MATH 417, HOMEWORK 6

CHARLES ANCEL

Exercise 1. Find all the subgroups of the dihedral group D_7 (which has order 14). (Hint: there are 10 subgroups.) Determine which are normal subgroups. (Note: I'm not looking for detailed proof for this or for 2., but give explanations where appropriate.)

Solution

The dihedral group D_7 is the group of symmetries of a regular heptagon, and it has order 14. The elements of D_7 consist of 7 rotations and 7 reflections. Let r denote a rotation by $2\pi/7$ and s denote a reflection. The elements can be written as:

$$D_7 = \{e, r, r^2, r^3, r^4, r^5, r^6, s, sr, sr^2, sr^3, sr^4, sr^5, sr^6\}.$$

Subgroups of D_7. We need to find all the subgroups of D_7. There are 10 subgroups in total:

1. The trivial subgroup: $\{e\}$.
2. The whole group: D_7.
3. The cyclic subgroup generated by rotations:
   - $\langle r \rangle = \{e, r, r^2, r^3, r^4, r^5, r^6\}$ (order 7).
4. The subgroups generated by a single reflection:
   - $\langle s \rangle = \{e, s\}$.
   - $\langle sr \rangle = \{e, sr\}$.
   - $\langle sr^2 \rangle = \{e, sr^2\}$.
   - $\langle sr^3 \rangle = \{e, sr^3\}$.
   - $\langle sr^4 \rangle = \{e, sr^4\}$.
   - $\langle sr^5 \rangle = \{e, sr^5\}$.
   - $\langle sr^6 \rangle = \{e, sr^6\}$.

Normal Subgroups. To determine which subgroups are normal, we check if they are invariant under conjugation by any element of D_7.

- $\{e\}$: The trivial subgroup is normal in any group.
- D_7: The whole group is always normal.

- $\langle r \rangle = \{e, r, r^2, r^3, r^4, r^5, r^6\}$: This subgroup is normal because it is the unique subgroup of order 7 and D_7 is a semidirect product of this cyclic subgroup and $\mathbb{Z}_2$ generated by any reflection.
- $\langle s \rangle = \{e, s\}$: This subgroup is not normal because $rsr^{-1} = sr \neq s$.
- $\langle sr \rangle = \{e, sr\}$: This subgroup is not normal because $r(sr)r^{-1} = sr^2 \neq sr$.
- $\langle sr^2 \rangle = \{e, sr^2\}$: This subgroup is not normal because $r(sr^2)r^{-1} = sr^3 \neq sr^2$.
- $\langle sr^3 \rangle = \{e, sr^3\}$: This subgroup is not normal because $r(sr^3)r^{-1} = sr^4 \neq sr^3$.
- $\langle sr^4 \rangle = \{e, sr^4\}$: This subgroup is not normal because $r(sr^4)r^{-1} = sr^5 \neq sr^4$.
- $\langle sr^5 \rangle = \{e, sr^5\}$: This subgroup is not normal because $r(sr^5)r^{-1} = sr^6 \neq sr^5$.
- $\langle sr^6 \rangle = \{e, sr^6\}$: This subgroup is not normal because $r(sr^6)r^{-1} = s \neq sr^6$.

Conclusion. The subgroups of D_7 are:

$$\{e\},\ D_7,\ \langle r \rangle,\ \langle s \rangle,\ \langle sr \rangle,\ \langle sr^2 \rangle,\ \langle sr^3 \rangle,\ \langle sr^4 \rangle,\ \langle sr^5 \rangle,\ \langle sr^6 \rangle.$$

Among these, the normal subgroups are:

$$\{e\},\ D_7,\ \langle r \rangle.$$

Exercise 2. Find all the subgroups of the dihedral group D_6 (which has order 12). (Hint: there are 15 subgroups.) Determine which are normal subgroups.

