Homework 2 Solutions

Section 3:

2. Determine whether $\phi : \mathbb{Z} \to \mathbb{Z}$ defined by $\phi(n) = -n$ is an isomorphism of binary algebraic structures from $\langle \mathbb{Z}, + \rangle$ to itself.

   Solution. Yes, ϕ is an isomorphism.

4. Determine whether $\phi : \mathbb{Z} \to \mathbb{Z}$ defined by $\phi(n) = n + 1$ is an isomorphism of binary algebraic structures from $\langle \mathbb{Z}, + \rangle$ to itself.

   Solution. No, ϕ is not an isomorphism. It doesn't satisfy the homomorphism property: $\phi(1 + 1) = \phi(2) = 2 + 1 = 3$, but $\phi(1) + \phi(1) = (1 + 1) + (1 + 1) = 4$, so $\phi(1 + 1) \neq \phi(1) + \phi(1)$.

6. Determine whether $\phi : \mathbb{Q} \to \mathbb{Q}$ defined by $\phi(x) = x^2$ is an isomorphism of binary algebraic structures from $\langle \mathbb{Q}, \cdot \rangle$ to itself.

   Solution. No, ϕ is not an isomorphism. It is neither one to one, nor onto: $\phi(-1) = 1 = \phi(1)$ and there is no $x \in \mathbb{Q}$ such that $\phi(x) = x^2 = -1$.

8. Determine whether $\phi : M_2(\mathbb{R}) \to \mathbb{R}$ defined by $\phi(A) = \det(A)$ is an isomorphism of binary algebraic structures from $\langle M_2(\mathbb{R}), \cdot \rangle$ to $\langle \mathbb{R}, \cdot \rangle$.

   Solution. No, ϕ is not an isomorphism. It is not one to one:

$$\phi\left(\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\right) = 1 = \phi\left(\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}\right).$$

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 $\mathbb{Q}$.
    a. Give the definition of a binary operation $*$ on $\mathbb{Q}$ such that ϕ is an isomorphism mapping $\langle \mathbb{Q}, + \rangle$ onto $\langle \mathbb{Q}, * \rangle$ and give the identity element for $*$ on $\mathbb{Q}$.

    Solution. If ϕ is to be an isomorphism, it must satisfy the homomorphism property. Then, for $a, b \in \mathbb{Q}$, we must have

$$\begin{aligned} a * b &= \left[3\left(\frac{a+1}{3}\right) - 1\right] * \left[3\left(\frac{b+1}{3}\right) - 1\right] \\ &= \varphi\left(\frac{a+1}{3}\right) * \varphi\left(\frac{b+1}{3}\right) \\ &= \varphi\left(\frac{a+1}{3} + \frac{b+1}{3}\right) \\ &= \varphi\left(\frac{a+b+2}{3}\right) \\ &= 3\left(\frac{a+b+2}{3}\right) - 1 \\ &= a + b + 1. \end{aligned}$$

    To find the identity element for $*$, we note that isomorphisms preserve identity elements. So we simply compute $\phi(0) = 3(0) - 1 = -1$. So -1 is the identity element for $*$.

b. Give the definition of a binary operation $*$ on $\mathbb{Q}$ such that ϕ is an isomorphism mapping $\langle \mathbb{Q}, * \rangle$ onto $\langle \mathbb{Q}, + \rangle$ and give the identity element for $*$ on $\mathbb{Q}$.

Solution. If ϕ is to be an isomorphism, it must satisfy the homomorphism property. Then, for $a, b \in \mathbb{Q}$, we must have

$$3(a * b) - 1 = \phi(a * b) = \phi(a) + \phi(b) = (3a - 1) + (3b - 1) = 3a + 3b - 2.$$

Solving for $a * b$, we must have $a * b = a + b - \frac{1}{3}$.

To find the identity element for $*$, we note that isomorphisms preserve identity elements. So we simply compute $\phi^{-1}(0) = \frac{0+1}{3} = \frac{1}{3}$. So $\frac{1}{3}$ is the identity element for $*$.

