Module IV : Morphisms, Ring and Field (MATH 2201)

The most general algebraic structure with two binary operations that we study here is called a ring.

1 Rings and Fields

A ring $(R, +, \cdot)$ is a nonempty set R together with two binary operations '$+$' and '$\cdot$' respectively called addition and multiplication such that the following conditions hold:

(i) $(R, +)$ is a commutative group.

(ii) $(R, \cdot)$ is a semigroup (i.e. multiplication is associative), and

(iii) $a \cdot (b + c) = a \cdot b + a \cdot c$, and $(a + b) \cdot c = a \cdot c + b \cdot c$, i.e. distributive properties hold in R.

Moreover, R is said to be *commuative* if the multiplication is commutative. R is called a *ring with unity* if it has an element e in R said to be a multiplicative identity in R with $a \cdot e = a = e \cdot a$ for all $a \in R$.

Examples:

1. $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$ are commutative rings with unity, where $'+'$ and $'\cdot'$ denotes usual addition and usual multiplication.

2. Let $n \in \mathbb{N}$. Then $(n\mathbb{Z}, +, \cdot)$ is a commutative ring without unity where $'+'$ and $'\cdot'$ denotes usual addition and usual multiplication..

3. Let $n \in \mathbb{N}$. Then $(M_n(\mathbb{R}), +, \cdot)$ is the ring of all $n \times n$ real matrices. It is a non-commutative ring with unity I_n being the unity in the ring. Here $'+'$ and $'\cdot'$ denotes matrix addition and matrix multiplication.

4. For a fixed positive integer n, $\mathbb{Z}_n$ is the class of residues of integers modulo n. $\mathbb{Z}_n = \{[0], [1], [2], ..., [n-1]\}$. Then $(\mathbb{Z}_n, +_n, \cdot_n)$ is a commutative ring with unity $[1]$. On $\mathbb{Z}_n$ we define addition and multiplication by $[a] +_n [b] = [a + b]$ and

$[a] \cdot_n [b] = [ab]$. Any $[a]$ or, $\bar{a} \in \mathbb{Z}$ implies $\bar{a} = \{b \in \mathbb{Z} : b \equiv a(\text{mod}n)\} = \{b \in \mathbb{Z} : n|(a-b)\}$.

5. $\mathbb{Z}[i] = \{a + ib : a, b \in \mathbb{Z}\}$ forms a commutative ring with unity called the ring of Gaussian integers.

6. Let us consider the set H of 2×2 complex matrices given by $H = \{\begin{pmatrix} a+ib & c+id \\ -c+id & a-ib \end{pmatrix} : a, b, c, d \in \mathbb{R}\}$ forms a ring of real quaternions with unity $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ with respect to matrix addition and matrix multiplication.

7. The set of all polynomials over $\mathbb{R}$ is denoted by $\mathbb{R}[x]$. If $f(x) = a_0 + a_1x + a_2x^2 + ... + a_nx^n$ and $g(x) = b_0 + b_1x + b_2x^2 + ... + b_mx^m$ be in $\mathbb{R}[x]$. Then $f(x) + g(x)$ and $f(x) \cdot g(x)$ are in $\mathbb{R}[x]$ under which it forms a commutative ring with unity. Moreover, the ring polynomials over $\mathbb{Z}$ is denoted by $\mathbb{Z}[x]$ and the ring of polynomials over $\mathbb{Q}$ is denoted by $\mathbb{Q}[x]$.

8. Let $(R, +)$ be a commutative group. On R we define multiplication by $a \cdot b = 0$ for all $a, b \in R$. Then $(R, +, \cdot)$ forms a ring called a zero ring.

9. Let X be a non-empty set and $P(X)$ be its power set. In $P(X)$ we define $'+'$ and $'\cdot'$ by $A + B = A \triangle B = (A \setminus B) \cup (B \setminus A)$ and $A \cdot B = A \cap B$. Then $(P(X), +, \cdot)$ is a ring. (Verify !)

Definition: Let R be a ring with unity 1. An element $a \in R$ is called an idempotent element if $a^2 = a$.

