MATH 343 · Group Theory

Chapter 7 Assigned Problems

Exercises 1, 4, 13, 16, 20, 35, and 59

Exercise 24 is not repeated here: it is proved in the Chapter 8 lecture slides.

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

Exercise 1: Question

Question

Let $H = \{0, \pm 3, \pm 6, \pm 9, \ldots\}$. Find all the left cosets of H in $\mathbb{Z}$.

Let n be a positive integer. Let $H = \{0, \pm n, \pm 2n, \pm 3n, \ldots\}$. Find all left cosets of H in $\mathbb{Z}$. How many are there?

$\mathbb{Z}$ is a group under addition, so a left coset is written $a + H = \{a + h \mid h \in H\}$.

Exercise 1: Solution (1 of 2)

H = {0, ±3, ±6, ...}: three cosets, and the reason there are no others.

Coset	Elements
0 + H = H	..., −6, −3, 0, 3, 6, ...
1 + H	..., −5, −2, 1, 4, 7, ...
2 + H	..., −4, −1, 2, 5, 8, ...

Why these are all the cosets, and all different

Lemma 7.1(6), aH = bH ⟺ $a^{-1}b \in H$, reads in additive notation

$$a + H = b + H \Leftrightarrow b - a \in H$$

Divide any integer a by 3: a = 3q + r with r ∈ {0, 1, 2}. Then a − r = 3q ∈ H, so a + H = r + H. If r ≠ s in {0, 1, 2}, then s − r is ±1 or ±2, which is not in H, so r + H ≠ s + H.

H has exactly three left cosets in ℤ: H, 1 + H and 2 + H.

Exercise 1: Solution (2 of 2)

H = {0, ±n, ±2n, …} = nℤ: the same argument, with 3 replaced by n.

Every coset is one of 0 + H, 1 + H, …, (n − 1) + H

Divide a by n: a = nq + r with 0 ≤ r < n. Then a − r = nq ∈ H, so a + H = r + H.

These n cosets are different

If 0 ≤ s < r < n, then 0 < r − s < n, so r − s is not a multiple of n, and r + H ≠ s + H.

$$\mathbb{Z} = (0 + n\mathbb{Z}) \cup (1 + n\mathbb{Z}) \cup \cdots \cup \big((n-1) + n\mathbb{Z}\big)$$

There are exactly n left cosets: |ℤ : nℤ| = n, although ℤ and nℤ are infinite.

The coset r + nℤ is the set of integers that leave remainder r on division by n, the congruence class of r modulo n. For example, 2 + 7ℤ = {…, −12, −5, 2, 9, 16, …} = 37 + 7ℤ.

Exercise 4: Question

Question

Find all of the left cosets of $\{1, 11\}$ in $U(30)$.

$U(30)$ is the set of positive integers less than 30 and relatively prime to 30, under multiplication modulo 30.

Exercise 4: Solution

List the group, count the cosets with Lagrange, then build them one at a time.

$$U(30) = \{1,7,11,13,17,19,23,29\}, \qquad H = \{1,11\}$$

H is closed, since 11 · 11 = 121 ≡ 1 (mod 30), so it is a subgroup (Theorem 3.3). By Lagrange's Theorem there are |U(30)|/|H| = 8/2 = 4 left cosets. Take an element not yet used and multiply it by H; by Lemma 7.1(5) the new coset does not overlap the earlier ones.

Coset	New product	Elements
1H = H	1 · 11 = 11	{1, 11}
7H	7 · 11 = 77 ≡ 17	{7, 17}
13H	13 · 11 = 143 ≡ 23	{13, 23}
19H	19 · 11 = 209 ≡ 29	{19, 29}

The left cosets of {1, 11} in U(30) are {1, 11}, {7, 17}, {13, 23} and {19, 29}.

U(30) is Abelian, so these are also the right cosets: aH = Ha.

Exercise 13: Question

Question

Let G be a group of order 60. What are the possible orders for the subgroups of G?

Exercise 13: Solution

Theorem to use: Lagrange — the order of a subgroup divides the order of the group.

If H is a subgroup of G, then |H| divides |G| = 60 (Theorem 7.1). The divisors of $60 = 2^2 \cdot 3 \cdot 5$ are

$$1,\ 2,\ 3,\ 4,\ 5,\ 6,\ 10,\ 12,\ 15,\ 20,\ 30,\ 60$$

Every one of these orders occurs

In $\mathbb{Z}_{60}$, the subgroup $\langle 60/d \rangle$ has order d for each divisor d (Theorem 4.3):

d	1	2	3	4	5	6	10	12	15	20	30	60
⟨60/d⟩	⟨0⟩	⟨30⟩	⟨20⟩	⟨15⟩	⟨12⟩	⟨10⟩	⟨6⟩	⟨5⟩	⟨4⟩	⟨3⟩	⟨2⟩	⟨1⟩

The possible orders are exactly the twelve divisors of 60.

