Solution 8

Normal subgroups, quotient groups, Isomorphism theorems for groups

Let G be a group. We denote by $Z(G)$ the center of G.

1. Show that $Z(S_n)$ is trivial for $n \geqslant 3$.

   Solution: Let $\sigma \in S_n \smallsetminus \{\mathrm{id}\}$. Then there exist $i, j \in \{1, 2, \ldots, n\}$ such that $\sigma(i) = j$ and $i \neq j$. Since $n \geqslant 3$, there exists $k \in \{1, 2, \ldots, n\} \smallsetminus \{i, j\}$. Let τ be the permutation switching i and k and fixing all other elements. Then

   $$\begin{aligned} \tau\sigma(i) &= j \\ \sigma\tau(i) = \sigma(k) &\overset{(*)}{\neq} \sigma(i) = j \end{aligned}$$

   where in the inequality (*) we used the fact that σ is a bijection. This implies that $\tau\sigma \neq \sigma\tau$, so that $\sigma \notin Z(S_n)$. By arbitrarity of $\sigma \neq \mathrm{id}$, and since $\mathrm{id} \in Z(S_n)$ by definition, we have proven that $Z(S_n) = \{\mathrm{id}\}$.

2. Show that any subgroup of a cyclic group is cyclic.

   Solution: Let $G = \langle g \rangle$ be a cyclic group generated by $g \in G$. Let $H < G$ be a subgroup of G. If $G = \{e_G\}$, then G is cyclic, generated by e_G.

   Else, there exists $n \in \mathbb{Z} \smallsetminus \{0\}$ such that $g^n \in H$. If $n < 0$, then $(g^n)^{-1} = g^{-n} \in H$ because H is closed under taking inverses, so that we know that there exists $m \in \mathbb{Z}_{>0}$ such that $g^m \in H$. Now let $m_0 = \min\{m \in \mathbb{Z}_{>0} : g^m = h\}$. We claim that

   $$H = \langle g^{m_0} \rangle,$$

   which proves that H is cyclic.

   The inclusion '$\supset$' in due to the fact that H is a subgroup containing g^{m_0}, so it must contain $\langle g^{m_0} \rangle$, which is by definition the intersection of all subgroups containing g^{m_0}. Conversely, suppose that $x \in H$. Write $x = g^h$ and $h = qm_0 + r$ for $0 \leqslant r < m_0$. Then

   $$g^r = g^{h - qm_0} = x(g^{m_0})^{-q} \in H$$

   because $x \in H$ and $(g^{m_0})^{-q} \in H$ as we have already proven the inclusion '$\supset$'. By minimality of m_0, we must have $r = 0$, so that $x = g^h = g^{qm_0} \in \langle g^{m_0} \rangle$, proving the inclusion '$\subset$'.

3. Let $G := \mathbb{R}/\mathbb{Z}$. Prove that G is isomorphic to the group $\{z \in \mathbb{C}^\times : |z| = 1\}$.

   Solution: Consider the group homomorphism $f : \mathbb{R} \longrightarrow \mathbb{C}^\times$ sending $x \mapsto e^{ix}$. We have seen in Assignment 7, Exercise 1, that $\ker(f) = 2\pi\mathbb{Z}$ and $\mathrm{Im}(f) = \{z \in \mathbb{C}^\times : |z| = 1\}$. By the First Isomorphism Theorem for groups, f induces an isomorphism

$$\overline{f} : \mathbb{R}/(2\pi\mathbb{Z}) \xrightarrow{\sim} \{z \in \mathbb{C}^\times : |z| = 1\}.$$

