10 10

10

10/10

Jonathon Menary
348074

Cryptography and Codes Assignment 1

1. Define operations on $\mathbb{N}$:

$$x \perp y = \gcd(x,y)$$
$$x \top y = \operatorname{lcm}(x,y)$$

Associativity

$$x \perp (y \perp z) = \gcd(x, \gcd(y,z)) = \gcd(\gcd(x,y), z) = (x \perp y) \perp z$$
$$x \top (y \top z) = \operatorname{lcm}(x, \operatorname{lcm}(y,z)) = \operatorname{lcm}(\operatorname{lcm}(x,y), z) = (x \top y) \top z$$

Commutativity

$$x \perp y = \gcd(x,y) = \gcd(y,x) = y \perp x$$
$$x \top y = \operatorname{lcm}(x,y) = \operatorname{lcm}(y,x) = y \top x$$

Neutral element

$$x \perp 0 = x$$
$$x \top 1 = x$$

Inverse

$x \perp \quad = 0$ no inverse

$x \top \quad = 1$ no inverse

Distributivity

$$x \perp (y \top z) = \gcd(x, \operatorname{lcm}(y,z)) = \operatorname{lcm}(\gcd(x,y), \gcd(x,z)) = (x \perp y) \top (x \perp z)$$
$$x \top (y \perp z) = \operatorname{lcm}(x, \gcd(y,z)) = \gcd(\operatorname{lcm}(x,y), \operatorname{lcm}(x,z)) = (x \top y) \perp (x \top z)$$

$(\mathbb{N}, \perp)$ and $(\mathbb{N}, \top)$ are both commutative semi-Groups

$(\mathbb{N}, \perp, 0)$ and $(\mathbb{N}, \top, 1)$ are both commutative monoids

$(\mathbb{N}, \perp, 0)$ and $(\mathbb{N}, \top, 1)$ are not groups, since there is no inverses

$(\mathbb{N}, \perp, 0, \top, 1)$ and $(\mathbb{N}, \top, 1, \perp, 0)$ are not Rings, since there are no inverses

$(\mathbb{N}, \perp, 0, \top, 1)$ and $(\mathbb{N}, \top, 1, \perp, 0)$ are not Fields, since there are no inverses

2. Define operations on $\mathbb{Z}$:

$$x \top y = \max\{x, y\}$$
$$x \perp y = \min\{x, y\}$$

Associativity

$x \top (y \top z) = \max(x, \max(y,z)) = \max(\max(x,y), z) = (x \top y) \top z$

$x \perp (y \perp z) = \min(x, \min(y,z)) = \min(\min(x,y), z) = (x \perp y) \perp z$

Commutativity

$x \top y = \max(x,y) = \max(y,x) = y \top x$

$x \perp y = \min(x,y) = \min(y,x) = y \perp x$

Neutral Element

$x \top \quad = x$ no neutral element

$x \perp \quad = x$ no neutral element

Inverse

$x \top \quad =$ no inverses

$x \perp \quad =$ no inverses

Distributivity

$x \top (y \perp z) = \max(x, \min(y,z)) = \min(\max(x,y), \max(x,z)) = (x \top y) \perp (x \top z)$

$x \perp (y \top z) = \min(x, \max(y,z)) = \max(\min(x,y), \min(x,z)) = (x \perp y) \top (x \perp z)$

$(\mathbb{Z}, \top)$ and $(\mathbb{Z}, \perp)$ are both commutative semi-Groups

$(\mathbb{Z}, \top)$ and $(\mathbb{Z}, \perp)$ are not monoids, since no neutral elements

$(\mathbb{Z}, \top)$ and $(\mathbb{Z}, \perp)$ are not groups, since no inverses

$(\mathbb{Z}, \top, \perp)$ and $(\mathbb{Z}, \perp, \top)$ are not rings, since no inverses

$(\mathbb{Z}, \top, \perp)$ and $(\mathbb{Z}, \perp, \top)$ are not Fields, since no inverses

3. $M = \left\{ \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \middle| \, n \in \mathbb{Z} \right\}$ Prove $(M, \cdot)$ is commutative group isomorphic to $(\mathbb{Z}, +, 0)$

Matrix multiplication is associative by defintion, so $(M, \cdot)$ is a semigroup. $(M, \cdot)$ is commutative because for any $n \in \mathbb{Z}$ we have for $n, m \in \mathbb{Z}$:

$$M(n) \cdot M(m) = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & n+m \\ 0 & 1 \end{pmatrix}$$

and:

$$M(m) \cdot M(n) = \begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & m+n \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & n+m \\ 0 & 1 \end{pmatrix}$$

Therefore, $(M, \cdot)$ is a commutative semi-group. $(M, \cdot)$ is also a commutative monoid with neutral element I_2 since:

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

$(M, \cdot, I_2)$ is also a group since every element of M has an inverse:

$$\begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & -n \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Define $h: G \to \mathbb{Z}$, therefore:

$$h(x \cdot y) = x + y$$

Suppose $x = y$ we conclude h to be one-to-one. h will also be onto, therefore, $(M, \cdot, I_2)$ is a Commutative group and is isomorphic to $(\mathbb{Z}, +, 0)$.

