MA 541: Modern Algebra I / Fall 2021
Homework assignment #3
Due Tuesday 10/5/21 before 5pm

(Edited 9/29/21 to add [mandatory non-challenge] problems (9) and (10), plus a small additional piece to problem (4). All edits in blue.)

Three ways to turn in your work on the due date: in class, before 5pm in the envelope hanging on MCS 127, or before 5pm emailed as an attachment to `buma541f2021@gmail.com`.

- If you handwrite your solutions, please try to turn in the original rather than email a scan; also, please staple or otherwise connect the pages of your work. Definitely write your name on the front page.
- If you email, please have the filename identify you, the homework number, and this course, in that order.
- **Challenge problems:** If you're able to, turn the challenge problems in separately (if it's too late for this assignment, that's ok). You may also turn in challenge problems later, after the deadline.

(1) Recall that we defined $\mathbb{Z}_m^\times$ as the subset of elements of $\mathbb{Z}_m$ that have multiplicative inverses. We showed that $\mathbb{Z}_m^\times$ is a group under multiplication modulo m.

(a) For $m = 4, 5, 6, 7, 8, 9, 10$, find and list all the elements of $\mathbb{Z}_m^\times$.

(b) For which m from part (1a) does $\mathbb{Z}_m^\times$ has 4 elements? For each of these m, does $\mathbb{Z}_m^\times$ have the same structure (that is, the same Cayley table, up to relabeling) as any of the groups listed in HW#2(2)? Which ones?

(c) Same question for those m from (1a) for which $\mathbb{Z}_m^\times$ has order 6 and groups listed in HW#2(4).

(2) A *monoid* $(M, \circ)$ is a set M with an associative binary operation $\circ : M \times M \to M$ and an identity element.

(a) Let $(M, \circ)$ be a monoid with identity element e. Show that the subset

$$M^\circ := \{x \in M : \text{ there exists } y \in M \text{ satisfying } x \circ y = y \circ x = e\}$$

is a group under $\circ$.

(b) In each part below, is $(M, \circ)$ is a monoid? Explain why or why not. If $(M, \circ)$ is a monoid, what is M°?

(i) $(M, \circ) = (\mathbb{C}, \times)$
(ii) $(M, \circ) = (\mathbb{Q}_{\geq 0}, \times)$
(iii) $(M, \circ) = (\mathbb{Z}^+, \circ)$, where $a \circ b := a^b$
(iv) $(M, \circ) = (\mathbb{R}_{\leq 0}, +)$
(v) $(M, \circ) = (\mathbb{Z}_m, \times)$
(vi) $(M, \circ) = (\mathrm{M}_2(\mathbb{R}), \times)$
(vii) Let S be a set, and let $\mathrm{Fun}(S)$ be the set of functions $f : S \to S$. Consider $(M, \circ) := (\mathrm{Fun}(S), \text{composition})$.

[The notation M° is not standard.]

(3) Let G be a group, and suppose that H and K are subgroups of G. Either prove or disprove with a counterexample each of the following.

(a) The intersection $H \cap K$ is a subgroup of G.
(b) The union $H \cup K$ is a subgroup of G.
(c) The set $HK = \{hk : h \in H, k \in K\}$ of pairwise products is a subgroup of G.

Do any of the false statements among the three above become true if we G assume that G is abelian? Explain.

(4) Find all the subgroups of Q_8, the quaternion group from HW#1(5). Explain why you've found them all. Arrange them in a subgroup diagram showing all the nested relationships. For each subgroup $H \subseteq Q_8$, determine whether H is cyclic and find all the generators of H if so.

(5) Let G be a group. Define the set

$$Z(G) := \{a \in G : xa = ax \text{ for all } x \in G\}.$$

(a) Show that $Z(G)$ is a subgroup of G.

The subgroup $Z(G)$ is called the *center* of G.

(b) Find $Z(G)$ for each of the following groups. Explain!
  (i) $G = \mathbb{Z}$
  (ii) $G = \mathrm{GL}_2(\mathbb{R})$
  (iii) $G = \mathrm{Symm}(\triangle)$, the symmetry group of an equilateral triangle
  (iv) $G = \mathrm{Symm}(\boxed{})$, the symmetry group of a nonsquare rectangle
  (v) $G = Q_8$, the quaternion group from HW#1(5)

(6) Let G be a group and $H \subseteq G$ a subgroup. Define a relation $\sim$ on G as follows:

$$a \sim b \quad \text{if } a^{-1}b \in H.$$

(a) Show that $\sim$ is an equivalence relation on G.
(b) What are the equivalence classes for $\sim$ if $G = \mathbb{Z}$ and $H = 3\mathbb{Z}$?
(c) What are the equivalence classes for $\sim$ if $G = \mathrm{Symm}(\triangle)$ and $H = \{1, \mathrm{flip}(|)\}$?
(d) Consider the relation $\approx$ on G given by

$$a \approx b \quad \text{if } ab^{-1} \in H.$$

Is $\approx$ an equivalence relation? Explain. If it is, what are the equivalence classes for $\approx$ in each of the cases (6b) and (6c)?

