# Discrete Structures (MA5.101)

Assignment Set -3

Name:- MANOHAR NAGA
Roll.NO:- 2021101128
Section: B

## Group Theory

1. Show that a cancellative semigroup can contain atmost one idempotent and if it exists it is an identity-element.

Answer:

Let $S$ be cancellative semigroup then,

① $\Rightarrow$ if $a.b = a.c \quad \forall a,b,c \in S$

$\Rightarrow \boxed{b=c}$

② $\Rightarrow$ if $b.a = c.a$

$\boxed{b=c}$

RTP: Cancellative semigroup can contain atmost one idempotent & if it exists it is an identity element.

First we prove that idempotent is identity element. Let $x \in S$ be the identity.

So, if $x.x = x$

$\Rightarrow e.x.x = e.x$

(since) $b.a = c.a \Rightarrow b=c$

$\Rightarrow e.x = e \quad (\because e \text{ is identity})$

$\Rightarrow \boxed{x=e}$

if $\exists$ idempotent 'x' then 'x' is identity element.

Now if suppose there are 2 idempotent element e, f $\Rightarrow$ e, f are identities

$\Rightarrow$ for some $a \in S$

we have

(i) $a.e = e.a = a$

(ii) $a.f = f.a = a$

$\Rightarrow a.e = a.f = a$

By cancellativity of 'S' ($\because a.b = a.c \Rightarrow b = c$)

$\Rightarrow \boxed{e = f}$

$\therefore$ 'S' can contain atmost one idempotent, if there are more than one they must be equal as $(e = f)$

$\therefore$ cancellative semigroup can contain atmost one idempotent and if it exists it is an identity element.

Hence, proved

(2) Let H be a subgroup of a Group G, and let $N = \bigcap_{x \in G} x.H.x^{-1}$. prove that N is a Normal subgroup of Group G

Answer:

Given a Group G with subgroup H

and $N = \bigcap_{x \in G} x.H.x^{-1} \quad \forall x \in G$

RTP: 'N' is a Normal subgroup of G

(i) N is a subgroup

(ii) N is a Normal subgroup

Now (i) let $x.H.x^{-1}$ be structure

then $x.H.x^{-1} \in N$ (by defn)

W.K.T $x.h.x^{-1} \in x.H.x^{-1}$

$\Rightarrow (x^{-1})^{-1}.h(x^{-1}) \in x.H.x^{-1}$ ($\because x \in G$, H is a subgroup)

Now let $x^{-1} = y$

$\Rightarrow y^{-1}.h.y \in x.H.x^{-1}$

Thus all these structures are subsets of N. that is $x.H.x^{-1} \in N$

Now RTP: intersection of $\bigcap_{x \in G} x.H.x^{-1}$ is a Normal subgroup

Let $H, K \in G$ be 2 normal subgroups

$\Rightarrow xH = Hx$

and

$xK = Kx$

e ⇒ identity element in $G/H/K$

W.K.T

$e \in H$, and $e \in K$

$\Rightarrow e \in H \cap K$

and $H \cap K \subseteq G$ — forms a subgroup

$\Rightarrow a.\vec{b} \in H \cap K$ $\forall a, b \in H \cap K$

Now let $\in G$ and

$y \in H \cap K$

$\Rightarrow \vec{x}.y.x \in H$ also $\vec{x}.y.x \in K$

$\Rightarrow \vec{x}.y.x \in H \cap K$

$\Rightarrow \vec{x}.y.x \subseteq H \cap K$ $\quad Y = H \cap K$

$\Rightarrow$ $H \cap K$ is a normal subgroup.

$\therefore$ $N = \bigcap_{x \in G} xH\vec{x}$ is also a normal subgroup under $G$

Hence, proved.

3. Prove that the inverse $\theta^{-1}$ of an isomorphism $\theta: S \to T$ of semigroups (monoids) S and T is also an isomorphism of semigroups (monoids) S and T.

