Problem 1. Let G be a finite group of order mn, where $\gcd(m,n) = 1$. Suppose that Q is a subgroup of G of order m. Let N be a normal subgroup of G.

a) Show that if H is a subgroup of G then $|H|$ can be written uniquely as $\alpha\beta$, where $\alpha|m$ and $\beta|n$.

In particular, $|N| = st$ with $s|m$ and $t|n$ and $|QN| = uv$ with $u|m$ and $v|n$.

b) Prove that $mt||QN|$. Conclude that $m = u$ and $t|v$.

c) Prove that $|QN/N|$ divides m. Conclude that $t = v$. Hint: Use the third isomorphism theorem.

d) Prove that $|QN/N| = m/s$. Conclude that $|N \cap Q| = s$.

Remark. Note that in the notation above we have $n = [G : Q]$ (Lagrange's Theorem). Thus our assumption is that $\gcd(|Q|, [G : Q]) = 1$. Any subgroup Q which satisfies this condition is called a **Hall subgroup** of G. So the can summarise the result of this problem as follows: if Q is a hall subgroup of G and N is a normal subgroup then $Q \cap N$ is a Hall subgroup of N.

Solution: a) By Lagrange's Theorem, $|H|||G| = mn$. Take $\alpha = \gcd(|H|, m)$, $\beta = \gcd(|H|, n)$. Then $\alpha||H|$, $\beta||H|$, $\gcd(\alpha, \beta) = 1$. It follows that $\alpha\beta||H|$. Now $\gcd(m/\alpha, |H|/\alpha) = 1$ and $\gcd(n/\beta, |H|/\beta) = 1$, so both m/α and n/β are relatively prime to $|H|/\alpha\beta$ and therefore $\gcd(mn/\alpha\beta, |H|/\alpha\beta) = 1$. On the other hand, $|H|/\alpha\beta$ divides $mn/\alpha\beta$. This can happen only if $|H|/\alpha\beta = 1$, which shows that $|H| = \alpha\beta$.

To show uniqueness, suppose that α_1, β_1 is another possibility. Then $\alpha_1|m$ and $\alpha_1||H|$ so $\alpha_1| \gcd(|H|, m) = \alpha$. Likewise, $\beta_1|\beta$. But $\alpha\beta = |H| = \alpha_1\beta_1$ so $\alpha = \alpha_1$ and $\beta = \beta_1$.

Remark. A shorter and simpler argument uses unique factorization of integers. $|H|$ is a product of prime powers and each of them divides either m or n but not both (since $\gcd(m, n) = 1$). Now α is the product of all those prime powers in $|H|$ which divide m and β is the product of the remaining prime powers in $|H|$ (i.e. those which divide n).

b) Since Q is a subgroup of QN, we have $m||QN|$. Similarly, N is a subgroup of QN so $st||QN|$ and therefore $t||QN|$. Since $\gcd(m,t) = 1$, we conclude that $mt||QN| = uv$. In particular, $m|uv$. Note that $\gcd(m,v) = 1$, so $m|u$. Recall now that $u|m$, so $u = m$. Similarly, $t|uv$ and $\gcd(u,t) = 1$, so $t|v$.

c) By the Third Isomorphism Theorem, the groups QN/N and $Q/(Q \cap N)$ are isomorphic, hence have the same order. But the order of $Q/(Q \cap N)$ divides the order of Q by Lagrange's Theorem, so we see that $|QN/N||m$.

d) By Lagrange's Theorem, $|QN/N| = uv/st = (u/s)(v/t) = (m/s)(v/t)$. Note that, by c), the order of $|QN/N|$ divides m. On the other hand, the factor v/t of $|QN/N|$ is prime to m, so it must be 1. Thus $|QN/N| = m/s$. Now recall that QN/N and $Q/(Q \cap N)$ are isomorphic, so $m/s = |Q/(Q \cap N)| = |Q|/|Q \cap N| = m/|Q \cap N|$. It follows that $s = |Q \cap N|$.

