) such that:
$$A = \bigcup_{i \in I} A_i$$
$$A_i \cap A_j = \phi \text{ if } \forall i, j \in I, i \neq j$$

Theorem 1.9

Let A be a non-empty set. If R defines an equivalence Relation on A, then the set of all equivalence classes of R form a partition of A

Proof for Theorem.

Define our collection $\{A_\alpha\}$ as the set of all equivalence classes of A. Clearly, $\bigcup_{\alpha \in I} A_\alpha = A$. If A only has one element, obviously, that singleton set makes up the partition. Let A_α and $A_{\alpha'}$ be equivalence classes of two elements a and a' in A. If aRa', then $A_\alpha = A_{\alpha'}$ since every element in the equivalence class of a will, from the transitive property, be in the equivalence class of a' . Suppose $\neg(aRa')$. If, then, $\exists x \in A_\alpha$ such that $x \in A_{\alpha'}$, this means that $xR\alpha$ and $xR\alpha'$, but from transitive property, this means $\alpha R\alpha'$, which is a contradiction. Therefore, the pairwise intersection is disjoint. ■

Theorem 1.10

If $\{A_i : i \in I\}$ is a partition of A, then there exists an equivalence relation R on A whose equivalence classes are $\{A_i : i \in I\}$.

Proof for Theorem.

Define $R(x, y)$ if and only if $\exists$ unique $m \in I$ such that $x \in A_m$ and $y \in A_m$.

$R(x, x)$ is obvious if non empty, hence R is reflexive.

Suppose $R(x, y)$ and $R(y, z)$. Then, there exists a unique $m \in I$ such that x, y are in A_m. Similarly, there exists a unique $n \in I$ such that y, z are in A_n . Obviously, if $n \neq m$, intersection of A_n and A_m would be non empty, hence, $n = m$. Hence, R is transitive.

Consider $R(x, y)$, which means $\exists$ unique $n \in I$ such that $x, y \in A_n \implies R(y, x)$. Hence, R is an equivalence relation. ■

2 Induction, Naturals, Rationals and the Axiom of Choice

Axiom 2.1: Peano Axioms, characterisation of $\mathbb{N}$

1. $1 \in \mathbb{N}$
2. every $n \in \mathbb{N}$ has a predecessor $n - 1 \in \mathbb{N}$ except 1
3. if $n \in \mathbb{N} \implies n + 1 \in \mathbb{N}$

Definition 2.2: (Sequence of something)

A sequence of some object is simply a collection of objects $\{O_l : l \in \mathbb{N}\}$ which can be counted.

Axiom 2.3: Well Ordering Property of $\mathbb{N}$

Every non empty subset of $\mathbb{N}$ has a least element.

Axiom 2.4: Weak Induction

For all subsets $S \subseteq \mathbb{N}$, $((1 \in S)\&((\forall k \in \mathbb{N})(k \in S \implies k + 1 \in S)) \iff S = \mathbb{N})$

Weak Induction's Negation:(One direction)
There exists subset $S_0 \subseteq \mathbb{N}$, $((1 \in S_0)\&((\forall k \in \mathbb{N})(k \in S_0 \implies k + 1 \in S_0))$ but $S_0 \neq \mathbb{N})$

Axiom 2.5: Strong Induction

For all subsets $S \subseteq \mathbb{N}$, $((1 \in S)\&((\forall k \in \mathbb{N})(1, 2, ...k \in S' \implies k + 1 \in S')) \iff S = \mathbb{N})$

Strong Induction's Negation:(One direction)
There exists subset $S' \subseteq \mathbb{N}$, $((1 \in S')\&((\forall k \in \mathbb{N})(1, 2, ...k \in S' \implies k + 1 \in S'))$ but $S' \neq \mathbb{N})$

Theorem 2.6

Weak Induction $\iff$ Strong Induction.

Proof for Theorem.

$\implies$) Suppose Weak induction is true, but not strong induction. Take our set to be that S' in the negation of the Strong Induction Statement. $S' \neq \mathbb{N}$ implies that, either $1 \notin S'$ or $\exists k \in \mathbb{N}$ such that $k \in S'$ but $k+1 \notin S'$. We know that $1 \in S'$, so it must be that $\exists k \in \mathbb{N}$ such that $k \in S'$ but $k+1 \notin S'$. $\{1\} \in S' \implies \{1,2\} \in S'$. Assume that for n, $\{1, 2, ..n\} \in S'$. This means that $\{1, 2, ...n+1\} \in S'$. This means that for every $n \in \mathbb{N}$, $\{1, 2, ...n\} \in S' \implies n \in S'$. Contradiction.
$\impliedby$)Suppose Strong Induction is true, but not weak induction. Take the set S_0 from the negation of Weak Induction. $S_0 \neq \mathbb{N}$. This means, from strong induction, either $1 \notin S_0$ or $\exists k \in \mathbb{N}$ such that $1, 2, \ldots, k \in S_0$ but $k+1 \notin S_0$. $1 \in S_0$, hence, $2 \in S_0$ and $\{1,2\} \in S_0$. assume that $\{1, 2, ...n\} \in S_0$. This means, $n \in S_0 \implies n+1 \in S_0$, which means that $\forall k \in \mathbb{N}, \{1, 2, ..k\} \in S_0 \implies k+1 \in S_0$. Therefore, S_0 is $\mathbb{N}$. ■

Theorem 2.7

Weak Induction $\iff$ Strong Induction $\iff$ Well ordering.

