§3.4 Isomorphisms

Shaoyun Yi

MATH 546/701I

University of South Carolina

Summer 2021

Review

- Group: abelian v.s. nonabelian & finite v.s. infinite
- Subgroup
  - cyclic ($\rightsquigarrow$ abelian): $|\langle a\rangle| = o(a)$; If $o(a) < \infty$, then $a^k = e \Leftrightarrow o(a)|k$.
  - **Lagrange's Theorem:** If $|G| = n < \infty$ and $H \subseteq G$, then $|H|\big|n$.
    - $o(a)|n$ for any $a \in G$.
    - Any group of prime order is cyclic.
- Constructing (sub)groups
  - $H \cap K$ is the largest subgroup contained in both H and K.
  - Product of two subgroups: HK is not always a subgroup of G.
    - If $h^{-1}kh \in K$ for all $h \in H$ and $k \in K$, then HK is a subgroup of G. And HK is the smallest subgroup containing both H and K.
    - $|HK| = |H||K|/|H \cap K|$ if G is a finite group.
  - Direct product: $G_1 \times G_2$ is a group under the operation $(*, \cdot)$.
    - $o\big((a_1, a_2)\big) = [o(a_1), o(a_2)]$
    - $|G_1 \times G_2| = |G_1| \cdot |G_2|$ if G_1, G_2 are finite groups.
    - $\mathbf{Z}_n \times \mathbf{Z}_m$ is cyclic $\Leftrightarrow \gcd(n, m) = 1$.
  - Subgroup generated by S: $\langle S\rangle$ is the smallest subgroup that contains S.
  - Field F: New groups defined over F.

Examples: Group Table in G with $|G| = 2$ or 3

Consider the group tables of the subgroup $\{\pm 1\}$ of $\mathbf{Q}^\times$ and the group $\mathbf{Z}_2$.

Multiplication in $\{\pm 1\}$

$\times$	1	-1
1	1	-1
-1	-1	1

Addition in $\mathbf{Z}_2$

$+$	$[0]$	$[1]$
$[0]$	$[0]$	$[1]$
$[1]$	$[1]$	$[0]$

Group table in G with $|G| = 2$

$*$	e	a
e	e	a
a	a	e

Group table in G with $|G| = 3$

$*$	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

In fact, G is cyclic, i.e. $b = a^2$

All groups with order 2 (or 3) must have the same algebraic properties.

Group Isomorphism

Let $(G_1, *)$ and $(G_2, \cdot)$ be two groups, and let $\phi : G_1 \to G_2$ be a function. Then ϕ is said to be a **group isomorphism** if

i) ϕ is one-to-one and onto, and

ii) $\phi(a * b) = \phi(a) \cdot \phi(b)$ for all $a, b \in G_1$.

In this case, G_1 is said to be **isomorphic** to G_2, and we write $G_1 \cong G_2$.

To prove that two groups are **isomorphic**, you need to

1) **define a function** ϕ (well-defined), and then
2) **verify** that ϕ is a **group isomorphism**.

Sometimes your first guess for ϕ is might not work, so you might need to try several different functions until you find one satisfying the requirements

Properties of Group Isomorphisms

Let $(G_1, *)$ and $(G_2, \cdot)$ be groups, and let $\phi : G_1 \to G_2$ be an isomorphism. Let e_1 and e_2 be the identity elements of G_1 and G_2, respectively. Then

i) $\phi(e_1) = e_2$.

ii) $\phi(a^{-1}) = \big(\phi(a)\big)^{-1}$ for all $a \in G_1$.

iii) $\phi(a^n) = \big(\phi(a)\big)^n$ for all $a \in G_1$ and all $n \in \mathbf{Z}$.

Proof: i) $\phi(e_1) \cdot \phi(e_1) = \phi(e_1 * e_1) = \phi(e_1) = \phi(e_1) \cdot e_2 \rightsquigarrow \phi(e_1) = e_2$

ii) $\phi(a^{-1}) \cdot \phi(a) = \phi(a^{-1} * a) = \phi(e_1) \overset{\text{i)}}{=} e_2 \rightsquigarrow \phi(a^{-1}) = \big(\phi(a)\big)^{-1}$

iii) By induction, we have

$$\phi(a_1 * a_2 * \cdots * a_n) = \phi(a_1) \cdot \phi(a_2) \cdot \ldots \cdot \phi(a_n) \quad \text{for } a_1, a_2, \ldots, a_n \in G_1.$$

In particular, $\phi(a^n) = \big(\phi(a)\big)^n$ for any positive integer n. Furthermore,

$$\phi(a^n) = \big(\phi(a)\big)^n \quad \text{for all } n \in \mathbf{Z}.$$

For $n < 0, n = -|n| \rightsquigarrow \phi(a^n) = \phi\big((a^{-1})^{|n|}\big) = \big(\phi(a^{-1})\big)^{|n|} \overset{\text{ii)}}{=} ((\phi(a))^{-1})^{|n|}$.

