SCSVMV

Department of Mathematics

LECTURE NOTES

PG-ABSTRACT ALGEBRA

Dr T N KAVITHA

Proposed Date as per Time-table	Details of Lecture Topics to be Covered	Actual Date of Topics Covered
	Unit-I	
L1, L2	Normal subgroups and Quotient Groups	
L3, L4	Homomorphism	
L5, L6	Cauchy's theorem for Abelian Group	
L7-L8	Sylow's theorem for Abelian Group	
L9-L10	Automorphism	
L11-L12	Cayley's theorem	
	Unit-I test	
	Unit-II	
L1, L2	Permutation groups	
L3, L4	Conjugacy	
L5-L6	Normalizer- Centre	
L7-L8	Cauchy theorem	
L9-L10	Sylow's theorem	
L11, L12	Direct Products	
	Unit-II test	
	Unit-III	
L1-L2	Rings	
L3-L4	Homomorphism	
L5-L6	Ideals	
L7-L8	Quotient rings	
L9-L10	Maximal ideal	
L11-L12	Field of Quotients of integral domain	
	Unit-III test	

UNIT 1- Normal Subgroups

Let G be an abelian group, the composition in G being denoted multiplicatively. Let H be any subgroup of G. If x is an element of G, then Hx is a right coset of H in G and xH is a left coset of H in G. Also G is abelian, therefore we must have $Hx=xH \forall x \in G$. However, it is possible that G is not abelian, yet it is possesses a subgroup H such that $Hx=xH \forall x \in G$. Such subgroups of G fall under the category of normal subgroups, and they are very important.

Definition

A subgroup N of a group G is said to be a normal subgroup of G if for every $x \in G$ and for every $n \in N$, $xnx^{-1} \in N$.
From this definition we can immediately conclude that N is a normal subgroup of G if and only if

$xNx^{-1} \subset N \forall x \in G$

Theorems of Normal Subgroups

Theorem 1: A subgroup N of a group G is normal if and only if $xNx^{-1} = N \ \forall x \in G$.

Proof:

Let $xNx^{-1}=N \forall x \in G$, then $xNx^{-1} \subset N \ \forall \ x \in G$. Therefore N is a normal subgroup of G.

Conversely, let N be a normal subgroup of G. Then

$xNx^{-1} \subset N \ \forall x \in G$——(i)

Also $x \in G \Rightarrow x^{-1} \in G$. Therefore we have

$x^{-1}N(x^{-1})^{-1} \subset N \ \forall x \in G \Rightarrow x^{-1}Nx \subset N \ \forall x \in G$

$\Rightarrow x(x^{-1}nx)x^{-1} \subset xNx^{-1} \forall x \in G$

$\Rightarrow N \subset x^{-1}Nx \forall x \in G$——(ii)

From (i) and (ii) we can conclude that $xNx^{-1}=N \forall x \in G$

Theorem 2: A subgroup N of a group G is a normal subgroup of G if and only if each left coset of N in G is a right coset of N in G.

Proof: Let N be a normal subgroup of G then

$xNx^{-1}=N \forall x \in G \Rightarrow (xNx-1)x=Nx \forall x \in G$

$\Rightarrow xN=Nx \forall x \in G \Rightarrow$ each left coset xN is the coset Nx

Conversely, let each left coset of N in G be a right coset of N in G. This means that if x is any element of G, then the left coset xN is also a right coset. Now $e \in N$, and therefore $xe=x \in xN$. So x must also belong to that right coset which is equal to left coset xN. But x is an element of the right coset Nx, and two right cosets are either disjointed or identical, i.e. if two right cosets contain one common element then they are identical. Therefore Nx is the unique right coset which is equal to the left coset xN.

Therefore, we have $xN=Nx \forall x \in G \Rightarrow xNx-1=Nxx-1 \forall x \in G$

$\Rightarrow xNx-1=N \forall x \in G$

$\Rightarrow$ N is normal a subgroup of G.

Theorem 3: A subgroup N of a group G is a normal subgroup of G if and only if the product of two right cosets of N in G is again a right coset of N in G.

Theorem 4: The intersection of two normal subgroups of a group is a normal subgroup.

Center of a Group

Definition: The set Z of all those elements of a group G which commute with every element of G is called the center of the group G. Symbolically

$Z=\{z \in G : zx = xz \Rightarrow x \in G\}$

Theorem: The center Z of a group G is a normal subgroup of G.

Proof:

We have $Z=\{z \in G : zx = xz \forall x \in G\}$. First we shall prove that Z is a subgroup of G.

Let $z_1,z_2 \in Z$, then $z_1x = xz_1$ and $z_2x = xz_2$ for all $x \in G$

We have $z_2x = xz_2$, for all $x \in G$

$\Rightarrow z_2^{-1}(z_2x)z_2^{-1} = z_2^{-1}(xz_2)z_2^{-1} \Rightarrow xz_2^{-1} = z_2^{-1}x \ \forall x \in G$

$$\Rightarrow z_2^{-1} \in Z$$

Now $(z_1z_2^{-1})x = z_1(z_2^{-1}x) = z_1(xz_2^{-1}) = (z_1x)z_2^{-1} = (xz_1)z_2^{-1} = x(z_1z_2^{-1}) \Rightarrow z_1z_2^{-1} \in Z$

Thus, $z_1,z_2 \in Z \Rightarrow z_1z_2^{-1} \in Z$

Therefore, Z is a subgroup of G.

Now, we shall show that Z is a normal subgroup of G. Let $x \in G$ and $z \in Z$, then

$xzx^{-1} = (xz)x^{-1} = (zx)x^{-1} = z \in Z$

Thus, $x \in G$, $z \in Z \Rightarrow xzx^{-1} \in Z$

Quotient Groups

Definition: If G is a group and N is a normal subgroup of group G, then the set G| N of all cosets of N in G is a group with respect to the multiplication of cosets. It is called the quotient group or factor group of G by N. The identity element of the quotient group G|N by N.

Theorem: The set of all cosets of a normal subgroup is a group with respect to multiplication of complexes as the composition.

Proof:

Let N be a normal subgroup of a group G. Since N is normal in G, therefore each right coset will be equal to the corresponding left coset.

Thus there is no distinction between right and left cosets and we shall simply call them cosets. Let G|N be the collection of all cosets of N in G, i.e. let
$G|N=\{Na : a \in G\}$

Closure Property: Let $a,b \in G$, then $(Na)(Nb)=N(aN)b=N(Na)b=NNab=Nab$

Since $ab \in G$, therefore Nab is also a coset of N in G. So $Nab \in G|N$. Thus G|N is closed with respect to coset multiplication.

Associativity: Let $a,b,c \in G$. Then $Na, Nb, Nc \in G|N$. We have

$Na[(Nb)(Nc)]=Na(Nbc)=Na(bc)=N(ab)c=(Nab)Nc$

$=[(Na)(Nb)]Nc$

Thus the product of G|N satisfies the associative law.

Existence of Identity:

We have $N=Ne \in G|N$. Also if Na is any element of G|N, then

$N(Na)=(Ne)(Na)=Nea=Na(Na)N=(Na)(Ne)=Nae=Na$

Therefore the coset N is the identity element.

Existence of Inverse:

Let $Na \in G|N$, then $Na^{-1} \in G|N$. We have

$(Na)(Na^{-1}) = Naa^{-1} = Ne = N(Na^{-1})(Na) = Na^{-1}a = Ne = N$

Therefore the coset Na^{-1} is the inverse of Na. Thus each element of G|N possesses an inverse.

Hence G|N **is a group with respect to the product of cosets.**

Examples of Quotient Groups

<u>Example 1</u>: If H is a normal subgroup of a finite group G, then prove that

o(G|H)=o(G)o(H)

<u>Solution</u>: o(G|H) = number of distinct right (or left) cosets of H in G, as G|H is the collection of all right (or left) cosets of H in G

= number of distinct elements in G number of distinct elements in H

=o(G)o(H)

by Lagrange's Theorem

Example 2: Show that every quotient group of a cyclic group is cyclic, but not conversely.

Solution:

Let H be a subgroup of a cyclic group G. Then H is also cyclic because every cyclic group is abelian. Therefore H is a normal subgroup of G.

Let aa be a generator of G and an be any element of G, where n is an integer. Then Han is any element of G|H.

Also, it can be easily proved that (Ha)n=Han for every integer n. Therefore, G|H is cyclic and its generator is Ha.

Its converse is not true; for example if P3 and A3 are the symmetric and alternating groups of the three symbols a,b,c then the quotient group P3|A3 is cyclic, whereas P3 is not.

Example 3: Show that every quotient group of an abelian group is abelian but its converse is not true.

Solution:

Let a,b∈G be arbitrary, then Ha,Hb are any two elements of the quotient group G|H. Then we have (Ha)(Hb)=Hab=Hba=(Hb)(Ha)

Therefore, G|H is an abelian.

Its converse is not true; for example if P3 and A3 are the symmetric and alternating groups of the three symbols a,b,c then the quotient group P3|A3 being of order **2** is abelian whereas P3 is not.

Group Homomorphism

By homomorphism we mean a mapping from one algebraic system with a like algebraic system which preserves structures.

Definition

Let G and G′ be any two groups with binary operation ∘ and ∘’ respectively. Then a mapping $f:G \to G'$ is said to be a homomorphism if for all $a,b \in G$,

$f(a \circ b) = f(a) \circ' f(b)$

A homomorphism f which at the same time is also onto is said to be an epimorphism.

A homomorphism f which at the same time is also one-one is said to be an monomorphism.

A group G′ is called a homomorphism image of a group G, if there exists a homomorphism f of G onto G′. A homomorphism of a group G into itself is called an endomorphism.

Examples:

(i) Let G be any group under binary operation ∘. If $f(x)=x$ for every $x \in G$ then $f:G \to G$ is a homomorphism because

$f(xy)=f(x)f(y)$

(ii) Let G be the group of integers under addition, let G′ be the group of integers under addition modulo n. If $f:G \to G'$ be defined by f(x)=remainder of x on division by n, then this is a homomorphism.

(iii) Let G be any group under addition. If $f(x)=e, \forall x \in G$ then the mapping $f:G \to G$ is a homomorphism because for all $x,y \in G$, $f(x,y)=e$ and $f(x)+f(y)=e+e=e$, so that

$f(x+y)=f(x)+f(y)$

(iv) Let G be the group of integers under addition and let $G'=G$. If for all $x \in G$, $f(x)=2x$, then f is a homomorphism because

$f(x+y)=2(x+y)=2x+2y=f(x)+f(y)$

Kernel of Homomorphism

Definition

If f is a homomorphism of a group G into a G′, then the set K of all those elements of G which is mapped by f onto the identity e′ of G′ is called the kernel of the homomorphism f.

Theorem:

Let G and G′ be any two groups and let e and e′ be their respective identities. If f is a homomorphism of G into G′, then

(i) $f(e)=e'$

(ii) $f(x^{-1})=[f(x)]^{-1}$ for all $x \in G$

(iii) K is a normal subgroup of G.

Proof:

(i) We know that for $x \in G$, $f(x) \in G'$.

$f(x) \cdot e' = f(x) = f(xe) = f(x).f(e)$, and therefore by using left cancellation law we have $e'=f(e)$ or $f(e)=e'$

(ii) Since for any $x \in G$, $xx^{-1} = e$, we get

$f(x).f(x^{-1})=f(xx^{-1})=f(e)=e'$

Similarly $x^{-1}x = e$, gives $f(x^{-1}) \cdot f(x)=e'$

Hence by the definition of $[f(x)]^{-1}$ in G′ we obtain the result

$f(x^{-1})=[f(x)]^{-1}$

(iii) Since $f(e)=e'$, $e \in K$, this shows that $K \neq \phi$,

now let $a,b \in K$, $x \in G$, $a \in K, b \in K$,

$\Rightarrow f(a)=e', f(b)=e'$

$\Rightarrow f(a)=e', f(b^{-1})=[f(b)]^{-1}=e'$

$\Rightarrow f(ab^{-1}) = f(a)[f(b)]^{-1} = e' \cdot e' = e'$

$\Rightarrow ab^{-1} \in K$

This establishes that K is a subgroup of G.

Now, to show that it is also normal we prove the following:

$f(x^{-1}ax)=f(x^{-1})f(a)f(x)$

$=[f(x)]^{-1}f(a)f(x)$

$=[f(x)]^{-1}e'f(x)$

$=[f(x)]^{-1}f(x)=e'$

Therefore, $x^{-1}ax \in K$, hence the result

Examples of Group Homomorphism

Here's some examples of the concept of group homomorphism.

Example 1:

Let G={1,–1,i,–i}, which forms a group under multiplication and I= the group of all integers under addition, prove that the mapping f from I onto G such that f(x)=in∀n∈I is a homomorphism.

Solution: Since f(x)=in,f(m)=im, for all m,n∈I

f(m+n)=im+n =im⋅in = f(m)⋅f(n)

Hence f is a homomorphism.

Example 2:

Show that the mapping f of the symmetric group Pn onto the multiplicative group G ′={1,–1} defined by f(α)=1 or –1.

According as α is an even or odd permutation in Pn is a homomorphism of Pn onto G ′.