   In order to conclude, we need to check that $\mathbb{R}/\mathbb{Z} \cong \mathbb{R}/(2\pi\mathbb{Z})$. This can be done by looking at the multiplication by 2π. More precisely, the map $m_{2\pi} : \mathbb{R} \longrightarrow \mathbb{R}$ sending $t \mapsto 2\pi t$ is a group isomorphism (it is additive by the distributive property in $\mathbb{R}$ and it has inverse $m_{(2\pi)^{-1}}$ sending $u \mapsto (2\pi)^{-1}u$). Composing $m_{2\pi}$ with the canonical projection $\mathbb{R} \longrightarrow \mathbb{R}/(2\pi\mathbb{Z})$ we obtain a surjective group homomorphism $\psi : \mathbb{R} \longrightarrow \mathbb{R}/(2\pi\mathbb{Z})$ sending $t \mapsto 2\pi t + (2\pi\mathbb{Z})$. Clearly, $\ker(\psi) = \mathbb{Z}$, so that by the First Isomorphism Theorem ψ induces a group isomorphism $G = \mathbb{R}/\mathbb{Z} \cong \mathbb{R}/(2\pi\mathbb{Z})$, which composed with $\overline{f}$ gives an isomorphism $G \cong \{z \in \mathbb{C}^\times : |z| = 1\}$.

   Aliter: Of course, one could directly define the group homomorphism $g : \mathbb{R} \longrightarrow \mathbb{C}^\times$ sending $r \mapsto e^{2\pi i r}$, and prove, similarly as in Assignment 7, Exercise 1, that $\ker(g) = \mathbb{Z}$ and $\mathrm{Im}(g) = \{z \in \mathbb{C}^\times : |z| = 1\}$. A single application of the First Isomorphism theorem will then give an isomorphism $G \xrightarrow{\sim} \{z \in \mathbb{C}^\times : |z| = 1\}$.

4. Let G be a group. Recall the group homomorphism $\rho : G \longrightarrow \mathrm{Aut}(G)$ seen in class, sending an element g to the automorphism $(x \mapsto gxg^{-1})$, that is the conjugation by x. We define the *group of inner automorphisms of* G as

$$\mathrm{Inn}(G) := \mathrm{Im}(\rho).$$

   (a) Prove that $\mathrm{Inn}(G) \lhd \mathrm{Aut}(G)$.

   We define the *group of outer automorphisms of* G as the quotient group $\mathrm{Out}(G) := \mathrm{Aut}(G)/\mathrm{Inn}(G)$.

   (b) Determine $\mathrm{Out}(S_3)$. [*Hint:* S_3 is generated by the two permutations: $\tau : (1 \mapsto 2 \mapsto 3 \mapsto 1)$ and $\sigma_{12} : (1 \mapsto 2 \mapsto 1,\ 3 \mapsto 3)$. Use Exercise 1]

   (c) Prove that $\mathrm{Out}(\mathrm{GL}_n(\mathbb{C})) \neq \{1\}$. [*Hint:* Complex conjugation, eigenvalues]

   (d) Suppose that $\mathrm{Aut}(G)$ is cyclic. Prove: G is abelian. [*Hint:* Exercise 2]

   Solution:

   (a) A general element of $\mathrm{Inn}(G)$ can be written as $\rho(g)$ for $g \in G$. It is the inner automorphism sending $x \mapsto gxg^{-1}$. Let $\sigma \in G$. Then, for each $x \in G$,

$$(\sigma\rho(g)\sigma^{-1})(x) = \sigma(g(\sigma^{-1}(x))g^{-1}) \overset{(*)}{=} \sigma(g)x\sigma(g^{-1}) \overset{(*)}{=} \sigma(g)x\sigma(g)^{-1}.$$

   In the equalities (*) we have used the fact that σ respects multiplication. By arbitrarity of x, this proves that $\sigma\rho(g)\sigma^{-1} = \rho(\sigma(g)) \in \mathrm{Inn}(G)$. Hence $\mathrm{Inn}(G)$ is stable under conjugation by elements in $\mathrm{Aut}(G)$, so that $\mathrm{Inn}(G) \lhd \mathrm{Aut}(G)$ by definition.

(b) As seen in class, the map $\rho : G \longrightarrow \mathrm{Aut}(G)$ has kernel $Z(G)$. For $G = S_3$ the map ρ is injective since $Z(S_3) = \{\mathrm{id}\}$ by Exercise 1. Hence $\mathrm{Inn}(S_3) \cong S_3$ has 6 elements.

