CC4/GE-4 / (Unit-1) Algebra-II

(*) A non empty set G is said to form a group with respect to a binary composition if

i) G is closed under the composition $*$

ii) $*$ is associative.

iii) there exists an element e in G such that $e*a = a*e = a, \forall a \in G$.

iv) for each a in G, there exists an element a' in G such that $a'*a = a*a' = e$.

The group is denoted by the symbol $(G,*)$.

(*) The element e is said to be the identity element of the group and there is only one such element in the group.

(*) The element a' is said to be an inverse of a and there is only one inverse for each a in G.

(*) $(G,*)$ is said to be a commutative group or abelian group if $a*b = b*a$, for all a,b in G.

Examples: 1) The set $\mathbb{Z}$ forms a commutative group with respects to addition:

i) Let $a,b \in \mathbb{Z}$, then $a+b \in \mathbb{Z}$, this shows that $\mathbb{Z}$ is closed under $+$.

ii) Addition is associative in $\mathbb{R}$, $\mathbb{Z} \subseteq \mathbb{R}$, so addition is associative in $\mathbb{Z}$.

iii) 0 is the identity element in $\mathbb{Z}$.

iv) for each $a \in \mathbb{Z}$, $-a \in \mathbb{Z}$ and $a+(-a)=0$; so $-a$ is the inverse of a.

v) for each pair of a,b in $\mathbb{Z}$, $a+b = b+a$, so '$+$' is commutative, so $(\mathbb{Z},+)$ is a commutative group.

2) $(\mathbb{Q},+)$ is commutative group 3) $(\mathbb{R},+)$ is commutative group.

4) $(\mathbb{C},+)$ is commutative group.

5) Let $M_2(\mathbb{R})$ be the set of all 2×2 matrices whose elements are real numbers.

$M_2(\mathbb{R})$ is a commutative group w.r.t $(+)$

(*) A group $(G, *)$ is said to be a finite group if G contains a finite number of elements.

Eg: $S = \{1, \omega, \omega^2\}$, where $\omega^3 = 1$, the composition table is shown below.

⊛	1	ω	ω^2
1	1	ω	ω^2
ω	ω	ω^2	1
ω^2	ω^2	1	ω

then S is commutative group under multiplication

Subgroup

Let $(G, *)$ be a group and H be a non empty subset of G. if $(H, *)$ is a group where $*$ is the induced composition, then $(H, *)$ is a subgroup of $(G, *)$

Eg: $(\mathbb{Z}, +)$ is a subgroup of $(\mathbb{Q}, +)$

Let $(G, *)$ be a group. Necessary and sufficient condition for a non empty subset H of G to form a subgroup of $(G, *)$ is that for $a, b \in H \Rightarrow a * b^{-1} \in H$.

Ring

A non empty set R is a ring with respect to two binary compositions $+$ and $\cdot$ if

i) $a + b \in R$, $\forall a, b \in R$.

ii) $a + (b + c) = (a + b) + c$, $\forall a, b, c$ in R.

iii) there exists 0 in R such that $0 + a = a + 0 = a$, $\forall a$ in R.

iv) for each a in R, there exists $-a$ in R such that $a + (-a) = 0$.

v) $a + b = b + a$, $\forall a, b$ in R.

vi) $a \cdot b \in R$, $\forall a, b \in R$.

vii) $a\cdot(b\cdot c) = (a\cdot b)\cdot c, \quad \forall a,b,c$ in R.

viii) $a\cdot(b+c) = a\cdot b + a\cdot c, \quad \forall a,b,c$ in R

ix) $(b+c)\cdot a = b\cdot a + c\cdot a, \quad \forall a,b,c$ in R.

then $(R,+,\cdot)$ is said to be a ring. R is commutative if $\cdot$ is commutative. If R has multiplicative unity i.e I such that $a\cdot I = I\cdot a = a, \forall a \in R$, then R is said to be the ring with unity.

Eg: $(\mathbb{Z},+,\cdot)$ is commutative ring with unity

$(\mathbb{Q},+,\cdot)$ is commutative ring with unity

$(\mathbb{R},+,\cdot)$ is commutative ring with unity.

5. Ring of Gaussian integers. Let us consider the subset of $\mathbb{C}$ given by $\mathbb{Z}[i] = \{a + ib : a,\ b \in \mathbb{Z}\}$.

