

H/wk 9, Solutions to selected problems

Ch. 2.8, Problem 7

If $H \triangleleft G$ and $|H| = 2$, show that $H \subseteq Z(G)$. Is this true when $|H| = 3$?

Solution.

Since $|H| = 2$, we have $H = \{1, a\}$, where $a \in G$ is such that $|a| = 2$.

Let $g \in G$ be arbitrary. Then $gHg^{-1} = \{g1g^{-1}, gag^{-1}\} = \{1, gag^{-1}\}$. Since $H \triangleleft G$, we have $gHg^{-1} = H$, that is $\{1, a\} = \{1, gag^{-1}\}$. Hence $a = gag^{-1}$, and so $ag = ga$. Since $g \in G$ was arbitrary, this means that $a \in Z(G)$. Also, obviously $1 \in Z(G)$. Therefore $H = \{1, a\} \subseteq Z(G)$, as required.

If $|H| = 3$ and $H \triangleleft G$, then H need not be contained in the center of G . For example, consider $G = S_3$ and $H = \langle (1\ 2\ 3) \rangle \leq S_3$. Since $|S_3| = 6$ and $|H| = 3$, we have $[S_3 : H] = \frac{6}{3} = 2$ and hence $H \triangleleft S_3$.

However, $H \not\subseteq Z(S_3)$. For example, $(1\ 2)(1\ 2\ 3) = (2\ 3)$ and $(1\ 2\ 3)(1\ 2) = (1\ 3)$. Hence $(1\ 2)(1\ 2\ 3) \neq (1\ 2\ 3)(1\ 2)$ and $(1\ 2\ 3) \notin Z(S_3)$ and therefore $H \not\subseteq Z(S_3)$.

Ch. 2.8, Problem 12.

Let $K \triangleleft G$, where K is cyclic. Show that every subgroup of K is normal in G .

Solution.

Let $K = \langle a \rangle$ for some $a \in G$. Let $H \leq K$ be an arbitrary subgroup. Since $H \leq K = \langle a \rangle$ it follows that $H = \langle a^d \rangle$ for some integer d .

If $|a| = 1$ then $a = 1$, $H = K = \{1\}$ and, obviously, $H \triangleleft G$. Thus from now on we will assume that $|a| > 1$.

Since K is normal in G , for every $g \in G$ we have $gKg^{-1} = K$. However, $gKg^{-1} = \langle gag^{-1} \rangle$, so that for every $g \in G$ we have $\langle gag^{-1} \rangle = \langle a \rangle$. Thus for every $g \in G$ the element gag^{-1} is a generator of $\langle a \rangle$.

Case 1. Suppose first that $|a| = \infty$.

We know from Ch 2.4 that in this case the only generators of $\langle a \rangle$ are a and a^{-1} .

Let $g \in G$ be arbitrary. Then $gag^{-1} = a$ or $gag^{-1} = a^{-1}$. If $gag^{-1} = a$ then $g\langle a^d \rangle g^{-1} = \langle a^d \rangle$, that is $gHg^{-1} = H$. If $gag^{-1} = a^{-1}$ then, $ga^d g^{-1} = a^{-d}$, $g\langle a^d \rangle g^{-1} = \langle a^{-d} \rangle = \langle a^d \rangle$, that is again $gHg^{-1} = H$. Thus for every $g \in G$ we have $gHg^{-1} = H$ and hence $H \triangleleft G$.

Case 2. Suppose now that $|a| = n < \infty$.

Let $g \in G$ be arbitrary. We know that $\langle gag^{-1} \rangle = \langle a \rangle$, which, by the results of Ch. 2.4, implies that $gag^{-1} = a^m$ for some integer m such that $\gcd(m, n) = 1$.

Then $gag^{-1} = a^m$ implies $ga^d g^{-1} = a^{md}$ and hence $g\langle a^d \rangle g^{-1} = \langle a^{md} \rangle$.

We claim that $\langle a^{md} \rangle = \langle a^d \rangle$. Indeed, the inclusion $\langle a^{md} \rangle \subseteq \langle a^d \rangle$ is obvious.

Since $\gcd(m, n) = 1$, there exist integers x, y such that $1 = xn + ym$ and hence $d = dxn + dym$. Therefore $a^d = a^{dxn} a^{dym} = (a^n)^{xn} (a^d)^{ym} = (a^d)^{ym}$

since $a^n = 1$. Thus $a^d = (a^d)^{ym}$ which implies that $\langle a^d \rangle \subseteq \langle a^{dm} \rangle$. Thus $\langle a^{md} \rangle = \langle a^d \rangle$ as claimed.