The group S_3 is generated by the 3-cycle $\tau : (1 \mapsto 2 \mapsto 3 \mapsto 1)$ and the switch σ_{12} as stated in the hint. Indeed, the subgroup $\langle \tau, \sigma_{12} \rangle$ of S_3 contains the four elements $\mathrm{id}, \tau, \tau^2, \sigma_{12}$, and since its cardinality must divide $\mathrm{Card}(S_3) = 6$ by Lagrange's Theorem, the only possibility is that $\langle \tau, \sigma_{12} \rangle = S_3$.

Any group homomorphism is uniquely determined by the image of a set of generators, because a general element can be written as a finite product of generators and their inverses and a group homomorphism respects multiplication by definition. This means that any $\psi \in \mathrm{Aut}(S_3)$ is uniquely determined by $\psi(\tau)$ and $\psi(\sigma_{12})$. A group isomorphism must respect the order of the elements in the group[1]. This means that $\psi(\tau) \in \{\tau, \tau^2\}$ since it must have order 3, whereas $\psi(\sigma_{12}) \in \{\sigma_{12}, \sigma_{13}, \sigma_{23}\}$ since it must have order 2. Hence we have at most $2 \cdot 3 = 6$ possibilities for ψ, meaning that $\mathrm{Card}(\mathrm{Aut}(S_3)) \leqslant 6$. Hence

$$6 = \mathrm{Card}(S_3) = \mathrm{Card}(\mathrm{Inn}(S_3)) \leqslant \mathrm{Card}(\mathrm{Aut}(S_3) \leqslant 6$$

which proves that $\mathrm{Inn}(S_3) = \mathrm{Aut}(S_3)$, so that $\mathrm{Out}(S_3)$ is the trivial group.

(c) The complex conjugation of each entry of a given matrix gives a group endomorphism $\varphi : \mathrm{GL}_n(\mathbb{C}) \longrightarrow \mathrm{GL}_n(\mathbb{C})$, which we denote by an upper bar. Indeed, for each $A, B \in \mathrm{GL}_n(\mathbb{C})$,

$$\det(\overline{A}) = \overline{\det}(A) \neq \overline{0} = 0 \text{ and}$$
$$\overline{AB} = \overline{A}\,\overline{B}$$

because the expression of the determinant of A, as well as the expressions of the entries of AB consist of sums and multiplications of the entries of A (and B), and complex conjugation respects both sum and multiplication. Clearly, $\varphi \circ \varphi = \mathrm{id}_{\mathrm{GL}_n(\mathbb{C})}$, so that $\varphi \in \mathrm{Aut}(\mathrm{GL}_n(\mathbb{C}))$.

Suppose that $\varphi \in \mathrm{Inn}(\mathrm{GL}_n(\mathbb{C}))$. Then φ sends each matrix to a similar matrix, so that by what we saw in Linear Algebra it preserves the eigenvalue. Clearly this is not the case, because the matrix $i \cdot \mathrm{Id}_n$ has the only eigenvalue i, whereas $\varphi(i \cdot \mathrm{Id}_n) = -i\mathrm{Id}_n$ has the only eigenvalue $-i$, contradiction. This proves that $\varphi \in \mathrm{Aut}(\mathrm{GL}_n(\mathbb{C})) \setminus \mathrm{Inn}(\mathrm{GL}_n(\mathbb{C}))$, so that $\mathrm{Out}(\mathrm{GL}_n(\mathbb{C})) = \mathrm{Aut}(\mathrm{GL}_n(\mathbb{C}))/\mathrm{Inn}(\mathrm{GL}_n(\mathbb{C}))$ is not trivial.

(d) Since $\mathrm{Aut}(G)$ is assumed to be cyclic, by Exercise 2 the group $\mathrm{Inn}(G)$ is cyclic as well. The First Isomorphism Theorem applied on ρ tells us that $G/Z(G) \cong$

[1]Let $f : G \longrightarrow H$ be a group homomorphism and $g \in G$. Then $f(g)^{\mathrm{ord}}_G(g) = f(g^{\mathrm{ord}}_G(g)) = f(e_G) = e_H$, so that $\mathrm{ord}_H(f(g))|\mathrm{ord}_G(g)$. If f is an isomorphism, the same can be done in the other direction, so that we obtain $\mathrm{ord}_H(f(g)) = \mathrm{ord}_G(g)$.