Definition: Let R be a ring with unity 1. Then R is called a Boolean ring if every element of R is idempotent, i.e., $a^2 = a$ for all $a \in R$. e.g. $(\mathbb{Z}_2, +_2, \cdot_2)$.

Follow the Theorem 18.8 in the next page:

for $|n|$ summands. Finally, we define

$$0 \cdot a = 0$$

for $0 \in \mathbb{Z}$ on the left side of the equations and $0 \in R$ on the right side. Actually, the equation $0a = 0$ holds also for $0 \in R$ on both sides. The following theorem proves this and various other elementary but important facts. Note the strong use of the distributive laws in the proof of this theorem. Axiom $\mathscr{R}_1$ for a ring concerns only addition, and axiom $\mathscr{R}_2$ concerns only multiplication. This shows that in order to prove anything that gives a relationship between these two operations, we are going to have to use axiom $\mathscr{R}_3$. For example, the first thing that we will show in Theorem 18.8 is that $0a = 0$ for any element a in a ring R. Now this relation involves both addition and multiplication. The multiplication $0a$ stares us in the face, and 0 is an *additive* concept. Thus we will have to come up with an argument that uses a distributive law to prove this.

18.8 Theorem If R is a ring with additive identity 0, then for any $a, b \in R$ we have

1. $0a = a0 = 0$,
2. $a(-b) = (-a)b = -(ab)$,
3. $(-a)(-b) = ab$.

Proof For Property 1, note that by axioms $\mathscr{R}_1$ and $\mathscr{R}_2$,

$$a0 + a0 = a(0 + 0) = a0 = 0 + a0.$$

Then by the cancellation law for the additive group $\langle R, + \rangle$, we have $a0 = 0$. Likewise,

$$0a + 0a = (0 + 0)a = 0a = 0 + 0a$$

implies that $0a = 0$. This proves Property 1.

In order to understand the proof of Property 2, we must remember that, by *definition*, $-(ab)$ is the element that when added to ab gives 0. Thus to show that $a(-b) = -(ab)$, we must show precisely that $a(-b) + ab = 0$. By the left distributive law,

$$a(-b) + ab = a(-b + b) = a0 = 0,$$

since a0 = 0 by Property 1. Likewise,

$$(-a)b + ab = (-a + a)b = 0b = 0.$$

For Property 3, note that

$$(-a)(-b) = -(a(-b))$$

by Property 2. Again by Property 2,

$$-(a(-b)) = -(-(ab)),$$

and $-(-(ab))$ is the element that when added to $-(ab)$ gives 0. This is ab by definition of $-(ab)$ and by the uniqueness of an inverse in a group. Thus, $(-a)(-b) = ab$. ◆

It is important that you *understand* the preceding proof. The theorem allows us to use our usual rules for signs.

Divisors of Zero: In a ring R, a non-zero element a is said to be a left divisor of zero if there exists a non-zero element b in R such that $a \cdot b = 0$ and a is said to be a right divisor of zero if there exists a non-zero element c in R such that $c \cdot a = 0$.

Examples:

1. In the ring $(\mathbb{Z}_6, +, \cdot)$, $\bar{2}, \bar{3}, \bar{4}$ are divisors of zero.
2. In the ring $M_2(\mathbb{R})$, $\begin{pmatrix} 1 & 2 \\ 2 & 4 \end{pmatrix} \cdot \begin{pmatrix} 2 & 6 \\ -1 & -3 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$. Here $\begin{pmatrix} 2 & 6 \\ -1 & -3 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 \\ 2 & 4 \end{pmatrix} \neq \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$. Hence $\begin{pmatrix} 1 & 2 \\ 2 & 4 \end{pmatrix}$ is a left divisor and $\begin{pmatrix} 2 & 6 \\ -1 & -3 \end{pmatrix}$ is a right divisor of zero.

Cancellation Law: The cancellation laws hold in a ring R if $a \cdot b = a \cdot c$ with $a \neq 0$ implies $b = c$ and $b \cdot a = c \cdot a$ with $a \neq 0$ implies $b = c$.

In $\mathbb{Z}_6$, $[2] \cdot [3] = [4] \cdot [3]$ but $[2] \neq [4]$. Hence cancellation law does not hold.

Theorem : The cancellation laws hold in a ring R if and only if R has no divisors of zero.