We have shown that for every $g \in G$ we have $g\langle a^d \rangle g^{-1} = \langle a^d \rangle$, that is $gHg^{-1} = H$. Therefore $H \triangleleft G$.

Ch. 2.8, Problem 17.

Let $D_n = \{1, a, \dots, a^{n-1}, b, ba, \dots, ba^{n-1}\}$ with $|a| = n$, $|b| = 2$ and $aba = b$.

(a) Show that every subgroup K of $\langle a \rangle$ is normal in D_n .

Solution.

Note that $aba = b$ implies $ba = a^{-1}b$ and hence $ba^i = a^{-i}b$ for every integer i . Similarly, $ab = ba^{-1}$ and hence $a^i b = ba^{-i}$ for every $i \in \mathbb{Z}$.

Let $K \leq \langle a \rangle$ be an arbitrary subgroup. Since $\langle a \rangle$ is cyclic, it follows that K is cyclic and $K = \langle a^d \rangle$ for some $d \geq 1$ such that $d|n$.

Let $(a^d)^j = a^{dj} \in K$ be an arbitrary element of K where $j \in \mathbb{Z}$.

For $i = 0, 1, \dots, n-1$ we have

$$a^i a^{dj} a^{-i} = a^{dj} \in K$$

and

$$ba^i a^{dj} a^{-i} b^{-1} = ba^{dj} b^{-1} = a^{-dj} b b^{-1} = a^{-dj} \in K.$$

Thus for every $g \in D_n$ we have $ga^{dj}g^{-1} \in K$. Since a^{dj} was an arbitrary element of K , it follows that $K \triangleleft D_n$.

(b) If n is odd and $K \triangleleft D_n$, show that $K = D_n$ or $K \subseteq \langle a \rangle$.

Solution.

Let $K \triangleleft D_n$ and suppose that $K \not\subseteq \langle a \rangle$. Then there exists $j \in \{0, 1, \dots, n-1\}$ such that $ba^j \in K$.

Since $K \triangleleft D_n$, it follows that $a^{-1}(ba^j)a \in D_n$. We have $a^{-1}(ba^j)a = baa^j a = ba^{j+2} \in K$. Since $ba^j \in K$ and $ba^{j+2} \in K$, and since K is a subgroup, it follows that $(ba^j)^{-1}(ba^{j+2}) = a^{-j}b^{-1}ba^{j+2} = a^2 \in K$.

Since n is odd, $n = 2l-1$ for some integer l . Then $1 = a^n = a^{2l-1} = a^{2l}a^{-1}$ and hence $a = a^{2l} = (a^2)^l$. Therefore $a \in K$ since $a^2 \in K$.

Since $a \in K$ and $ba^j \in K$, it follows that $ba^j a^{-j} = b \in K$. Thus $a, b \in K$. Therefore $D_n = K$ since every element of D_n is expressible in terms of a and b .

Ch. 2.8, Problem 20.

(a) Let $n = 2m$ where m is odd. Show that $D_n \cong C_2 \times D_m$.

Solution.

Recall that $D_n = \{1, a, \dots, a^{n-1}, b, ba, \dots, ba^{n-1}\}$ with $|a| = n$, $|b| = 2$ and $aba = b$. We also have $ba^i = a^{-i}b$ and $a^i b = ba^{-i}$ for every $i \in \mathbb{Z}$.

We have $|a^m| = n/m = 2$. Put $H = \langle a^m \rangle = \{1, a^m\}$. Thus H is a cyclic group of order 2, so that $H \cong C_2$.

Consider the set $K = \{1, a^2, a^4, \dots, a^{2m}, b, ba^2, ba^4, \dots, ba^{2m}\} \subseteq D_n$. It is not hard to check that $K \leq D_n$. Moreover, $|a^2| = n/2 = m$ and $a^2 b a^2 =$

$ba^{-2}a^2 = b$. Thus $|a^2| = m$, $|b| = 2$ and $a^2ba^2 = b$. Hence, by definition of the dihedral groups, K is a dihedral group of order $2m$, that is $K \cong D_m$.

Since by assumption $n = 2m$ and m is odd, $a^m \notin K$, so that $H \cap K = \{1\}$.

We claim that $H \triangleleft D_n$ and $K \triangleleft D_n$.

The fact that $H \triangleleft D_n$ follows from part (a) of Problem 17 since $H \subseteq \langle a \rangle$.

