Name: Rajal Rajesh shetty
CWID: 10477484.

Assignment-8

Exercise 8.1

a) Find $<(3,2)> \in \mathbb{Z}_4 \times \mathbb{Z}_3$ write multiples of $(3,2)$ one by one until all elements of $<(3,2)>$ are exhausted.

(a) Consider the group $\mathbb{Z}_4 \times \mathbb{Z}_3$.
Let $(3,2) \in \mathbb{Z}_4 \times \mathbb{Z}_3$.

$<3,2> = (3,2) = (3,2)$

$(3,2)^2 = (3,2)\cdot(3,2) = (2,1)$

reason
$(6=2$ in $\mathbb{Z}_4$
$4=1$ in $\mathbb{Z}_3)$

$(3,2)^3 = (3,2)\cdot(2,1) = (1,0)$

$(3,2)^4 = (3,2)\cdot(1,0) = (0,2)$

$(3,2)^5 = (3,2)(0,2) = (3,1)$ | $(3,2)^6 = (3,2)\cdot(3,1) = (2,0)$

$(3,2)^7 = (3,2)\cdot(2,0) = (1,2)$ | $(3,2)^8 = (3,2)\cdot(1,2) = (0,1)$

$(3,2)^9 = (3,2)\cdot(0,1) = (3,0)$ | $(3,2)^{10} = (3,2)\cdot(3,0) = (2,2)$

$(3,2)^{11} = (3,2)\cdot(2,2) = (1,1)$ | $(3,2)^{12} = (3,2)\cdot(1,1) = \underbrace{(0,0)}_{\text{identity of } \mathbb{Z}_4\times\mathbb{Z}_3}$

Hence, $<(3,2)> = \mathbb{Z}_4 \times \mathbb{Z}_3$.

(b) $U_5 \times \mathbb{Z}_3$.

$(3,2)^1 = (3,2)$

$(3,2)^2 = (3,2)\cdot(3,2) = (9,4) = (4,1)$ | $(3,2)^3 = (3,2)\cdot(4,1) = (3\cdot4, 2+1) = (2,0)$

$(3,2)^4 = (3,2)\cdot(2,0) = (3\cdot2, 2+0) = (1,2)$ | $(3,2)^5 = (3,2)\cdot(1,2) = (3\cdot1, 2+2) = (3,1)$

$(3,2)^6 = (3,2)\cdot(3,1) = (3\cdot3, 2+1) = (4,0)$ | $(3,2)^7 = (3,2)\cdot(4,0) = (3\cdot4, 2+0) = (2,2)$

$(3,2)^8 = (3,2)\cdot(2,2) = (3\cdot2, 2+2) = (1,1)$

$(3,2)^9 = (3,2)\cdot(1,1) = (3,3) = (3,0)$

$(3,2)^{10} = (3,2)\cdot(3,0) = (3\cdot3, 2+0) = (4,2)$

$(3,2)^{10} = (3,2)\cdot(4,2) = (3\cdot4, 2+2) = (2,1)$

$(3,2)^{11} = (3,2)\cdot(4,2) = (3\cdot4, 2+2) = (2,1)$

$(3,2)^{12} = (3,2)\cdot(2,1) = (3\cdot2, 2+1) = \underbrace{(1,0)}_{}$ Identity of $U_5\times\mathbb{Z}_3$.

Exercise 8.2

Consider any ring R. ST if its characteristics $\chi(R)=0$ then for any $a \in R$ we have $n.a=0$.

$\Rightarrow$ Consider a ring of Z_n. where n is prime. without loss of generality its $\chi(Z_n) \neq 0$

then $Z_n = \{a \mod n \mid a \in Z\}$, n is prime.

In Z_n for any element have characteristics $n.a=0$, $\forall a \in Z_n$.

$\therefore$ In Z_n, (n is prime) all elements have order of n.

$\therefore$ for any $a \in R$, $n.a=0$.

Exercise 8.3

Let F be a field & $F(x) \in F[x]$. S.T if $f(x)$ is divisible by a polynomial degree $g(x) = a_n x^n + \cdots$ of deg n, then it is divisible by some monic polynomial of degree n.

