Exercise 1

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?

Solution:

The left cosets are $H, 1 + H, 2 + H$. To see that there are no others, notice that for any integer m we can write $m = 3q + r$ where $0 \leq r < 3$ by the division algorithm. So, $m + H = r + 3q + H = r + H$, where $r = 0, 1$ or 2.

For the second part, there are n left cosets: $0 + \langle n \rangle, 1 + \langle n \rangle, \ldots, (n - 1) + \langle n \rangle$. This follows from the same reasoning: any integer m can be written as $m = nq + r$ where $0 \leq r < n$, so $m + H = r + H$ for some $r \in \{0, 1, 2, \ldots, n - 1\}$.

Exercise 2

Rewrite the condition $a^{-1} b \in H$ given in property 6 of the lemma in this chapter in additive notation. Assume that the group is Abelian.

Solution:

In additive notation, the inverse operation becomes negation and the group operation becomes addition. Therefore, $a^{-1} b$ becomes $-a + b = b - a$.

Thus, the condition $a^{-1} b \in H$ in additive notation is: $b - a \in H$.

Exercise 3

Let H be as in Exercise 1. Use Exercise 2 to decide whether or not the following cosets of H are the same.

a. $11 + H$ and $17 + H$
b. $-1 + H$ and $5 + H$
c. $7 + H$ and $23 + H$

Solution:

By Exercise 2, two cosets $a + H$ and b + H are equal if and only if $b - a \in H = \{0, \pm 3, \pm 6, \pm 9, \ldots\}$.

a. $11 + H = 17 + H$ because $17 - 11 = 6 \in H$.

b. $-1 + H = 5 + H$ because $5 - (-1) = 6 \in H$.

c. $7 + H \neq 23 + H$ because $23 - 7 = 16 \notin H$ (since 16 is not a multiple of 3).

Exercise 4

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

Solution:

First, we note that $U(30) = \{1, 7, 11, 13, 17, 19, 23, 29\}$ has order 8. Let $H = \{1, 11\}$, which has order 2.

By Lagrange's Theorem, the number of left cosets is $|U(30)|/|H| = 8/2 = 4$.

The four distinct left cosets are:

- $H = \{1, 11\}$
- $7H = \{7, 77\} = \{7, 17\}$ (since $77 \equiv 17 \pmod{30}$)
- $13H = \{13, 143\} = \{13, 23\}$ (since $143 \equiv 23 \pmod{30}$)
- $19H = \{19, 209\} = \{19, 29\}$ (since $209 \equiv 29 \pmod{30}$)

Exercise 5

Let a belong to a group and $|a| = 30$. How many left cosets of $\langle a^5 \rangle$ in $\langle a \rangle$ are there? List them. Do the same for $\langle a^4 \rangle$ in $\langle a \rangle$.

Solution:

Since $|a| = 30$, we have $|\langle a \rangle| = 30$.

For $\langle a^5 \rangle$: We have $|\langle a^5 \rangle| = 30/\gcd(5, 30) = 30/5 = 6$.

By Lagrange's Theorem, the number of left cosets is $|\langle a \rangle|/|\langle a^5 \rangle| = 30/6 = 5$.

The five cosets are: $\langle a^5 \rangle, a\langle a^5 \rangle, a^2\langle a^5 \rangle, a^3\langle a^5 \rangle, a^4\langle a^5 \rangle$.

For $\langle a^4 \rangle$: We have $|\langle a^4 \rangle| = 30/\gcd(4, 30) = 30/2 = 15$.

Note that $\langle a^4 \rangle = \langle a^2 \rangle$ because $\gcd(4, 30) = 2 = \gcd(2, 30)$.

By Lagrange's Theorem, the number of left cosets is $|\langle a \rangle|/|\langle a^4 \rangle| = 30/15 = 2$.

The two cosets are: $\langle a^4 \rangle$ and $a\langle a^4 \rangle$.

Exercise 6

Give an example of a group G and subgroups H and K such that
$HK = \{hk \mid h \in H, k \in K\}$ is not a subgroup of G.

Solution:

Consider the dihedral group D_3, which is the group of symmetries of an equilateral triangle.

Let F and F' be two distinct reflections in D_3. Define:

- $H = \{R_0, F\}$ (the identity and one reflection)
- $K = \{R_0, F'\}$ (the identity and a different reflection)

Then $HK = \{R_0, F, F', FF'\}$. However, the product of two distinct reflections is a rotation, and this set is not closed under the group operation. For instance, if we multiply F by itself, we get R_0, but if we multiply FF' by F, we get F', and if we multiply F' by FF', we get F. The set HK contains 4 elements but is not closed under multiplication, so it is not a subgroup.