Proof: Let R be a ring in which cancellation laws hold and suppose $a \cdot b = 0$ for some $a, b \in R$. If $a \neq 0$, then $a \cdot b = a \cdot 0$ implies $b = 0$ by cancellation laws. Similarly, $b \neq 0$ implies $a = 0$. So there can be no divisors of zero.

Conversely, suppose R has no divisors of zero and let $a \cdot b = a \cdot c$ with $a \neq 0$. Then $a \cdot b - a \cdot c = a \cdot (b - c) = 0$. Since $a \neq 0$, $b - c = 0$, so $b = c$. Hence cancellation law holds. A similar argument can be shown to prove that $b \cdot a = c \cdot a$ with $a \neq 0$ implies $b = c$.

Units: In a ring R with unity $1(\neq 0)$, a multiplicative inverse or, unit is an element $b \in R$ such that $a \cdot b = b \cdot a = 1$.

Example:

1. In $(\mathbb{Z}, +, \cdot)$, 1 and -1 are the only units.
2. In $(\mathbb{Q}, +, \cdot)$, every non-zero element is a unit.
3. In $(\mathbb{Z}_6, +_6, \cdot_6)$, $\bar{1}, \bar{5}$ are the units.

4. In $(\mathbb{Z}_5, +_5, \cdot_5)$, every non-zero element is a unit.

Note: If a is a unit in a ring R with unity 1, then a is not a divisor of zero. Since if a is a unit then $a \cdot b = b \cdot a = 1$. Let c be a non-zero element such that $a \cdot c = 0$. Then $b \cdot (a \cdot c) = b \cdot 0 = 0$, which implies $(b \cdot a) \cdot c = 1 \cdot c = c = 0$. Thus, a contradiction arrives.

Theorem : In the ring $(\mathbb{Z}_n, +_n, \cdot_n)$ a non-zero element $\bar{m}$ is a unit if and only if $\gcd(m, n) = 1$.

Proof: The ring $(\mathbb{Z}_n, +_n, \cdot_n)$ is a commutative ring with unity $\bar{1}$. Let $\bar{m}$ be a unit in the ring. Then there exists a non-zero element $\bar{u}$ in the ring such that $\bar{m} \cdot \bar{u} = \bar{1}$. $\bar{m} \cdot \bar{u} = \bar{1}$ implies, $mu \equiv 1 (\text{mod } n)$. So $mu - 1 = nv$ for some integer v, or, $mu - nv = 1$. This proves that $\gcd(m, n) = 1$.

Conversely, let $\bar{m}$ be an element in the ring such that $\gcd(m, n) = 1$. Then for some integers u and v, $um + vn = 1$. So, $um \equiv 1 (\text{mod } n)$. Clearly, $u \neq 0$. Let $u > n$, then applying division algorithm $u \equiv r (\text{mod } n)$, $0 < r < n$. $u \equiv r (\text{mod } n) \Rightarrow um \equiv rm (\text{mod } n) \Rightarrow rm \equiv 1 (\text{mod } n) \Rightarrow \bar{r} \cdot \bar{m} = \bar{1}$. Hence $\bar{m}$ is a unit.

Note: In n is prime then every non-zero element in the ring $(\mathbb{Z}_n, +_n, \cdot_n)$ is a unit.

Characteristic of a Ring: The least positive integer n (if exists) such that $na = 0 \; \forall \, a \in R$ is called characteristic of a ring R. If no such integer exists then Char $R = 0$.

Examples: Char $\mathbb{Z} = 0$, Char $\mathbb{Z}_n = n$.

Integral Domain: A commutative ring with unity which contains no divisor of zero.

Examples:

1. $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$.

2. Let $n \in \mathbb{N}$. Then $(n\mathbb{Z}, +, \cdot)$ is a commutative ring without unity not containing divisor of zero, but not an integral domain.

3. Let $n \in \mathbb{N}$. Then $(M_n(\mathbb{R}), +, \cdot)$ is the ring of all $n \times n$ real matrices. It is a non-commutative ring with unity and hence not an integral domain.

4. $(\mathbb{Z}_5, +_5, \cdot_5)$ is a commutative ring with unity [1] containing no divisor of zero. Hence it is an integral domain.

