Homework 4

Exercises

1. Consider the relation of congruence mod 4 on $\mathbb{Z}$: $a \equiv_4 b$ if $a - b = 4k$, for some $k \in \mathbb{Z}$.
   (a) What integers are in the equivalence class of 18?
   (b) What integers are in the equivalence class of 31?
   (c) How many distinct equivalence classes are there?

2. Let $n \in \mathbb{Z}^+$. Prove that the relation $\equiv_n$ on $\mathbb{Z}$ given by

   $$a \equiv_n b \text{ means that } a - b \text{ is a multiple of } n,$$

   is an equivalence relation. This is relation is called **congruence modulo** n.

3. Let $a, b, c, d \in \mathbb{Z}$. Prove **one** of the following (they are both true):
   (a) If $a \equiv_n c$ and $b \equiv_n d$, then $a + b \equiv_n c + d$.
   (b) If $a \equiv_n c$ and $b \equiv_n d$, then $a \cdot b \equiv_n c \cdot d$.

4. In this problem we consider the following Question:

   $$\textit{If } a \cdot b \equiv_n 0\textit{, does this mean } a \equiv_n 0 \textit{ or } b \equiv_n 0\textit{?}$$

   This certainly will not hold for any $n \in \mathbb{Z}^+$, since $3 \cdot 8 \equiv_{12} 0$, even though $3 \not\equiv_{12} 0$ and $8 \not\equiv_{12} 0$.
   (a) Consider $n = 2$. Prove that if $a \cdot b \equiv_2 0$, then $a \equiv_2 0$ or $b \equiv_2 0$.
   Hint: Have we proved a relevant Theorem already?
   (b) Consider $n = 4$. Prove that the answer to this Question is yes or find a counterexample showing the answer is no.
   (c) (*Optional, i.e., not graded*) Can you think of a condition on n that will guarantee the answer to the Question is yes?

5. Let $*$ be a unital associative binary operation on a set A with identity $e \in A$ and consider

   $$A^\times := \{a \in A : a \text{ is invertible with respect to } *\}.$$

   Show that $A^\times$ is a group with respect to $*$.

   Remark: You need to show that $*$ defines a binary operation satisfying the group axioms on $A^\times$. Note that we already have the associativity of $*$ by assumption, so don't worry about that. ***You should show****: that $A^\times$ is* ***closed*** *under $*$ (i.e., that $a, b \in A^\times$ means $a * b \in A^\times$), that $A^\times$ contains the identity $e \in A$, and that every $a \in A^\times$ has an inverse $a^{-1} \in A^\times$.*

6. Prove that the set $\mathrm{GL}_2(\mathbb{R}) := \{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{Mat}_{2\times 2}(\mathbb{R}) : ad - bc \neq 0\}$ is a group with respect to matrix multiplication. You may use without proof that matrix multiplication is associative.

   Remark: Use the previous problem as a Lemma! Show that, for any 2×2 matrix, being invertible is equivalent to having a non-zero determinant. You may use freely the fact that $\det(CD) = \det(C)\det(D)$ for all $C, D \in \mathrm{Mat}_{2\times 2}(\mathbb{R})$.

7. Let $*$ be a unital associative binary operation on a set A. Let R be the relation on A defined as follows: if $a, b \in A$, then aRb if there exists an invertible element $t \in A$ such that $b = t^{-1} * a * t$.[1]

   (a) Prove that R is an equivalence relation on A.

   (b) If $*$ is commutative, what are the equivalence classes of R?

   (c) Consider $A = \mathrm{D}_6$, the group of rigid symmetries for an equilateral triangle described in class. We enumerated a few special functions: r rotates clockwise by $120°$, s flips the triangle across a fixed axis of symmetry, and e does nothing at all (the identity function, i.e., the "trivial symmetry"). We also saw that $r^3 = e$ and $s^2 = e$, as well as $rs = sr^2$ (so symmetries do not always commute with each other): in particular, $r^{-1} = r^2$ and $s^{-1} = s$. Lastly, we showed

   $$\mathrm{D}_6 = \{e, r, r^2, s, sr, sr^2\}$$

   is an exhaustive list of all the symmetries.

   Compute the equivalence classes of D_6 with respect to the relation R. **This problem is about experimenting with an equivalence relation, not writing a formal argument, and will be explored more systematically in a future course on abstract algebra**—don't stress about proving your results exhaustively!

References

[1] You might be used to this sort of setup from linear algebra; when $A = \mathrm{Mat}_{n\times n}(\mathbb{R})$, this kind of conjugation is known as a change-of-basis.