$\Rightarrow$ Suppose $f(x)$ is divisible by $g(x)$ then there exists some polynomial $h(x)$ in $F(x)$ ST $F(x) = g(x).h(x)$.

since $g(x) = a_n x^n + a_{n-1} x^{n-1} + a_{n-2} x^{n-2} + \cdots + a_1 x + a_0$; $a_n \neq 0$

$f(x) = (a_n x^n + a_{n-1} x^{n-1} + a_{n-2} x^{n-2} + \cdots + a_1 x + a_0) h(x)$

Take a_n common

$$f(x) = (x^n + b_{n-1} x^{n-1} + \cdots + b_1 x + b_0)(a_n h(x))$$

where,

$$b_i = \frac{a_i}{a_n} \text{ for } i = 0, 1, 2, \ldots, n-1.$$

it is clear that $f(x)$ is divisible by

$x^n + b_{n-1} x^{n-1} + \cdots + b_1 x + b_0$.

which is monic polynomial of degree n.

Hence proved

Exercise 8.4 check if the following polynomials are irreducible or not.

(a) $f(x) = x^3+2x-1 \in \mathbb{Z}_3[x]$.

(b) $f(x) = x^3+2x^2+2x+1 \in \mathbb{Z}_5[x]$

(c) To check if $f(x) = x^4+x^3+x^2+x+1 \in \mathbb{Z}_2[x]$ is irreducible you will need to consider lineal factors & quadratic factors.

$\Rightarrow$

(a) Reducibility test for degree 2 & 3 :- Let F be a field if $f(x) \in F(x)$ & $\deg f(x) = 2$ or 3 then $f(x)$ is reducible over F iff $f(x)$ has zero in F.

$f(x) = x^3+2x-1 \in \mathbb{Z}_3(x)$

$\mathbb{Z}_3$ is a field. $f(x)$ is reducible iff $f(x)$ has zero in $\mathbb{Z}_3$.

$\mathbb{Z}_3 = \{0, 1, 2\}$.

$f(0) = -1$.
$f(1) = 1+2-1 = 2$.
$f(2) = 8+4-1 = 11 \bmod 3 = 2$

$f(x)$ has no zero in $\mathbb{Z}_3$.

$\Rightarrow f(x)$ is irreducible//

(b) $f(x) = x^3+2x^2+2x+1$ in $\mathbb{Z}_5[x]$.

$\deg f(x) = 3$. & $\mathbb{Z}_5$ is field.

$f(x)$ is reducible iff $f(x)$ has zero in $\mathbb{Z}_5$.

$\mathbb{Z}_5 = \{0,1,2,3,4\}$

$f(0) = 1$

$f(1) = 1+2+2+1 = 1 \bmod 5$.

$f(2) = 8+8+4+1 = 1 \bmod 5$.

$f(3) = 27+18+6+1 = 2 \bmod 5$.

$f(4) = 64+32+8+1 = 0$.

So, 4 is a root of $f(x)$, hence $(x-4)$ is factor of $F(x)$.

$\therefore f(x)$ is reducible & can be expressed as $f(x) = g(x).h(x)$

$= x^3+x^2+x^2+x+x+1$
$= x^2(x+1)+x(x+1)+(x+1)$
$= (x^2+x+1)(x+1) \in \mathbb{Z}_5[x]$
$\Rightarrow$ reducible

$$
\begin{array}{r|l}
 & x^2+x+1 \\
\hline
x-4 & x^3+2x^2+2x+1 \\
 & x^3+x^2 \\
\hline
 & x^2+2x \\
 & x^2+x \\
\hline
 & x+1 \\
 & x+1 \\
\end{array}
$$

(c) $f(x) = x^4 + x^3 + x^2 + x + 1$ in $\mathbb{Z}_2[x]$.

deg $f(x) = 4$.

if $f(x)$ is not irreducible then $f(x) = g(x) \cdot h(x)$

Case 1: $\deg g(x) = 1$ & $\deg h(x) = 3$.

$\Rightarrow f(x)$ has zero in $\mathbb{Z}_2$. $\mathbb{Z}_2 = \{0, 1\}$.

$f(0) = 1$.

$f(1) = 5 \bmod 2 = 1$.

$\Rightarrow f(x)$ has no zero in $\mathbb{Z}_2$.

$f(x)$ is not reducible in polynomial of degree one & polynomial of degree 3.

Case 2: $\deg g(x) = 2$ & $\deg h(x) = 2$.

we know that $\mathbb{Z}_2[x]$ there exist only one irredicible quadratic polynomial which is $x^2 + x + 1$.

if we assume $f(x)$ is reducible then $f(x) = (x^2+x+1)(x^2+x+1)$

$(x^2+x+1)(x^2+x+1) = x^4 + x^2 + 1$ in $\mathbb{Z}_2[x]$

$f(x) \neq x^4 + x^2 + 1$

$\Rightarrow$ our assumption is wrong.

$f(x)$ is not reducible in product of 2 quadratic polynomials.

