Question 1

Let $K < H < G$ be subgroups. Show that $[G : K] = [G : H][H : K]$

Solution: Assuming that $[G : H]$ and $[H : K]$ is finite. By definition, $[H : K]$ is the number of left coset of K in H, so let $n = [G : H]$, we know that $\{ g_1H, g_2H, \dots, g_nH \}$ forms a partition of G. and let $m = [H : K]$ so that $\{ h_1K, h_2K, \dots, h_mK \}$ forms a partition of H.

Now, let $\bar{\cup}$ denote the operation union, which an assertion that the set is disjoint. Then, $g_i(h_1K \bar{\cup} h_2K \bar{\cup} \cdots \bar{\cup} h_mK)$ a left coset of H in G. Moreover, for each value of i, we must get a disjoint set, since it is a member of the partition of G mentioned above. Therefore,

$$g_1(h_1K \bar{\cup} h_2K \bar{\cup} \cdots \bar{\cup} h_mK) \bar{\cup} \cdots \bar{\cup} g_n(h_1K \bar{\cup} h_2K \bar{\cup} \cdots \bar{\cup} h_mK) = G$$

and by distributing the g_i inside of the parentheses, a partition of G into cosets of K is created.

Note: Cconsider any g_ih_jK and $g_{i'}h_{j'}$. If $i \neq i'$ that g_ih_jK is in a partition g_i of G but $g_{i'}h_{j'}K$ cannot be in the same coset in G, as it would contradict that the set of $\{ g_iH \}$ forms a partition. Similarly, if $j \neq j'$ then g_ih_jK would be in the partition h_jK of g_iH but $g_{i'}h_{j'}K$ cannot be in the same coset even if $g_{i'}H = g_iH$ as it would contradict that $\{ h_j \}$ partitions H. So $g_ih_jK \cap g_{i'}h_{j'}K = \emptyset$ whenever $(i, j) \neq (i', j')$

Since the parition has nm elements, $[G : K] = nm = [G : H][H : K]$ by definition.

Otherwise, if $[G : H]$ or $[H : K]$ is infinite, then there G should be partition into an infinite number of partitions by K Hence, $[G : K]$ should be infinite, and $[G : K] = [G : H][H : K]$ still holds, taking that multiplication with infinite number returns infinite number.

Question 2

Assume that both H and K have finite index in G. Prove that $H \cap K$ has finite index in G.

Solution: Firstly, if H and K have finite index in G, then denote the index of H as n and the index of K as m. Then, there is a partition of G into disjoint $\{ g_1H, g_2H, \dots, g_nH \}$ and a partition of G into dishoint $\{ g'_1K, g'_2K, \dots, g'_mK \}$.

Consider if $gK = K$ and $gH = H$, then $g \in K$ and $g \in H$, which means $g \in H \cap K$. Now,

$$\{ g_1, \dots, g_n \} (H \cap K) = \{ g_1 \dots, g_n \} H \cap \{ g_1, \dots, g_n \} K = \{ g_1, \dots, g_n \} K$$

Since it is possible to choose g_1 so that $g_1 \in H \cap K$ without loss of generality. So $\{ g_1, \dots, g_n \} (H \cap K) = \{ g_1, \dots, g_n \} K$ but $g_1 \in K$. So $\{ g_1(H \cap K), \dots, g_n(H \cap K) \}$ must cover a partition of K into cosets of $H \cap K$ in the sense that it might cover some other cosets of K. However, the size of the set of coset of $(H \cap K)$ that partitions K must be less than or equal to n, hence finite.

Now, since $[K : H \cap K]$ is finite, $[G : K]$ is finite, and $K \cap H < K < G$ as subgroup. Then the problem 1 asserts that $[G : H \cap K]$ is finite.

Question 3

Show that $S_n = \langle (1\ 2), (1\ 2\ 3 \cdots n) \rangle$ for all $n \geq 2$

Solution: For $n = 2$, $S_2 = \langle (1\ 2) \rangle$ trivially, as $(1\ 2)^2 = id$.