Any group isomorphism preserves general products, the identity and inverses.

Example

$$\phi\colon (G_1, *, e_1) \xrightarrow{\cong} (G_2, \cdot, e_2) \begin{cases} \phi \text{ is one-to-one and onto, } \textit{and} \\ \phi(a * b) = \phi(a) \cdot \phi(b) \text{ for all } a, b \in G_1. \end{cases}$$

ϕ preserves general products, the identity element and inverses of elements.

To prove $G_1 \cong G_2$, you need to $\begin{cases} \textbf{define } \phi \text{ (well-defined), and then} \\ \textbf{verify} \text{ that } \phi \text{ is an isomorphism.} \end{cases}$

Prove that $(\mathbf{R}, +) \cong (\mathbf{R}^+, \cdot)$.

Proof: We need a function $\phi : \mathbf{R} \to \mathbf{R}^+$ that has the following properties:

- sends real numbers to positive real numbers
- sends **addition** to **multiplication**
- sends the identity $e_1 = 0$ of $(\mathbf{R}, +)$ to the identity $e_2 = 1$ of $(\mathbf{R}^+, \cdot)$

$\boxed{\text{Try } \phi(x) = e^x}$ i) $\phi(x) = e^x > 0$ for all $x \in \mathbf{R}$. That is, $\phi(x) \in \mathbf{R}^+$.

ii) ϕ is one-to-one ($e^{x_1} = e^{x_2} \rightsquigarrow x_1 = x_2$) and onto (for any $y \in \mathbf{R}^+$, take $x = \ln y \in \mathbf{R}$). iii) $\phi(x_1 + x_2) = e^{x_1 + x_2} = e^{x_1} \cdot e^{x_2} = \phi(x_1) \cdot \phi(x_2)$. $\square$

More Properties of Isomorphisms

$$\phi\colon (G_1, *, e_1) \xrightarrow{\cong} (G_2, \cdot, e_2) \begin{cases} \phi \text{ is one-to-one and onto, } \textit{and} \\ \phi(a * b) = \phi(a) \cdot \phi(b) \text{ for all } a, b \in G_1. \end{cases}$$

i) The inverse of a group isomorphism is a group isomorphism.
ii) The composite of two group isomorphisms is a group isomorphism.

Proof: i) Let $\phi : G_1 \to G_2$ be a group isomorphism. Then there is an inverse function $\theta : G_2 \to G_1$. To show that θ is a group isomorphism.

• θ is one-to-one and onto. ✓

• Let $a_2, b_2 \in G_2$ and $\theta(a_2) = a_1,\ \theta(b_2) = b_1$. $\rightsquigarrow \phi(a_1) = a_2,\ \phi(b_1) = b_2$.
So $\phi(a_1 * b_1) = \phi(a_1) \cdot \phi(b_1) = a_2 \cdot b_2 \rightsquigarrow \theta(a_2 \cdot b_2) = a_1 * b_1 = \theta(a_2) * \theta(b_2)$

ii) Let $\phi : (G_1, *) \to (G_2, \cdot)$ and $\psi : (G_2, \cdot) \to (G_3, \star)$ be isomorphisms.
$\rightsquigarrow \psi\phi$ is one-to-one and onto. To show $\psi\phi$ preserves products. If $a, b \in G_1$

$$\psi\phi(a * b) = \psi(\phi(a*b)) = \psi(\phi(a)\cdot\phi(b)) = \psi(\phi(a)) \star \psi(\phi(b)) = \psi\phi(a) \star \psi\phi(b)$$

The isomorphism $\cong$ is an equivalence relation. (Reflexive, Symmetric, Transitive)

Example 1

Prove $(\langle i\rangle, \cdot) \cong (\mathbf{Z}_4, +_{[\,]})$. Recall $\langle i\rangle = \{1, i, -1, -i\}$, $\mathbf{Z}_4 = \{[0],[1],[2],[3]\}$

We have seen that both $(\langle i\rangle, \cdot)$ and $(\mathbf{Z}_4, +_{[\,]})$ are cyclic groups of order 4.