4. $G = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix} \right\}$

Show $\left(G, \cdot \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\right)$ is a commutative Group.

Matrix Multiplication is associative by definition so $\left(G, \cdot, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\right)$ is a semi-group. It is also a commutative semi-group since all matrices in the set are square and can all be row reduced to the identity matrix.

$\left(G, \cdot, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\right)$ is also a commutative monoid with neutral element $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, since For any matrix M in G we have:

$$M \cdot \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = M$$

and $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ is an element of G. We can also say that $\left(G, \cdot, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\right)$ is a group as all elements of G are invertible since none of there $\det = 0$, and the inverse of all matrices in G is them self, thus for any matrix M in G we have:

$$M \cdot M = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Therefore, $\left(G, \cdot, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\right)$ is a commutative group.

5. Define operations on $\mathbb{Z}$

$$x \perp y = x + y + 3$$
$$x \top y = xy + 3x + 3y + 6$$

a) Prove $(\mathbb{Z}, \perp)$ is a commutative group

Associativity:

$x \perp (y \perp z) = x + (y + z + 3) + 3 = (x + y + 3) + z + 3 = (x \perp y) \perp z$

Commutativity:

$x \perp y = x + y + 3 = y + x + 3 = y \perp x$

Neutral Element:

$x \perp -3 = x - 3 + 3 = x$

Inverse:

$x \perp (-x - 6) = -3$

Therefore since $(\mathbb{Z}, \perp)$ is a commutative semigroup, $(\mathbb{Z}, \perp, -3)$ is a commutative monoid, and every element has an inverse $(\mathbb{Z}, \perp, -3)$ is a commutative group.

b) Prove $(\mathbb{Z}, \top)$ is a commutative monoid

Associativity:

$x \top (y \top z) = x(yz + 3y + 3z + 6) + 3x + 3(yz + 3y + 3z + 6) + 6$ $\quad 6z + 3z$

$= xyz + 3xy + 3xz + 6x + 3x + 3yz + 9y + 9z + 18 + 6$

$= (xyz + 3xz + 3yz + 6z) + (3xy + 9x + 9y + 18) + 3z + 6$

$= (xy + 3x + 3y + 6)z + 3(xy + 3x + 3y + 6) + 3z + 6 = (x \top y) \top z$

Commutativity:

$x \top y = xy + 3x + 3y + 6 = yx + 3y + 3x + 6 = y \top x$

Neutral Element:

$x \top -2 = -2x + 3x - 6 + 6 = x$

Therefore since $(\mathbb{Z}, \top)$ is a commutative semigroup, $(\mathbb{Z}, \top, -2)$ is a commutative monoid, and is not a group since inverses could be in $\mathbb{Q}$.

c) Prove T is distributive over $\perp$

Distributivity:

$$
\begin{aligned}
x \top (y \perp z) &= x(y+z+3) + 3x + 3(y+z+3) + 6 \xrightarrow{} +6 +3 \\
&= \cancel{xy} + xz + \cancel{3x} + 3x + \cancel{3y} + 3z + 9 \cancel{+6} \\
&= (xy + 3x + 3y + 6) + (xz + 3x + 3z + 6) + 3 \\
&= (x \top y) \perp (x \top z)
\end{aligned}
$$

d) Prove $(\mathbb{Z}, \perp, -3, \top, -2)$ is a commutative ~~ring~~ without divisors of 0

$(\mathbb{Z}, \perp, -3, \top, -2)$ is a commutative ring since we have proven that $(\mathbb{Z}, \perp, -3)$ is a commutative group, that $(\mathbb{Z}, \top, -2)$ is a commutative monoid, and that $\top$ is distributive over $\perp$.

$(\mathbb{Z}, \perp, -3, \top, -2)$ has no divisors of 0 since $x \in \mathbb{Z}$.

e) The invertible element of some x in $(\mathbb{Z}, \perp, -3)$ is equal to $-x-6$, such that $x \perp (-x-6) = -3$.

The invertible element of some x in $(\mathbb{Z}, \top, -2)$ is equal to $\frac{-3x-8}{x+3}$, however, this will not always be in $\mathbb{Z}$, as an example for $x=1$, $\frac{-3x-8}{x+3} = \frac{-11}{4}$

$\frac{11}{4}$ therefore $(\mathbb{Z}, \top, -2)$ is not invertible.

6. $S = \{a, b, c, d\}$ $T = \{0, 1\}$

Not Uniquely Decodable

$K(a) = 01$
$K(b) = 10$
$K(c) = 110$
$K(d) = 0110$

Counterexample - $K(ab) = K(d) = 0110$

Uniquely Decodable

$K(a) = 0010$
$K(b) = 1100$
$K(c) = 1000$
$K(d) = 0001$

$K : S \to T^*$ is injective therefore this is a uniquely decodable code