$\mathbb{Z}[i]$ is the set of all complex numbers of the form $a + ib$, where a and b are integers.

$\mathbb{Z}[i]$ forms a ring under addition and multiplication of complex numbers. This is a commutative ring with unity.

This ring is called the *ring of Gaussian integers.*

6. Ring of Gaussian numbers. Let us consider the subset of $\mathbb{C}$ given by $\mathbb{Q}[i] = \{a + ib : a,\ b \in \mathbb{Q}\}$.

$\mathbb{Q}[i]$ is the set of all complex numbers of the form $a + ib$, where a and b are rational numbers.

$\mathbb{Q}[i]$ forms a ring under addition and multiplication of complex numbers. This is a commutative ring with unity.

This ring is called the *ring of Gaussian numbers.*

7. Ring of Quaternions. Let us consider the set H of 2×2 complex matrices given by

$$H = \left\{ \begin{pmatrix} a+ib & c+id \\ -c+id & a-ib \end{pmatrix} : a, b, c, d \in \mathbb{R} \right\}.$$

$\begin{pmatrix} a+ib & c+id \\ -c+id & a-ib \end{pmatrix}$ can be expressed as $aI + bJ + cK + dL$, where

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},\ J = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix},\ K = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix},\ L = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}.$$

$(H, +, .)$ is a ring with respect to matrix addition and matrix multiplication. This is a non-commutative ring with unity, $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ being the unity.

This ring is called the *ring of real quaternions.*

The subset $\left\{ \begin{pmatrix} a+ib & c+id \\ -c+id & a-ib \end{pmatrix} : a, b, c, d \in \mathbb{Q} \right\}$ forms a ring with unity. This ring is called the *ring of rational quaternions.* This is also a non-commutative ring with unity.

The subset $\left\{ \begin{pmatrix} a+ib & c+id \\ -c+id & a-ib \end{pmatrix} : a, b, c, d \in \mathbb{Z} \right\}$ forms a ring with unity. This ring is called the *ring of integral quaternions.* This is also a non-commutative ring with unity.

3.4. Field.

A commutative skew field is a field.

In other words, a non-trivial ring R with unity is a field if it be commutative and each non-zero element of R is a unit.

Therefore, a non-empty set F forms a field with respect to two binary compositions + and ., if

(i) $a+b \in F$ for all a, b in F;

(ii) $a+(b+c)=(a+b)+c$ for all a, b, c in F;

(iii) there exists an element, called the zero element and denoted by 0, in F such that $a+0=a$ for all a in F;

(iv) for each element a in F there exists an element, denoted by $-a$, in F such that $a+(-a)=0$;

(v) $a+b=b+a$ for all a, b in F;

(vi) $a.b \in F$ for all a, b in F;

(vii) $a.(b.c)=(a.b).c$ for all a, b, c in F;

(viii) there exists an element, called the identity element and denoted by I, in F such that $a.I=a$ for all a in F;

(ix) for each *non-zero* element a in F there exists an element, denoted by a^{-1}, in F such that $a.(a^{-1})=I$;

(x) $a.b=b.a$ for all a, b in F;

(xi) $a.(b+c)=a.b+a.c$ for all a, b, c in F.

The field is denoted by $(F,+,.)$, or by F.

Examples.

1. The rings $(\mathbb{Q}, +, .)$, $(\mathbb{R}, +, .)$, $(\mathbb{C}, +, .)$ are familiar examples of a field. They are respectively called the field of all rational numbers, often denoted by $\mathbb{Q}$; the field of all real numbers, often denoted by $\mathbb{R}$; the field of all complex numbers, often denoted by $\mathbb{C}$.

2. The set $\{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$ forms a commutative ring with unity under addition and multiplication. The multiplicative inverse of $a + b\sqrt{2}$ where $(a, b) \neq (0, 0)$ is $\frac{a}{a^2-2b^2} + \frac{-b}{a^2-2b^2}\sqrt{2}$ and this belongs to the set because $a^2 - 2b^2 \neq 0$ and $\frac{a}{a^2-2b^2} \in \mathbb{Q}$, $\frac{-b}{a^2-2b^2} \in \mathbb{Q}$. Thus each non-zero element is a unit. Therefore the set forms a field. This is denoted by $\mathbb{Q}[\sqrt{2}]$.