Answer: Given, a mapping $\theta: S \to T$ is an isomorphism of semigroups (monoids)

$\Rightarrow$ Let $\langle S, \cdot \rangle$ and $\langle T, * \rangle$ be two structures (semigroups / Monoids)

Then $\theta(s_1 \cdot s_2) = \theta(s_1) * \theta(s_2)$ $\forall s_1, s_2 \in S$

isomorphism $\Rightarrow$ $\theta: S \to T$ is a Bijection

RTP: $\bar{\theta}: T \to S$ is also an isomorphism

(i) $\bar{\theta}$ is a homomorphism

(ii) $\bar{\theta}$ is Bijective

(i) As $\theta: S \to T$ is bijective, let $\theta(s_1) = t_1$, $\theta(s_2) = t_2$

$\forall s_1, s_2 \in S$ & $\forall t_1, t_2 \in T$ $\Rightarrow$ $s_1 = \bar{\theta}(t_1)$ — (1)

$s_2 = \bar{\theta}(t_2)$ — (2)

Now $\theta(s_1 \cdot s_2) = \theta(s_1) * \theta(s_2)$

$\Rightarrow \theta(s_1 \cdot s_2) = t_1 * t_2$

Now apply $\bar{\theta}(\,)$ on b/s

$\Rightarrow \bar{\theta}(\theta(s_1 \cdot s_2)) = \bar{\theta}(t_1 * t_2)$ ($\because \bar{f}(f(x)) = x$)

$\Rightarrow s_1 \cdot s_2 = \bar{\theta}(t_1 * t_2)$

$\Rightarrow \bar{\theta}(t_1 * t_2) = s_1 \cdot s_2$

$\Rightarrow \boxed{\bar{\theta}(t_1 * t_2) = \bar{\theta}^{-1}(t_1) \cdot \bar{\theta}^{-1}(t_2)}$ (from ①, ②)

Hence, $\bar{\theta}: T \to S$ for $\langle T, * \rangle$ & $\langle S, \cdot \rangle$

$\boxed{\bar{\theta}(t_1 * t_2) = \bar{\theta}(t_1) \cdot \bar{\theta}(t_2)} \quad \forall t_1, t_2 \in T$

Thus $\bar{\theta}: T \to S$ is a homomorphism

(ii) $\bar{\theta}: T \to S$ is a bijection

(Given) $\theta: S \to T$ is a bijection let $s_1, s_2 \in S$
$t_1, t_2 \in T$

$\Rightarrow \theta(s_1) = t_1 \Rightarrow \bar{\theta}(t_1) = s_1$ - ①

$\theta(s_2) = t_2 \Rightarrow \bar{\theta}(t_2) = s_2$ - ②

Injection $\Rightarrow s_1 = s_2 \Leftrightarrow \theta(s_1) = \theta(s_2)$

Injection for $\bar{\theta} \Rightarrow$ let $t_1 = t_2$

$\Rightarrow \theta(s_1) = \theta(s_2)$

$\Leftrightarrow s_1 = s_2$ (∵ ①, ②)

$\Leftrightarrow \bar{\theta}(t_1) = \bar{\theta}^{-1}(t_2)$

Hence $\boxed{t_1 = t_2 \Leftrightarrow \bar{\theta}^{-1}(t_1) = \bar{\theta}^{-1}(t_2)}$

$\bar{\theta}$ is an injection

Surjection: Range of $\theta = T$ (∵ $\theta$ is onto)

$\Rightarrow \forall t \in T \quad \exists s \in S$

s/t $\theta(s) = t$

$\Rightarrow s = \bar{\theta}^{-1}(t) \Rightarrow \bar{\theta}^{-1}(t) = s$

$\Rightarrow \forall s \in S \quad \exists t \in T$

s/t $\bar{\theta}(t) = s$

$\boxed{\therefore \bar{\theta}^{-1} \text{ is a surjection}}$

(10) Find all
degree 2
Sol Note
Irreducibl
$= \begin{bmatrix} x^2 + \\ 2x \end{bmatrix}$
Solving
form $\Rightarrow$
Now for
Then,
$a_2$
1
1

(3) Continued---

Hence from (i), (ii)

$\bar{\theta} : T \to S$ is both bijective and homomorphism

Hence, $\bar{\theta}' : T \to S$ is an isomorphism

where the structures, S, T can semigroups / monoids

Hence, proved.

④ Let $f: G \to G'$ be a group epimorphism and let H be the normal subgroup that be the kernel of the epimorphism. Then, prove that $G'$ is isomorphic to $G/H$.