$\cdot$	1	i	-1	$-i$
1	1	i	-1	$-i$
i	i	-1	$-i$	1
-1	-1	$-i$	1	i
$-i$	$-i$	1	i	-1

$\cdot$	i^0	i^1	i^2	i^3
i^0	i^0	i^1	i^2	i^3
i^1	i^1	i^2	i^3	i^0
i^2	i^2	i^3	i^0	i^1
i^3	i^3	i^0	i^1	i^2

$+_{[\,]}$	[0]	[1]	[2]	[3]
[0]	[0]	[1]	[2]	[3]
[1]	[1]	[2]	[3]	[0]
[2]	[2]	[3]	[0]	[1]
[3]	[3]	[0]	[1]	[2]

The elements of $\mathbf{Z}_4$ appear in the addition table in $\mathbf{Z}_4$ precisely the **same positions** as the exponents of i did in the multiplication table in $\langle i\rangle$.

Define $\phi : \mathbf{Z}_4 \to \langle i\rangle$ by $\phi([n]) = i^n$. To show ϕ is a group isomorphism.

- Well-defined: If $[n] = [m]$, i.e., $n \equiv m \pmod 4$, then $i^n = i^m$. [Why?]
- ϕ is one-to-one and onto. ✓
- ϕ preserves the respective operations:
  $\phi([n]+[m]) = \phi([n+m]) = i^{n+m} = i^n \cdot i^m = \phi([n]) \cdot \phi([m])$. □

Example 2

Let H be a subgroup of a group G. For any a in G, we have $aHa^{-1} \cong H$.

We have already showed that aHa^{-1} is a subgroup of G in §3.2.

Proof: Define $\phi : H \to aHa^{-1}$ by $\phi(h) = aha^{-1}$ for all $h \in H$.

- Well-defined: It is easy to see that $\phi(h) \in aHa^{-1}$.
- one-to-one: $\phi(h_1) = \phi(h_2) \rightsquigarrow ah_1a^{-1} = ah_2a^{-1} \rightsquigarrow h_1 = h_2$
- onto: If $y \in aHa^{-1}$, then $y = aha^{-1}$ for some $h \in H$. Thus $\phi(h) = y$.
- ϕ respects multiplication in H: For $h, k \in H$,

$$\phi(hk) = ahka^{-1} = ah(a^{-1}a)ka^{-1} = (aha^{-1})(aka^{-1}) = \phi(h)\phi(k).$$

Thus, ϕ is a group isomorphism. $\square$

Another way to show that ϕ is one-to-one and onto

Define a function $\phi^{-1}: G_2 \to G_1$, and **verify** that ϕ^{-1} is the inverse of ϕ.

That is, need to check $\quad \phi^{-1} \circ \phi = 1_{G_1} \quad$ and $\quad \phi \circ \phi^{-1} = 1_{G_2}$.

Recall that $(\mathbf{R}, +) \cong (\mathbf{R}^+, \cdot)$: We define $\phi\colon \mathbf{R} \to \mathbf{R}^+$ by letting $\phi(x) = e^x$.

To show ϕ is one-to-one and onto, define $\phi^{-1}: \mathbf{R}^+ \to \mathbf{R}$ by $\phi^{-1}(y) = \ln y$.

- Well-defined ✓
- **Verify** that this is the inverse function of ϕ:

$$\phi(\phi^{-1}(y)) = \phi(\ln y) = e^{\ln y} = y, \quad \phi^{-1}(\phi(x)) = \phi^{-1}(e^x) = \ln e^x = x.$$

Recall $aHa^{-1} \cong H$: We define $\phi\colon H \to aHa^{-1}$ by letting $\phi(h) = aha^{-1}$.

To show that ϕ is one-to-one and onto, we define $\phi^{-1}: aHa^{-1} \to H$ by

$$\phi^{-1}(b) = a^{-1}ba \quad \text{for all } b \in aHa^{-1}. \quad (\text{Well-defined ✓})$$

Verify that this is the inverse function of ϕ:

$$\phi(\phi^{-1}(b)) = \phi(a^{-1}ba) = a(a^{-1}ba)a^{-1} = b$$
$$\phi^{-1}(\phi(h)) = \phi^{-1}(aha^{-1}) = a^{-1}(aha^{-1})a = h$$

Some Structural Properties Preserved by Isomorphisms

Let $\phi : G_1 \to G_2$ be an isomorphism of groups.

i) If a has order n in G_1, then $\phi(a)$ has order n in G_2.

ii) If G_1 is abelian, then so is G_2.

iii) If G_1 is cyclic, then so is G_2.

