MA 541: Modern Algebra I / Fall 2021
Homework assignment #6
Due Tuesday 11/9/21 before 5pm

Three ways to turn in your work on the due date: in class, before 5pm in the envelope hanging on MCS 127, or before 5pm emailed as an attachment to `buma541f2021@gmail.com`.

- If you handwrite your solutions, please try to turn in the original rather than emailing a scan. Please staple or otherwise connect the pages of your work. Definitely write your name on the front page.
- If you email, please have the filename identify you, the homework number, and this course, in that order.
- **Challenge problems:** Please turn solutions to challenge problems in separately. You may also turn in challenge problems later, after the deadline on the main set.

(1) Let $\sigma, \tau \in S_{15}$ be the permutations

$$\sigma = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\ 13 & 2 & 15 & 14 & 10 & 6 & 12 & 3 & 4 & 1 & 7 & 9 & 5 & 11 & 8 \end{bmatrix},$$

$$\tau = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\ 14 & 9 & 10 & 2 & 12 & 6 & 5 & 11 & 15 & 3 & 8 & 7 & 4 & 1 & 13 \end{bmatrix}.$$

Express each of the following in cycle notation: σ, τ, $\sigma\tau$, $\tau\sigma$, τ^{-1}, σ^{100}. Determine whether each of these six permutations is odd or even.

(2) (a) How many elements in S_8 have cycle structure $(5, 3)$? An element with cycle structure $(5, 3)$ is a product of two disjoint cycles, a 5-cycle and a 3-cycle. What is the order of such an element?

(b) How many elements in S_{15} have cycle structure $(6, 5, 4)$? An element with cycle structure $(6, 5, 4)$ is a product of three disjoint cycles, a 6-cycle, a 5-cycle, and a 4-cycle. What is the order of such an element?

(3) Let $f : G \to H$ be a homomorphism between two groups G and H with identity elements e_G and e_H, respectively.

(a) If A is a subgroup of G, show that $f(A)$ is a subgroup of H. In particular, show that the image $\operatorname{im} f$ is a subgroup of H.

Recall that the *kernel* of f is the set of elements of G that map to the identity in H under f. That is, $\ker f = f^{-1}(e_H) = \{g \in G : f(g) = e_H\}$.

(b) If B is a subgroup of H, show that $f^{-1}(B)$ is a subgroup of G. In particular show that $\ker f$ is a subgroup of G.

(c) Show that $\ker f = \{e_G\}$ if and only if f is injective.

(4) **Subgroups of finite cyclic groups:** Fix a positive integer m.

(a) Since every subgroup of a cyclic group is cyclic (Judson Theorem 4.10), we know that every subgroup of $\mathbb{Z}_m$ has the form $a\mathbb{Z}_m$ for some integer a. What is the order of $a\mathbb{Z}_m$?

(b) How many elements of $\mathbb{Z}_m$ have order d? Explain.

(c) Show that $\displaystyle\sum_{d|m} \varphi(d) = m$. (Here φ is the Euler phi function.)

(d) Show that $\mathbb{Z}_m$ has a unique cyclic subgroup of order d for every $d \mid m$. Identify all the elements of $\mathbb{Z}_m$ that generate this subgroup.

(5) **More on orders:** Suppose that G is a group, and $a, b \in G$ are two commuting elements of finite order. Let $m = \operatorname{ord}(a)$ and $n = \operatorname{ord}(b)$.

(a) Show that the order of ab divides $\operatorname{lcm}(m, n)$.

(b) Show by example that $\operatorname{ord}(ab)$ may be strictly smaller than $\operatorname{lcm}(m, n)$.

(c) If $\gcd(m, n) = 1$, prove that $\operatorname{ord}(ab) = mn$.

(d) Prove that G always has an element of order $\operatorname{lcm}(m, n)$.

(e) Show by example that (5c) and (5d) need not be true if a and b do not commute.

(6) (a) Suppose $\gcd(m, n) = 1$. Show that the map

$$\mathbb{Z}_{mn}^{\times} \to \mathbb{Z}_m^{\times} \times \mathbb{Z}_n^{\times}$$

sending $[a]_{mn}$ to $\big([a]_m, [a]_n\big)$ is an isomorphism of groups. (Don't forget to show that this map is surjective. Come ask me for a hint if you're struggling.)

(b) If $\gcd(m, n) = 1$, show that $\varphi(mn) = \varphi(m)\varphi(n)$.

(c) For a prime number p and an integer $r \geq 1$, compute $\varphi(p^r)$. Explain.

(d) Can $\mathbb{Z}_k^{\times}$ and $\mathbb{Z}_m^{\times} \times \mathbb{Z}_n^{\times}$ ever be isomorphic except if m and n are relatively prime and $k = mn$? Give an example or explain that this is impossible.

(7) Let G be a group, and $H \subseteq G$ a subgroup. For any element $a \in G$, write aH for the set of products $\{ah : h \in H\}$. This is a *left coset* of H in G.

(a) For $a \in G$, show that the map $H \to aH$ given by $h \mapsto ah$ is a bijection of sets.

(b) Show that $aH = H$ if and only if $a \in H$.

(c) Show that $aH = bH$ if and only if $a^{-1}b \in H$.

Now suppose that G is abelian, and finite of order n.

(d) Show that $a^n = 1$ for any $a \in G$. (*Hint:* Compare $\prod_{g \in G} g$ and $\prod_{g \in G} ag$.) Conclude that $\operatorname{ord}(a) \mid n$ for any $a \in G$.

(8) **Challenge problem**

(a) We showed in class that a k-cycle in S_n can be expresses as a product of $k-1$ transpositions. Show that fewer than $k-1$ transpositions will never do.

(b) More generally, suppose $\sigma \in S_n$ is a product of r cycles counting singletons — more properly said, σ partitions $\{1, 2, \ldots, n\}$ into r orbits. Show that σ may be expressed as the product of $n-r$ transpositions, and no fewer will do.