Solution:-

Given, $f: G \to G'$ is a group epimorphism and H is normal subgroup also the "kernel" of the epimorphism

RTP: $G'$ is isomorphic to $G/H$

By the universal property of a quotient, there is a natural homomorphism

$\bar{f}: G/H \to G'$

suppose that $x$ is in the kernel of $\bar{f}$. Then $x$ has the form $gH$ and by the definition of $\bar{f}$, $f(x) = \varphi(g)$.

Thus $g$ is in the kernel of $\varphi$ and so $g \in H$. In this case $(x = H)$, the identity of $G/H$.

So the kernel of $\bar{f}$ is trivial and $\bar{f}$ is injective.

Hence $\bar{f}$ is an isomorphism

(5) Prove that a cyclic group is necessarily abelian. But the converse is NOT True

Answer:

Let $G$ be a cyclic group

$\Rightarrow G = \{g^n \mid n \in \text{positive integers}\}$

Now

(1) RTPt $G$ is abelian group i.e.,

$a.b = b.a \quad \forall a, b \in G$

Let $a = g^{k_1}$

$b = g^{k_2}$ as $G$ is cyclic

$\Rightarrow a.b = g^{k_1} \cdot g^{k_2} = g^{(k_1+k_2)}$

$= g^{k_2+k_1}$

$= g^{k_2} \cdot g^{k_1}$

$\boxed{a.b = b.a}$

Hence, $G$ is abelian

(2) RTP: If $G$ is abelian it need not be cyclic

we can prove this using a Counter Example

Let $G = Z_m \times Z_n$ where $m, n \in$ +ve Integers $\setminus \{0\}$

$\{Z_k =$ cyclic group of order $k\}$

As a direct product of two cyclic groups $Z_m, Z_n$

$\Rightarrow$) The Group $G$ is abelian

Now we find the order of $G$

Let $(x,y) \in G$ $\quad x = g_m^k \in Z_m$ $\quad k \in +ve$ Integers

$y = g_n^k \in Z_n$

Now if identity in $G = e$

then order of $G$ is $k$ if $(g_m^k, g_n^k) = (e,e)$

as the order of $g_m(Z_m) = m$

the order of $g_n(Z_n) = n$

the order of $G$ = least common multiple of $(m,n)$

$= LCM(m,n)$

W.K.T: $\boxed{LCM(m,n) > \max(m,n)}$.

Hence no element in $G$ has order $= LCM(m,n)$

$\therefore G$ is NOT cyclic but it is abelian

Hence, proved.

⑥ Given the following parity-check matrix, H:

$$H = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 \end{pmatrix}$$

(i) Encode the message $\langle 1\,1\,1\,0 \rangle$ using H.

(ii) Decode the recieved tuple $\langle 1\,1\,0\,0\,0\,1\,1 \rangle$ assuming that error, if any, is a single error.

Sol: Given parity-check matrix H

(i)

$$H = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 \end{pmatrix}$$
$$x_1\ x_2\ x_3\ x_4\ x_5\ x_6\ x_7$$

message $= \langle 1\,1\,1\,0 \rangle$

$= \langle x_3\ x_5\ x_6\ x_7 \rangle$

Let encoded message $= \langle y_1\ y_2\ y_3\ y_4\ y_5\ y_6\ y_7 \rangle$

Now copy the values as:

$y_3 = x_3 = 1$

$y_5 = x_5 = 1$

$y_6 = x_6 = 1$

$y_7 = x_7 = 0$

$y_1 = y_3 \cdot h_{13} \oplus y_5 h_{15} \oplus y_6 h_{16} \oplus y_7 h_{17}$

$= 1.1 \oplus 1.1 \oplus 1.1 \oplus 0.0$

$y_1 = 1$

$y_2 \oplus y_3 \oplus y_6 \oplus y_7 = 0 \Rightarrow y_2 = 0$

$y_3 \oplus y_4 \oplus y_5 \oplus y_7 = 0 \Rightarrow y_4 = 0$

$\therefore$ The Encoded message is $\langle 1010110 \rangle$

(iii) The recieved tuple is $x' = \langle 1100011 \rangle$

The error syndrome 3-tuple is

$$\text{syndrome} = x' H^t = \langle 1100011 \rangle \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 1 & 1 \\ 0 & 0 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix}$$

$= \langle 1 \oplus 1, 1 \oplus 0 \oplus 1 \oplus 1, 0 \oplus 0 \oplus 1 \rangle$

$= \langle 0, 1, 1 \rangle$

$\therefore$ There is an error in ~~position~~ tuple $i = (0,1,1) = x_7$ in $H$

in the recieved tuple $x'$.