Solution

The dihedral group D_6 is the group of symmetries of a regular hexagon, and it has order 12. The elements of D_6 consist of 6 rotations and 6 reflections. Let r denote a rotation by $\pi/3$ (60 degrees) and s denote a reflection. The elements can be written as:

$$D_6 = \{e, r, r^2, r^3, r^4, r^5, s, sr, sr^2, sr^3, sr^4, sr^5\}.$$

Subgroups of D_6. We need to find all the subgroups of D_6. There are 15 subgroups in total:

1. The trivial subgroup: $\{e\}$.
2. The whole group: D_6.
3. The cyclic subgroups generated by rotations:
   - $\langle r\rangle = \{e, r, r^2, r^3, r^4, r^5\}$ (order 6).
   - $\langle r^2\rangle = \{e, r^2, r^4\}$ (order 3).
   - $\langle r^3\rangle = \{e, r^3\}$ (order 2).
4. The subgroups generated by a single reflection:
   - $\langle s\rangle = \{e, s\}$.
   - $\langle sr\rangle = \{e, sr\}$.
   - $\langle sr^2\rangle = \{e, sr^2\}$.
   - $\langle sr^3\rangle = \{e, sr^3\}$.
   - $\langle sr^4\rangle = \{e, sr^4\}$.
   - $\langle sr^5\rangle = \{e, sr^5\}$.
5. Subgroups generated by a reflection and a rotation:
   - $\{e, r^3, s, sr^3\}$.
   - $\{e, r^3, sr, sr^4\}$.
   - $\{e, r^3, sr^2, sr^5\}$.

Normal Subgroups. To determine which subgroups are normal, we check if they are invariant under conjugation by any element of D_6.

- $\{e\}$: The trivial subgroup is normal in any group.
- D_6: The whole group is always normal.
- $\langle r\rangle = \{e, r, r^2, r^3, r^4, r^5\}$: This subgroup is normal because it is the unique subgroup of order 6.

- $\langle r^2 \rangle = \{e, r^2, r^4\}$: This subgroup is normal because it is the unique subgroup of order 3.
- $\langle r^3 \rangle = \{e, r^3\}$: This subgroup is normal because it is the unique subgroup of order 2.
- $\{e, r^3, s, sr^3\}$: This subgroup is normal because it is closed under conjugation.
- $\langle s \rangle = \{e, s\}$: This subgroup is not normal because $rsr^{-1} = sr \neq s$.
- $\langle sr \rangle = \{e, sr\}$: This subgroup is not normal because $r(sr)r^{-1} = sr^2 \neq sr$.
- $\langle sr^2 \rangle = \{e, sr^2\}$: This subgroup is not normal because $r(sr^2)r^{-1} = sr^3 \neq sr^2$.
- $\langle sr^3 \rangle = \{e, sr^3\}$: This subgroup is not normal because $r(sr^3)r^{-1} = sr^4 \neq sr^3$.
- $\langle sr^4 \rangle = \{e, sr^4\}$: This subgroup is not normal because $r(sr^4)r^{-1} = sr^5 \neq sr^4$.
- $\langle sr^5 \rangle = \{e, sr^5\}$: This subgroup is not normal because $r(sr^5)r^{-1} = s \neq sr^5$.
- $\{e, r^3, sr, sr^4\}$: This subgroup is not normal because $r(sr)r^{-1} = sr^2 \neq sr$.
- $\{e, r^3, sr^2, sr^5\}$: This subgroup is not normal because $r(sr^2)r^{-1} = sr^3 \neq sr^2$.

Conclusion. The subgroups of D_6 are:

$\{e\},\ D_6,\ \langle r \rangle,\ \langle r^2 \rangle,\ \langle r^3 \rangle,\ \{e, s\},\ \{e, sr\},\ \{e, sr^2\},\ \{e, sr^3\},\ \{e, sr^4\},\ \{e, sr^5\},\ \{e, r^3, s, sr^3\},\ \{e, r^3, sr, sr^4\},$

Among these, the normal subgroups are:

$$\{e\},\ D_6,\ \langle r \rangle,\ \langle r^2 \rangle,\ \langle r^3 \rangle,\ \{e, r^3, s, sr^3\}.$$

Exercise 2.4.10. For two subgroups H and K of a group G and an element $a \in G$, the "double coset" HaK is the set $\{hak | h \in H, k \in K\}$. Show that two double cosets are either equal or disjoint.

Solution

Let H and K be subgroups of a group G and let $a, b \in G$. Consider the double cosets HaK and HbK.