Proof for Theorem.

$\implies$) Suppose that, on the contrary, S_0 is a non empty subset of $\mathbb{N}$, with no least element. Does 1 exist in S_0? No, for that will be the least element. Likewise, then, 2 does not belong in S_0. Assume that $\{1, 2, ...n\} \notin S_0$. Does $n+1$ exist in S_0? No, for that will become the least element then. From Strong Induction, $\mathbb{N} - S_0 = \mathbb{N} \implies S_0 = \phi$. Contradiction.
$\impliedby$)Suppose $\exists S_0 \subseteq \mathbb{N}$ such that $1 \in S_0$ and $\forall k \in \mathbb{N}$, $k \in S_0 \implies k+1 \in S_0$. Suppose on the contrary, S_0 is not $\mathbb{N}$. $\mathbb{N} - S_0$ is then, non-empty. From Well Ordering, there is a least element $q \in \mathbb{N} - S_0$. $\implies, q-1 \in S_0$. But this would imply $q-1+1 \in S_0$. Contradiction. $\mathbb{N} - S_0$ is empty. ■

Definition 2.8: (Finite Sets)

A set X is said to be finite, with n elements in it, if $\exists n \in \mathbb{N}$ such that there exists a bijection $f : \{1, 2.., n\} \to X$. Set X is *infinite* if it is non-finite.

Theorem 2.9

If A and B are finite sets with m and n elements respectively, and $A \cap B = \phi$, then $A \cup B$ is finite, with $m+n$ elements.

Proof for Theorem.

$f : \mathbb{N}_m \to A$ and $g : \mathbb{N}_n \to B$.

Define $h : \mathbb{N}_{m+n} \to A \cup B$ given by:

$$h(i) = \begin{cases} f(i) \text{ if } i = 1, 2...m \\ g(i-1) \text{ if } i = m+1, m+2, ...m+n \end{cases}$$

If $i = 1, 2, ...m$,$h(i)$ covers all the elements in A through f. If $i = m+1, ...m+n$, $h(i)$ covers all the elements in B through g.

Moreover, $h(i) \neq h(j); i \in [1, m], j \in [m+1, m+n]$ since $A \cap B = \phi$ ■

Theorem 2.10

If C is infinite, and B is finite, then $C - B$ is infinite.

Proof for Theorem.

Suppose $C - B$ is finite. We have $B \cap (C - B) = \phi$ and $B \cup (C - B) = C \cup B$

$n(C \cup B) = n(B \cup (C - B)) = n(B) + n(C - B)$ This implies $C \cup B$ is finite. Contradiction.

■

Theorem 2.11

Theorem: Suppose T and S are sets such that $T \subseteq S$. Then:

a) If S is finite, T is finite.

b)If T is infinite, S is infinite.

Proof for Theorem.

Given that S is finite, there is a function $f : \mathbb{N}_m \to S$. Suppose that S has 1 element. Then either T is empty, or S itself, which means T is finite. Suppose that, upto n, it is true that, if S is finite with n elements, all its subsets are finite. Consider S with $n+1$ elements.

$f : \mathbb{N}_{n+1} \to S$.

If $f(n+1) \in T$, consider $T_1 := T - \{f(n+1)\}$ We have $T_1 \subseteq S - \{f(n+1)\}$, and since $S - \{f(n+1)\}$ is a finite set with $n-1$ elements, from induction hypothesis, T_1 is finite. Moreover, since $T = T \cup \{f(n+1)\}$, T is also finite with one more element than T_1.

If $f(n+1) \notin T$, then $T \subseteq S - \{f(n+1)\}$, we are done.

(b) is simply the contrapositive of (a). ■

Definition 2.12: (Countable Sets)

A set S is said to be *countable*,or *denumerable* if, either S is finite, or $\exists f : \mathbb{N} \to S$ which is a bijection. If S is *not countable*, S is said to be *uncountable*

Theorem 2.13

The set $\mathbb{N} \times \mathbb{N}$ is countable.

Proof for Theorem.

The number of points on diagonals $1, 2, ...l$ are: $\psi(k) = 1 + 2 + ...k = \frac{k(k+1)}{2}$

The point (m, n) occurs on the $(m + n - 1$ th diagonal, on which the number $m + n$ is an invariant. The (m, n) point occurs m points down the diagonal. So, to characterise a point, it is enough to specify the diagonal it falls in, and its ordinate (the "rank" of that point on that diagonal). Count the elements till the $m + n - 2$nd diagonal, then add m, and this would be the position of the point (m, n).
Define $r : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ given by $r(m, n) = \psi(m + n - 2) + m$ That this is a bijection is pretty clear because we are counting the position of the point (m, n). For a given point (m, m), there can only be one unique diagnonal on which it exists, and on the diagonal, its rank is unique. Moreover, for every $q \in N$, there corresponds an (m, n) such that $r(m, n) = q$, for, we simply count along each diagonal in the "zig-zag" manner until we reach that (m, n) for which the position is given by q. Therefore, r is a bijection. (There are other explicit bijections too) ■

Theorem 2.14

The following are equivalent:

1. S is countable
2. $\exists$ a surjective function from $\mathbb{N} \to S$
3. $\exists$ an injective function from $S \to \mathbb{N}$

Proof for Theorem.

