# Department of Mathematics
## Guru Nanak Dev University, Amritsar-143005
Lecture notes on 'Basics of Group Theory' & assignment #1

In these notes, we will discuss some of the basic concepts of set theory. Including the order properties, the algebraic properties of real numbers under the binary operations of 'usual addition'& 'usual multiplication' are revisited in order to have a motivation for the notion of an algebraic group. We assume the existence of the set of real numbers and do not make any attempt to define it.

---

## 0.1 Properties of real numbers: A motivation

**Definition:** Let $S$ be a nonempty set. A relation $\prec$ on $S$ is called an 'order relation' if for all $x, y, z \in S$ the following hold:
(a) *Comparability*: for all $x \neq y$ either $x \prec y$ or $y \prec x$
(b) *Non reflexivity*: $x \not\prec x$ for all $x$
(c) *Transitivity*: if $x \prec y$ and $y \prec z$ then $x \prec z$

An order relation is also called a 'simple order' or 'linear order'.

**Definition:** A strict partial order denoted by the symbol $\prec$ on a $S$ is a relation on $S$ satisfying Non reflexivity and transitivity. Note that a linear order is also a strict partial order.

**Definition:** Let $\prec$ be a strict partial order on set $S$. A partial order denoted by the symbol $\preceq$ on $S$ is the one which satisfies the following:
(a) *Reflexivity*: $x \preceq x$ for all $x \in S$
(b) *Antisymmetry*: $x \preceq y$ and $y \preceq x$ implies $x = y$ for all $x, y \in S$
(c) *Transitivity*: if $x \preceq y$ and $y \preceq z$ then $x \preceq z$

**Definition:** A set $X$ with a linear order $\prec$ is called an ordered set. A subset $S \subset X$ is also an ordered set with the restriction of the order of $X$ onto it. $S \subset X$ is said to be bounded above in $X$ if there is a $x \in X$ such that for all $s \in S$ and $s \neq x$, $s \prec x$. Similarly we can define a set $T \subset X$ to be bounded below if there is a $y \in X$ s.t. $y \prec t$ for all $y \neq t \in T$.

**Definition:** Let $X$ be an ordered set. A subset $S$ of $X$ is said to have least upper bound in $X$ if there is an upper bound $\alpha \in X$ of $S$ and if $\beta \in X$ is another different upper bound of $S$ then $\alpha \prec \beta$. This $\alpha$ whenever exists is called the least upper bound of $S$ and is denoted by $\sup S$. Similarly one can define the greatest among all the lower bound of $S$ denoted by $\inf S$.

**Remark:** There is a difference between *maximal element* of a set and its sup depending upon which order among the linear or strict partial order is imposed over the set. Let $A$ be a strict partially ordered set. Then an element $\gamma \in A$ is said to be a maximal element of $A$ if there does not exist any element $x \in A$ s.t. $\gamma \prec x$. The notion of maximal element is required while dealing with the sets with strict partial order.

**Definition:** An ordered set $X$ is said to have least upper bound property if for every *nonempty* subset $S$ of $X$ which is bounded above in $X$, $\sup S$ exists in $X$.

**Axiom 1:** There exists an ordered field $(\mathbb{R}, <)$ having least upper bound property.
We will denote the order on $\mathbb{R}$ by $<$ w.r.t. which it satisfies least upper bound property and the ordered pair $(\mathbb{R}, <)$ is called as the real line. We usually omit $<$ and use the same symbol $\mathbb{R}$ to denote the real line.

**Theorem 0.1 (Archimedean property).** *Let $0 < x < y$ be real numbers. Then there is a positive integer $n$ s.t. $y < nx$.*

*Proof.* Let $A := \{nx \in \mathbb{R} \mid nx \leq y \text{ for all } n \in \mathbb{Z}_+\}$. Then $A$ is bounded above by $y \in \mathbb{R}$ and by least upper bound property of $\mathbb{R}$ $\sup A$ exists in $\mathbb{R}$. Let $\alpha = \sup A$, $0 < x \leq \alpha$ and $0 \leq \alpha - x < \alpha$ which means $\alpha - x$ is not an upper bound of $A$. Hence there is a positive integer $m$ s.t. $\alpha - x < mx$ or $\alpha < (m+1)x$. This is a contradiction. □

Let us list the axioms satisfied by the real numbers which are the elements of $\mathbb{R}$ w.r.t. the commutative binary operations of addition $+$, multiplication $\cdot$ and the linear order $<$.

#### Algebraic properties

1. $x + (y + z) = (x + y) + z$; $x \cdot (y \cdot z) = (x \cdot y) \cdot z$ for all $x, y, z \in \mathbb{R}$
2. There is a unique element called zero, denoted by 0 and a unique element called one, denoted by 1 s.t.
   $x + 0 = 0 + x = x$; $x \cdot 1 = 1 \cdot x = x$ for all $x \in \mathbb{R}$

[1] **Jitender Singh**; E-mail: sonumaths@gmail.com; Web page: https://sites.google.com/site/sonumaths2/

3. For each $x \in \mathbb{R}$ there is a unique $y \in \mathbb{R}$ s.t. $x + y = y + x = 0$. For each $x \neq 0$ there is a unique $y \neq 0$ s.t. $x \cdot y = y \cdot x = 1$

4. $x + y = y + x$; $x \cdot y = y \cdot x$ for all $x, y \in \mathbb{R}$

5. $x \cdot (y + z) = x \cdot y + x \cdot z$

**Mixed algebraic and order properties**

6. $x + y < x + z$ implies $y < z$
   If $x < y$ and $0 < z$ then $x \cdot z < y \cdot z$

**Order properties**

7. The linear order $<$ has least upper bound property

8. If $x < y$ then there is a $z \in \mathbb{R}$ s.t. $x < z$ and $z < y$

The pair $(\mathbb{R}, +)$ along with the first three properties listed above leads to an important algebraic object called group which we define now.

## 0.2 Group

**Definition:** A group is a nonempty set $G$ with a binary operation $* : G \times G \to G$ such that following axioms are always satisfied:
(1) $x * (y * z) = (x * y) * z$ for all $x, y, z \in G$
(2) there is a $1_G \in G$ called *the identity element* of $G$ which satisfies $1_G * x = x * 1_G = x$ for all $x \in G$
(3) for each $x \in G$ there is a $y \in G$ called *the inverse* of $x$ such that $x * y = y * x = 1_G$.

**Definition:** A group $(G, *)$ is called abelian group if for all $x, y \in G$

$$x * y = y * x.$$

If a group is not abelian, it is called non-abelian.

