Reading: Sections 2 and 3. Start Section 4 if possible.

Section 2 Problems: You should be able to work out all problems.

- Note that the T/F problems (24, 27-35) are could appear in either Tu/Th quizzes. They could appear on a Tuesday quiz because they can be used to check whether you know a definition, e.g., 24a, 24e or 24g-j. Problems 14-16 are more directly related to checking your knowledge of definitions, so more likely to appear on a Tuesday quiz.
- Problems 5-6 can be followed by 12-13. Problems 12-13 have to do with *counting*. (Problems 23-27 in Section 0 also had to do with counting. A general question hidden behind that suite of exercises asks *how many distinct ways are there to partition a set of n elements*.) There is a very broad umbrella term for a variety of subfields that study and apply counting techniques, called *combinatorics*. Check out our UWL Faculty by Research Interest page to see whether we have any faculty who specialize in such areas.

Section 3 Problems: You should be able to work out all problems, except the following problems that you may skip: 20, 23, 24-25, 28, 34.

- That said, I strongly encourage you to try 23 and 24-25. More than the problems themselves, these provide great examples of learning techniques that you should try and apply throughout the course. For instance, problem 23 asks for a **proof synopsis**, something that you should attempt to generate for every theorem/result in the course. Problems 24-25 give an example of taking a given concept (that of an **identity**), looking at its definition closely, and then trying to vary it to form new (sub)concepts. Next, it takes the new (sub)concepts and investigates how they are related to the previous concept; and also whether the new (sub)concepts can be used to generate new theorems (e.g., take a theorem that uses the old concept, and try and se whether the theorem remains true with the old concept replaced with the new concept).

The following problems are **due on 11:59pm Tuesday 9/25**. Submit both LaTeX and pdf files to the appropriate D2L Dropbox.
Please name the files using the following format:

LastName_FirstName_MTH411_Fall2018_HW_2

You may discuss the problems with your classmates, but your write-up must be your own. Any problems marked with an asterisk (*) denote problems you can not discuss with anyone except for me.

Please include the statements of the problems in your HW submissions. For the Extra problems you can copy the statements from the LaTeX file that generated this pdf. However, you will have to transcribe the remaining problems from Fraleigh.

Section 2: 9-11, 14-16, 18, 20, 22, 26, 36, 37
Section 3: 6-10 ,11-13, 16-18, 21-22, 31, 33

2.09 Determine whether the binary operation $*$ defined is commutative and associative. $*$ defined on $\mathbb{Q}$ by letting $a * b = ab/2$.

Commutative: As multiplication is commutative.

$$a * b = \frac{ab}{2} = \frac{ba}{2} = b * a$$

Thus, $*$ is commutative.

Associative:

$$(a * b) * c = \frac{ab}{2} * c = \frac{\frac{ab}{2}c}{2} = \frac{abc}{4}$$

$$a * (b * c) = a * \frac{bc}{2} = \frac{\frac{bc}{2}a}{2} = \frac{abc}{4}$$

Thus, $*$ is associative

Therefore, $*$ is both commutative and associative.

2.10 Determine whether the binary operation $*$ defined is commutative and associative. $*$ defined on $\mathbb{Z}^+$ by letting $a * b = 2^{ab}$

Commutative: Let $a, b \in \mathbb{Z}^+$. Then,

$$a * b = 2^{ab} = 2^{ba} = b * a$$

Therefore, $*$ is commutative.

Associative: Let $a, b, c \in \mathbb{Z}^+$ Then,

$$(a * b) * c = 2^{ab} * c = 2^{abc}$$

$$a * (b * c) = a * 2^{bc} = 2^{abc}$$

Therefore, $*$ is associative.

Therefore, $*$ is both commutative and associative.

2.11 Determine whether the binary operation $*$ defined is commutative and associative. $*$ defined on $\mathbb{Z}^+$ by letting $a * b = a^b$.

Commutative: Let $a = 2, b = 3$. Then,

$$a * b = 2 * 3 = 2^3 = 8$$

$$b * a = 3 * 2 = 3^2 = 9$$

As $8 \neq 9$. Thus, $*$ is not commutative.

Associative: Let $a = 2, b = 3, c = 2$. Then,

$$(a * b) * c = (2 * 3) * 2 = 2^3 * 2 = 8 * 2 = 8^2 = 64$$

$$a * (b * c) = 2 * (3 * 2) = 2 * 3^2 = 2 * 9 = 2^9 = 512$$

As $64 \neq 512$. Thus, $*$ is not associative.