Similarly, $\mathbb{Q}[\sqrt{3}]$, $\mathbb{Q}[\sqrt{5}]$, $\mathbb{Q}[\sqrt{7}]$, ... are fields.

3. The ring $(\mathbb{Z}_5, +, .)$ is a commutative ring with unity and each non-zero element of the ring is a unit. Therefore the ring $(\mathbb{Z}_5, +, .)$ is a field. As it contains a finite number of elements, it is a *finite* field.

Similarly, $(\mathbb{Z}_3, +, .)$, $(\mathbb{Z}_7, +, .)$, ... are finite fields.

3.5. Subring.

Let $(R, +, .)$ be a ring and S be a non-empty subset of R such that S is stable under $+$ and $.$, i.e.,

$$a \in S,\ b \in S \Rightarrow a + b \in S \text{ and } a.b \in S.$$

$+$ is a mapping from $R \times R$ to R. Since S is stable under $+$, the restriction of $+$ to $S \times S$, say $\oplus$, is a mapping from $S \times S$ to S and $\oplus : S \times S \to S$ is defined by

$$a \oplus b = a + b \text{ for all } a, b \in S.$$

Since S is stable under $.$, the restriction of $.$ to $S \times S$, say $\odot$, is a mapping from $S \times S$ to S and $\odot : S \times S \to S$ is defined by

$$a \odot b = a.b \text{ for all } a, b \in S.$$

If S forms a ring under the restriction compositions, S is said to be a *subring* of R. In this case we also say that R is an *over-ring* of S.

In other words, a non-empty subset S of R is said to be a *subring* of $(R, +, .)$ if S forms a ring under the compositions $+$ and $.$ restricted to S.

If S is a subring of $(R, +, .)$ it follows that $(S, +)$ is a subgroup of the group $(R, +)$ and $(S, .)$ is a subsemigroup of the semigroup $(R, .)$.

Therefore the zero element in R is also the zero element in S and the additive inverse of an element in S is also the additive inverse of the same element in R.

Nothing can be said about the equality or even about the existence of the unities of R and S. It may be possible that R and S have different unities, or S may have no unity while R has one such.

Examples.

1. Let R be a ring. Then R itself can be considered as a subring of R. This is said to be the *improper subring* of R.

The zero element of R forms a ring by itself. This is said to be the *trivial subring* of R.

2. $(\mathbb{Z}, +, .)$ is a ring with unity. $(2\mathbb{Z}, +, .)$ is a subring of the ring $(\mathbb{Z}, +, .)$ but the subring does not contain the unity.

3. $\mathbb{Z} \times \mathbb{Z}$ is a ring under addition $+$ and multiplication $.$ defined by $(a, b) + (c, d) = (a + c, b + d)$ and $(a, b).(c, d) = (ac, bd)$ for $(a, b), (c, d) \in \mathbb{Z} \times \mathbb{Z}$.

It is a commutative ring with unity, $(1, 1)$ being the unity.

Let us consider the subset S of $\mathbb{Z} \times \mathbb{Z}$ given by $S = \{(a, 0) : a \in \mathbb{Z}\}$.

Then S forms a ring under addition and multiplication restricted to S. So S is a subring of $\mathbb{Z} \times \mathbb{Z}$.

$(1,0)$ is the unity in S, since $(1,0).(a,0) = (a,0)$ for all $(a,0) \in S$.

Therefore the unity in the subring S is different from the unity in the ring $\mathbb{Z} \times \mathbb{Z}$.

Let us consider the subset T of $\mathbb{Z} \times \mathbb{Z}$ given by $T = \{(a,a) : a \in \mathbb{Z}\}$. Then T is a subring of $\mathbb{Z} \times \mathbb{Z}$.

$(1,1)$ is the unity in T and it is same as the unity in the ring $\mathbb{Z} \times \mathbb{Z}$.

4. $(\mathbb{Q}, +, .)$ is a ring with unity, 1 being the unity. $(\mathbb{Z}, +, .)$ is a subring of the ring $(\mathbb{Q}, +, .)$.

Here the unity in the subring is same as that in the ring.

Theorem 3.5.1. Let $(R, +, .)$ be a ring. A non-empty subset S of R forms a subring of R if and only if

(i) $(S, +)$ is a subgroup of $(R, +)$, and

(ii) S is closed under multiplication.

