MA 541: Modern Algebra I / Fall 2021
Homework assignment #7
Due Thursday 11/18/2021 by 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. Consider using a pen rather than a pencil.
- 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) **Cosets:** For each of the following groups G and subgroups H, determine $[G : H]$. If there are finitely many (left) cosets, list them all. Can you think of a conceptual interpretation for each coset? If there are infinitely many cosets, describe them geometrically.

(a) $G = \mathbb{Q}^\times$, $H = \mathbb{Q}^+$
(b) $G = \mathbb{Z}_{12}$, $H = 3\mathbb{Z}_{12}$
(c) $G = \mathbb{C}^\times$, $H = \mathbb{R}^+$
(d) $G = \mathbb{C}^\times$, $H = \mathbb{T}$. (Recall that $\mathbb{T} = \{z \in \mathbb{C} : |z| = 1\}$.)
(e) $G = D_4$, $H = \langle f \rangle$. (Recall that $D_4 = \mathrm{Symm}(\square)$ and $f = \mathrm{flip}(|)$.)
(f) $G = S_4$, $H = \mathrm{Symm}({}^3_4\square^2_1)$
(g) $G = \mathbb{R}^2$, $H = (1, 2)\mathbb{Z}$

(2) If H and K are subgroups of a group G, then the set of products

$$HK = \{hk : h \in H, k \in K\}$$

need not be a subgroup of G (see (3c) on HW #3), but it IS a union of cosets of K. On the other hand, $H \cap K$ is a subgroup of H, so that H is a union of cosets of $H \cap K$. Show that there's a natural set bijection between sets of left cosets

$$HK/K \to H/H \cap K \qquad \text{given by} \qquad hK \mapsto h(H \cap K).$$

Conclude that $|HK| = \dfrac{|H|\,|K|}{|H \cap K|}$.

(3) Let G be a group. For $a, b \in G$, we say that a is *conjugate to* b (or a is a *a conjugate of* b) if there exists some $g \in G$ such that $a = gbg^{-1}$. The element a then is the result of *conjugating* b *by* g.

Convince yourself that a is conjugate to b if and only if there exists some $h \in G$ so that $a = h^{-1}bh$ — or, in the notation (5b) from the midterm, if and only if there is an $h \in G$ so that $a = c_h(b)$.

(a) Show that the relation "is conjugate to" is an equivalence relation on G. The equivalence class under the conjugation relation is called a *conjugacy class*.

(b) Find the result of conjugating the element $(1\ 7\ 5\ 2\ 3)(4\ 6)$ of S_7 by $(2\ 4)$. Do you notice anything?

(c) Find all the elements of S_3 that are conjugate to $(1\ 2\ 3)$.
What do you think will happen if you do this for $(1\ 2\ 3)$ in S_4?

(d) Find all the elements of A_4 that are conjugate to $(1\ 2\ 3)$.

(e) Decompose D_4 into a union of conjugacy classes.

(4) **Internal direct products of groups.**

(a) Suppose that G is a group and H and K are two subgroups of G satisfying the following three properties:

(i) Every element of H commutes with every element of K.

(ii) $H \cap K = \{1\}$.

(iii) $HK = G$.

Prove that the map $H \times K \to G$ sending (h, k) to hk is an isomorphism of groups.

(b) Show that $\mathbb{C}^{\times} \cong \mathbb{R}^{+} \times \mathbb{T}$.

(5) **Dihedral groups:** For $n \geq 3$, let $D_n = \langle r, f \mid r^n = f^2 = 1, fr = r^{-1}f \rangle$ be the group of symmetries of a regular n-gon, as defined in class.

(a) Find $Z(D_n)$. It may be helpful to consider the cases of odd and even n separately.

(Here $Z(G)$ is the *center* of of a group G, the set of elements of G that commute with every element of G, defined in (5) of HW #3.)

(b) Set $n = 6$. Show that $H = \langle r^2, f \rangle$ is a subgroup of D_6 isomorphic to D_3. Give both an algebraic and a geometric explanation.

(c) Show that $D_6 \cong D_3 \times \mathbb{Z}_2$ by constructing an explicit isomorphism (and proving that it is one).

(6) **Groups of order 8:** The goal of this problem is to show that every group of order 8 is isomorphic to exactly one of

$$\mathbb{Z}_8, \quad \mathbb{Z}_4 \times \mathbb{Z}_2, \quad \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2, \quad D_4, \quad Q_8.$$

Let G be a group of order 8. If G has an element of order 8, then G is cyclic and isomorphic to $\mathbb{Z}_8$. So eliminate this case and assume that every element of G has order 1, 2, or 4.

(a) If every element of G has order dividing 2, show that $G \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.

(b) Otherwise, let $a \in G$ have order 4. Let $H = \langle a \rangle$. Choose any $b \in G - H$. Show that $G = H \cup Hb$.

(c) If every $b \in G - H$ has order 2, show that $G \cong D_4$.

(d) Otherwise we can find $b \in G - H$ of order 4. Prove that $a^2 = b^2$. (*Hint:* (2).)

(e) To understand the multiplication structure on G completely, it remains to identify ba as an element of Hb. Show that either $ba = ab$ or $ba = a^3 b$.

(f) Complete the proof!

(7) **$\mathbb{Z}_p^\times$ is cyclic.**

(a) Find all the roots of the polynomial $X^2 + 3X - 4$ in $\mathbb{Z}_{21}$? How many are there?

(b) Suppose G is a finite abelian group. Let M be the maximum of the orders of any of the elements of G. Prove that $g^M = 1$ for any element $g \in G$.
(*Hint:* Use (5d) on HW #6.)

(c) Let p be prime. Assume the following statement from ring theory as a black box:

$$\boxed{\text{A polynomial of degree } n \text{ has no more than } n \text{ roots in } \mathbb{Z}_p.}$$

Use (7b) to show that the group $\mathbb{Z}_p^\times$ is cyclic.

(8) **Optional challenge problem: Cyclicity of units mod odd prime powers:** Now let p be an odd prime.

(a) Show that for every $n \geq 1$ the group $\mathbb{Z}_{p^n}^\times$ has an element of order $p - 1$.
(*Hint:* Start with an integer a that generates $\mathbb{Z}_p^\times$ (see problem **??**), and show that the order of a in $\mathbb{Z}_{p^n}^\times$ must be *divisible* by $p - 1$.)

(b) Show that $1 + p$ has order p^{n-1} in $\mathbb{Z}_{p^n}^\times$.
(*Hint:* for $b \in p\mathbb{Z}$ and $k \geq 1$, show that $1 + b \equiv 1$ modulo p^k if and only if $(1 + b)^p \equiv 1$ modulo p^{k+1}.)

(c) Conclude that $\mathbb{Z}_{p^k}^\times$ is a cyclic group.

(9) **Optional challenge problem: Which $\mathbb{Z}_N^\times$ are cyclic?**

(a) Explain where your argument in (8) above fails for $p = 2$.

(b) Show that $\mathbb{Z}_{2^k}^\times$ is never cyclic if $k \geq 3$.

(c) Show that $\mathbb{Z}_N^\times$ is cyclic if and only if $N = 1, 2, 4$, an odd prime power, or twice an odd prime power.