Exercise 8

Let a and b be elements of a group G and H and K be subgroups of G. If $aH = bK$, prove that $H = K$.

Solution:

$aH = bK$ implies $H = a^{-1}bK$ which means $a^{-1}bK $is a subgroup but then we must have $a^{-1}bK = K$ since K is the only left coset of K which is a group. So, $H = a^{-1}bK = K$.

Exercise 9

If H and K are subgroups of G and g belongs to G, show that $g(H \cap K) = gH \cap gK$.

Solution:

We prove both inclusions.

(⊆) Let $x \in g(H \cap K)$. Then $x = ga$ for some $a \in H \cap K$. Since $a \in H \cap K$, we have $a \in H$ and $a \in K$. Therefore:

- $x = ga \in gH$ (since $a \in H$)
- $x = ga \in gK$ (since $a \in K$)

Thus, $x \in gH \cap gK$.

(⊇) Let $x \in gH \cap gK$. Then:

- $x \in gH$, so $x = gh$ for some $h \in H$
- $x \in gK$, so $x = gk$ for some $k \in K$

Therefore, $gh = gk$. By left cancellation, $h = k$.

Since $h \in H$ and $k \in K$ and $h = k$, we have $h \in H \cap K$.

Thus, $x = gh \in g(H \cap K)$.

We conclude that $g(H \cap K) = gH \cap gK$.

Exercise 13

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

Solution:

By Lagrange's Theorem, the order of any subgroup of G must divide the order of G.

Since $|G| = 60 = 2^2 \cdot 3 \cdot 5$, the divisors of 60 are: $1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30, 60$.

Therefore, the possible orders for the subgroups of G are:
$1, 2, 3, 4, 5, 6, 10, 12, 15, 20, 30, 60$.

Exercise 14

Suppose that K is a proper subgroup of H and H is a proper subgroup of G. If $|K| = 42$ and $|G| = 420$, what are the possible orders of H?

Solution:

By Lagrange's Theorem:

- $|K|$ divides $|H|$, so 42 divides $|H|$
- $|H|$ divides $|G|$, so $|H|$ divides 420

Therefore, $|H|$ must be a multiple of 42 and a divisor of 420.

The divisors of 420 that are multiples of 42 are: $42, 84, 210, 420$.

Since K is a proper subgroup of H, we have $|K| < |H|$, so $42 < |H|$.

Since H is a proper subgroup of G, we have $|H| < |G|$, so $|H| < 420$.

Therefore, the possible orders of H are: 84 and 210.

Exercise 15

Let G be a group with $|G| = pq$, where p and q are prime. Prove that every proper subgroup of G is cyclic.

Solution:

By Lagrange's Theorem, the order of any subgroup of G must divide $|G| = pq$.

The divisors of pq are: $1, p, q, pq$.

A proper subgroup has order strictly less than $|G| = pq$, so the possible orders for proper subgroups are: $1, p, q$.

- The subgroup of order 1 is $\{e\}$, which is cyclic (generated by e).
- Any subgroup of order p (a prime) is cyclic by Corollary 3 of Lagrange's Theorem (every group of prime order is cyclic).
- Any subgroup of order q (a prime) is cyclic by the same corollary.

Therefore, every proper subgroup of G is cyclic.

Exercise 16

Recall that, for any integer n greater than 1, $\phi(n)$ 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 $a^{\phi(n)} \mod n = 1$.

Solution:

This is Euler's Theorem. We prove it using Lagrange's Theorem.

The set $U(n)$ of units modulo n (i.e., the set of integers relatively prime to n under multiplication modulo n) forms a group of order $\phi(n)$.

If a is relatively prime to n, then we may assume $a \in U(n)$.

By Corollary 2 of Lagrange's Theorem, for any element a in a finite group G, we have $a^{|G|} = e$ (the identity element).

Applying this to $U(n)$, we get:
$a^{|U(n)|} = a^{\phi(n)} \equiv 1 \pmod{n}$

Therefore, $a^{\phi(n)} \mod n = 1$.

Exercise 17

Compute $5^{15} \mod 7$ and $7^{13} \mod 11$.

