E. Dummit's Math 1465 ~ Intensive Mathematical Reasoning, Fall 2024 ~ Homework 11, due Wed Dec 4th.

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. Compute each of the following things related to cycle decompositions:
   (a) The cycle decomposition of the product $(3\,4\,5)\cdot(4\,2\,1)$ in S_5.
   (b) The cycle decomposition of the product $(1\,3\,2\,5)\cdot(3\,6)\cdot(1\,6\,4)$ in S_7.
   (c) The cycle decomposition of the inverse of $(1\,5)(2\,6\,3\,4\,7)$ in S_7.
   (d) The 2nd, 3rd, 4th, 5th, and 2024th powers of the element $(4\,9)$ in S_{10}.
   (e) The 2nd, 3rd, 4th, 5th, and 2024th powers of the element $(1\,3\,2\,8\,5)$ in S_{10}.
   (f) The 2024th power of the element $(1\,3\,2\,8\,5)(4\,9)(6\,7\,10)$ in S_{10}.

---

2. Calculate / find the following things relating to orders:
   (a) The order of the residue class $\overline{3}$ in the group of residue classes modulo 12 under addition.
   (b) The order of the residue class $\overline{2}$ in the group of invertible residue classes modulo 5 under multiplication.
   (c) The order of the residue class $\overline{5}$ in the group of invertible residue classes modulo 11 under multiplication.
   (d) 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 $D_{2\cdot 5}$.
   (e) The 6 possible orders of elements in S_5. [Hint: The order of a permutation is the lcm of its cycle lengths.]
   (f) An element of S_{12} having (i) order 12, (ii) order 18, (iii) order 60.
   (g) The possible orders of the subgroups of $D_{2\cdot 5}$, and an example of a subgroup of each possible order.
   (h) All possible orders of a subgroup of an arbitrary group G, if G has order 30.

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

3. Let I be an indexing set and let G be a group. 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.

---

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

---

5. Suppose that $\varphi : G \to H$ is a group isomorphism.
   (a) Let $g_1, g_2 \in G$. Show that $g_1g_2 = g_2g_1$ if and only if $\varphi(g_1)\varphi(g_2) = \varphi(g_2)\varphi(g_1)$.
   (b) Deduce that G is abelian if and only if H is abelian. [Hint: For $h_1, h_2 \in H$ take $h_1 = \varphi(g_1)$ and $h_2 = \varphi(g_2)$ for some $g_1, g_2 \in G$.]

---

6. 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?]

---

7. Let G be a group and let H be a subgroup of G. Define the relation R on G by saying $g_1 \, R \, g_2$ when there exists $h \in H$ such that $g_1 = g_2 h$ (in other words, when g_1 and g_2 are in the same left H-coset). Prove that R is an equivalence relation.

---

8. Let S be a nonempty set and $\mathcal{P}(S)$ be the power set of S (the set of all subsets of S). For subsets A and B of S, define the operations $A \oplus B = (A \cap B^c) \cup (A^c \cap B)$ and $A \odot B = A \cap B$ on $\mathcal{P}(S)$. (Note that $A \oplus B$ is simply the symmetric difference $A \Delta B$ described on homework 2.)

(a) Show that the addition and multiplication operations on $\mathcal{P}(S)$ are commutative.

(b) Show that the addition and multiplication operations on $\mathcal{P}(S)$ are associative. [Hint: You may use a Venn diagram for $\oplus$.]

(c) Show that multiplication distributes over addition. [Hint: Use a Venn diagram.]

(d) Show that $\emptyset$ is an additive identity and S is a multiplicative identity, and that every set A is its own additive inverse. Does every set A have a multiplicative inverse?

(e) Is $\mathcal{P}(S)$ a group under the operation $\oplus$? Is $\mathcal{P}(S)$ a group under the operation $\odot$? Is $\mathcal{P}(S)$ a field under the operations $\oplus$ and $\odot$? Briefly explain why or why not.

Remark: The power set $\mathcal{P}(S)$ together with these two operations $\oplus$ and $\odot$ form what is called the Boolean ring of S, which is an example of a commutative ring with 1. Boolean rings allow us to study logic and sets using algebra, and in particular help explain the analogies between the logic of propositions and the algebra of sets (namely, that the associated Boolean rings are isomorphic to one another, and therefore any property of propositional logic has a counterpart for sets).
