Semigroup

A finite or infinite set $‘S'$ with a binary operation $‘o'$ (Composition) is called semigroup if it holds following two conditions simultaneously −

- **Closure** − For every pair $(a, b) \in S,\ (aob)$ has to be present in the set S.
- **Associative** − For every element $a, b, c \in S, (aob)oc = ao(boc)$ must hold.

Example

The set of positive integers (excluding zero) with addition operation is a semigroup. For example, $S = \{1, 2, 3, \dots\}$

Here closure property holds as for every pair $(a, b) \in S, (a + b)$ is present in the set S.

For example, $1 + 2 = 3 \in S]$

Associative property also holds for every element $a, b, c \in S, (a + b) + c = a + (b + c)$.

For example, $(1 + 2) + 3 = 1 + (2 + 3) = 5$

Monoid

A monoid is a semigroup with an identity element. The identity element (denoted by e or E) of a set S is an element such that $(aoe) = a$, for every element $a \in S$. An identity element is also called a **unit element**. So, a monoid holds three properties simultaneously − **Closure, Associative, Identity element**.

Example

The set of positive integers (excluding zero) with multiplication operation is a monoid. $S = \{1, 2, 3, \dots\}$

Here closure property holds as for every pair $(a, b) \in S, (a \times b)$ is present in the set S.

[For example, $1 \times 2 = 2 \in S$ and so on]

Associative property also holds for every element $a, b, c \in S, (a \times b) \times c = a \times (b \times c)$

[For example, $(1 \times 2) \times 3 = 1 \times (2 \times 3) = 6$ and so on]

Identity property also holds for every element $a \in S, (a \times e) = a$ [For example, $(2 \times 1) = 2, (3 \times 1) = 3$ and so on]. Here identity element is 1.

Group

A group is a monoid with an inverse element. The inverse element (denoted by I) of a set S is an element such that $(aoI) = (Ioa) = a$, for each element $a \in S$. So, a group holds four properties simultaneously - i) Closure, ii) Associative, iii) Identity element, iv) Inverse element. The order of a group G is the number of elements in G and the order of an element in a group is the least positive integer n such that an is the identity element of that group G.

Examples

The set of $N \times N$ non-singular matrices form a group under matrix multiplication operation.

The product of two $N \times N$ non-singular matrices is also an $N \times N$ non-singular matrix which holds closure property.

Matrix multiplication itself is associative. Hence, associative property holds.

The set of $N \times N$ non-singular matrices contains the identity matrix holding the identity element property.

As all the matrices are non-singular they all have inverse elements which are also nonsingular matrices. Hence, inverse property also holds.

Abelian Group

An abelian group G is a group for which the element pair $(a, b) \in G$ always holds commutative law. So, a group holds five properties simultaneously - i) Closure, ii) Associative, iii) Identity element, iv) Inverse element, v) Commutative.

Example

The set of positive integers (including zero) with addition operation is an abelian group. $G = \{0, 1, 2, 3, \ldots\}$

Here closure property holds as for every pair $(a, b) \in S, (a + b)$ is present in the set S.

[For example, $1 + 2 = 2 \in S$ and so on]

Associative property also holds for every element $a, b, c \in S, (a + b) + c = a + (b + c)$

[For example, $(1 + 2) + 3 = 1 + (2 + 3) = 6$ and so on]

Identity property also holds for every element $a \in S, (a \times e) = a$ [For example,

$(2 \times 1) = 2, (3 \times 1) = 3$ and so on].

Here, identity element is 1.

Commutative property also holds for every element $a \in S, (a \times b) = (b \times a)$ [For example, $(2 \times 3) = (3 \times 2) = 3$ and so on]

Cyclic Group and Subgroup

A **cyclic group** is a group that can be generated by a single element. Every element of a cyclic group is a power of some specific element which is called a generator. A cyclic group can be generated by a generator 'g', such that every other element of the group can be written as a power of the generator 'g'.

Example

The set of complex numbers $\{1, -1, i, -i\}$ under multiplication operation is a cyclic group.

There are two generators − i and $-i$ as $i^1 = i, i^2 = -1, i^3 = -i, i^4 = 1$ and also $(-i)^1 = -i, (-i)^2 = -1, (-i)^3 = i, (-i)^4 = 1$ which covers all the elements of the group. Hence, it is a cyclic group.