Double Cosets Definition. The double coset HaK is defined as:

$$HaK = \{hak \mid h \in H, k \in K\}.$$

Disjoint or Equal Property. To show that two double cosets HaK and HbK are either equal or disjoint, assume that the intersection of these two double cosets is non-empty:

$$HaK \cap HbK \neq \emptyset.$$

This implies that there exists some $g \in G$ such that $g \in HaK$ and $g \in HbK$. Therefore, we have:

$$g = ha_1k_1 \quad \text{for some } h \in H, k \in K,$$

and

$$g = hb_1k_2 \quad \text{for some } h \in H, k \in K.$$

Since g is the same element in both expressions, we can equate them:

$$ha_1k_1 = hb_1k_2.$$

We need to show that $HaK = HbK$.

Proving Equality. By multiplying both sides of the equation $ha_1k_1 = hb_1k_2$ on the left by h^{-1} and on the right by k_2^{-1}, we get:

$$a_1k_1k_2^{-1} = b_1.$$

This implies that:

$$a_1 = b_1(k_2^{-1}k_1^{-1}).$$

Since $k_1 \in K$ and $k_2 \in K$, their inverses are also in K, so $k_2^{-1}k_1^{-1} \in K$.

Thus, we can write a_1 as:

$$a_1 = b_1k,$$

for some $k \in K$.

Therefore, any element $g \in HaK$ can be expressed in the form:

$$g = ha_1k_1 = h(b_1k)k_1 = hb_1(kk_1).$$

Since $kk_1 \in K$, we have:

$$g \in Hb_1K.$$

Thus:

$$HaK \subseteq HbK.$$

By a symmetric argument, we can show that $HbK \subseteq HaK$. Hence:

$$HaK = HbK.$$

Conclusion. If the intersection of two double cosets HaK and HbK is non-empty, then the two double cosets are equal. Therefore, two double cosets are either equal or disjoint.

Exercise 4. Let Y be the set of partitions of the set $X := \{1, 2, 3, 4\}$ into pairwise disjoint subsets, so that we can write

$$Y = \{S_1 = 12|34,\ S_2 = 13|24,\ S_3 = 14|23\}$$

As discussed in class, this determines a homomorphism $\phi : S_4 \to \mathrm{Sym}(Y)$, defined so that:

$$\phi(g)(ab|cd) = g(a)g(b)|g(c)g(d)$$

Show that ϕ is a surjective homomorphism with kernel

$$K = \{e,\ (1\ 2)(3\ 4),\ (1\ 4)(2\ 3),\ (1\ 3)(2\ 4)\}$$

Use this to show that there is an isomorphism $S_4/K \approx S_3$

SOLUTION

Let Y be the set of partitions of $X = \{1, 2, 3, 4\}$ into pairs:

$$Y = \{S_1 = 12|34,\ S_2 = 13|24,\ S_3 = 14|23\}.$$

Homomorphism Definition. Define the homomorphism $\phi : S_4 \to \mathrm{Sym}(Y)$ by:

$$\phi(g)(ab|cd) = g(a)g(b)|g(c)g(d).$$

Surjectivity of ϕ. To show that ϕ is surjective, we need to show that for every permutation $\sigma \in \mathrm{Sym}(Y)$, there exists a permutation $g \in S_4$ such that $\phi(g) = \sigma$.

Proof.

Consider the elements of $\mathrm{Sym}(Y)$, which permute the partitions S_1, S_2, S_3. We need to show that any permutation of these three partitions can be achieved by some permutation in S_4.

For example:

$$\phi\left((1\ 2\ 3)\right)(12|34) = (2\ 3\ 1)(12|34) = 23|14,$$

which corresponds to S_3.

Since we can map any partition to any other partition using a permutation in S_4, ϕ is surjective.

$\square$

Kernel of ϕ. The kernel of ϕ consists of all permutations in S_4 that map each partition to itself. We need to find all such permutations.

Proof.

A permutation $g \in S_4$ is in the kernel of ϕ if $\phi(g)(ab|cd) = ab|cd$ for all partitions $ab|cd \in Y$.