Solution:

For $5^{15} \mod 7$:

By Euler's Theorem (Exercise 16), since $\gcd(5, 7) = 1$ and $\phi(7) = 6$, we have:
$5^6 \equiv 1 \pmod 7$

Now, $15 = 6 \cdot 2 + 3$, so:
$5^{15} = 5^{12} \cdot 5^3 = (5^6)^2 \cdot 5^3 \equiv 1^2 \cdot 5^3 \equiv 125 \pmod 7$

Computing $125 \mod 7$: $125 = 17 \cdot 7 + 6$, so $125 \equiv 6 \pmod 7$.

Therefore, $5^{15} \mod 7 = 6$.

For $7^{13} \mod 11$:

By Euler's Theorem, since $\gcd(7, 11) = 1$ and $\phi(11) = 10$, we have:
$7^{10} \equiv 1 \pmod{11}$

Now, $13 = 10 + 3$, so:
$7^{13} = 7^{10} \cdot 7^3 \equiv 1 \cdot 7^3 \equiv 343 \pmod{11}$

Computing $343 \mod 11$: $343 = 31 \cdot 11 + 2$, so $343 \equiv 2 \pmod{11}$.

Therefore, $7^{13} \mod 11 = 2$.

Exercise 20

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

Solution:

By Lagrange's Theorem, $|H \cap K|$ must divide both $|H| = 12$ and $|K| = 35$.

The only common divisor is 1.

Therefore, $|H \cap K| = 1$.

Generalization: If H and K are subgroups of a group G and $\gcd(|H|, |K|) = 1$ (i.e., $|H|$ and $|K|$ are relatively prime), then $|H \cap K| = 1$.

This is because $|H \cap K|$ must divide both $|H|$ and $|K|$, and the only positive integer that divides two relatively prime numbers is 1.

Exercise 21

For any integer $n \geq 3$, prove that D_n has a subgroup of order 4 if and only if n is even.

Solution:

Recall that D_n is the dihedral group of order $2n$, consisting of n rotations and n reflections.

(⇐) If n is even, then D_n has a subgroup of order 4:

Since n is even, the rotation R_{180} (rotation by 180 degrees) exists and has order 2.

Let F be any reflection in D_n. Then F has order 2.

Consider the set $K = \{R_0, R_{180}, F, FR_{180}\}$.

We can easily see that this set is closed under the group operation and inversion:

- $R_{180}^2 = R_0$
- $F^2 = R_0$
- $(FR_{180})^2 = FR_{180}FR_{180} = F^2R_{180}^2 = R_0$
- $R_{180} \cdot F = FR_{180}$ (or $FR_{-180} = FR_{180}$)
- $F \cdot R_{180} = FR_{180}$
- $R_{180} \cdot FR_{180} = F$
- $FR_{180} \cdot R_{180} = F$

Therefore, K is a subgroup of order 4.

(⇒) If D_n has a subgroup of order 4, then n is even:

Suppose K is a subgroup of D_n with $|K| = 4$.

By Lagrange's Theorem, $|K|$ divides $|D_n| = 2n$, so 4 divides $2n$.

This means $2n = 4m$ for some integer m, which gives $n = 2m$.

Therefore, n is even.

Exercise 23

Suppose that G is an Abelian group with an odd number of elements. Show that the product of all of the elements of G is the identity.

Solution:

Let $|G| = 2k + 1$ for some non-negative integer k (since $|G|$ is odd).

Since G has odd order, by Lagrange's Theorem, no element can have order 2. This is because if $x \in G$ has order 2, then $|\langle x \rangle| = 2$ divides $|G|$, which contradicts the fact that $|G|$ is odd.

Therefore, for every element $x \in G$ with $x \neq e$, we have $x \neq x^{-1}$ (since $x = x^{-1}$ would imply $x^2 = e$, giving $|x| \in \{1, 2\}$).

Now consider the product of all elements of G. Since G is Abelian, we can rearrange the product. For each non-identity element x, we can pair it with its inverse x^{-1} (which is distinct from x):

$$\prod_{g \in G} g = e \cdot \prod_{\substack{x \in G \\ x \neq e}} x = e \cdot \prod_{i=1}^{k} (a_i \cdot a_i^{-1}) = e \cdot \prod_{i=1}^{k} e = e$$

Therefore, the product of all elements of G is the identity.

Exercise 24

Prove that every group of order 4 is Abelian.

Solution:

Let G be a group of order 4.

Case 1: G has an element of order 4.

If $a \in G$ has $|a| = 4$, then $\langle a \rangle = \{e, a, a^2, a^3\}$ has order 4. Since $|\langle a \rangle| = |G|$, we have $G = \langle a \rangle$, so G is cyclic. Every cyclic group is Abelian.

