2/1/18

Lecture - 1

⇒ Course Topic:

Groups: 1. Group homomorphism, Rings and Fields

2. Vector spaces, Linear maps, ~~direct~~ direct products, direct sums, linear independence, bases and dimension, rank nullity, dual spaces, dual basis.

3. Matrices, Determinants as the multilinear alternating, normalized map, properties of determinants, determinant of product, determinants of the inverse, characteristic polynomial, eigen-values, eigen vectors, eigen basis, Caylay Hamilton theorem, triangular form, charecteristic subspaces.

4. Linear systems, Gauss-Jordon elimination, row-echolon form, reduced row-echolon form, matric inversion, similiar and equivalent matrices

⇒ Grading:

Mid 1: 20%

Mid 2: 20%

End : 35%

Project : 25%

⇒ Reference books:

1. Linear Algebra by Huffman and Ray Kunze, Prentice Hall, Eagleword Cliff, New Jerry.
2. Linear Algebra and it's application by Gilbert Strang
3. Linear Algebra: A geometric approach by S Kumaresan

⇒ Group

→ A nonempty set of elements G is said to form a group.

If in G, there is a defined binary operation $*$ such that

monoid { semi-group {

1) $a, b \in G \Rightarrow a*b \in G$ (Closure)
2) $a, b, c \in G \Rightarrow a*(b*c) = (a*b)*c$ (Associative)

3) $\exists$ an element $e \in G$ such that $a*e = e*a = a$
4) For every $a \in G$, $\exists$ an element $a^{-1} \in G$ s.t. $a*a^{-1} = a^{-1}*a = e$ (Inverse)

→ Eg :- Integers under addition is group
Integers under multiplication is monoid

→ If $a*b = b*a$ then group is called Abelian group.

→ Eg :- 1. $G = \{1, -1\}$ → group

2. Let G be the set of all 2×2 matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$, $a, b, c, d \in R$ s.t. $ad - bc \neq 0$. Show that G is a group with matrix multiplication.

→ Closure :

$$\begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix} * \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix} = \begin{pmatrix} a_1a_2 + b_1c_2 & a_1b_2 + b_1d_2 \\ \cdots & \cdots \end{pmatrix}$$

Since $a_1, a_2, b_1, b_2, c_1, c_2, d_1, d_2 \in R \Rightarrow a_1a_2 + b_1c_2, \ldots \in R$.

→ Associativity

$$\begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix} * \left(\begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix} * \begin{pmatrix} a_3 & b_3 \\ c_3 & d_3 \end{pmatrix} \right) =$$

$$\left(\begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix} * \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix} \right) * \begin{pmatrix} a_3 & b_3 \\ c_3 & d_3 \end{pmatrix}.$$

→ Identity.

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} * \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

Identity element e.

→ Inverse exist because $\left| \begin{pmatrix} a & b \\ c & d \end{pmatrix} \right| \neq 0$

5/1/18

Lecture-2

→ If $(G,*)$ is a group, then

i) the identity element of G is unique.

ii) Every $a \in G$, has an ~~inverse~~ unique inverse in

iii) For any $a \in G$, $(a^{-1})^{-1} = a$.

iv) For $a, b \in G$, $(a*b)^{-1} = b^{-1} * a^{-1}$

→ Let e and f are two identity elements.

$$e*f = f*e = f$$
$$f*e = e*f = e$$
$$\therefore \boxed{f = e}$$

→ Let a' and a'' are two inverse of $a \in G$

→ If a' is inverse of a

$$a*a' = a'*a = e$$

→ If a'' is inverse of a

$$a*a'' = a''*a = e$$

→ $a'*e = a'$

$$\therefore a' = a'*(a*a'')$$
$$= (a'*a)*a'' \quad \text{(Associative property)}$$
$$= e*a''$$
$$= a''$$

→ We need to prove $(a*b)*(b^{-1}*a^{-1}) = e$

$$\text{L.H.S} = a*(b*b^{-1})*a^{-1}$$
$$= (a*e)*a^{-1}$$
$$= a*a^{-1} = e$$

~~Let~~ &

→ Order of an element 'a' $\in G$ is the least positive integer m such that

$$a^m = e.$$

$$(\underbrace{a*a*----}_{m\text{ times}}) = e.$$

→ Theorem: Let $a \in (G, *)$ then $O(a) = O(a^{-1})$

→ Let $O(a) = n$

$\Rightarrow a^n = e$ (where n is the least positive integer)

$$(a^{-1})^n = a^{-n} = (a^n)^{-1} = e^{-1} = e$$

Proof is not complete, we should also show n is the least positive integer. for a^{-1}

→ Let $O(a^{-1}) = m < n$

$(a^{-})^m = e.$

$\Rightarrow a^{-m} = e.$

$\Rightarrow a^n * a^{-m} = a^n * e.$

$a^{n-m} = e * e = e$

Here $n-m$ is +ve integer

$\therefore O(a) = n-m$

→ Hence contradiction because our assumption is that $O(a) = n$.

→ $O(a) \rightarrow$ infinite

If no positive powers of a equals to identity.

DIY. Case 2 for previous theorem:
If $O(a) \to$ infinite.

→ Theorem: If an element a of a group is of order 'n' i.e. $O(a) = n$, then $a^m = e$ iff n is a divisor of m.

→ Let 'n' is not a divisor of m.

$m \geq n \Rightarrow m = xn + y \qquad 0 \leq y < n$

$\qquad\qquad\qquad\qquad\qquad x, y \in I$

$$a^m = e$$
$$\Rightarrow a^{xn+y} = e$$
$$\Rightarrow a^{xn} \cdot a^y = e$$
$$\Rightarrow (a^n)^x \cdot a^y = e$$
$$\Rightarrow e^x \cdot a^y = e$$
$$\Rightarrow a^y = e \Rightarrow O(a) = y \quad (\because 0 < y < n)$$

Contradiction because given $O(a) = n$

→ So only correct choice for y is to be $0 \Rightarrow m = x$

Case 2
→ Let $O(a^{-1}) = m$ where $m =$ finite

$$\Rightarrow O(a^{-1})^m = a^{-m} = e$$
$$\Rightarrow a^m * a^{-m} = a^m * e$$
$$\Rightarrow e = a^m * e = a^m$$

⇒ contradiction because $m \to$ infinite.