Proof. Let S be a subring of R. Then both the conditions (i) and (ii) are satisfied.

Conversely, let the conditions (i) and (ii) be satisfied in S.

Since (i) holds, $(S, +)$ is a commutative group. Since (ii) holds, S is closed under multiplication.

We need only to verify that multiplication is associative on S and the distributive laws hold in S. But these are hereditary properties and since they hold in R, they hold in the subset S.

Therefore S is a subring.

Theorem 3.5.2. Let $(R, +, .)$ be a ring and S be a non-empty subset of R. Then S is a subring of R if and only if

(i) $a \in S$, $b \in S \Rightarrow a - b \in S$; and (ii) $a \in S$, $b \in S \Rightarrow a.b \in S$.

3.6. Subfield.

A non-empty subset K of a field F is said to be a *subfield* of F if the elements of K form a field with respect to the compositions on F restricted to K.

Theorem 3.6.1. Let F be a field. A non-empty subset K is a subfield of F if and only if

(i) $a \in K,\ b \in K \Rightarrow a - b \in K$; and

(ii) $a \in K,\ 0 \neq b \in K \Rightarrow a.b^{-1} \in K$.

Proof left to the reader.

Examples.

1. $(\mathbb{R}, +, .)$ is a field. $\mathbb{Q} \subset \mathbb{R}$ and $(\mathbb{Q}, +, .)$ is a field. Therefore $(\mathbb{Q}, +, .)$ is a subfield of the field $(\mathbb{R}, +, .)$.

2. Let $\mathbb{Q}[\sqrt{2}]$ be the subset of $\mathbb{R}$ defined by $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$. Then $\mathbb{Q}[\sqrt{2}]$ is a non-empty subset of $\mathbb{R}$.

Let $a + b\sqrt{2} \in \mathbb{Q}[\sqrt{2}],\ c + d\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$. Then $a, b, c, d \in \mathbb{Q}$.

$(a + b\sqrt{2}) - (c + d\sqrt{2}) = (a - c) + (b - d)\sqrt{2} \in \mathbb{Q}[\sqrt{2}] \ldots$ (i)

Let $p + q\sqrt{2}$ be a non-zero element of $\mathbb{Q}[\sqrt{2}]$. Then $(p, q) \neq (0, 0)$.

$(p+q\sqrt{2})^{-1} = \frac{p}{p^2-2q^2} + \frac{-q\sqrt{2}}{p^2-2q^2} \in \mathbb{Q}[\sqrt{2}]$, since $p^2 - 2q^2 \neq 0$ for rational p, q where $(p, q) \neq (0, 0)$ and $\frac{p}{p^2-2q^2} \in \mathbb{Q}, \frac{-q}{p^2-2q^2} \in \mathbb{Q}$.

$(a + b\sqrt{2})(p + q\sqrt{2})^{-1} = \frac{ap-2bq}{p^2-2q^2} + \frac{bp-aq}{p^2-2q^2}\sqrt{2} \in \mathbb{Q}[\sqrt{2}] \ldots$ (ii)

From (i) and (ii) it follows that $\mathbb{Q}[\sqrt{2}]$ is a subfield of the field $\mathbb{R}$.

Real vector space.

A non-empty set V is said to form a *real vector space* (or a vector space over the field $\mathbb{R}$) if

(i) there is a binary composition $(+)$ on V, called 'addition', satisfying the conditions –

V1. $\alpha + \beta \in V$ for all $\alpha, \beta \in V$;

V2. $\alpha + \beta = \beta + \alpha$ for all $\alpha, \beta \in V$;

V3. $\alpha + (\beta + \gamma) = (\alpha + \beta) + \gamma$ for all $\alpha, \beta, \gamma \in V$;

V4. there exists an element θ in V such that $\alpha + \theta = \alpha$ for all $\alpha \in V$;

V5. for each α in V there exists an element $-\alpha$ in V such that $\alpha + (-\alpha) = \theta$;

and (ii) there is an external composition of $\mathbb{R}$ with V, called 'multiplication by real numbers' satisfying the conditions –

V6. $c\alpha \in V$ for all $c \in \mathbb{R}$, all $\alpha \in V$;

V7. $c(d\alpha) = (cd)\alpha$ for all $c, d \in \mathbb{R}$, all $\alpha \in V$;

V8. $c(\alpha + \beta) = c\alpha + c\beta$ for all $c \in \mathbb{R}$, all $\alpha, \beta \in V$;

V9. $(c + d)\alpha = c\alpha + d\alpha$ for all $c, d \in \mathbb{R}$, all $\alpha \in V$;

V10. $1\alpha = \alpha$, 1 being the identity element in $\mathbb{R}$.