$\therefore f(x)$ is irreducible.//

Another way or

$f(x) = x^3(x+1) + x^2 + x + 1$.

if $f(x)$ is reducible

$\exists f(x) = g(x) \cdot h(x)$.

$g(x)$ can be $x, x+1, x^2, x^2+1$.

all the $g(x) \mid x^3(x+1)$ if $f(x) \mid g(x)$, we need $g(x) \mid x^2+x+1$, but x^2+x+1 is irreducible, $\therefore f(x)$ is irreducible

Exercise 8.5

Find the remainder of division of $2x^6+x^2-1$ by x^2+3x+2 in $\mathbb{Z}_5(x)$.

$$2x^4+4x^3+4x^2+3$$

$$x^2+3x+2 \;\big)\; 2x^6+x^2-1$$

$$(-)\; 2x^6+6x^5+4x^4$$

$$-6x^5-4x^4+x^2-1$$

$$\Downarrow$$

$$4x^5+x^4+x^2+4 \quad \text{in } \mathbb{Z}_5(x)$$

$$(-)\; 4x^5+12x^4+8x^3$$

$$-11x^4-8x^3+x^2+4$$

$$\Downarrow$$

$$4x^4+2x^3+x^2+4 \quad \text{in } \mathbb{Z}_5(x)$$

$$(-)\; 4x^4+12x^3+8x^2$$

$$-10x^3-7x^2+4$$

$$\Downarrow$$

$$0x^3+3x^2+4 \quad \text{in } \mathbb{Z}_5(x)$$

$$(-)\; 3x^2+9x+6$$

$$-9x-2$$

$$\Rightarrow x+3$$

//

thus the remainder of division $2x^6+x^2-1$ by x^2+3x+2 in $\mathbb{Z}_5(x)$ is $x+3$ //

$$2x^6+x^2-1 = (x^2+3x+2)(2x^4+4x^3+4x^2+3)+(x+3)$$

Exercise 8.6

for $f(x) = 4x^4 - x^3 + 3x^2 + x - 2$ & $g(x) = 4x^5 + x^3$ in $\mathbb{Z}_5[x]$

use the euclidean algo. to find

(a) $\gcd(f(x), g(x))$

(b) polynomials $\alpha(x), \beta(x) \in \mathbb{Z}_5(x)$ satisfying $\gcd(f(x), g(x)) = \alpha(x) f(x) + \beta(x) g(x)$

$\Rightarrow$ $f(x) = 4x^4 - x^3 + 3x^2 + x - 2$

$= 4x^4 + 4x^3 + 3x^2 + x + 3$ in $\mathbb{Z}_5(x)$

$g(x) = 4x^5 + x^3$.

(a) $\deg(g(x)) > \deg(f(x))$

$$
\begin{array}{r|l}
 & x - 1 \\
4x^4 + 4x^3 + 3x^2 + x + 3 & 4x^5 + x^3 \\
 & 4x^5 + 4x^4 + 3x^3 + 3x^2 + 3x \\
\hline
 & -4x^4 - 2x^3 - x^2 - 3x \\
 & \underset{(+)}{-}4x^4 \underset{(+)}{-} 4x^3 \underset{(+)}{-} 3x^2 \underset{(+)}{-} x \underset{(+)}{-} 3 \\
\hline
 & 2x^3 + 2x^2 - 2x + 3
\end{array}
$$

$4x^5 + x^3 = (4x^4 + 4x^3 + 3x^2 + x + 3)(x + 4) + (2x^3 + 2x^2 + 3x + 3)$ in $\mathbb{Z}_5(x)$ -(1)

$$
\begin{array}{r|l}
 & 2x \\
2x^3 + 2x^2 + 3x + 3 & 4x^4 + 4x^3 + 3x^2 + x + 3 \\
 & 4x^4 + 4x^3 + x^2 + x \\
\hline
 & 2x^2 + 3
\end{array}
$$

$4x^4 + 4x^3 + 3x^2 + x + 3 = (2x^3 + 2x^2 + 3x + 3).(2x) + 2x^2 + 3$ -(2)

$$
\begin{array}{r|l}
 & x + 1 \\
2x^2 + 3 & 2x^3 + 2x^2 + 3x + 3 \\
 & \underset{(-)}{2x^3} \underset{(-)}{+} 3x \\
\hline
 & 2x^2 + 3 \\
 & \underset{(-)}{2x^2} \underset{(-)}{+} 3 \\
\hline
 & 0
\end{array}
$$

$(2x^3 + 2x^2 + 3x + 3) = (2x^2 + 3)(x + 1) + 0$

we have,

$4x^5 + x^3 = (4x^4 + 4x^3 + 3x^2 + x + 3)(x + 4) + (2x^3 + 2x^2 + 3x + 3)$

$4x^4 + 4x^3 + 3x^2 + x + 3 = (2x^3 + 2x^2 + 3x + 3)(2x) + (2x^2 + 3)$

$2x^3 + 2x^2 + 3x + 3 = (2x^2 + 3)(x + 1) + 0$

Last non zero remainder is $2x^2+3$.