Therefore, $*$ is neither commutative nor associative.

For 2.14 - 2.16, correct the definition of the italicized term without reference to the text, if correction is needed, so that it is in a form acceptable for publication.

2.14 A binary operation $*$ is *commutative* if and only if $a * b = b * a$.
Corrected: A binary operation $*$ on S is *commutative* if and only if $a * b = b * a$.

2.15 A binary operation $*$ on a set S is *associative* if and only if, for all $a, b, c \in S$, we have $(b * c) * a = b * (c * a)$.
Definition for *associative* is correct as stated.

2.16 A subset H of a set S is *closed* under a binary operation $*$ on S if $(a * b) \in H$ for all $a, b \in S$.
Corrected: A subset H of a set S is *closed* under a binary operation $*$ on S if $(a * b) \in H$ for all $a, b \in H$.

For 2.18, 2.20, and 2.22, determine whether the definition of $*$ does give a binary operation on the set. In the event that $*$ is not a binary operation, state whether Condition 1, Condition 2, or both of these conditions on page 24 are violated.

Condition 1: Exactly one element is assigned to each possible ordered pair of elements of S.
Condition 2: For each ordered pair of elements of S, the element assigned to it is again in S.

2.18 On $\mathbb{Z}^+$, define $*$ by letting $a * b = a^b$
Binary operation, as exactly one element is assigned to each possible ordered pair of elements, and $a^b \in \mathbb{Z}^+$ if both $a, b \in \mathbb{Z}^+$

2.20 On $\mathbb{Z}^+$, define $*$ by letting $a * b = c$ where c is the smallest integer greater than a and b.
Binary operation, as exactly one element is assigned to each possible ordered pair of elements, as there is exactly one smallest integer greater than both a and b, and c is a positive integer if both a, b are positive integers.

2.22 On $\mathbb{Z}^+$, define $*$ by letting $a * b = c$ where c is the largest integer less than the product of a and b.
Not a binary operation, as condition 2 is violated as

$$1 * 1 = 0$$

$$0 \notin \mathbb{Z}^+$$

2.26 Prove that if $*$ is an associative and commutative binary operation on a set S, then

$$(a * b) * (c * d) = [(d * c) * a)] * b$$

for all $a, b, c, d \in S$. Assume the associative law only for triples as in the definition, that is, assume only

$$(x * y) * z = x * (y * z)$$

for all $x, y, z \in S$.

Proof. Let $a, b, c, d \in S$. Assume $*$ is an associative and commutative binary operation on a set S. Observe.

$$\begin{aligned}(a * b) * (c * d) &= (c * d) * (a * b) \text{ by commutative} \\ &= (d * c) * (a * b) \text{ by commutative} \\ &= (d * c) * a * b \text{ by associative} \\ &= [(d * c) * a)] * b \text{ by associative}\end{aligned}$$

Therefore, as $(a * b) * (c * d) = [(d * c) * a)] * b$ the statement is true. □

2.36 Suppose that $*$ is an *associative binary* operation on a set S. Let $H = \{a \in S | a * x = x * a \text{ for all } x \in S\}$. Show that H is closed under $*$.

Proof. Let $a, b \in H$. Let $x \in S$. Observe.

$$\begin{aligned}a * b * x &= a * (b * x) \\ &= a * (x * b) \\ &= a * x * b \\ &= (a * x) * b \\ &= (x * a) * b \\ &= x * a * b \\ &= x * (a * b)\end{aligned}$$

Therefore, H is closed under $*$. □

2.37 Suppose that $*$ is an associative and commutative binary operation on a set S. Show that $H = \{a \in S | a * a = a\}$ is closed under $*$.

Proof. Let $a, b \in H$. Consider

$$\begin{aligned}(a * b) * (a * b) &= a * b * a * b \\ &= a * a * b * b \\ &= (a * a) * (b * b) \\ &= a * b\end{aligned}$$

Therefore, H must be closed under $*$. □

For 3.06-3.10, determine whether the given map ϕ is an isomorphism of the first binary structure with the second. If not an isomorphism, why not?

3.06 $< \mathbb{Q}, \cdot >$ with $< \mathbb{Q}, \cdot >$ where $\phi(x) = x^2$ for $x \in \mathbb{Q}$.
Not isomorphic. Let $x = 1$ and $y = -1$ Then, $\phi(x) = 1$ and $\phi(y) = 1$. But, $x \neq y$.
Thus, ϕ is not injective.
Therefore, as ϕ fails to be bijective, ϕ is not a isomorphism.