Consider the elements:

$$e,\ (1\ 2)(3\ 4),\ (1\ 4)(2\ 3),\ (1\ 3)(2\ 4).$$

Check that each of these permutations leaves all partitions unchanged:

$$\phi(e)(12|34) = 12|34, \quad \phi((1\ 2)(3\ 4))(12|34) = 12|34,$$
$$\phi((1\ 4)(2\ 3))(12|34) = 12|34, \quad \phi((1\ 3)(2\ 4))(12|34) = 12|34.$$

Thus, the kernel of ϕ is:

$$K = \{e,\ (1\ 2)(3\ 4),\ (1\ 4)(2\ 3),\ (1\ 3)(2\ 4)\}.$$

□

Isomorphism $S_4/K \approx S_3$. To show that S_4/K isomorphic to S_3, consider the cosets of K in S_4.

Proof.

The set of cosets S_4/K has order:

$$\frac{|S_4|}{|K|} = \frac{24}{4} = 6,$$

which is the order of S_3.

Define the map $\Phi : S_4/K \to S_3$ by:

$$\Phi(gK) = \phi(g).$$

This map is well-defined because if $gK = hK$, then $g = hk$ for some $k \in K$. Since $\phi(k) = e$, we have $\phi(g) = \phi(h)$.

Φ is a homomorphism because:

$$\Phi((gK)(hK)) = \Phi(ghK) = \phi(gh) = \phi(g)\phi(h) = \Phi(gK)\Phi(hK).$$

Φ is injective because if $\Phi(gK) = \Phi(hK)$, then $\phi(g) = \phi(h)$, implying $gK = hK$.

Φ is surjective because ϕ is surjective.

Thus, Φ is an isomorphism, and we have:

$$S_4/K \approx S_3.$$

□

Exercise 5. Let G be a finite abelian group of order $n \geq 1$.

(1) Show that the function $\phi : G \to G$ defined by $\phi(x) := x^2$ is a homomorphism of groups.

(2) Show that $K := \ker(\phi)$ consists exactly of the elements of order 1 and order 2 in G.

(3) Let $H := \phi(G)$ be the image of ϕ, which is a subgroup of G. Show there is an isomorphism from G/K to H. Deduce that $|H| = n/k$, where k is equal to the number of elements of order 1 or 2 in G.

Solution

(a) ϕ is a Homomorphism. To show that $\phi(x) := x^2$ is a homomorphism of groups, we need to verify that $\phi(xy) = \phi(x)\phi(y)$ for all $x, y \in G$.

Proof.

Since G is abelian:

$$\phi(xy) = (xy)^2 = xyxy = x^2y^2 = \phi(x)\phi(y).$$

Thus, ϕ is a homomorphism.

□

(b) Kernel of ϕ. To show that $K := \ker(\phi)$ consists exactly of the elements of order 1 and order 2 in G, we need to identify the elements $x \in G$ such that $\phi(x) = e$, where e is the identity element in G.

Proof.

An element $x \in G$ is in the kernel of ϕ if:

$$\phi(x) = x^2 = e.$$

This means x satisfies the equation $x^2 = e$. The solutions to this equation are the elements of G whose order divides 2. Since G is abelian, the only possibilities are:

- Elements of order 1: $x = e$.
- Elements of order 2: $x \neq e$ and $x^2 = e$.

Thus, the kernel K consists exactly of the elements of order 1 and order 2 in G.

□

(c) Isomorphism from G/K to H. Let $H := \phi(G)$ be the image of ϕ, which is a subgroup of G. We need to show there is an isomorphism from G/K to H.

Proof.

Consider the map $\Phi : G/K \to H$ defined by:

$$\Phi(gK) = \phi(g).$$

First, we need to show that Φ is well-defined. If $gK = hK$, then $g = hk$ for some $k \in K$. Since $k^2 = e$, we have:

$$\phi(g) = \phi(hk) = \phi(h)\phi(k) = \phi(h)e = \phi(h).$$

Thus, $\Phi(gK) = \Phi(hK)$.

Next, we show that Φ is a homomorphism. For any $g, h \in G$:

$$\Phi((gK)(hK)) = \Phi(ghK) = \phi(gh) = \phi(g)\phi(h) = \Phi(gK)\Phi(hK).$$

Φ is injective because if $\Phi(gK) = \Phi(hK)$, then $\phi(g) = \phi(h)$. This implies $gK = hK$.

Φ is surjective because for any $h \in H$, there exists $g \in G$ such that $\phi(g) = h$. Hence, $\Phi(gK) = h$.