Solution: We know that the product of two permutations both even or both odd is even while the product of one even and one odd permutation is odd. We shall show that

f(αβ)=f(α)f(β)∀α,β∈Pn

(i) if α,β are both even, then

$f(\alpha\beta)=1=1\cdot 1=f(\alpha)\cdot f(\beta)$

(ii) if α,β are both odd, then

$f(\alpha\beta)=1=(-1)\cdot(-1)=f(\alpha)\cdot f(\beta)$

(iii) if α is odd and β is even, then

$f(\alpha\beta)=-1=(-1)\cdot 1=f(\alpha)\cdot f(\beta)$

(iv) if α is even and βis odd, then

$f(\alpha\beta)=-1=1\cdot(-1)=f(\alpha)\cdot f(\beta)$

Thus $f(\alpha\beta)=f(\alpha)f(\beta)\forall\alpha,\beta\in Pn$. Also obviously f is onto G′.

Therefore f is a homomorphism of Pn onto G′.

Example 3:

Show that a homomorphism from s simple group is either trivial or one-to-one.

Solution: Let G be a simple group and f be a homomorphism of G into another group G′. Then the kernel f is a normal subgroup of G. But the only normal subgroups of the simple group G are G and {e}. Hence either K=G or K={e}. If K=G, the f–image of each element of G is the identity of G′, as such the homomorphism f is trivial one. If K={e}, the homomorphism f is one-to-one.

Cayley's Theorem

Cayley's Theorem:

Every group is isomorphic to a permutation group.

Proof: Let G be a finite group of order n. If a∈G, then ∀x∈G, ax∈G. Now consider a function from G into G, defined by

$f_a(x) = ax\forall x\in G$

For $x,y \in G, fa(x)=fa(y) \Rightarrow ax=ay \Rightarrow x=y$. Therefore, the function fa is one-one.

The function fa is also onto because if x is any element of G then there exists an element $a^{-1}x$ such that

$fa(a^{-1}x) = a(a^{-1}x)=(aa^{-1})x = ex = x$

Thus fa is one-one from G onto G. Therefore, fa is a permutation on G. Let G′ denote the set of all such one-to-one functions defined on G corresponding to every element of G, i.e. $G'=\{fa:a \in G\}$

Now, we show that G′ is a group with respect to the product of functions.

(i) <u>Closure Axiom</u>: Let $fa,fb \in G'$ where $a,b \in G$, then

$(fa \circ fb)x=fa[fb(x)]=fa(bx)=a(bx)=(ab)x=fab(x) \forall x \in G$

Since $ab \in G$, therefore $fab \in G'$ and thus G′ is closed under the product of functions.

(ii) <u>Associative Axiom</u>: Let $fa,fb,fc \in G'$ where $a,b,c \in G$, then

$fa \circ (fb \circ fc)=fa \circ fbc=fa(bc)=f(ab)c=fab \circ fc=(fa \circ fb) \circ fc$

The product of functions is associative in G′.

(iii) <u>Identity Axiom</u>: If e is the identity element in G, then fe is the identity of G′ because $\forall fx \in G'$ we have $fe \circ fx = fex = fx$ and $fx \circ fe = fxe = fx$.

(iv) <u>Inverse Element</u>: If a^{-1} is the inverse of a in G, then fa^{-1} is the inverse of fa in G′ because $fa^{-1} \circ fa = fa^{-1}a = fe$ and $fa \circ fa^{-1} = faa^{-1} = fe$

Hence G′ is a group with respect to the composite of functions denoted by the symbol ∘.

Now consider the function g and G into G′ defined by $g(a)=fa \forall a \in G$.
g is one-one because for $a,b \in G$.

$g(a)=g(b) \Rightarrow fa=fb \Rightarrow fa(x)=fb(x)$

$\Rightarrow ax=bx \Rightarrow a=b, \forall x \in G$

g is onto because if $f_a \in G'$ then for $a \in G$, we have $g(a)=f_a$

g preserves composition in G and G′ because if $a,b \in G$ then

$g(ab)=f_{ab}=f_a \circ f_b=g(a)\circ g(b)$

Hence $G \cong G'$.

References

Text Book:
Topics in Algebra, I.N.Heristein, Wiley india Pvt.Ltd, Second edition, 2006.

Reference Books:
1. Contemporary Abstract Algebra, Joseph A.Gallian, Brooks/Cole, Ninth edition, 2017.
2. A first course in abstract algebra, Fraleigh J.B, Narosa publications, Seventh edition, 2013.
3. Algebra, Serge Lang, Springer-Verlag New York, Third edition, 2002.
4. Algebra, Artin M, Prentice-Hall, New Jersey, Second edition, 1991.
5. Abstract Algebra, David. S. Dummit, Richarad M. Foote, John-Wiley & sons, Third edition, 2004

Weblink more: https://www.emathzone.com/tutorials/group-theory/cayleys-theorem.html#ixzz6U9DWmqWv

Video link:

NPTEL COURSE: https://www.youtube.com/watch?v=OjvZxxLb_78

UNIT 2- Conjugacy in a Group

<u>Conjugate Element</u>: If a, b∈G, then b is said to be a conjugate of a in G if there exists an element x ∈G such that $b = x^{-1}ax$.

Symbolically, we shall write a ~b for this and shall refer to this relation as conjugacy.

Then b ~a ⇔ $b = x^{-1}ax$ for some x∈G

DEF: equivalence relation

(i) **Reflexivity:** a ~a∀a∈G

(ii)Symmetric: a~b ⇒b~a

(iii) Transitivity: a~b, b~c ⇒a~c

<u>Theorem</u>: Conjugacy is an equivalence relation in a group.

<u>Proof</u>:

(i) Reflexivity: Let a∈G, then $a = e^{-1}ae$, hence a ~a∀a∈G, i.e. the relation of conjugacy is reflexive.

(ii) Symmetric: Let a~b so that there exists an element x∈G such that $a = x^{-1}bx$, a,b∈G. Now

$$a\sim b \Rightarrow a=x^{-1}bx \Rightarrow xa=x(x^{-1}bx)$$

$$\Rightarrow xax^{-1}=(xx^{-1})b(xx–1) \Rightarrow b=xax^{-1} \Rightarrow b=(x^{-1})^{-1}ax^{-1}, x\in G \Rightarrow b\sim a$$

Thus a~b=b~a. Hence the relation is symmetric.

(ii) **Transitivity:** Let there exist two elements x,y∈G

such that $a = x^{-1}bx$ and $b = y^{-1}cy$ for a,b,c∈G.

Hence a~b, b~c

$$\Rightarrow a=x^{-1}bx \text{ and} \Rightarrow b=x^{-1}cx \Rightarrow a=x^{-1}(y^{-1}cy)x \Rightarrow a=(x^{-1}y^{-1})c(yx) \Rightarrow a=(yx)^{-1}c(yx)$$

Here yx∈G and G are the group. Therefore a~b,b~c ⇒ a~c.

Hence the relation is transitive.

Thus conjugacy is an equivalence relation on G.

Conjugate Classes: For a∈G, let C(a)={x: x∈G and a~x}, C(a), the equivalence class of a in G under a conjugacy relation is usually called the conjugate class of a in G. It consists of the set of all

distinct elements of the type $y^{-1}ay$.
In other words, a group G is isomorphic to the group G′ if there exists a one-one onto mapping of G and G′ such that the image of the product of two elements is the product of the images of the elements with respect to the composition in the respective group.

The last condition may also be stated as follows:

If $ab = c$ where $a,b,c \in G$ and $f(a)=a'$, $f(b)=b'$, $f(c)=c'$ then $a'b'=c'$ where $a',b',c' \in G'$.

UNIT 3

Rings
Homomorphism
Ideals
Quotient rings
Maximal ideal
Field of Quotients of integral domain

Ring

A ring in the mathematical sense is a set S together with two binary operators $+$ and $*$ (commonly interpreted as addition and multiplication, respectively) satisfying the following conditions:

1. Additive associativity: For all $a, b, c \in S$, $(a+b)+c = a+(b+c)$,
2. Additive commutativity: For all $a, b \in S$, $a+b = b+a$,
3. Additive identity: There exists an element $0 \in S$ such that for all $a \in S$, $0+a = a+0 = a$,
4. Additive inverse: For every $a \in S$ there exists $-a \in S$ such that $a+(-a) = (-a)+a = 0$,
5. Left and right distributivity: For all $a, b, c \in S$, $a*(b+c) = (a*b)+(a*c)$ and $(b+c)*a = (b*a)+(c*a)$,
6. Multiplicative associativity: For all $a, b, c \in S$, $(a*b)*c = a*(b*c)$ (a ring satisfying this property is sometimes explicitly termed an associative ring).

Rings may also satisfy various optional conditions:

7. Multiplicative commutativity: For all $a, b \in S$, $a*b = b*a$ (a ring satisfying this property is termed a commutative ring),
8. Multiplicative identity: There exists an element $1 \in S$ such that for all $a \neq 0 \in S$, $1*a = a*1 = a$ (a ring satisfying this property is termed a unit ring, or sometimes a "ring with identity"),
9. Multiplicative inverse: For each $a \neq 0$ in S, there exists an element $a^{-1} \in S$ such that for all $a \neq 0 \in S$, $a*a^{-1} = a^{-1}*a = 1$, where 1 is the identity element.

Definition

A **ring** is a set R together with two operations $(+)$ and $(\cdot)$ satisfying the following properties (ring axioms):

(1) R is an abelian group under addition. That is, R is closed under addition, there is an additive identity (called 0), every element $a \in R$ has an additive inverse $-a \in R$, and addition is associative and commutative.

(2) R is closed under multiplication, and multiplication is associative:

$$\begin{aligned} \forall a,b \in R \quad & a\cdot b \in R \\ \forall a,b,c \in R \quad & a\cdot(b\cdot c) = (a\cdot b)\cdot c. \end{aligned}$$

(3) Multiplication distributes over addition:

$$\forall a,b,c \in R \quad a\cdot(b+c) = a\cdot b + a\cdot c \quad \text{and} \quad (b+c)\cdot a = b\cdot a + c\cdot a.$$

A ring is usually denoted by $(R, +, \cdot)$ and often it is written only as R when the operations are understood. □

A **ring** is a set R together with two operations (+) and (·) satisfying the following properties (ring axioms):

(1) R is an abelian group under addition. That is, R*R* is closed under addition, there is an additive identity (called 00), every element a\in R*a*∈*R* has an additive inverse -a\in R−*a*∈*R*, and addition is associative and commutative.

(2) R*R* is closed under multiplication, and multiplication is associative:\begin{aligned} \forall a,b&\in R &a\cdot b&\in R\\ \forall a,b,c&\in R &a\cdot (b\cdot c) &=(a\cdot b) \cdot c. \end{aligned}∀*a*,*b*∀*a*,*b*,*c*∈*R*∈*R**a*⋅*b**a*⋅(*b*⋅*c*)∈*R*=(*a*⋅*b*)⋅*c*.

(3) Multiplication distributes over addition:\forall a,b,c\in R\quad a\cdot \left(b+c \right) =a\cdot b+a\cdot c\quad \text{and}\quad \left(b+c \right) \cdot a=b\cdot a+c\cdot a.∀*a*,*b*,*c*∈*R**a*⋅(*b*+*c*)=*a*⋅*b*+*a*⋅*c*and(*b*+*c*)⋅*a*=*b*⋅*a*+*c*⋅*a*.

A ring is usually denoted by (R,+, \cdot)$(R,+,\cdot)$ and often it is written only as RR when the operations are understood. _\square□

Elementary Properties of Rings

Some basic elementary properties of a ring can be illustrated with the help of the following theorem, and these properties are used to further develop and build concepts on rings.

Theorem:

If R is a ring, then for all a,b are in R.

(a) $a\cdot 0=0\cdot a=aa\cdot 0=0\cdot a=a$
(b) $a(-b)=(-a)b=-(ab)a(-b)=(-a)b=-(ab)$
(c) $(-a)(-b)=ab(-a)(-b)=ab$

Proof:

(a) We know that
$a0=a(0+0)=a0+a0\forall a\in R$[usingdistributive law]$a0=a(0+0)=a0+a0\forall a\in R$[usingdistributive law]

Since RR is a group under addition, applying the right cancellation law,
$a0=a0+a0\Rightarrow a+a0=a0+a0\Rightarrow a0=0a0=a0+a0\Rightarrow a+a0=a0+a0\Rightarrow a0=0$

Similarly, $0a=(0+0)a=0a+0a\forall a\in R$[usingdistributive law]$0a=(0+0)a=0a+0a\forall a\in R$[usingdistributive law]
$\therefore 0+0a=0a+0a$[because$0=0a+0a$]$\therefore 0+0a=0a+0a$[because$0=0a+0a$]

Applying right cancellation law for addition, we get $0=0a0=0a$ i.e. $0a=00a=0$

Thus $a0=0a=0a0=0a=0$

(b) To prove that $a(-b)=-aba(-b)=-ab$ we should show that $ab=a(-b)=0ab=a(-b)=0$

We know that $a[b+(b)]=a0=0a[b+(b)]=a0=0$ because $b+(-b)=0b+(-b)=0$ with the above result **(a)**
$ab+a(-b)=0$[bydistributivelaw]$ab+a(-b)=0$[bydistributivelaw]
$\therefore a(-b)=-(ab)\therefore a(-b)=-(ab)$

Similarly, to show $(-a)b=-ab(-a)b=-ab$, we must show that $ab+(-a)b=0ab+(-a)b=0$

But $ab+(-a)b=[a+(-a)]b=0b=0ab+(-a)b=[a+(-a)]b=0b=0$
$\therefore -(a)b=-(ab)\therefore -(a)b=-(ab)$ hence the result.