Hence, the decoded tuple is obtained by flipping $x_7$

$\Rightarrow$ The decoded Message $= \langle 1100010 \rangle$

(7) Let the Null space of an $r \times n$ canonical parity check matrix be a group code that satisfies the following conditions;

* for each coordinate there is some code word with a 1 in that position
* for each pair of coordinates there is some code word that has different values in those two positions.

(a) prove that the set of code words with a 0 in the $i$th coordinate is a subgroup of that code.

Solution:-

Let $C_{0i}$ : the set of code with a '0' in the $i^{th}$ coordinate

R.T.P:- $C_{0i}$ is a subgroup i.e.,

R.T.P:- $\forall x, y \in C_{0i}$, where $\bar{y}$ is the inverse of $y$ in $\langle C_{0i}, \oplus \rangle$

we note that '0' is the identity in $\langle C_{0i}, \oplus \rangle$ and so $y \oplus y = 0 \quad \forall y \in C_{0i}$

$\Rightarrow$ Each element is its own inverse in $\langle C_{0i}, \oplus \rangle$

∴ R.T.P $x \oplus y \in C_{0i}$

Since $x, y \in C_{0i}$, so

$x = \langle x_1, x_2, \ldots, x_i \ldots x_n \rangle$ with $x_i = 0$

and $y = \langle y_1, y_2, \ldots, y_i \ldots y_n \rangle$ with $y_i = 0$

$$\therefore x \oplus y = \langle x_1 \oplus y_1, x_2 \oplus y_2 \ldots x_i \oplus y_i \ldots x_n \oplus y_n \rangle$$
$$= \langle x_1 \oplus y_1, x_2 \oplus y_2, \ldots, 0, \ldots x_n \oplus y_n \rangle$$
$$\in C_{0i}$$

(b) prove that the average weight of a code word is $\frac{n}{2}$.

Solution:-

Consider all the columns, $C_i$ of H which are n-tuple code words:

$$C_1 = \langle c_{11}, c_{12}, \ldots, c_{1i}, \ldots, c_{1n} \rangle$$
$$C_2 = \langle c_{21}, c_{22}, \ldots, c_{2i}, \ldots c_{2n} \rangle$$
$$\vdots$$
$$C_n = \langle c_{r1}, c_{r2} \ldots, c_{ri}, \ldots c_{rn} \rangle$$

Since H is an $r \times n$ parity-check matrix

If we perform columnwise Addition (Modulo-2, $\oplus$)

then we get the set

$C_i$ : Set of code words with a 1 in the $i^{th}$ coordinate

Now,

$C_{1i} = C - C_{0i}$, because

$x, y \in C_{1i} \Rightarrow x \oplus y^{-1} \in C_{0i}$. [by coset relation $g_1 R g_2$ iff $g_1^{-1} \cdot g_2 \in H$]

$\Rightarrow x \oplus y \in C_{0i}$

$\therefore \|C_{0i}\| = \|C_{1i}\| = \frac{\|C\|}{2} = \frac{k}{2}$ where

$k = [C : C_{1i}]$ is the number of cosets $C_{1i}$ relative to C.