The elements of V are called *vectors* and the elements of $\mathbb{R}$ are called *scalars*. $\mathbb{R}$ is said to be the *ground field* (or the *field of scalars*) of the vector space V.

Examples.

1. **Real vector space $\mathbb{R}^n$.** Let V be the set of all ordered n-tuples $\{(a_1, a_2, \ldots, a_n) : a_i \in \mathbb{R}\}$.

Let $+$ be a composition on V, called 'addition', defined by

$(a_1, a_2, \ldots, a_n) + (b_1, b_2, \ldots, b_n) = (a_1 + b_1, a_2 + b_2, \cdots, a_n + b_n)$

and an external composition of $\mathbb{R}$ with V, called 'multiplication by real numbers' be defined by

$c(a_1, a_2, \ldots, a_n) = (ca_1, ca_2, \cdots, ca_n), c \in \mathbb{R}$.

Then the conditions **V1-V10** are satisfied. Therefore V is a real vector space and it is denoted by $\mathbb{R}^n$.

$(0, 0, \ldots, 0)$ is the null vector of $\mathbb{R}^n$ and it is denoted by θ.

In a similar manner the vector spaces $\mathbb{R}^2, \mathbb{R}^3, \mathbb{R}^4, \ldots$ are defined. The set $\mathbb{R}$ itself forms a real vector space.

2. **Real vector space $\mathbb{C}$.** $\mathbb{C}$ is the set of all complex numbers $\{a + ib : a \in \mathbb{R}, b \in \mathbb{R}, i = \sqrt{(-1)}\}$.

Let $+$ be a composition on $\mathbb{C}$, called 'addition', defined by

$(a + ib) + (c + id) = (a + c) + i(b + d)$;

4.3. Sub-spaces.

Let V be a vector space over a field F with respect to addition (+) and multiplication by elements of F.

Let W be a non-empty subset of V. If W be stable under + and . then the restriction of + to $W \times W$ is a mapping from $W \times W$ to W and the restriction of . to $F \times W$ is a mapping from $F \times W$ to W. The restriction of +, say $\oplus$, is a composition on W and is defined by $\alpha \oplus \beta = \alpha + \beta$ for all $\alpha, \beta \in W$. The restriction of ., say $\odot$, is an external composition of F with W and is defined by $c \odot \alpha = c.\alpha$ for all $c \in F$ and all $\alpha \in W$.

If W forms a vector space over F with respect to $\oplus$ and $\odot$, then W is said to be a *sub-vector space* or a *linear subspace* or a *subspace* of V.

Theorem 4.3.1. A non-empty subset W of a vector space V over a field F is a subspace of V if and only if

(i) $\alpha \in W$, $\beta \in W \Rightarrow \alpha + \beta \in W$; and (ii) $\alpha \in W$, $c \in F \Rightarrow c\alpha \in W$.

Proof. Let the conditions hold in W.

Let $\alpha, \beta \in W$. Since F is a field, $-1 \in F$ where 1 is the identity element in F. By (ii) $-1\beta \in W$, i.e., $-\beta \in W$.

Then by (i) $\alpha + (-\beta) \in W$, i.e., $\alpha - \beta \in W$.

Thus $\alpha, \beta \in W \Rightarrow \alpha - \beta \in W$.

This proves that W is a subgroup of the additive group V. Since V is a commutative group, W is also a commutative subgroup of V.

Therefore the conditions **V1-V5** for a vector space are satisfied in W. **V6** is satisfied in W by(ii). The conditions **V7-V10** are satisfied in W since they are hereditary properties. Thus W is by itself a vector space over F and so W is a subspace of V.

The necessity of the conditions (i) and (ii) follows from the definition of a vector space.

Note. The two conditions (i) and (ii) can also be expressed as the single condition – $a\alpha + b\beta \in W$ for all $\alpha, \beta \in W$ and all $a, b \in F$.

Examples.