Case 2: G has no element of order 4.

By Lagrange's Theorem, every element of G has order dividing 4, so the possible orders are 1, 2, or 4. Since we're in Case 2, every non-identity element has order 2.

Let $a, b \in G$ be distinct non-identity elements. Then $a^2 = e$ and $b^2 = e$.

Consider ab. Since $|G| = 4$ and $G = \{e, a, b, ab\}$, we have $(ab)^2 = e$ (as ab must have order dividing 4, and it's not the identity).

Now, $(ab)^2 = abab = e$. Multiplying on the left by a and on the right by b:
$a(abab)b = aeb$
$a^2 bab^2 = ab$
$ba = ab$

Since a and b were arbitrary distinct non-identity elements, and every element has order 2, we can show that any two elements of G commute. Therefore, G is Abelian.

Exercise 27

Let $|G| = 33$. What are the possible orders for the elements of G? Show that G must have an element of order 3.

Solution:

By Lagrange's Theorem, the order of any element must divide $|G| = 33 = 3 \cdot 11$.

The divisors of 33 are: 1, 3, 11, 33.

Therefore, the possible orders for elements of G are: 1, 3, 11, 33.

Proof that G must have an element of order 3:

If G has an element x of order 33, then x^{11} has order $33/\gcd(11, 33) = 33/11 = 3$, so we're done.

So assume G has no element of order 33.

By the Corollary of Theorem 4.4, the number of elements of order 11 in G is a multiple of $\phi(11) = 10$.

Therefore, G has either 0, 10, 20, or 30 elements of order 11.

Including the identity element (which has order 1), we have accounted for at most $30 + 1 = 31$ elements.

Since $|G| = 33$, there are at least $33 - 31 = 2$ elements unaccounted for.

By Lagrange's Theorem (Corollary 2), these remaining elements must have order dividing 33. Since they're not the identity and not of order 11 or 33, they must have order 3.

Therefore, G must have an element of order 3.

Exercise 28

Suppose G is a non-Abelian group with $|G| = 8$. Prove that G has an element of order 4.

Solution:

By Lagrange's Theorem, the possible orders for elements of G are: 1, 2, 4, 8.

Claim: Not all non-identity elements can have order 2.

Suppose, for contradiction, that every non-identity element has order 2. Then for any $a, b \in G$:
$(ab)^2 = e$
$abab = e$

Multiplying on the left by a and on the right by b:
$a(abab)b = aeb$
$a^2 bab^2 = ab$
$bab = ab$ (since $a^2 = b^2 = e$)

Multiplying on the left by $b^{-1} = b$:
$ab = ba$

This shows that G is Abelian, contradicting our assumption that G is non-Abelian.

Therefore, G must have an element of order 4 or 8.

If G has an element of order 8, then G is cyclic (hence Abelian), which contradicts our assumption.

Therefore, G must have an element of order 4.

Exercise 29

Prove that any group of order 55 must have exactly one subgroup of order 5 or exactly 11 subgroups of order 5.

Solution:

Let G be a group with $|G| = 55 = 5 \cdot 11$.

Case 1: G is cyclic.

By Theorem 4.3, a cyclic group has exactly one subgroup of each order dividing the group order. Therefore, G has exactly one subgroup of order 5.

Case 2: G is not cyclic.

By Lagrange's Theorem, elements of G have order 1, 5, 11, or 55. Since G is not cyclic, no element has order 55.

By the corollary to Theorem 4.4, the number of elements of order 11 is a multiple of $\phi(11) = 10$.

If G had two distinct subgroups H and K of order 11, then $|H \cap K|$ divides both 11 (a prime), so $|H \cap K| = 1$. This means H and K share only the identity, contributing $10 + 10 = 20$ elements of order 11.

But if there were more than 20 elements of order 11, say 30, then we'd have at least 3 distinct subgroups of order 11. However, $|HK| = |H||K|/|H \cap K| = 11 \cdot 11/1 = 121 > 55$, which is impossible.

Therefore, G has exactly 10 elements of order 11 (one subgroup of order 11).

This leaves $55 - 10 - 1 = 44$ elements (excluding the identity and elements of order 11).

By the corollary to Theorem 4.4, the number of elements of order 5 is a multiple of $\phi(5) = 4$.

Since we have 44 elements remaining and each subgroup of order 5 contributes 4 non-identity elements, we have $44/4 = 11$ subgroups of order 5.

