MATH 343 · Group Theory

Chapter 3 Assigned Problems

Exercises 1, 17, 21, 27, 38, and 71

Exercises 55 and 67 are not repeated here: both are proved in the Chapter 4 lecture slides.

Solutions based on Gallian, Contemporary Abstract Algebra, 10th edition

Exercise 1: Question

Question

For each group in the following list, find the order of the group and the order of each element in the group.

$$\mathbb{Z}_{12}, \qquad U(10), \qquad U(12), \qquad U(20), \qquad D_4$$

What relation do you see between the orders of the elements of a group and the order of the group?

Exercise 1: Solution (1 of 3)

Find the order of each group and of each of its elements: $\mathbb{Z}_{12}$, U(10), U(12), U(20), and D_4.

$\mathbb{Z}_{12}$ under addition modulo 12: $|\mathbb{Z}_{12}| = 12$

$$1 \cdot 8 = 8, \quad 2 \cdot 8 = 16 \equiv 4, \quad 3 \cdot 8 = 24 \equiv 0 \pmod{12} \quad \Rightarrow \quad |8| = 3$$

a	0	1	2	3	4	5	6	7	8	9	10	11
|a|	1	12	6	4	3	12	2	12	3	4	6	12

U(10): |U(10)| = 4

a	1	3	7	9
|a|	1	4	4	2

U(12): |U(12)| = 4

a	1	5	7	11
|a|	1	2	2	2

$$3^2 = 9, \quad 3^3 \equiv 7, \quad 3^4 \equiv 1 \pmod{10}; \qquad 5^2 \equiv 7^2 \equiv 11^2 \equiv 1 \pmod{12}$$

Exercise 1: Solution (2 of 3)

Orders of the elements of U(20) and D_4.

U(20) under multiplication modulo 20: |U(20)| = 8

a	1	3	7	9	11	13	17	19
|a|	1	4	4	2	2	4	4	2

$$13^2 \equiv 9, \quad 13^3 \equiv 17, \quad 13^4 \equiv 1; \qquad 9^2 \equiv 11^2 \equiv 19^2 \equiv 1 \pmod{20}$$

D_4: $|D_4| = 8$

x	R_0	R_{90}	R_{180}	R_{270}	H	V	D	D'
|x|	1	4	2	4	2	2	2	2

R_{90} and R_{270} first return to R_0 at the fourth power; R_{180} and the four reflections are their own inverses.

Exercise 1: Solution (3 of 3)

What relation do you see between the orders of the elements of a group and the order of the group?

Group	|G|	Orders of its elements
$\mathbb{Z}_{12}$	12	1, 2, 3, 4, 6, 12
U(10)	4	1, 2, 4
U(12)	4	1, 2
U(20)	8	1, 2, 4
D_4	8	1, 2, 4

In each group, the order of every element divides the order of the group.

Lagrange's Theorem (Chapter 7) proves this for every finite group.

The converse fails: 4 divides |U(12)| and 8 divides |U(20)| and $|D_4|$, but none of these groups has an element of that order.

Exercise 17: Question

Question

For any group elements a and x, prove that

$$\left|xax^{-1}\right| = |a|$$

Exercise 17: Solution

Prove that $|xax^{-1}| = |a|$ for all elements a and x of a group.

Powers of a conjugate

$$(xax^{-1})^n = (xax^{-1})(xax^{-1})\cdots(xax^{-1}) = xa^nx^{-1}$$

For $n \geq 1$ the inner products $x^{-1}x$ equal e and cancel (formally, by induction on n).

The same exponents give the identity

$$(xax^{-1})^n = e \Leftrightarrow xa^nx^{-1} = e \Leftrightarrow a^n = x^{-1}ex = e$$

First equivalence: the identity above. Second: multiply by x^{-1} on the left, x on the right.

So a and xax^{-1} have the same positive exponents n giving e. If $|a| = m$, the least such exponent is m for both; if a has infinite order, neither has one.

Therefore $|xax^{-1}| = |a|$.

Exercise 21: Question

Question

For each divisor k > 1 of n, define

$$U_k(n) = \{x \in U(n) \mid x \bmod k = 1\}$$

For example, $U_3(21) = \{1, 4, 10, 13, 16, 19\}$ and $U_7(21) = \{1, 8\}$.

