# Discrete Structures (MA5.101)

Discrete Structures (MA5.101)

*International Institute of Information Technology, Hyderabad*
**Assignment Set 3 (Monsoon 2021)**
Group Theory, Group Codes, Ring and Field
Deadline: March 1, 2022 (Monday), 23:55 PM
Total Marks: 150
**Instructions:** Submit ONLY handwritten scanned pdf file in the course moodle under Assignments directory.

February 19, 2022

## Group Theory

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

[10]

2. Let $H$ be a subgroup of a group $G$, and let $N = \cap_{x \in G} xHx^{-1}$. Prove that $N$ is a normal subgroup of $G$.

[10]

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

[10]

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

[10]

5. Prove that a cyclic group is necessarily abelian. But, the converse is not true.

[10]

## Group Codes

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 received tuple $\langle$ 1 1 0 0 0 1 1 $\rangle$ assuming that error, if any, is a single-error.

[5 + 5 = 10]

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.
(b) Prove that the average weight of a code word is $\frac{n}{2}$. (Hint: The cosets of the subgroup of Part (a) are of equal size)

[10 + 10 = 20]

# Ring and Field

8. The characteristic of any field (finite or infinite) 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 the characteristic of any field is either prime or infinite.

[10]

9. In the algebra of polynomials modulo $p(x)$, where $p(x)$ is a polynomial of degree $n$ over a field $K$, prove that the polynomials form a **field** with respect to polynomial addition and multiplication if and only if $p(x)$ is irreducible.

[10]

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

[10]

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

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

[10]

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

[10]

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

$$x^5 + 88x^4 + 73x^3 + 83x^2 + 51x + 67$$
$$x^3 + 97x^2 + 40x + 38$$

[10]

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:

$$\{a9\} \cdot \{9e\}$$

[10]

**************** **End of Question Paper** ********************