3.07 $< \mathbb{R}, \cdot >$ with $< \mathbb{R}, \cdot >$ where $\phi(x) = x^3$ for $x \in \mathbb{R}$.

Injective: Let $a, b \in \mathbb{R}$. Notice, $\phi(a) = \phi(b)$ which implies $a^3 = b^3 \to a = b$.
Thus, ϕ is injective.

Surjective: Let $b \in \mathbb{R}$. Then, there must exist an arbitrary a such that $\phi(a) = b$. Let $a = \sqrt[3]{b}$. Then, $\phi(a) = b$
Thus, ϕ is surjective.

Let $a, b \in \mathbb{R}$.

$$\phi(a * b) = \phi(a \cdot b) = (ab)^3 = a^3 \cdot b^3 = \phi(a) \cdot \phi(b)$$

Therefore, ϕ is a homomorphism. As ϕ is a bijective homomorphism, ϕ must be isomorphic.

3.08 $< M_2(\mathbb{R}), \cdot >$ with $< \mathbb{R}, \cdot >$ where $\phi(A)$ is the determinate of matrix A.
Not isomorphic. Let $A = \begin{bmatrix} 4 & 1 \\ 2 & 2 \end{bmatrix}$ and $B = \begin{bmatrix} 2 & 2 \\ 1 & 2 \end{bmatrix}$. Then, $\det(A) = 2$ and $\det(B) = 2$. But $A \neq B$.
Thus, ϕ fails to be injective.
Thus, ϕ fails to be bijective.
Therefore, ϕ fails to be an isomorphism.

3.09 $< M_1(\mathbb{R}), \cdot >$ with $< \mathbb{R}, \cdot >$ where $\phi(A)$ is the determinate of matrix A.

Proof. Let $A = [a]$ and $B = [b]$ for some $a, b \in \mathbb{R}$. Assume $\phi(A) = \phi(B)$. Then,

$$\det(A) = \det(B)$$

$$a = b$$

Thus, ϕ is injective.

Assume $r \in \mathbb{R}$. Then, there must exist a $C \in M_1(\mathbb{R})$ such that $\phi(C) = r$.
Let $C = [r]$. Then, $\phi(C) = \det(r) = r$.
Thus, ϕ is surjective.

Let $A = [a]$ and $B = [b]$. Then,

$$\phi(A * B) = \phi([a] \cdot [b]) = \det(ab) = ab = \det(a)\det(b) = \phi(A) \cdot \phi(B)$$

Thus, ϕ is homomorphic.

Therefore, as ϕ is bijective and homomorphic, ϕ must be isomorphic. □

3.10 $< \mathbb{R}, + >$ with $< \mathbb{R}^+, \cdot >$ where $\phi(r) = .5^r$ for $r \in \mathbb{R}$.

Proof. Let $q, p \in \mathbb{R}$. Then,

$$\begin{aligned} \phi(q) &= \phi(p) \\ 0.5^q &= .5^p \\ q &= p \end{aligned}$$

Thus, ϕ is injective.

Assume $q \in \mathbb{R}^+$. Then, there must exist a $p \in \mathbb{R}$ such that $\phi(p) = q$. Let $p = \log_{0.5}(q)$. Then, $\phi(p) = q$
Thus, ϕ is surjective.
Let $p, q \in \mathbb{R}$. Then,

$$\phi(p \cdot q) = \phi(p + q) = 0.5^{p+q} = 0.5^p \cdot 0.5^q = \phi(p) \cdot \phi(q)$$

Thus, ϕ is homomorphic.

Therefore, as ϕ is bijective and homomorphic, ϕ must be isomorphic. □

For 3.11 - 3.13 let F be the set of all functions f mapping $\mathbb{R}$ into $\mathbb{R}$ that have derivatives of all orders. Determine if they are isomorphism. Why or why not?

3.11 $< F, + >$ with $< F, + >$ where $\phi(f) = f'$, the derivative of f.
Let $f = (x + 2)$ and $g = (x + 3)$. Then, $\phi(f) = 1$ and $\phi(g) = 1$. But $f \neq g$.
Thus, ϕ is not injective.
Thus, ϕ is not bijective.
Therefore, ϕ is not isomorphic.

3.12 $< F, + >$ with $< \mathbb{R}, + >$ where $\phi(f) = f'(0)$
Let $f = x^2$ and $g = x^3$. Then, $\phi(f) = 0$ and $\phi(g) = 0$. But $f \neq g$.
Thus, ϕ is not injective.
Thus, ϕ is not bijective.
Therefore, ϕ is not isomorphic.