$(1 \implies 2)$ is obvious
$(2 \implies 3)$ $f : \mathbb{N} \to S$, every element of of S has atleast one preimage in $\mathbb{N}$. Define a function from $S \to \mathbb{N}$ by taking for each $s \in S$ the least such $n \in \mathbb{N}$ such that $f(n) = s$. This defines an injection.
$(3 \implies 1)$ If there is an injection from $S \to \mathbb{N}$, then there is a bijection from $S \to$ a subset of $\mathbb{N}$, which implies S is countable. ■

Corollary 2.15

The set of Rational Numbers $\mathbb{Q}$ is countable.

Proof for Corollary.

We know that a surjection from $\mathbb{N} \times \mathbb{N}$ to $\mathbb{Q}$ exists (where $f(0, 0) = 0$, and $f(m, n) = \frac{m}{n}$). We know that $\mathbb{N} \times \mathbb{N}$ is bijective to $\mathbb{N}$. This means $\mathbb{N}$ is surjective to $\mathbb{Q}$. We are Done. ■

Theorem 2.16

Every infinite subset of a countable set is countable.

Proof for Theorem.

Consider $N_s \subseteq \mathbb{N}$ which is infinite.

Define $g(1)$ = least number in N_s

Having defined $g(n)$, define $g(n+1)$= least number in N_s which is larger than $g(n)$.

That it is an injection is obvious, for $g(m) > g(n)$ if $m > n$.

Suppose it is not a surjection, i.e, $g(\mathbb{N}) \neq N_s \implies g(\mathbb{N}) \subset N_s \implies N_s - g(\mathbb{N}) \neq \phi$
Therefore, $N_s - g(\mathbb{N})$ has a least element, k. This means that $k-1$ is in $g(\mathbb{N})$. Therefore, there exists q in $\mathbb{N}$ such that $g(q) = k-1$. But then, $g(q+1)$= least number in N_s such that it is bigger than $g(q)$. This would, ofcourse be, k, which means $k = g(q+1)$, which puts k in $g(\mathbb{N})$. Contradicton. Hence, $g(\mathbb{N}) = N_s$, therefore, g is a bijection from $\mathbb{N} \to N_s$. Since every countable set is bijective to $\mathbb{N}$, and every infinite subset of a countable set is bijective to an infinite subset of $\mathbb{N}$, the theorem holds generally for countable sets. ■

Theorem 2.17

$\mathbb{N} \times \mathbb{N} \cdots \mathbb{N}$ is bijective to $\mathbb{N}$

Proof for Theorem.

$\mathbb{N} \times \mathbb{N}$ is bijective to $\mathbb{N}$ obviously. Assuume that $f : \mathbb{N} \to \mathbb{N} \cdots \mathbb{N}($ n times $)$ is bijective.

Consider $g : \mathbb{N} \times \mathbb{N} \to \mathbb{N} \cdots \mathbb{N}(n+1$ times $)$ given by $g(m,n) = (f(m), n)$. Clearly, this is bijective. ■

2.1 Axiom of Choice

Axiom 2.18: Axiom of Choice (AC)

For any collection of non empty sets $C = \{A_l : l \in L\}$, there exists a function f called the "counting function" which maps each set A_l to an element in A_l.
Formally: $f : C \to \bigcup_l A_l$ such that $\forall l \in L, f(A_l) \in A_l$

Theorem 2.19

Countable union of Countable sets is countable *(This theorem is an example of a theorem that requires* Axiom of Choice*)*

Proof for Theorem.

Suppose we are given a sequence of countable sets $\{S_n : n \in \mathbb{N}\}$. Since each S_j is countable, we have for each j, at least one bijective map $f_j : \mathbb{N} \to S_j$. Define $k : \mathbb{N} \times \mathbb{N} \to \bigcup_j S_j$ given by: $k(m, n) = f_m(n)$. Suppose $x \in \bigcup_j S_j$, i.e, $x \in S_j$ for some j. This means that, $f(n) = x$ for some n. Therefore, $k(j, n) = x$. Hence, k is surjective. From theorem 2.14, we are done.

(**Remark:** Keep in mind, for each S_j, there are a myriad of functions $(f_j)_k : \mathbb{N} \to S_j$. For each S_j, which is countably infinite, we have to choose one of the many functions that biject $\mathbb{N}$ to S_j. So we have a countable collection of sets $C = \{E_j : j \in \mathbb{N}\}$, where E_j denotes the set of all functions that biject $\mathbb{N}$ into S_j. So for every element in C, we need to choose one element in each element of C. This is where the Axiom of Choice comes into play.) ■

Theorem 2.20

If $f : A \to B$ is a surjection, then B is bijective to a subset of A

Proof for Theorem.

We are told that $f(A) = B$, i.e, for every $b \in B$, $\exists x_b$(many such x_b-s are possible) such that $f(x_b) = b$. Define a functino $g : B \to A$ as: $g(b) =$ one of those x_b such that $f(x_b) = b$. g is bijective to the set of all the chosen x_b for every b ■

Remark.

We make use of the Axiom of Choice in the previous theorem when we choose an x_b from a set of all possible x_b-s for b. Let A_b be the set of all possible x_b-s. Then the collection $\{A_b : b \in B\}$ is a collection of non-empty sets. And we are to select "one" element from each A_b. This requires AC.

Definition 2.21: (Power Set of a set)

Power set of A, denoted by $P(A)$ is the set of all subsets of A.

Theorem 2.22: Cantor's Theorem

For any set A, there *does not exist* any surjection from A onto $P(A)$

Proof for Theorem.

