Problem 3.2

ϕ is an isomorphism since it is one-to-one and onto and $\phi(n+m) = -(n+m) = (-n)+(-m) = \phi(n) + \phi(m)$ for all $m, n \in \mathbb{Z}$.

Problem 3.8

ϕ is not an isomorphism because it is not one-to-one. Consider the following two matrices

$$A = \begin{bmatrix} 3 & 0 \\ 0 & 2 \end{bmatrix}, B = \begin{bmatrix} 2 & 0 \\ 0 & 3 \end{bmatrix}.$$

It is clear that $A \neq B$. However $\det(A) = \det(B) = 6$, hence ϕ is not one-to-one and therefore not an isomorphism.

Problem 3.11

ϕ is not an isomorphism because it is not one-to-one. Consider $f(x) = x^2+3$ and $g(x) = x^2+4$. Note that $f'(x) = g'(x) = 2x$. However since $f(x) \neq g(x)$, ϕ is not one-ton-one and hence not an isomorphism.

Problem 3.19

Part A

Define the binary operation $*$ by

$$a * b = \frac{(a+1)\cdot(b+1)}{3} - 1.$$

Note that this satisifes the homorphism property since

$$\phi(x \cdot y) = 3xy - 1.$$

and

$$\begin{aligned} \phi(x) * \phi(y) &= (3x-1) * (3y-1) \\ &= \frac{(3x-1+1)\cdot(3y-1+1)}{3} - 1 \\ &= \frac{3x \cdot 3y}{3} - 1 \\ &= \frac{9xy}{3} - 1 \\ &= 3xy - 1. \end{aligned}$$

Therefore since $\phi(x \cdot y) = \phi(x) * \phi(y)$, ϕ is homomorphic and since it is a bijection it is an isomorphism between $\langle \mathbb{Q}, \cdot \rangle$ and $\langle \mathbb{Q}, * \rangle$. The identity element for $*$ is 2 since for all $a \in \mathbb{Q}$,

$$\begin{aligned} 2 * a &= \frac{(2+1)(a+1)}{3} - 1 \\ &= a + 1 - 1 = a. \end{aligned}$$

and

$$\begin{aligned} a * 2 &= \frac{(a+1)(2+1)}{3} - 1 \\ &= a + 1 - 1 = a. \end{aligned}$$

.

Part B

Since ϕ is one-to-one and onto, it is invertible. Therefore

$$\phi^{-1}(x) = \frac{x+1}{3}.$$

Since ϕ^{-1} must also be an isomorphism

$$\begin{aligned} a * b &= \phi^{-1}(3a-1) \cdot \phi^{-1}(3b-1) \\ &= \phi^{-1}((3a-1) \cdot (3b-1)) \\ &= \phi^{-1}(9ab - 3a - 3b + 1) \\ &= \frac{9ab - 3a - 3b + 1 + 1}{3} \\ &= 3ab - a - b + \frac{2}{3}. \end{aligned}$$

The identity element of $\langle \mathbb{Q}, \cdot \rangle$ is preserved under ϕ, therefore the identity element of $\langle \mathbb{Q}, * \rangle$ is

$$\phi^{-1}(1) = \frac{2}{3}.$$

3.26

Proof. Let $\langle S, * \rangle$ and $\langle S', *' \rangle$ be binary algebraic structures and assume there exists an isomorphism $\phi : S \to S'$. Consider the inverse map $\phi^{-1} : S' \to S$. Since ϕ is an isomorphism, it is one-to-one and onto and therefore its inverse is also one-to-one and onto. Let $a', b' \in S'$. By the properties of inverses

$$\phi(\phi^{-1}(a' *' b')) = a' *' b'.$$

Since ϕ is an isomorphism

$$\begin{aligned}\phi(\phi(a') * \phi(b')) &= \phi(\phi^{-1}(a')) *' \phi(\phi^{-1}(b')) \\ &= a' *' b'.\end{aligned}$$