(c) Proving $(-a)(-b)=ab(-a)(-b)=ab$ is a special case of forgoing the article. However its proof is given as:
$(-a)(-b)=-[a(-b)]=[-(ab)]=ab(-a)(-b)=-[a(-b)]=[-(ab)]=ab$

This is because $-(-x)=x-(-x)=x$ **is a consequence of the fact that in a group, the inverse of the inverse of an element is the element itself.**

Examples of Rings

Example 1:

A Gaussian integer is a complex number a+iba+ib, where aa and bb are integers. Show that the set J(i)J(i) of Gaussian integers forms a ring under the ordinary addition and multiplication of complex numbers.

Solution:

Let a1+ib1a1+ib1 and a2+ib2a2+ib2 be any two elements of J(i)J(i), then

(a1+ib1)+(a2+ib2)=(a1+a2)=i(b1+b2)=A+iB(a1+ib1)+(a2+ib2)=(a1+a2)=i(b1+b2)=A+iB

and

(a1+ib1)⋅(a2+ib2)=(a1a2–b1b2)+i(a1b2+b1a2)=C+iD(a1+ib1)⋅(a2+ib2)=(a1a2–b1b2)+i(a1b2+b1a2)=C+iD

These are Gaussian integers and therefore J(i)J(i) is closed under addition as well as the multiplication of complex numbers. Addition and multiplication are both associative and commutative compositions for complex numbers.

Also, multiplication distribution with respect to addition. The additive inverse of a+ib∈J(i)a+ib∈J(i) is (–a)+(–b)i∈J(i)(–a)+(–b)i∈J(i) as

(a+ib)=(–a)+(–b)i=(a–a)+(b–b)i=0+0i=0(a+ib)=(–a)+(–b)i=(a–a)+(b–b)i=0+0i=0

The Gaussian integer 1+0⋅i1+0⋅i is the multiplicative identity. Therefore, the set of Gaussian integers is a commutative ring with unity.

Example 2: Prove that the set of residue **{0, 1, 2, 3, 4}** modulo **5** is a ring with respect to the addition and multiplication of residue classes (**mod 5**).

Solution: Let **R = {0, 1, 2, 3, 4}.** Addition and multiplication tables for given set **R** are:

+ mod 5	**0**	**1**	**2**	**3**	**4**	**mod 5**	**0**	**1**	**2**	**3**	**4**
0	**0**	**1**	**2**	**3**	**4**	**0**	**0**	**0**	**0**	**0**	**0**
1	**1**	**2**	**3**	**4**	**0**	**1**	**0**	**1**	**2**	**3**	**4**
2	**2**	**3**	**4**	**0**	**1**	**2**	**0**	**2**	**4**	**1**	**3**
3	**3**	**4**	**0**	**1**	**2**	**3**	**0**				
4	**4**	**0**	**1**	**2**	**3**	**4**					

From the addition composition table the following is clear:

(i) Since all elements of the table belong to the set, it is closed under addition (**mod 5**).

(ii) Addition (**mod 5**) is always associative.

(iii) $0 \in R 0 \in R$ is the identity of addition.

(iv) The additive inverse of the elements **0, 1, 2, 3, 4** are **0, 4, 3, 2, 1** respectively.

(v) Since the elements equidistant from the principal diagonal are equal to each other, the addition (**mod 5**) is commutative.

From the multiplication composition table, we see that **(R, .)** is a semi group, i.e. following axioms hold good.

(vi) Since all the elements of the table are in **R**, the set **R** is closed under multiplication (mod 5).

(vii) Multiplication (**mod 5**) is always associative.

(viii) The multiplication (**mod 5**) is left as well as right distributive over addition (**mod 5**).

Hence $(R,+,\cdot)(R,+,\cdot)$ is a ring.

Special Types of Rings

1. Commutative Rings

A ring RR is said to be a commutative if the multiplication composition in RR is commutative, i.e.

$ab=ba \forall a,b \in Rab=ba \forall a,b \in R$

2. Rings With Unit Element

A ring RR is said to be a ring with unit element if RR has a multiplicative identity, i.e. if there exists an element RR denoted by 11, such that

$1 \cdot a=a \cdot 1 \forall a \in R1 \cdot a=a \cdot 1 \forall a \in R$

The ring of all $n \times nn \times n$ matrices with element as integers (rational, real or complex numbers) is a ring with unity. The unity matrix

In=⎡⎣⎢⎢⎢⎢⎢⎢⎢100⋮0010⋮0001⋮0⋯⋯⋯⋱⋯000⋮1⎤⎦⎥⎥⎥⎥⎥⎥⎥In=[100⋯0010⋯0001⋯0⋮⋮⋮⋱⋮000⋯1]

is the unity element of the ring.

3. Rings With or Without Zero Divisors

While dealing with an arbitrary ring RR, we may find elements aa and bb in RR, where neither of which is zero and their product may be zero. We call such elements divisors of zero or zero divisors.

Definition:

A ring element $a(\neq 0)a(\neq 0)$ is called a divisor of zero if there exists an element $b(\neq 0)b(\neq 0)$ in the ring such that either
$ab=0ab=0$ or $ba=0ba=0$

We also say that a ring RR is without zero divisors if the product of no two non-zero elements of the same is zero, i.e. if
$ab=0\Rightarrow ab=0\Rightarrow$ either $a=0a=0$ or $b=0b=0$ or both $a=0a=0$ and $b=0b=0$

Cancellation Laws in a Ring

Cancellation Laws in a Ring

We say that cancellation laws hold in a ring RR if
$ab=bc(a\neq 0)\Rightarrow b=cab=bc(a\neq 0)\Rightarrow b=c$ and $ba=ca(a\neq 0)\Rightarrow b=cba=ca(a\neq 0)\Rightarrow b=c$ where a,b,c a,b,c are in RR

Thus in a ring with zero divisors, it is impossible to define a cancellation law.

Theorem:

A ring has no divisor of zero if and only if the cancellation laws holds in R

Proof:

Suppose that RR has no zero divisors. Let a,b,ca,b,c be any three elements of RR such that $a\neq 0, ab=aca\neq 0, ab=ac$.

Now

$ab=ac\Rightarrow ab–ac=0\Rightarrow a(b–c)=0\Rightarrow b–$
$c=0$[becauseRiswithoutzerodivisoranda$\neq 0$]$\Rightarrow b=cab=ac\Rightarrow ab–ac=0\Rightarrow a(b–c)=0\Rightarrow b–$
$c=0$[becauseRiswithoutzerodivisoranda$\neq 0$]$\Rightarrow b=c$

Thus the left cancellation law holds in RR. Similarly, it can be shown that the right cancellation law also holds in RR.

Conversely, suppose that the cancellation law holds in RR. Let $a,b\in Ra,b\in R$ and if possible
let $ab=0ab=0$ with $a\neq 0,b\neq 0a\neq 0,b\neq 0$ then $ab=a\cdot 0ab=a\cdot 0$ (because $a\cdot 0=0a\cdot 0=0$).

Since $a\neq 0,ab=a\cdot 0\Rightarrow b=0a\neq 0,ab=a\cdot 0\Rightarrow b=0$

Hence we get a contradiction to our assumption that b≠0b≠0 and therefore the theorem is established.

Division Ring

A ring is called a division ring if its non-zero elements form a group under the operation of multiplication.

Pseudo Ring

A non-empty set RR with binary operations ++ and ×× satisfying all the postulates of a ring except right and left distribution laws is called pseudo ring if

(a+b)⋅(c+d)=a⋅c+a⋅d+b⋅c+b⋅d(a+b)⋅(c+d)=a⋅c+a⋅d+b⋅c+b⋅d

for all a,b,c,d∈Ra,b,c,d∈R

Notes:

(1) There are two further requirements one might impose on a ring S that lead to interesting classes of rings. For instance, if multiplication is commutative, the ring is called a **commutative ring.** The theory of commutative rings differs quite significantly from the the theory of non-commutative rings; commutative rings are better understood and have been more extensively studied. Most of the examples and results in this wiki will be for commutative rings. Again there may be an element 1 in R such that for all elements a in R, $a \cdot 1 = 1 \cdot a = a$. If such an element exists, we call it the unity of the ring, and the ring is called a **ring with unity.** Else it is called a ring without unity or a "rng" (a ring without i).

(2) If R is a commutative ring and $a, b, c \in R$ such that $a, b \neq 0$ and $a \cdot b = c$, then a and b are said to be divisors of c. If in a commutative ring R with unity, there is no divisor of the additive identity, i.e. 0, then R is said to be an **integral domain.** Thus a commutative ring R with unity is said to be an integral domain if for all elements a, b in R, $a \cdot b = 0$ implies either $a = 0$ or $b = 0$.

(3) If every nonzero element in a commutative ring with unity has a multiplicative inverse as well, the ring is called a field. Fields are fundamental objects in number theory, algebraic geometry, and many other areas of mathematics. If every nonzero element in a ring with unity has a multiplicative inverse, the ring is called a **division ring** or a **skew field.** A field is thus a commutative skew field. Non-commutative ones are called strictly skew fields.

Examples of Rings

This section lists many of the common rings and classes of rings that arise in various mathematical contexts.

(1) The ring $\mathbb{Z}$ of integers is the canonical example of a ring. It is an easy exercise to see that $\mathbb{Z}$ is an integral domain but not a field.

(2) There are many other similar rings studied in algebraic number theory, of the form $\mathbb{Z}[\alpha]$, where α is an algebraic integer. For example, $\mathbb{Z}\left[\sqrt{2}\right] = \{a + b\sqrt{2} : a, b \in \mathbb{Z}\}$ is a ring, an integral domain, to be precise. Also we have the ring of Gaussian integers $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$, where i is the imaginary unit.

(3) If R is a ring, then so is the ring $R[x]$ of polynomials with coefficients in R. In particular, when $R = \mathbb{Z}/p\mathbb{Z}$ is the finite field with p elements, $R[x]$ has many similarities with $\mathbb{Z}$. For example, there is a Euclidean algorithm and hence unique factorization into irreducibles. See the introduction to algebraic number theory for details.

More generally, if X is a set and R is a ring, the set of functions from X to R is a ring, with the natural operations of pointwise addition and multiplication of functions. For many sets X, this ring has many interesting subrings constructed by restricting to functions with properties that are preserved under addition and multiplication. If $X = R = \mathbb{R}$, for instance, there are subrings of continuous functions, differentiable functions, polynomial functions, and so on.

(4) The set of $n \times n$ matrices with entries in a commutative ring R is a ring, which is non-commutative for $n \geq 2$. This ring has a unity, the identity matrix. But it may have divisors of zero. E.g. $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$. This shows that $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ and $\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$ are divisors of zero in the ring $M_2(R)$.

(5) Another classical example is the ring of quaternions, the set of expressions of the form $a + bi + cj + dk$, where $a, b, c, d \in \mathbb{Z}$ and i, j, k satisfy the relations

$$i^2 = j^2 = k^2 = ijk = -1.$$

This has numerous applications in physics. This is a strictly skew field.

Examples of Rings

This section lists many of the common rings and classes of rings that arise in various mathematical contexts.

(1) The ring \mathbb ZZ of integers is the canonical example of a ring. It is an easy exercise to see that \mathbb ZZ is an integral domain but not a field.

(2) There are many other similar rings studied in algebraic number theory, of the form {\mathbb Z}[\alpha]Z[*α*], where \alpha*α* is an algebraic integer. For example, {\mathbb Z}\left[\sqrt{2}\right] = \{ a+b\sqrt{2} \colon a,b \in {\mathbb Z}\}Z[2]={*a*+*b*2:*a*,*b*∈Z} is a ring, an integral domain, to be precise. Also we have the ring of Gaussian integers {\mathbb Z}[i] = \{ a+bi \colon a,b \in {\mathbb Z}\}Z[*i*]={*a*+*bi*:*a*,*b*∈Z}, where i*i* is the imaginary unit.

(3) If R*R* is a ring, then so is the ring R[x]*R*[*x*] of polynomials with coefficients in R*R*. In particular, when R = {\mathbb Z}/p{\mathbb Z}*R*=Z/*p*Z is the finite field with p*p* elements, R[x]*R*[*x*] has many similarities with \mathbb ZZ. For example, there is a Euclidean algorithm and hence unique factorization into irreducibles. See the introduction to algebraic number theory for details.

More generally, if X*X* is a set and R*R* is a ring, the set of functions from X*X* to R*R* is a ring, with the natural operations of pointwise addition and multiplication of functions. For many sets X*X*, this ring has many interesting subrings constructed by restricting to functions with properties that are preserved under addition and multiplication. If X = R = {\mathbb R}*X*=*R*=R, for instance, there are subrings of continuous functions, differentiable functions, polynomial functions, and so on.