We also have $[D_n : K] = \frac{|D_n|}{|K|} = \frac{2n}{2m} = \frac{2 \cdot 2m}{2m} = 2$. Therefore $K \triangleleft D_n$.

Finally, notice that $|H| \cdot |K| = |D_n|$. Indeed, $|H| = 2$, $|K| = 2m$ and $|D_n| = 2n = 4m$, so that $2 \cdot 2m = 4m$.

Thus we have verified that $|D_n| = |H||K|$, $H \triangleleft D_n$, $K \triangleleft D_n$, $H \cap K = \{1\}$, $H \cong C_2$ and $K \cong D_m$. Therefore by Theorem 6 in Ch 2.8 we have $D_n \cong H \times K \cong C_2 \times D_m$.

(b) Is $D_{12} \cong C_3 \times D_4$?

Solution.

No, $D_{12} \not\cong C_3 \times D_4$ since these groups have different numbers of elements of order 2.

It is not hard to check (this was a problem from h/wk 8, namely problem 25(b) from Ch. 2.6) that in the group D_n we have $|ba^j| = 2$ for every $j = 0, 1, \dots, n-1$. Also, if n is even, there is exactly one element of order 2 in $\langle a \rangle$, namely $a^{n/2}$. Thus for every even $n \geq 2$ the group D_n has exactly $n+1$ elements of order 2. In particular, D_{12} has 13 elements of order 2.

On the other hand, the only elements of order 2 in $C_3 \times D_4$ are elements of the form $(1, g)$ where $g \in D_4$ and $|g| = 2$. The number of such elements is $4 + 1 = 5$.

Since $5 \neq 13$, it follows that $D_{12} \not\cong C_3 \times D_4$.

Ch. 2.9 Problem 8.

Let $K \leq H \leq G$ be finite groups with $K \triangleleft G$. Show that H/K is a subgroup of G/K and $[G/K : H/K] = [G : H]$.

Solution.

Recall that since $K \triangleleft G$, we have $gK = Kg$ for every $g \in G$ and $G/K = \{gK : g \in G\} = \{Kg : g \in G\}$. Also, $K \triangleleft G$ obviously implies $K \triangleleft H$ and $H/K = \{hK : h \in H\} = \{Kh : h \in H\}$.

Let $h_1, h_2 \in H$ be arbitrary, so that h_1K and h_2K are arbitrary elements of H/K . Then, by definition of multiplication in G/K , we have $h_1K \cdot h_2K = h_1h_2K \in H/K$ since $h_1h_2 \in H$.

Also, for an arbitrary $h \in H$ defining an arbitrary element hK of H/K we have $h^{-1} \in H$ and hence $h^{-1}K \in H/K$. By definition of the group G/K we have $h^{-1}K$ is the inverse of hK in G/K . Finally, the identity element of G/K is $1K = K$ and since $1 \in H$, we have $1K \in H/K$. Thus indeed $H/K \leq G/K$ is a subgroup.

By Lagrange's theorem we have $|G/K| = [G : K] = |G|/|K|$ and $|H/K| = [H : K] = |H|/|K|$. Hence, again by Lagrange's Theorem,

$$[G/K : H/K] = \frac{|G/K|}{|H/K|} = \frac{|G|/|K|}{|H|/|K|} = \frac{|G|}{|H|} = [G : H],$$

as required.

Ch. 2.9, Problem 10.

If $K \triangleleft G$ has index m in G , show that $g^m \in K$ for every $g \in G$.

Solution.

Consider the factor group G/K . Then $|G/K| = [G : K] = m$. By Corollary 2 in Ch. 2.6, since G/K is a group of order m , the m -th power of every element of G/K is equal to the identity element $1K$ of G/K . Thus for any $g \in G$ we have $g^m K = (gK)^m = 1K = K$ which implies that $g^m \in K$, as required.

Ch. 2.9, Problem 17.

If G is abelian let $T(G)$ be the set of all elements of G of finite order.

(a) Show that $T(G)$ is a subgroup of G - the **torsion subgroup**.

Solution.

Let $a, b \in T(G)$, so that $|a| = n < \infty$, $|b| = m < \infty$. Then, since G is abelian, we have $(ab)^{nm} = a^{nm}b^{nm} = (a^n)^m(b^m)^n = 1$. Thus ab has finite order and hence $ab \in T(G)$.