Suppose, on the contrary, a surjection $\psi : A \to P(A)$ exists. For every subset A_s of A, there exists an element x of A such that $\psi(x) = A_s$. Either this x exists in A_s, or it doesnt. Conider $D := \{x \in A : x \notin \psi(x)\}$. D is a subset of A, so there must be some element $y \in A$ such that $\psi(y) = D$. does y belong in D? If so, $y \notin \psi(y) = D$. Which means $y \notin D$. If, though, $y \notin D$, that implies $y \notin \psi(y) \implies y \in D$. Contradictions left and right. ■

3 Elementary Results regarding Integers

Definition 3.1

1. (Divides) We say $a \in \mathbb{Z} \setminus \{0\}$ divides $b \in \mathbb{Z}$ if there exists an integer δ such that $a\delta = b$. We denote it by $a|b$.

2. (GCD) We call a number d the "Greatest Common Divisor" of two integers a and b if $d|a$ and $d|b$, and d is the largest such number that divides both a and b (that the largest such number exists is clear, since divisors are finite).

3. (LCM) We call a number l the "Least Common Multiple" of two integers a and b if $a|l$ and $b|l$ and l is the smallest such integer.

Definition 3.2: Prime Number

A number p in $\mathbb{N}$ is *prime* if it has only itself and 1 as divisors. Non-primes are called composite.

Theorem 3.3

1. The GCD d of $a, b \in \mathbb{Z}$ is unique, and has the property that, if any other integer q is a divisor of a and b, then q divides d.

2. The LCM l of $a, b \in \mathbb{Z}$ is unique, and has the property that, if another integer p is a multiple of a and b, then l divides p.

3. If LCM of a, b and GCD of a, b are l and d respectively, then $dl = ab$.

Proof for Theorem.

(1) This will be proved below with the division algorithm. For now note that, if every divisor divides d, then d is the GCD.

(2) This is also proved using the divison algorithm. For now note that if every multiple of a, b is divisible by a multiple l, then it is the least common multiple.

(3) Suppose d is the unique GCD of a, b and l is the unique LCM of a, b.

Note that $d|ab$ which means $dc_0 = ab$ for some c_0. $c_0 = a(\frac{b}{d})$ and $c_0 = b(\frac{a}{d})$. This means c_0 is a multiple of a and b which means $l|c_0$. We have $lq_0 = c_0$ for some q_0. This means $dlq_0 = dc_0 = ab$. $(dq_0)(\frac{l}{a}) = b$ and $(dq_0)(\frac{l}{b}) = a$ which makes dq_0 a divisor. This would necessarily mean $q_0 = 1$, whence, we are done.

■

3.1 Euclid's Divison Algorithm

Lemma 3.4: The Lemma

Given integers $a, b \in \mathbb{Z}$ with $b \neq 0$, we get a unique $q \in \mathbb{Z}$ and $r \in \mathbb{Z}$ such that:

$$a = bq + r$$

with $0 \leq r < |b|$.

Proof for Lemma

We Prove for the case that $a, b \in \mathbb{N}$. Assume that for $a_0 \in \mathbb{N}$, the divison lemma works, i.e, $\exists q_0$ and r_0 so that

$$a_0 = bq_0 + r_0$$

with $0 \leq r < |b|$. Look at $a_0 + 1 = bq_0 + r_0 + 1$. We have that, either $r_0 + 1 = b$, or $r_0 + 1 < b$. If its the former, then we see that $a_0 + 1 = bq_0 + b = b(q_0 + 1) + 0$ whence we see that the new quotient is $q_0 + 1$ and the new remainder is 0. Hence, by induction, the lemma is proved.

For the cases where $a < 0$ or $b < 0$, we can simply multiply by -1 to get the result. ■

The Algorithm:

We start with $a, b \in \mathbb{Z} \setminus \{0\}$, and without loss of generality, we assume that $a \geq b$. We then have:

$$a = bq_0 + r_0 \text{ with } 0 \leq r_0 < |b|$$
$$b = r_0 q_1 + r_1 \text{ with } 0 \leq r_1 < r_0 < |b|$$
$$r_0 = r_1 q_2 + r_2 \text{ with } 0 \leq r_2 < r_1 < r_0 < |b|$$
$$r_1 = r_2 q_3 + r_3 \text{ with } 0 \leq r_3 < r_2 < r_1 < r_0 < |b|$$
$$\vdots$$
$$r_{n_0-1} = r_{n_0} q_{n_0+1} + r_{n_0+1} \text{ with } 0 \leq r_{n_0+1} < r_{n_0} \cdots b$$
$$r_{n_0} = r_{n_0+1} q_{n_0+2} + r_{n_0+2} \text{ with } 0 \leq r_{n_0+2} < r_{n_0+1} \cdots < b$$

Since we cannot have a sequence of strictly decreasing positive integers, we note that at some point, $r_n = 0 (= r_{n_0+2}$ for our sake).

We would then have (in the last step),

$$r_{n_0} = r_{n_0+1} q_{n_0+2} + 0$$

and back substituting,

$$r_{n_0-1} = r_{n_0+1}(q_{n_0+2} q_{n_0+1} + 1)$$

$$r_{n_0-2} = (r_{n_0+1}(q_{n_0+2}q_{n_0+1} + 1))q_{n_0} + r_{n_0+1}q_{n_0+2}$$

And finally we would end up with

$$a = r_{n_0+1}(\text{something}_1)$$

and

$$b = r_{n_0+1}(\text{something}_2)$$

with the added fact that r_{n_0+1} divides every remainder r_n in the division algorithm performed with a and b.