⇒ Subgroup: A non-empty subset H of a group G is said to be subgroup of G if under the operation in G, * H itself forms a group

→ A non-empty subset H of a group G is a subgroup of G
iff

1) $a, b \in H \Rightarrow a * b \in H$
2) $a \in H \Rightarrow a^{-1} \in H$

(Only this 2 properties are enough to prove H is a group)
(If given finite subset H then only property 1 is enough to prove group).

→ Identity exist
If $a \in H$ then $a^{-1} \in H$ (by 2)
$a * a^{-1} = e \in H$ (by 1)
→ Associativity holds is trivial and holds for any subset.

→ Theorem: If H is a non-empty finite subset of a group G and H is closed under multiplication, then H is a subgroup of G.

9/1/18 → Suppose, $a \in H$ thus $a^2 = a * a \in H$ ... $a^m \in H$ ....
Since H is closed. The infinite collection of elements $a, a^2, \ldots, a^m, \ldots$ must belong to H. (However H is a finite set)
Hence, there must be repetition of elements in the collection i.e. for some integer $a^r = a^s$ $(r > s > 0)$
→ By cancellation, in G
$$a^{r-s} = a^s * a^{-s} = e \in H \Rightarrow r-s \geq 1 \Rightarrow r-s-1 \geq 0$$
($a \in H \Rightarrow a \in G$ and G is a group)

9/01/18

Lecture - 3

$$a * a^{r-s-1} \in a^{r-s} = e*a$$

$$\therefore \quad a^{r-s-1} = a^{-1} \in H$$

Q. Let G be a group of integers under addition. Let H be the subset consisting of all multiples of 5 (i.e. $H = \{5m \mid m \in G\}$). Show that H is a subgroup.

Def^{n} ~~Let G be~~

→ Closure.

If $a, b \in G$ $5a, 5b \in H$

$a+b \in G$ $5a + 5b = 5(a+b) \in H$

→ Inverse.

G is a group $\therefore \forall a \ \exists$ an inverse s.t.

$a * a^{-1} = 0$.

$a^{-1} = -a. \in G$

$5a + (-5a) = 0$

$5a \in H$.

$-5a \in H$

Def^{n} Let G be a group and H is a subgroup of G, for $a, b \in G$, we say that a is congruent to b, written as $a \equiv b \bmod H$ if $a * b^{-1} \in H$.

→ $A = \{1, 2, 3, 4\}$

$A * A = \{\underset{\text{Reflexive}}{(1,1)}, \ldots\}$

Camlin Page
Date / /

Theorem The relation $\boxed{a \equiv b \bmod H}$ is an equivalence relation

① Reflexive: $a \equiv a \bmod H$ holds $\forall a \in G$
$\Rightarrow a * a^{-1} = e \in H$

② Symmetric: $a \equiv b \bmod H$
$a * b^{-1} \in H$.
$\Rightarrow (a * b^{-1})^{-1} \in H$ (H is a group)
$\Rightarrow (b^{-1})^{-1} * a^{-1} \in H$
$\Rightarrow b * a^{-1} \in H$.
$\Rightarrow b \equiv a \bmod H$.

③ Transitive: If $a \equiv b \bmod H$ and $b \equiv c \bmod H$
To show $a \equiv c \bmod H$
We know $a * b^{-1} \in H$ and $b * c^{-1} \in H$.
Then by closure. $(a * b^{-1}) * (b * c^{-1}) \in H$
by assoc property $a * (b^{-1} * b) * c^{-1} \in H$
(existence of identity) $a * e * c^{-1} \in H$
$a * c^{-1} \in H$
$\therefore a \equiv c \bmod H$

Problems

① The intersection of two subgroups of a group $(G, *)$ is a subgroup of G.

② The union of two subgroups is a subgroup iff one is combined in other.

→ ① Suppose $(G, *)$ is a group
$H_1, H_2 \rightarrow$ subgroups of G
To show: $(H_1 \cap H_2)$ is a subgroup of G.

→ Let $a, b \in H_1 \cap H_2$.

$\Rightarrow$ $a \in H_1$ $\quad$ $b \in H_1$ → H_1 is a subgroup

$a \in H_2$ $\quad$ $b \in H_2$. → H_2 is a subgroup

$a * b \in H_1$
$a * b \in H_2$. $\Big\rangle$ → $a * b \in H_1 \cap H_2 \Rightarrow H_1 \cap H_2$ is

Let $a \in H_1 \cap H_2$ → $a^{-1} \in H_1 \cap H_2$

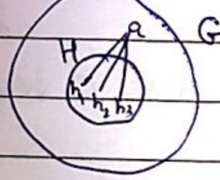
↳ $a \in H_1$ $\qquad$ $a \in H_2$

↓ $\qquad$ ↓

$a^{-1} \in H_1$ $\qquad$ $a^{-1} \in H_2$.

↳ $a^{-1} \in H_1 \cap H_2$ → ∴ inverse exists

Def^{-n} If H is a subgroup of G, $a \in G$, then $Ha = \{h * a \mid h \in H\}$.
Ha is called the right coset of H in



$Ha = \{h_1 * a, h_2 * a, \ldots, h_n * a\}$

Left coset : $aH = \{a * h \mid h \in H\}$.

Lemma: For all $a \in G$

$Ha = \{x \in G \mid a \equiv x \mod H\}$.

$= Cl[a]$

↳ This is called class of equivalence of a.

→ ① $Ha \subset Cl[a]$
② $Ha \supset Cl[a]$ $\Big\rangle$ → $Ha = Cl[a]$

→ ① Let $x \in Cl[a]$

$\Rightarrow a * x^{-1} \in H$

$\Rightarrow (a * x^{-1})^{-1} \in H$ ($\because$ H is a subgroup)

$\Rightarrow x * a^{-1} \in H \Rightarrow x * a^{-1} = h$ (where $h \in H$).

$\Rightarrow (x * a^{-1}) * a = h * a$

$\Rightarrow x = h * a \in Ha$.

$\therefore Cl[a] \subset Ha$

② Let $x \in Ha$

$\Rightarrow \exists h \in H \quad x = h * a$

$\Rightarrow x^{-1} = (h * a)^{-1} = a^{-1} * h^{-1}$.

