Math 411: Honors Algebra I
Problem Set 3
due: September 25, 2019

Emily Riehl

Exercise 1. Prove that $(gh)^{-1} = h^{-1}g^{-1}$ for all elements g, h in a group G.

Proof. Since $(gh) \cdot (h^{-1}g^{-1}) = ghh^{-1}g^{-1} = gg^{-1} = e$ we must have $h^{-1}g^{-1} = (gh)^{-1}$ because $(gh)^{-1}$ is defined to be the element of G that multiplies with gh to give you e. □

Exercise 2. The multiplication operation $- \cdot - \colon G \times G \to G$ for a group G can be specified by writing down its **multiplication table**: the columns and the rows are each labelled by the elements of G, and then the entry in row g and column h is the product $g \cdot h$.

G	e	g	h	$\cdots$	k
e	e	g	h	$\cdots$	k
g	g	g^2	$g \cdot h$	$\cdots$	$g \cdot k$
h	h	$h \cdot g$	h^2	$\cdots$	$h \cdot k$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$
k	k	$k \cdot g$	$k \cdot h$	$\cdots$	k^2

(i) Explain the pattern that you see in the first row and first column of the table (indexed by the identity element e).
(ii) Prove that every row and every column of the multiplication table of a group contains all elements of that group exactly once (like a Sudoko diagram).

Proof. For (i), multiplication with the identity $e \cdot - \colon G \to G$ or $- \cdot e \colon G \to G$ gives the identity function. This is why the first row and first column are copies of the row and column headers.

For (ii), we will show that the row labeled h has a copy of each group element appearing exact once. That is, we will show that for each $g \in G$ there exists a unique $k \in G$ so that $h \cdot k = g$. Multiplying this desired equation on the left by h^{-1} we see that we necessarily have $k = h^{-1}g$, and indeed with this definition of k we have $h \cdot h^{-1}g = g$. The argument for columns is similar. □

Exercise 3. Let g be an element of finite order in a group G and let $n \in \mathbb{Z}$. Prove that $g^n = e$ if and only if the order of g divides n.

Proof. Let k be the order of g and suppose k divides n. Then $n = ka$ for some integer a and $g^n = g^{ka} = (g^k)^a = e^a = e$. If k does not divide n then $n = ka + r$ for some $0 < r < k$ (by the division algorithm). Then $g^n = g^{ka+r} = (g^k)^a \cdot g^r = e \cdot g^r$. Since r is less than the order of g we have $g^r \neq e$ so $g^n \neq e$ in this case. □

Exercise 4. Prove that every element in a finite group has finite order.

Proof. An element has finite order if some finite power of it is the identity. Let $g \in G$ with G a group of order n. Then the elements $g^0, g, g^2, \dots, g^n$ cannot all be distinct. But if $g^i = g^j$ for some $i < j$, then $g^{j-i} = e$. □

Exercise 5. The hour-hand group has twelve elements $\{1, 2, 3, \dots, 12\}$ with addition defined by "addition of hours": e.g. $8 + 6 = 2$ because six hours after 8 o'clock is 2 o'clock. Prove that this defines a group by specifying an identity element, justifying associativity (it's okay to wave your hands on this point), and calculating the inverse of each elements. Have we encountered this group by another name?

Proof. This is isomorphic to the group $\mathbb{Z}/12$ discussed in class with addition modulo 12 and $[0]$ serving as the identity. □

Exercise 6.

(i) Sketch a proof that the unit circle centered at the origin in $\mathbb{R} \times \mathbb{R}$ defines a group with identity element $(1, 0)$ and with addition defined by "adding angles," where the angle of a unit vector is measured counterclockwise starting from the positive x axis.
(ii) Is this group abelian?
(iii) How does this group relate to the group $(\mathbb{C}^\times, \times, 1)$?[1]

[1] We don't have the language to describe this relationship precisely yet, but use your own words to describe your intuition.

Proof. (i) is annoying to justify, which is why I said it is okay to "sketch." For (ii) the answer is yes, since the sum of angles $\alpha + \beta$ is the same as the sum $\beta + \alpha$. For (iii) there is an injective group homomorphism from the unit circles $\{(x, y) \in \mathbb{R}^2 \mid x^2 + y^2 = 1\}$ to $(\mathbb{C}^\times, \times, 1)$ defined by $(x, y) \mapsto x + iy$ whose image is the unit circle. This gives a second proof that the group is abelian, since subgroups of abelian groups are abelian. □

Exercise 7. Let C be any category and fix an object $A \in \mathsf{C}$. Let $\mathsf{Aut}_{\mathsf{C}}(A)$ be the set of **automorphisms** of A in C:

$$\mathsf{Aut}_{\mathsf{C}}(A) := \{f \colon A \to A \in \mathsf{C} \mid f \text{ is an isomorphism}\}.$$

(i) Prove that $\mathsf{Aut}_{\mathsf{C}}(A)$ is a group with composition as its multiplication operation. What is the identity element?

(ii) Explain why the set $\mathsf{End}_{\mathsf{C}}(A)$ of **endomorphisms** of A in C defined by

$$\mathsf{End}_{\mathsf{C}}(A) := \{f \colon A \to A \in \mathsf{C}\}$$

is not a group under composition.

Proof. To see that the automorphisms of A define a group note that composition in any category is associative and has an identity element, namely the identity morphism. Because $\mathsf{Aut}_{\mathsf{C}}(A)$ contains only isomorphisms, each element $g \in \mathsf{Aut}_{\mathsf{C}}(A)$ has an inverse $g^{-1} \in \mathsf{Aut}_{\mathsf{C}}(A)$. This is the only reason why *endomorphisms* do not form a group: they have an associative composition operation with identities but do not always have inverses. □

Dept. of Mathematics, Johns Hopkins Univ., 3400 N Charles St, Baltimore, MD 21218
E-mail address: eriehl@math.jhu.edu