List the elements of $U_4(20)$, $U_5(20)$, $U_5(30)$, and $U_{10}(30)$.

Prove that $U_k(n)$ is a subgroup of U(n).

Exercise 21: Solution (1 of 2)

List the elements of $U_4(20)$, $U_5(20)$, $U_5(30)$, and $U_{10}(30)$.

x ∈ U(20)	1	3	7	9	11	13	17	19
x mod 4	1	3	3	1	3	1	1	3
x mod 5	1	3	2	4	1	3	2	4

$$U_4(20) = \{1,9,13,17\}, \qquad U_5(20) = \{1,11\}$$

x ∈ U(30)	1	7	11	13	17	19	23	29
x mod 5	1	2	1	3	2	4	3	4
x mod 10	1	7	1	3	7	9	3	9

$$U_5(30) = \{1,11\}, \qquad U_{10}(30) = \{1,11\}$$

Exercise 21: Solution (2 of 2)

Prove that $U_k(n)$ is a subgroup of U(n), where k > 1 is a divisor of n.

$U_k(n)$ is finite, so the Finite Subgroup Test (Theorem 3.3) applies

Nonempty

$$1 \bmod k = 1 \ \ (\text{since } k > 1) \ \ \Rightarrow \ \ 1 \in U_k(n)$$

Closed

$$a, b \in U_k(n) \ \ \Rightarrow \ \ a = ks + 1, \ \ b = kt + 1$$

$$ab = k(kst + s + t) + 1 \equiv 1 \pmod{k}$$

In U(n) the product is ab mod n = ab − qn, an element of U(n). Since k divides n,

$$ab \bmod n = ab - qn \equiv ab \equiv 1 \pmod{k}$$

So ab mod n ∈ $U_k(n)$, and $U_k(n)$ ≤ U(n) by Theorem 3.3.

Why k | n matters: in U(5), the set {x : x mod 2 = 1} = {1, 3} is not closed, as 3 · 3 mod 5 = 4.

Exercise 27: Question

Question

Show the following, so that U(14) is cyclic.

$$U(14) = \langle 3 \rangle = \langle 5 \rangle$$

Is U(14) = ⟨11⟩?

Show that no element generates U(20), so that U(20) is not cyclic.

$$U(20) \neq \langle k \rangle \quad \text{for every } k \in U(20)$$

Exercise 27: Solution (1 of 2)

Show that U(14) = ⟨3⟩ = ⟨5⟩, and decide whether U(14) = ⟨11⟩.

$$U(14) = \{1,3,5,9,11,13\}, \qquad |U(14)| = 6$$

k	1	2	3	4	5	6
$3^k \bmod 14$	3	9	13	11	5	**1**
$5^k \bmod 14$	5	11	13	9	3	**1**
$11^k \bmod 14$	11	9	**1**	11	9	**1**

$$\langle 3 \rangle = \langle 5 \rangle = \{1,3,5,9,11,13\} = U(14)$$

Since $11^3 = 1$, writing $n = 3q + r$ with $0 \le r < 3$ gives $11^n = 11^r$. Hence

$$\langle 11 \rangle = \{1,9,11\} \neq U(14)$$

U(14) is cyclic with generators 3 and 5; the element 11 does not generate it.

Exercise 27: Solution (2 of 2)

Show that U(20) ≠ ⟨k⟩ for every k in U(20).

$$U(20) = \{1,3,7,9,11,13,17,19\}, \qquad |U(20)| = 8$$

k	1	3	7	9	11	13	17	19
k^2 mod 20	1	9	9	1	1	9	9	1

Every square is 1 or 9, and $9^2 = 81 \equiv 1 \pmod{20}$. Hence

$$k^4 = 1 \quad \text{for every } k \in U(20)$$

Write any integer n as n = 4q + r with 0 ≤ r < 4. Then

$$k^n = \left(k^4\right)^q k^r = k^r \quad \Rightarrow \quad \langle k \rangle \subseteq \{1, k, k^2, k^3\}$$

So |⟨k⟩| ≤ 4 < 8 = |U(20)| for every k in U(20), and U(20) is not cyclic.

Exercise 38: Question

Question

If H and K are subgroups of G, show that H ∩ K is a subgroup of G.

$$H \leq G, \quad K \leq G \quad \Rightarrow \quad H \cap K \leq G$$

Can you see that the same proof shows that the intersection of any number of subgroups of G, finite or infinite, is again a subgroup of G?