**Notation:** We will denote the group $(G, *)$ simply by $G$ when the binary operation is understood. Also we write for any $x \in G$ $x * x * \cdots * x (n - \text{times}) = x^n$ and for any $y,\ z \in G$ we write $y * z = yz$.

**Example:** $(\mathbb{R}, +)$ is a group since real numbers satisfy the three algebraic properties mentioned above under the binary operation of addition. Check that $(\mathbb{Q}, +)$, $(\mathbb{Z}, +)$ are also groups under the binary operation of usual addition.

**Example:** Define $\mathbb{R}^\times := \mathbb{R} - \{0\}$. Then $(\mathbb{R}^\times, \cdot)$ is a group under usual multiplication of real numbers. This is called multiplicative group of real numbers.
With similar definitions, check that $(\mathbb{Q}^\times, \cdot)$ and $(\mathbb{C}^\times, \cdot)$ are also groups.

**Example:** Consider the $n-$dimensional vector space $\mathbb{R}^n(\mathbb{R})$. $G$ be the set of all invertible linear transformations $T : \mathbb{R}^n \to \mathbb{R}^n$. Then $G$ is a group under the binary operation 'composition of maps' $\circ : G \times G \to G$ defined by

$$(T_1 \circ T_2)(x) = T_1(T_2(x))$$

for all $T_1, T_2$ in $G$ and $x \in \mathbb{R}^n$. This can be verified as follows:
(1) for all $T_1, T_2, T_3$ in $G$, and all $x \in \mathbb{R}^n$,
$(T_1 \circ (T_2 \circ T_3))(x) = T_1((T_2 \circ T_3)(x)) = T_1(T_2(T_3(x))) = (T_1 \circ T_2)(T_3(x)) = ((T_1 \circ T_2) \circ T_3)(x)$; therefore

$$T_1 \circ (T_2 \circ T_3) = (T_1 \circ T_2) \circ T_3 \ \forall\ T_1, T_2, T_3 \in G$$

(2) The identity element of $G$ is the identity map $I_G : \mathbb{R}^n \to \mathbb{R}^n$ defined by $I_G(x) = x$. Note that $I_G$ is an invertible linear map of $\mathbb{R}^n$ and for all $x \in \mathbb{R}^n$ and any $T \in G$, $(I_G \circ T)(x) = I_G(T(x)) = T(x) = T(I_G(x)) = (T \circ I_G)(x)$.
(3) For any $T \in G$ the inverse of $T$ is the map $T^{-1} : \mathbb{R}^n \to \mathbb{R}^n$ s.t. $T \circ T^{-1} = I_G = T^{-1} \circ T$. We just need to show that $T^{-1} \in G$ i.e. $T^{-1}$ is a linear map. For this first note that every element of $\mathbb{R}^n$ can be represented as an image of some element of $\mathbb{R}^n$ under $T \in G$. Now consider for all $T(x), T(y) \in \mathbb{R}^n$ the expression $T^{-1}(\alpha T(x) + \beta T(y)) = (T^{-1} \circ T)(\alpha x + \beta y) = \alpha x + \beta y = \alpha T^{-1}(T(x)) + \beta T^{-1}(T(y))$ for all $\alpha, \beta \in \mathbb{R}$ and $x, y \in \mathbb{R}^n$. This proves that $T^{-1} \in G$.

**Remark:** We know that for a fixed basis, a linear transformation $T : \mathbb{R}^n \to \mathbb{R}^n$ can be uniquely represented by a $n \times n$ matrix with real entries i.e.

$$T(x) = Ax,\ \forall x \in \mathbb{R}^n,\ A \in GL_n(\mathbb{R})$$

where we define $GL_n(\mathbb{R})$ to be the set of all $n \times n$ invertible matrices with all real entries. So there is a one to one correspondence between the set of all invertible linear transformations of $\mathbb{R}^n$ and the set $GL_n(\mathbb{R})$. It is easy to check that the set $GL_n(\mathbb{R})$ with the binary operation of matrix multiplication is a group. This group is known as 'general linear group of $n \times n$ matrices over the field $\mathbb{R}$ '. In general $GL_n(\mathbb{F})$ denotes the general linear group with matrix entries coming from the field $\mathbb{F}$.

**Example:** Define $O_n(\mathbb{R}) := \{A \in GL_n(\mathbb{R}) : AA^t = I\}$. Then $O_n(\mathbb{R})$ with the binary operation of matrix multiplication is a group and it is called the orthogonal group of $n \times n$ matrices over the field $\mathbb{R}$. We will discuss orthogonal group $O_2(\mathbb{R})$. Let us investigate how the linear transformation of coordinates takes place in the plane $\mathbb{R}^2$ which fix the origin. If $(x, y)$ are coordinates of a point in $\mathbb{R}^2$ w.r.t. older system of coordinates and $(x', y')$ are the coordinates of the same point in the new system of

coordinates which is obtained by rotating the older system of coordinates by an angle $\theta \in [-\pi, \pi]$ we can write the following relations:

$$x' = x\cos\theta + y\sin\theta;\ y' = -x\sin\theta + y\cos\theta,$$

These equations can be represented as the following matrix equation:

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \tag{0.1}$$

Note that the matrix

$$R_\theta = \begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix} \tag{0.2}$$

is an orthogonal matrix and therefore $R_\theta \in O_2(\mathbb{R})$. Therefore $R_\theta$ can be identified by a rotation of a straight line through the origin in the plane by an angle $\theta$ radians. Note that if $\theta_1, \theta_2 \in [-\pi, \pi]$ then

$$R_{\theta_1} R_{\theta_2} = R_{\theta_1+\theta_2}.$$

**Definition:** We also define an out of plane flip to be the linear map $s : \mathbb{R}^2 \to \mathbb{R}^2$ by the following

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \tag{0.3}$$

where the matrix

$$S = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \tag{0.4}$$

is also an orthogonal matrix.

**Remark:** 'a rotation by an angle $\theta_2$ followed by a rotation with an angle $\theta_1$ as defined above', is equivalent to a rotation by an angle $\theta_1 + \theta_2$.

**Remark:** Observe that

$$R_\theta S = \begin{pmatrix} -\cos\theta & \sin\theta \\ \sin\theta & \cos\theta \end{pmatrix} = SR_\theta^{-1}$$

**Definition:** Let $X$ be a nonempty set. A permutation of $X$ is a bijection $\sigma : X \to X$.

**Example:** Note that every invertible linear map $T : \mathbb{R}^n \to \mathbb{R}^n$ is a bijection, therefore a permutation. So is the linear map defined by each rotation $R_\theta$ of the plane $\mathbb{R}^2$.