(7) **William's *original* question (challenge problem):** Suppose $(G, \circ)$ is a set that we do not assume to be associative. Suppose further that G satisfies the "unique solution to linear equations property" from HW#2(5): for every $a, b \in G$, there exists a unique $x \in G$ satisfying $a \circ x = b$ and a unique $y \in G$ satisfying $y \circ a = b$. (We might alternatively call this the *sudoku property*. Why?) Must G be a group? Prove that it is or give a counterexample.

(8) **Gausian integers (challenge problem):** The Gaussian integers

$$Z[i] := \{a + bi : a, b \in \mathbb{Z}\}$$

is an additive subgroup of $\mathbb{C}$. Consider the relation $\equiv_{1+2i}$ on $\mathbb{Z}[i]$, where for α, β in $\mathbb{Z}[i]$ we say that $\alpha \equiv_{1+2i} \beta$ if there exists a $\gamma \in \mathbb{Z}[i]$ so that $\alpha - \beta = (1 + 2i)\gamma$.

(a) Show that $\equiv_{1+2i}$ ("congruence modulo $1+2i$") is an equivalence relation on $\mathbb{Z}[i]$.

(b) Write $\mathbb{Z}[i]_{1+2i}$ for the set of equivalence classes of $\mathbb{Z}[i]$ under $\equiv_{1+2i}$. Is $\mathbb{Z}[i]_{1+2i}$ a finite or an infinite set? If it is finite, how many equivalence classes are there? List or describe them all, giving explicit representatives.

(Suggestion: plot $\mathbb{Z}[i]$ in the complex plane on graph paper, and then plot the multiples of $1 + 2i$. What do the equivalence classes for $\equiv_{1+2i}$ look like in your diagram? Sometimes it's helpful to consider the *norm* (square of the absolute value) of a Gaussian integer:

$$N(a + bi) := a^2 + b^2$$

as a way of keeping track of distance.)

(c) Show that $\mathbb{Z}[i]_{1+2i}$ is an abelian group under addition. It has the same Cayley table as another group that we have studied. Explain!

(9) **Well-definition:** Which of the following "wannabe"-functions on sets of equivalence classes are well defined, and hence actually functions? In each case, either prove well-definition or give a (counter)example that shows that this is not a true function.

Below we denote an element of $\mathbb{Z}_m$ as $[a]_m$ for clarity.

(a) $\mathbb{Q} - \{1\} \longrightarrow \mathbb{Z}$ sending $\frac{a}{b}$ to $\frac{1}{a-b}$

(b) $\mathbb{Q} - \{1\} \longrightarrow \mathbb{Z}$ sending $\frac{a}{b}$ to $\frac{a+b}{a-b}$.

(c) $\mathbb{Z}_{18} \to \mathbb{Z}_6$ sending $[a]_{18}$ to $[a]_6$

(d) $\mathbb{Z}_6 \to \mathbb{Z}_{18}$ sending $[a]_6$ to $[a]_{18}$

(e) $\mathbb{Z}_{35} \to \mathbb{Z}_{15}$ sending $[a]_{35}$ to $[9a]_{15}$

(f) $\mathbb{Z}_m^\times \to \mathbb{Z}_m^\times$ sending $[a]_m$ to $[b]_m$ where $b \in \mathbb{Z}$ is any number that satisfies $ab \equiv_m 1$

(g) $\mathbb{Z}_m \to \mathbb{T}$ sending $[a]_m$ to $e^{2\pi i a/m}$ (Recall that $\mathbb{T} = \{z \in \mathbb{C} : |z| = 1\}$.)

(10) (a) Find all the subgroups of $\mathbb{Z}_{12}$. For each subgroup $H \subseteq \mathbb{Z}_{12}$, list all the elements of H, determine whether H is cyclic, and find all the generators if so. Arrange the subgroups in a subgroup diagram.

(b) Same question for $\mathbb{Z}_3 \times \mathbb{Z}_4$.

(c) Same question for $\mathbb{Z}_{13}^\times$.

Any observations?