$\therefore\ 2x^2+3 = 2(x^2+3\times 2^{-1})$ in $\mathbb{Z}_5(x)$

$= 2(x^2+3\times 3)$

$= 2(x^2+9)$

$= 2(x^2+4)$ in $\mathbb{Z}_5(x)$

$\therefore\ \gcd(f(x), g(x)) = x^2+4$ //

(b)

$2x^2+3 = 4x^4+4x^3+3x^2+x+3 - (2x^3+2x^2+3x+3)(2x)$

$= (4x^4+4x^3+3x^2+x+3) - (2x)(4x^5+x^3-(x+4)(4x^4+4x^3+3x^2+x+3))$

$= (4x^4+4x^3+3x^2+x+3)(1+2x(x+4)) - (2x)(4x^5+x^3)$

$= f(x)\cdot(1+2x^2+3x) - (2x)\,g(x)$

$= (2x^2+3x+1)\cdot f(x) - (2x)\,g(x)$

$= (2x^2+3x+1)\cdot f(x) + 3x\cdot g(x)$

$x^2+4 = 2^{-1}(2x^2+3x+1)f(x) + 2^{-1}\cdot 3x\cdot g(x)$

$= (6x^2+9x+3)f(x) + 9x\cdot g(x)$

$= (x^2+4x+3)\cdot f(x) + 4x\cdot g(x)$

$f(x) = 4x^4+4x^3+3x^2+x+3$

$g(x) = 4x^5+x^3$

$\therefore\ \alpha(x) = x^2+4x+3$

$\beta(x) = 4x$ //

Exercise 8.7

S.T the set of complex number $\mathbb{C}$ with standard complex addition & multiplicatn is a vector space over a field $\mathbb{R}$.

$\Rightarrow$ proof. $\mathbb{C} = \{a+ib, a, b \in \mathbb{R}\}$

Let $z_1 = a_1 + ib_1$, $z_2 = a_2 + ib_2 \in \mathbb{C}$ with $a_1, b_1, a_2, b_2 \in \mathbb{R}$.

$z_1 + z_2 = (a_1+a_2) + i(b_1+b_2) \in \mathbb{C}$ with $a_1 + a_2 \in \mathbb{R}$, $b_1 + b_2 \in \mathbb{R}$.

$\therefore$ $\mathbb{C}$ is closed under addition.

- Let $K \in \mathbb{R}$ & $z = a+ib \in \mathbb{C}$

$Kz = K(a+ib) = Ka + Kib \in \mathbb{C}$

$= Ka + i(Kb) \in \mathbb{C}$

$\therefore$ $\mathbb{C}$ is closed under scalar multiplication.

- $z_1 = a_1+ib_1$, $z_2 = a_2+ib_2$, $z_3 = a_3+ib_3 \in K$.

now, $(z_1+z_2)+z_3 = ((a_1+a_2)+i(b_1+b_2)) + z_3$

$= ((a_1+a_2)+i(b_1+b_2)) + (a_3+ib_3)$

$= (a_1+a_2+a_3)+i(b_1+b_2+b_3)$

$= (a_1+ib_1) + \{(a_2+a_3)+i(b_2+b_3)$

$= z_1 + (z_2+z_3)$

$\therefore$ addition is associative on $\mathbb{C}$.

- $0 \in \mathbb{C}$ with $(a+ib)+0 = 0+(a+ib)$

& $(a+ib)+(-a-ib) = 0$.

$\because$ $a, b \in \mathbb{R} \Rightarrow -a, -b \in \mathbb{R}$ $\therefore$ $-a-ib \in \mathbb{C}$.

- $\alpha, \beta \in \mathbb{R}$ & $z = a+ib \in \mathbb{C}$

now $\alpha(\beta z) = \alpha(a\beta + i\beta b) = a\alpha\beta + i\alpha\beta b$

$= \beta(a\alpha + i\alpha b)$

$= \beta(\alpha(a+ib)) = \beta(\alpha z)$

& $1 \in \mathbb{C}$ with $1 \cdot z = z$ holds.

now $(\alpha+\beta)z = (\alpha+\beta)(a+ib)$

$$= (\alpha+\beta)a + i(\alpha+\beta)b$$

$$= (\alpha a + i\alpha b) + \beta a + i\beta b$$

$$= \alpha(a+ib) + \beta(a+ib)$$

$$= \alpha z + \beta z$$

Hence $(\mathbb{C}, +, \cdot)$ satisfy all conditions to form a vector space.