3.13 $< F, + >$ with $< F, + >$ where $\phi(f)(x) = \int_0^x f(t)dt$ Let g be a constant function defined by $g(x) = 1 \forall x \in \mathbb{R}$ As all derivatives $n \geq 0$ are defined as $g^n(x) = 0 \forall x \in \mathbb{R}$. As g must be element in F, there must exist a function f such that $\phi(f)(x) = g(x)$. Then, $\phi(f)(x) = \int_0^x f(t)dt$. Let $x = 0$. Then, $\phi(f)(0) = \int_0^0 f(t)dt = 0$ and $g(0) = 1$. Thus, $\phi(f) \neq g$. Thus, ϕ is not surjective.
Therefore, ϕ is not an isomorphism.

3.16 The map $\phi : \mathbb{Z} \to \mathbb{Z}$ defined by $\phi(n) = n + 1$ for $n \in \mathbb{Z}$ is one to one and onto $\mathbb{Z}$. Give the definition of a binary operation $*$ on $\mathbb{Z}$ such that ϕ is an isomorphism mapping.

3.16a $< \mathbb{Z}, + >$ onto $< \mathbb{Z}, * >$ As ϕ is a bijection, we need to define $*$ such that ϕ is a homomorphism. That is $\phi(m+n) = \phi(m) * \phi(n)$ for $m, n \in \mathbb{Z}$ Let $*$ be defined as $m * n = m + n - 1$ for $m, n \in \mathbb{Z}$. Using this definition, let $m, n \in \mathbb{Z}$

$$\phi(m+n) = m + n + 1$$

and

$$\begin{aligned} \phi(m) * \phi(n) &= (m+1) * (n+1) \\ &= (m+1) + (n+1) + 1 - 1 \\ &= m + n + 1 + 1 - 1 \\ &= m + n + 1 \end{aligned}$$

Thus, $\phi(m+n) = \phi(m) * \phi(n)$ which makes ϕ homomorphic.
Therefore, ϕ is an isomorphism.

As 1 is the identity element of $\mathbb{Z}$ under multiplication, and ϕ is an isomorphism, $\phi(1)$ maps to the identity element of $\mathbb{Z}$ under $*$. $\phi(1) = 1 + 1 = 2$. Therefore, the identity element of $\mathbb{Z}$ under $*$ is 2

3.16b $< \mathbb{Z}, * >$ onto $< \mathbb{Z}, + >$ As ϕ is a bijection, we need to define $*$ such that ϕ is a homomorphism. That is $\phi(m+n) = \phi(m) * \phi(n)$ for $m, n \in \mathbb{Z}$ Let $*$ be defined as $m * n = m + n + 1$ for $m, n \in \mathbb{Z}$. Using this definition, let $m, n \in \mathbb{Z}$

$$\phi(m) + \phi(n) = (m+1) + (n+1) = m + n + 2$$

and

$$\begin{aligned} \phi(m * n) &= (m * n) + 1 \\ &= (m + n + 1) + 1 \\ &= m + n + 1 + 1 - 1 \\ &= m + n + 2 \end{aligned}$$

Thus, $\phi(m * n) = \phi(m) + \phi(n)$ which makes ϕ homomorphic.
Therefore, ϕ is an isomorphism.

As 1 is the identity element of $\mathbb{Z}$ under multiplication, and ϕ is an isomorphism, ϕ must map to the identity element of $\mathbb{Z}$ under $*$ to 1. Let i be the identity of $< \mathbb{Z}, * >$. $\phi(i) = 1 = i + 1$. Thus, $i = 0$ Therefore, the identity element of $\mathbb{Z}$ under $*$ is 0

3.17 The map $\phi : \mathbb{Z} \to \mathbb{Z}$ defined by $\phi(n) = n + 1$ for $n \in \mathbb{Z}$ is one to one and onto $\mathbb{Z}$. Give the definition of a binary operation $*$ on $\mathbb{Z}$ such that ϕ is an isomorphic mapping.