5. $(\mathbb{Z}_6, +_6, \cdot_6)$ is a commutative ring with unity [1] containing divisor of zero. Hence it is not an integral domain.

Theorem : The ring $(\mathbb{Z}_n, +_n, \cdot_n)$ is an integral domain if and only if n is prime.

Proof: Let $(\mathbb{Z}_n, +_n, \cdot_n)$ be an integral domain and n be a composite number. Then $n = pq$ where p, q are positive integers and $1 < p < n$, $1 < q < n$. Then $\bar{p}, \bar{q} \in \mathbb{Z}_n$ and $\bar{p} \cdot \bar{q} = \bar{n} = \bar{0}$. This implies that $(\mathbb{Z}_n, +_n, \cdot_n)$ contains divisor of zero which is a contradiction. Hence our hypothesis was wrong and n is prime.

Conversely, let n be a prime and the ring $(\mathbb{Z}_n, +_n, \cdot_n)$ be a commutative ring with unity $\bar{1}$. Let $\bar{m}$ be a non-zero element in the ring ($\mathbb{Z}_n$. Then $0 < m < n$. Since n is prime, $\gcd(m, n) = 1$. Then for some integers u and v, $um + vn = 1$. So, $um \equiv 1 (\text{mod } n)$. Clearly, $u \neq 0$. Let $u > n$, then applying division algorithm $u \equiv r (\text{mod } n)$, $0 < r < n$. $u \equiv r (\text{mod } n) \Rightarrow um \equiv rm (\text{mod } n) \Rightarrow rm \equiv 1 (\text{mod } n) \Rightarrow \bar{r} \cdot \bar{m} = \bar{1}$. Hence $\bar{m}$ is a unit and thus not a divisor of zero. Therefore it is an integral domain.

Theorem : The characteristic of an integral domain is either zero or prime.

Proof: Let the characteristic of an integral domain D be m. Let m be a composite number ($m \neq 1$ since D is a non-trivial ring). Then $m = pq$ where p, q are integers and $1 < p < m$, $1 < q < m$. Let I be the unity in D. Since Char$D = m$, m is the least positive integer for which $mI = 0$. But $mI = pI \cdot qI$. Since D has no divisor of zero, either $pI = 0$ or, $qI = 0$. In either case we have a contradiction since Char$D = m$. Therefore, m is prime. If there exists no such positive integer then Char$D = 0$.

Skew-field (Division ring:) A non-trivial ring with unity where every non-zero element is a unit is a skew-field.

Field: A commutative skew-field is a field.

Properties of a Field:

1. **A field is an integral domain.** Since presence of unit means divisor of zero cannot exist. Hence the property follows.

2. **A finite integral domain is a field.** Consider the commutative ring with unity $(\mathbb{Z}, +, \cdot)$ where $'+'$ and $'\cdot'$ denotes usual addition and usual multiplication and the commutative ring with unity $(\mathbb{Z}_5, +_5, \cdot_5)$. Both are Integral domains.

Since only units in $\mathbb{Z}$ are 1 and -1, whereas every non-zero element is a unit in $\mathbb{Z}_5$. Hence $\mathbb{Z}_5$ is a field.

Subring : Let $(R, +, \cdot)$ be a ring and S be a non-empty subset of R. Then S is a subring of R if and only if

(i) $a, b \in S \Rightarrow a - b \in S$

(ii) $a, b \in S \Rightarrow a \cdot b \in S$

Subfield : Let $(F, +, \cdot)$ be a field and S be a non-empty subset of F. Then S is a subfield of F if and only if

(i) $a, b \in S \Rightarrow a - b \in S$

(ii) $a \in S, b(\neq 0) \in S \Rightarrow a \cdot b^{-1} \in S$

Practice Problems:(*some are already done in class*)