$\mathrm{Inn}(G)$, so that $G/Z(G)$ is cyclic as well and we can write $\langle uZ(G)\rangle = G/Z(G)$ for some $u \in G$. This means that for each $g \in G$ there exists $n_g \in \mathbb{Z}$ such that $gZ(G) = (uZ(G))^{n_g} = u^{n_g}Z(G)$, i.e., such that $g = u^{n_g}y_g$ for some $y_g \in Z(G)$.

Let $g, h \in G$ and write $g = u^{n_g}y_g$, $h = u^{n_h}y_h$ for $y_g, y_h \in Z(G)$. Then

$$gh = u^{n_g}y_g u^{n_h}y_h = u^{n_g}u^{n_h}y_h y_g = u^{n_h}u^{n_g}y_h y_g = u^{n_h}y_h u^{n_g}y_g = hg.$$

The fact used in the equation above that two powers of u commute can be proven with an easy induction. This proves that G is abelian, as desired.

5. Let G be a group and H, K finite subgroups of G such that $\mathrm{Card}(H)$ and $\mathrm{Card}(K)$ are coprime.

   (a) Prove that $H \cap K = \{1\}$.

   (b) Suppose moreover that G is finite and $\mathrm{Card}(G) = \mathrm{Card}(H) \cdot \mathrm{Card}(K)$. Prove that $HK = G$.

   Solution:

   (a) Clearly, $e_G \in H \cap K$. Moreover, for $x, y \in H \cap K$, $xy^{-1} \in H$ because H is a subgroup of G and $xy^{-1} \in K$ because K is a subgroup of G. Hence $H \cap K$ is a subgroup of G and as such it is tautologically a subgroup of both H and K. By Lagrange's theorem, $\mathrm{Card}(H \cap K)$ divides both the cardinality of H and the cardinality of K. Since those two cardinalities are coprime, $\mathrm{Card}(H \cap K) = 1$ and $H \cap K$ is trivial.

   (b) If $H \lhd G$, the second isomorphism theorem gives an isomorphism

   $$\begin{aligned} K/(H \cap K) &\xrightarrow{\sim} HK/H \\ x(H \cap K) &\longmapsto xH. \end{aligned}$$

   which gives an equality of cardinalities

   $$\frac{\mathrm{Card}(K)}{\mathrm{Card}(H \cap K)} = \frac{\mathrm{Card}(HK)}{\mathrm{Card}(H)} \tag{1}$$

   from which we obtain by part (a) that $\mathrm{Card}(HK) = \mathrm{Card}(H)\mathrm{Card}(K) = \mathrm{Card}(G)$.

   Clearly equality (1) is enough to conclude, even when $H \not\lhd G$. In general, this equality can be proven by measuring how not uniquely an element $x \in HK$ can be written as $x = hk$ for $h \in H$ and $k \in K$. To do so, look at the map of sets $m : H \times K \longrightarrow HK$ sending $(h, k) \mapsto hk$. This map is well-defined and surjective by definition of HK.

   Fix $h_0 \in H$ and $k_0 \in K$. We want to find all $(h, k) \in H \times K$ such that $m(h_0, k_0) = m(h, k)$, i.e., $h_0k_0 = hk$. For $d := h_0^{-1}h \in H$, we see that

$h = h_0 d$ and $k = h^{-1} h_0 k_0 = d^{-1} k_0$, which means that $d = k^{-1} k_0 \in K$, so that $d \in H \cap K$ and $(h, k) = (h_0 d, d^{-1} k_0)$. Conversely, for each $d \in H \cap K$ we have $m(h_0 d, d^{-1} k_0) = m(h_0, k_0)$, and for $d \neq d'$ the elements $(h_0 d, d^{-1} k_0)$ and $(h_0 d', d'^{-1} k_0)$ do not coincide. This proves that

$$\mathrm{Card}(\{(h, k) \in H \times K : m(h, k) = m(h_0, k_0)\}) = \mathrm{Card}(H \cap K).$$

Partitioning $H \times K$ into subsets of elements with equal image under m, and using surjectivity of m, we can conclude that

$$\mathrm{Card}(H)\mathrm{Card}(K) = \mathrm{Card}(H \times K) = \mathrm{Card}(HK)\mathrm{Card}(H \cap K),$$

which implies equality (1) and hence the fact that $HK = G$.