Therefore since both equations are equal to $a' *' b'$, it follows that

$$\begin{aligned}\phi(\phi^{-1}(a' *' b')) &= \phi(\phi^{-1}(a') * \phi^{-1}(b')) \\ \phi^{-1}(a' *' b') &= \phi^{-1}(a') * \phi^{-1}(b'),\end{aligned}$$

meaning ϕ^{-1} is a homorphism. Therefore since ϕ^{-1} is one-to-one, onto, and homomorphic, it is an isomorphism from $\langle S', *' \rangle$ to $\langle S, * \rangle$. ■

3.28

Proof. Let A be a set of binary algebraic structures and define a relation $\simeq$ over A such that

$$\langle S, * \rangle \simeq \langle S', *' \rangle \iff \langle S, * \rangle \text{ is isomorphic to } \langle S', *' \rangle.$$

Proceed to show that $\simeq$ is an equivalence relation.

(Reflexivity) Let $\langle S, * \rangle \in A$. Define a mapping $\phi : S \to S : a \mapsto a$. Let $a, b \in S$ and assume $\phi(a) = \phi(b)$. Then $a = b$, hence ϕ is one-to-one. Let $b \in S$. Then $\phi(b) = b$, meaning ϕ is onto. Additionally, $\phi(a * b) = a * b = \phi(a) * \phi(b)$ meaning ϕ is homomorphic. Therefore ϕ is an isomorphism, meaning $\langle S, * \rangle \simeq \langle S, * \rangle$.

(Symmetry) Let $\langle S, * \rangle, \langle S', *' \rangle \in A$. Assume that $\langle S, * \rangle \simeq \langle S', *' \rangle$. By the result in (3.26), it follows there is an isomorphic map from $\langle S', *' \rangle$ to $\langle S, * \rangle$, meaning $\langle S', *' \rangle \simeq \langle S, * \rangle$.

(Transitivty) Let $\langle S, * \rangle, \langle S', *' \rangle, \langle S'', *'' \rangle \in A$. For simplicity, denote each structure by its set. Assume $S \simeq S'$ and $S' \simeq S''$. Therefore S is isomorphic to S' and S' is isomorphic to S''. By the result in (3.27), S is isomorphic to S''. Hence $S \simeq S''$

Since $\simeq$ is reflexive, symmetric, and transitive, it is an equivalent relation. ■

3·33

Part A

Proof. Let $H \subseteq M_2(\mathbb{R})$ such that an element of H is of the form $\begin{bmatrix} a & -b \\ b & a \end{bmatrix}$ with $a, b \in \mathbb{R}$. Define a map $\phi : \mathbb{C} \to H$ such that for a complex number z in its cartesian form $a + bi$

$$\phi(z) = \begin{bmatrix} a & -b \\ b & a \end{bmatrix}.$$

Examine the conditions for ϕ to be an isomorphism.

(One-to-One) Let $z_1, z_2 \in \mathbb{C}$. Then there exists $a, b, c, d \in \mathbb{R}$ such that $z_1 = a + bi$ and $z_2 = c + di$. Assume $\phi(z_1) = \phi(z_2)$. Then

$$\begin{aligned} \phi(z_1) &= \phi(z_2) \\ \phi(a + bi) &= \phi(c + di) \\ \begin{bmatrix} a & -b \\ b & a \end{bmatrix} &= \begin{bmatrix} c & -d \\ d & c \end{bmatrix}. \end{aligned}$$

For the two matrices to be equal, $a = c$ and $b = d$. Therefore $z_1 = z_2$, hence ϕ is one-to-one.

(Onto) Let $M \in H$. Then there exists $a, b \in \mathbb{R}$ such that $M = \begin{bmatrix} a & -b \\ b & a \end{bmatrix}$ Let $z = a + bi \in \mathbb{C}$. Then

$$\phi(z) = \begin{bmatrix} a & -b \\ b & a \end{bmatrix} = M.$$

Therefore ϕ is onto.

(Homomorphic) Let $z_1, z_2 \in \mathbb{C}$. Then there exists $a, b, c, d \in \mathbb{R}$ such that $z_1 = a + bi$ and $z_2 = c + di$. It follows that

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

Additionally,

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

Therefore $\phi(z_1 + z_2) = \phi(z_1) + \phi(z_2)$ meaning ϕ is homomorphic.