Therefore, G has exactly 11 subgroups of order 5.

Exercise 35

Let H and K be subgroups of a finite group G with $H \subseteq K \subseteq G$. Prove that $|G:H| = |G:K||K:H|$.

Solution:

Recall that the index $|G:H|$ is defined as the number of left cosets of H in G, which equals $|G|/|H|$ for finite groups.

Similarly:

- $|G:K| = |G|/|K|$
- $|K:H| = |K|/|H|$

Now we compute:
$|G:K| \cdot |K:H| = \frac{|G|}{|K|} \cdot \frac{|K|}{|H|} = \frac{|G|}{|H|} = |G:H|$

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

Exercise 38

Let G be a group and $|G| = 21$. If $g \in G$ and $g^{14} = e$, what are the possibilities for $|g|$?

Solution:

By Lagrange's Theorem, $|g|$ must divide $|G| = 21 = 3 \cdot 7$.

So the possible orders are: 1, 3, 7, 21.

Additionally, since $g^{14} = e$, we know that $|g|$ divides 14 by the property that $g^n = e$ if and only if $|g|$ divides n.

Since $14 = 2 \cdot 7$, the divisors of 14 are: 1, 2, 7, 14.

The order $|g|$ must divide both 21 and 14. The common divisors are: 1, 7.

Therefore, the possibilities for $|g|$ are: 1 and 7.

Exercise 50

Prove that an Abelian group of order 20 has an element of order 5. Does your proof generalize to prove that every Abelian group of order $4p$ where p is prime has a subgroup of order p?

Solution:

Let G be an Abelian group with $|G| = 20 = 4 \cdot 5$.

By Lagrange's Theorem, elements of G have order dividing 20, so possible orders are: 1, 2, 4, 5, 10, 20.

Case 1: If G has an element of order 20, then its 4th power has order $20/\gcd(4, 20) = 20/4 = 5$. Done.

Case 2: If G has an element of order 10, then its square has order $10/\gcd(2, 10) = 10/2 = 5$. Done.

Case 3: G has no elements of order 20 or 10.

Then all non-identity elements have order 2, 4, or 5. Suppose G has no element of order 5. Then all non-identity elements have order 2 or 4. Clearly $G $ has a subgroup of order 4 say H. Pick a not in $ H$, then the subgroup $\langle a \rangle H$ has order: $|\langle a \rangle H| = |\langle a \rangle||H|/|\langle a \rangle \cap H|$ which is either 8 or 16 a contradiction to Lagrange Thm.

Therefore, we must have an element of order 5.

Generalization: Yes, the proof generalizes. For an Abelian group of order $4p$ where p is prime, by similar case analysis, we can show that there must exist an element whose order is divisible by p, hence a subgroup of order p.

Exercise 60

Prove that A_5 has a subgroup of order 12.

Solution:

It contains A_4 as a subgroup.

Exercise 61

Prove that A_5 has no subgroup of order 30.

Solution:

Suppose, for contradiction, that H is a subgroup of A_5 with $|H| = 30$.

Since $|A_5| = 60$ and $|H| = 30$, the index $|A_5 : H| = 60/30 = 2$.

Claim: H must contain all elements of A_5 of order 3.

There are 20 elements of order 3 in A_5 (these are the 3-cycles, and there are $\binom{5}{3} \cdot 2 = 20$ of them).

Suppose $\alpha \in A_5$ has order 3 but $\alpha \notin H$. Since $|A_5 : H| = 2$, there are exactly two cosets: H and αH.

Therefore, $A_5 = H \cup \alpha H$.

Now consider α^2. We have $\alpha^2 H$ is a coset of H. Since there are only two cosets, either $\alpha^2 H = H$ or $\alpha^2 H = \alpha H$.

If $\alpha^2 H = \alpha H$, then $\alpha^2 = \alpha h$ for some $h \in H$, giving $\alpha = h \in H$, contradicting our assumption.

Therefore, $\alpha^2 H = H$, which means $\alpha^2 \in H$.

But then $\langle \alpha \rangle = \langle \alpha^2 \rangle \subseteq H$ (since $|\alpha| = 3$ is prime), so $\alpha \in H$, again contradicting our assumption.

Therefore, all 20 elements of order 3 must be in H.

Claim: H must contain all elements of A_5 of order 5.

By the same argument (using the fact that $|A_5 : H| = 2$), all 24 elements of order 5 in A_5 must be in H.