6. Let G be a group. For $a, b \in G$, define their *commutator* as

$$[a, b] := aba^{-1}b^{-1} \in G.$$

Define the *commutator subgroup of* G as

$$[G, G] := \langle \{[a, b] : a, b \in G\} \rangle.$$

(a) Prove that G is abelian if and only if $[G, G]$ is trivial.

(b) Prove that $[G, G] \lhd G$.

(c) The *abelianization of* G is defined as the quotient group $G^{\mathrm{ab}} := G/[G, G]$. Prove: G^{ab} is an abelian group.

(d) Let $\pi : G \longrightarrow G^{\mathrm{ab}}$ be the canonical projection. Prove: for each abelian group A and group homomorphism $\varphi : G \longrightarrow A$, there exists a unique group homomorphism $\overline{\varphi} : G^{\mathrm{ab}} \longrightarrow A$ such that $\overline{\varphi} \circ \pi = \varphi$. [*Hint:* First, show that $[G, G] \subseteq \ker(\varphi)$]

Solution:

(a) Suppose that G is abelian. For any $a, b \in G$, $[a, b] = aba^{-1}b^{-1} = baa^{-1}b^{-1} = e_G$, so that $[G, G] =< e_G >= \{e_G\}$. Conversely, since $[G, G]$ contains all commutators, if $[G, G]$ is trivial then $[a, b] = aba^{-1}b^{-1} = e_G$ for all $a, b \in G$ and this is equivalent to $ab = ba$ for all $a, b \in G$, so that G is abelian.

(b) Let $u \in [G, G]$ and $g \in G$. Then

$$gug^{-1} = gug^{-1}u^{-1}u = [g, u]u \in [G, G],$$

so that $[G, G] \lhd G$.

(c) For every $x, y \in G$, we can write

$$\begin{aligned}(x[G, G])(y[G, G]) &= xy[G, G] = yxx^{-1}y^{-1}xy[G, G] \\ &= yx[x^{-1}, y^{-1}][G, G] = yx[G, G] = (y[G, G])(x[G, G]).\end{aligned}$$

This proves that G^{ab} is abelian.

(d) For every $g, h \in G$,

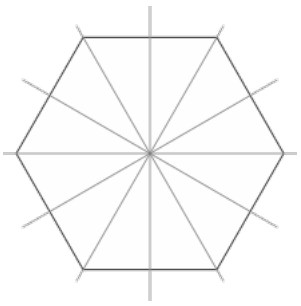
$$\varphi([g,h]) = \varphi(ghg^{-1}h^{-1}) = [\varphi(g), \varphi(h)] = e_A$$

by part (a). This tells us that $\ker(\varphi)$ contains all commutators and hence the whole $[G,G]$. Because of this, the map

$$\begin{aligned} \overline{\varphi} : G^{\mathrm{ab}} = G/[G,G] &\longrightarrow A \\ g[G,G] &\longmapsto \varphi(g) \end{aligned}$$

is a well-defined ring homomorphism, and it is the unique one for which we obtain $\overline{\varphi} \circ \pi = \varphi$, because this equality of maps implies that each $g[G,G] = \pi(g)$ can only be sent by $\overline{\varphi}$ to $\varphi(g)$.

7. Let $n \geqslant 3$ be an integer. Let D_n be the group of affine transformations of $\mathbb{R}^2$ mapping a regular polygon X_n of n sides to itself. Those transformations can be described in terms of permutations of the vertices of X_n. The group D_n contains $2n$ elements: n counterclockwise rotations by $2\pi k/n$ for $k = 0, \ldots, n-1$ around the center of X_n, as well as n symmetries with respect to lines through its center. In the picture below are drown, for $n = 6$, the symmetry axes of the 6 symmetries, the 6 rotations not being represented:



(a) Let T be the rotation by $2\pi/n$, and S one of the n symmetries. Prove that $STS^{-1} = T^{-1}$ [*Hint:* Notice that an element of D_n is uniquely determined by where it maps two adjacent vertices of X_n]

(b) Notice that for each integer k the element ST^k has order 2, and deduce that

$$D_n = \{\mathrm{id}, T, \ldots, T^{n-1}, S, ST, \ldots, ST^{n-1}\}.$$

(c) Determine $Z(D_n)$ for all n.