Note − A **cyclic group** is always an abelian group but not every abelian group is a cyclic group. The rational numbers under addition is not cyclic but is abelian.

A **subgroup** H is a subset of a group G (denoted by $H \leq G$) if it satisfies the four properties simultaneously − **Closure, Associative, Identity element**, and **Inverse**.

A subgroup H of a group G that does not include the whole group G is called a proper subgroup (Denoted by $H < G$). A subgroup of a cyclic group is cyclic and a abelian subgroup is also abelian.

Example

Let a group $G = \{1, i, -1, -i\}$

Then some subgroups are $H_1 = \{1\}, H_2 = \{1, -1\}$,

This is not a subgroup − $H_3 = \{1, i\}$

because that $(i)^{-1} = -i$ is not in H_3

Definition

A **ring** is a set R together with a pair of binary operations + and . satisfying the axioms:

1. R is an abelian group under the operation + ,
2. The operation . is associative (and it is of course closed also),
3. The operations satisfy the *Distributive Laws*:
   For $\forall\ a, b, c \in R$ we have $(a + b).c = (a.c + b.c)$ and $a.(b + c) = a.b + a.c$.

Remarks

a. The *additive identity* is called the **zero** of the ring and is written 0.
   Note that $0.a = a.0 = 0$ for all $a \in R$ (See Exercises 1 Qu 1)

b. *Sometimes* the ring has a multiplicative identity. If it does, we call it a **Ring with identity** and write the multiplicative identity as 1.

c. Even if the ring has an identity, it may not be possible to find multiplicative inverses. In particular (if $|R| > 1$) the element 0 will never have an inverse.

d. The operation . is not necessarily commutative. If it is, we call R a **commutative ring**.

Examples

1. The integers $\mathbf{Z}$ with the usual addition and multiplication is a commutative ring with identity. The only elements with (multiplicative) inverses are ± 1.

2. The integers modulo n: $\mathbf{Z}_n$ form a commutative ring with identity under addition and multiplication modulo n. This is a finite ring $\{0, 1, \ldots , n - 1\}$ and the elements a which are coprime to n are the ones which are invertible.

3. The sets $\mathbf{Q}$, $\mathbf{R}$, $\mathbf{C}$ are all commutative rings with identity under the appropriate addition and multiplication. In these every non-zero element has an inverse.

4. The quaternions $\mathbf{H} = \{a + ib + jc + kd \mid a, b, c, d \in \mathbf{R}\}$ mentioned in the last section form a *non-commutative* ring with identity under the appropriate addition and a multiplication which satisfies the rules:
   $$i^2 = j^2 = k^2 = i\,j\,k = -1.$$
   In fact one can find an inverse for any non-zero quaternion using the trick:

$$(a + ib + jc + kd)(a - ib - jc - kd) = a^2 + b^2 + c^2 + d^2$$
as in the similar method for finding the inverse of a complex number.

5. The set of all 2×2 real matrices forms a ring under the usual matrix addition and multiplication.
   This is a non-commutative ring with identity $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.
   In fact, the set of $n \times n$ matrices with entries in *any ring* forms a ring.

6. Just as we can specify a finite group by giving its multiplication table, we can specify a finite ring by giving addition and multiplication tables.
   For example, $R = \{0, a, b, c\}$ with tables

+	0	a	b	c
0	0	a	b	c
a	a	0	c	b
b	b	c	0	a
c	c	b	a	0

.	0	a	b	c
0	0	0	0	0
a	0	0	a	a
b	0	0	b	b
c	0	0	c	c

   Then it is true (but almost impossible to check) that these do satisfy the ring axioms.
   In fact these are the addition and multiplication tables of
   $$0 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \quad a = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \quad b = \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix} \quad c = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$
   where arithmetic is done modulo 2.

7. **Polynomials**
   As indicated in the last section these are some of the most important examples of rings.

   Definition

   Let R be a commutative ring with an identity. Then a **polynomial with coefficients in R in an indeterminate** x is something of the form

   $$a_0 + a_1x + a_2x^2 + ... + a_nx^n \text{ where } a_i \in R.$$
   One adds and multiplies polynomials "in the usual way".
   The ring of such polynomials is denoted by $R[x]$.