**Definition:** Consider the set $S_X$ consisting of *all* permutations of $X$ under the binary operation 'composition of mappings'. It is easy to check that $(S_X, \circ)$ is a group. This is called permutation group of $X$.

**Remark:** Let us consider the symmetry preserving rotations of a regular $n-$gon in $\mathbb{R}^2$. This means a permutation $\sigma : \mathbb{R}^2 \to \mathbb{R}^2$ s.t. $\sigma(x) = R_{2\pi k/n} \cdot x$ for some $k \in \mathbb{Z}$. Observe that $R_{2\pi k/n} = R_{2\pi/n} \cdots R_{2\pi/n}(n - \text{times}) = (R_{2\pi/n})^k$. If we define $\sigma(x) := R_{2\pi/n} \cdot x$ then the set

$$H_n = \{I_H = \sigma^0, \sigma^1, \sigma^2, ..., \sigma^{n-1} \mid \sigma^n = I_H\}$$

where we define $I_H(x) = \sigma^0(x) = x$, is a group under the composition of mappings. Let $V = \{v_1, v_2, ..., v_n\}$ be the set of all vertices of a regular $n-$gon. Then it is evident that for all $t \in \mathbb{R}$

$$\sigma(tv_k) = \begin{cases} tv_{k+1} & \text{if } k \neq n \\ tv_1 & \text{if } k = n \end{cases};\ s(tv_k) := tv_{n-k+1},$$

for all $k = 1, 2..., n$. Note that $\sigma^n(v_k) = v_k$ and $s^2(v_k) = s(v_{n-k+1}) = v_{n-(n-k+1)+1} = v_k$ for all the values of $k$.

**Definition: (Dihedral group)** Define for each $n = 3, 4, ...$

$$D_{2n} := \{\sigma^0, ..., \sigma^{n-1}, s\sigma^0, , ..., s\sigma^{n-1}\}$$

where

$$\sigma^n = s^2 = \sigma^0,\ \sigma s = s\sigma^{-1} (\because R_\theta S = SR_\theta^{-1})$$

is a group under the composition of mappings and it is called the dihedral group of order $2n$.

**Definition: (Order of a group)** Let $G$ be a group. G is said to be finite if there is a positive integer $N$ and an injective map $f : G \to \{1, 2, ..., N\}$. G is called infinite if it is not finite. $|G|$ denotes the total number of distinct elements in $G$ and it is called its order. For example order of the dihedral group $D_{2n}$ is $|D_{2n}| = 2n$. Order of an infinite group is defined to be infinite e.g. $|GL_n(\mathbb{R})|$ is infinite.

**Definition: (Order of an element of a group)** Let $x \in G$ then order of $x$ denoted by $|x|$ is the smallest positive integer $n$ such that $x^n = 1_G$.

**Example:** Note that $|1_G| = 1$. Let us calculate order of each of the elements in the dihedral group

$$D_6 := \{1, \sigma, \sigma^2, s, s\sigma, s\sigma^2 \mid \sigma^3 = 1 = s^2;\ \sigma s = s\sigma^{-1}\}.$$

Since $\sigma^2 \neq 1$ and $\sigma^3 = 1$ therefore $|\sigma| = 3$. Similarly $|s| = 2$. Consider $(s\sigma)^2 = s\underline{\sigma s}\sigma = ss\sigma^{-1}\sigma = 1$ therefore $|s\sigma| = 2$. Similarly we can check that $|s\sigma^2| = 2$.

## 0.3 Permutation group

Let $X$ be a finite set with $n$ elements. Then the permutation group f $X$ is denoted by $S_n$. The permutation $\mu \in S_3$ defined by $1 \mapsto 2; 2 \mapsto 1; 3 \mapsto 3$ is represented by $\mu = (12)(3)$ and we can express explicitly

$$S_3 := \{(1)(2)(3), (12)(3), (13)(2), (23)(1), (123), (132)\}$$

This identification is convenient to obtain the composition of any number of permutation. For example one can directly calculate

$$\underleftarrow{(12)(3) \circ (132)} = (13)(2); \ \underleftarrow{(12)(3) \circ (12)(3)} = (1)(2)(3)$$

etc where the under-left arrow denote the order of evaluation of the image of a point under the composition of the permutations. We now write for convenience $(1) \approx (1)(2)(3)$ and $(12) \approx (12)(3)$ omitting the mention of the images fixed by the permutation. In this regard we see that

$$S_3 = \{(1), (12), (13), (23), (123), (132)\}.$$

**Definition:** Let $m$ be a positive integer. An $m-$cycle in the permutation group $S_n (m \leq n)$ is a permutation $\sigma \in S_n$ s.t. $\sigma = (\mu(1)\ \mu(2)\ \cdots\ \mu(m)$ for some permutation $\mu \in S_n$.

For example in $S_5$ the permutation $(254)$ is a $3-$cycle because

$$(254) = (\mu(1)\ \mu(2)\ \mu(3))$$

where $\mu = (125)(34)$ while the permutation $(1245)$ is a 4-cycle since

$$(1245) = (\nu(1)\ \nu(2)\ \nu(3)\ \nu(4))$$

where $\nu = (345)$.

**Remark:** Note that $|S_n| = n!$. If $\sigma \in S_n$ is an m-cycle then $|\sigma| = m$. This can be checked from the following. By definition $\sigma = (\mu(1)\ \mu(2)\ \cdots \mu(m))$ form some $\mu \in S_n$. Observe that for any $k = 1, 2, ..., (m-1)$, $\boxed{\sigma^{m-k}(\mu(k)) = \mu(m)}$ and therefore $\sigma^m(\mu(k)) = \sigma^k(\mu(m)) = \sigma^{k-1}(\mu(1)) = \sigma^{k-2}(\mu(2)) = \cdots = \sigma^0(\mu(k))$. Therefore $\sigma^m = \sigma^0$. Moreover, as $\mu \in S_n$, and $\sigma^{m-k}(\mu(k)) = \mu(m) \neq \mu(k)$ for all $k = 1, 2, ..., m-1$, it follows that $\sigma^{m-k}(\mu(k)) \neq \sigma^0$ for all $k = 1, 2, ..., m-1$. We have proved that $m$ is the least positive integer for which $\sigma^m = \sigma^0$. Hence $|\sigma| = m$.