$\Rightarrow a * x^{-1} = h^{-1} \in H$ ($\because$ H is a subgroup)

$\Rightarrow a \equiv x \mod H$

$\therefore x \in Cl[a]$

$\therefore Ha \subset Cl[a]$

→ From ① & ② $Ha = Cl[a]$.

12/1/18

Lecture - 4

⇒ Cyclic group : If the elements of a group a generated from a single element 'a' by composition, then the group is said to be cyclic. The element 'a' is called the generator of the cyclic group. The group is denoted by $\{a\}$.

① If a is the generator of a cyclic group then a^{-1} is also it's generator.

② Every cyclic group is abelian.

→ ① Since a is the generator, a^n is an element of the group

$$a^n = (a^{-1})^{-n}. \quad (a^{-1} \text{ is also the generator})$$

② If we take two arbitrary elements $b, c \in G$

Let a be the generator of group G.

$$\Rightarrow b = a^r, \quad c = a^s \quad (\text{for some int } r, s)$$

$$b * c = a^r \cdot a^s = a^{r+s}$$

$$= a^{s+r} \quad (\text{Int are comm.})$$

$$= a^s \cdot a^r = c * b.$$

→ If G is a finite group and H is a subgroup of G, then $O(H)$ is a divisor of $O(G)$.

→ Suppose G is a finite group and H is a subgroup of G.

i) If $O(H) = O(G)$ ✓

ii) If $H \in G$ then let us ~~measure~~ assume $O(H) = r$.

→ Let $a \in G$, $a \notin H$.
Let $h_1, h_2, \ldots, h_r$ r elements in H.
then 'a' will combine with all elements in H. — first line
i.e. $h_1 * a, h_2 * a, ---, h_r * a$. — second line.

→ We claim that all centres of the second line.
① different from each other
② different from first line.

① $h_i * a = h_j * a$.
from cancellation
$h_i = h_j$ → this is not possible from our assumption

② $h_i = h_j * a$
$a = h_j^{-1} * h_i = h_k$.

i.e. $a \in H$ but it contradicts our assumption of $a \notin H$. So, $h_i \neq h_j * a$

So, far we have listed $2O(H)$ elements of this elements account for all elements of G then we are done. $[O(H) / O(G)]$

If this is not the case, then choose an element $b \in G$, which are not present in those two lines.

Scanned by CamScanner

$h_1, h_2, \ldots, h_r$
$h_1 * a, h_2 * a, \ldots, h_r * a$
$h_1 * b, h_2 * b, \ldots, h_r * b$

$a * b = ?$
May lie in first line or outside all three lines.

① $h_i * a = h_j * b$

$$b = h_j^{-1} * h_i * a = h_k * a \in 2^{nd} \text{ line}$$

but b does not lie so contradiction

② $h_i * b = h_j * b$
cancellation
$h_i = h_j$ (Contradiction

→ Lagrange's Theorem (Above process).

→ $\boxed{Ha = Cl[a]}$ ← Right coset.
↳ Equivalence class in G will partition entire set G.

DIY → Show that between two right cosets Ha and Hb there exists one to one correspondence.

Camlin Page
Date / /

Def^n A subgroup N of G is said to be a normal subgroup of G if for every $g \in G$ and $n \in N$

$$gng^{-1} \in N.$$

$$gng^{-1} = \{gn_1g^{-1}, gn_2g^{-1}, \dots, gn_kg^{-1}\}$$
$$n_1, n_2, \dots, n_k \in N.$$

Equivalently if by gng^{-1} we mean the set of all gng^{-1} $n \in N$, the N is a normal subgroup of G iff.

$$gng^{-1} \subset N \quad \text{for every} \quad g \in G.$$

Lemma If N is a normal subgroup of G iff ~~$gng^{-1} \subset N$~~ $gNg^{-1} = N$ for every $g \in G$.

Proof :

① If $gNg^{-1} = N \Rightarrow gNg^{-1} \subset N$
$\Rightarrow N$ is normal subgroup so from def^n
$gNg^{-1} \subset N$ is true.

If N is a normal subgroup $\Rightarrow$
Then if $g \in G$, $gNg^{-1} \subset N$

② $g^{-1}Ng = g^{-1}N(g^{-1})^{-1} \subset N \quad (g^{-1} \in G)$

$$N = g\underbrace{(g^{-1}Ng)}_{\in N}g^{-1} \subset gNg^{-1}$$

16/1/18 Lecture-5

Camlin Page
Date / /

Q. The subgroup N of G is normal subgroup if every left coset of N in G is a right coset of N in G.

Proof If N is a normal subgroup of G then for every $g \in G$, we have

$$gNg^{-1} = N$$
$$(gNg^{-1})g = Ng$$

$$gN(g^{-1}g) = Ng$$
$$\boxed{gN = Ng}$$

→ Converse.

$$gN = Ng \quad \forall g \in G$$
$$gNg^{-1} = Ngg^{-1}$$
$$gNg^{-1} = N$$

* Suppose that N is a normal subgroup of G, and $a, b \in G$ then.
$$NaNb = Nab.$$

$$NaNb = NNab$$
$$= N^2ab$$
$$= Nab \quad \text{(Closure)}$$

Q. Let G/N denote the collection of right cosets of N in G. Show that G/N forms a group w.r.t this coset multiplication.

→ Let $Ng_1 \in G/N$ $\quad g_1, g_2 \in G$.
$Ng_2 \in G/N$

$Ng_1 Ng_2 = Ng_1g_2 = Nc$ ($c = g_1g_2 \in G$
$\in G/N$ $\because G$ is closed)

Closure proved.

→ Let $X, Y, Z \in G/N$
$X = Na$
$Y = Nb$
$Z = Nc$

$(XY)Z = (NaNb)Nc$
$= (Nab)Nc$
$= Nabc$
$= Na(bc)$
$= X(YZ)$

Associative proved

→ Consider the element $N = Ne \in G/N$.
If $X \in G/N$, $X = Na$ for $a \in G$
$XN = NaNe = Nae$
$= Na = X$ ($\because e$ is the identity element of G)

$NX = NeNa = Nea = Na = X$.

Identity proved.