Proof: i) Assume $a \in G_1$ with $a^n = e_1$. So $(\phi(a))^n = \phi(a^n) = \phi(e_1) = e_2$. $\rightsquigarrow o(\phi(a))|n$. To show $n|o(\phi(a))$: Since ϕ is an isomorphism, there exists ϕ^{-1} s.t. $\phi^{-1}(\phi(a)) = a$. So $a^{o(\phi(a))} = \phi^{-1}(\phi(a))^{o(\phi(a))} = \phi^{-1}(e_2) = e_1$ ✓.

ii) Let $\phi(a_1) = a_2$ and $\phi(b_1) = b_2$ for $a_1, b_1 \in G_1$ and $a_2, b_2 \in G_2$. Then

$a_2 \cdot b_2 = \phi(a_1) \cdot \phi(b_1) = \phi(a_1 * b_1) \overset{!}{=} \phi(b_1 * a_1) = \phi(b_1) \cdot \phi(a_1) = b_2 \cdot a_2$.

iii) Suppose G_1 is cyclic with $G_1 = \langle a \rangle$. For any $y \in G_2$, we have $y = \phi(x)$ for some $x \in G_1$. Write $x = a^n$ for some $n \in \mathbf{Z}$. Then

$$y = \phi(x) = \phi(a^n) = (\phi(a))^n.$$

Thus G_2 is cyclic, generated by $\phi(a)$. $\square$

This gives us a technique for proving that two groups are **not isomorphic**.

Examples: Prove that two Groups are NOT Isomorphic.

$$\phi : G_1 \xrightarrow{\cong} G_2 \begin{cases} \text{If } a \text{ has order } n \text{ in } G_1, \text{ then } \phi(a) \text{ has order } n \text{ in } G_2. \\ \text{If } G_1 \text{ is abelian (resp. cyclic), then so is } G_2. \end{cases}$$

$(\mathbf{R}, +) \ncong (\mathbf{R}^\times, \cdot)$

In $(\mathbf{R}^\times, \cdot)$, there is an element of order 2, namely, -1.
In $(\mathbf{R}, +)$, there is no element of order 2. (If so, $2x = 0 \rightsquigarrow x = 0$) □

$(\mathbf{R}^\times, \cdot) \ncong (\mathbf{C}^\times, \cdot)$

In $(\mathbf{R}^\times, \cdot)$, only 1 and -1 have finite orders, i.e., $o(1) = 1$ and $o(-1) = 2$.
In $(\mathbf{C}^\times, \cdot)$, there are elements of other finite orders. e.g., $o(i) = 4$. □

$\mathbf{Z}_4 \ncong \mathbf{Z}_2 \times \mathbf{Z}_2$

$\mathbf{Z}_4$ is cyclic. That is, there is an element ($[1]_4$ or $[3]_4$) of order 4 in $\mathbf{Z}_4$.
$\mathbf{Z}_2 \times \mathbf{Z}_2$ is not cyclic. Any non-identity element must have order 2. □

$\mathbf{Z}_9 \times \mathbf{Z}_9 \ncong \mathbf{Z}_3 \times \mathbf{Z}_3 \times \mathbf{Z}_3 \times \mathbf{Z}_3$

In the 1st group, there are elements of order 9. e.g., $([1]_9, [1]_9)$.
In the 2nd group, any non-identity element must have order 3. □

Examples: Groups of Order 6: S_3, $\mathrm{GL}_2(\mathbf{Z}_2)$, $\mathbf{Z}_6$, $\mathbf{Z}_2 \times \mathbf{Z}_3$

- The first two groups (S_3 and $\mathrm{GL}_2(\mathbf{Z}_2)$) are nonabelian.
- The last two groups ($\mathbf{Z}_6$ and $\mathbf{Z}_2 \times \mathbf{Z}_3$) are abelian (in fact, cyclic).

$$\mathbf{Z}_6 \cong \mathbf{Z}_2 \times \mathbf{Z}_3$$

Proof: Let $\mathbf{Z}_6 = \langle [1]_6 \rangle, \mathbf{Z}_2 \times \mathbf{Z}_3 = \langle [1]_2, [1]_3 \rangle$. Define $\phi : \mathbf{Z}_6 \to \mathbf{Z}_2 \times \mathbf{Z}_3$ by

$$\phi([1]_6) = ([1]_2, [1]_3).$$

And so $\phi([n]_6) = \phi(n[1]_6) = n\phi([1]_6) = n([1]_2, [1]_3) = ([n]_2, [n]_3)$.