(d) Let now $n = 4$. Prove that $\langle S \rangle \lhd \langle S, T^2 \rangle \lhd D_4$, but $\langle S \rangle \not\lhd D_4$, and determine explicitly the left and right cosets of $\langle S \rangle$ in D_4.

Solution:

(a) As suggested by the hint, an element of D_n is uniquely determined by where it maps two adjacent vertices. If n is odd, each of the n symmetry axes passes through a vertex and in the midpoint of the opposite side. If n is even, half of those axes pass through two opposite vertices and the other half of them passes through midpoints of opposite sides.

We start by examining the case in which the axis describing the symmetry S passes through at least one vertex. Label such a vertex with 1 and the other vertices with $2, 3, \ldots, n$ in counterclowise order. Hence $T(k) = k + 1$ for $k = 1, \ldots, n-1$ and $T(n) = 1$. Clearly, $S^2 = \mathrm{id}_{X_n} = T^0$. In particular, $S = S^{-1}$. Notice moreover that $S(n) = 2$. Now apply $STS^{-1} = STS$ to the vertex 1. Since the symmetry axis of S passes through 1, we get:

$$\begin{aligned} S(1) = 1,\ T(1) = 2,\ S(2) = n &\implies STS(1) = n = T^{-1}(1); \\ S(2) = n,\ T(n) = 1,\ S(1) = 1 &\implies STS(2) = 1 = T^{-1}(2). \end{aligned}$$

This implies that $STS = T^{-1}$ in this case.

The only remaining case is the one in which n is even and the symmetry axis describing S passes through the midpoints of two opposite sides. Number the vertices of one of the two sides as 1 and 2 so that 2 is after 1 in counterclockwise order, and keep on numbering the other vertices as $3, \ldots, n$ in this order. Again, $T(k) = k + 1$ for $k = 1, \ldots, n-1$ and $T(n) = 1$, whereas for S we know that $S(1) = 2$ and $S(3) = n$. Then

$$\begin{aligned} S(1) = 2,\ T(2) = 3,\ S(3) = n &\implies STS(1) = n = T^{-1}(1); \\ S(2) = 1,\ T(1) = 2,\ S(2) = 1 &\implies STS(2) = 1 = T^{-1}(2). \end{aligned}$$

Again, $STS = T^{-1}$, as desired.

(b) Since S switches the vertices into a clockwise order (and back), while T does not, we see that $ST^k \neq T^\ell$ for each k and ℓ. Moreover, since T has order n, for each $0 \leqslant k < \ell \leqslant n-1$ we know that $T^k \neq T^\ell$ and $ST^k \neq ST^\ell$, which implies that we can write

$$D_n = \{\mathrm{id}, T, \ldots, T^{n-1}, S, ST, \ldots, ST^{n-1}\}$$

as desired. In fact, for each k we know by part (a) that

$$(ST^k)^2 = ST^kST^k = (STS)^kT^k = T^{-k}T^k = \mathrm{id},$$

so that the n elements ST^k are indeed the n axial symmetries.

(c) We know that $x \in Z(D_n)$ if and only if for each $g \in D_n$, $gxg^{-1} = x$. Clearly, $\mathrm{id} \in Z(D_n)$. Now we look at which other elements of D_n are stable under conjugation by any other element. In order to perform computations in D_n, we will repeatedly use that $ST^k = T^{-k}S$ because of part (a).

