Fall 2019, Math 620: Week 1 Problem Set
Due: Thursday, September 5th, 2019
Introduction to Groups

Discussion problems. The problems below should be completed 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) $G = \mathbb{R} \times \mathbb{R}$; $(a, b) * (c, d) = (ac, bd)$.
(f) $G = \mathbb{R}^* \times \mathbb{R}$ where $\mathbb{R}^*$ denotes the nonzero real numbers; $(a, b) * (c, d) = (ac, bc + d)$.

(D2) *Group element orders.* For a group $(G, \cdot)$ and $a \in G$, the *order* of a, denoted $|a|$, is the smallest $k \in \mathbb{Z}_{\geq 1}$ such that $a^k = e$, or $|a| = \infty$ is no such k 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 $|a| = n$. 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.
(d) Suppose $(G, \cdot)$ is *cyclic* (that is, $G = \{a^r : r \in \mathbb{Z}\}$ for some $a \in G$) and that $|G| = n$. Turn the following "proof sketch" into a complete, rigorous proof that $G \cong (\mathbb{Z}_n, +)$.

Proof. Since G is cyclic, there is some $a \in G$ with $G = \{a^r : r \in \mathbb{Z}\}$. The map
$$\begin{aligned} \varphi : G &\longrightarrow \mathbb{Z}_n \\ a^r &\longmapsto [r]_n \end{aligned}$$
is well-defined (that is, $a^r = a^t$ implies $\varphi(a^r) = \varphi(a^t)$) by part (b). From there, verifying φ is an isomorphism is straightforward. □

(e) Give a sketch of a proof that if G is infinite and cyclic then $G \cong \mathbb{Z}$.

(D3) *Group automorphisms.* An *automorphism* of a group G is an isomorphism $G \to G$. The set of automporphisms of G, denoted $\mathrm{Aut}(G)$, is itself a group under composition.

(a) Find all elements of $\mathrm{Aut}(\mathbb{Z})$. Hint: where can an automorphism send $1 \in \mathbb{Z}$?
(b) Find $\mathrm{Aut}(\mathbb{Z}_6)$, $\mathrm{Aut}(\mathbb{Z}_7)$, and $\mathrm{Aut}(\mathbb{Z}_8)$.
(c) State and prove a characterization of $\mathrm{Aut}(\mathbb{Z}_n)$.

(D4) *Prove or disprove.* Determine whether each of the following statements is true or false.

(a) Every element of an infinite group has infinite order.
(b) For any groups G_1 and G_2, we have $\mathrm{Aut}(G_1 \times G_2) \cong \mathrm{Aut}(G_1) \times \mathrm{Aut}(G_2)$.

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

(H1) Suppose $(G, *)$ is a group, where $G = \{0, 1, 2, 3, 4, 5, 6, 7\}$ and $*$ is an operation satisfying

(i) $a * b \le a + b$ 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.

(H2) 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; $a * b = |a| \cdot b$.

(H3) 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!

(H4) Identify a subgroup of $GL_2(\mathbb{R})$ isomorphic to D_4. Identify a subgroup isomorphic to $\mathbb{Z}_6$.

(H5) 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.

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

(c) The group $(\mathbb{Q}, +)$ is cyclic.

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) A *graph* H is a collection E of 2-element subsets of $\{1, \ldots, n\}$ (called *edges*). An *automorphism* of a graph is a permutation σ of the integers $1, \ldots, n$ such that $\{a, b\} \in E$ if and only if $\{\sigma(a), \sigma(b)\} \in E$. The set $\mathrm{Aut}(H)$ of automorphisms of a graph H is a group under composition (you are not required to prove this). For example, if H is the 4-cycle graph, with edges $\{1, 2\}$, $\{2, 3\}$, $\{3, 4\}$, and $\{4, 1\}$, then $\mathrm{Aut}(H) \cong D_4$.

Identify a graph H whose automorphism group $\mathrm{Aut}(H)$ is isomorphic to $(\mathbb{Z}_5, +)$.