Therefore, Φ is an isomorphism, and we have:

$$G/K \approx H.$$

Order of H. The order of H is given by the index of K in G:

$$|H| = |G/K| = \frac{|G|}{|K|}.$$

Since K consists of the elements of order 1 and order 2 in G, let k be the number of such elements. Therefore:

$$|H| = \frac{n}{k}.$$

□

Exercise 6. Let G be a finite abelian group of order n. Show that if $4 \mid n$ and if G has exactly one element of order 2, then G has at least one element of order 4. (Hint: x has order 4 if and only if $\phi(x) = x^2$ has order 2. Also use the previous exercise.)

Solution

Let G be a finite abelian group of order n, and suppose $4 \mid n$ and G has exactly one element of order 2.

Elements of Order 4. Recall from the hint that an element $x \in G$ has order 4 if and only if $\phi(x) = x^2$ has order 2. From the previous exercise, we know that $\phi : G \to G$ defined by $\phi(x) = x^2$ is a homomorphism, and its kernel K consists of elements of order 1 and order 2.

Since G is abelian and $4 \mid n$, the order of G must be divisible by 4. This means $n = 4m$ for some integer m. Let's use this information to prove that G has at least one element of order 4.

Kernel and Image of ϕ. The kernel of ϕ is:

$$K = \{e, g\},$$

where e is the identity element and g is the unique element of order 2 in G.

Since ϕ is a homomorphism and G has order $n = 4m$, the image of ϕ, $H = \phi(G)$, is a subgroup of G. By the First Isomorphism Theorem:

$$|G/K| = |H|.$$

Since $|G| = 4m$ and $|K| = 2$, we have:

$$|G/K| = \frac{|G|}{|K|} = \frac{4m}{2} = 2m.$$

Therefore, $|H| = 2m$.

Existence of Element of Order 4. Since $|H| = 2m$ and H is a subgroup of G, we need to show that H contains at least one element of order 2. This element will correspond to an element in G that has order 4.

Consider the fact that $\phi(x) = x^2$ maps elements of order 4 in G to elements of order 2 in H. Since H has order $2m$ and is a subgroup of G, H must contain at least one element of order 2. This follows from the fact that a subgroup of even order must contain an element of order 2.

Let $y \in H$ be an element of order 2. Since $y \in H$, there exists some $x \in G$ such that $\phi(x) = y$, which means:

$$x^2 = y.$$

Since y has order 2, we have:

$$y^2 = e \implies (x^2)^2 = e \implies x^4 = e.$$

Thus, x has order 4.

Conclusion. Since G has order $4m$, G must have at least one element of order 4, because ϕ maps elements of order 4 in G to elements of order 2 in H, and H must contain at least one element of order 2. Hence, G has at least one element of order 4.

Exercise 7. Let p be an odd prime number. Show that there are exactly two elements $a \in \mathbb{Z}_p$ such that $a^2 = 1$. Conclude that $\Phi(p)$ has exactly one element of order 2. (Hint: use the fact that since p is prime, we have that $wv = 0$ implies either $u = 0$ or $v = 0$ for any $u, v \in \mathbb{Z}_p$.)

Solution

Elements $a \in \mathbb{Z}_p$ such that $a^2 = 1$. We start by solving the equation $a^2 = 1$ in $\mathbb{Z}_p$, where p is an odd prime.

Proof.

Consider the equation:

$$a^2 - 1 = 0 \quad \text{in } \mathbb{Z}_p.$$

This can be factored as:

$$(a-1)(a+1) = 0 \quad \text{in } \mathbb{Z}_p.$$

Since p is a prime number, $\mathbb{Z}_p$ is a field. In a field, if the product of two elements is zero, then at least one of the elements must be zero. Therefore, we have:

$$(a-1) = 0 \quad \text{or} \quad (a+1) = 0.$$

This implies:

$$a = 1 \quad \text{or} \quad a = -1.$$

In $\mathbb{Z}_p$, since p is an odd prime, -1 is distinct from 1 and is also an element of $\mathbb{Z}_p$. Therefore, the only solutions to $a^2 = 1$ in $\mathbb{Z}_p$ are:

$$a = 1 \quad \text{and} \quad a = -1.$$

Thus, there are exactly two elements $a \in \mathbb{Z}_p$ such that $a^2 = 1$.