• well-defined: If $[n_1]_6 = [n_2]_6$, then $[n_1]_2 = [n_2]_2$ and $[n_1]_3 = [n_2]_3$. ✓

• one-to-one: For $([n_1]_2, [n_1]_3) = ([n_2]_2, [n_2]_3)$, to show $[n_1]_6 = [n_2]_6$.
We have $2|(n_1 - n_2)$ and $3|(n_1 - n_2)$. $\rightsquigarrow$ $6|(n_1 - n_2)$ since $\gcd(2,3) = 1$. ✓

• Since $|\mathbf{Z}_6| = |\mathbf{Z}_2 \times \mathbf{Z}_3| = 6$, any one-to-one mapping must be onto. ✓

• For any $m, n \in \mathbf{Z}$, $\phi([n]_6 + [m]_6) = \phi([n+m]_6) = ([n+m]_2, [n+m]_3) = ([n]_2 + [m]_2, [n]_3 + [m]_3) = ([n]_2, [n]_3)([m]_2, [m]_3) = \phi([n]_6)\phi([m]_6)$. $\square$

Prove that $\mathrm{GL}_2(\mathbf{Z}_2) \cong S_3$

In §3.3, we described S_3 by letting $e = (1), a = (123)$ and $b = (12)$ and so

$$S_3 = \{e, a, a^2, b, ab, a^2 b\}, \quad \text{where } a^3 = e,\ b^2 = e,\ ba = a^2 b.$$

Also in §3.3, we saw that those 6 elements in $\mathrm{GL}_2(\mathbf{Z}_2)$ and their orders are

$$\begin{array}{ccccccc} & \left[\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right] & \left[\begin{smallmatrix}1&1\\1&0\end{smallmatrix}\right] & \left[\begin{smallmatrix}0&1\\1&1\end{smallmatrix}\right] & \left[\begin{smallmatrix}0&1\\1&0\end{smallmatrix}\right] & \left[\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right] & \left[\begin{smallmatrix}1&0\\1&1\end{smallmatrix}\right] \\ \text{order} & 1 & 3 & 3 & 2 & 2 & 2 \end{array}$$

To establish the connection between S_3 and $\mathrm{GL}_2(\mathbf{Z}_2)$, let

$$e = \left[\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right],\ a = \left[\begin{smallmatrix}1&1\\1&0\end{smallmatrix}\right],\ b = \left[\begin{smallmatrix}0&1\\1&0\end{smallmatrix}\right]. \quad \rightsquigarrow a^3 = e,\ b^2 = e,\ ba = a^2 b$$

Each element of $\mathrm{GL}_2(\mathbf{Z}_2)$ can be expressed uniquely as one of e, a, a^2, b, ab, a^2b.

Let $\phi((123)) = \left[\begin{smallmatrix}1&1\\1&0\end{smallmatrix}\right]$, $\phi((12)) = \left[\begin{smallmatrix}0&1\\1&0\end{smallmatrix}\right]$ and extend this to all elements by

$$\phi((123)^i(12)^j) = \left[\begin{smallmatrix}1&1\\1&0\end{smallmatrix}\right]^i \left[\begin{smallmatrix}0&1\\1&0\end{smallmatrix}\right]^j \quad \text{for } i = 0, 1, 2 \text{ and } j = 0, 1.$$

ϕ is a group isomorphism.

The unique forms of the respective elements show ϕ is one-to-one and onto

The multiplication tables are identical shows ϕ respects the two operations.

An easier way to check that ϕ which preserves products is one-to-one

Let $\phi : G_1 \to G_2$ be a function s.t. $\phi(a * b) = \phi(a) \cdot \phi(b)$ for all $a, b \in G_1$. Then ϕ is one-to-one if and only if $\phi(x) = e_2$ implies $x = e_1$ for all $x \in G_1$.

Proof: $(\Rightarrow)$ If ϕ is one-to-one, then only e_1 can map to e_2.

