E. Dummit's Math 1365 ~ Intro to Proof, Fall 2022 ~ Homework 11, due Thu Dec 8th.

Justify all responses with clear explanations and in complete sentences unless otherwise stated. Write up your solutions cleanly and neatly, and clearly identify all problem numbers. Identify all pages containing each problem when submitting the assignment.

Part I: No justifications are required for these problems. Answers will be graded on correctness.

1. For each set G with the given operation, identify whether or not G is a group under the operation:
   (a) The positive real numbers under addition.
   (b) The positive real numbers under multiplication.
   (c) The set of functions $f : \mathbb{R} \to \mathbb{R}$ under pointwise addition: $(f \star g)(x) = f(x) + g(x)$ for each real x.
   (d) The set of functions $f : \mathbb{R} \to \mathbb{R}$ under function composition: $(f \star g)(x) = f(g(x))$ for each real x.
   (e) The set of bijections $f : \mathbb{R} \to \mathbb{R}$ under function composition: $(f \star g)(x) = f(g(x))$ for each real x.

---

2. Compute / find each of the following:
   (a) The product $(sr^2)(r^5)$ in the dihedral group $D_{2\cdot 5}$.
   (b) The product $(sr^2)(sr^3)(r^2)(s)$ in the dihedral group $D_{2\cdot 6}$.
   (c) The cycle decomposition of the permutation $\sigma \in S_8$ with $\sigma(1) = 4$, $\sigma(2) = 8$, $\sigma(3) = 5$, $\sigma(4) = 3$, $\sigma(5) = 2$, $\sigma(6) = 7$, $\sigma(7) = 6$, and $\sigma(8) = 1$.
   (d) The cycle decomposition of the product $(3\,4\,5) \cdot (4\,2\,1)$ in S_5.
   (e) The cycle decomposition of the product $(1\,3\,2\,5) \cdot (3\,6) \cdot (1\,6\,4)$ in S_7.
   (f) The cycle decomposition of the inverse of $(1\,5)(2\,6\,3\,4\,7)$ in S_7.
   (g) The 2022nd power of the element $(4\,9)$ in S_{10}.
   (h) The 2nd, 3rd, 4th, 5th, and 2022nd powers of the element $(1\,3\,2\,8\,5)$ in S_{10}.
   (i) The 2022nd power of the element $(1\,3\,2\,8\,5)(4\,9)(6\,7\,10)$ in S_{10}.
   (j) All possible orders of a subgroup of G, if G has order 30.
   (k) An abelian group of order 6.
   (l) A non-abelian group of order 6.
   (m) A non-abelian group of order 24.
   (n) The subgroup lattice of $\mathbb{Z}/24\mathbb{Z}$.
   (o) The least upper bound in $\mathbb{R}$ of the set of rational numbers $\{0.9, 0.99, 0.999, 0.9999, 0, 99999, \dots\}$.
   (p) The least upper bound in $\mathbb{R}$ of the set of rational numbers $\{a/b : a, b \in \mathbb{Z}_{>0} \text{ and } a^2 \le 3b^2\}$.

---

3. As noted in class, the order of any element in S_n is the least common multiple of the lengths of its cycles.

   Example: The element $(1\,2\,3\,4)(5\,6\,7\,8\,9\,10)$ in S_{10} has order $\text{lcm}(4, 6) = 12$.
   (a) What are the possible orders of an element of S_5? [Hint: There are 6 possibilities.]
   (b) Find an example of an element of S_5 of each possible order.
   (c) Find an example of an element of S_{10} of order 20.

---

4. Consider the dihedral group $D_{2\cdot 5}$ of order 10.
   (a) Identify the orders of each of the 10 elements e, r, r^2, r^3, r^4, s, sr, sr^2, sr^3, sr^4 of $D_{2\cdot 5}$.
   (b) Find the eight different subgroups of $D_{2\cdot 5}$.
   (c) Draw the subgroup lattice for $D_{2\cdot 5}$.

Part II: Solve the following problems. Justify all answers with rigorous, clear arguments.

5. Prove that the intersection $S = \bigcap_{i \in I} G_i$ of an arbitrary collection of subgroups G_i of G is also a subgroup of G.

---

6. Suppose G is a group with the property that $g^2 = e$ for every $g \in G$. Prove that G is abelian.

---

7. Suppose G is a group. Recall that if $g \in G$ then the subgroup generated by g, denoted $\langle g \rangle$, is the set of all powers of g: $\langle g \rangle = \{\dots, g^{-3}, g^{-2}, g^{-1}, e, g, g^2, g^3, \dots\}$. We say that G is cyclic if there exists an element $g \in G$ such that $\langle g \rangle = G$, and we call such an element g a generator of G.

   Example: The group $(\{1, -1\}, \cdot)$ is cyclic and generated by the element -1.

   Example: The group $(\mathbb{Z}, +)$ is cyclic and generated by the additive identity 1.

   (a) Show that the group $(\mathbb{Z}/m\mathbb{Z}, +)$ is cyclic by identifying a generator.

   (b) Show that if G has order n, then G is cyclic if and only if G contains an element of order n.

   (c) Show that the group $G = \{1, i, -1, -i\}$ under multiplication is cyclic, where $i = \sqrt{-1}$.

   (d) Show that the Klein 4-group $V_4 = \{e, a, b, ab\}$ with $a^2 = b^2 = (ab)^2 = e$ is not cyclic.

   (e) Show that every group of prime order p is cyclic. [Hint: What orders are possible for a non-identity element?]

---

8. [Optional] The goal of this problem is to prove that if an operation $\star$ is associative, meaning that $(a \star b) \star c = a \star (b \star c)$ for all a, b, c, then the placement of parentheses in a composition is irrelevant. For concreteness, define $a_1 \star a_2 \star \cdots \star a_n$ to be the composition $a_1 \star (a_2 \star (a_3 \star \cdots \star (a_{n-2} \star (a_{n-1} \star a_n))) \cdots))$ where all of the associations are pushed to the right: then $a_1 \star a_2 \star \cdots \star a_n = a_1 \star (a_2 \star \cdots \star a_n)$.

   (a) Prove that $(a_1 \star \cdots \star a_k) \star a_{k+1} = a_1 \star \cdots \star a_k \star a_{k+1}$ for every positive integer k. [Hint: Induct on k.]

   (b) Prove that $(a_1 \star \cdots \star a_k) \star (a_{k+1} \star \cdots \star a_n) = a_1 \star \cdots \star a_n$ for all positive integers n and k with $k < n$. [Hint: Fix k and induct on n.]

   (c) Let $n \geq 1$ and let $c(a_1, \dots, a_n)$ be some composition formed from $a_1, \dots, a_n$ with terms appearing in that order. Prove that $c(a_1, \dots, a_n) = a_1 \star \cdots \star a_n$ and deduce that all such compositions have the same value. [Hint: By considering the last $\star$ evaluated, explain why there exists some $1 \leq k < n$ and some compositions c', c'' such that $c(a_1, \dots, a_n) = c'(a_1, \dots, a_k) \star c''(a_{k+1}, \dots, a_n)$.]

   (d) Conclude in particular that the placement of parentheses in the product of elements in any group is irrelevant (and, as a further special case, that the placement does not matter for sums or products of integers).