(4) The set of n \times n*n*×*n* matrices with entries in a commutative ring R*R* is a ring, which is non-commutative for n \ge 2*n*≥2. This ring has a unity, the identity matrix.

But it may have divisors of zero. E.g. \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}=\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}(1000)(0001)=(0000). This shows that \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}(1000) and \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}(0001) are divisors of zero in the ring { M }_{ 2 }\left(R \right)*M*2(*R*).

(5) Another classical example is the ring of quaternions, the set of expressions of the form a+bi+cj+dk*a*+*bi*+*cj*+*dk*, where a,b,c,d \in {\mathbb Z}*a*,*b*,*c*,*d*∈Z and i,j,k*i*,*j*,*k* satisfy the relationsi^2=j^2=k^2=ijk=-1.*i*2=*j*2=*k*2=*ijk*=−1.This has numerous applications in physics. This is a strictly skew field.

Group Isomorphism

Definition

Let G and G′ be any two groups with binary operation $\circ$ and $\circ$‘, respectively. If there exists a one-one onto mapping $f:G\to G'f:G\to G'$ such that

$f(a\circ b)=f(a)\circ{}^{‘}f(b),\forall a,b\in G$

In this case, the group GG is said to be isomorphic to the group G′, and the mapping ff is said to be an isomorphism. If GG is isomorphic to G′, we write $G\simeq G$ ′ or $G\cong G'$.

Properties of Isomorphism

Theorem 1:

If isomorphism exists between two groups, then the identities correspond, i.e. if $f:G\to G'$ is an isomorphism and e,e' are respectively the identities in G,G', then $f(e)=e'$.

Theorem 2:

If isomorphism exists between two groups, then the identities correspond, i.e. if $f:G\to G'$ is an isomorphism and $f(a)=a'$, where $a\in G,a'\in G'$ then $f(a–1)=a'–1=[f(a)]–1f(a–1)=a'–1$

$=[f(a)]–1$.

Theorem 3:

In an isomorphism the order of an element is preserved, i.e. if $f:G\to G'f:G\to G'$ is an isomorphism, and the order of aa is nn, then the order of f(a)f(a) is also nn.

Proof:

As $f(a)=a'$, then we have $f(a\cdot a)=f(a)\cdot f(a)=a'\cdot a'=a'^2$ and in general we can write it as $f(an)=a'n$.

But $f(an)=f(e)=e'$, by using the statement of Theorem 1,

therefore $a'n=e'$. Also $a'm\neq e'$ for $m<n$, i.e. $o(a')=n$.

It follows that the order of an element of G, if finite, is equal to the order of its image in G′. If the order of aa is infinite, we can similarly show that the order of a′ cannot be finite.

Theorem 4:

The relation of isomorphism in the set of groups is an equivalence relation.

Isomorphism of Cyclic Groups

Theorem 1:

Cyclic groups of the same order are isomorphic.

Proof: Let G and′G′ be two cyclic groups of order n, which are generated by a and b respectively. Then

G={a,a2,a3,…,an=e}

and

G′={b,b2,b3,…,bn=e′}

The mapping f:G→G′, defined by f(ar)=br, is isomorphism.

f(ar⋅as)=f(ar+s)=br+s=br⋅bs=f(ar)⋅f(as)

Therefore the groups are isomorphic.

<u>Theorem 2</u>:
An infinite cyclic group is isomorphic to the additive group of integers.

<u>Proof</u>: Let G be an infinite cyclic group, generated by a, then

G={…,a–2,a–1,a0=e,a1,a2,a3,…}={ar:risaninteger}

The mapping f:G→Z, defined by f(ar)=r is an isomorphism, for it is one-one onto, and further,

f(ar⋅as)=f(ar+s)=r+s=f(ar)+f(as)

It follows that GG is isomorphic to Z.

<u>Theorem 3</u>:
A cyclic group of order nn is isomorphic to the additive group of residue classes modulo nn.

<u>Proof</u>: Let GG be an infinite cyclic group, generated by aa, then

G={a,a2,a3,…,an–1,an=e}

Let G’ be the additive group or residue classes (modn), i.e.

G′={[1],[2],[3],…,[n]=[0]}

The mapping f:G→G′, defined by f(ar)=[r], is isomorphism, for it is one-one onto, and further,

f(ar⋅as)=f(ar+s)=[r+s]=[r]+[s]=f(ar)+f(as)

It follows that G is isomorphic to G′.

<u>Theorem 4</u>:
A subgroup of the infinite cyclic group is isomorphic to the additive group of integral multiples of an integer.

<u>Proof</u>:

Let G={…,a–2,a–1,a0=e,a1,a2,a3,…} and let H be a subgroup of G, given by,

$H=\{\dots,a-2m,a-m,a0=e,am,a2m,\dots\}=\{(am)n:n\in Z\}$

Then H is isomorphic to the additive group H′, given by

$H'=\{0,\pm m,\pm 2m,\pm 3m,\dots\}=\{nm:n\in Z\}$

The mapping $f:H\to H'$, defined by $f(amn)=nm$, is isomorphism, for it is one-one onto, and if $r,s\in Z$, then

$f(arm\cdot asm)=f(a(r+s)m)=(r+s)m=rm+sm=f(arm)+f(asm)$

It will be observed that H is itself an infinite cyclic group, and as such it is isomorphic to G. Thus a subgroup of an infinite cyclic group is isomorphic to the group itself.

Examples of Group Isomorphism

Example 1: Show that the multiplicative group G consisting of three cube roots of unity $1,\omega,\omega2$ is isomorphic to the group G′ of residue classes (mod3) under addition of residue classes (mod3)

Solution:
Let us consider the composition tables of two structures G,G′ as given below:

×	1	ω	ω2
1	1	ω	ω2
ω	ω	ω2	1
ω2	ω2	1	ω

+(mod3)	{0}	{1}	{2}
{0}	{0}	{1}	{2}
{1}	{1}	{2}	{0}
{2}	{2}	{0}	{1}

From this table it is evident that if $1,\omega,\omega2$ are replaced by {0},{1},{2} respectively in the composition table for G, we get the composition table G′. This leads to the fact that mapping f of G onto G′ defined by $f(1)=\{0\}$, $f(\omega)=\{1\}$, $f(\omega2)=\{2\}$ is an isomorphism. Also:

$f(\omega\cdot\omega2)=f(1)=\{0\}=\{1\}+\{2\}=f(\omega)+f(\omega2)$

Example 2: Show that the additive group $G=\{\dots,-2,-1,0,1,2,\dots\}$ is an isomorphic to the additive group $G'=\{\dots,-2m,-m,0,m,2m,\dots\}$ for any given integer mm.

Solution:
We define a mapping ff by $f:G\to G':f(a)=ma$, where $a\in G,ma\in G'$ and show that f is an isomorphism of G onto G′.

We see that ff is one-one since two different elements of G have two different f– image in G′ is the f– image of an element of G.

Again:

$f(a+b)=m(a+b)=ma+mb \Rightarrow f(a+b)=f(a)+f(b)$

Thus ff is composition preserving as well. Hence ff is an isomorphic mapping of G onto G′

UNIT 5- Vector Space

Before giving the formal definition of an abstract vector space, we define what is known as an external composition in one set over another. We have already defined a binary composition in a set AA as a mapping of $A\times AA\times A$ to AA. This may be referred to as an internal composition in AA. Now, let AA and BB be two non-empty sets. Then a mapping $f:A\times B\rightarrow Bf:A\times B\rightarrow B$ is called an external composition in BB over AA.

__Definition__: Let $(F,+,\times)(F,+,\times)$ be a field. Then a set VV is called a vector space over the field FF if VV is an abelian group under an operation which is denoted by ++, and if for every $a\in Fa\in F$, $u\in Vu\in V$ there is defined an element auau in VV such that

(i) $a(u+v)=au+ava(u+v)=au+av$, for all $a\in Fa\in F$, $u,v\in Vu,v\in V$.

(ii) $(a+b)u=au+bu(a+b)u=au+bu$, for all $a,b\in Fa,b\in F$, $u\in Vu\in V$.

(iii) $a(bu)=(ab)ua(bu)=(ab)u$, for all $a,b\in Fa,b\in F$, $u\in Vu\in V$.

(iv) $1\cdot u=u\cdot 11\cdot u=u\cdot 1$ represents the unity element of FF under multiplication.

The following notations will be constantly used in the forthcoming tutorials.

(1) Generally FF will be the field whose elements shall often be referred to as scalars.

(2) VV will denote the vector space over FF whose elements shall be called vectors.

Thus to test that VV is a vector space over FF, the following axioms should be satisfied:

(V1): $(V,+)(V,+)$ is an abelian group.

(V2): Scalar multiplication is distributive over addition in VV, i.e. $a(u+v)=au+ava(u+v)=au+av$, for all $a\in Fa\in F$, $u,v\in Vu,v\in V$.

(V3): Distributive of scalar multiplication over addition in FF, i.e. $(a+b)u=au+bu(a+b)u=au+bu$, for all $a,b\in Fa,b\in F$, $u\in Vu\in V$.

(V4): Scalar multiplication is associative, i.e. $a(bu)=(ab)ua(bu)=(ab)u$, for all $a,b\in Fa,b\in F$, $u\in Vu\in V$.

(V5): Property of unity: Let $1\in F1\in F$ be the unity of FF, then $1\cdot u=u\cdot 11\cdot u=u\cdot 1$ for all $u\in Vu\in V$.

A vector space VV over a field FF is expressed by writing V(F)V(F). Sometimes writing only VV is sufficient provided the context makes it clear which field has been considered.

If the field is RR, the set of real numbers, then VV is said to be a real vector space. If the field is QQ, the set of rational numbers, then VV is said to be a rational vector space. Finally, if the field is CC, the set of complex numbers, VV is called a complex vector space.

Vector Subspace

Let VV be a vector space over the field FF. Then a non-empty subset WW of VV is called a vector space of VV if under the operations of VV, WW itself is a vector space over FF. In other words, WW is a subspace of VV whenever

w1,w2∈Ww1,w2∈W and α,β∈F⇒αw1+βw2∈W

<u>Example</u>:
Prove that the set WW of ordered tried (a1,a2,0)(a1,a2,0) where a1,a2∈Fa1,a2∈F is a subspace of V3(F)V3(F).

<u>Solution</u>:
Let a=(a1,a2,0)a=(a1,a2,0) and b=(b1,b2,0)b=(b1,b2,0) be two elements of WW.

Therefore a1,a2,b1,b2∈Fa1,a2,b1,b2∈F let a,b∈Fa,b∈F then

aα+bβ=a(a1,a2,0)+b(b1,b2,0)=(aa1,aa2,0)+(bb1,bb2,0)=(aa1+bb1,aa2+bb2,0)∈Waα+bβ=a(a1,a2,0)+b(b1,b2,0)=(aa1,aa2,0)+(bb1,bb2,0)=(aa1+bb1,aa2+bb2,0)∈W

Because aa1+bb1,aa2+bb2∈Faa1+bb1,aa2+bb2∈F.

Linear Dependence and Linear Independence Vectors

<u>Linear Dependence</u>
Let V(F)V(F) be a vector space and let S={u1,u2,…,un}S={u1,u2,…,un} be a finite subset of VV. Then SS is said to be linearly dependent if there exists scalar α1,α2,…,αn∈Fα1,α2,…,αn∈F, not all zero, such that

α1u1+α2u2+⋯+αnun=0α1u1+α2u2+⋯+αnun=0

<u>Linear Independence</u>
Let V(F)V(F) be a vector space and let S={u1,u2,…,un}S={u1,u2,…,un} be a finite subset of VV. Then SS is said to be linearly independent if,

∑i=0nαiui=0,αi∈F∑i=0nαiui=0,αi∈F

This holds only when αi=0,i=1,2,3,…,nαi=0,i=1,2,3,…,n.

An infinite subset SS of VV is said to be linearly independent if every finite subset SS is linearly independent, otherwise it is linearly dependent.

<u>Example 1</u>: Show that the system of three vectors (1,3,2)(1,3,2), (1,–7,–8)(1,–7,–8), (2,1,–1)(2,1,–1) of V3(R)V3(R) is linearly dependent.

<u>Solution</u>: For α1,α2,α3∈Rα1,α2,α3∈R.

α1(1,3,2)+α2(1,–7,–8)+α3(2,1,–1)⇔(α1+α2+3α3,3α1–7α2+α3,2α1–8α2–α3)=0⇔α1+α2+3α3=0,3α1–7α2+α3=0,2α1–8α2–α3=0⇔α1=3,α2=1,α3=–2α1(1,3,2)+α2(1,–7,–8)+α3(2,1,–1)⇔(α1+α2+3α3,3α1–7α2+α3,2α1–8α2–α3)=0⇔α1+α2+3α3=0,3α1–7α2+α3=0,2α1–8α2–α3=0⇔α1=3,α2=1,α3=–2

Therefore, the given system of vectors is linearly dependent.

Example 2: Consider the vector space $R3(R)R3(R)$ and the subset $S=\{(1,0,0),(0,1,0),(0,0,1)\}S=\{(1,0,0),(0,1,0),(0,0,1)\}$ of $R3R3$. Prove that SS is linearly independent.

