So, $\phi((r+n\mathbb{Z})(s+n\mathbb{Z})) = \phi(k+n\mathbb{Z}) = \bar{k} = \bar{r}\bar{s} = \phi(r+n\mathbb{Z})\phi(s+n\mathbb{Z})$

So, ϕ is a homomorphism. Hence ϕ is an isomorphism

Hence $\mathbb{Z}_n \simeq \mathbb{Z}/n\mathbb{Z}$

2. Consider the rings $\mathbb{Z}$ and $\mathbb{Z}_6$. Let $f: \mathbb{Z} \to \mathbb{Z}_6$ be defined by $f(z) = \bar{n}$ for all $n \in \mathbb{Z}$. Show that f is a homomorphism and find Ker$f$.

Solution: Let $m, n \in \mathbb{Z}$. Then $f(m+n) = \overline{m+n} = \bar{m}+\bar{n} = f(m)+f(n)$ and $f(mn) = \overline{mn} = \bar{m}\cdot\bar{n}$. Hence f is a homomorphism.

Now
$$\begin{aligned}\text{Ker} f &= \{n \in \mathbb{Z} : f(n) = \bar{0}\} \\ &= \{n \in \mathbb{Z} : \bar{n} = \bar{0}\} \\ &= \{n \in \mathbb{Z} : n = 6k \text{ where } k \in \mathbb{Z}\} \\ &= 6\mathbb{Z}\end{aligned}$$

3. Show that the mapping $f: \mathbb{Z}[\sqrt{2}] \to \mathbb{Z}[\sqrt{3}]$ defined by $f(a+b\sqrt{2}) = a+b\sqrt{3}$, $a, b \in \mathbb{Z}$ is a group homomorphism but not a ring homomorphism

Proof: Let $a+b\sqrt{2},\ c+d\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$. Then
$$\begin{aligned} f((a+b\sqrt{2})+(c+d\sqrt{2})) &= f((a+c)+(b+d)\sqrt{2}) \\ &= (a+c)+(b+d)\sqrt{3} \\ &= (a+b\sqrt{3})+(c+d\sqrt{3}) \\ &= f(a+b\sqrt{3})+f(c+d\sqrt{3})\end{aligned}$$

Hence f is a group homomorphism. Clearly f is surjective as for $c+d\sqrt{3} \in \mathbb{Z}[\sqrt{3}]$, $\exists\ c+d\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$ such that $f(c+d\sqrt{2}) = c+d\sqrt{3}$.

Hence $f(1) = 1$. Then $f(2) = f(1+1) = f(1) + f(1) = 2$

But $f(\sqrt{2}\cdot\sqrt{2}) = f(2) = 2$

But $f(\sqrt{2})f(\sqrt{2}) = f(0+1\cdot\sqrt{2})f(0+1\sqrt{2}) = (0+1\cdot\sqrt{3})(0+1\cdot\sqrt{3})$
$= 3$

So, $f(\sqrt{2}\cdot\sqrt{2}) \neq f(\sqrt{2})\cdot f(\sqrt{2})$

Hence f is not a ring homomorphism.

4. Show that the ring $2\mathbb{Z}$ is not isomorphic to $5\mathbb{Z}$

Proof: Suppose, if possible, $\exists$ a ring isomorphism $f: 2\mathbb{Z} \to 5\mathbb{Z}$. Hence f is a group isomorphism of $(2\mathbb{Z},+)$ onto $(5\mathbb{Z},+)$. But $2\mathbb{Z}$ and $5\mathbb{Z}$ are both cyclic groups. 2 is a generator of $2\mathbb{Z}$. Hence $f(2)$ must be a generator of the group $5\mathbb{Z}$. Now we know that 5 and -5 are the only generators of $5\mathbb{Z}$. So, $f(2) = 5$ or -5. Suppose $f(2) = 5$.

Then $f(4) = f(2+2) = f(2) + f(2) = 5+5 = 10$

and again, $f(4) = f(2\cdot 2) = f(2)\cdot f(2) = 5\cdot 5 = 25$

This implies $10 = 25$, which is absurd. If $f(2) = -5$, then proceeding in a similar way, we can arrive at some absurd conclusion. Hence $\nexists$ no ring isomorphism $f: 2\mathbb{Z} \to 5\mathbb{Z}$.