$(\Leftarrow)$ For $\phi(x_1) = \phi(x_2)$ for some $x_1, x_2 \in G_1$, to show $x_1 = x_2$.

$\phi(x_1 * x_2^{-1}) = \phi(x_1) \cdot \phi(x_2^{-1}) = \phi(x_1) \cdot (\phi(x_2))^{-1} = \phi(x_2) \cdot (\phi(x_2))^{-1} = e_2$

$\rightsquigarrow x_1 * x_2^{-1} = e_1$ (by assumption), and thus $x_1 = x_2$. $\square$

$$\mathbf{Z}_{mn} \cong \mathbf{Z}_m \times \mathbf{Z}_n \quad \text{if } \gcd(m, n) = 1.$$

Proof: Recall that (in §3.3) $\mathbf{Z}_m \times \mathbf{Z}_n$ is cyclic if and only if $\gcd(m, n) = 1$.

Define $\phi \colon \mathbf{Z}_{mn} \to \mathbf{Z}_m \times \mathbf{Z}_n$ by $\phi([x]_{mn}) = ([x]_m, [x]_n)$. Show ϕ is an isomorphism.

- well-defined: If $[x]_{mn} = [y]_{mn}$, then $[x]_m = [y]_m$ and $[x]_n = [y]_n$. ✓
- For $x, y \in \mathbf{Z}$, $\phi([x]_{mn} + [y]_{mn}) = \phi([x + y]_{mn}) = ([x + y]_m, [x + y]_n) = ([x]_m + [y]_m, [x]_n + [y]_n) = ([x]_m, [x]_n)([y]_m, [y]_n) = \phi([x]_{mn})\phi([y]_{mn})$ ✓
- one-to-one: $\phi([x]_{mn}) = ([0]_m, [0]_n) \rightsquigarrow m|x, n|x \rightsquigarrow mn|x \rightsquigarrow [x]_{mn} = [0]_{mn}$ ✓
- Since $|\mathbf{Z}_{mn}| = |\mathbf{Z}_m \times \mathbf{Z}_n|$, any one-to-one mapping must be onto. $\square$

Example

Show that the group $G_1 = \{f_{m,b} : \mathbf{R} \to \mathbf{R} \mid f_{m,b}(x) = mx + b, m \neq 0\}$ of affine functions under composition of functions is isomorphic to the group

$$G_2 = \left\{ \begin{bmatrix} m & b \\ 0 & 1 \end{bmatrix} : m \neq 0 \right\} \quad \text{under matrix multiplication.}$$

Define $\phi : G_1 \to G_2$ by $\phi(f_{m,b}) = \begin{bmatrix} m & b \\ 0 & 1 \end{bmatrix}$. To show ϕ is an isomorphism.

well-defined: For $f_{m,b} \in G_1$, we have $\phi(f_{m,b}) \in G_2$ since $m \neq 0$. ✓

For any $f_{m_1,b_1}, f_{m_2,b_2} \in G_1$, to show $\phi(f_{m_1,b_1} \circ f_{m_2,b_2}) = \phi(f_{m_1,b_1})\phi(f_{m_2,b_2})$.

For any $x \in \mathbf{R}$, we have $f_{m_1,b_1} \circ f_{m_2,b_2}(x) = \cdots = m_1 m_2 x + (m_1 b_2 + b_1)$.

$\rightsquigarrow$ $\phi(f_{m_1,b_1} \circ f_{m_2,b_2}) = \phi(f_{m_1 m_2, m_1 b_2 + b_1}) = \begin{bmatrix} m_1 m_2 & m_1 b_2 + b_1 \\ 0 & 1 \end{bmatrix}$;

Also $\phi(f_{m_1,b_1})\phi(f_{m_2,b_2}) = \begin{bmatrix} m_1 & b_1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} m_2 & b_2 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} m_1 m_2 & m_1 b_2 + b_1 \\ 0 & 1 \end{bmatrix}$. ✓

one-to-one: $\phi(f_{m,b}) = \begin{bmatrix} m & b \\ 0 & 1 \end{bmatrix} = e_2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \rightsquigarrow m = 1, b = 0$. To show $f_{1,0} = e_1$

$$f_{1,0} \circ f_{m,b}(x) = f_{1,0}(mx + b) = mx + b \overset{\checkmark}{=} f_{m,b}(x); \quad f_{m,b} \circ f_{1,0}(x) \overset{\checkmark}{=} f_{m,b}(x)$$

onto: It is obvious by definition of ϕ. $\square$