Proof that any divisor divides the GCD: Suppose that z is a divisor of a and b. From $a = bq_0 + r_0$, and

$$\frac{a}{z} = \frac{b}{z}q_0 + \frac{r_0}{z}$$

we see that z divides r_0. From $b = r_0q_1 + r_1$ and

$$\frac{b}{z} = \frac{r_0}{z}q_1 + \frac{r_1}{z}$$

we see that z divides r_1 too. Suppose z divides all remainders till r_{n_0}. $r_{n_0-1} = r_{n_0}q_{n_0+1} + r_{n_0+1}$ gives us $\frac{r_{n_0-1}}{z} = \frac{r_{n_0}}{z}q_{n_0+1} + \frac{r_{n_0+1}}{z}$ whence we see that r_{n_0+1} is divisible by z. Therefore, r_{n_0+1} is the GCD.

Proof that any multiple is divisible by LCM: Suppose that l and m are multiples of a, b and l is the least such multiple. Then $l \leq m$ with equality case being trivial. Suppose $l < m$. From Euclid's division lemma, we have $m = lq_0 + r_0$ with $0 < r_0 < l < m$. Both a and b divide m and l, which means

$$\frac{m}{a} = \frac{l}{a}q_0 + \frac{r_0}{a}$$

and

$$\frac{m}{a} = \frac{l}{a}q_0 + \frac{r_0}{a}$$

Which makes r_0 a multiple of a and b, which is absurd.

Theorem 3.5: Bezout's Theorem

If $a, b \in \mathbb{Z} \setminus \{0\}$, then there exists $x, y \in \mathbb{Z}$ so that $\gcd(a, b) = xa + yb$

Proof for Theorem.

From the first equation we see

$$a = bq_0 + r_0 \implies r_0 = a - bq_0$$

putting r_0 in the 2nd equation we see:

$$b = (a - bq_0)q_1 + r_1 \implies r_1 = b - (a - bq_0)q_1$$

Putting r_1 and r_0 into the 3rd equation, we get, likewise, r_2 in terms of a and b (a linear combination of a and b) As such, we can keep doing this to express r_{n_0+1} as a linear combination of a and b, like, $xa + yb$. ■

Theorem 3.6: Fundamental Theorem of Arithmetic

Given an integer $a > 1$, we can decompose a as a product of primes uniquely (upto ordering)

Proof for Theorem.

If $a = 2$, obviously we can. Suppose we can decompose every positive integer q $1 < q < n_0$ as a product of primes. Consider $n_0 + 1 = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n} + 1$. Either $p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n} + 1$ is a prime or is composite. If it is prime, we are done. If it is a composite number, then $p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n} + 1 = xy$ where x and y are numbers smaller than $n_0 + 1$. But since x and y can be expressed as a product of primes, we see that $n_0 + 1$ can also be represented as a product of primes.

Suppose $a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}$, but also $a = p_1^{\alpha'_1} p_2^{\alpha'_2} \cdots p_m^{\alpha'_m}$.
We have ($m \geq n$):

$$1 = p_1^{\alpha_1 - \alpha'_1} p_2^{\alpha_2 - \alpha'_2} \cdots p_n^{\alpha_n - \alpha'_n} p_{n+1}^{-\alpha'_{n+1}} \cdots p_m^{-\alpha'_m}$$

$$1 = p_1^{\alpha'_1 - \alpha_1} p_2^{\alpha'_2 - \alpha_2} \cdots p_n^{\alpha'_n - \alpha_n} p_{n+1}^{\alpha'_{n+1}} \cdots p_m^{\alpha'_m}$$

Obviously, not all $\alpha_j - \alpha'_j$ are positive, in the same way they all aren't negative. Suppose some of these powers are positive, while some negative. Consider some $p_j^{\delta_j}$ for which the power is negative, which moves it to the denominator. We have:

$$1 = \frac{\text{some primes raised to negative} \cdot \text{ some primes raised to positive}}{p_j^{\delta_j}}$$

If we multiply the negative powers out to both sides, we get to a stage where we see that p_j divides a product of primes (raised to positive powers). But, p_j is different from all the primes, and hence does not divide any of them individually, which means, from the lemma(s) below, that p_j actually does not divide the whole product. A contradiction. Hence, the only case remaining is that of product of primes raised to 0 powers, which makes it unique.

Requisite Lemmas:

Lemma: Suppose m is such that gcd(a, m)= 1, and $|ab$. Then, we have that $m|b$.
To see this, we use Bezout's Theorem: there exists x and y integers such that $ax + my = 1$. This means $abx + mby = b \implies \frac{ab}{m}x + by = \frac{b}{m}$ whence it becomes clear.

Lemma: If a prime p divides z^n for some integer z and some natural n, then p divides z.

To see this, Suppose that p does not divide z. Which means, from the lemma above, that p divides z^{n-1}, which likewise means it divides z^{n-2} and finally reaching to a contradiction that it finally divides z. ■

If we arrange the primes $p_1, p_2, \cdots p_n$ in ascending order, we find that this representation becomes the only one (no order permutations).