Total weight of the code $C = \sum_{i=1}^{n} \|C_i\|$

$\therefore$ Average weight of a code word

$$= \frac{\sum_{i=1}^{n} \|C_i\|}{\|C\|} = \frac{\sum_{i=1}^{n} (k/2)}{k} = \frac{k/2}{k} \cdot \sum_{i=1}^{n} 1$$

$$= \frac{1}{2} \cdot (1+1+\cdots+1+1) \quad (n \text{ times})$$

$$= \frac{n}{2}.$$

$=$

(8) The characteristic of any field is the order of 1 in the additive group of the field. In other words, the characteristic of a field F is the order of 1 in $\langle F, + \rangle$. prove that characteristic of any field is either prime or infinite

Solution:

Given, a field $F \Rightarrow \langle F, + \rangle$

RTP: The characteristic of F is prime or infinite

Let 'k' be the characteristic of field 'F' and let us say $k \notin$ prime numbers

(i) characteristic of F is prime

ie, $k \in$ composite numbers

$\Rightarrow \exists\ a, b$ s/t, $c = a + b$ — (1)

where $1 \leq a, b \leq c$

Now let $x \in F$ & $x \neq 0$

$\Rightarrow x + x = 2x \in F$ ($\because$ F is closed under +)

Now as 'k' is characteristic of F

$\Rightarrow k.(2x) = 0$

$\Rightarrow (a+b).2x = 0$

$\Rightarrow 2ax + 2bx = 0$

Now as $a, b \geq 1$

$x \neq 0$

$2ax > 0, \quad 2bx > 0$

$\Rightarrow 2ax + 2bx = 0$

but $2ax \neq 0$ and $2bx \neq 0$

This is a contradiction that F has no zero divisors

~~Note~~ Example:

$(Z_p, +_p, \cdot_p)$ is GF(p) $p \in$ prime

then $Z_p = \{0, \ldots, p-1\}$

as 'p' is prime no other number less than 'p' divides it.

i.e., $Z_p \pmod p \neq 0$

$\therefore 1+1+1 \ldots +1$ (p times) $\pmod p = 0$

$\therefore Z_p$ has characteristic = $p \in$ Prime

s/t $\boxed{p.1 = 0}$ $(p \pmod p = 0)$

(ii) characteristic of F can infinite

Let characteristic of F is of additive order of 1 i.e., the small integer $n > 1$

s/t $n.1 = 1+1+\ldots+1+1$ (n times) $= 0$

If there is no such integer the field is said to be zero.

It follows the map $z \to c$ where 'z' is integers and 'c' is characteristic of F.

$z \to c$ is given by $n \to n.1$ is an injection

So, $|z| \leq |c|$

In particular 'c' is infinite

Hence, we can say that characteristic of any field is either prime or Infinite.

Hence, proved.

(9) In the algebra of polynomials
$P(x)$, where $P(x)$ is irreducible polynomial of degree n over a field K.
Prove that the polynomials form a field with respect to polynomial addition and multiplication iff $P(x)$ is irreducible

Solution

Given a polynomial $P(x)$

RTP: $\langle Z_{P(x)}, +_{P(x)}, \cdot_{P(x)} \rangle$ forms a field iff $P(x)$ is irreducible.

($\Rightarrow$) $\langle Z_{P(x)}, +_{P(x)}, \cdot_{P(x)} \rangle$ is a field

RTP: $P(x)$ is irreducible.

let us say $P(x)$ is reducible

$\Rightarrow P(x) = P_1(x) \cdot P_2(x)$ $\quad 0 < P_1(x), P_2(x) < P(x)$ degree of diff

$\because Z_{P(x)}$ is a field $\exists h(x)$ s/t

$P_1^{-1}(x) = h^{*}(x)$

$\Rightarrow$ Inverse doesn't exist because $P(x)$ and $P_1(x)$ are not co-primes

This is a contradiction

$\therefore$ If $Z_{P(x)}$ is a Field, then $P(x)$ is irreducible.

($\Leftarrow$)

RTPt: If $p(x)$ is irreducible, then

$\langle Z_{p(x)}, +_{p(x)}, \cdot_{p(x)} \rangle$ forms a Field

for any polynomial $p(x)$

$\langle Z_{p(x)}, +_{p(x)}, \cdot_{p(x)} \rangle$ forms an Integral Domain.

But if $p(x)$ is irreducible then for some polynomial $g(x)$ $\exists [g(x)]^{-1} \in Z_{p(x)}$ as $\boxed{\gcd(p(x), g(x)) = 1}$

($\because$ $p(x)$ = irreducible)

If $p(x)$ is irreducible then $Z_{p(x)}$ forms a field

Hence, polynomials form a Field w.r.t Polynomial addition and multiplication iff $p(x)$ is irreducible

Hence, proved. $\Rightarrow$

(10) Find all the irreducible polynomials of degree 2 over the Galois Field GF(3).