1. Show that the ring of matrices $\{\begin{pmatrix} 2a & 0 \\ 0 & 2b \end{pmatrix} : a, b \in \mathbb{Z}\}$ contains divisors of zero and does not contain the unity.
2. Examine if the ring of matrices $\{\begin{pmatrix} a & b \\ 2b & a \end{pmatrix} : a, b \in \mathbb{R}\}$ contains divisors of zero.
3. Find the units in the ring of integral quaternions.
4. Prove that the ring $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$, the ring of Gaussian integers is an integral domain.
5. Prove that the ring $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Z}\}$, the ring of Gaussian integers is an integral domain.
6. Find the units in the ring $\mathbb{Z}_{10}$. Prove that the units in the ring form a cyclic group under multiplication.
7. Show that $\mathbb{Z}_2$ is an integral domain whereas the matrix ring $M_2(\mathbb{Z}_2)$ has divisors of zero.
8. Let R be a commutative ring with unity of characteristic 3. Compute and simplify $(a + b)^9$ for $a, b \in R$.

9. Let R be a commutative ring with unity of characteristic 4. Compute and simplify $(a+b)^4$ for $a, b \in R$.

10. Show that the matrix $\begin{pmatrix} 1 & 2 \\ 2 & 4 \end{pmatrix}$ is a divisor of zero in $M_2(\mathbb{Z})$.

11. Prove that the ring of matrices $\{\begin{pmatrix} a & b \\ 2b & a \end{pmatrix} : a, b \in \mathbb{Q}\}$ is a field.

12. Examine if the ring of matrices $\{\begin{pmatrix} a & b \\ 2b & a \end{pmatrix} : a, b \in \mathbb{R}\}$ is a field.

13. Prove that the set of matrices $\{\begin{pmatrix} a & b \\ 3b & a \end{pmatrix} : a, b \in \mathbb{Q}\}$ forms a field under matrix addition and matrix multiplication.

14. Let R be a ring. The centre of R is the subset $Z(R)$ defined by $Z(R) = \{x \in R : xr = rx \ \forall\, r \in R\}$. Then prove that $Z(R)$ is a subring of R.

15. Prove that $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$ is a subfield of the field R.

2 Morphisms of Groups

Let $(G, \circ)$ and $(G', \star)$ be two groups. We establish the maps that relate the two groups. Such a map gives us information about one of the groups from known structural properties of the other. If we have an isomorphism between G and G' then one is just a structural copy of the other.

Homomorphism: A mapping $\phi : G \longrightarrow G'$ is said to be a homomorphism if

$$\phi(a \circ b) = \phi(a) \star \phi(b) \text{ for all } a, b \in G.$$

Monomorphism: A one-to-one (injective) homomorphism.

Epimorphism: An onto (surjective) homomorphism.

Isomorphism: A homomorphism which is both one-to-one and onto (bijective).

Automorphism: An isomorphism from group G to itself.

Worked Examples:

1. For any groups G and G' there is always at least one homomorphism called **trivial homomorphism** defined by $\phi(a) = e_{G'}$ for all $a \in G$, $e_{G'}$ being the identity element of G'. [We have for all $a, b \in G$, $\phi(a \circ b) = e_{G'} = e_{G'} \star e_{G'} = \phi(a) \star \phi(b)$.]

2. Let $G = (\mathbb{Z}, +)$, $G' = (2\mathbb{Z}, +)$ and a mapping $\phi : G \longrightarrow G'$ be defined by $\phi(a) = 2a$, $a \in G$. Then for all $a, b \in G$, $\phi(a) = 2a$ and $\phi(b) = 2b$, $\phi(a + b) = 2(a + b) = 2a + 2b = \phi(a) + \phi(b)$. Hence ϕ is a homomorphism. Also ϕ is injective and surjective. Since $x_1 \neq x_2 \Rightarrow 2x_1 \neq 2x_2 \Rightarrow \phi(x_1) \neq \phi(x_2)$. Hence ϕ is injective. Again, let $\phi(x) = y$. Then $2x = y$, i.e., $x = \frac{y}{2}$. Since y is a multiple of 2 hence $x \in \mathbb{Z}$. Thus every image y has a pre-image $\frac{y}{2}$ in the domain of ϕ. So ϕ is surjective. Hence ϕ is an isomorphism.

3. Let $G = (\mathbb{Z}, +)$ and $\phi : G \longrightarrow G$ be defined by $\phi(a) = a + 1$, $a \in G$. Then ϕ is not a homomorphism. (Verify!)