Lagrange's Theorem only lists candidates. A particular group of order 60 need not have a subgroup of each order, just as A_4, of order 12, has no subgroup of order 6 (lecture slides).

Exercise 16: Question

Question

Recall that, for any integer n greater than 1, ϕ(n) denotes the number of positive integers less than n and relatively prime to n. Prove that if a is any integer relatively prime to n, then

$$a^{\varphi(n)} \bmod n = 1.$$

This is Euler's Theorem. Fermat's Little Theorem (Corollary 5 in the lecture) is the case where n is a prime p, with ϕ(p) = p − 1.

Exercise 16: Solution (1 of 2)

Theorem to use: Corollary 4 of Lagrange's Theorem, $a^{|G|} = e$, in the group $G = U(n)$.

U(n) has ϕ(n) elements

U(n) = {k | 1 ≤ k < n and gcd(k, n) = 1}, under multiplication modulo n. These are exactly the numbers that ϕ(n) counts, so

$$|U(n)| = \varphi(n)$$

a mod n is an element of U(n)

Put r = a mod n, so a = qn + r with 0 ≤ r < n. A common divisor of r and n also divides a = qn + r; since gcd(a, n) = 1, this gives gcd(r, n) = 1. Also r ≠ 0, because gcd(0, n) = n > 1.

So r = a mod n lies in U(n).

Exercise 16: Solution (2 of 2)

Apply Corollary 4 to r in U(n), then return from r to a.

U(n) is a group of order $\phi(n)$, so Corollary 4 of Theorem 7.1 gives $r^{\phi(n)} = 1$ in U(n), that is,

$$r^{\varphi(n)} \bmod n = 1$$

Since $a \equiv r \pmod{n}$, also $a^{\phi(n)} \equiv r^{\phi(n)} \pmod{n}$ (Chapter 0, Exercise 11).

So $a^{\phi(n)}$ mod n = 1 for every integer a relatively prime to n.

Example: the last digit of 7^{2026}

For n = 10: U(10) = {1, 3, 7, 9}, so $\phi(10) = 4$, and $2026 = 506 \cdot 4 + 2$. Hence

$$7^{2026} = \left(7^4\right)^{506} \cdot 7^2 \equiv 1 \cdot 49 \equiv 9 \pmod{10}$$

The hypothesis gcd(a, n) = 1 is needed: gcd(2, 10) = 2, and $2^4 = 16 \equiv 6 \pmod{10}$.

Exercise 20: Question

Question

Suppose H and K are subgroups of a group G. If $|H| = 12$ and $|K| = 35$, find $|H \cap K|$. Generalize.

Exercise 20: Solution (1 of 2)

Theorem to use: Lagrange, applied inside H and inside K.

H ∩ K is a subgroup of H and of K

H ∩ K is a subgroup of G (Chapter 3, Exercise 38). It is contained in H, so it is a subgroup of H; in the same way it is a subgroup of K.

Lagrange's Theorem, twice

$$|H \cap K| \text{ divides } |H| = 12 \qquad \text{and} \qquad |H \cap K| \text{ divides } |K| = 35$$

The only positive integer that divides both $12 = 2^2 \cdot 3$ and $35 = 5 \cdot 7$ is 1.

$|H \cap K| = 1$, that is, $H \cap K = \{e\}$.

Exercise 20: Solution (2 of 2)

Generalize: the same two applications of Lagrange's Theorem, for any finite H and K.

Generalization

If H and K are finite subgroups of a group G, then $|H \cap K|$ divides $\gcd(|H|, |K|)$. In particular, if $|H|$ and $|K|$ are relatively prime, then $H \cap K = \{e\}$.

Examples

In $\mathbb{Z}_{420}$: $\langle 35 \rangle$ has 12 elements, $\langle 12 \rangle$ has 35, and $\langle 35 \rangle \cap \langle 12 \rangle = \{0\}$.

In $\mathbb{Z}_{12}$: $\langle 2 \rangle$ has 6 elements and $\langle 3 \rangle$ has 4, and $\langle 2 \rangle \cap \langle 3 \rangle = \{0, 6\}$, of order $\gcd(6, 4) = 2$.

In S_3: $\{(1), (12)\} \cap \{(1), (13)\} = \{(1)\}$, although $\gcd(2, 2) = 2$.

So "divides gcd(|H|, |K|)" cannot be improved to "equals gcd(|H|, |K|)".

Exercise 35: Question

Question

Let H and K be subgroups of a finite group G with H ⊆ K ⊆ G. Prove that

$$|G:H| = |G:K|\,|K:H|.$$

|G:H| is the index of H in G: the number of left cosets of H in G.

