Submit hand-written (or typed) solutions at the beginning of class

---

Let $U(n)$ be the group of units in $\mathbb{Z}_n$ with multiplication module n as binary operation, that is,

$$\begin{aligned} U(n) &= \{x \in \mathbb{Z}_n : x \text{ has an inverse under } \cdot, \text{ multiplication modulo } n\} \\ &= \{x \in \mathbb{Z}_n : x \text{ and } n \text{ are relatively prime, meaning} \gcd(x, n) = 1\} \end{aligned}$$

1 $U(n)$

(a.) Complete the Cayley tables for $U(10)$ and $U(12)$

$\cdot$	1	3	7	9
1				
3		9		
7		1		
9				

$\cdot$	1	5	7	11
1				
5		1		
7		11		
11				

(b.) Find the order of the group $U(10)$, and the order of each element in the group.

(c.) Is $U(10)$ cyclic or non-cyclic? Explain why or why not.
(Hint: See Example 9 in Chapter 3, pg 65.)

(d.) Find the order of the group $U(12)$, and the order of each element in the group.

(e.) Is $U(12)$ cyclic or non-cyclic? Explain why or why not.
(Hint: See the explanation for why certain $U(n)$ are cyclic vs not cyclic, in Chapter 4 pg 76.)

(f.) Let $n \geq 3$. Prove that there is an element $k \in U(n)$ of order 2, that is, $k^2 = 1$ and $k \neq 1$.
(Hint: What is such an element for $U(10)$?)

2 Good Mathematical Writing

Read the three-page article Some Guidelines for Good Mathematical Writing by Francis Su.

(a.) What should you assume of your audience as you write your homework?

(b.) Why is the proof by contradiction on the third page not really a proof by contradiction?

(c.) What's the difference in meaning between these three phrases?

"Let $A = 12$."   "So $A = 12$."   "$A = 12$."

(d.) Write down tips (from the article) that are new to you. There may be items that you disagree with, and if so please explain.

Note that, in this class, for quizzes/exams/submitted homework, we will adopt the convention explained in "Avoid shorthand in formal writing" on page 2 of Su's article (even if you disagree with this convention).

3 Subgroup

Let H be a subgroup of G and let $g \in G$. Define gHg^{-1} to be the set $gHg^{-1} = \{ghg^{-1} : h \in H\}$. Prove that gHg^{-1} is a subgroup of G.
<u>Proof</u>:

(i) First, we will prove that e is in the set gHg^{-1}:
Since H is a subgroup of G, we know that H contains the identity element e of G, so $e = geg^{-1}$ is in the set gHg^{-1}.

(ii) Second, we will prove that gHg^{-1} is closed under the operation of G:
((STUDENT FILLS IN)).

(iii) Third, we will prove that gHg^{-1} is closed under taking inverses:
Let a be in the set gHg^{-1}. Then $a = g\ h_1\ g^{-1}$ for some $h_1 \in H$. The inverse of a is

$$\begin{aligned} a^{-1} &= (g\ h_1\ g^{-1})^{-1} \\ &= (g^{-1})^{-1}\ h_1^{-1}\ g^{-1} \quad \text{by the “socks-shoes property”} \\ &= g\ h_1^{-1}\ g^{-1} \quad \text{since } (g^{-1})^{-1} = g \end{aligned}$$

Since H is a subgroup of G, we know that H is closed under taking inverses. Therefore, since h_1 is in H, the inverse h_1^{-1} is also in H. Thus $a^{-1} = g\ h_1^{-1}\ g^{-1}$ is in the set gHg^{-1}.

4 Union of subgroups

(a.) Prove that it is impossible for a group G to be the union of two proper subgroups.

(Hint: See Gallian Chapter 3 Exercise 15 on pg 69)

(b.) Let G denote the rectangle “mattress group” (the symmetry group of a non-square rectangle) consisting of four rigid motions. Write G as the union of three proper subgroups.

5 Arithmetic

Suppose a, b, c are elements of a group G, and suppose $|a| = 6$ and $|b| = 7$. Express $(a^4c^{-2}b^4)^{-1}a^3$ without using negative exponents.

(Hint: Use “socks-shoes” property for inverses, laws of exponents, and the order of a and b. For a similar exercise, see Gallian Chapter 3 Exercise 7 on pg 69)

6 D_4

Consider D_4, the symmetry group of a square (or the “square mattress” group).

(a.) Find the order of the “square mattress” group D_4, and the order of each element in the group.

(b.) Let f be the horizontal flip (whose mirror is the vertical line). Compute $C(f)$, the centralizer of f.

(c.) Let R denote the counterclockwise rotation by 90^o. Compute $C(R)$, the centralizer of R.

(Hint: see Chapter 3 Example 15, pg 68)