Solution: For $\alpha1,\alpha2,\alpha3\in R\alpha1,\alpha2,\alpha3\in R$.

$$\alpha1(1,0,0)+\alpha2(0,1,0)+\alpha3(0,0,1)=(0,0,0)\Leftrightarrow(\alpha1,\alpha2,\alpha3)=(0,0,0)\Leftrightarrow\alpha1=0,\alpha2=0,\alpha3=0\alpha1(1,0,0)+\alpha2(0,1,0)+\alpha3(0,0,1)=(0,0,0)\Leftrightarrow(\alpha1,\alpha2,\alpha3)=(0,0,0)\Leftrightarrow\alpha1=0,\alpha2=0,\alpha3=0$$

This shows that if any linear combination of the elements of SS is zero then the coefficient must be zero. SS is linearly independent.

Basis of a Vector Space

A subset SS of a vector space $V(F)V(F)$ is said to be a basis of $V(F)V(F)$, if

(i) SS consists of a linearly independent vector, and

(ii) SS generates $V(F)V(F)$, i.e. $L(S)=VL(S)=V$, i.e. each vector in VV is a linear combination of a finite number of elements of SS.

For example the set $\{(1,0,0),(0,1,0),(0,0,1)\}\{(1,0,0),(0,1,0),(0,0,1)\}$ is a basis of the vector space $V3(R)V3(R)$ over the field of real numbers.

Dimension

The dimension of a vector space $V(F)V(F)$ is the number of elements in a basis of $V(F)V(F)$.

Example:

Show that the set $S=\{(1,2,1),(2,1,0),(1,-1,2)\}S=\{(1,2,1),(2,1,0),(1,-1,2)\}$ forms a basis for $V3(F)V3(F)$.

Solution:

For $a1,a2,a3\in Fa1,a2,a3\in F$, then $a1(1,2,1)+a2(2,1,0)+a3(1,-1,2)=0a1(1,2,1)+a2(2,1,0)+a3(1,-1,2)=0$

$$\Rightarrow(a1+2a2+a3,2a1+a2-a3,a1+2a3)=(0,0,0)\Rightarrow a1+2a2+a3=0,2a1+a2-a3=0,a1+33=0\Rightarrow a1=a2=a3=0\Rightarrow(a1+2a2+a3,2a1+a2-a3,a1+2a3)=(0,0,0)\Rightarrow a1+2a2+a3=0,2a1+a2-a3=0,a1+33=0\Rightarrow a1=a2=a3=0$$

Hence the given set is linearly independent.

Now let

$$(1,0,0)=x(1,2,1)+y(2,1,0)+z(1,-1,2)=(x+2y+z,2x+y-z,x+2z)$$
$$(1,0,0)=x(1,2,1)+y(2,1,0)+z(1,-1,2)=(x+2y+z,2x+y-z,x+2z)$$

So that $x+2y+z=1,2x+y-z=0,x+2z=0x+2y+z=1,2x+y-z=0,x+2z=0$
$\therefore x=-29,y=59,z=19\therefore x=-29,y=59,z=19$

Thus, the unit vector $(1,0,0)(1,0,0)$ is a linear combination of the vectors of the given set, i.e.

(1,0,0)=–29(1,2,1)+59(2,1,0)+19(1,–1,2)(1,0,0)=–29(1,2,1)+59(2,1,0)+19(1,–1,2)
(0,1,0)=49(1,2,1)–19(2,1,0)–29(1,–1,2)(0,1,0)=49(1,2,1)–19(2,1,0)–29(1,–1,2)
(0,0,1)=13(1,2,1)–13(2,1,0)+13(1,–1,2)(0,0,1)=13(1,2,1)–13(2,1,0)+13(1,–1,2)

Since V3(F)V3(F) is generated by the unit vectors(1,0,0)(1,0,0), (0,1,0)(0,1,0), (0,0,1)(0,0,1), we see that every element of V3(F)V3(F) is a linear combination of the given set SS. Hence the vectors of this set form a basis of V3(F)V3(F).

Section 9 – Orbits, Cycles, and the Alternating Groups

Instructor: Yifan Yang

Fall 2006

Outline

Orbits and cycles

Even and odd permutations

The alternating groups

Orbits

Lemma

Let σ be a permutation of a set A. Then the relation $\sim$ on A defined by

$$a \sim b \Leftrightarrow b = \sigma^n(a) \text{ for some integer } n$$

is an equivalence relation.

Definition

The equivalence classes determined by the above equivalence relation are the orbits of σ.

Orbits

Proof.
We check

1. Reflexive: $a \sim a$ for all $a \in A$ since $a = \sigma^0(a)$.
2. Symmetric: If $a \sim b$, i.e., if $b = \sigma^n(a)$, then $a = \sigma^{-n}(b)$ and thus $b \sim a$.
3. Transitive: If $a \sim b$ and $b \sim c$, then $b = \sigma^n(a)$ and $c = \sigma^m(b)$ for some $m, n \in \mathbb{Z}$. It follows that $c = \sigma^m(b) = \sigma^m(\sigma^n(a)) = \sigma^{m+n}(a)$. Thus $a \sim c$.

$\square$

Orbits

Example

Let

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 8 & 6 & 7 & 4 & 1 & 5 & 2 \end{pmatrix}$$

To find the orbit containing 1, we apply σ repeatedly, obtaining

$$1 \to 3 \to 6 \to 1 \to 3 \to 6 \to \cdots .$$

Thus, the orbit containing 1 is $\{1, 3, 6\}$. Likewise, we have

$$2 \to 8 \to 2 \to 8 \to 2 \to 8 \to \cdots ,$$
$$4 \to 7 \to 5 \to 4 \to 7 \to 5 \to \cdots .$$

We conclude that there are three orbits $\{1, 3, 6\}, \{2, 8\}, \{4, 5, 7\}$.

In-class exercises

Find the orbits of the following permutations.

1. $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 7 & 1 & 2 & 8 & 5 & 9 & 6 & 4 \end{pmatrix}$.
2. $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 8 & 2 & 7 & 1 & 5 & 4 & 3 & 6 & 9 \end{pmatrix}$.
3. $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 8 & 7 & 4 & 9 & 1 & 3 & 6 & 5 \end{pmatrix}$.

Cycles

Observe that a permutation σ can be decomposed into a product of several permutations, each of which acts non-trivially on at most one of the orbits. For example, we have

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 4 & 5 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 5 & 4 \end{pmatrix}$$

where the orbits are $\{1, 2, 3\}$ and $\{4, 5\}$, and we decompose it into a product of two permutations, one acting on $\{1, 2, 3\}$ and the other on $\{4, 5\}$. This motivates the following definition.

Cycles

Definition

A permutation $\sigma \in S_n$ is a cycle if it has at most one orbit containing more than one element. (That is, σ acts non-trivially on at most one orbit.) The length of a cycle is the number of elements in the largest cycle.

Notation

Since cycles have at most one orbit containing more than one element, we can represent cycles using only information of the largest orbit. Suppose that in the largest orbit of a cycle σ we have $x_1 \to x_2 \to x_3 \to \cdots \to x_n \to x_1$. Then we write

$$\sigma = (x_1, x_2, \ldots, x_n).$$

Examples

1. $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}$ is not a cycle since the orbits are $\{1, 2, 3\}$ and $\{4, 5\}$. Both of them have more than one element.
2. $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 4 & 5 \end{pmatrix}$ and $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 5 & 4 \end{pmatrix}$ are both cycles. The orbits of the former are $\{1, 2, 3\}$, $\{4\}$, and $\{5\}$, and those of the latter are $\{1\}$, $\{2\}$, $\{3\}$, and $\{4, 5\}$. The lengths are 3 and 2, respectively. Moreover, in the cyclic notations, they are $(1, 2, 3)$ and $(4, 5)$.

Cycles

Theorem (9.8)

Every permutation σ of a finite set is a product of disjoint cycles.

Proof.

Let $B_1, \ldots, B_r$ be the orbits of σ. Define cycles τ_i by

$$\tau_i(x) = \begin{cases} \sigma(x), & \text{if } x \in B_i, \\ x, & \text{if } x \notin B_i. \end{cases}$$

Then $\sigma = \tau_1 \tau_2 \ldots \tau_r$. Clearly, these τ_i are disjoint. $\square$

Example

In $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 2 & 4 & 1 \end{pmatrix}$, we have

$$1 \to 3 \to 2 \to 5 \to 1 \to 3 \cdots$$
$$4 \to 4 \to 4 \to 4 \to 4 \to 4 \cdots$$

Thus, we write $\sigma = (1, 3, 2, 5)$, or $\sigma = (3, 2, 5, 1) = (2, 5, 1, 3) = (5, 1, 3, 2)$. (It is fine, though not necessary to write $\sigma = (1, 3, 2, 5)(4)$.)

Example

In $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 8 & 6 & 7 & 4 & 1 & 5 & 2 \end{pmatrix}$ We have

$$1 \to 3 \to 6 \to 1 \to 3 \to 6 \to \cdots ,$$
$$2 \to 8 \to 2 \to 8 \to 2 \to 8 \to \cdots ,$$
$$4 \to 7 \to 5 \to 4 \to 7 \to 5 \to \cdots .$$

Thus, $\sigma = (1, 3, 6)(2, 8)(4, 7, 5)$. Also,
$\sigma = (2, 8)(4, 7, 5)(1, 3, 6) = (4, 7, 5)(8, 2)(3, 6, 1) = \cdots$. But
$\sigma \neq (1, 6, 3)(2, 8)(4, 7, 5)$.

Remarks

1. The multiplication of disjoint cycles are commutative. For example, we have

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix} = (1,2,3)(4,5) = (4,5)(1,2,3).$$

2. Up to the order of the cycles, the representation of a permutation as a product of cycles is unique.
3. A product of several cycles can still be a cycle. For example, we have $(1,2)(1,3) = (1,3,2)$.

In-class exercise

Express the following permutations as products of disjoint cycles.

1. $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 7 & 1 & 2 & 8 & 5 & 9 & 6 & 4 \end{pmatrix}$.
2. $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 8 & 2 & 7 & 1 & 5 & 4 & 3 & 6 & 9 \end{pmatrix}$.
3. $(1,3,2,5)(4,2,8,7)(3,9,1,2)(6,9)$.

Transposition

Definition

A cycle of length 2 is a transposition.

Theorem (9.12)

Any permutation of a finite set of at least two elements is a product of transposition.

Proof.

If σ is the identity element, we have $\sigma = (1,2)(1,2)$. Otherwise, write σ as a product of cycles. Now for each cycle $(a_1, a_2, \ldots, a_n)$ we have

$$(a_1, a_2, \ldots, a_n) = (a_1, a_n)(a_1, a_{n-1}) \ldots (a_1, a_2).$$

This proves the theorem. □

Examples

1. We have $(1, 2, 3) = (1, 3)(1, 2)$.
2. We have$(2, 5, 1, 3) = (2, 3)(2, 1)(2, 5)$. Also, $(2, 5, 1, 3) = (5, 1, 3, 2) = (5, 2)(5, 3)(5, 1)$, and $(2, 5, 1, 3) = (1, 3, 2, 5) = (1, 5)(1, 2)(1, 3)$. Thus, there are more than one way to write a cycle as a product of transpositions.
3. We have $(1, 2, 3, 4) = (1, 4)(1, 3)(1, 2)$. Also $(1, 2, 3, 4) = (1, 2)(3, 4)(1, 2)(1, 3)(1, 4)(3, 4)(1, 2)$.

Even and odd permutations

Theorem (9.15)

No permutation in S_n can be expressed both as a product of an even number of transpositions and as a product of an odd number of transpositions.

Proof

It suffices to prove that if $\tau = (i, j)$, $i \neq j$, is a transposition, and $\sigma \in S_n$, then the number of orbits of σ and that of $\tau\sigma$ differ by 1. To see why this suffices, note that if $\sigma = \tau_1\tau_2 \ldots \tau_r$, then $\sigma = \tau_1 \ldots \tau_r\iota$, where ι is the identity permutation. Since the number of orbits of ι is n, the number of orbits of σ will be congruent to $n + r$ modulo 2. Thus, r must be congruent to $n +$ (the number of orbits of σ) modulo 2.

Proof of Theorem 9.15, continued.

Write $\sigma \in S_n$ as a product of disjoint cycles.

Case 1. i and j are in two different cycles. Say, $\sigma = (i, a_1, \dots, a_r)(j, b_1, \dots, b_s)\mu_1 \dots \mu_m$, where the cycles are disjoint. (r and s could be 0.) Then

$$\begin{aligned}(i,j)\sigma &= (i,j)(i, a_1, \dots, a_r)(j, b_1, \dots, b_s)\mu_1 \dots \mu_m \\ &= (i, a_1, \dots, a_r, j, b_1, \dots, b_s)\mu_1 \dots \mu_m.\end{aligned}$$

In this case, the number of orbits of $\tau\sigma$ is one less than that of σ.

Case 2. i and j are in the same cycle. Assume that $\sigma = (i, a_1, \dots, a_r, j, b_1, \dots, b_s)\mu_1 \dots \mu_m$. Then

$$(i,j)\sigma = (i, a_1, \dots, a_r)(j, b_1, \dots, b_s)\mu_1 \dots \mu_m.$$

In this case, the number of orbits of $\tau\sigma$ is one more than that of σ. $\square$

Even and odd permutations

Definition

A permutation of a finite set is even or odd according to whether it can be expressed as a product of an even number of transpositions or an odd number of transpositions.