## 0.4 Equivalence relations

**Definition: (equivalence relation)** A relation $\sim$ on a set $S \neq \emptyset$ is said to be equivalence relation if it is
(a) *Reflexive*: $x \sim x\ \forall\ x \in S$
(b) *Symmetric*: If $x \sim y$ in $S$ then $y \sim x$
(c) *Transitive*: If $x \sim y$ and $y \sim z$ in $S$ then $x \sim z$

**Definition: (equivalence classes)** Let $\sim$ be an equivalence relation on a set $S$. Then for a $x \in S$ the equivalence class of $x$ under the equivalence relation $\sim$ is defined as the set:

$$\bar{x} := \{y \in S : y \sim x\}$$

**Example: (residue classes modulo $n > 1$)** Let $n > 1$ be a positive integer. Define a relation $\equiv$ on $\mathbb{Z}$ by the following:

$$x \equiv y \ \text{ if } \ n \text{ divides } x - y, \ x, y \in \mathbb{Z}$$

It is easy to check that the relation $\equiv$ is (a) reflexive since $n$ divides $0 = x - x$ for every $x \in \mathbb{Z}$ (b) symmetric since for any $x, y \in \mathbb{Z}$ s.t. $x \equiv y$ means $n$ divides $x - y \ \Rightarrow\ n$ divides $y - x$ or $y \equiv x$. (c) transitive since $x \equiv y$ and $y \equiv z$ means $n$ divides $x - y$ and $y - z$. But then $n$ divides their sum $x - y + y - z = x - z$ i.e. $x \equiv z$. It follows that $\equiv$ is an equivalence relation on the set of integers $\mathbb{Z}$. Here equivalence class of $k = 0, 1, 2, ..., (n-1)$ is

$$\bar{k} := \{y \in \mathbb{Z} : y = nx + k \ \text{ for some integer } x\}$$

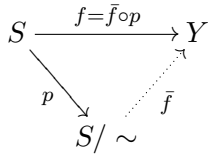
Note that the sets $\bar{k} = \overline{n + k}$ therefore there are only $n$ different equivalence classes of $\equiv$ in $\mathbb{Z}$. Denote the set of equivalence classes of $\equiv$ modulo $n$ by

$$\mathbb{Z}/n\mathbb{Z} := \{\bar{0}, \bar{1}, ..., \overline{n-1}\}.$$

**Theorem 0.2.** *Let $\sim$ be an equivalence relation on a set $S \neq \emptyset$. Then any two equivalence classes of $\sim$ in $S$ are either disjoint or they are same.*

*Proof.* Let $\bar{x}$ and $\bar{y}$ be any two equivalence classes of $\sim$ in $S$. If $\bar{x} \neq \bar{y}$ suppose that $\bar{x} \cap \bar{y} \neq \emptyset$. If possible let us suppose that $z \in \bar{x} \cap \bar{y}$ then $z \in \bar{x}$ which means $z \sim x$ and $z \in \bar{y}$ so $z \sim y$. By symmetry of $\sim$ $y \sim z$. As $y \sim z$ and $z \sim x$ by transitivity $y \sim x$ this means $y \in \bar{x}$. Now for every $a \in \bar{y}$ $a \sim y$ and as $y \sim x$ again by transitivity of $\sim$ $a \sim x$. It follows that $\bar{y} \subset \bar{x}$. By interchanging the role of $x$ and $y$ we will obtain $\bar{x} \subset \bar{y}$. Hence $\bar{x} = \bar{y}$. $\square$

**Theorem 0.3.** *Let us denote $S/\sim$ as the set of equivalence classes of an equivalence relation $\sim$ on a set $S$. Then the map $p : S \to S/\sim$ defined by $p(x) = \bar{x}$ is surjective. If $f : S \to Y$ is another function such that whenever $x \sim y$ in $S$ gives $f(x) = f(y)$ then there is a mapping $\bar{f} : S/\sim \to Y$ for which $f = \bar{f} \circ p$ i.e. the following diagram commutes:*



*Proof.* Clearly $p$ is surjective. Define $\bar{f}(\bar{x}) = f(x)$ for all $\bar{x} \in S/\sim$. We establish that $\bar{f}$ is well defined. For this let $\bar{x} = \bar{y}$. This means $x \sim y$ but then $f(x) = f(y)$ or $\bar{f}(\bar{x}) = \bar{f}(\bar{y})$. Finally, we have

$$f(x) = \bar{f}(\bar{x}) = (\bar{f} \circ p)(x) \ \forall \ x \in S$$

which proves that $f = \bar{f} \circ p$. □

**Definition:** Let $S \neq \emptyset$. A partition $\pi$ of $S$ is a set of disjoint subsets of $S$ such that union of all members of $\pi$ equals $S$.

**Remark:** It follows from the above definition and the theorem 0.2 that the set of equivalence classes of a set forms its partition. In fact the converse is also true and follows from the next result.

**Theorem 0.4.** *A set $\pi$ consisting of subsets of $S$ such that $\cup_{A\in\pi} = S$, is a partition of $S$ if and only if each member of $\pi$ is an equivalence class of some equivalence relation on $S$.*

*Proof.* If each member of $\pi$ is an equivalence class of some equivalence relation $\sim$ on $S$. It is given that $\cup_{A\in\pi} = S$. Therefore by theorem 0.2 it follows that $\pi$ is a partition of $S$.
Conversely let $\pi$ be a partition of $S$. Define a relation $\sim$ on $S$ by the following:

$$x \sim y \text{ if } x, y \in C_\alpha$$

for some $C_\alpha \in \pi$. It is easy to check that $\sim$ is an equivalence relation. Define the surjective map $f : S \to \pi$ s.t. $f(a) = C_\alpha$ if $a \in C_\alpha$ where $C_\alpha \in \pi$. By theorem 0.3 $f$ factors as a mapping $\bar{f} : S/\sim \to \pi$ which is onto. We just need to show that $\bar{f}$ is injective. For this let $\bar{f}(\bar{x}) = \bar{f}(\bar{y})$, then $x, y \in C_\alpha$ for some index $\alpha$, therefore $x \sim y$ this implies $\bar{x} = \bar{y}$. □

## 0.5 Group of residue classes modulo $n$

**Theorem 0.5 (Division algorithm).** *Let $a \neq 0,\ b \neq 0$ be integers. Then there exist unique integers $q$ and $r$ such that*

$$a = qb + r \quad \textit{and} \quad 0 \leq r < |b|.$$

*Proof.* The proof is divided into the following two cases:
**Case I:** $0 < |b| < |a|$. Using Archimedean property of $\mathbb{R}$ there is a positive integer $m$ such that $|a| < m|b|$. Choose smallest (well ordering of $\mathbb{Z}^+$) such $m = (n+1)$ such that $n|b| \leq |a| < (n+1)|b|$. Then $0 \leq |a| - n|b| < |b|$. Define $s := |a| - n|b|$ such that $|a| = n|b| + s$, where $0 \leq s < |b|$. We find that $a = qb + r,\ 0 \leq r < |b|$ where
(i) $q = -(n+1)\frac{|b|}{b};\ r := -s + |b|$ for $a < 0$ and
(ii) $q := n\frac{|b|}{b};\ r := s$ for $a > 0$.
**Case II:** $0 < |a| < |b|$. Here we see that $|a| = |b|0 + |a|$. It follows that $a = qb + r,\ 0 < r < |b|$ where
(i) $q := 0,\ r := a$ for $a > 0$ and
(ii) $q := -\frac{|b|}{b},\ r := |b| + a$ for $a < 0$.
Finally, uniqueness of $q$ follows from the uniqueness of $n$ (in case I) & $b$ (in case II). The uniqueness of $r$ follows from the uniqueness of $n,\ a$ and $b$. □