→ Suppose $X \in G/N$
$X = Na$, $a \in G$.
$Na^{-1} \in G/N$ $\quad (\because a^{-1} \in G)$
$NaNa^{-1} = Naa^{-1} = Ne = N$.
$Na^{-1}Na = Na^{-1}a = Ne = N$.

$\therefore Na^{-1}$ is the inverse of G/N group

→ Hence proved G/N is a group called Quotient group.

⇒ Homomorphism.

Def^n A mapping ϕ from a group $(G,*)$ into a group $(G,\circ)$ is called homomorphism if for all $a,b \in G$

$$\boxed{\phi(a*b) = \phi(a)\circ\phi(b)}$$

Q. Let G be a group of integers under addition.

$$\phi : (G,+) \to (G,+)$$

$\forall x \in G$ $\phi(x) = 2x$
Show that ϕ is homomorphism.

→ $$\phi(x+y) = \cancel{\phi(x)+\phi} \; 2(x+y)$$
$$= 2x + 2y$$
$$= \phi(x) + \phi(y).$$

Q. Let G be a group of all non-zero real numbers under multiplication.

$\bar{G} = \{+1, -1\}$, where $1\cdot 1 = 1$, $(-1)\cdot(-1)$ $1(-1) = (-1)1 = -1$.

Define $\phi : G \to \bar{G}$

$\phi(x) = 1$ if x is positive
$= -1$ if x is negative.

Find ϕ is homomorphism or not?

$\rightarrow$ Let $a, b \in N$.

① $a > 0, b > 0$

$\phi(a * b) = 1$
$= 1 \cdot 1$
$= \phi(a) \cdot \phi(b)$

② $a > 0, b < 0$

$\phi(a * b) = -1$
$= 1 \cdot -1$
$= \phi(a) \cdot \phi(b)$

③ $a < 0, b > 0$

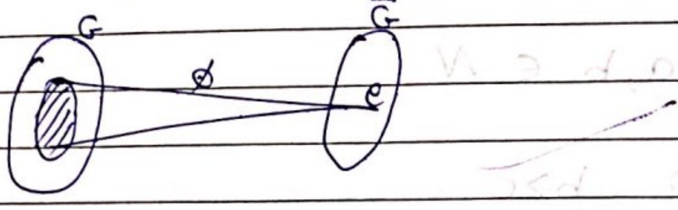
$\phi(a * b) = -1$
$= -1 \cdot 1$
$= \phi(a) \cdot \phi(b)$

④ $a < 0, b < 0$

$\phi(a * b) = 1$
$= -1 \cdot -1$
$= \phi(a) \cdot \phi(b)$

Def^{-n}. If ϕ is a homomorphism of G into $\bar{G}$ then kernel of ϕ, K_ϕ is defined by

$K_\phi = \{x \in G \mid \phi(x) = \bar{e}$, $\bar{e}$ is the identity element



Lemma If ϕ is a homomorphism of G into $\bar{G}$ then show that.

① $\phi(e) = \bar{e}$

② $\phi(x^{-1}) = \{\phi(x)\}^{-1}$ $\forall x \in G$.

①
$$\phi(x) \cdot \bar{e} = \phi(x)$$
$$= \phi(xe)$$
$$= \phi(x)\phi(e)$$

$$\boxed{\phi(x)\,\bar{e} = \phi(x)\phi(e)}$$

$\Rightarrow$ $\phi(e) = \bar{e}$.

②
$$\phi(x) = \bar{e}$$
$\Rightarrow$ $\bar{e} = \phi(xx^{-1})$

$\Rightarrow$ $\bar{e} = \phi(x)\phi(x^{-1})$

Similiarly
$$\bar{e} = \phi(x^{-1})\phi(x).$$

$\therefore$ $\phi(x^{-1}) = \{\phi(x)\}^{-1}$.

Camlin Page
Date / /

Lemma 2 Suppose G is a group and N is a normal subspace of G define the mapping ϕ from G to G/N by $\phi(x) = N(x)$. $\forall x \in G$.
Then show that ϕ is a homomorphism of G onto G/N.

Lemma 3 If ϕ is a homomorphism of G onto $\bar{G}$ with kernel K, then K is a normal subgroup of G.

Lemma 3 Proof

→ ① If $x, y \in K$,

$$\left.\begin{array}{l}\phi(x) = \bar{e}\\ \phi(y) = \bar{e}\end{array}\right\} \quad \phi(xy) = \phi(x)\,\phi(y) = \bar{e}\cdot\bar{e} = \bar{e}$$

$\Rightarrow xy \in K$ } K is closed

② If $x \in K \Rightarrow \phi(x) = \bar{e}$

$\phi(x^{-1}) = \{\phi(x)\}^{-1} = \{\bar{e}\}^{-1} = \bar{e}$

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

① & ② $\Rightarrow$ K is a subgroup of G.

③ For every $g \in G$, $k \in K$ $gkg^{-1} \in K$
i.e. $\phi(gkg^{-1}) = \bar{e}$ (To show)

$$\phi(gkg^{-1}) = \phi(g)\,\phi(k)\,\phi(g^{-1})$$
$$= \phi(g)\,\bar{e}\,\phi(g^{-1})$$
$$= \phi(g)\,\phi(g^{-1}) \quad (\because \bar{e} \text{ is identity element})$$

$= \phi(g) \cdot \{\phi(g)\}^{-1}$
$= \bar{e}$.

$\Rightarrow gkg^{-1} \in K$ } K is a normal subgroup of

Lemma 2 Proof
$\rightarrow$ ① Let $x, y \in G$.

$\phi(xy) = Nxy$
$= NxNy$ (∵ N is a normal subgroup)
$= \phi(x)\phi(y)$

$\Rightarrow \phi$ is homomorphism.

$\boxed{DIY}$ ② Onto proof

Camlin Page
Date / /

Def^{n} A homomorphism ϕ from ~~the~~ G to $\bar{G}$ is said to be isomorphic if ϕ is one to one.

Two groups G, G^* are said to be isomorphic if there is an isomorphism of G onto G^*

$G \approx G^*$.

① $G \approx G$

② $G \approx G^* \Rightarrow G^* \approx G$.

③ $G \approx G^*$, $G^* \approx G^{**}$
$\rightarrow G \approx G^{**}$.

19/1/18 Lecture-6

⇒ Rings :

Def^{-n} A non-empty set R is said to be an consective ring if in R there are defined two operations denoted by + and • respectively. Such that for all a, b, c ∈ R

→ Properties .