We start with computing the conjugates of the axial symmetries ST^k.

$$T^\ell ST^k (T^\ell)^{-1} = ST^{-\ell} T^{k-\ell} = ST^{k-2\ell},$$

which is different from ST^k when $\ell = 1$. Hence $ST^k \notin Z(D_n)$ for all k.
Now we look at the rotations T^k for $k = 1 \in \{1, \dots, n-1\}$. It is clear that T^k commutes with all rotations T^ℓ, so that we are left to check whether it commutes with all ST^ℓ.

$$ST^\ell T^k (ST^\ell)^{-1} = ST^\ell T^k ST^\ell = T^- k,$$

which coincides with T^k if and only if $n = 2k$.
Hence the size of the center depends on the parity of n. More precisely, we have proven that

$$Z(D_n) = \begin{cases} \{1\}, & n \text{ is odd} \\ \{1, T^{\frac{n}{2}}\}, & n \text{ is even.} \end{cases}$$

(d) We notice that $\langle S \rangle = \{1, S\}$, whereas $\langle S, T^2 \rangle = \{1, S, T^2, ST^2\}$ (because $T^2 S = SST^2 S = ST^{-2} = ST^2$). Hence $[D_4 : \langle S, T^2 \rangle] = [\langle S, T^2 \rangle : \langle S \rangle] = 2$ so that $\langle S \rangle \lhd \langle S, T^2 \rangle \lhd D_4$ because subgroup of index two are always normal[2]. But $TST^{-1} = SSTST^{-1} = ST^{-2} \notin \langle S \rangle$, so that $\langle S \rangle$ is not normal in D_4.
We know that there are $[D_4 : \langle S \rangle] = [D_4 : \langle S, T^2 \rangle][\langle S, T^2 \rangle : \langle S \rangle] = 4$ left (resp., right) cosets of $\langle S \rangle$ in D_4 and those are obtained by mulplying $\langle S \rangle$ on the left (resp., on the right) by elements of D_4:

- The left cosets of $\langle S \rangle$ are

$$\langle S \rangle = \{1, S\},\ ST\langle S \rangle = \{ST, T^3\},$$
$$ST^2\langle S \rangle = \{ST^2, T^2\},\ ST^3\langle S \rangle = \{ST^3, T\}.$$

- The left cosets of $\langle S \rangle$ are

$$\langle S \rangle = \{1, S\},\ \langle S \rangle ST = \{ST, T\},$$
$$\langle S \rangle ST^2 = \{ST^2, T^2\},\ ST^3 \langle S \rangle ST^3 = \{ST^3, T^3\}.$$

This makes it clear that $\langle S \rangle \not\lhd D_4$, as left and right cosets do not coincide.

8. Let G be a group and H, K subgroups of G.

(a) Prove that the intersection $xH \cap yK$ of two cosets of H and K respectively is either empty or a coset of $H \cap K$.

[2]Indeed, if a subgroup has index two, then left and right cosets of this subgroup coincide, as they both are given by the subgroup itself and its complement.

(b) Prove that each coset of $H \cap K$ is an intersection of a coset of H with a coset of K.

(c) Prove that if H and K have finite index in G, then $H \cap K$ has finite index as well.

Solution:

(a) Suppose that $xH \cap yK$ is non-empty and let $g \in xH \cap yK$. This means that $g = xh = yk$ for some $h \in H$ and $k \in K$. Then, for each $u \in H \cap K$, $gu = xhu = yku$, implying that $gu \in xH \cap yK$. This proves that $g(H \cap K) \subset xH \cap yK$. Conversely, if $g' = xh' = yk' \in xH \cap yK$ for some $h' \in H$ and $k' \in K$, then $g^{-1}g' = (xh)^{-1}xh' = h^{-1}h' \in H$, and $g^{-1}g' = (yk)^{-1}yk' = k^{-1}k' \in K$, so that $g^{-1}g' \in H \cap K$. This means that $g' \in g(H \cap K)$. We can then conclude that $g(H \cap K) = xH \cap yK$, so that $xH \cap yK$ is a coset of $H \cap K$.

(b) Let $g(H \cap K)$ be a coset of $H \cap K$. Then $g \in gH \cap gK$ and by the proof of part (a) we can conclude that $g(H \cap K) = gH \cap gK$.

(c) By part (b), we have an inequality

$$[G : (H \cap K)] \leqslant [G : H] \cdot [G : K]$$

and we can conclude because the right hand side is finite by assumption.