**Theorem 0.6 (Euclidean algorithm).** *Let $m, n$ be positive integers and $d := \gcd(m, n)$. Then there exist integers $x$ and $y$ such that $mx + ny = d$.*

*Proof.* If $m$ divides $n$ then $\gcd(m, n) = m$ and

$$\left(\frac{n}{m} - 1\right) m - n = m$$

and we are done with $x = \left(\frac{n}{m} - 1\right)$ and $y = -1$. So assume that $d := \gcd(m, n) \neq m, n$ and that $n > m$. For convenience define $r_{-2} := n$ and $r_{-1} := m$. Using division algorithm repeatedly, we find two sequences $\{q_j\}$, and $\{r_j\}$ of integers s.t.

$$r_j = q_{j+2} r_{j+1} + r_{j+2},\ 0 < r_{j+2} < r_{j+1} \tag{0.5}$$

for each $j = -2, -1, 0, 1....$ Note that $\{r_j\}$ is a strictly decreasing sequence of positive integers therefore it is well ordered. So there is a positive integer $N$ such that

$$r_{N-1} = q_{N+1} r_N. \tag{0.6}$$

From the Eq.(0.6) it follows that $r_N$ divides $r_{N-1}$. By back substitution of $r_{N-1}$ in Eq. (0.5) for $j = N - 2$ we see that $r_N$ divides $r_{N-2}$. On repeating the back substitution process, we see that $r_N$ divides each member of the sequence $\{r_j\}$. It follows that $r_N$ divides $r_{-1}$ and $r_{-2}$. We have proved that $r_N$ divides $d$.
From Eq.(0.5) for $j = -2$ we see that $d$ divides $r_0$. Since $d$ divides $r_{-1}$ and $r_0$, from Eq.(0.5) for $j = -1$ it follows that $d$ divides $r_1$. By repeating this process, we see that $d$ divides all members of the sequence $\{r_j\}$. In particular $d$ divides $r_N$. Hence $d = r_N$.
Finally by forward substitution of $r_0$ from the expression for $r_{-2}$ in the equation for $r_{-1}$ we obtain

$$r_{-1} = q_1(r_{-2} - q_0 r_{-1}) + r_1.$$

or

$$r_1 = (1 + q_1 q_0) r_{-1} - q_1 r_{-2}.$$

By repeating the substitution process, we see that every member of the sequence $\{r_j\}$ is linear integer combination of $r_{-1}$ and $r_{-2}$. In particular there are integers $x$ and $y$ s.t. $r_N = x r_{-1} + y r_{-2}$. □

**Remark:** The integers $x$ and $y$ in the Euclidean algorithm are not unique for instance if we take $m = 3$ and $n = 7$ we have $3 \times -2 + 1 \times 7 = 1$ and $3 \times -9 + 4 \times 7 = 1$ are satisfied by $x = -2, y = 1$ and $x = -9, y = 4$.

**Remark:** A *converse of the theorem0.6* is also true. i.e. 'if there are integers $x$ and $y$ such that $mx + ny = d$ and $d$ is a common divisor of $m$ and $n$, then $d = \gcd(m, n)$.' This can be seen as follows. Since $d$ is a common divisor $d \leq \gcd(m, n)$. For reverse inequality, we see that $\gcd(m, n)$ divides $mx + ny = d$ hence $\gcd(m, n) \leq d$. It follows that $\gcd(m, n) = d$.

### Group of residue classes modulo $n$

Now consider again the set $\mathbb{Z}/n\mathbb{Z}$ and define a binary operation $+$ on it as follows:

$$\bar{x} + \bar{y} = \overline{x + y}$$

Observe that $\bar{x} + (\bar{y} + \bar{z}) = \bar{x} + \overline{y + z} = \overline{x + (y + z)}$. Since $x + (y + z) = (x + y) + z$ as $x, y, z \in \mathbb{R}$ therefore $\overline{x + (y + z)} = \overline{(x + y) + z} = \overline{x + y} + \bar{z} = (\bar{x} + \bar{y}) + \bar{z}$. This shows that associative law holds in $\mathbb{Z}/n\mathbb{Z}$. Also for all $\bar{x} \in \mathbb{Z}/n\mathbb{Z}$ $\bar{0} \in \mathbb{Z}/n\mathbb{Z}$ s.t.

$$\bar{0} + \bar{x} = \overline{0 + x} = \bar{x} = \overline{x + 0} = \bar{x} + \bar{0}$$

therefore $\bar{0}$ is the identity element. Finally for any $x \in \mathbb{Z}/n\mathbb{Z}$ $0 \leq x < n$ therefore $0 \leq n - x < n$; hence $\overline{n - x} \in \mathbb{Z}/n\mathbb{Z}$ s.t.

$$\overline{n - x} + \bar{x} = \overline{n - x + x} = \bar{n} = \bar{0} = \bar{x} + \overline{n - x}$$

therefore $\overline{n - x}$ is the inverse of $x$ in $\mathbb{Z}/n\mathbb{Z}$. We have proved that $\mathbb{Z}/n\mathbb{Z}$ is a group under the binary operation $+$ defined above. This is called *group of residue classes modulo n*.

**Remark:** Here we define a binary operation $\cdot$ on the set

$$(\mathbb{Z}/n\mathbb{Z})^{\times} := \{\bar{x} \in \mathbb{Z}/n\mathbb{Z} : \gcd(x, n) = 1\}$$

as follows:

$$\bar{x} \cdot \bar{y} = \overline{xy}$$

where $xy$ stands for usual multiplication of integers $x$ and $y$. We shall show that $(\mathbb{Z}/n\mathbb{Z})^{\times}$ is a group under the binary operation just defined. Associative law is easy to check. Also here the identity element is $\bar{1}$ since for each $\bar{x} \in (\mathbb{Z}/n\mathbb{Z})^{\times}$

$$\bar{x} \cdot \bar{1} = \overline{x1} = \bar{x} = \bar{1} \cdot \bar{x}$$

Finally for any $\bar{x} \in (\mathbb{Z}/n\mathbb{Z})^{\times}$ $\gcd(x, n) = 1$ therefore by Euclidean algorithm, there exist integers $u$ and $v$ s.t.

$$ux + vn = 1 \text{ or } \overline{ux + vn} = \bar{1}(\text{why?})$$

Thus $\bar{1} = \overline{ux} = \bar{u} \cdot \bar{x} = \bar{x} \cdot \bar{u}$. This shows that $\bar{u}$ is the inverse of $\bar{x}$. This completes the proof.