$(R,+)$ → commutative group

1. $a+b \in R$
2. $a+b = b+a \quad \forall a,b \in R$
3. $a+(b+c) = (a+b)+c \quad \forall a,b,c \in R$
4. There is an element 0 in R such that $a+0 = 0+a = a$ $(\forall a \in R)$ — additive identity w.r.t + or zero element
5. There exists an element $a \in R$ such that $a+(-a) = (-a)+a = 0$.

$(R,\cdot)$ → semigroup

6. $a\cdot b \in R$
7. $a\cdot(b\cdot c) = (a\cdot b)\cdot c$
8. $a\cdot(b+c) = a\cdot b + a\cdot c$
   $(b+c)\cdot a = b\cdot a + c\cdot a$

$(R,+,\cdot)$ → Commutative group $(R,+)$
→ Semi group $(R,\cdot)$
→ Distributed property.

→ $(R,+,\cdot)$ is called a commutative ring
$\forall a,b \in R$
$a\cdot b = b\cdot a$

Camlin Page
Date / /

→ Let $(R, +, \cdot)$ be a ring. Then $(R, +, \cdot)$ is a ring with multiplicative identity (unit element) iff
$\exists$ an element $1 \in R$ such that
$1 \cdot a = a \cdot 1 = a$.

Prob: ① Show that the mathematical structure $(P(S), \Delta, \cap)$ is a ring. Is there any multiplicative identity of the ring?
DIY

$$A \Delta B = \{x \mid x \in A \cup B \quad x \notin A \cap B.$$
$P(S)$ is power set of S.

→ An element a of the ring $(R, +, \cdot)$ with unit element '1' is called invertible if there exists an inverse $a^{-1} \in R$ of the element $a \in R$ under multiplication such that

$$aa^{-1} = a^{-1}a = 1 \text{ (unit element)}$$

→ Eg: $(Z, +, \cdot)$
$Z^* = \{1, -1\}$

$(R^*, +, \cdot)$ call elements have inverses.
$R^* = R - \{0\}$.

→ Let R' be the set of ordered pairs of real numbers i.e. $R' = R \times R$, and addition $\oplus$ and multiplication $\odot$ in R' is defined as.

$(a,b) \oplus (c,d) = (a+c, b+d)$

$(a,b) \odot (c,d) = (ac, bd)$

Show that $(R', \oplus, \odot)$ is a commutative ring.

Prob. ① If $a, b \in R$ $(R, +, \cdot) \rightarrow$ ring then

$a+b = a+c.$

$\Rightarrow b = c.$

Prob. ② If any ring $(R, +, \cdot)$, if $a \in R$, then

$a \cdot 0 = 0 \cdot a = 0.$

Prob. ③ If $(R, +, \cdot)$ or a ring with unit element 1 such that $R \neq \{0\}$ then 0 & 1 are distinct.

→ ① $\exists$ an element $(-a)$ such that $(-a)+a = 0$

$\Rightarrow a+b = a+c.$

$\Rightarrow (-a)+a+b = (-a)+a+c$

$\Rightarrow b = c.$

②
$$a \cdot 0 = a \cdot (0+0)$$
$$= a0 + a0 \quad \text{(Distributive)}$$

$\therefore$ $\cancel{a \cdot 0} + 0 = \cancel{a0} + a \cdot 0$

$a \cdot 0 = 0$

$0 \cdot a = 0.$

→ A ring $(R, +, \cdot)$ is said to have divisors of zero if there exists two non-zero elements $a, b \in R$ such that $\boxed{a \cdot b = 0}$

Prob. Let $(R, +, \cdot)$ be a ring and $a, b, c \in R$ then show that

1) $-(a \cdot b) = (-a) \cdot b = a \cdot (-b)$
2) $(-a) \cdot (-b) = ab$
3) $a \cdot (b - c) = a \cdot b - a \cdot c$
4) $(b - c) \cdot a = b \cdot a - c \cdot a$
5) $(-1) \cdot (-a) = a$
6) $(-1) \cdot (-1) = 1$

→ 1) $-1 \cdot (a \cdot b) = (-1 \cdot a) \cdot b \; \cancel{= (a \cdot -1) \cdot b}$

$-(a \cdot b) = (a \cdot b) \cdot -1 = \cancel{a \cdot (-1 \cdot b)} \; a \cdot (b \cdot -1).$

2) $(-a) \cdot (-b) \; \cancel{= (-1 \cdot a) \cdot (-1 \cdot b)}$

$= (a \cdot -1) \cdot (-1 \cdot b)$

$= a \cdot (-1 \cdot -1) \cdot b$

$= a \cdot 1 \cdot b = a \cdot b$

3) $a \cdot (b - c) = \cancel{a \cdot b - a \cdot c}$ ~~8th p~~

$= a \cdot (b + (-1 \cdot c))$

$= a \cdot b + a \cdot (-1 \cdot c)$ (8th property)

$= a \cdot b - a \cdot c$

4) $(b - c) \cdot a = (b + (-1) \cdot c) \cdot a$

$= b \cdot a + (-1) \cdot c \cdot a$

$= b \cdot a - c \cdot a$

5) $(-1) \cdot (-a) = (-1) \cdot (-1 \cdot a) = (-1 \cdot -1) \cdot a$

$= a.$

Camlin Page
Date / /

23/1/18

Lecture-7

Lecture 1.3: Groups in science, art and mathematics
© Matthew Macauley
Clemson University, Math 4120, Modern Algebra

⇒ Subrings

Def^{-n} → Let $(R,+,\cdot)$ be a ring and $\phi \neq S \subseteq R$ then the ordered triple $(S,+,\cdot)$ is a subring of R if and only if $(S,+,\cdot)$ is a ring.

→ From the def^{-n} of subring it is clear that $(S,+,\cdot)$ is a subgroup of $(R,+)$ of ~~this~~ ring then $a,b \in S$.

i) $a+b \in S$ ⟩ $a-b \in S$.
if $b \in S \Rightarrow -b \in S$

ii) $a,b \in S \Rightarrow a\cdot b \in S$.

DIY If this two properties hold then it is sufficient to show that S is subring.