3.17a $< \mathbb{Z}, \cdot >$ onto $< \mathbb{Z}, * >$ As ϕ is a bijection, we need to define $*$ such that ϕ is a homomorphism. That is $\phi(mn) = \phi(m) * \phi(n)$ for $m, n \in \mathbb{Z}$ Let $*$ be defined as $m * n = mn - n - m + 2$ for $m, n \in \mathbb{Z}$. Using this definition, let $m, n \in \mathbb{Z}$

$$\phi(mn) = mn + 1$$

and

$$\begin{aligned}\phi(m) * \phi(n) &= (m+1) * (n+1) \\ &= (mn + m + n + 1) - m - 1 - n - 1 + 2 \\ &= mn + 1\end{aligned}$$

Thus, $\phi(mn) = \phi(m) * \phi(n)$ which makes ϕ homomorphic.
Therefore, ϕ is an isomorphism.

As 1 is the identity element of $\mathbb{Z}$ under multiplication, and ϕ is an isomorphism, $\phi(1)$ maps to the identity element of $\mathbb{Z}$ under $*$. $\phi(1) = 1 + 1 = 2$. Therefore, the identity element of $\mathbb{Z}$ under $*$ is 2

3.17b $< \mathbb{Z}, * >$ onto $< \mathbb{Z}, \cdot >$ As ϕ is a bijection, we need to define $*$ such that ϕ is a homomorphism. That is $\phi(m * n) = \phi(m) \cdot \phi(n)$ for $m, n \in \mathbb{Z}$ Let $*$ be defined as $m * n = mn + m + n$ for $m, n \in \mathbb{Z}$. Using this definition, let $m, n \in \mathbb{Z}$

$$\phi(m)\phi(n) = (m+1)(n+1) = mn + m + n + 1$$

and

$$\phi(m * n) = mn + m + n + 1$$

Thus, $\phi(m * n) = \phi(m)\phi(n)$ which makes ϕ homomorphic.
Therefore, ϕ is an isomorphism.

As 1 is the identity element of $\mathbb{Z}$ under multiplication, and ϕ is an isomorphism, ϕ must map to the identity element of $\mathbb{Z}$ under $*$ to 1. Let i be the identity of $< \mathbb{Z}, * >$. $\phi(i) = 1 = i + 1$. Thus, $i = 0$ Therefore, the identity element of $\mathbb{Z}$ under $*$ is 0

3.18 The map $\phi : \mathbb{Q} \to \mathbb{Q}$ defined by $\phi(x) = 3x - 1$ for $x \in \mathbb{Q}$ is one to one and onto $\mathbb{Q}$. Give the definition of a binary operation $*$ on $\mathbb{Q}$ such that ϕ is an isomorphic mapping. In each case, give the identity element for $*$ on $\mathbb{Q}$.

3.18a $< \mathbb{Q}, + >$ onto $< \mathbb{Q}, * >$ As ϕ is a bijection, we need to define $*$ such that ϕ is a homomorphism. That is $\phi(x + y) = \phi(x) * \phi(y)$ for $x, y \in \mathbb{Q}$ Let $*$ be defined as $x * y = x + y + 1$ for $x, y \in \mathbb{Q}$. Using this definition, let $x, y \in \mathbb{Q}$

$$\phi(x + y) = 3(x + y) - 1 = 3x + 3y - 1$$

and

$$\phi(x) * \phi(y) = (3x - 1) + (3y - 1) + 1 = 3x + 3y - 1$$

Thus, $\phi(x + y) = \phi(x) * \phi(y)$ which makes ϕ homomorphic.
Therefore, ϕ is an isomorphism.

As 0 is the identity element of $\mathbb{Q}$ under addition, and ϕ is an isomorphism, $\phi(0)$ maps to the identity element of $\mathbb{Q}$ under $*$. $\phi(0) = 3(0) - 1 = -1$. Therefore, the identity element of $\mathbb{Q}$ under $*$ is -1

3.18b $< \mathbb{Q}, * >$ onto $< \mathbb{Q}, + >$ As ϕ is a bijection, we need to define $*$ such that ϕ is a homomorphism. That is $\phi(x * y) = \phi(x) + \phi(y)$ for $x, y \in \mathbb{Q}$ Let $*$ be defined as $x * y = x + y - \frac{1}{3}$ for $x, y \in \mathbb{Q}$. Using this definition, let $x, y \in \mathbb{Q}$

$$\phi(x) + \phi(y) = (3x - 1) + (3y - 1) = 3x + 3y - 2$$

and

$$\begin{aligned} \phi(x * y) &= 3(x * y) - 1 \\ &= 3(x + y - \frac{1}{3}) - 1 \\ &= 3x + 3y - 1 - 1 \\ &= 3x + 3y - 2 \end{aligned}$$

Thus, $\phi(x * y) = \phi(x) + \phi(y)$ which makes ϕ homomorphic.
Therefore, ϕ is an isomorphism.