**Remark:** What is the order of the group $(\mathbb{Z}/n\mathbb{Z})^{\times}$? Note that every $\bar{x} \in (\mathbb{Z}/n\mathbb{Z})^{\times}$ is such that $\gcd(x, n) = 1$. Therefore total number of such elements is equal to the total number of positive integers less then $n$ and coprime to $n$. This number is called Euler's phi function $\varphi(n)$. Therefore we can write

$$|\,(\mathbb{Z}/n\mathbb{Z})^{\times}\,| = \varphi(n).$$

If $n = \prod_{i=1}^{r} p_i^{e_i}$ is the decomposition of $n$ into product of prime powers where $p_i$ are distinct primes and $e_i$ are non-negative integers, then it is easy to establish that

$$\varphi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right)$$

**Example:** If we take $n = 6$ we have

$$\mathbb{Z}/6\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$$

while

$$(\mathbb{Z}/6\mathbb{Z})^{\times} = \{\bar{1}, \bar{5}\}.$$

**Remark:** The group $(\mathbb{Z}/n\mathbb{Z})^{\times}$, $n = 2, 3, ...$ is also known as the group of units of the residue classes modulo $n$ and is denoted $U_n$.

## 0.6 Group of arithmetic functions

**Definition:** (**Arithmetic function**) An arithmetic function is a map $f : \mathbb{Z}^+ \to \mathbb{C}$.

Let $\mathcal{A}$ be the set of all arithmetic functions $f$ which satisfy $f(1) \neq 0$. Define a binary operation $*$ on $\mathcal{A}$ as follows:

$$(f * g)(n) = \sum_{d|n} f(d) g\left(\frac{n}{d}\right), \text{ for all } f, g \in \mathcal{A},\ n \in \mathbb{Z}^+$$

where summation runs over all positive divisors of $n$. Then $(\mathcal{A}, *)$ is an abelian group with the identity

$$e(n) := \begin{cases} 1 \text{ if } n = 1 \\ 0 \text{ if } n > 1 \end{cases}$$

and inverse of any $f \in \mathcal{A}$ to be the arithmetic function $g$ which can be calculated recursively from the following

$$g(n) = -\frac{1}{f(1)} \sum_{d|n,\ d<n} f(d) g\left(\frac{n}{d}\right)$$

What is the inverse of the arithmetic function $I \in \mathcal{A}$ s.t. $I(n) = 1$ for all $n \in \mathbb{Z}^+$? **Hint:** Check that $I * \mu = \mu * I = e$ where $\mu$ is the Möbius function.

## 0.7 Generators and relations

**Definition:** Let $S$ be a subset of a group $G$ and $S^{-1} := \{s^{-1} : s \in S\}$. If every element of $G$ can obtained from the elements of the set $S \cup S^{-1}$ by operating them finite number of times (finite product of elements of $S \cup S^{-1}$), we say that $S$ is a set of generators of $G$. We indicate this by notation $G = \langle S \rangle$ and say that $G$ is generated by the set $S$. If $S = \{x_1, ..., x_k\}$ is a finite set and $S$ generates $G$ we write $G = \langle x_1, ..., x_k \rangle$ . The equations satisfied by the *generators* i.e. the elements of $S$ are called *relations*. Generators and relations together constitute a presentation of the group.

**Example:** Consider the dihedral group $D_6$

$$D_6 = \left\langle \sigma, s \mid \sigma^3 = \sigma^0 = s^2; \sigma s = s\sigma^{-1} \right\rangle$$

is a presentation of $D_6$ where the set of generators of $D_6$ is $\{\sigma, s\}$ and the relations are $\sigma^3 = \sigma^0 = s^2; \sigma s = s\sigma^{-1}$.

**Example:** Let us verify that a presentation of the permutation group $S_n$ is given by

$$S_n = \left\langle (12), (12\cdots n) | (12)^2 = (1) = (12\cdots n)^n \right\rangle .$$

**Step 1:** Any $\sigma \in S_n$ is equal to a finite product of $m-$cycles for $1 \leq m \leq n$. Each $m-$cycles $(a_1...a_m)$is equal to the product of at most $2-$cycles i.e.

$$(a_1...a_m) = (a_1a_m)(a_1a_{m-1}) \cdots (a_1a_2).$$

In fact this shows that every element of $S_n$ is generated by the set of $n-1$ generators $\{(a_1a_2), ..., (a_1, a_n)\}$ where $a_1, ..., a_n \in \{1, 2, ..., n\}$. Choose $a_i = i$ so that

$$S_n = \langle (12), (13), ..., (1n) \rangle .$$

**Step 2:** We now show that every element of the form $(1k),\ k = 2..., n$ is generated by (12) and (12...n). This follows from the following calculations

$$(12...n)^k(12)(12...n)^{-k} = (k,\ k+1),\ k = 0, 1, ..., n-1$$

and that

$$(1, k+1) = (1k)(k, k+1)(1k),\ k = 2, ..., n-1.$$

**Remark:** Note from the last example that any 2-cycle $(ij)$ may be decomposed into product of three 2-cycles:

$$(ij) = (aj)(ai)(aj)$$

for distinct $i, j, a \in \{1, 2, ..., n\}$.

## 0.8 Fields and Skew-Fields

**Definition:** A skew-field is a set $\mathbb{K}$ together with two binary operations called addition (denoted "+") and multiplication (denoted "$\cdot$") satisfying the following:
(1) $x \cdot (y + z) = x \cdot y + x \cdot z$; $(y + z) \cdot x = y \cdot x + z \cdot x$.
(2) $\mathbb{K}$ is an abelian group under addition with identity element denoted by "0".
(3) $\mathbb{K}^\times$ is a group under multiplication with the identity element denoted by "1".
A skew-field in which multiplication is commutative is called a field.