<u>Exercise 8.8</u>

Let F be a vector space. S.T. $F^n = \{(\alpha_1, \ldots, \alpha_n) \mid \alpha_1 \ldots \alpha_n \in F\}$ with $+$ and $\cdot$ defined by

$$(\alpha_1, \ldots, \alpha_n) + (\beta_1, \ldots, \beta_n) = (\alpha_1 + \beta_1, \ldots, \alpha_n + \beta_n),$$

$$c(\alpha_1, \ldots, \alpha_n) = (c\alpha_1, \ldots, c\alpha_n)$$

is a vector space over F.

$\Rightarrow$ $F^n = \{(\alpha_1, \alpha_2, \ldots, \alpha_n) \mid \alpha_1, \alpha_2 \ldots \alpha_n \in F\}$

addition: let $x = (\alpha_1, \alpha_2, \ldots, \alpha_n)$, $y = (\beta_1, \beta_2, \ldots, \beta_n)$

$\alpha_i \in F$, $\beta_i \in F$.

$\therefore x + y = (\alpha_1 + \beta_1, \ldots, \alpha_n + \beta_n)$ 4 $\alpha_i \beta_i \in F^n$

$\therefore F^n$ is closed under addition.

Scalar multiplicat^n: Let $x = (\alpha_1, \alpha_2 \ldots \alpha_n) \in F^n$ 4 $c \in F$

$cx = c(\alpha_1, \alpha_2 \ldots \alpha_n) = (c\alpha_1, c\alpha_2, \ldots, c\alpha_n)$

$\because c \in F, \alpha_i \in F, \Rightarrow c\alpha_i \in F$

$\therefore cx \in F^n$

Let $x = (\alpha_1, \alpha_2 \ldots \alpha_n)$ $y = (\beta_1, \beta_2 \ldots \beta_n)$

$z = (\gamma_1, \gamma_2 \ldots \gamma_n) \in F^n$

$\therefore (x+y) + z = (\alpha_1 + \beta_1, \alpha_2 + \beta_2, \ldots, \alpha_n + \beta_n) + (\gamma_1, \gamma_2 \ldots \gamma_n)$

$= (\alpha_1+\beta_1+\gamma_1, \ldots, \alpha_n+\beta_n+\gamma_n) = (\alpha_1, \alpha_2 \ldots \alpha_n) + (\beta_1+\gamma_1 + \beta_2\gamma_2 + \ldots \beta_n+\gamma_n)$

$= x+(y+z)$

$\therefore$ addition is associative on F^n.

Let $x = (\alpha_1 \cdot \alpha_2, \ldots \alpha_n) \in F^n$ & $(0, 0, \ldots 0) \in F^n$.

with $x+0 = x$.

& consider $(-\alpha_1, -\alpha_2 \ldots -\alpha_n) \in F^n$.

with $(\alpha_1 \ldots \alpha_n) + (-\alpha_1 \ldots \alpha_n) = (0, 0 \ldots 0)$

$\therefore x + (-x) = 0$ holds.

Let $\alpha, \beta \in F$ & $x = (\alpha_1, \alpha_2 \ldots \alpha_n) \in F^n$.

$\therefore \alpha(\beta x) = \alpha(\beta\alpha_1, \beta\alpha_2 \ldots \beta\alpha_n)$

$= (\alpha\beta\alpha_1, \ldots \alpha\beta\alpha_n)$

$= \alpha\beta(\alpha_1, \ldots \alpha_n) = (\alpha\beta)x$.

& $1 = (1, 1, \ldots 1) \in F^n$ & $x = (\alpha_1 \ldots \alpha_n) \in F^n$

with $1.n = (1\alpha_1, 1\alpha_2 \ldots 1\alpha_n) = (\alpha_1 \ldots \alpha_n) = x$

Let $\alpha, \beta \in F$ & $x \in F^n$.

$(\alpha+\beta)x = ((\alpha+\beta)\alpha_1, (\alpha+\beta)\alpha_2, \ldots (\alpha+\beta)\alpha_n)$

$= (\alpha\alpha_1, \alpha\alpha_2 \ldots \alpha\alpha_n) + (\beta\alpha_1, \beta\alpha_2 \ldots \beta\alpha_n)$

$= (\alpha x + \beta x)$ holds.

hence, $(F^n, +, \cdot)$ is a vector space over Field F.