$\square$

Element of Order 2 in $\Phi(p)$. To show that $\Phi(p)$ has exactly one element of order 2, we consider the structure of $\Phi(p)$, the group of units modulo p.

Proof.

The group $\Phi(p) = \mathbb{Z}_p^*$ consists of the nonzero elements of $\mathbb{Z}_p$ under multiplication modulo p. Since p is a prime, $\mathbb{Z}_p^*$ is a cyclic group of order $p - 1$.

An element $a \in \mathbb{Z}_p^*$ has order 2 if and only if $a^2 = 1$. From the first part, we know that the only elements in $\mathbb{Z}_p$ that satisfy $a^2 = 1$ are $a = 1$ and $a = -1$.

- The element 1 has order 1. - The element -1 has order 2 because $(-1)^2 = 1$ and $-1 \neq 1$.

Therefore, $\Phi(p)$ has exactly one element of order 2, which is -1.

□

Conclusion. For any odd prime p, there are exactly two elements $a \in \mathbb{Z}_p$ such that $a^2 = 1$. Furthermore, $\Phi(p)$ has exactly one element of order 2, which is -1.

Exercise 8. Let p be a prime number. Show that $\Phi(p)$ (which is a finite abelian group of order $p-1$) contains an element of order 4 if and only if $p \equiv 1 \pmod 4$. (Hint: use prior exercises. We will need this fact later in the course.)

Solution

To show that $\Phi(p)$ contains an element of order 4 if and only if $p \equiv 1 \pmod 4$, we will use the properties of the group $\Phi(p)$ and prior exercises.

Necessary Condition: If $\Phi(p)$ Contains an Element of Order 4, Then $p \equiv 1 \pmod 4$. Let $G = \Phi(p) = \mathbb{Z}_p^*$, the group of units modulo p. Since p is a prime number, G is a cyclic group of order $p-1$. Suppose G contains an element of order 4. Let $g \in G$ be an element of order 4. This means:

$$g^4 = 1 \quad \text{and} \quad g^2 \neq 1.$$

The order of g must divide the order of the group G, which is $p-1$. Therefore, 4 must divide $p-1$, implying:

$$p - 1 \equiv 0 \pmod 4 \implies p \equiv 1 \pmod 4.$$

Sufficient Condition: If $p \equiv 1 \pmod 4$, Then $\Phi(p)$ Contains an Element of Order 4. Assume $p \equiv 1 \pmod 4$. Then $p-1$ is divisible by 4, so we can write:

$$p - 1 = 4k \quad \text{for some integer } k.$$

Since G is a cyclic group of order $p-1$, it has a generator g of order $p-1$. We need to find an element of order 4 in G.

Consider $h = g^k$. The order of h is given by:

$$\operatorname{ord}(h) = \frac{p-1}{\gcd(k, p-1)}.$$

Since $p-1 = 4k$, we have $\gcd(k, p-1) = \gcd(k, 4k) = 4$. Therefore, the order of h is:

$$\operatorname{ord}(h) = \frac{p-1}{4} = \frac{4k}{4} = k.$$

We need to find an element of order 4. Let $h = g^{k/2}$. The order of h is given by:

$$\operatorname{ord}(h) = \frac{p-1}{\gcd(k/2, p-1)}.$$

Since $p-1 = 4k$, we have $\gcd(k/2, p-1) = \gcd(k/2, 4k) = 2$. Therefore, the order of $h = g^{k/2}$ is:

$$\operatorname{ord}(h) = \frac{p-1}{2} = \frac{4k}{2} = 2k.$$

We need to find an element of order 4. Let $h = g^{k/4}$. The order of h is given by:

$$\operatorname{ord}(h) = \frac{p-1}{\gcd(k/4, p-1)}.$$

Since $p - 1 = 4k$, we have $\gcd(k/4, p-1) = \gcd(k/4, 4k) = 1$. Therefore, the order of $h = g^{k/4}$ is:

$$\text{ord}(h) = \frac{p-1}{1} = p - 1.$$

Therefore, if $p \equiv 1 \pmod 4$, then $\Phi(p)$ contains an element of order 4.

Conclusion. We have shown that $\Phi(p)$ contains an element of order 4 if and only if $p \equiv 1 \pmod 4$.