AN ALTERNATE LOOK AT GCD AND LCM:

Suppose that $a = p_1^{q_1} p_2^{q_2} \cdots p_n^{q_n}$ and $b = p_1^{r_1} p_2^{r_2} \cdots p_n^{r_n} \cdots p_m^{r_m}$. Since all numbers whatsoever are product of primes, we have that every divisor is of the form (for a number $z = p_1^{l_1} p_2^{l_2} \cdots p_k^{l_k}$) $p_1^{j_1} p_2^{j_2} \cdots p_k^{j_k}$ with $j_1 \leq l_1, j_2 \leq l_2 \cdots j_k \leq l_k$. The number of divisors for a given $z = p_1^{l_1} p_2^{l_2} \cdots p_k^{l_k}$ would therefore be: $\binom{(l_1+1)}{1}\binom{(l_2+1)}{1}\cdots\binom{(l_k+1)}{1}$.

We note that, given $a = p_1^{x_1} p_2^{x_2} \cdots p_m^{x_m}$ and $b = p_1^{y_1} p_2^{y_2} \cdots p_m^{y_m}$ with $x_j, y_j \geq 0$,

$$gcd(a, b) = p_1^{min(x_1,y_1)} p_2^{min(x_2,y_2)} \cdots p_m^{min(x_m,y_m)}$$

and

$$lcm(a, b) = p_1^{max(x_1,y_1)} p_2^{max(x_2,y_2)} \cdots p_m^{max(x_m,y_m)}$$

Euler Totient Function (ϕ):

The Euler Totient function ϕ is defined as follows:

$$\phi(n) = \text{ number of positive integers } z \text{ less than or equal to } n \text{ such that } gcd(n, z) = 1$$

For primes p, every number smaller than p is coprime to p, hence $\phi(p) = p-1$ More generally we have for primes p and natural q, $\phi(p^q) = p^q - p^{q-1}$.

Proof. Consider $\phi(p^k) = ||$all such numbers x such that $x \leq p^k$ and $gcd(x, p^k) = 1||$. Note that apart from the multiples of $p, p^2, p^3 \cdots$, all else are coprimes with p^k. The numbers that are not coprimes with p^k can be counted as: $1p, 2p, \cdots p(p), \cdots (p^2)p \cdots p^{k-1}p$. Hence, the number of multiples of p in this list are p^{k-1}. Total number of "numbers" smaller or equal to p^k are obviously, p^k. From here, the answer is obvious. □

Just accept the following fact

Fact 3.7

If $(m, n) = 1$, then $\phi(mn) = \phi(m)\phi(n)$

3.2 Modular Arithmetic:

Given $n \in \mathbb{N}$ and the set of all integers $\mathbb{Z}$, we define the following equivalence class:

$$aRb \iff n|(b-a)$$

We have aR obviously. If aRb, obviously bRa. If aRb and bRc, then $n|(b-a)$ and $n|(c-b)$ which means $n|(b-a)+(c-b) \implies n|c-a$. Hence, R is an equivalce relation. Consider arbitrary $a \in \mathbb{Z}$. A number x is in the equivalence class of a under the relation defined above if and only if $n|(x-a)$ which means $\exists z \in \mathbb{Z}$ so that $nz = x-a \implies x = a+nz$. A number x is in the equivalence class of a under R (also called as *congruence class of* a*mod*n) if and only if x is a plus an integral multiple of n.

It is also fruitful to view this from the following perspective:

Conjecture: *zRa (i.e, $n|z-a$) if and only if z, when divided by n, gives the same remainder as a when divided by n.*

Proof. ($\implies$) Consider $n|z-a$ which means $\exists p$ so that $z = a+pn$. If $a < n$, we have the remainder when a is divided by n, as a itself, whence we see that the remainder when z is divided by x is a as well. If $a > n$, then $a = qn + r_0$ with $0 \leq r_0 < n$. We then have $z = pn + a = pn + qn + r_0 = z_0 n + r_0$ where $r_0 < n$. Therefore, same remainder.

($\impliedby$) Suppose z and a give the same remainder when divided by n. This means $z = q_z n + r$ and $a = q_a n + r$ which means $z - a = (q_z - q_a)n$ which means $n|z-a$. □

Notation: We say zRb in the above context if either $n|z-b$ or z and b share the same remainders when divided by n. The equivalence class of a in this context is sometimes also called as *congruence class of* a*mod(*n*)*. A symbolic way to say zRa in this context is

$$z \equiv a\text{mod}(n)$$

We also denote the congruence class (or residue class) of an integer a by $\overline{a}$.

Theorem 3.8

If z is a given integer, and n is a given natural number, then the congruence class that z falls in would be one of the congruence classes formed by the $n-1$ numbers before n. Therefore, the entire partition created by R can be listed out as the congruence classes of the $n-1$ numbers before n

Proof for Theorem.

Suppose $z < n$. then obviously there is an integer q less than n (which is z itself) so that $q \equiv z\text{mod}(n)$. If $z > n$, then $z = qn + r$ where $0 \leq r < n$, which also means that, when r is divided by n, the remainder is r, just like z. This means $z \equiv r\text{mod}(n)$. From here it is clear that every number in Z would be in the equivalence class of some integer less than n. It is also obvious that for any two integers less than n, they each form unique residue classes. ■

From the previous lemma, it is clear to see that all the residue classes, or "partitions" of $\mathbb{Z}$ under the congruence mod (n) relation, can be succinctly listed out as

$$\overline{0}, \overline{1}, \overline{2} \cdots \overline{n-1}$$

.

