# GU4041: Intro to Modern Algebra I

Professor Michael Harris
Solutions by Iris Rosenblum-Sellers

Homework 3

1) Let $X$ be a set with two elements, $e$ and $f$.

a) Can you define a binary operation

$$\star : X \times X \to X$$

that is not associative?

Answer: Yes; for example, let $\star$ be given by the multiplication table

| $\star$ | $e$ | $f$ |
|---|---|---|
| $e$ | $f$ | $e$ |
| $f$ | $f$ | $e$ |

Then we have $e \star (e \star f) = e \star e = f$, but $(e \star e) \star f = f \star f = e$.

b) Suppose $e$ is a two-sided identity for $\star$, in other words

$$e \star e = e, e \star f = f, f \star e = f$$

(Here we write $e \star e$ rather than $\star(e, e)$, as usual). How many operations are there? Are they all necessarily commutative? Associative?

Answer: In the general case of $a$, we have four choices to make; where we send each element of the multiplication table. By making $e$ a two-sided identity, we remove three of the choices: $e \star e, e \star f$, and $f \star e$, leaving only $f \star f$. Since we can map $f \star f$ to either $e$ or $f$, we have precisely two operations satisfying this. It is clear that each are commutative; an element always commutes with itself, so our only option for noncommutativity was to map $e \star f$ and $f \star e$ to different elements. Since they're each mapped to $f$, either operation is commutative. For associativity, we realize that any expression $(x \star y) \star z$ or $x \star (y \star z)$ is equivalent to one with all of the copies of $e$ removed, since they're the identity. Therefore, if a "possibly nonassociative expression" has at least one copy of $e$ in it, such as $(f \star f) \star e$, is compared to $f \star (f \star e)$, we may immediately see that dropping the copy of $e$ leads us to comparing the product of two elements, and any expression involving two elements always associates. Therefore, the only expression that we might consider being nonassociative is the one with no copies of $e$ in it, $(f \star f) \star f$, as compared with $f \star (f \star f)$. However, recognizing that $f \star f \in X$, and that we already showed that commutativity holds, means that the two expressions are equal.

2)

a) Let $(X, \star)$ and $(Y, \circ)$ be two sets with binary operations. Suppose

$$f : X \to Y$$

is a bijection that defines an isomorphism of binary structures, i.e.

$$f(x_1 \star x_2) = f(x_1) \circ f(x_2).$$

Show that $f^{-1}: Y \to X$ is also an isomorphism of binary structures.
Answer:

*Proof.* Let $y_1, y_2 \in Y$. Since $f$ is an isomorphism, we know that $f(f^{-1}(y_1) \star f^{-1}(y_2)) = f(f^{-1}(y_1)) \circ f(f^{-1}(y_2)) = y_1 \circ y_2$. Then we apply $f^{-1}$ to each side, and obtain $f^{-1}(f(f^{-1}(y_1) \star f^{-1}(y_2))) = f^{-1}(y_1 \circ y_2)$. The left side reduces to $f^{-1}(y_1) \star f^{-1}(y_2)$, so the expression reduces to $f^{-1}(y_1 \circ y_2) = f^{-1}(y_1) \star f^{-1}(y_2)$, so $f^{-1}$ is also an isomorphism. □

b) Deduce from (a) that if $X = Y$ and $\star = \circ$, then the identity map from $X$ to itself defines an isomorphism of binary structures.

Answer:

*Proof.* (Easy way): We note $\mathrm{id}_X$ is certainly a bijection, as for any $x \in X$, $\mathrm{id}_X(x) = x$, giving us surjectivity, and if $x_1 \neq x_2$, then $\mathrm{id}_X(x_1) \neq \mathrm{id}_X(x_2)$, so we have bijectivity. It also respects binary operation structure: $\mathrm{id}_X(x_1 \star x_2) = x_1 \star x_2 = \mathrm{id}_X(x_1) \star \mathrm{id}_X(x_2)$. Therefore, it's an isomorphism □

*Proof.* (Harder way): We note that for any isomorphisms, their composition is an isomorphism. It is a set theory fact that the composition of two functions, the former of which is injective, yields an injective function, and the composition of two functions, the latter of which is surjective, yields a surjective function, so the composition of two bijections is a bijective function. Then let $f: X \to Y, g: Y \to Z$ be isomorphisms, with respect to structures $\star$ on $X, \circ$ on $Y$, and $*$ on $Z$. Then $(g \circ f)(x_1 \star x_2) = g(f(x_1 \star x_2)) = g(f(x_1) \circ f(x_2)) = g(f(x_1)) * g(f(x_2))$, so the composition of two isomorphisms is an isomorphism. Then it's clear by part a that if $f: X \to Y$ is an isomorphism, then $f^{-1} \circ f: X \to X = \mathrm{id}_X$ is also an isomorphism. □

3) Let $n \geq 3$ be an integer. Let $\Delta_n$ be a regular polygon with $n$ sides in the complex plane, with one vertex at the point 1 and the other vertices on the unit circle $x^2 + y^2 = 1$. Let $\mu_n$ denote the set of vertices of $\Delta_n$.

a) Use either the exponential function or trigonometric functions to list the coordinates of the points in $\mu_n$

Answer: It is clear that the vertices of $\Delta_n$ will be equidistant around the unit circle from one another. Then they should differ by some $e^{ik}$, where $k$ is a real constant. Since the first coordinate is at 1, we should also see that tracing out the distance $n$ times (but no fewer) takes us back to 1, i.e. $e^{ikn} = 1$, and in particular $kn = 2\pi$, such that this is the first time this occurs. Then $k = \frac{2\pi}{n}$, so each has the form $e^{\frac{2\pi i m}{n}}$. So $\mu_n = \{e^{\frac{2\pi i m}{n}}, m \in \mathbb{Z}\}$.
Note that if we'd prefer to use trigonometric functions, we simply use Euler's formula to rewrite the valid points as $\cos\left(\frac{2\pi i m}{n}\right) + i \sin\left(\frac{2\pi i m}{n}\right)$.

b) Show that the subset $\mu_n \subset \mathbb{C}$ is a group under multiplication.