**Example:** The set of all real numbers $\mathbb{R}$ is a field. Also $\mathbb{R}^2$ is a field with componentwise addition but a different multiplication rule. These are described by:

$$(x, y) + (z, t) = (x + z, y + t)$$

$$(x, y) \cdot (z, t) = (xz - yt, xt + yz)$$

It is surprising to know that $\mathbb{R}^n$ can be made into a field only for $n = 1$ and 2 (Frobenius 1877). However it is known that $\mathbb{R}^4$ can be made into a skew-field via the multiplication rule that we describe now. Denote element $(x, y, z, w)$ of $\mathbb{R}^4$ by symbols $x+y\mathbf{i}+z\mathbf{j}+w\mathbf{k}$ and define a multiplication rule for the symbols $\{\mathbf{1}, \mathbf{i}, \mathbf{j}, \mathbf{k}\}$ such that $\mathbf{1} = e_1,\ \mathbf{i} = e_2,\ \mathbf{j} = e_3,\ \mathbf{k} = e_4$, as follows:

$$\mathbf{1} \cdot \mathbf{x} = \mathbf{x} \cdot \mathbf{1} = \mathbf{x} \text{ for all } \mathbf{x} \in \mathbb{R}^4,$$

$$\mathbf{i} \cdot \mathbf{1} = \mathbf{1} \cdot \mathbf{i};\ \mathbf{j} \cdot \mathbf{1} = \mathbf{1} \cdot \mathbf{j};\ \mathbf{k} \cdot \mathbf{1} = \mathbf{1} \cdot \mathbf{k},$$

$$\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = -\mathbf{1},$$

$$\mathbf{i} \cdot \mathbf{j} = \mathbf{k};\ \mathbf{j} \cdot \mathbf{k} = \mathbf{i};\ \mathbf{k} \cdot \mathbf{i} = \mathbf{j},$$

$$\mathbf{j} \cdot \mathbf{i} = -\mathbf{k};\ \mathbf{k} \cdot \mathbf{j} = -\mathbf{i};\ \mathbf{i} \cdot \mathbf{k} = -\mathbf{j}.$$

Using these multiplication rules $\mathbb{R}^4$ becomes a skew field denoted by $\mathbb{H}$ with the component wise addition and the following product formula

$$(a+b\mathbf{i}+c\mathbf{j}+d\mathbf{k})\cdot(x+y\mathbf{i}+z\mathbf{j}+w\mathbf{k}) = (ax-by-cz-dw)+$$

$$(ay+bx+cw-dz)\mathbf{i}+(az+cx+dy-bw)\mathbf{j}+(aw+dx+bz-cy)\mathbf{k}$$

The skew-field $\mathbb{H}$ is called the *quarternions*. To verify that $\mathbb{H}$ is a skew field the only difficult part is to see multiplicative inverse of the element $X = a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}$ which is

$$X^{-1} := \frac{a - b\mathbf{i} - c\mathbf{j} - d\mathbf{k}}{a^2 + b^2 + c^2 + d^2}.$$

**Example:** The set $Q_8 := \{\pm 1, \pm\mathbf{i}, \pm\mathbf{j}, \pm\mathbf{k}\}$ where $\mathbf{i}, \mathbf{j}, \mathbf{k}$ are as defined in $\mathbb{H}$ is a non abelian group of order 8 under the binary operation as multiplication rule of the skew field $\mathbb{H}$. $Q_8$ is called *quarternion group*.

## 0.9 Cancelation Laws in Groups

**Proposition 0.7.** *Let $G$ be a group. The equations $ax = b$ and $ya = b$ in $G$ have unique solutions for $x, y \in G$. In particular left and right cancelation laws hold in $G$, i.e.*

$$au = av \Rightarrow u = v;\ ub = vb \Rightarrow u = v,\ \forall\ u, v, a, b \in G.$$

*Proof.* Since $a \in G$ $a^{-1} \in G$ and we operate $a^{-1}$ from the left to both sides of the equation $ax = b$. We see that $a^{-1}ax = a^{-1}b$ or $x = a^{-1}b \in G$. Similarly we have $y = ba^{-1}$. Uniqueness of $x$ and $y$ follows from the uniqueness of $a^{-1}$ and $b^{-1}$.
To verify the left cancelation law we left multiply both sides of $au = av$ by $a^{-1}$ and obtain $a^{-1}au = a^{-1}av$ or $u = v$. Similarly the right cancelation law follows by right multiplication to the both sides of $ub = vb$ by $b^{-1}$. □

A partial converse of the above proposition holds which can be stated as the following

**Proposition 0.8.** *Let $G$ be a nonempty set with an associative binary operation. If the equations $ax = b$ and $ya = b$ have solutions in $G$ then $G$ is a group.*

*Proof.* We need to prove the existence of identity element and inverse of every element of $G$ in $G$. It follows that $G$ is a group with $1_G$ as the solution of the equations $ax = a$ and $ya = a$ and for any $g \in G$, $g^{-1}$ as the element of $G$ as a solution of the equations $gx = 1_G$ and $yg = 1_G$. □

## 0.10 Subgroups

**Definition:** A subset $H$ of a group $G$ is said to be a subgroup of $G$ if $H$ itself is a group under the binary operation of $G$ restricted to $H$. If $H$ is a subgroup of $G$ we denote this by $H \leq G$.

**Examples.** The following can be easily verified:

1. For every group $G$, $\{1_G\} \leq G$ and $G \leq G$. The subgroup $\{1_G\}$ is called trivial subgroups of $G$ and is denoted simply by 1. Any subgroup $H$ of $G$ such that $H \neq G$ is called its proper subgroup.
2. The orthogonal group $O_n(\mathbb{R})$ is a subroup of the group $GL_n(\mathbb{R})$.
3. Consider the dihedral group $D_{2n} = \langle r, s \mid r^n = 1 = s^2,\ rs = sr^{-1} \rangle$. The subsets $R_{2n} := \{1, r, ..., r^{n-1}\}$ and $S := \{1, s\}$ are subgroups of $D_{2n}$. There are other subgroups as well. Find out all of them.
4. The subset $H = \{\bar{0}, \bar{2}, \bar{4}, \bar{6}\}$ is a subgroup of $\mathbb{Z}/8\mathbb{Z}$.
5. $\mathbb{Z} \leq \mathbb{Q} \leq \mathbb{R} \leq \mathbb{C}$.
6. The set $H := \{(1), (123), (132)\}$ is a subgroup of $S_3$.
7. If $H$ and $K$ are subgroups of a group $G$ then $H \cap K \leq G$.
8. If $H \leq K$ and $K \leq G$ then $H \leq G$.
9. For any $x \in G$ the subset $\langle x \rangle \leq G$ called cyclic subgroup of $G$ generated by $x$.