Sol Note that '3' is prime Number.

Irreducible polynomial in GF(3) of degree 2

$$= \begin{bmatrix} x^2+1, & x^2+x+2, & x^2+2x+2 \\ 2x^2+x+1, & 2x^2+2x+1, & 2x^2+2 \end{bmatrix} - 5$$

Solving :- polynomials in GF(3) are of the form $\Rightarrow [a_2x^2 + a_1x + a_0]$ $a_0, a_1, a_2 \in Z_p = Z_3 = \{0,1,2\}$

Now for degree = 2

$\Rightarrow a_2 \in \{1,2\}$

Then,

| $a_2$ | $a_1$ | $a_0$ | $f(x) = a_2x^2 + a_1x + a_0$ |
|---|---|---|---|
| 1 | 0 | 0 | $x^2$ |
| 1 | 0 | 1 | $x^2+1$ |
| 1 | 0 | 2 | $x^2+2$ |
| 1 | 1 | 0 | $x^2+x$ |
| 1 | 1 | 1 | $x^2+x+1$ |
| 1 | 1 | 2 | $x^2+x+2$ |
| 1 | 2 | 0 | $x^2+2x$ |
| 1 | 2 | 1 | $x^2+2x+1$ |
| 1 | 2 | 2 | $x^2+2x+2$ |
| 2 | 0 | 0 | $2x^2$ |
| 2 | 0 | 1 | $2x^2+1$ |
| 2 | 0 | 2 | $2x^2+2$ |

| $a_2$ | $a_1$ | $a_0$ | $f(x) = a_2x^2 + a_1x + a_0$ |
|---|---|---|---|
| 2 | 1 | 0 | $2x^2 + x$ |
| 2 | 1 | 1 | $2x^2 + x + 1$ |
| 2 | 1 | 2 | $2x^2 + x + 2$ |
| 2 | 2 | 0 | $2x^2 + 2x$ |
| 2 | 2 | 1 | $2x^2 + 2x + 1$ |
| 2 | 2 | 2 | $2x^2 + 2x + 2$ |

Now, the polynomials i

$x^2, x^2+x, x^2+2x, 2x^2, 2x^2+x, 2x^2+2x$

are NOT irreducible as they can be expressed as $f(x) = x.g(x)$

Now a polynomial is irreducible in GF(3)

if $f(a) \neq 0$ for Range $= \{0, 1, 2\}$

[ if $f(a) = 0$

$\Rightarrow f(x) = g(x).(x-a)$

$\Rightarrow$ reducible ]