Answer: We first show that multiplication is a well-defined binary operation from $\mu_n \times \mu_n$ to $\mu_n$, i.e. that the set is closed under multiplication. To see this, we note $e^{\frac{2\pi i m_1}{n}} e^{\frac{2\pi i m_2}{n}} = e^{\frac{2\pi i (m_1 + m_2)}{n}}$, and since $m_1 + m_2 \in \mathbb{Z}$, this is in $\mu_n$. We know that ordinary multiplication is associative. We now note that $1 = e^{\frac{2\pi i 0}{n}}$ is the multiplicative identity for ordinary multiplication, so it is for elements of $\mu_n$ as well. Lastly, we note that for any element of $\mu_n, e^{\frac{2\pi i m}{n}}$, we have $e^{\frac{2\pi i(-m)}{n}} e^{\frac{2\pi i m}{n}} = e^0 = 1 = e^{\frac{2\pi i m}{n}} e^{\frac{-2\pi i m}{n}}$. Therefore, $(\mu_n, \times)$ is a group.

c) Define an isomorphism of groups $f: \mathbb{Z}/n\mathbb{Z} \to \mu_n$.

Answer: We will see in part $d$ that there are several acceptable solutions, but the most natural one is $f([m]) = e^{\frac{2\pi i m}{n}}$. We have to check well-definedness; it could be the case that taking different representatives of $[m]$ yields different values of $f$, but we see that this is not the case; any representative of $[m]$ will be of the form $kn + m_0$, where $k \in \mathbb{Z}, m_0 \in \mathbb{Z}$, and $0 \leq m_0 < n$. Then we note

$$e^{\frac{2\pi i m}{n}} = e^{\frac{2\pi i (nk + m_0)}{n}} = e^{\frac{2\pi n k}{n}} e^{\frac{2\pi i m_0}{n}} = \left(e^{2\pi}\right)^k e^{\frac{2\pi i m_0}{n}} = (1)^k e^{\frac{2\pi i m_0}{n}} = e^{\frac{2\pi i m_0}{n}}$$

Then this is a well-defined function. It remains to show that it is a group homomorphism:

$$f([m_1]+[m_2]) = e^{\frac{2\pi i(m_1+m_2)}{n}} = e^{\frac{2\pi i m_1}{n}} e^{\frac{2\pi i m_2}{n}} = f([m_1])f([m_2])$$

d) Does part (c) have a unique solution? Explain.

Answer: Part c does not have a unique solution. In general, if we want an isomorphism between two cyclic groups, we have to map a generator in the domain to a generator in the codomain, and the rest is done for us. The generators of the cyclic group of $n$ elements are the equivalence classes of numbers which are relatively prime with $n$. In particular, $[1]$ always works, as does $[-1]$. If $n$ is prime, everything but $[0]$ works. However, in a case like 12, only $[1], [5], [7]$ and $[11]$ work.

4) List all subgroups of the Klein 4-group and of the cyclic group $\mathbb{Z}/4\mathbb{Z}$. How many subgroups contain 3 elements in each case?

Answer:

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \leqslant \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}; \{([1],[0]),([0],[0])\} \leqslant \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}; \{([0],[1]),([0],[0])\} \leqslant \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

$$\{([1],[1]),([0],[0])\} \leqslant \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}; \{([0],[0])\} \leqslant \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

$$\mathbb{Z}/4\mathbb{Z} \leqslant \mathbb{Z}/4\mathbb{Z}; \{[2],[0]\} \leqslant \mathbb{Z}/4\mathbb{Z}; \{[0]\} \leqslant \mathbb{Z}/4\mathbb{Z}$$

Note that no subgroups contain exactly 3 elements.

5) Let $X$ be a set with 3 elements. How many distinct binary operations

$$X \times X \to X$$

are there?

Answer: We have $3^2 = 9$ choices to make, since we need to pick one of the elements, and then another one (and order does matter). For each choice, we can map the two elements chosen to any of the three elements, so we have 3 options for each choice. Then 3 options for each choice, to the power of 9 choices, is $3^9 = 1983$. 6) A $2 \times 2$ matrix $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is *idempotent* if $A^2 = A$.

a) Check that the matrices $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ and $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ are both idempotents (you don't need to write this down). Find an idempotent matrix that is not equal to either of these.

Answer: An idempotent matrix not equal to either of these is $\begin{pmatrix} 0 & -1 \\ 0 & 1 \end{pmatrix}$. b) Suppose $A$ is idempotent and invertible. Show that $A = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

Answer: Let $A$ be idempotent and invertible. Then $A^2 = A$, so $A^{-1}A^2 = A^{-1}A$. Then $(A^{-1}A)A = (A^{-1}A)$, so $IA = I$, so $A = I$.