Using definition, it is often tedious if not difficult in verifying that a certain subset $H$ of a group $G$ is its subgroup. To overcome this, we have the following lemma which gives us a necessary check for whether a subset of a group is a subgroup or not.

**Lemma 0.9. (Subgroup criterion)** *A subset $H$ of a group $G$ is a subgroup of $G$ if and only if the following two axioms are satisfied.*
*(1) $H \neq \emptyset$*
*(2) $xy^{-1} \in H$ for all $x, y \in H$.*

*Proof.* If $H$ is a subgroup of $G$ then $H$ itself is a group therefore (1) and (2) hold. Conversely let (1) and (2) hold. Since $H \subset G$ and $G$ is a group, associative law holds in $H$. By (1) there exists an $x \in H$ and by (2) $xx^{-1} = 1_G \in H$; clearly $1_G = 1_H$. Also for any $x \in H$ $1_G x^{-1} = x^{-1} \in H$. Finally for $x, y \in H$, $y^{-1} \in H$ and therefore $x(y^{-1})^{-1} = xy \in H$ thus $H$ is closed under multiplication. Hence $H \leq G$. □

**Definition: (Group table)** Let $G := \{x_1, x_2, ..., x_n\}$ be a finite group of order $n$ with $x_1 = 1_G$. The multiplication table or group table of $G$ is the $n \times n$ matrix $(a_{ij})_{n \times n}$ such that $a_{ij} := x_i x_j$.

**Remark:** It is easy to see that a finite group is abelian if and only if its group table is a symmetric matrix.

## 0.11 References:


1. James R. Munkres. *Topology*, Prentice Hall of India, 2nd Ed. (2007).
2. D.S. Dummit and R. Foote. *Abstract Algebra*, John Wiley (2007).
3. J. A. Gallian. *Contemporary Abstract Algebra*, Narosa(1999).
4. K. Tapp. *Matrix Groups for Undergraduates*, AMS (2005)
5. McCleary. *A First Course in Topology*, AMS (2006).

# Exercises

1. Prove that a nonempty set $A$ is simply ordered if and only if every finite subset of it is simply ordered.
2. Prove that between any two real numbers, there is a rational number.
3. Find at least one solution of the equation $10x + 6y = 2$ for $x, y \in \mathbb{Z}$.
4. Prove that the equation $x^2 = 2$ has no solution in integers.
5. If $R_\theta = \begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix}$, show that for any $\theta_1, \theta_2 \in \mathbb{R}$, $R_{\theta_1} R_{\theta_2} = R_{\theta_1+\theta_2}$.
6. Define a relation $\sim$ on a group $G$ via the following: $x \sim y$ in $G$ if and only if $x = g^{-1}yg$, for some $g \in G$. Prove that $\sim$ is an equivalence relation on $G$. Determine the set of equivalence classes of this relation.
7. Determine orders of all elements of the permutation group $S_4$.
8. Let $G$ be a group and $x \in G$. Define $\text{Stab}(x) := \{g \in G \mid gxg^{-1} = x\}$. Prove that $\text{Stab}(x) \leq G$.
9. Show that $\mathbb{R}^n$ is a group under the component wise addition rule i.e. for $(x_1, ..., x_n) \in \mathbb{R}^n$ and $(y_1, ..., y_n) \in \mathbb{R}^n$ we define
$$(x_1, ..., x_n) + (y_1, ..., y_n) = (x_1 + y_1, ..., x_n + y_n).$$
10. Prove that the identity element $1_G$ of a group $G$ is unique. Also establish that for any $x \in G$ $x^{-1}$ is uniquely determined.
11. Show that for any two elements $x$ and $y$ of a group $G$ $(xy)^{-1} = y^{-1}x^{-1}$ and $(x^{-1})^{-1} = x$.
12. Assume that $G = \{1, a, b, c\}$ is a group of order 4 with identity 1. Assume that $G$ has no element of order 4. Prove that $G$ is abelian.
13. Let $x \in G$ be an element of finite order $n$. Prove that the elements $1, x, x^2, ..., x^{n-1}$ are all distinct. Deduce that $|x| \leq |G|$.
14. If $x^2 = 1_G$ for all $x \in G$, prove that $G$ is abelian.
15. Let $G$ be a group of order 100. Prove that there is an element of order 2 in $G$.
16. Let $n > 1$ be a positive integer. Prove that $n$ $n-$th roots of unity form a group under usual multiplication.
17. Write a presentation of each of the following groups: $Q_8$, $\mathbb{Z}$, $\mathbb{Z}/20\mathbb{Z}$, $D_{12}$.
18. Show that the permutation group $S_n$ is non-abelian for all $n > 2$.
19. $\sigma$ be a $m-$cycle show that $\sigma^i$ is also an $m-$cycle if and only if $\gcd(i, m) = 1$.
20. Show that if $m \leq n$ then the number of $m-$cycles in $S_n$ is given by
$$\frac{n(n-1)(n-2)\cdots(n-m+1)}{m}.$$
21. Let $G := \{x \in \mathbb{R} \mid 0 \leq x < 1\}$. Define a binary relation $*$ on $G$ such that
$$x * y = x + y - [x + y]$$
where $[\cdot]$ denote the greatest integer function. Show that $(G, *)$ is a group.
22. Let $x, g$ be elements of a group $G$. Show that $|x| = |x^{-1}| = |gxg^{-1}|$. Deduce that $|xg| = |gx|$.
23. Define direct product $\mathbb{Z} \times \mathbb{Z}$ of the additive group $(\mathbb{Z}, +)$ with the binary operation of addition $\oplus$ defined by
$$(x, y) \oplus (a, b) = (x + a, y + b).$$
Show that $(\mathbb{Z} \times \mathbb{Z}, \oplus)$ is a group.
24. Let $f$, $F$ be two arithmetic functions such that $F(n) := \sum_{d|n} f(d)$. Prove the Möbius inversion formula $f(n) = \sum_{d|n} \mu(d) F\left(\frac{n}{d}\right)$ where $\mu$ is the Möbius function. Also show that $\sum_{d|n} \varphi(d) = n$.
25. Let $G$ be a group and $x \in G$. Define a subset $H := \{x^n \mid n \in \mathbb{Z}\}$. Show that $H$ is a subgroup of $G$.
26. If $x$ is an element of infinite order in a group $G$, then show that the elements $x^n$, $n \in \mathbb{Z}$ are all distinct.
27. Let $G$ be a group and define
$$Z(G) := \{x \in G \mid gx = xg \ \forall \ g \in G\}.$$
Prove that $Z(G) \leq G$. The subgroup $Z(G)$ is called *center of* $G$.