Since ϕ is one-to-one, onto, and homomorphic, it is an isomorphism between $\langle \mathbb{C}, + \rangle$ and $\langle H, + \rangle$. ■

Part B

Proof. Let $H \subseteq M_2(\mathbb{R})$ such that an element of H is of the form $\begin{bmatrix} a & -b \\ b & a \end{bmatrix}$ with $a, b \in \mathbb{R}$. Define a map $\phi : \mathbb{C} \to H$ such that for a complex number z in its cartesian form $a + bi$

$$\phi(z) = \begin{bmatrix} a & -b \\ b & a \end{bmatrix}.$$

From Part A, ϕ is one-to-one and onto. Examine ϕ for the homomorphism property.

(Homomorphic) Let $z_1, z_2 \in \mathbb{C}$. Then there exists $a, b, c, d \in \mathbb{R}$ such that $z_1 = a + bi$ and $z_2 = c + di$. It follows that

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

Additionally,

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

Therefore $\phi(z_1 + z_2) = \phi(z_1)\phi(z_2)$ meaning ϕ is homomorphic.

Since ϕ is one-to-one, onto, and homomorphic, it is an isomorphism between $\langle \mathbb{C}, \cdot \rangle$ and $\langle H, \cdot \rangle$. ■

4.6

$\langle \mathbb{C}, * \rangle$ is not a group since there is no inverse element for 0.

4.9

Consider the following equation for each respective group with x being an element of a given group, e being the associated identity, and $*$ being the associated operation. Then the equation

$$x * x * x = e$$

will have 1 solution in $\mathbb{R}$, 1 solution in $\mathbb{R}^*$, but 3 solutions in U. Therefore $\langle U, \cdot\rangle$ cannot be isomorphic to either $\langle \mathbb{R}, +\rangle$ or $\langle \mathbb{R}^*, \cdot\rangle$.

4.11

The set of all $n \times n$ diagonal matrices under matrix addition is a group.

Proof. Let D_n denote the set of all $n \times n$ diagonal matrices define the binary structure $\langle D_n, +\rangle$ where + is normal matrix addition. Examine the three axioms of a group.

(Associativity) Let $A, B, C \in D_n$. Then it quickly follows that

$$A + (B + C) = (A + B) + C$$

since matrix addition is associative.

(Identity Element) Let e be the $n \times n$ matrix with all zero entries. Clearly $e \in D_n$ and given a matrix $A \in D_n$,

$$A + e = e + A = A.$$

hence e is the indentity element.

(Inverse) Let $A \in D_n$. Let A' be the diagonal matrix where the diagonal is the negation of A. Therefore

$$A + A' = A' + A = A - A = e.$$

Since $\langle D_n, +\rangle$ follows the three axioms of a group, it is a group. ■

4.29

Proof. Let G be a finite group with an even number of elements. Consider the following set

$$S = \{a \in G : a \neq a'\}.$$

Note that $|S|$ must be even since entries are paired by a, a'. Since $|G|$ is even and $|S|$ is even, $|G - S|$ must also be even. $|G - S| \neq 0$ since the identity element $e \in G$ is in G but not in S, so it is in $G - S$. However, since $|G - S|$ is even, there must be at least one other element in $G - S$, meaning there is another element $a \in G$ that isnt the identity such that $aa = a$ ■

4.31

Proof. Let $\langle G, *\rangle$ be a group. Let $e \in G$ denote the identity element of G. It is trivial that e is idempotent for $*$ since $e * e = e$. Therefore there is at least one idempotent for $*$. Assume towards contradiction there exists an element $x \in G \neq e$ that is also an idempotent for $*$. Since x is an idempotent,

$$x * x = x.$$

Since x is an element of a group, x has an inverse x'. Therefore

$$\begin{aligned} x * x &= x \\ x * x * x' &= x * x' \\ x * e &= e \\ x &= e. \end{aligned}$$