Definition 3.9: $\mathbb{Z}/n\mathbb{Z}$

The set of all equivalence classes (or residue classes) under the relation defined by n on $\mathbb{Z}$ is denoted by

$$\mathbb{Z}/n\mathbb{Z}$$

which is basically $\overline{0}, \overline{1}, \overline{2} \cdots \overline{n-1}$

Theorem 3.10

If $a_1 \equiv b_1 \text{mod}(n)$ and $a_2 \equiv b_2 \text{mod}(n)$, then $a_1 + a_2 \in \overline{b_1 + b_2}$ and $a_1 a_2 \in \overline{b_1 b_2}$

Proof for Theorem.

(1) We have $a_1 = b_1 + kn$ and $a_2 = b_2 + ln$ which gives $a_1 + a_2 = (k_l)n + \overline{b_1 + b_2}$ where we see that $a_1 + a_2$ is integer multiple of $n + b_1 + b_2$. Therefore, $a_1 + a_2 \in \overline{b_1 + b_2}$.

Consider $a_1 a_2 = (kn + b_1)(ln + b_2) = (kln^2 + b_2 kn + b_1 ln) + b_1 b_2$. Obvious from here. ■

Definition 3.11: Modular Arithmetic

Treating the residue classes that form $\mathbb{Z}/n\mathbb{Z}$ as elements with which arithmetic can be done, we define addition and multiplication as follows:

$$\overline{a} + \overline{b} = \overline{a + b}$$

i.e, the sum of two residue classes is the residue class of the sum of an element from the class of a and the class of b. (This sum is well defined from the previous theorem.)

$$\overline{a}\overline{b} = \overline{ab}$$

i.e, the product of residue class of a and b is the residue class of the product of an element in the class of a and an element from the class of b. (Yet again, well defined)

Definition 3.12: $(\mathbb{Z}/n\mathbb{Z})^*$

$$(\mathbb{Z}/n\mathbb{Z})^* := \{\overline{a} \in \mathbb{Z}/n\mathbb{Z} : \exists \overline{c} \in \mathbb{Z}/n\mathbb{Z} \text{ such that } \overline{c} \cdot \overline{a} = \overline{1}\}$$

Lemma 3.13

If $gcd(a, n) = 1$, i.e, a and n are coprimes, then every element in the residue class of $a$mod(n) is coprimes with n

Proof for Lemma

Consider $z = a + kn$ for some k to be "non coprimes with n". i.e, $gcd(z, n) = j \neq 1$. We have $j|a + kn$ and $j|n$. But this means directly that $j|a$ whence we see that $j \neq 1$ is a divisor of a and n. Absurd. ■

Lemma 3.14

If $a \in \overline{a} \in \mathbb{Z}/n\mathbb{Z}$, $a \leq n$ and if $gcd(a, n) = j$, then for any $z \in \overline{a}$, $gcd(z, n) = j$.

Proof for Lemma

$gcd(a, n) = k$. Consider $gcd(a + gn, n)$. We apply the division algorithm:

$$(a + gn) = g_0(n) + a$$

$$n = g_1 a + r_1$$

$$\vdots$$

Notice that after step (1), the procedure is exactly the same as the procedure to find $gcd(a, n)$. The last living remainder is the GCD, and from here we can clearly see that the gcd are the same.

■

Lemma 3.15

If $1 \leq a \leq n$, with $n \geq 2$, and $(a, n) = j \neq 1(\geq 2)$, then there exists a number $1 \leq b < n$ so that $\overline{a} \cdot \overline{b} = \overline{0}$. A corollary of this is that there exists *no* $c \in \mathbb{Z}$ so that $\overline{a} \cdot \overline{c} = \overline{1}$

Proof for Lemma

We know $gcd(a, n) = j \neq 1(\geq 2)$. This means $j\alpha = a$, $j\mu = n$ where $\alpha < a$ and $\mu < n$. We can see that $a\mu = j\mu\alpha = n\alpha$. So the b in the lemma is the μ here. Therefore, $\overline{a} \cdot \overline{b} = \overline{0}$. Suppose $ac \equiv 1mod(n)$. This means from the multiplicative property of mod(n), we have $ac(b) \equiv bmod(n)$, but if you commute the multiplication, we see

$$c(ab) = \overline{c} \cdot \overline{ab} = \overline{c} \cdot \overline{0} \equiv 0mod(n)$$

But this would imply $b \equiv 0mod(n)$ which is not true. Hence, there can be no c so that $ac \equiv 1mod(n)$. ■

Proposition 3.16

$\mathbb{Z}/n\mathbb{Z}^*$ is the same as $\{\overline{a} \in \mathbb{Z}/n\mathbb{Z} : (a, n) = 1\}$

Proof. Let

$$A = \{\overline{a} \in \mathbb{Z}/n\mathbb{Z} : \exists \overline{z} \in \mathbb{Z}/n\mathbb{Z} \text{ such that } \overline{z} \cdot \overline{a} = \overline{1}\}$$

and

$$B = \{\overline{b} \in \mathbb{Z}/n\mathbb{Z} : (b, n) = 1\}$$

Consider an arbitrary $\overline{a}$ in B such that $\forall z \in \overline{a}$ we have $gcd(z, n) = 1$. We know that $z = a + k_z n$. From Bezout Identity, we have x_z and y_z so that $x_z(a + k_z n) + y_z(n) = 1$ which gives us $x_z a = (-y_z - k_z x_z)(n) + 1$. We see That $x_z a \in \overline{1}$. Consider arbitrary $t \in \overline{x_z}$. We have $t = x_z + jn$ or $x_z = t - jn$. Plugging this back we have $x_z a = (t - jn)a = (-y_z - k_z(t - jn))n + 1$ whence we can easily see that $ta \in \overline{1}$. Therefore, $\overline{a} \cdot \overline{x} = \overline{1}$. Therefore, if $\overline{b}$ is such that $(b, n) = 1$, then an inverse exists for it. Hence, $B \subseteq A$.