Example

1. The identity permutation is equal to $(1, 2)(1, 2)$. Thus, the identity permutation is even.
2. Let $\sigma = (a_1, \ldots, a_n$ be a cycle. Then $\sigma = (a_1, a_n) \ldots (a_1, a_2)$. Thus, if the length n is even, then the cycle is an odd permutation. If the length is odd, then the cycle is an even permutation.
3. Let $\sigma = (1, 3, 6, 5)(2, 8, 4)$. Since $(1, 3, 6, 5)$ is odd and $(2, 8, 4)$ is even, σ is odd.

Alternating groups

Theorem (9.20)

If $n \geq 2$, then the set A_n of all even permutations of $\{1, 2, \ldots, n\}$ forms a subgroup of order $n!/2$ of S_n.

Proof.

The statement has two parts, one claiming that A_n is a subgroup, and the other asserting that $|A_n| = n!/2$. We first show that A_n is a subgroup. We need to check

1. Closed: If σ_1 and σ_2 are both products of an even number of transpositions, so is $\sigma_1\sigma_2$.
2. Identity: $\mathrm{id} = (1, 2)(1, 2)$, which is even.
3. Inverse: If $\sigma = \tau_1\tau_2 \ldots \tau_{2n}$ is a product of an even number of transpositions τ_j, then $\sigma^{-1} = \tau_{2n}^{-1}\tau_{2n-1}^{-1} \ldots \tau_1^{-1}$ is also even.

Proof of Theorem 9.20, continued

We now prove that $|A_n| = n!/2$. It suffices to prove that the number of even permutations in $S_n$is equal to the number of odd permutations in S_n.

Let B_n be the set of all odd permutations in S_n. (Note that B_n is not a subgroup since it is not closed under multiplication.) Define $\lambda : A_n \to B_n$ by $\lambda(\sigma) = (1, 2)\sigma$. We claim that λ is one-to-one and onto. This shows that
$|A_n| = |B_n| = |S_n|/2 = n!/2$.

One-to-one: If $(1, 2)\sigma_1 = (1, 2)\sigma_2$, then by the left cancellation law, we have $\sigma_1 = \sigma_2$. Thus λ is one-to-one.

Onto: If $\sigma \in B_n$ is an odd permutation, then $(1, 2)\sigma$ is even and we have $\lambda((1, 2)\sigma) = (1, 2)(1, 2)\sigma = \sigma$. Thus, λ is onto. $\square$.

Alternating groups

Definition (9.21)

The subgroup of S_n consisting of the even permutations of n letters is the alternating group A_n on n letters.

Example

1. A_3 has $3!/2 = 3$ elements. They are id, $(1, 2, 3)$, and $(1, 3, 2)$.
2. A_4 has $4!/2 = 12$ elements. They are id, 8 3-cycles $(1, 2, 3), (1, 3, 2), \ldots$, and $(1, 2)(3, 4)$, $(1, 3)(2, 4)$, and $(1, 4)(2, 3)$.

Homework

Do Problems 10, 12, 13, 18, 27, 29, 34, 39 of Section 9.

PART - A- unit 1

1. A trivial subgroup consists of ___________
a) Identity element
b) Coset
c) Inverse element
d) Ring
View Answer

Answer: a
Explanation: Let G be a group under a binary operation * and a subset H of G is called a subgroup of G if H forms a group under the operation *. The trivial subgroup of any group is the subgroup consisting of only the Identity element.

2. Minimum subgroup of a group is called _____________
a) a commutative subgroup
b) a lattice
c) a trivial group
d) a monoid
View Answer

Answer: c
Explanation: The subgroups of any given group form a complete lattice under inclusion termed as a lattice of subgroups. If o is the Identity element of a group(G), then the trivial group(o) is the minimum subgroup of that group and G is the maximum subgroup.

3. Let K be a group with 8 elements. Let H be a subgroup of K and $H<K$. It is known that the size of H is at least 3. The size of H is __________
a) 8
b) 2
c) 3
d) 4

Answer: d
Explanation: For any finite group G, the order (number of elements) of every subgroup L of G divides the order of G. G has 8 elements. Factors of 8 are 1, 2, 4 and 8. Since given the size of L is at least 3(1 and 2 eliminated) and not equal to G(8 eliminated), the only size left is 4. Size of L is 4.

4. __________ is not necessarily a property of a Group.
a) Commutativity
b) Existence of inverse for every element
c) Existence of Identity
d) Associativity

Answer: a
Explanation: Grupoid has closure property; semigroup has closure and associative; monoid has closure, associative and identity property; group has closure, associative, identity and inverse; the abelian group has group property and commutative.

5. A group of rational numbers is an example of __________
a) a subgroup of a group of integers
b) a subgroup of a group of real numbers
c) a subgroup of a group of irrational numbers
d) a subgroup of a group of complex numbers
View Answer

Answer: b
Explanation: If we consider the abelian group as a group rational numbers under binary operation + then it is an example of a subgroup of a group of real numbers.

6. Intersection of subgroups is a ___________
a) group
b) subgroup
c) semigroup
d) cyclic group
View Answer

Answer: b
Explanation: The subgroup property is intersection closed. An arbitrary (nonempty) intersection of subgroups with this property, also attains the similar property.

7. The group of matrices with determinant _________ is a subgroup of the group of invertible matrices under multiplication.
a) 2
b) 3
c) 1
d) 4
View Answer

Answer: c
Explanation: The group of real matrices with determinant 1 is a subgroup of the group of invertible real matrices, both equipped with matrix multiplication. It has to be shown that the product of two matrices with determinant 1 is another matrix with determinant 1, but this is immediate from the multiplicative property of the determinant. This group is usually denoted by(n, R).

8. What is a circle group?
a) a subgroup complex numbers having magnitude 1 of the group of nonzero complex elements

b) a subgroup rational numbers having magnitude 2 of the group of real elements
c) a subgroup irrational numbers having magnitude 2 of the group of nonzero complex elements
d) a subgroup complex numbers having magnitude 1 of the group of whole numbers
View Answer

Answer a

9. A normal subgroup is _____________
a) a subgroup under multiplication by the elements of the group
b) an invariant under closure by the elements of that group
c) a monoid with same number of elements of the original group
d) an invariant equipped with conjugation by the elements of original group

Answer: d
Explanation: A normal subgroup is a subgroup that is invariant under conjugation by any element of the original group that is, K is normal if and only if gKg-1=K for any g belongs to G Equivalently, a subgroup K of G is normal if and only if gK=Kg for any g belongs to G.Normal subgroups are useful in constructing quotient groups and in analyzing homomorphisms.
10. Two groups are isomorphic if and only if ___________ is existed between them.
a) homomorphism
b) endomorphism
c) isomorphism
d) association
View Answer

(a) Answer: c
Explanation: Two groups M and K are isomorphic (M ~= K) if and only if there exists an isomorphism between them. An isomorphism f:M -> K between two groups M and K is a mapping which satisfies two conditions: 1) f is a bijection and 2) for every x,y belongs to M, we have f(x*My) = f(x) * Kf(y).

11. Two conjugate subgroups are
Centralizer

Normal
Homomorphic
Isomorphic
12. Automorphism and inner automorphism of a group G are
Abelian
Conjugate
Normal
None of the option given

13. Every subgroup of a abelian group is
Equivalent
Center
Conjugate
normal
14. The intersection of any collection of normal subgroups of a group is

Equivalent
abelian
normal
Not abelian

15. Equivalence relation between subgroups of a group is a relation
Isomorphic
Conjugacy
Homomorphic
Isomorphic and conjugacy

Part B

76. The set A(G) of all automorphism of a group is
None of the option given
Not group
Group
Normal sub group

77. Every group of order P^6 where P is a prime number is
Normal
Cyclic
Abelian
Conjugate

78. Any two conjugate subgroups have same
None of the option given
Order
Order and center
center

79. Automorphism of a finite group is
Abelian
Normal
Finite
infinite
80. Group obtained by the direct product of sylow - p group is
Normal
Abelian
Center

commutator

81.The group $Z_m \times Z_n$ is cyclic if
(a) m n = 1 (b) m + n = 1 (c) g.c.d(m, n) = 1 (d) l.c.m(m,n) = 1

82. The number of conjugate classes of Q8 is
(a) 8 (b) 4 (c) 7 (d) 5

83.The number of groups of order 49 is
(a) 4 (b) 1 (c) 7 (d) 2

84. The number of elements of order 4 in $Z_2 \times Z_4$ is
(a) 8 (b) 4 (c) 6 (d) 2

85.The number of conjugacy classes of elements of order 4 in S3 is
(a) 6 (b) 1 (c) 0 (d) 2
86.What is the largest order of any element in U(900):
(a) 900 (b) 40 (c) 60 (d) 100

1. The number of permissible cycle types in S5 is
(a) 7 (b) 4 (c) 5 (d) None

2.The number of 3-sylow subgroups of group of order 25 is
(a) 1 (b) 3 (c) 0 (d) 5

3.The group $Z_m \times Z_n$ is cyclic if
(a) m n = 1 (b) m + n = 1 (c) g.c.d(m, n) = 1 (d) l.c.m(m,n) = 1

4. The number of conjugate classes of Q8 is
(b) 8 (b) 4 (c) 7 (d) 5

Give the conjugacy classes and the class equation for Q8. [Hint: Let Q8 act on itself by conjugation. Then the conjugacy classes are the distinct orbits, and the class equation is given by the orders of these classes. The class equation is something like: “8 = 1 + 1 + 1 + 2 + 3”.]
Solution. Since Z(Q8) = {1, −1}, we have O1 = {1} and O−1 = {−1}. [Moreover, these are the only orbits, or conjugacy classes in this case, that have only one element.] Observe that for all x, y ∈ Q8, we have (−x) · y · (−x) −1 = −1 · x · y · (−1 · x) −1 = −1 · x · y · x −1 · (−1)−1 = −1 · x · y · x −1 · −1 = x · y · x −1 [since −1 ∈ Z(Q8)]. This makes things easier to compute, and one gets: Oi = {i, −i}, Oj = {j, −j}, Ok = {k, −k}, Hence the class equation is: 8 = 1 + 1 + 2 + 2 + 2

5. The number of groups of order 49 is
(b) 4 (b) 1 (c) 7 (d) 2

6. The number of elements of order 4 in $Z_2 \times Z_4$ is
(b) 8 (b) 4 (c) 6 (d) 2
Since **Z4** has φ(**4**) = 2 **elements of order 4**, it follows that **Z2 ⊕ Z4**, and hence Aut(Z20), has **4 elements of order 4**. On the other hand, since **4** · (x, y) = (0,0) **for** every (x, y) **∈ Z2 ⊕ Z4**, Lagrange's theorem tells us that the possible **orders** of **elements** are 1, 2 or **4**.
7. The number of simple groups of order 60 is
(a) 1 (b) 10 (c) 60 (d) 6

8. The number of conjugacy classes of elements of order 4 in S3 is
(b) 6 (b) 1 (c) 0 (d) 2
So **S3** has three **conjugacy classes**: {(1)}, {(12),(13),(23)}, {(123),(132)}.

9. What is the largest order of any element in U(900):
(b) 900 (b) 40 (c) 60 (d) 100

10. If G is an abelian group of order 20, then the number of possible isomorphism classes of G is

(a) 2 (b) 6 (c) 5 (d) 20

11. The number of sylow 3-subgroups of A4 is
(a) 1 (b) 24 (c) 4 (d) 5

12. If G is an abelian group of order 60, then number of sylow 5-subgroups of G is
(b) 10 (b) 9 (c) 60 (d) 6

Part- A- unit 2

16. Which of the following is abelian
S4
S5
S3
S2

17. Let G be a finite group. Let H be a subgroup of G. Then which of the following divedes the order of G
Index of H
Order of G
Order of H
All the given options are correct

18. Let D4 $= \{ \langle a,b \rangle;\ a^4 = b^2 = (ab)^2 = 1) \}$ be a dihedral group of order 8. then which of the following is a subgroup of D4.
$\{ \langle a,b \rangle;\ b^2 = 1) \}$
$\{ \langle a,b \rangle;\ (ab)^2 = 1) \}$
$\{ \langle a^3,b \rangle;\ (a^3b)^2 = 1) \}$
$\{ \langle a,b \rangle;\ a^4 = b^2 = 1) \}$

19. Let An be the set of all even permutatios of Sn isa subgroup of Sn. Then order of An is
n!
n+ 1/2

n!/2
n! / 3

20. If X and Y are two sets, then $X \cap (XUY)' =0$
X

$X \cap Y$
Y
Ø

21. Let G be a cyclic group of order 24. then order of a^9 is

4
6
2
8

22. Any group G can be embedded in a group of bijective mappings of certain sets is a statement of

Lagrange’s theorem
Isomorphism theorem
Cauchy’s theorem
Caley’s theorem

23. The symmetries of rectangle form a
Permutation group of order 3, S3
Dihedral group of order 8
optic group
kleins 4 group D4