Prob. Let $(R,+,\cdot)$ be a ring and $\phi \neq S \subseteq R$ then $(S,+,\cdot)$ is a subring of $(R,+,\cdot)$ iff
i) $a-b \in S$ where $a,b \in S$
ii) $a\cdot b \in S$ where $a,b \in S$

→ We only need to show distributive property.

$$a\cdot(b+c) = \underbrace{\underset{\in S}{a\cdot b} + \underset{\in S}{a\cdot c}}_{\in S}$$

Let $(R', +, \circ)$ be a subring of the ring $(R, +, \circ)$

↳ 1) If the ring $(R, +, \circ)$ has a unit element 1 and if this element 1 belongs to R' then 1 is the unit element of the subring R' ($(R', +, \circ) \to$ unitary subring of $(R, +, \circ)$)

2) The ring $(R, +, \circ)$ has an identity element while $(R', +, \circ)$ has no unit element.

Eg :- $(\mathbb{Z}, +, \cdot) \to$ (Even Integers, $+, \cdot$)

3) Both the ring $(R, +, \circ)$ and the subring $(R', +, \circ)$ posses an unit element but the unit element of $(R, +, \circ)$ does not belong to $(R', +, \circ)$

4) The subring $(R', +, \circ)$ has an ~~identity~~ unit element but the ring $(R, +, \cdot)$ has no unit element.

Prob: Incase (3) and (4) show that the unit element of this subring must be a divisor of zero in the parent ~~set~~ ring.

Eg for 3): Let R be all 2×2 matrix have $(Z \times Z)$ and R' be 2×2 matrix where only $(1,1)$ have value rest all 0. $R = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ $R' = \begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix}$

→ Let $(S, +, \circ)$ be a subring of $(R, +, \circ)$

$1' \to (S, +, \circ)$ $\qquad 1' \in S$
$1 \to (R, +, \circ)$ $\qquad 1 \in R$

Then $\exists$ an element $a \in R$ s.t. $a1' \neq a$.

~~as~~ $(a \cdot 1')1' = a(1' \cdot 1') = a1'$

$\to (a1')1' = a1'$

$\rightarrow (a1'-a)1' = 0$

We know $1' \neq 0$

also if $a1' - a = 0$

$a1' = a$

$\therefore 1' = 1$ $\rightarrow$ against our assumption

$\therefore a1' - a \neq 0$

$\rightarrow$ $1'$ is the divisor of 0.

Def^{n} ① A commutative ring is said to be an integral domain if it has no zero divisor.

Eg :- $(Z, +, \cdot)$

Def^{n} ② A ring is said to be an divisor ring if it's non-zero elements forms a group under multiplication.

Def^{n} ③ A field is a commutative divisor ring.

$R^{+} = R - \{0\}$. $(R^{+}, +, \cdot)$

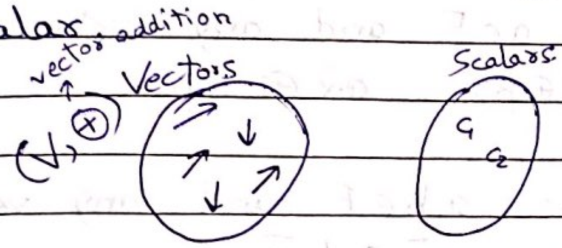
Visualizing Group Theory 1 (Video)

30/1/18

Vector Space
Lecture-8

1. Vector addition ⇒ vector/vector → vector
2. Dot product ⇒ vector/vector → scalar
3. Cross product ⇒ vector/vector → vector
4. Scalar Multiplication ⇒ scalar/vector → vector.

→ We can see there are 2 spaces, vector and scalar.

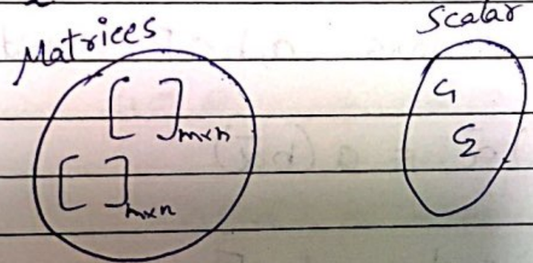


Scalar add^n/mult.

$(F, +, \cdot)$

Vector/Scalar operation (Dot product)

Example 2



There are intra-inter relation b/w this classes.

→ Let F be a given field whose elements are called scalars and V be a non-void set whose elements are labelled as vectors. The set V is a vector space or linear space over the field F if the following axioms are satisfied:

① For any two vectors $\bar{\alpha}, \bar{\beta} \in V$, $\bar{\alpha} \oplus \bar{\beta} \in V$.
② For any two vectors $\bar{\alpha}, \bar{\beta} \in V$, $\bar{\alpha} \oplus \bar{\beta} = \bar{\beta} \oplus \bar{\alpha}$
③ For any three vectors $\bar{\alpha}, \bar{\beta}, \bar{\gamma} \in V$,
$(\bar{\alpha} \oplus \bar{\beta}) \oplus \bar{\gamma} = \bar{\alpha} \oplus (\bar{\beta} \oplus \bar{\gamma})$.

④ $\exists$ unique vector $\bar{\emptyset} \in V$ s.t. $\bar{\alpha} \oplus \bar{\emptyset} = \bar{\emptyset} \oplus \bar{\alpha} = \bar{\alpha}$
$\forall \bar{\alpha} \in V$

⑤ For any vector $\bar{\alpha} \in V$, $\exists$ a unique vector $\bar{\alpha} \in V$ s.t. $\bar{\alpha} \oplus (-\bar{\alpha}) = \bar{\varnothing} = (-\bar{\alpha}) + (\bar{\alpha})$ — $(V, \oplus)$ Commutative group

⑥ For any element $a \in F$ and any vector $\bar{\alpha} \in V$, $a\bar{\alpha} \in V$ $\longrightarrow$ scalar multiplication.

⑦ For any element $a \in F$ and any vector $\bar{\beta}, \bar{\alpha} \in V$, $a(\bar{\alpha} \oplus \bar{\beta}) = a\bar{\alpha} \oplus a\bar{\beta}$

⑧ For any two scalars $a, b \in F$ and any vector $\bar{\alpha} \in V$, $(a+b)\bar{\alpha} = a\bar{\alpha} \oplus b\bar{\alpha}$.