Problem 2. Let G and H be groups. On the set $G \times H$ define a multiplication by $(g,h)(a,b) = (ga, hb)$.

a) Prove that $G \times H$ with above defined multiplication is a group. It is called the **product** of G and H.

b) Prove that the maps $\pi_G : G \times H \longrightarrow G$ and $\pi_H : G \times H \longrightarrow H$ defined by $\pi_G(g,h) = g$ and $\pi_H(g,h) = h$ are homomorphisms. What are the kernels of these maps?

c) Suppose that $G = H$ and let $\Delta = \{(a,b) \in G \times G : a = b\}$. Prove that Δ is a subgroup of $G \times G$ which is isomorphic to G. Prove that Δ is normal iff G is abelian. If G is abelian, show that $G \times G/\Delta$ is isomorphic to G.

d) Let $f_1 : Q \longrightarrow G$ and $f_2 : Q \longrightarrow H$ be homomorphisms. Define $f : Q \longrightarrow G \times H$ by $f(a) = (f_1(a), f_2(a))$. Prove that f is a homomorphism and that $\ker f = \ker f_1 \cap \ker f_2$. Conclude that if A, B are normal subgroups of a group G then $G/(A \cap B)$ is isomorphic to a subgroup of $(G/A) \times (G/B)$.

Solution: a) We need to check the axioms. For associativity,

$$[(a,b)(m,n)](g,h) = (am, bn)(g,h) = ((am)g, (bn)h) = (a(mg), b(nh)) =$$

$$= (a,b)(mg, nh) = (a,b)[(m,n)(g,h)].$$

The identity of $G \times H$ is (e, e):

$$(g, h)(e, e) = (ge, he) = (g, h) = (eg, eh) = (e, e)(g, h).$$

Finally, the inverse of (g, h) is (g^{-1}, h^{-1}):

$$(g, h)(g^{-1}, h^{-1}) = (gg^{-1}, hh^{-1}) = (e, e).$$

b) We have

$$\pi_G((g, h)(a, b)) = \pi_G(ga, hb) = ga = \pi_G(g, h)\pi_G(a, b).$$

This shows that π_G is a homomorphism and same argument works for π_H. The kernel of π_G is the set of all pairs (g, h) such that $g = e$, so it is $\{e\} \times H$ (which is naturally isomorphic to H). Similarly, the kernel of π_H is $G \times \{e\}$.

c) Consider the map $f : G \longrightarrow G \times G$ defined by $f(g) = (g, g)$. Clearly Δ is the image of f. Note now that f is a homomorphism:

$$f(gh) = (gh, gh) = (g, g)(h, h) = f(g)f(h).$$

Since the image of a homomorphism is a subgroup, Δ is a subgroup. (Alternatively, you can just check directly that Δ is a subgroup). Since the kernel of f is trivial, we see that f gives an isomorphism between G and Δ.

Suppose that G is not abelian. Thus there are two elements g, h in G such that $gh \neq hg$, i.e. $hgh^{-1} \neq g$. Note that $(g, g) \in \Delta$ and $(h, e) \in G \times G$ but $(h, e)(g, g)(h, e)^{-1} = (hgh^{-1}, g) \notin \Delta$. Thus Δ is not normal in $G \times G$. Conversely, if G is abelian then so is $G \times G$, hence every subgroup of $G \times G$ is normal. In particular $\Delta \lhd G \times G$.

Suppose now that G is abelian. Consider the map $\phi : G \times G \longrightarrow G$ defined by $\phi(g, h) = gh^{-1}$. Note that ϕ is a homomorphism:

$$\phi((g, h)(a, b)) = \phi(ga, hb) = (ga)(hb)^{-1} = gab^{-1}h^{-1} = gh^{-1}ab^{-1} = \phi(g, h)\phi(a, b).$$

Since $g = \phi(g, e)$ for any $g \in G$, we see that ϕ is surjective. The kernel of ϕ consists of elements (g, h) such that $gh^{-1} = e$, i.e. $g = h$. Thus $\ker \phi = \Delta$. By the First Isomorphism Theorem, $G \times G/\Delta$ and G are isomorphic.

d) We have

$$f(ab) = (f_1(ab), f_2(ab)) = (f_1(a)f_1(b), f_2(a)f_2(b)) = (f_1(a), f_2(a))(f_1(b), f_2(b)) = f(a)f(b)$$

so f is a homomorphism. Note that $f(a) = e$ iff $f_1(a) = e$ and $f_2(a) = e$. This means that $\ker f = \ker f_1 \cap \ker f_2$.

Let now $f_1 : G \longrightarrow G/A$ and $f_2 : G \longrightarrow G/B$ be the canonical homomorphisms. Then f is a homomorphism from G to $(G/A)\times(G/B)$ whose kernel is $\ker f_1 \cap \ker f_2 = A \cap B$. By the First Isomorphism Theorem, the image of f (which is a subgroup of $(G/A) \times (G/B)$) is isomorphic to $G/(A \cap B)$.