Also, if $a \in T(G)$, that is $|a| < \infty$ then $|a^{-1}| = |a| < \infty$ and hence $a^{-1} \in T(G)$. Finally $|1_G| = 1 < \infty$ and hence $1_G \in T(G)$. Thus indeed $T(G) \leq G$ is a subgroup of G .

(b) Call G a **torsion-free group** if $T(G) = \{1\}$. Show that if G is abelian then $G/T(G)$ is torsion-free.

Solution.

Note first that since G is abelian, every subgroup of G is normal in G (in particular $T(G)$ is normal in G and every factor-group of G is again abelian). In particular, $G/T(G)$ is an abelian group.

Suppose $gT(G) \in T(G/T(G))$ where $g \in G$. We need to show that $gT(G) = 1T(G)$.

Let $n < \infty$ be the order of $gT(G)$ in the group $G/T(G)$. By definition of multiplication in $G/T(G)$ this means that $1T(G) = (gT(G))^n = g^n T(G)$ and hence $g^n \in T(G)$. Let $m = |g^n|$. Since $g^n \in T(G)$, this means that $m < \infty$. Thus $1 = (g^n)^m = g^{mn}$. Hence g has finite order $|g| \leq mn < \infty$ in G , that is $g \in T(G)$. Therefore $gT(G) = 1T(G)$ as required.

(c) Call G a **torsion group** if $T(G) = G$. If H is a subgroup of an abelian group G , show that G is a torsion group if and only if both H and G/H are torsion groups.

Solution.

Suppose that H and G/H are torsion groups. Let $g \in G$ be arbitrary. since G/H is a torsion group, the element gH has a finite order m in G/H and therefore $(gH)^m = g^m H = 1H$. This implies that $g^m \in H$. Since H is a torsion group, we have $|g^m| = n < \infty$. Then $g^{mn} = (g^m)^n = 1$ which implies that $|g| \leq mn < \infty$ and $g \in T(G)$. Since $g \in G$ was arbitrary, it follows that $G = T(G)$, as required.

Suppose now that G is a torsion group. Since $H \leq G$ and for every $h \in H$ the order of h in H is equal to the order of h in G (which is finite), it follows that every element of H has finite order, and so H is a torsion group. Let $gH \in G/H$ be an arbitrary element. Since G is a torsion group, $|g| = n < \infty$ and $g^n = 1$ in G . Therefore in G/H we have $(gH)^n = g^n H = 1H$, so that gH has order $\leq n < \infty$ in G/H . Thus every element of G/H has finite order, and G/H is a torsion group.

Ch. 2.9, Problem 18.

If $K \leq H \leq G$, where $K \triangleleft G$ and $[G : K]$ is finite, then prove that $[G/K : H/K]$ is also finite and that $[G/K : H/K] = [G : H]$.

Solution.

By a result of Problem 31 in Ch. 2.6 (whose solution is included below for completeness) we have $[G : K] = [G : H][H : K]$ and hence both $[G : H]$ and $[H : K]$ are finite.

By definition of the groups G/K we have $|G/K| = [G : K]$ and $|H/K| = [H : K]$.

Also by the result of Problem 9, Ch 2.9, above, H/K is a subgroup of G/K . Since the group G/K is finite, by Lagrange's Theorem we have:

$$[G/K : H/K] = \frac{|G/K|}{|H/K|} = \frac{[G : K]}{[H : K]} = [G : H]$$

where the last equality holds since $[G : K] = [G : H][H : K]$.

Solution of Problem 31 in Ch. 2.6

We need to show that if $K \leq H \leq G$ then $[G : K] = [G : H][H : K]$. In particular, $[G : K]$ is finite if and only if both $[G : H]$ and $[H : K]$ are finite.

Solution.

Let I be a set (possibly infinite) such that $[H : K] = |I|$ and let J be a set (possibly infinite) such that $[G : H] = |J|$.

Choose a collection $(h_i)_{i \in I}$ of elements of H such that $H = \sqcup_{i \in I} h_i K$. Similarly, choose a collection $(g_j)_{j \in J}$ of elements of G such that $G = \sqcup_{j \in J} g_j H$. Then we have

$$G = \sqcup_{j \in J} g_j H = \sqcup_{j \in J} g_j (\sqcup_{i \in I} h_i K) = \sqcup_{j \in J, i \in I} g_j h_i K$$

Thus we have expressed G as a disjoint union of $|I| \cdot |J|$ -many left cosets of K . By definition of $[G : K]$ this implies that $[G : K] = |I| \cdot |J| = [H : K][G : H]$, as required.