$\therefore$ we check for the remaining polynomials

if $f(a) = 0$

$x^2+1$ is irreducible

$f(0) = 1$

$f(1) = 1+1 = 2$

$f(2) = 4+1 = 5$

$x^2+2$

$f(1) = 1^2+2 = 3 \pmod 3 = 0$ - NOT irreducible

$x^2+x+1 = f(x)$

$\Rightarrow f(1) = 1+1+1 = 3 \pmod 3 = 0$ – Reducible

$f(x) = \boxed{x^2+x+2}$ Irreducible

$\Rightarrow f(0) = 0+0+2 = 2$

$f(1) = 1+1+2 = 4 \pmod 3 = 1$

$f(2) = 4+2+2 = 2$

$f(x) = x^2+2x+1$

$\Rightarrow f(1) = 1+2+1 = 4$

$f(2) = 4+4+1 = 9 \pmod 3 = 0$ – Reducible

$f(x) = \boxed{x^2+2x+2}$ – Irreducible

$\Rightarrow f(0) = 2$

$f(1) = 5 \pmod 3 = 2$

$f(2) = 4+4+2 = 2$

$f(x) = 2x^2+1$

$\Rightarrow f(1) = 3 \pmod 3 = 0$ – Reducible

$f(x) = \boxed{2x^2+2}$ – Reducible

$\Rightarrow f(0) = 2$

$f(1) = 1$ ~~but~~

$f(2) = 2$

$f(x) = 2(x^2+1) = k.p(x)$ – $p(x)$ – Irreducible

~~2 is not trivial (1, f(x))~~

$\Rightarrow k.p(x)$ – Irreducible

~~but~~

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

$\Rightarrow f(1) = 3 \pmod 3 = 0$ – Reducible

$f(x) = \boxed{2x^2+x+1}$ – Irreducible

$\Rightarrow f(0) = 1$

$f(1) = 1$

$f(2) = 8+2+1 = 2$

and for Irreducible $f(x) = 2x^2+x+2$, $f(2) = 0$ – Reducible

$f(x) = \boxed{2x^2+2x+1}$, $f(0) = 1$, $f(1) = 2$, $f(2) = 1$

$f(x) = 2x^2+2x+2 = 2(x^2+x+1)$ – Reducible

$2 \nmid (1, f(x))$

(11) Using the Euclidean gcd to obtain integers $x$ and $y$ satisfying.

$$\gcd(1769, 2378) = 1769x + 2378y$$

Sol $\gcd(1769, 2378) = 1769x + 2378y$

($*$ = Multiplication)

Find $x, y$?

We have

$$2378 = 1 * 1769 + 609$$
$$1769 = 2 * 609 + 551$$
$$609 = 1 * 551 + 58$$
$$558 = 9 * 58 + 29$$
$$58 = 2 * \boxed{29} + 0$$

$\therefore \boxed{\gcd(1769, 2378) = 29}$

Now by Backtracking the values for

$$29 = 551 - 9 \times 58$$
$$= 551 - 9 \times (609 - 551)$$
$$= 10 * 551 - 9 * 609$$
$$= 10 * (1769 - 2 * 609) - 9 * 609$$
$$= 10 * 1769 - 29 * 609$$
$$= 10 * 1769 - 29 * (2378 - 1769)$$
$$= 39 * 1769 + (-29) * 2378$$
$$= 1769x + 2378y$$

$\therefore \boxed{x = 39, \quad y = -29}$

(12) Using the extended Euclidean gcd algorithm, find the multiplicative Inverse of 1234 in GF(4321).

Sol Given, number = 1234 in GF(4321)

Find: Multiplicative Inverse of 1234?

Here, $m = 4321$ and $b = 1234$

we need to find $b^{-1} \pmod m$ i.e; $1234^{-1} \pmod{4321}$

Applying the extended Euclid's gcd algorithm, we have the following Table with r

begin:

$$Q = \left\lfloor \frac{A_3}{B_3} \right\rfloor$$

Set $(T_1, T_2, T_3) \rightarrow (A_1 - QB_1, A_2 - QB_2, A_3 - QB_3)$

Set $(A_1, A_2, A_3) \rightarrow (B_1, B_2, B_3)$

Set $(B_1, B_2, B_3) \rightarrow (T_1, T_2, T_3)$

go to begin!

| Q | $A_1$ | $A_2$ | $A_3$ | $B_1$ | $B_2$ | $B_3$ | $T_1$ | $T_2$ | $T_3$ |
|---|---|---|---|---|---|---|---|---|---|
| – | 1 | 0 | 4321 | 0 | 1 | 1234 | – | – | – |
| 3 | 0 | 1 | 1234 | 1 | -3 | 619 | 1 | -3 | 619 |
| 1 | 1 | -3 | 619 | -1 | 4 | 615 | -1 | 4 | 615 |
| 1 | -1 | 4 | 615 | 2 | -7 | 4 | 2 | -7 | 4 |
| 153 | 2 | -7 | 4 | -307 | 1075 | 3 | -307 | 1075 | 3 |
| 1 | -307 | 1075 | 3 | 309 | -1082 | 1 | 309 | -1082 | 1 |

Since $B_3 = 1$, so $\gcd(m, b) = B_3 = 1$ ∴ multiplicative Inverse will be

$b^{-1} \pmod m = B_2 = -1082$, but $-1082$ is -ve

$\Rightarrow b^{-1} \pmod m = (m - 1082) \pmod m$

$b^{-1} = \boxed{3239} \pmod m$

verification: $b \cdot b^{-1} \pmod m = 1234 \cdot (3239) \pmod{4321}$

$= 1$

(13) Determine the gcd of the following pair of polynomials over GF(101):

