E. Dummit's Math 5111 ~ Algebra 1, Fall 2020 ~ Homework 7, due Fri Oct 30th.

Justify all responses with proof and in complete sentences unless otherwise stated. Write up your solutions cleanly and neatly, and clearly identify all problem numbers. You may use results from earlier parts of problems in later parts, even if you were unable to solve the earlier parts.

---

1. Compute / find each of the following:
   (a) The product $(sr^2)(sr^3)(r^2)(s)$ in $D_{2\cdot 6}$.
   (b) 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 $\sigma(8) = 1$.
   (c) The product $(1\,3\,2\,5)(3\,6)(1\,6\,4)$ in S_7.
   (d) The 2020th power of the element $(1\,3\,2\,8\,5)(4\,9)(6\,7\,10)$ in S_{10}.
   (e) All possible orders of an element in S_5, and an example of an element with each possible order.
   (f) The subgroup lattice of $\mathbb{Z}/24\mathbb{Z}$.
   (g) The subgroup lattice of $D_{2\cdot 5}$.
   (h) The order of the subgroup of S_4 generated by the elements $(1\,2)(3\,4)$ and $(1\,3)(2\,4)$.
   (i) A generator of the cyclic group $(\mathbb{Z}/17\mathbb{Z})^\times$.
   (j) Whether the set S of elements of odd order in S_5 is a subgroup of S_5, and whether it is a normal subgroup.
   (k) Whether the set S = the set of all complex roots of unity (i.e., the elements of finite order in $\mathbb{C}^\times$) is a subgroup of $\mathbb{C}^\times$, and whether it is a normal subgroup.
   (l) Whether $S = \{e, (1\,2\,3\,4), (1\,3)(2\,4), (1\,4\,3\,2)\}$ is a subgroup of S_4, and whether it is a normal subgroup.

---

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

---

3. Show that the groups $\mathbb{Z}/24\mathbb{Z}$, $(\mathbb{Z}/12\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$, $(\mathbb{Z}/2\mathbb{Z})^3 \times (\mathbb{Z}/3\mathbb{Z})$, $D_{2\cdot 12}$, S_4, and $S_3 \times (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$ are pairwise non-isomorphic.

---

4. Show that $\langle a, b : a^2 = b^2 = (ab)^n = e \rangle$ is a presentation of $D_{2\cdot n}$.

---

5. Let H be a subgroup of G and $a, b \in G$. Show that H is normal in G if and only if $ab \in H$ implies $ba \in H$.

---

6. Let p be a prime and take H to be the set of matrices of the form $\begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix}$ for $a, b, c \in \mathbb{F}_p$.
   (a) Show that H is a subgroup of $G = GL_3(\mathbb{F}_p)$, but that it is not a normal subgroup of G.
   (b) If p is odd, show that every nonidentity element of H has order p. Deduce that there exist non-abelian groups of order p^3 for p odd. [Hint: Let $N = \begin{bmatrix} 0 & a & b \\ 0 & 0 & c \\ 0 & 0 & 0 \end{bmatrix}$ and compute $(I_3 + N)^p$, noting $N^3 = 0$.]
   (c) For $p = 2$, this group is isomorphic to one of the groups of order 8 you have seen before. Which one?
   - Remark: We may take the elements a, b, c to be drawn from an arbitrary commutative ring with identity. The resulting group is known as the Heisenberg group and, in the case where $R = \mathbb{R}$, can be used to give a group-theoretic model for Heisenberg's uncertainty principle.

---

7. Suppose G is a finite abelian group of order $n > 1$. Recall that an integer is squarefree if it is not divisible by the square of any prime.

   (a) If n is squarefree, prove that G is cyclic. [Hint: By Cauchy's theorem, there exists an element of order p for each prime p dividing G. Multiply all of these elements together.]

   (b) If p is prime and $n = p^a m$ where m is not divisible by p, show that the group $(\mathbb{Z}/p\mathbb{Z})^a \times (\mathbb{Z}/m\mathbb{Z})$ is not cyclic if $a > 1$. Deduce that if n is not squarefree, then there is a non-cyclic abelian group of order n.

---

8. Let F be a field. Prove that the additive and multiplicative groups of F cannot be isomorphic.

---

9. The goal of this problem is to characterize subgroups and cosets in additive abelian groups purely in terms of the group operation. Suppose S is a nonempty subset of an additive abelian group G.

   (a) Prove that S is a subgroup of G if and only if the set $S - S = \{a - b : a, b \in S\}$ is equal to S.

   (b) Prove that S is a coset of some subgroup of G if and only if the set $S + S - S = \{a + b - c : a, b, c \in S\}$ is equal to S.