   Remarks

   a. Note that each non-zero polynomial has a finite degree: the largest n for which $a_n \neq 0$.

   b. The indeterminate x is **not** a member of R. Neither are x^2, x^3, ... They are simply "markers" to remind us how to add and multiply.
      One could (and maybe should) define a polynomial to be a sequence $(a_0, a_1, a_2, ...)$ in which only finitely many of the terms are non-zero.
      Exercise: Write down how to add and multiply two such sequences.

   c. Two polynomials are equal if and only if all of their coefficients are equal.

Integral domains and Fields

These are two special kinds of ring

Definition

If a, b are two ring elements with $a, b \neq 0$ but $ab = 0$ then a and b are called **zero-divisors**.

Example

In the ring $\mathbf{Z}_6$ we have $2.3 = 0$ and so 2 and 3 are zero-divisors.
More generally, if n is not prime then $\mathbf{Z}_n$ contains zero-divisors.

Definition

An **integral domain** is a commutative ring with an identity ($1 \neq 0$) with no zero-divisors.
That is $ab = 0 \Rightarrow a = 0$ or $b = 0$.

Examples

1. The ring $\mathbf{Z}$ is an integral domain. (This explains the name.)

2. The polynomial rings $\mathbf{Z}[x]$ and $\mathbf{R}[x]$ are integral domains.
   (Look at the degree of a polynomial to see how to prove this.)

3. The ring $\{a + b\sqrt{2} \mid a, b \in \mathbf{Z}\}$ is an integral domain.
   (Proof?)

4. If p is prime, the ring $\mathbf{Z}_p$ is an integral domain.
   (Proof?)

Definition

A **field** is a commutative ring with identity ($1 \neq 0$) in which every non-zero element has a multiplicative inverse.

Examples

The rings $\mathbf{Q}, \mathbf{R}, \mathbf{C}$ are fields.

Remarks

a. If a, b are elements of a field with $ab = 0$ then if $a \neq 0$ it has an inverse a^{-1} and so multiplying both sides by this gives $b = 0$. Hence there are no zero-divisors and we have:

Every field is an integral domain.

b. The axioms of a field F can be summarised as:
   i. $(F, +)$ is an abelian group
   ii. $(F - \{0\}, .)$ is an abelian group
   iii. The distributive law.

The example **Z** shows that some integral domains are not fields.

Theorem

Every finite integral domain is a field.

Proof

The only thing we need to show is that a typical element $a \neq 0$ has a multiplicative inverse.
Consider a, a^2, a^3, ... Since there are only finitely many elements we must have $a^m = a^n$ for some $m < n$(say).
Then $0 = a^m - a^n = a^m(1 - a^{n-m})$. Since there are no zero-divisors we must have $a^m \neq 0$ and hence $1 - a^{n-m} = 0$ and so $1 = a(a^{n-m-1})$ and we have found a multiplicative inverse for a. □

More examples

1. If p is prime $\mathbf{Z}_p$ is a field. It has p elements.

2. Consider the set of things of the form $\{a + bx \mid a, b \in \mathbf{Z}_2\}$ with x an "indeterminate".
   Use arithmetic modulo 2 and multiply using the "rule" $x^2 = x + 1$.
   Then we get a field with 4 elements: $\{0, 1, x, 1 + x\}$.
   For example: $x(1 + x) = x + x^2 = x + (1 + x) = 1$ (since we work modulo 2). Thus every non-zero element has a multiplicative inverse.

3. Consider the set of things of the form $\{a + bx + cx^2 \mid a, b, c \in \mathbf{Z}_2\}$ where we now use the rule $x^3 = 1 + x$.
   This gives a field with 8 elements: $\{0, 1, x, 1 + x, x^2, 1 + x^2, x + x^2, 1 + x + x^2\}$.
   For example, $(1 + x^2)(x + x^2) = x + x^2 + x^3 + x^4 = x + x^2 + (1 + x) + x(1 + x) = 1 + x$ since we work modulo 2.

   Exercise: Experiment by multiplying together elements to find multiplicative inverses.
   (e.g. Since $x^3 + x = 1$ we have $x(x^2 + 1) = 1$ and $x^{-1} = 1 + x^2$.

4. Consider the set of things of the form $\{a + bx \mid a, b \in \mathbf{Z}_3\}$ with arithmetic modulo 3 and the "rule" $x^2 = -1$ (so its a bit like multiplying in **C** !).
   Then we get a field with 9 elements: $\{0, 1, 2, x, 1 + x, 2 + x, 2x, 1 + 2x, 2 + 2x\}$.
   Exercise: Find mutiplicative inverses.