Section 4:

4. Let $*$ be defined on $\mathbb{Q}$ by letting $a * b = ab$. Determine whether $*$ gives a group structure on $\mathbb{Q}$. If no group results, give the first axiom in the order $\mathscr{G}_1$, $\mathscr{G}_2$, $\mathscr{G}_3$ (from the definition of a group) that does not hold.

   Solution. $\langle \mathbb{Q}, * \rangle$ is not a group. $\mathscr{G}_3$ is the first axiom that doesn't hold: 0 has no inverse since $0 * a = 0a = 0 \neq 1$ for all $a \in \mathbb{Q}$.

8. We can also consider multiplication $\cdot_n$ modulo n in $\mathbb{Z}_n$. For example, $5 \cdot_7 6 = 2$ in $\mathbb{Z}_7$ because $5 \cdot 6 = 30 = 4(7) + 2$. The set $\{1, 3, 5, 7\}$ with multiplication $\cdot_8$ modulo 8 is a group. Give the table for this group.

   Solution.

$\cdot_8$	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

   [Note: This group is isomorphic to V (the Klein 4-group).]

9. Show that the group $\langle U, \cdot \rangle$ is not isomorphic to either $\langle \mathbb{R}, + \rangle$ or $\langle \mathbb{R}^*, \cdot \rangle$.

   Claim: $\langle U, \cdot \rangle \not\cong \langle \mathbb{R}, + \rangle$

   Proof. Suppose, for the sake of contradiction, that $\phi : U \to \mathbb{R}$ is an isomorphism from $\langle U, \cdot \rangle$ to $\langle \mathbb{R}, + \rangle$. Then, since isomorphisms preserve identity elements (as shown in class), we must have $\phi(1) = 0$. Now, each element $z \in \{1, -1, i, -i\} =: S \subset U$ satisfies $z^4 = 1$. Then, for $z \in S$, we have

   $$0 = \phi(1) = \phi(z^4) = \phi(z \cdot z \cdot z \cdot z) = \phi(z) + \phi(z) + \phi(z) + \phi(z) = 4\phi(z).$$

   But this implies that $\phi(z) = 0$ for each $z \in S$, namely that ϕ is not injective, a contradiction. Hence there is no such isomorphism and so $\langle U, \cdot \rangle \not\cong \langle \mathbb{R}, + \rangle$. □

   Claim: $\langle U, \cdot \rangle \not\cong \langle \mathbb{R}^*, \cdot \rangle$

   Proof. Suppose, for the sake of contradiction, that $\phi : U \to \mathbb{R}^*$ is an isomorphism from $\langle U, \cdot \rangle$ to $\langle \mathbb{R}^*, \cdot \rangle$. Then, since isomorphisms preserve identity elements (as shown in class), we must have $\phi(1) = 1$. Now, each element $z \in \{1, -1, i, -i\} =: S \subset U$ satisfies $z^4 = 1$. Then, for $z \in S$, we have

   $$1 = \phi(1) = \phi(z^4) = \phi(z \cdot z \cdot z \cdot z) = \phi(z) \cdot \phi(z) \cdot \phi(z) \cdot \phi(z) = \phi(z)^4.$$

   But this implies that $\phi(z) = \pm 1$ for each $z \in S$. Since there are 4 elements in S whose images lie in a 2-element set (i.e. $\{1, -1\}$), ϕ is not injective, a contradiction. Hence there is no such isomorphism and so $\langle U, \cdot \rangle \not\cong \langle \mathbb{R}^*, \cdot \rangle$. □

31. If $*$ is a binary operation on a set S, an element x of S is an **idempotent for** $*$ if $x * x = x$. Prove that a group has exactly on idempotent element.

Proof. Let $\langle G, * \rangle$ be a group with identity element e. Then, by definition, $e * e = e$, so e is an idempotent for $*$. Let $x \in G$ be an idempotent for $*$. Then

$$x * x = x = x * e$$

and so, by the left-cancellation law, $x = e$. Therefore G has exactly one idempotent element. □

34. Let G be a group with a finite number of elements. Show that for any $a \in G$, there exists an $n \in \mathbb{Z}^+$ such that $a^n = e$.