24. The union of all positive even and all positive odd integers is
Z
Z+
W
N

25. The set of cube roots of unity is a subgroup of
R
R+
C
C-{0}

26. If n(U) = 700, n(A) = 200, n(B)=300 and n(A∩B)=100 then n(A^I ∩ B^I) =?
400
240
600
300

27. In a group of even order there at least ______ elements of order 2.
2
1
3
None of the options given

28. Let G be a cyclic group. Then which of the following is cyclic
Homomorphc of G
Centre of G
All of the given option
Subgroup of G

29. In S4 group of permutation, number of even permutation is
16
12
24
4

30. The group Sn is called
None of the given options

Symmetric group of degree n
Polynomial group of degree n
Dihidral group of degree n

Part B= unit 2

86. If a group is neither periodic nor torsion free then G is
Mixed group
Symmetric group
Infinite group
Free group

87. Let G be a cyclic group of order 10. the number of subgroups of G is
2
4
5
10

88. Suppose that n(A) = 3 and n(B) = 6 then what can be minimum number of elements
6
9
3
18

89. Ø: R^+ -> R is an isomorphism. Then for all x Ɛ R^+ which of the following is true.
Ø(x) = log(x)
Ø(x) = x
Ø(x) = $x^2 + 1$
Ø(x) = tan(x)

90 which of the following is cyclic group

Z
R
C
Q

90. Number of non- empty subsets of the set { 1,2,3,4}

14
16
15
17

91. Let G be a group and a, b Ɛ G then order of a^{-1} =

b^{-1}
b
bab^{-1}
ab

92. R+ is a group of non - zero positive real number under multiplication. Then which of the following group under addition is isomorphic to R+
Q
Z
C
R

93. Let X has n elements. The set Sn of all permutations of X is a group with respect to mappings
Composition
Addition
Multiplication
inverse

94. The group in which every element except the identity element has infinite order is called
Locally infinite
All of these options
Torsion free
A-Periodic

95. Which of the following is even permutation

1	2	3	4
2	3	1	4

None of the option given

1	2	3	4
2	4	1	3

1	2	3	4
2	1	4	3

Unit 3- MCQ- RINGS- I MSC - ALGEBRA

1. The integer modulo n

2 points

forms a ring for any natural number n
forms a ring if n is prime
is always an integral domain
is not an integral domain if n is prime

2. Z[i] is

2 points

an integral domain
a field
a non-commutative ring
a commutative ring but not an integral domain

3. For n ≥ 2, the n-by-n matrices with coefficients in R forms

2 points

a commutative ring

a non-commutative ring

a commutative ring but not an integral domain

a non commutative ring having no divisor of zero

4. H={a+bi+cj+dk: a,b,c,d in R}. Multiplication is defined by i^2=j^2=k^2=-1, ij=-ji=k, jk=-kj=i, ki=-ik=j. H forms a

2 points

a filed

a commutative ring but not an integral domain

a skew field

a commutative ring having zero divisor

5. Let R be a finite ring and a,b in R such that ab=1. Then
ba=1
ba! = 1
ba=0
$ba^{-1} = 1$

6. R be a ring such that a^2=a for each a in R.
R is commutative
R may not be commutative
R is a field
None of these

7. Let R be a ring and a,b,c in R such that ab=ca=1. Then

c=b and a is not a unit
c=b and a is a unit
c != b and a is not a unit
c !=b and a is a unit

8. Let R be a ring and a, b in R such that ab=1. Then

ba is the only idempotent of R
ba and 1-ba are idempotent elements of R
neither ba nor 1-ba is an idempotent of R
1-ba is the only idempotent of R

9. R is a finite commutative ring with more than one element and no divisor of zero.
Then R is
R is a field
R is not necessarily a field
R is not a integral domain
None of the above

10. 2Z forms

an integral domain
a division ring
a field
a commutative ring

11. R is a ring such that x^3=x for all x in R. Which of the following is true?

2 points

3x=0
4x=0
5x=0
6x=0

12. Which of the following property is possesed by Z and Z_n for all n

2 points

a^2=a implies a=0 or a=1
ab=0 implies a=0 and b=0

a+b=a+c implies b=c
For nonzero a, ab=ac implies b=c

13. In the ring of complex numbers, S={ai | a in Z} is

2 points

a subgroup under addition and a subring
a subgroup under addition but not a subring
neither a subgroup nor a subring
subring but not a subgroup under addition

14. Which of the following is not a subring of ring Z?

2 points

2Z U 3Z
2Z intersection 3Z
2Z
3Z

15. (R,+,.) is a ring

2 points

In (R,.), unique solution exists for ax=b
In (R,.), unique solution exists for ya=b
In (R,+), unique solution exists for ax=b
None of the above

Part B

1. Which of the following is not an integral domain?

2 points

Z[x]

R[x]

Z/6Z

{a+b√2: a,b in Z}

2. Smallest subfield of R containing √5

2 points

{r+s√5: r,s in Z}

{r+s√5: r,s in R}

{r+s√5: r,s in Q}

None of the above

3. How many ideals of Z/12Z are there?

2 points

6

12

5

7

4. If R is commutative ring with unit element, M is an ideal of R and R/M is finite integral domain, then
(a) M is a maximal ideal of R
(b) M is not a maximal ideal of R
(c) M is minimal ideal of R
(d) none of these.

5. If R is a commutative ring, with unit element then
(a) every maximal ideal is prime ideal
(B) every prime ideal is maximal ideal
(c) every ideal is prime ideal
(d) every ideal is maximal ideal.

6. If R is an integral domain with unit element, then
(a) R[x] is not a commutative ring
(b) R[x] have a unit element
© any unit in R[x] is unit in R
(d) any unit in R[x] is not an unit in R.

7. If the ring R has left identity e, and right identity e, then
@ $e_1 = e_2$
(c) $e_1 = me_2$
(b) $e_1 \setminus e_2$
(d) none of these.

8. Let R be a ring, U ≠ Ø ⊂R is ideal of R then,
A: U is a subgroup of R under addition
B: For all u Ɛ U and r Ɛ R; ur, ru Ɛ U
(A) A and B both are true
(b) only A is true
(c) only B is true
(d) both A and B are false.
9. If R is a ring in which $a^4 = a$, ∀ a ∈ R, then

(a) R is commutative
(b) R is not commutative
(c) R is zero ring
(d) none of these.

10. If the ring R is such that $(ab)^2 = a^2 b^2$, a, b ∈ R, then
(a) R is commutative
(b) R is not commutative
(c) R is zero ring
(d) none of these.

39. A ring R with binary operation addition is an Abelian group. It with binary operation multiplication, ¥ a, b e R, a. b= b.a, then R is
a commutative ring
(b) integral domain
(c) field
(d) null ring.

1.An integral domain D is of characteristic zero if

(a) ma = 0, a ≠ 0 Ɛ D=> m = 0

(b) a = 0, a ≠0 Ɛ D=> m ≠ 0

(c) ma = 0, a ≠ 0 Ɛ D=> m = a

(d) ma = 0, a ≠ 0 Ɛ D=> m ≠ a. ANS: A

2. A commutative division ring is -

(a) finite integral domain

(b) integral domain

(c) zero ring

(d) none of these. ANS: A

3. If R is a commutative ring with unit element, M is maximum ideal of R iff --

(a) R/M is a field

(b) M/R is a field

(c) RM is a field

(d) none of these. ANS: A

4. If F is a field then its only ideals are,

A: F, a field itself

B: (0)

(a) A and B are true

(b) A is true, B is false

(c) A is false, B is true

(d) A and B false. ANS: A

5. The ring of complex numbers C = {x + iy: x, y are real numbers, i = √-1} is---

(a) not an integral domain

(b) an integral domain

(c) ordered set

(d) none of these. ANS: B

6. If I is an integral domain and $a \neq 0$ Ɛ I then

(a) $a^2 = 0$

(b) $a^2 \geq 0$

(c) $a \neq 0$

(d) none of these ANS: C

7. Let R and R' be two arbitrary rings, Ø: R→ R' defined as Ø(a) = 0 for all a Ɛ R, then

(a) Ø is homomorphism

(b) Ø is automorphism

(c) Øis isomorphism

(d) none of these. ANS: A

8. If in a ring with unity $(xy)^2 = x^2y^2$, Ɐ x, y Ɛ R, then-----

(a) R is commutative ring

(b) R is an integral domain

(c) R is field

(d)none of these ANS: B

9. If I is a ideal in ring R then --

(a) R/I is a ring

(b) RI is a ring

(c) R + I is a ring

(d) none of these. ANS: A

10. A ring (R, +, .) is said to have zero divisor if-

(a) a, b Ɛ R, a. b = 0 => $a \neq 0$ or $b \neq 0$

(b) a, b Ɛ R, a. b = 0 => a = 0 or b= 0

(c) a, b Ɛ R, a. b = 0 => a =0 or b≠ 0

(d) a, b Ɛ R, a. b = 0 => a ≠ 0 or b= 0 ANS: a

11. A ring (R, +, ·) is said to have a ring without zero divisor if

(a) a, b Ɛ R, a. b = 0 => a ≠ 0 or b≠ 0

(b) a, b Ɛ R, a. b = 0 => a ≠ 0 or b = 0

(c) a, b Ɛ R, a. b = 0 => a = 0 or b = 0

(d) a, b Ɛ R, a. b = 0 => a = 0 or b≠ 0 ANS: C

12. An element a Ɛ (R, +, .) a ring is nilpotent if for some positive integer n ---

(a) $a^n = 0$

(c) $a^n = a$

(c) $a^n = 1$

(d) none of these. ANS: A

13. A field is a

(a) vector space

(b) integral domain

(c) division ring

(d) commutative division ring. ANS:D

14. An integral domain D is of finite characteristic, if ∀ aƐ D, there exist   m a positive integer such that

(a) ma = 1

(c) ma = 0

(b) ma = a

(d) none of these. ANS: B

15. If the ring R is finite and commutative with unit element, then

(a) every prime ideal is a maximal ideal

(b) every ideal is maximal ideal

(c) every maximal ideal is prime ideal

(d) (a) and (c) are both true. ANS: A

Part B

1.Which of the following statements is false?

(a) F[x] is an integral domain

(b) F[x] is Euclidean ring

(c) F[x] is principal ideal ring

(d) F[x] is not a group. ANS: D

2. If the ring R is an integral domain then

(a) R[x] is an integral domain

(b) R[x] is not an integral domain

(c) R[x] is a field

(d) R[x] is a commutative division ring, ANS:A

3. If integral domain D is of finite characteristic, then its characteristic is

(a) odd number

(b) even number

(c) prime number

(d) natural number. ANS:C

4. The set of complex number of the form x + iy is a field with respect to ordinary addition and multiplication, then the unit and zero elements are respectively

(a) 1 + i0 and 0 + i0

(b) 0 + i and 1 + i.0

(c) 0 and 1

(d) i and -i.   ANS: A

5. If C = {x + iy: x, y Ɛ R, i = √-1) is a field with respect to ordinary addition and multiplication, then the multiplicative inverse of non-zero element of a + ib Ɛ C is

(a) a + b

(b) $(a / a^2 + b^2) + i(-b/ a^2 + b^2)$

© $(a^2 + ib) / (a^2 + b^2)$

(d) none of these.   ANS: B

6. The following statement is false.

(a) Every field is an integral domain

(b) Every finite integral domain is a field

(d) Every integral domain is a field.

(c) Every field is a ring

ANS: D

7. A commutative ring R with unity is called integral domain if a, b Ɛ R-

(a) ab = 0 => a ≠0, b ≠0

(b) ab = 0   => a = 0 (or) b = 0

(c) ab = 0 =>a = b

(d) none of these. ANS: B

8. Check the correct statement

(a) Every subgroup of a cyclic group is cyclic

(b) If G is an infinite cyclic group, then G has exactly two generators and G is isomorphic to the additive group of integers.

(c) Every finite group of composite order possesses proper subgroups.

(d) all of the above.   ANS: D

9. Degree of Q (√2,√3) over Q where is the field of rational numbers is

(a) 4

(c) 1

(b) 3

(d) 2   ANS: A

10. The relation between the fields Q(√2) and Q (3 + V2) where Q is the field of rational numbers is

(a) Q (√2) + Q(3 + √2)=0

(b) Q (√2) = Q (3 + √2)

(c) Q (√2) * Q (3 + √2) = 0

(d) Q(√2) / Q(3 + √2) = 0   ANS: B

Unit 5- I msc - MCQ- Algebra

1. Let {v1, v2, … , vn} be independent vectors in a vector space V:
   - A) α1v1 + α2v2 + … + αnvn = 0 where not all the scalars αi are zero.
   - B) If dim V = n then {v1, v2, … , vn} spans V.
   - C) Some vi is a linear combination of the others.
   - D) There exists ij such that vi = αvj for some scalar α.

2. Let {u, v, w, z} be independent vectors in a vector space V.
   - A) {u + v, v + w, w + z, z + u} spans V.
   - B) {u + v, v + w, w + z, z + u} is independent.
   - C) Span {u + v,v + w, w + z,z + u} is contained in span {u, v, w z}.
   - D) {u + v, v + w, w + z, z + u} is a basis of V.

3. Let {v1, v2, … , vn} be dependent, nonzero vectors in a vector space V.
   - A) There exists ij such that vi = kvj for some scalar k.
   - B) {v1} is dependent.
   - C) Span {v1, v2, …, vn} has dimension smaller than n.
   - D) {vi, vj} is independent for some i ≠ j.