Problem 3. Consider the dihedral group $D_{2n} = \{I, T, ..., T^{n-1}, S, ST, ..., ST^{n-1}\}$ of order $2n$. Let $f : D_{2n} \longrightarrow A$ be a homomorphism, where A is an abelian group.

a) Prove that $T^2 \in \ker f$.

b) Prove that if n is odd then the image of f has either one or two elements. Give example of a homomorphism f whith image of order 2.

c) Let n be even. Define a map $g : D_{2n} \longrightarrow \mathbb{Z}/2\mathbb{Z} \times Z/2\mathbb{Z}$ by

$$g(S^aT^b) = (a + 2\mathbb{Z}, b + 2\mathbb{Z}).$$

Prove that g is a surjective homomorphism and find its kernel.

d) Prove that if n is even then the image of f is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times Z/2\mathbb{Z}$ or $\mathbb{Z}/2$ or the trivial group.

Solution: a) Recall that $TS = ST^{-1}$. Since f is a homomorphism and A is abelian, we have $f(TS) = f(T)f(S) = f(S)f(T)$ and $f(ST^{-1}) = f(S)f(T)^{-1}$. Thus $f(S)f(T) = f(S)f(T)^{-1}$ and $f(T) = f(T)^{-1}$. This means that $f(T)^2 = e$, i.e. $f(T^2) = e$. Thus $T^2 \in \ker f$.

b) Suppose that $n = 2k-1$ is odd. Then $T = TT^{2k-1} = T^{2k} = (T^2)^k \in \ker f$. Thus, $\ker f$ contains the subgroup $< T >= \{I, T, T^2, ..., T^{n-1}\}$ which has index 2 in D_{2n}. It follows that either $\ker f =< T >$ or $\ker f = D_{2n}$. In the former case, the image of f has 2 elements and in the latter case it has one element (by the first isomorphism theorem).

To get an example note that $< T >$ is a normal subgroup of D_{2n} of index 2. Thus the canonical homomorphism $D_{2n} \longrightarrow D_{2n}/ < T >$ has image of order 2.

c) Note that g is well defined, since if $b_1 \equiv b_2 \pmod{n}$ then $b_1 \equiv b_2 \pmod{2}$ (for n odd, this is would not be true). Recall that $(S^aT^b)(S^mT^k) = S^{a+m}T^{k+(-1)^m b}$. Since $k + (-1)^m b \equiv k + b \pmod{2}$ we see that

$$g((S^aT^b)(S^mT^n)) = ((a+m)+2\mathbb{Z}, (k+(-1)^m b)+2\mathbb{Z}) = ((a+m)+2\mathbb{Z}, (k+b)+2\mathbb{Z}) =$$

$$= (a + 2\mathbb{Z}, b + 2\mathbb{Z}) + (m + 2\mathbb{Z}, k + 2\mathbb{Z}) = g(S^aT^b)g(S^mT^k).$$

This shows that g is a homomorphism. The kernel of g consists of S^aT^b such that a and b are even, so $\ker g =< T^2 >$. Now $g(S) = (1 + 2\mathbb{Z}, 0 + 2\mathbb{Z})$, $g(T) = (0 + 2\mathbb{Z}, 1 + 2\mathbb{Z})$, $g(ST) = (1 + 2\mathbb{Z}, 1 + 2\mathbb{Z})$, so g is surjective.

d) By a), we have $< T^2 > \subseteq \ker f$. By c), $D_{2n}/ < T^2 >$ is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times Z/2\mathbb{Z}$. The image of f is isomorphic to $D_{2n}/\ker f$. Let M be the subgroup of $\mathbb{Z}/2\mathbb{Z} \times Z/2\mathbb{Z}$ which corresponds to $\ker f$ in the Correspondence Theorem. By the second isomorphism theorem, $D_{2n}/\ker f$ is isomorphic to $(\mathbb{Z}/2\mathbb{Z} \times Z/2\mathbb{Z})/M$. If M is trivial, then we see that the image of f is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times Z/2\mathbb{Z}$. If $|M| = 2$ then $(\mathbb{Z}/2\mathbb{Z} \times Z/2\mathbb{Z})/M$ has 2 elements, hence it is isomorphic to $\mathbb{Z}/2\mathbb{Z}$. Finally, if $|M| = 4$ then the image of f is trivial.