We showed that if x is in B, it must be in A. Consider x not in B. i.e, it is not co-primes with n. From the previous proposition, we see that there would exist no c so that $\overline{x} \cdot \overline{c} = \overline{1}$, i.e, no inverse element for any x not in B. Inexistence in B therefore implies inexistsnce in A, which gives us $A \subseteq B$. We can conclude that $A = B$ or in pithy words:

> "The set of all congruence classes b so that $gcd(b, n) = 1$ is the same as the set of all congruence classes b so that there exists another congruence clas c so that $\overline{b} \cdot \overline{c} = \overline{1}$ "

Symbolically:

$$\{\overline{b} \in \mathbb{Z}/n\mathbb{Z} : gcd(b, n) = 1\} = \{\overline{b} \in \mathbb{Z}/n\mathbb{Z} : \exists \overline{c} \in \mathbb{Z}/n\mathbb{Z} : \overline{b} \cdot \overline{c} = \overline{1}\} = (\mathbb{Z}/n\mathbb{Z})*$$

□

Theorem 3.17: Generalised Bezout's Identity

Suppose $j_1, j_2 \cdots j_n$ are given integers such that $gcd(j_1, j_2 \cdots j_n) = d$, then there exists integers $x_1, x_2 \cdots x_n$ so that $x_1 j_1 + x_2 j_2 \cdots x_n j_n = d$

Proof for Theorem.

We prime decompose each of $j_1, j_2 \cdots j_n$. For j_k, we have

$$j_k = p_1^{q_1^k} p_2^{q_2^k} \cdots p_{n_k}^{q_{n_k}^k}$$

We note that the gcd of all these numbers are the minimum of each index for each prime multiplied throughout. An important bit of information will be cricual here:

$$min\{w_1, w_2 \cdots w_k, w_{k+1} \cdots w_n\} = min\{min\{w_1, w_2 \cdots w_k\}, min\{w_{k+1}, w_{k+2} \cdots w_n\}\}$$

So we split $gcd(j_1, j_2, \cdots j_n)$ into $gcd(gcd(j_1, j_2), gcd(j_3 \cdots, j_n))$ = some linear combination of j_1, j_2 and $gcd(j_3, \cdots j_n)$. Do the same split to $gcc(j_3, \cdots j_n)$, to keep getting linear combinations, until finally you find $gcd(j_1, j_2 \cdots j_n) = x_1 j_1 + x_2 j_2 \cdots x_n j_n$ ■

CHAPTER 2

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 $a_1, a_2, \ldots a_n \in G$, the expression $a_1 \cdot a_2 \cdot \cdots \cdot a_n$ 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. □

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 $u = b$ □

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 $n = m$.

□

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. □

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. □

> ***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.

$\implies$) 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.

$\impliedby$) 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).

$\Longleftarrow$) 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, $(r^n s)(r^m s) = r^n(sr^m)s = r^n(r^{-m})$ 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 1.25

The set $\{1, r, r^2 \cdots r^{n-1}; s; rs, r^2 s, \cdots r^{n-1} s\}$ 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. ■

1.2 More basix, Homomorphisms, isomorphisms, centers

Definition 1.26: 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 1.27: Group Isomorphism

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

Theorem 1.28

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 1.29: 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 1.30

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 1.31: 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 1.32

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 1.33: 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 1.34

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, $k_1(k_2) = k_2 k_1$. Hence, the group is abelian. ■

Definition 1.35: 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 1.36: 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 1.37: 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 1.38

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 1.39

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

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 $z a_j z^{-1}$ which are in $\langle S \rangle$, which means finally that $zsz^{-1} \in \langle S \rangle$. Hence, we are done with showing that $\langle S \rangle \triangleleft N_G(S)$. Suppose $\langle S \rangle \triangleleft K$ for some subgroup K. This means that for every element $k \in K$ and every $s \in \langle S \rangle$, $ksk^{-1} \in \langle S \rangle$.

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 1.40

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

Proof for Theorem.

$\Longrightarrow$) 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.

$\Longleftarrow$) 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 1.41: $G//H$

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 "≡" 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 1.42: 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 1.43

(**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 1.44

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 $b' \in bH$. $a'b' = ahbh'$. $b^{-1}a^{-1}a'b' = (b^{-1}a^{-1}ahbh') = b^{-1}hbh' \in H$. Hence, $ab \equiv a'b' mod(H)$ and the operation is well defined.

Under this operation, when does $G//H$ become a group? We require: associativity, closure, identity and inverse. $[a] \cdot [e] = [e][a] = [a]$ where $[e]$ is just H. This shall be our idenity. Consider $[a]$ and $[b]$. By definition, $[a] \cdot [b] = [ab]$, which gives closure.

Theorem 1.45

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

1.3 Even more basix, Gnerators etc.

Definition 1.46: 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 1.47

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.

CHAPTER 3

TBD