4. Let denote a basis of M2 ^{2}.
   - A) B must contain an invertible matrix.
   - B) B cannot contain a matrix A such that $A^2 = 0$.
   - C) If X is in R ^{2} and Ax = 0 for every A in B, then x = 0.
   - D) B must contain a symmetric matrix.

5. Let {A1, A2, …, An} be an independent set of matrices in Mn n, n ≥ 2.

A) {A1, A2, … , An} spans Mn n.

B) {A1^T, A2^T, … , An^T} is independent.

C) A1 + A2 + … + An = 0.

D) {A1, A2,… An-1, B} is independent where B = A1 + A2 + … + An-1.

6. Let L/K be a finite extension of fields. Which of the following assertions are correct:

A. If the characteristic of K is zero, then L/K is normal.

B. If the characteristic of K is zero, then L/K is separable.

C. If L/K is normal, then L/K is a Galois extension.

D. If the characteristic of K is positive, then L/K is normal if and only if it is separable.

Answer:

- (A) is not correct (counterexample: Q(√3 2)/Q is not normal).
- (B) is correct (result from 1st semester)
- (C) is not correct (if L/K is not separable; counterexample Fp(T 1/p)/F(T)).
- (D) is not correct (counterexample: Fp(T1/p)/Fp(T) is normal but not separable).

---

2. Let L/K be a finite extension of fields. Which of the following assertions are correct:

A. If L = K(x), where x is a root of a separable polynomial in K[X], then L/K is separable.

B. There exists x ∈ L such that L = K(x).

C. For any embedding σ of K in an algebraic closed-field K¯ , there exists τ : L → K¯ which extends σ.

Answer:

- (A) is correct (result from 1st semester)
- (B) is not correct in general (result from 1st semester, example is Fp(X1/p, Y 1/p).)

• (C) is correct (result from 1st semester).

3. Is it true that if K is a finite field, then any finite extension L/K is a Galois extension? What about any algebraic extension?
A. This is correct because any finite extension of K is a finite field,

B. Any extension of finite fields is Galois by a result from the class.
C. This is not the case for algebraic extensions with the definition in class because such extensions may be of infinite degree.
D. All the option given are correct

Answer: This is correct because any finite extension of K is a finite field, and any extension of finite fields is Galois by a result from the class. This is not the case for algebraic extensions with the definition in class because such extensions may be of infinite degree. (With proper definitions, in fact, any algebraic extension of a finite field is Galois).

4. Let K be a field, $\bar{K}$ an algebraic closure of K and $P \in K[X]$ a non-constant polynomial. Let $L \subset \bar{K}$ denote the splitting field of P in $\bar{K}$. Which of the following assertions are correct:

A. The extension L/K is a normal extension.
B. If $x \in \bar{K}$ is a root of P, then L = K(x).
C. The extension L/K is a Galois extension.
D. If the polynomial P is irreducible, then L/K is a Galois extension.
E. If the characteristic of K is zero, then L/K is a Galois extension.

Answer:
• (A) is correct (one of basic example of normal extension)
• (B) is not correct, because a single root of P might not be enough (counterexample: $K = Q$, $P = X3 - 2$; then Q(
√3
2) is not the splitting field of P).
• (C) is not always correct (only if P is separable; counterexample is K = Fp(T), P = Xp − T).
• (D) is not always correct (only if P is separable; same counterexample).
• (E) is correct (because L/K is always separable in that case).

5. Let K be a field, $\bar{K}$ an algebraic closure of K and $L \subset \bar{K}$ a finite extension of K such that L/K is a Galois extension. Let $K \subset E \subset L$ be an intermediate extension. Which of the following assertions are correct:

A. The extension L/E is a Galois extension.
B. The extension E/K is a normal extension.
C. The extension E/K is a separable extension.

Answer:
• (A) is correct (basic result from Galois correspondance)
• (B) is not correct (counterexample: K = Q, L splitting field of X3−2, E = Q(√3 2); the E/Q is not normal).
• (C) is correct (subextensions of separable extensions are separable, as follows for instance from the characterization using separability of minimal polynomials).

6. Let K be a field, $\bar{K}$ an algebraic closure of K and $L \subset \bar{K}$ a finite extension of K such that L/K is a Galois extension, and let G be its Galois group. Which of the following assertions are correct:

A. For any subgroup H of G, the intermediate extension $E = L^H$ is a normal extension of K.
B. Two subgroups H_1 and H_2 of G are equal if and only if $L^{H1} = L^{H2}$.
C. Any subgroup H of G is the Galois group of some extension E/K for some $E \subset L$.
D. Any subgroup H of G is the Galois group of some extension L/E for some $E \subset L$.

Answer:
• (A) is not correct ($E = L^H$ is normal over K if and only if H is a normal subgroup of K)
• (B) is correct (injectivity of the map $H \to L^H$ in the Galois correspondance)
• (C) is not correct (counterexample: if $G = S_3$ is the symmetric group and H is generated by a cycle of length 3, so that H has order 3, then an intermediate E with Gal(E/K) = H would correspond to a normal subgroup K < G with $[S_3 : K] = [L : E] = 2$, but one can see easily that there is no normal subgroup of order 2 in S_3)
• (D) is correct (Galois correspondance: one can take $E = L^H$ since $H = Gal(L/L^H)$)

7. Let K be a field, $\bar{K}$ an algebraic closure of K and $L \subset \bar{K}$ a finite extension of K such that L/K is a Galois extension, and let G be its Galois group. Let $x \in L$ be given and $\sigma_0 \in G$ a non-trivial element. Which of the following assertions are correct:

A. If $\sigma_0(x) = x$, then $x \in K$.
B. If G is cyclic and $\sigma_0(x) = x$, then $x \in K$.
C. The element $\sum_{\sigma \in G} \sigma(x)^2$ belongs to K.
D. If the set of all σ(x), for σ ranging over G, contains at most two elements, then $[K(x) : K] \leq 2$.

Answer:
• (A) is not correct (by Galois correspondance, $x \in K$ if and only if $\sigma(x) = x$ for all $\sigma \in G$; so $\sigma_0(x) = x$ does not imply $x \in K$ unless σ_0 generates G)
• (B) is not correct (although G is cyclic, it might be that σ_0 is not a generator)
• (C) is correct (by Galois correspondance, one checks by reordering the sum that the sum y indicated satisfies $\tau(y) = y$ for all $\tau \in G$, so that $y \in L^G = K$).
• (D) is correct (the assumption implies that the separable degree of K(x)/K is at most 2, since the roots of the minimal polynomial P of x are among the values σ(x), by transitivity of the action of the Galois group of the splitting field of P on the set of roots).

8. Let K be a field, $\bar{K}$ an algebraic closure of K and $L \subset \bar{K}$ a finite extension of K of degree 2. Which of the following assertions are correct:
A. The extension L/K is separable.
B. The extension L/K is normal.
C. If the characteristic of K is zero, then there exists $y \in L$ such that L = K(y) and $y^2 \in K^\times$.
D. Both the answers - The extension L/K is normal. & If the characteristic of K is zero, then there exists $y \in L$ such that L = K(y) and $y^2 \in K^\times$.

Answer:
• (A) is not correct (counterexample if $F2(\sqrt{T})/F2(T)$)
• (B) is correct (result from the class)
• (C) is correct (result from th

9. A Ring is said to be commutative if it also satisfies the property
a) monoid

b)associative
c) Commutativity of addition

d) Commutativity of multiplication.

View Answer

Answer: d
Explanation: A Ring is said to be commutative if it also satisfies the Commutativity of multiplication.

10.An ‘Integral Domain’ is

a) semigroup under + and .

b) monoid under + and .

c) Ring without zero diviser

d) none of the option given

Answer: c
Explanation:An ‘Integral Domain’ satisfies

11. For the group Sn of all permutations of n distinct symbols, what is the number of elements in Sn?
a) n
b) n-1
c) 2n
d) n!
View Answer

Answer: d
Explanation: There there are n distinct symbols there will be n! elements.

12. For the group Sn of all permutations of n distinct symbols, Sn is an abelian group for all values of n.
a) statement given is True
b) statement given is False

1. a is correct since For n>2 it does not form a Abelian Group.

2. a & b both are wrong since For n>2 it does not form a Abelian Group.

3. b is correct since For n>2 it does not form a Abelian Group.

4. b is wrong since For n>2 it does not form a Abelian Group.

Answer: b
Explanation: For n>2 it does not form a Abelian Group.

13. Is S a ring from the following multiplication and addition tables?

+	a	b	x	a	b
a	a	b	a	a	a
b	b	a	b	a	b

a) Yes
b) No
c) Can't Say
d) Insufficient Data
View Answer

Answer: a
Explanation: S is a ring as it satisfies the properties G-i to R-iii.

14. Does the set of residue classes (mod 3) form a group with respect to modular addition?
a) Yes, The identity element is 0
b) No
c) Can't Say
d) Insufficient Data
View Answer

Answer: a
Explanation: Yes. The identity element is 0, and the inverses of 0, 1, 2 are respectively 0, 2, 1.

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

15. If $f(x)=x^7+x^5+x^4+x^3+x+1$ and $g(x)=x^3+x+1$, find f(x) x g(x).
a) $x^{12} + x^5 + x^3 + x^2 + x + 1$
b) $x^{10} + x^4 + 1$
c) $x^{10} + x^4 + x + 1$
d) $x^7 + x^5 + x + 1$
View Answer

Answer: c
Explanation: Perform Modular Multiplication.

PART B

1. If $f(x)=x^7+x^5+x^4+x^3+x+1$ and $g(x)=x^3+x+1$, find the quotient of f(x) / g(x).

a) x^4+x^3+1
b) x^4+1
c) x^5+x^3+x+1
d) x^3+x^2
View Answer

Answer: b
Explanation: Perform Modular Division.

2. Primitive Polynomial is also called a ____
i) Perfect Polynomial
ii) Prime Polynomial
iii) Irreducible Polynomial
iv) Imperfect Polynomial

a) ii) and iii)
b) only iii)
c) iv) and ii)
d) None
View Answer

Answer: a
Explanation: Irreducible polynomial is also called a prime polynomial or primitive polynomial.

3. Which of the following are irreducible polynomials?
i) X^4+X^3
ii) 1
iii) X^2+1
iv) X^4+X+1

a) i) and ii)
b) only iv)
c) ii) iii) and iv)

d) All of the options
View Answer

Answer: d
Explanation: All of the mentioned are irreducible polynomials.

4. Find the HCF/GCD of $x^6+x^5+x^4+x^3+x^2+x+1$ and x^4+x^2+x+1.
a) $x^4+x^3+x^2+1$
b) x^3+x^2+1
c) x^2+1
d) x^3+x^2+1
View Answer

Answer: b
Explanation: Use Euclidean Algorithm and find the GCD. GCD = x^3+x^2+1.

5. On multiplying $(x^5 + x^2 + x)$ by $(x^7 + x^4 + x^3 + x^2 + x)$ in GF(28) with irreducible polynomial $(x^8 + x^4 + x^3 + x + 1)$ we get
a) $x^{12}+x^7+x^2$
b) $x^5+x^3+x^3$
c) $x^5+x^3+x^2+x$
d) $x^5+x^3+x^2+x+1$
View Answer

Answer: d
Explanation: Multiplication gives us $(x^{12} + x^7 + x^2)$ mod $(x^8 + x^4 + x^3 + x + 1)$.
Reducing this via modular division gives us, $(x^5+x^3+x^2+x+1)$

6. Find the minimum polynomial of the matrix

2	1	0	0
0	2	0	0
0	0	2	0
0	0	0	5

1) $(t-2)^3 (t-5)$ 3) t^3+t^2 2) $(t-2)^2 (t-5)$ 4) none of these
159. If 0 is an eigen value of T if and only if T is

1. A singular 3) non-singular 2) null matrix 4) none of these

7. Find the minimal polynomial m(t) of the matrix
A=

λ	α
0	λ

for a ≠ 0.
1) $(t-\lambda)$ 3) $(t-\lambda)^3$ 2) $(t-\lambda)^2$ 4) none of these
8. Let a, b, c be elements of a field F and

0	0	c
1	0	b
0	1	a

find the minimal polynomial

1) $x^3 + ax^2 + bx + c$ 3) $ax^3 - bx^2 - cx + 1$ 2) $x^3 - ax^2 - bx - c$ 4) none of these

9. A vector space V over F is said to be ---------if there is defined for any two ordered pair of vectors u,veV an element (u, v) in F such that

i) $(u, v) = \overline{(v, u)}$

ii) $(u,u) \geq 0$ and $(u,u)=0$ iff $u=0$

iii) $(au+bv, w)=a(u,v)+b(v,w)$ for all u,v,w and a,b Ɛ F

1) inner product space 2) subspace 3) dual space 4) none of these

10. Every finite dimentional inner product space has an orthonormal basis

1. Cauchy - schwarz theorem

2. Gram-schmidt orthogonalisation process

3. Riemann theorem

4. None of these

https://www.sanfoundry.com/advanced-cryptography-questions-answers/
https://www.pakmath.com/2019/03/12/algebra-mcqs-test-05/4/