Now, for $n > 2$, notice that $(1\ 2\ 3 \cdots n)^{k-1} = \begin{pmatrix} 1 & 2 & \cdots & k-1 & k & \cdots & n \\ k & k+1 & \cdots & n & 1 & \cdots & k-1 \end{pmatrix}$ and that

$$\begin{aligned}
(1\ 2 \cdots n)^{-k}(12)(1\ 2 \cdots n)^k &= (1\ 2 \cdots n)^{-k} \begin{pmatrix} 1 & 2 & \cdots & k-1 & k & k+1 & \cdots & n \\ k & k+1 & \cdots & n & 2 & 1 & \cdots & k-1 \end{pmatrix} \\
&= \begin{pmatrix} 1 & 2 & \cdots & k & k+1 & \cdots & n \\ 1 & 2 & \cdots & k+1 & k & \cdots & n \end{pmatrix} \\
&= (k\ k+1)
\end{aligned}$$

Now, A transposition $(a\ b)$ is the product $(b-1\ b) \cdots (a+1\ a+2)(a\ a+1)(a+1\ a+2) \cdots (b-1\ b)$ Therefore, $(a\ b)$ for any a, b is in the group $\langle (1\ 2), (1\ l2 \cdots n) \rangle$

Now, since S_n is generated by transposition, $S_n = \langle (a\ b) \mid \forall a, b \rangle$, then S_n is generated by $\langle (1\ 2), (1\ 2 \cdots n) \rangle$

Question 4

Let G be a group of order pq, where p and q are primes. Prove that every proper subgroup of G is cyclic.

Solution: Firstly, we know that G is not trivial, as if it is the case, the order of G will be $1 \neq pq$ for any prime p, q. Let S be a subgroup of G, then by lagrange's theorem, $|G| = [G : S]\,|S|$, which means that $|S| = 1$, p, or q must hold. If $|S| = 1$, then S is trivially cyclic. Otherwise, An assumption that $|S| = p$ can be made without loss of generality.

Consider an element $s \in S$ such that s is not the identity. Now, $\langle s \rangle < S$ and $|\langle s \rangle| > 1$, so $|\langle s \rangle|$ must divides $|S|$ by the lagrange's theorem. However, since $|S| = p$, then $|\langle s \rangle|$ must be p.

Since $|S| = |\langle s \rangle|$ with $\langle s \rangle \leq S$, then, $S = \langle s \rangle$ is generated by one element, hence cyclic.

Question 5

Find a homomorphism $\phi : G \to H$ such that the image of ϕ is not normal in H.

Solution: Let $H = D_6 = \{\, 1, r, r^2, f, fr, fr^2 \,\}$. Then, consider $\phi : G = \mathbb{Z}/2\mathbb{Z} = \{\, \bar{0}, \bar{1} \,\} \to \{\, 1, f \,\}$ be a homomorphism where

$$\phi(\bar{0}) = 1$$
$$\phi(\bar{1}) = f$$

Then ϕ is a homomorphism since $\bar{0}$ is the identity of G and 1 is the identity of H. and $\phi(\bar{1} + \bar{1}) = \phi(\bar{0}) = 1 = f \cdot f = \phi(\bar{1}) \cdot \phi(\bar{1})$ Then, $\operatorname{im} \phi = \{\, 1, f \,\}$ and $rfr^{-1} = r^2 f \notin \{\, 1, f \,\}$. This asserts that $\operatorname{im} \phi$ is not normal in H.

Question 6

Show that every subgroup of index 2 is normal.

Solution: Let S be a subgroup of G with index 2. Then the coset $\{\, S, gS \,\}$ partitions G for some element $g \in G$. Note that $g \notin S$, since otherwise, $gS = S$ contradicts that S has index 2.

Now, consider the right coset Sg. We know that $g \notin S$. By assuming that $\exists s \in S, sg \in S$, we get $s^{-1}sg = g \in S$ by closure of S since sg and s^{-1} are both in S. Therefore, $\forall s \in S, sg \notin S$ Since $\{\, S, gS \,\}$ partitions G, and $Sg \neq S$ with $Sg \subset G$. The only possibility is that $Sg = gS$. Thus, S must be normal.

Question 7

Let $\phi : G \to G'$ be an epimorphism and $H \lhd G'$ a normal subgroup. Prove that $\phi^{-1}(H) \lhd G$ and $(G/\phi^{-1}(H)) \simeq G'/H$.

Solution: Consider $\varphi : G' \to G'/H$ such that $\varphi : g' \mapsto g'H$, then the homomorphism is an epimorphism since for every $g'H \in G'/H$, there is such g' that $\varphi(g') = g'H$. Consider $\ker \varphi = \{\, h \mid \varphi(h) = H \,\} = \{\, h \mid h \in H \,\} = H$. This means that $\varphi \circ \phi : G \to G'/H$ with $\varphi \circ \phi : g \mapsto \phi(g)H$ is an epimorphism with

$$\ker(\varphi \circ \phi) = \{\, h \mid \phi(h) \in H \,\} = \phi^{-1}(H)$$

Then by the first isomorphism theorem, $G'/\ker(\varphi \circ \phi) \simeq \operatorname{im}(\varphi \circ \phi)$, Hence $G/\phi^{-1}(H) \simeq G/H$

Question 8

Let m be a positive integer. Show that the map $\phi : \mathbb{Q}/\mathbb{Z} \to \mathbb{Q}/\mathbb{Z}$ given by $q + \mathbb{Z} \mapsto mq + \mathbb{Z}$ is a homomorphism and find $\ker(\phi)$

Solution: Consider the given definition of ϕ. Let $[q]$ denotes the equivalent class of $q + \mathbb{Z}$ in $\mathbb{Q}/\mathbb{Z}$. In other words, $[q] = q + n$ for some integer n. Then for $[q] = [q']$,

$$\exists n \quad \phi([q]) = [mq] = [mq + mn] = [mq'] = \phi([q'])$$

asserts that ϕ is well defined.