Exercise 35: Solution (1 of 2)

Theorem to use: Corollary 1 of Lagrange's Theorem, |G:H| = |G|/|H|, three times.

H ⊆ K and both are subgroups of G, so H is a subgroup of K, and |K:H| makes sense. Corollary 1, applied to the pairs (G, H), (G, K) and (K, H), gives

$$|G:H| = \frac{|G|}{|H|}, \qquad |G:K| = \frac{|G|}{|K|}, \qquad |K:H| = \frac{|K|}{|H|}$$

Multiply the last two:

$$|G:K|\,|K:H| = \frac{|G|}{|K|} \cdot \frac{|K|}{|H|} = \frac{|G|}{|H|} = |G:H|$$

So |G:H| = |G:K| |K:H|.

The hypothesis H ⊆ K is needed: without it, |K:H| is not even defined.

Exercise 35: Solution (2 of 2)

What the formula means: each coset of K splits into |K:H| cosets of H.

Example: G = $\mathbb{Z}_{12}$, K = ⟨2⟩ of order 6, H = ⟨4⟩ of order 3

Coset of K	The cosets of H inside it
K = {0, 2, 4, 6, 8, 10}	H = {0, 4, 8} and 2 + H = {2, 6, 10}
1 + K = {1, 3, 5, 7, 9, 11}	1 + H = {1, 5, 9} and 3 + H = {3, 7, 11}

Two cosets of K, each made of two cosets of H: four cosets of H in all.

$$|\mathbb{Z}_{12}:\langle 4\rangle| = 4 = 2 \cdot 2 = |\mathbb{Z}_{12}:\langle 2\rangle|\,|\langle 2\rangle:\langle 4\rangle|$$

Another chain: $S_4 \supseteq A_4 \supseteq V = \{(1), (12)(34), (13)(24), (14)(23)\}$, with $|S_4:V| = 6 = 2 \cdot 3 = |S_4:A_4|\,|A_4:V|$.

Exercise 59: Question

Question

Use properties of cosets to prove that for any subgroup H of S_n either every member of H is an even permutation or exactly half of the members is even.

(See Exercise 27 in Chapter 5.)

Exercise 59: Solution (1 of 3)

Let K be the set of even members of H. The tool: cosets of K in H.

K is a subgroup of H

$K = H \cap A_n$. A_n is a subgroup of S_n (Theorem 5.6), so K is a subgroup of S_n (Chapter 3, Exercise 38), and $K \subseteq H$.

Case 1: every member of H is even

Then K = H, and there is nothing more to prove.

Case 2: H has an odd member σ

Claim: the odd members of H are exactly the elements of the coset $\sigma K = \{\sigma k \mid k \in K\}$.

σK consists of odd members of H. For $k \in K$, $\sigma k \in H$ by closure, and σk is odd · even = odd.

Every odd member of H lies in σK. Let $\beta \in H$ be odd. Then $\sigma^{-1}\beta \in H$, and since σ^{-1} is odd like σ, $\sigma^{-1}\beta$ is odd · odd = even. So $\sigma^{-1}\beta \in K$, and $\beta = \sigma(\sigma^{-1}\beta) \in \sigma K$.

Exercise 59: Solution (2 of 3)

Case 2, continued: H is the union of the two cosets K and σK, and they have the same size.

$$H = K \cup \sigma K, \qquad K \cap \sigma K = \emptyset$$

Every member of H is even (so in K) or odd (so in σK), and no permutation is both (Theorem 5.5).

K and σK have the same size, as in Lemma 7.1(7)

$$\lambda : K \to \sigma K, \qquad \lambda(k) = \sigma k$$

Step 1 (well defined) $k \in K \Rightarrow \sigma k \in \sigma K$

Step 2 (one-to-one) $\sigma k_1 = \sigma k_2 \Rightarrow k_1 = k_2$ (cancellation)

Step 3 (onto) each element of σK is $\sigma k = \lambda(k)$

So λ is a one-to-one correspondence, and |σK| = |K|.

Exercise 59: Solution (3 of 3)

Case 2, concluded: count the members of H.

$$|H| = |K| + |\sigma K| = 2|K|$$

So exactly half of the members of H are even.

Example: H = ⟨(1234)⟩ in S_4, with σ = (1234)

Member of H	(1)	(1234)	(13)(24)	(1432)
Parity	even	odd	even	odd

K = {(1), (13)(24)} and σK = (1234)K = {(1234), (1432)}: two even members out of four.

In the language of Lagrange: the cosets of K in H are K and σK, so |H:K| = 2, and |K| = |H|/2 by Corollary 1.