Exercise 38: Solution

Show that $H \cap K \leq G$, and that any intersection of subgroups of G is a subgroup of G.

Two subgroups: the One-Step Subgroup Test

Nonempty

$$e \in H \text{ and } e \in K \quad \Rightarrow \quad e \in H \cap K$$

Test ab^{-1}

$$a, b \in H \cap K \quad \Rightarrow \quad ab^{-1} \in H \text{ and } ab^{-1} \in K$$

because H and K are subgroups. So $ab^{-1} \in H \cap K$, and $H \cap K \leq G$ by Theorem 3.1.

Any collection of subgroups

$$H_i \leq G \text{ for all } i \in I \quad \Rightarrow \quad \bigcap_{i \in I} H_i \leq G$$

Same proof, for any index set I: e lies in every H_i, and if a, b lie in every H_i, so does ab^{-1}.

This is why ⟨S⟩, the intersection of all subgroups containing S, is a subgroup.

Exercise 71: Question

Question

Let G be a group and let H be a subgroup of G. For any fixed x in G, define

$$xHx^{-1} = \{xhx^{-1} \mid h \in H\}$$

Prove the following.

(a) xHx^{-1} is a subgroup of G.

(b) If H is cyclic, then xHx^{-1} is cyclic.

(c) If H is Abelian, then xHx^{-1} is Abelian.

The group xHx^{-1} is called a conjugate of H.

Exercise 71(a): Solution

Prove that xHx^{-1} is a subgroup of G.

Nonempty

$$e \in H \quad \Rightarrow \quad e = xex^{-1} \in xHx^{-1}$$

Two elements

$$a = xh_1x^{-1}, \quad b = xh_2x^{-1}, \qquad h_1, h_2 \in H$$

$$b^{-1} = \left(x^{-1}\right)^{-1} h_2^{-1} x^{-1} = x\, h_2^{-1}\, x^{-1}$$

$$ab^{-1} = xh_1\left(x^{-1}x\right)h_2^{-1}x^{-1} = x\left(h_1h_2^{-1}\right)x^{-1}$$

Since H is a subgroup, $h_1h_2^{-1} \in H$, and therefore $ab^{-1} \in xHx^{-1}$.

By the One-Step Subgroup Test (Theorem 3.1), $xHx^{-1} \leq G$.

Exercise 71(b): Solution

Suppose $H = \langle h \rangle$ is cyclic. Prove that xHx^{-1} is cyclic.

Powers of xhx^{-1}, for every integer n

n ≥ 1

$$\left(xhx^{-1}\right)^n = xh^n x^{-1} \qquad \text{(Exercise 17)}$$

n = 0

$$\left(xhx^{-1}\right)^0 = e = xh^0x^{-1}$$

n = −m < 0

$$\left(xhx^{-1}\right)^{-m} = \left(\left(xhx^{-1}\right)^{-1}\right)^m = \left(xh^{-1}x^{-1}\right)^m = xh^{-m}x^{-1}$$

The last step applies the case n ≥ 1 to the element h^{-1}.

$$xHx^{-1} = \{xh^n x^{-1} \mid n \in \mathbb{Z}\} = \{\left(xhx^{-1}\right)^n \mid n \in \mathbb{Z}\} = \langle xhx^{-1} \rangle$$

So xHx^{-1} is cyclic, generated by xhx^{-1}.

Exercise 71(c): Solution

Suppose H is Abelian. Prove that xHx^{-1} is Abelian.

Take any two elements of xHx^{-1}:

$$xh_1x^{-1}, \quad xh_2x^{-1}, \qquad h_1, h_2 \in H$$

$$\left(xh_1x^{-1}\right)\left(xh_2x^{-1}\right) = xh_1h_2x^{-1} = xh_2h_1x^{-1} = \left(xh_2x^{-1}\right)\left(xh_1x^{-1}\right)$$

The outer equalities cancel $x^{-1}x = e$; the middle one uses $h_1h_2 = h_2h_1$ in H.

Any two elements of xHx^{-1} commute, so xHx^{-1} is Abelian.

Together, (a)–(c) say that conjugation preserves structure: a conjugate of a subgroup is a subgroup, and it is cyclic or Abelian whenever H is.