⑨ For any two scalars $a, b \in F$ and any vector $\bar{\alpha} \in V$.

$$(a \cdot b)\bar{\alpha} = a(b\bar{\alpha})$$

⑩ For the unit scalar $1 \in F$ and any vector $\bar{\alpha} \in V$, $1\bar{\alpha} = \bar{\alpha}$.

$$(F, +) \begin{cases} \to 0 \text{ (Zero element)} \\ \to 1 \text{ (Identity element)} \end{cases}$$

→ Suppose field is R it is called Real vector space. $V(R)$

→ Suppose field is C is called Complex vector space. $V(I)$

Prob^o → If $V(F)$ is a vector space over field F and $\bar{\varnothing}, \bar{\alpha}, \bar{\beta} \in V$, $0, a, b \in F$ then show that

1) $a\bar{\varnothing} = \bar{\varnothing}$ 2) $0\bar{\alpha} = \bar{\varnothing}$ 3) $a(-\bar{\alpha}) = -(a\bar{\alpha})$

4) $(-a)\bar{\alpha} = -(a\bar{\alpha})$ 5) $a(\bar{\alpha} - \bar{\beta}) = a\bar{\alpha} - a\bar{\beta}$

6) $a\bar{\alpha} = \bar{\varnothing} \Rightarrow a = 0$ or $\bar{\alpha} = \bar{\varnothing}$.

Scanned by CamScanner

7) $a\bar{\alpha} = b\bar{\alpha} \not\Rightarrow a = b$.

→ 1) $a\bar{\phi} = a(\bar{\phi} \oplus \bar{\phi})$

$= a\bar{\phi} \oplus a\bar{\phi}$

$a\bar{\phi} \oplus \bar{\phi} = a\bar{\phi} \oplus a\bar{\phi}$

$a\bar{\phi} = \bar{\phi}$

2) $0\bar{\alpha} = (0+0)\bar{\alpha}$

$= 0\bar{\alpha} \oplus 0\bar{\alpha}$

$0\bar{\alpha} \oplus \bar{\phi} = 0\bar{\alpha} \oplus 0\bar{\alpha}$.

$0\bar{\alpha} = \bar{\phi}$.

3) $a(\bar{\alpha} \oplus -(\bar{\alpha})) = a\bar{\alpha} \oplus a(-\bar{\alpha})$.

$a\bar{\phi} = a\bar{\alpha} \oplus a(-\bar{\alpha})$.

$\bar{\phi} = a\bar{\alpha} \oplus a(-\bar{\alpha})$.

$a(-\bar{\alpha}) = -a\bar{\alpha}$.

($\because$ $a\bar{\alpha}$ is inverse of $a(-\bar{\alpha})$).

4) $[a + (-a)]\bar{\alpha} = a\bar{\alpha} \oplus (-a)\bar{\alpha}$.

$0\bar{\alpha} = a\bar{\alpha} \oplus (-a)\bar{\alpha}$

$\bar{\phi} = a\bar{\alpha} \oplus (-a)\bar{\alpha}$

$(-a)\bar{\alpha} = -a\bar{\alpha}$

5) $a(\bar{\alpha} - \bar{\beta}) = a(\bar{\alpha} \oplus (-\bar{\beta}))$

$= a\bar{\alpha} \oplus a(-\bar{\beta})$

$= a\bar{\alpha} - a\bar{\beta}$.

Prob. Find out whether $V = \left\{ \begin{bmatrix} x_1 & x_2 \\ x_3 & x_4 \end{bmatrix}, x_i \in R \right\}$ is a vector space over $(R, +)$?

2/2/18

Lecture - 9

Property: A non-empty subset W of V is a subspace of V iff

i) $\bar{\alpha}, \bar{\beta} \in W \Rightarrow \bar{\alpha} \oplus \bar{\beta} \in W$ (W is closed w.r.t vector addition)

ii) $\bar{\alpha} \in W, c \in F \Rightarrow c\bar{\alpha} \in W$ (closed w.r.t scalar multiplication)

→ F is a field, $1 \in F$

$\Rightarrow -1 \in F$

$\therefore -1\bar{\alpha} \in V$

$\Rightarrow -\bar{\alpha} \in V$ (by (ii)) —— V_5

(by (i)) $\bar{\alpha} \oplus -\bar{\alpha} = \bar{\phi} \in V$ V_4

→ $a\bar{\alpha} \oplus b\bar{\beta} \in W$ $\forall \bar{\alpha}, \bar{\beta} \in W$
$\forall a, b \in I$

If $a = b = 1$

→ $\bar{\alpha} \oplus \bar{\beta} \in W$.

If $a = 0$

$0\bar{\alpha} \oplus b\bar{\beta} \in W$

$\bar{\phi} \oplus b\bar{\beta} \in W$

$\therefore b\bar{\beta} \in W$.

Prob. 1) Let R^3 be the vector space of all 3-Tuples over the field of real numbers $(R, +, \cdot)$ with vector addition defined by

$(x_1, y_1, z_1) \oplus (x_2, y_2, z_2) = (x_1+x_2, y_1+y_2, z_1+z_2)$

Show that $W = \{(x_1, y_1, 0) . x_1, y_1 \in R\}$ is a subspace of R^3.

Prob 2) $V = \left\{ \begin{bmatrix} x_1 & x_2 \\ x_3 & x_4 \end{bmatrix}, x_i \in R \right\}$ is a vector space over the field of $(R, +, \cdot)$.

Show that $W = \left\{ \begin{bmatrix} x_1 & x_2 \\ x_2 & x_4 \end{bmatrix}, x_i \in R \right\}$ is a subspace of V.

1) Let $(x_1, y_1, 0)$, $(x_2, y_2, 0) \in W$

① $(x_1, y_1, 0) \oplus (x_2, y_2, 0) = (x_1 + x_2, y_1 + y_2, 0) \in W$

② $c \cdot (x_1, y_1, 0) = (cx_1, cy_1, 0) \quad c \in F$

$\in W$.

→ Hence proved W is subspace.