Now, consider

$$\phi([a] + [b]) = \phi([a + b]) = m[a + b] = [ma + mb] = [ma] + [mb] = \phi([a]) + \phi([b])$$

With the above equation, $\phi([a]+[b]) = \phi([a]) + \phi([b])$, so ϕ is a homomorphism.

Lastly, consider $\ker\phi = \{\, [q] \mid \phi([q]) = [0] \,\}$. It follows that $\ker\phi = \{\, [q] \mid [mq] = 0 \,\}$. However, $[mq] = 0$ is the same as $mq \in \mathbb{Z}$, and $q = \frac{a}{b}$ for some $a, b \in \mathbb{Z}$. Now, $mq \in \mathbb{Z}$ means that $m\frac{a}{b} \in \mathbb{Z}$, which is true whenever $b|m$.

So $\ker\phi = \{\, [\frac{a}{b}] \mid b|m, a \in \mathbb{Z} \,\}$. Note that for $a \geq b$, $[\frac{a}{b}] = [\frac{a-b}{b}]$. And similarly for $a \leq -b$. Therefore, $\ker\phi = \{\, [\frac{a}{b}] \mid a, b \in \mathbb{Z}, b|m, -b < a < b \,\}$

Question 9

Let $K \lhd G$ and $H \lhd G'$ be a normal subgroups. Show that $K \times H \lhd G \times G'$ and $(G \times G')/(K \times H) \simeq (G/K) \times (G'/H)$.

Solution: Firstly, for any any $(g, g') \in G \times G'$,

$$(g, g')K \times H = (g, g')\{\, (k, h) \mid k \in K, h \in H \,\} = gK \times g'H = Kg \times Hg' = K \times H(g, g')$$

Therefore, $K \times H$ is a normal subgroup of $G \times G'$

Now, consider φ, a homomorphism from $G \times G'$ to $(G/K) \times (G'/H)$ where $\varphi : (g, g') \mapsto (gK, g'H)$. Then, since K and H are normal subgroups, it is clear that φ is surjective, as $\{\, gK \,\}$ partitions G, so $\varphi_G : g \mapsto gK$ is surjective, and similar for H.

For $\ker\varphi$, consider that $\varphi((g, g')) = e$ means that $gK = e$ and $g'H = e$. This situation happens when $g \in K$ and $g' \in H$, hence, when $(g, g') \in K \times H$.

Therefore, by the first isomorphism theorem, $(G \times G')/\ker\varphi \simeq \operatorname{im}\varphi$, which in this case is $(G \times G')/(K \times H) \simeq (G/K) \times (G'/H)$

Question 10

Let G be a group of order p^2, where p is a prime. Show that either G is cyclic or every nontrivial element of G has order p.

Solution: For a group G of order p^2, if not every nontrivial element of G has order p, then there must be some element g that the order of g is not p and not 1.

Claim 1

For a finite group G, every element $g \in G$, $|g|$ divides $|G|$.

Proof: For an element g with order n, $\langle g \rangle$ is a subgroup of G. Moreover, $|\langle g \rangle| = n$ since for $1 \leq i, j \leq n$ if $i \neq j$ then $g^i \neq g^j$. This follows from the fact that if $g^i = g^j$ then $g^i - j = g^0$, thus $i - j = 0$ or $i - j|n$. However, since $\langle g \rangle$ is a subgroup of G, then $n = |\langle g \rangle|$ divides $|G|$ by lagrange's theorem. Hence, the order of g divides $|G|$. $\square$

However, by claim 1, $|g| \mid |G|$, so $|g| = 1$, p, or p^2 must hold. From the assumption, there must be an element g such that $g \neq p$, and $g \neq 1$. So $\exists g,\ |g| = p^2$. Since there is such element g, then $|\langle g \rangle| = p^2$, so G must be generated by g. Hence, G is cyclic.

Therefore, a group G is either cyclic, or the assumption that not all nontrivial elements are order p does not hold. Which is translated naturally into the question statement. which means that $\langle g \rangle = G$.