5. Prove that the fields $\mathbb{R}$ and $\mathbb{C}$ are not isomorphic

Solution: Suppose, if possible, $f: \mathbb{R} \to \mathbb{C}$ is an isomorphism from $\mathbb{R}$ onto $\mathbb{C}$. Then $\exists\, r \in \mathbb{R}$ such that $f(r) = i$

So, $f(r^2) = f(r)\cdot f(r) = i^2 = -1$. Now since f is an onto homomorphism, $f(1)$ is the identity of $\mathbb{C}$. So, $f(1) = 1$ and hence $f(-1) = -f(1) = -1$ as $f(-a) = -f(a)$. So, $f(r^2) = -1 = f(-1)$. As f is injective, $r^2 = -1$. But there is no such real number r satisfying $r^2 = -1$. So there does not exist any isomorphism from $\mathbb{R}$ onto $\mathbb{C}$. Hence $\mathbb{R}$ and $\mathbb{C}$ are not isomorphic.

Unit 2 : Linear Algebra

Vector space over a field

Definition 2.1 Let V be a non-empty set and $\oplus$ be a binary operation on V. Let $(F, +, \cdot)$ be a field and let $\odot$ be a mapping from $F \times V$ to V, called scalar multiplication. If $(c, \alpha) \in F \times V$ then $\odot(c, \alpha)$ is denoted by $c \odot \alpha$. $\oplus$ is called vector addition. V is said to be a vector space over the field F if the following conditions are satisfied:

V1. $\alpha \oplus \beta \in V$ for all $\alpha, \beta \in V$ (you need not mention it as it is automatically satisfied since $\oplus$ is a binary operation on V)

V2. $\alpha \oplus \beta = \beta \oplus \alpha$ for all $\alpha, \beta \in V$,

V3. $\alpha \oplus (\beta \oplus \gamma) = (\alpha \oplus \beta) \oplus \gamma$ for all $\alpha, \beta, \gamma \in V$,

V4. there exists an element θ in V such that $\alpha \oplus \theta = \theta \oplus \alpha = \alpha$ for all $\alpha \in V$,

V5. for each $\alpha \in V$, there exists an element $-\alpha \in V$ such that $\alpha \oplus (-\alpha) = (-\alpha) \oplus \alpha = \theta$,

V6. $c \odot \alpha \in V$ for all $\alpha \in V$ (you also need not mention it as it is automatically satisfied since $\odot$ is a mapping from $F \times V$ to V)

V7. $c \odot (d \odot \alpha) = (c \cdot d) \odot \alpha$ for all $c, d \in F$, all $\alpha \in V$

V8. $c \odot (\alpha \oplus \beta) = (c \odot \alpha) \oplus (c \odot \beta)$ for all $c \in F$, all $\alpha, \beta \in V$

V9. $(c + d) \odot \alpha = (c \odot \alpha) \oplus (d \odot \alpha)$ for all $c, d \in F$, all $\alpha \in V$

V10. $1 \odot \alpha = \alpha$, for all $\alpha \in V$, 1 being the multiplicative identity in F.

The vector space is denoted by $(V, F, +, \cdot, \oplus, \odot)$. The elements of V are called vectors and the elements of F are called scalars. F is called the ground field or field of scalars of the vector space.

Four symbols $+, \cdot, \oplus, \odot$ denote four different mappings;

$+ : F \times F \to F$, $\cdot : F \times F \to F$, $\oplus : V \times V \to V$ $\odot : F \times V \to V$.

From now on, we write for both $+$, and $\oplus$, the symbol $+$, for both $\cdot$ and $\odot$, the symbol $\cdot$ We also sometimes denote $c \cdot d$ by cd and $c \odot \alpha$ by $c\alpha$.

So, with this new notation, a non-empty set V is said to be a vector space over a field F if there is a binary operation $+$ on V, called vector addition, satisfying the following ~~properties~~ conditions:

V1. $\alpha + \beta \in V$ for all $\alpha, \beta \in V$

V2. $\alpha + \beta = \beta + \alpha$ for all $\alpha, \beta \in V$

V3. $\alpha + (\beta + \gamma) = (\alpha + \beta) + \gamma$ for all $\alpha, \beta, \gamma \in V$

V4. $\exists$ an element $\theta \in V$ such that

$\alpha + \theta = \alpha$ for all $\alpha \in V$

V5. For each $\alpha \in V$, $\exists$ an element $-\alpha \in V$ such that

$\alpha + (-\alpha) = \theta$

and there is also a mapping $\cdot$ from $F \times V$ to V, called scalar multiplication, satisfying the conditions

V6. $c\alpha \in V$ for all $c \in F$ and $\alpha \in V$

V7. $c(d\alpha) = (cd)\alpha$ for all $c, d \in F$ and for all $\alpha \in V$

V8. $c(\alpha + \beta) = c\alpha + c\beta$ for all $c \in F$ and for all $\alpha, \beta \in V$

V9. $(c+d)\alpha = c\alpha + d\alpha$ for all $c \in F$ and for all $\alpha \in V$

V10. $1\alpha = \alpha$ for all $\alpha \in V$, 1 being the multiplicative identity in F.