$x^5 + 88x^4 + 73x^3 + 83x^2 + 51x + 67$

$x^3 + 97x^2 + 40x + 38$

Sol Given $A = BQ + R$

$A = x^5 + 88x^4 + 73x^3 + 83x^2 + 51x + 67$ in GF(101)

$B = x^3 + 97x^2 + 40x + 38$

$x^2 + 92x + 98$

$x^3 + 97x^2 + 40x + 38 \overline{)\ x^5 + 88x^4 + 73x^3 + 83x^2 + 51x + 67}$

$x^5 \pm 97x^4 \pm 40x^3 \pm 38x^2$

$92x^4 + 33x^3 + 45x^2 + 51x$

$\underline{92x^4 \pm 36x^3 \pm 44x^2 \pm 62x}$

$98x^3 + x^2 + 90x + 67$

$\underline{98x^3 \pm 12x^2 \pm 82x \pm 88}$

$90x^2 + 8x + 80$

$\Rightarrow R = 90x^2 + 8x + 80$

$Q = x^2 + 92x + 98$

$R \neq 0$

$\Rightarrow B = Q'R + R_1$

$55x + 22$

$90x^2 + 8x + 80 \overline{)\ x^3 + 97x^2 + 40x + 38}$

$x^3 \pm 36x^2 \pm 57x$

$61x^2 + 84x + 38$

$\underline{61x^2 \pm 75x \pm 43}$

$9x + 96$

$\Rightarrow Q' = 55x + 22$

$R_1 = 9x + 96$

$R_1 \neq 0$

$\therefore R = Q_1' R_1 + R_2$

$$
\begin{array}{r|l}
 & 10x + 85 \\
\hline
9x + 96 & 90x^2 + 8x + 80 \\
 & \underline{-90x^2 \pm 51x} \\
 & \quad 58x + 80 \\
 & \quad \underline{58x \pm 80} \\
 & \quad\quad 0
\end{array}
$$

$\Rightarrow R_2 = 0$

$\therefore R_1 = \gcd(A, B) = \gcd(B, R) = \gcd(R_1, R_1)$

$\therefore$ GCD of Given two polynomials

$= \boxed{9x + 96}$ in GF(101)

[In GF(101) if $x < 0$ then $(101 + x \pmod{101})$ is to be taken as $x \pmod{101}$]

GCD $= x + 78$ also

as $9x + 96$ and $x + 78$ are

associates of each other

(14) Compute the product of the following two bytes (in hexadecimal) in $GF(2^8)$ under $m(x) = x^8+x^4+x^3+x+1$ as an irreducible polynomial

$\{a9\}.\{9e\}$

Sol: Given, $m(x) = x^8+x^4+x^3+x+1$

$\Rightarrow x^8 \pmod{m(x)} = (0001\ 1011)$

Find: Product $= \{a9\}.\{9e\}$

$\Rightarrow$ Let $f(x) = (1010\ 1001) = x^7+x^5+x^3+1$

$g(x) = (1001\ 1110) = x^7+x^4+x^3+x^2+x$

$\Rightarrow f(x).g(x) = \{a9\}.\{9e\}$

$= x^7.g(x) \oplus x^5.g(x) \oplus x^3.g(x) \oplus 1.g(x)$

$g(x) = (1001\ 1110)$

$\Rightarrow x.g(x) = 00111100$
$\oplus\ 00011011$
$00100111$

$\Rightarrow x^2.g(x) = 01001110$

$\Rightarrow x^3.g(x) = 10011100$

$\Rightarrow x^4.g(x) = 00111000$
$\oplus\ 00011011$
$00100011$

$\Rightarrow x^5.g(x) = 01000110$

$\Rightarrow x^6 \cdot g(x) = 10001100$

$\Rightarrow x^7 \cdot g(x) = 00011000$
$\oplus\ 00011011$
$00000011$

Now
$f(x) \cdot g(x) =$ 0000 0011 $- x^7 \cdot g(x)$
0100 0110 $- x^5 \cdot g(x)$
1001 1100 $- x^3 \cdot g(x)$
$\oplus$ 1001 1110 $- g(x)$
0100 0111

$f(x) \cdot g(x) = x^6 + x^2 + x + 1 = (47)$

$\Rightarrow \{a9\} \cdot \{9e\} = \{47\}$ — Hexadecimal