Fall 2021, Math 620: Week 1 Problem Set
Due: Thursday, September 2nd, 2021
Introduction to Groups

Discussion problems. The problems below should be worked on in class.

(D1) *Checking group axioms.* Determine which (if any) of the group axioms are violated by each of the following sets G under the given operation $*$. **Brief** justifications are sufficient for this problem (no formal proof is required).

(a) $G = \mathbb{Z}$; $a * b = a - b$.
(b) $G = \mathbb{Z}_{\geq 0}$; $a * b = a + b$.
(c) $G = \mathbb{Z}_{10}$; $a * b = ab$ (i.e. standard multiplication in $\mathbb{Z}_{10}$).
(d) $G = \{1, 3, 7, 9\} \subset \mathbb{Z}_{10}$; $a * b = ab$ (i.e. standard multiplication in $\mathbb{Z}_{10}$).
(e) $G = (\mathbb{R} \times \mathbb{R}) \setminus \{(0, 0)\}$; $(a, b) * (c, d) = (ac, bd)$.

(D2) *Group element orders.* For a group $(G, \cdot)$ and $a \in G$, the *order* of a, denoted $|a|$, is the smallest $n \in \mathbb{Z}_{\geq 1}$ such that $a^n = e$, or $|a| = \infty$ is no such n exists.

(a) Find the order of each element of D_4. Do the same for $\mathbb{Z}$.
(b) Fix a group $(G, \cdot)$ and an element $a \in G$ with $|a| = n$. **After copying it onto the board in its entirety**, locate and correct an error in the following proof that $a^k = e$ if and only if $n \mid k$.

Proof. Suppose $a^k = e$, and write $k = qn + r$ for some $q, r \in \mathbb{Z}$ with $0 \leq r < n$. Then

$$e = a^k = (a^n)^q a^r = e^q a^r = a^r,$$

so by the minimality of n, we must have $r = 0$. As such, $n \mid k$. □

(c) Prove that if G is finite and $a \in G$, then $|a|$ is finite.

(D3) *Isomorphisms.* We say two groups $(G, \cdot)$ and $(G', \cdot)$ are *isomorphic* if there exists a bijection $\varphi : G \to G'$ such that $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$ for all $a, b \in G$. Intuitively, isomorphic groups have identical algebraic structure, and the elements have just been "relabeled".

(a) In the expression "$\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$" above, identify the group each "$\cdot$" occurs in.
(b) Argue that $(2\mathbb{Z}, +) \cong (\mathbb{Z}, +)$.
(c) A group $(G, \cdot)$ is called *cyclic* if $G = \{a^r : r \in \mathbb{Z}\}$ for some $a \in G$. The goal of this problem is to prove that up to isomorphism, $(\mathbb{Z}_n, +)$ are the only finite cyclic groups.
  (i) Argue that each $(\mathbb{Z}_n, +)$ is cyclic. How many choices are there for "a" in $\mathbb{Z}_8$?
  (ii) The remainder of this question is to prove that if $(G, \cdot)$ is cyclic and $|G| = n$, then $G \cong (\mathbb{Z}_n, +)$.
  Since G is cyclic, and fix $a \in G$ with $G = \{a^r : r \in \mathbb{Z}\}$. Consider the map

$$\begin{aligned} \varphi : G &\longrightarrow \mathbb{Z}_n \\ a^r &\longmapsto [r]_n. \end{aligned}$$

  Before we do **anything** we must ensure this map is "well-defined" (that is to say, the rule used to define φ doesn't attempt to send some element of the domain to two different elements of the codomain). Discuss what the potential issue is with this map. Then, prove that φ is indeed well-defined using (D2)(b).
  Hint: what is the order of a?
  (iii) Now, prove that φ is an isomorphism.
(d) Give a sketch of a proof that if G is infinite and cyclic then $G \cong \mathbb{Z}$.

Homework problems. You must submit *all* homework problems in order to receive full credit.

(H1) Determine whether each of the following sets G form a group under the given operation $*$. Prove your assertions.

(a) $G = \{1, 3, 5, 7, 9\} \subset \mathbb{Z}_{10}$; $a * b = ab$ (i.e. standard multiplication in $\mathbb{Z}_{10}$).

(b) $G = \mathbb{R}$; $a * b = a + b + 3$.

(c) G is the set of nonzero real numbers; $a * b = |a| \cdot b$.

(H2) Suppose G is a group and $a, b \in G$. Using **only group axioms**, prove $(ab)^{-1} = b^{-1}a^{-1}$. Be especially careful with associativity! In particular, any triple products xyz should be written as either $(xy)z$ or $x(yz)$.

(H3) Identify a subgroup of $GL_2(\mathbb{R})$ isomorphic to D_4. Identify a subgroup isomorphic to $\mathbb{Z}_6$.

(H4) Determine whether each of the following statements is true or false. Prove your assertions.

(a) Every infinite group G has at least one proper, nontrivial subgroup.
Note: a subgroup $H \subseteq G$ is *proper* if $H \neq G$ and *nontrivial* if $H \neq \{e\}$.

(b) If $(G, \cdot)$ is a group and $a, b, \in G$ with $|a| = n$ and $|b| = m$, then $|ab| \leq \text{lcm}(n, m)$.

Challenge problems. Challenge problems are not required for submission, but bonus points will be awarded for submitting a partial attempt or a complete solution.

(C1) Suppose $(G, *)$ is a group, where $G = \{0, 1, 2, 3, 4, 5, 6, 7\}$ and $*$ is an operation satisfying

(i) $a * b \leq a + b$ for every $a, b \in G$, and

(ii) $a * a = 0$ for every $a \in G$.

Write out the operation table for G, and **briefly** justify why this is the only possibility.