2) Let $\bar{\alpha} = \begin{bmatrix} x_1 & x_2 \\ x_2 & x_4 \end{bmatrix} \in W$ and $\bar{\beta} = \begin{bmatrix} y_1 & y_2 \\ y_2 & y_4 \end{bmatrix} \in W$

① $\begin{bmatrix} x_1 & x_2 \\ x_2 & x_4 \end{bmatrix} + \begin{bmatrix} y_1 & y_2 \\ y_2 & y_4 \end{bmatrix} = \begin{bmatrix} x_1+y_1 & x_2+y_2 \\ x_2+y_2 & x_4+y_4 \end{bmatrix}$

$\therefore \bar{\alpha} + \bar{\beta} \in W$

② $c \cdot \begin{bmatrix} x_1 & x_2 \\ x_2 & x_4 \end{bmatrix} = \begin{bmatrix} cx_1 & cx_2 \\ cx_2 & cx_4 \end{bmatrix} \in W$

$\therefore c\bar{\alpha} \in W$

→ Hence proved W is subspace.

Property: The intersection of any two subspace of a vector space $V(F)$ is also a subspace.

→ Let W_1, W_2 be two subspace of the vector space $V(F)$.

→ $W_1 \cap W_2$ is non-empty.

$\therefore \bar{\phi} \in W_1 \cap W_2$ } If $W_1 \cap W_2 = \{\bar{\phi}\}$ (trivial) but $W_1 \cap W_2 \neq \{\bar{\phi}\}$

→ To show: $a\bar{\alpha} \oplus b\bar{\beta} \in W_1 \cap W_2$.

$$\left.\begin{array}{l}\bar{\alpha} \in W_1 \cap W_2 \\ \bar{\beta} \in W_1 \cap W_2\end{array}\right\} a, b \in F.$$

$$\left.\begin{array}{l}\bar{\alpha} \in W_1 \\ \bar{\beta} \in W_1\end{array}\right\} \Rightarrow a\bar{\alpha} \oplus b\bar{\beta} \in W_1 \quad (\because W_1 \text{ is subspace of } V)$$

$$\left.\begin{array}{l}\bar{\alpha} \in W_2 \\ \bar{\beta} \in W_2\end{array}\right\} \Rightarrow a\bar{\alpha} \oplus b\bar{\beta} \in W_2 \quad (\because W_2 \text{ is subspace of } V).$$

$\therefore a\bar{\alpha} \oplus b\bar{\beta} \in W_1 \cap W_2$.

Prob. If $W_1 = \{(a,0,0), a \in F\}$
$W_2 = \{(0,b,0), b \in F\}$

Is $W_1 \cup W_2$ is a subspace?

→ $\bar{\alpha} \in W_1 \Rightarrow \bar{\alpha} \in W_1 \cup W_2$
$\bar{\alpha} = (a,0,0)$ —— (i)

$\bar{\beta} \in W_2 \Rightarrow \bar{\beta} \in W_1 \cup W_2$.

$\bar{\beta} = (0, b, 0)$ —— (ii).

$\rightarrow x\bar{\alpha} \oplus y\bar{\beta} = (xa, yb, 0) \notin W_1 \cup W_2$.

Property The union of two subspaces is a subspace iff one is contained in other.

$\Rightarrow$ Proof: Let $W_1, W_2 \in V(F)$

$\rightarrow$ If $W_1 \subset W_2$, $W_1 \cup W_2 = W_2$
$W_2 \subset W_1$, $W_1 \cup W_2 = W_1$ $\Big\} \Rightarrow W_1 \cup W_2$ is a subspace since $W_1, W_2 \rightarrow$ subspace.

$\rightarrow$ Let us assume $W_1 \cup W_2$ is subspace.

$\rightarrow W_1 \cup W_2 \Rightarrow$ subspace of V

$W_1 \not\subset W_2 \rightarrow \exists$ element $\alpha \in W_2$, $\alpha \notin W_1$

$W_2 \not\subset W_1 \rightarrow \exists$ element $\beta \in W_1$, $\beta \notin W_2$.

$\bar{\alpha} \in W_2 \Rightarrow \bar{\alpha} \in W_1 \cup W_2$

$\bar{\beta} \in W_1 \Rightarrow \bar{\beta} \in W_1 \cup W_2$.

$\bar{\alpha} \oplus \bar{\beta} \in W_1 \cup W_2$

$\bar{\alpha} \oplus \bar{\beta} \in W_1$ or $\bar{\alpha} \oplus \bar{\beta} \in W_2$

$\rightarrow$ If $\bar{\alpha} \oplus \bar{\beta} \in W_1$

$\bar{\alpha} \oplus \bar{\beta} \in W_1$

$\Rightarrow \bar{\alpha} \oplus \bar{\beta} \oplus (-\bar{\beta}) \in W_1$ $\quad (\because \bar{\beta} \in W_1 \Rightarrow -\bar{\beta} \in W_1)$

$\Rightarrow \bar{\alpha} \oplus (\bar{\beta} \oplus -\bar{\beta}) \in W_1$

$\Rightarrow \bar{\alpha} \oplus \bar{\emptyset} \in W_1$.

$\Rightarrow \bar{\alpha} \in W_1$ (Contradiction)

Camlin Page
Date / /

→ If W is a subspace of a vector space V over the field F, then for all $a_1, a_2, \dots, a_n \in F$ and for all

$$\bar{\alpha}_1, \bar{\alpha}_2, \dots, \alpha_n \in W$$

$$a\bar{\alpha}_1 \oplus a_2\bar{\alpha}_2 \oplus \cdots \oplus a_n\bar{\alpha}_n \in W.$$

Q.

→ Linear Span : If V(F) is a vector space and $\bar{\alpha}_1, \bar{\alpha}_2, \dots, \bar{\alpha}_k \in V$ and $c_1, c_2, \dots, c_k \in F$ then $c_1\bar{\alpha}_1 + \cdots + c_k\bar{\alpha}_k$ is also called the linear combination of vectors, $\bar{\alpha}_1, \bar{\alpha}_2, \dots, \bar{\alpha}_k$.

$$\bar{\alpha} = \sum_{i=1}^{k} c_i\bar{\alpha}_i \in V.$$

Prob. $\bar{\alpha} = (8, 17, 36)$ is a linear combination of vectors $\bar{\alpha}_1 = (1, 0, 5)$, $\bar{\alpha}_2 = (0, 3, 4)$
$\bar{\alpha}_3 = (1, 1, 1)$.

→ $c_1 = 3$, $c_2 = 4$, $c_3 = 5$.