4. Let $G = (\mathbb{Z}, +)$, $G' = (\mathbb{Z}_n, +_n)$ and a mapping $\phi : G \longrightarrow G'$ be defined by $\phi(a) = \overline{a}$, $a \in G$. Then $\phi(a + b) = \overline{a + b} = \overline{a} +_n \overline{b} = \phi(a) +_n \phi(b)$. Hence ϕ is a homomorphism.

Properties of Homomorphism: Let $(G, \circ)$ and $(G', \star)$ be two groups and a mapping $\phi : G \longrightarrow G'$ is a homomorphism. Then

1. $\phi(e_G) = e_{G'}$
2. $\phi(a^{-1}) = \{\phi(a)\}^{-1}$ for all $a \in G$
3. if $a \in G$ then $\phi(a^n) = \{\phi(a)\}^n, n$ being an integer.
4. if $a \in G$ and $O(a)$ is finite then $O(\phi(a))$ is a divisor of $o(a)$.
5. $\phi(G)$ is a subgroup of G'.
6. if G is commutative then $\phi(G)$ is commutative.
7. if G is cyclic then $\phi(G)$ is cyclic.

Kernel of ϕ : Let $(G, \circ)$ and $(G', \star)$ be two groups and a mapping $\phi : G \longrightarrow G'$ is a homomorphism. Then the kernel of ϕ(denoted by $ker\,\phi$) is a subset of G defined by $ker\,\phi = \{a \in G : \phi(a) = e_{G'}\}$.

Theorem : $ker\,\phi$ is a normal subgroup of G.

Proof : $ker\,\phi$ is a non-empty set since $\phi(e_G) = e_{G'}$, i.e., $e_G \in ker\,\phi$. Let $a, b \in ker\,\phi$. Then $\phi(a \circ b^{-1}) = \phi(a) \star \{\phi(b)\}^{-1} = e_{G'} \star {e_{G'}}^{-1} = e_{G'}$. This implies $a \circ b^{-1} \in ker\,\phi$. Thus, $ker\,\phi$ is a subgroup of G.

Let $g \in G$, $h \in ker\,\phi$. Then $\phi(g \circ h \circ g^{-1}) = \phi(g) \star \phi(h) \star \{\phi(g)\}^{-1} = \phi(g) \star \{\phi(g)\}^{-1} = \phi(g \circ g^{-1}) = \phi(e_G) = e_{G'}$. Thus $g \circ h \circ g^{-1} \in ker\,\phi$. Thus $ker\,\phi$ is a normal subgroup of G.

Theorem : Let $(G, \circ)$ and $(G', \star)$ be two groups and a mapping $\phi : G \longrightarrow G'$ is an epimorphism. Then ϕ is an isomorphism if and only if $ker\,\phi = \{e_G\}$.

Theorem : Let $(G, \circ)$ and $(G', \star)$ be two groups and a mapping $\phi : G \longrightarrow G'$ is an isomorphism. Then

(i) G' is commutative if and only if G is commutative.

(ii) G' is cyclic if and only if G is cyclic.

(iii) ϕ^{-1} is also an isomorphism.

First Isomorphism Theorem: Let f be a homomorphism of a group G onto an another group G_1. Then $G/ker\,f \backsimeq f(G)$.

Practice Problems:

1. Let $G = S_3$, $G' = (\{1, -1\}, \cdot)$ and let $\phi : G \longrightarrow G'$ be defined by

$$\phi(\alpha) = 1 \text{ if } \alpha \text{ is an even permutation in } S_3$$
$$= -1 \text{ if } \alpha \text{ is an odd permutation in } S_3$$

   Examine if ϕ is a homomorphism. (*done in class*)

2. Show that $(\mathbb{Z}, +)$ and $(\mathbb{Q}, +)$ are not isomorphic. (*done in class*)

3. Let $G = (\mathbb{Z}_5, +)$ and $\phi : G \longrightarrow G$ be defined by $\phi(\bar{x}) = 3\bar{x}$. Show that ϕ is an isomorphism.

4. Show that $8\mathbb{Z}/72\mathbb{Z} \cong \mathbb{Z}_9$.

5. Prove that $\mathbb{Z}_8$ is not a homomorphic image of $\mathbb{Z}_{15}$.