But now H contains at least $1 + 20 + 24 = 45$ elements (identity, elements of order 3, and elements of order 5).

Since $|H| = 30 < 45$, we have a contradiction.

Therefore, A_5 has no subgroup of order 30.

Exercise 69

Let $G = \{(1), (12)(34), (1234)(56), (13)(24), (1432)(56), (56)(13), (14)(23), (24)(56)\}$.

a. Find the stabilizer of 1 and the orbit of 1.
b. Find the stabilizer of 3 and the orbit of 3.
c. Find the stabilizer of 5 and the orbit of 5.

Solution:

Part (a): Stabilizer and orbit of 1.

The stabilizer of 1 consists of all permutations in G that fix 1:

- (1) fixes 1
- $(12)(34)$ moves 1 to 2, so doesn't fix 1
- $(1234)(56)$ moves 1 to 2, so doesn't fix 1
- $(13)(24)$ moves 1 to 3, so doesn't fix 1
- $(1432)(56)$ moves 1 to 4, so doesn't fix 1
- $(56)(13)$ moves 1 to 3, so doesn't fix 1
- $(14)(23)$ moves 1 to 4, so doesn't fix 1
- $(24)(56)$ fixes 1

Therefore, $\text{stab}_G(1) = \{(1), (24)(56)\}$.

The orbit of 1 consists of all elements that 1 can be mapped to:

- (1) maps 1 to 1
- $(12)(34)$ maps 1 to 2
- $(1234)(56)$ maps 1 to 2
- $(13)(24)$ maps 1 to 3
- $(1432)(56)$ maps 1 to 4
- $(56)(13)$ maps 1 to 3
- $(14)(23)$ maps 1 to 4
- $(24)(56)$ maps 1 to 1

Therefore, $\text{orb}_G(1) = \{1, 2, 3, 4\}$.

Part (b): Stabilizer and orbit of 3.

The stabilizer of 3 consists of all permutations in G that fix 3:

- (1) fixes 3
- $(12)(34)$ moves 3 to 4
- $(1234)(56)$ moves 3 to 4
- $(13)(24)$ moves 3 to 1
- $(1432)(56)$ moves 3 to 2
- $(56)(13)$ moves 3 to 1
- $(14)(23)$ moves 3 to 2
- $(24)(56)$ fixes 3

Therefore, $\text{stab}_G(3) = \{(1), (24)(56)\}$.

The orbit of 3: By similar analysis, $\text{orb}_G(3) = \{1, 2, 3, 4\}$.

Part (c): Stabilizer and orbit of 5.

The stabilizer of 5 consists of all permutations in G that fix 5:

- (1) fixes 5
- $(12)(34)$ fixes 5
- $(1234)(56)$ moves 5 to 6
- $(13)(24)$ fixes 5
- $(1432)(56)$ moves 5 to 6
- $(56)(13)$ moves 5 to 6
- $(14)(23)$ fixes 5
- $(24)(56)$ moves 5 to 6

Therefore, $\text{stab}_G(5) = \{(1), (12)(34), (13)(24), (14)(23)\}$.

The orbit of 5: $\text{orb}_G(5) = \{5, 6\}$.

Exercise 71

Let $G = GL(2, \mathbb{R})$ and $H = SL(2, \mathbb{R})$. Let $A \in G$ and suppose that $\det A = 2$. Prove that AH is the set of all 2×2 matrices in G that have determinant 2.

Solution:

We need to prove two inclusions.

($\subseteq$) Every element of AH has determinant 2:

Let $B \in AH$. Then $B = Ah$ for some $h \in H = SL(2, \mathbb{R})$.

By definition of $SL(2, \mathbb{R})$, we have $\det h = 1$.

Using the multiplicative property of determinants:
$\det B = \det(Ah) = (\det A)(\det h) = 2 \cdot 1 = 2$

Therefore, every element of AH has determinant 2.

($\supseteq$) Every matrix in G with determinant 2 is in AH:

Let $B \in G$ with $\det B = 2$.

Consider $C = A^{-1}B$. Then:
$\det C = \det(A^{-1}B) = (\det A^{-1})(\det B) = \frac{1}{\det A} \cdot \det B = \frac{1}{2} \cdot 2 = 1$

Since $\det C = 1$, we have $C \in SL(2, \mathbb{R}) = H$.

Therefore, $A^{-1}B = C \in H$, which implies $B = AC \in AH$.

Conclusion: We have shown that AH equals the set of all 2×2 matrices in $GL(2, \mathbb{R})$ with determinant 2.