Proof. Suppose G has m elements and consider the set $S = \{a^0, a^1, a^2, \ldots, a^m\}$. Since G is closed under its operation, each element of S is in G and so $S \subseteq G$. We can therefore conclude that $|S| \leq |G| = m$, i.e. S has at most m distinct elements. It must therefore be the case that there are some $0 \leq k < \ell \leq m$ such that $a^k = a^\ell$ (else S would consist of $m + 1$ elements). But then

$$a^k * a^{\ell - k} = a^\ell = a^k = a^k * e$$

and so by the left-cancellation law, we have $a^{\ell - k} = e$. Since $\ell > k$, we have $\ell - k \in \mathbb{Z}^+$ and so, setting $n = \ell - k$, we are done. □

Additional Exercises:

1. Let G be a group and $a \in G$. Prove that $(a')' = a$.

Proof. Since $(a')'$ is an inverse for a' and a' is an inverse for a, we have

$$a' * (a')' = e = a' * a.$$

By the left-cancellation law, we have $(a')' = a$. □

2. Let $\langle S, * \rangle$ be a binary algebraic structure and define $\mathrm{Aut}(S)$ to be the set of isomorphisms from S to S. That is,

$$\mathrm{Aut}(S) = \{f : S \to S \mid f \text{ is an isomorphism}\}.$$

Prove that $\langle \mathrm{Aut}(S), \circ \rangle$ is a group, where $\circ$ is the usual function composition. You do not need to prove that $\circ$ is associative (this is well-known) and you may use results proved in class, so long as you cite them.

Proof. We first show that $\mathrm{Aut}(S)$ is closed under $\circ$. Let $f, g \in \mathrm{Aut}(S)$. Then, by definition of isomorphism, f and g are bijective and satisfy

$$f(s * t) = f(s) * f(t) \quad \& \quad g(s * t) = g(s) * g(t)$$

for all $s, t \in S$. Now the composition of bijective functions is bijective, so $f \circ g$ is bijective and, for $s, t \in S$, we have

$$(f \circ g)(s * t) = f(g(s * t)) = f(g(s) * g(t)) = f(g(s)) * f(g(t)) = (f \circ g)(s) * (f \circ g)(t).$$

Therefore $f \circ g$ is a bijection from S to itself satisfying the homomorphism property, namely $f \circ g$ is an isomorphism and is therefore in $\mathrm{Aut}(S)$. So $\mathrm{Aut}(S)$ is closed under $\circ$.

It is well-known that composition is associative, so we omit the proof of this fact.

We claim that id_S is an identity element for $\circ$. Note that id_S is a bijection and, for $s, t \in S$,

$$\mathrm{id}_S(s * t) = s * t = \mathrm{id}_S(s) * \mathrm{id}_S(t).$$

Therefore id_S is a bijection from S to itself satisfying the homomorphism property, namely $\mathrm{id}_S \in \mathrm{Aut}(S)$. Also, given $f \in \mathrm{Aut}(S)$, we have

$$\mathrm{id}_S \circ f = f = f \circ \mathrm{id}_S$$

so id_S is indeed an identity element for $\circ$.

Finally, we proved in class that if $\phi : S \to S'$ is an isomorphism of binary algebraic structures $\langle S, * \rangle$ and $\langle S', *' \rangle$, then so is its *inverse function* $\phi^{-1} : S' \to S$. Therefore, given $f \in \mathrm{Aut}(S)$, we also have $f^{-1} \in \mathrm{Aut}(S)$ and

$$f \circ f^{-1} = \mathrm{id}_S = f^{-1} \circ f$$

(this is the characterization of an inverse function). Hence each element of $\mathrm{Aut}(S)$ has an inverse element in $\mathrm{Aut}(S)$ with respect to $\circ$.

We have shown that $\mathrm{Aut}(S)$ is closed under $\circ$, observed that $\circ$ is associative, produced an identity element for $\circ$ in $\mathrm{Aut}(S)$, and verified that every element of $\mathrm{Aut}(S)$ has an inverse with respect to $\circ$ in $\mathrm{Aut}(S)$. Therefore $\langle \mathrm{Aut}(S), \circ \rangle$ is a group. $\square$

[Note: We have distinguished between an *inverse function* and an *inverse element under composition*, even though they wind up meaning the same thing in this context.]