As 0 is the identity element of $\mathbb{Q}$ under addition, and ϕ is an isomorphism, ϕ must map some element, i to the identity element of $\mathbb{Q}$ under addition.

$$\begin{aligned} \phi(i) &= 0 \\ 3i - 1 &= 0 \\ i &= \frac{1}{3} \end{aligned}$$

Therefore, the identity element of $\mathbb{Q}$ under $*$ is $\frac{1}{3}$

For 2.21,2.22 correct the definition of the italicized term without reference to the text, if correction is needed, so that it is in a form acceptable for publication.

3.21 A function $\phi : S \to S'$ is an *isomorphism* if and only if $\phi(a * b) = \phi(a) * \phi(b)$

Let $< S, * >$ and $< S', *' >$ be binary algebraic structures. A function $\phi : S \to \S'$ is an isomorphism if and only if ϕ is injective, surjective, and satisfies $\forall a, b \in S, \phi(a * b) = a *' b$

3.22 Let $*$ be a binary operation on a set S. An element e of S with the property $s * e = s = e * s$ is an *identity element for* $*$ for all $s \in S$.
Let $*$ be a binary operation on a set S. An element e of S with the property $x * e = e * x = x$ for all $x \in S$ is an identity element.

3.31 Give a careful proof for a skeptic that the indicated property of a binary structure $< S, * >$ is indeed a structural property. (In Theorem 3.14 we did this for the property, "There is an identity element for $*$."). For each $c \in S$, the equation $x * x = c$ has a solution x in S.

Proof. Let $< S, * >$ be a binary structure with the property that $\forall c \in S, x * x = c$ has a solution x in S.
Suppose $< S', *' >$ is a binary structure that is isomorphic to $< s, * >$. Then, there

must exist a bijective isomorphic mapping $\phi : S \to S'$.
Let $c' \in S'$. We need to show that the property holds for $< S', *' >$. That is $x' * x' = c'$ has a solution x' in S'. As ϕ is surjective, there must exist a $c \in S$ such that $\phi(c) = c'$. As $x * x = c$, then $\phi(x) \in S'$ and $\phi(x) *' \phi(x) = \phi(x * x) = \phi(c) = c'$ Thus, $x' = \phi(x)$ is a solution to $x' * x' = c'$.
Therefore, $\forall c \in S, x * x = c$ has a solution x in S is a structural property. □

3.33 Let H be the subset of $M_2(\mathbb{R})$ consisting of all matrices of the form $\begin{bmatrix} a & -b \\ b & a \end{bmatrix}$ for $a, b \in \mathbb{R}$. Exercise 23 of Section 2 shows that H is closed under both matrix addition and matrix multiplication.

Let $\phi : \mathbb{C} \to H$ be define as $\phi(a + bi) = \begin{bmatrix} a & -b \\ b & a \end{bmatrix}$ for $a, b \in \mathbb{R}$. ϕ must be bijective by definition.

3.33a Show that $< \mathbb{C}, + >$ is isomorphic to $< H, + >$

Proof.

$$\begin{aligned} \phi[(a + bi) + (c + di)] &= \phi[(a + c) + (b + d)i] \\ &= \begin{bmatrix} a + c & -(b + d) \\ b + d & a + c \end{bmatrix} \\ &= \begin{bmatrix} a & -b \\ b & a \end{bmatrix} + \begin{bmatrix} c & -d \\ d & c \end{bmatrix} \\ &= \phi(a + bi) + \phi(c + di) \end{aligned}$$

Therefore, $< \mathbb{C}, + >$ is isomorphic to $< H, + >$ □

3.33b Show that $< \mathbb{C}, \cdot >$ is isomorphic to $< H, \cdot >$

Proof.

$$\begin{aligned} \phi[(a + bi) \cdot (c + di)] &= \phi[(ac - bd) + (ad + bc)i] \\ &= \begin{bmatrix} ac - bd & -(ad + bd) \\ ad + bc & ac - bd \end{bmatrix} \\ &= \begin{bmatrix} a & -b \\ b & a \end{bmatrix} \cdot \begin{bmatrix} c & -d \\ d & c \end{bmatrix} \\ &= \phi(a + bi) \cdot \phi(c + di) \end{aligned}$$

Therefore, $< \mathbb{C}, \cdot >$ is isomorphic to $< H, \cdot >$ □