However, this contradicts the assumption that $a \neq e$. Therefore there cannot be any other idempotents for $*$ besides an identity element e. By the uniqueness of the identity element, there is only one identity for G, hence e is the only idempotent for $*$. ■

4.32

Proof. Let G be a group with identity $*$ and assume that for all $x \in G$ that $x * x = e$. Therefore for all $x \in G$

$$\begin{aligned} x * x &= e \\ x * x * x' &= e * x' \\ x * e &= x' \\ x &= x'. \end{aligned}$$

Let $a, b \in G$. Consider $(a * b) * (a * b)$. Then

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

Therefore G is abelian. ■

4.33

Proof. Proceed with induction. Let G be an abelian group with $a, b \in G$. Consider the base case where $n = 1$. Then

$$(a * b)^1 = a * b = a^1 * b^1.$$

Therefore the base case holds. Assume for some fixed $n \in \mathbb{Z}^+$ that $(a * b)^n = a^n * b^n$. Then

$$\begin{aligned}(a * b)^{n+1} &= (a * b) * (a * b)^n \\ &= a * b * a^n * b^n \\ &= a * a^n * b * b^n \\ &= a^{n+1} * b^{n+1}.\end{aligned}$$

Therefore the $n + 1$ case holds, meaning for $n \in \mathbb{Z}^+$ that for all $a, b \in G$ that $(a * b)^n = a^n * b^n$. ■

4.34

Proof. Let G be a finite group and let $a \in G$. Consider the set $S = \{a, a^2, a^3, \ldots, a^m, a^{m+1}\}$ where $m = |G|$. Since there are $m + 1$ elements in S, there has to be a repeat otherwise S would contain $m + 1$ unique elements which is larger than $|G|$. Therefore there exists $\alpha, \beta \in \mathbb{Z}^+$ such that $\alpha \neq \beta$ and $a^\alpha = a^\beta$. Without loss of generality let $\alpha < \beta$. Then

$$\begin{aligned} a^\beta &= a^\alpha \\ a^{\beta-\alpha} &= e. \end{aligned}$$

Since $\alpha < \beta$, $\beta - \alpha > 0$ meaning $\beta - \alpha \in \mathbb{Z}^+$. Therefore for any $a \in G$ there exists a $n \in \mathbb{Z}^+$ such that $a^n = e$. ■

4.37

Proof. Let G be a group and $a, b, c \in G$. Assume that $a * b * c = e$. Then

$$\begin{aligned} a * b * c &= e \\ a' * a * b * c &= e * a' \\ b * c &= a' \\ b * c * c' &= a' * c' \\ b &= a' * c' \\ b * c &= a' * c' * c \\ b * c &= a' \\ b * c * a &= a' * a \\ b * c * a &= e. \end{aligned}$$

Therefore for all $a, b, c \in G$, if $a * b * c = e$ then $b * c * a = e$. ■

4.41

Proof. Let G be a group and $g \in G$. Define the map $i_g : G \to G$ such that $i_g(x) = gxg'$ for $x \in G$. Check the conditions that i_g is an isomorphism of G with itself.

(One-to-One) Let $a, b \in G$ and assume that $i_g(a) = i_g(b)$. Then

$$\begin{aligned} i_g(a) &= i_g(b) \\ gag' &= gbg' \\ gag'g &= gbg'g \\ ga &= gb \\ g'ga &= g'gb \\ a &= b. \end{aligned}$$

Therefore i_g is one-to-one.

(Onto) Let $b \in G$ and let $a = g'bg$. Then

$$\begin{aligned} i_g(a) &= gag' \\ &= gg'bgg' \\ &= b. \end{aligned}$$

Therefore i_g is onto.

(Homomorphic) Let $a, b \in G$. Then

$$i_g(ab) = gabg'.$$

and

$$\begin{aligned} i_g(a)i_g(b) &= gag'gbg' \\ &= gabg'. \end{aligned}$$

Therefore $i_g(ab) = i_g(a)i_g(b)$, meaning i_g is homomorphic.

Therefore since i_g is one-to-one, onto, and homomorphic, it is an isomorphism of G with itself.

■