Problem 26.
If H is a subgroup of G, prove that the group $N(H)/C(H)$ is isomorphic to a subgroup of $\mathrm{Aut}(H)$.

Proof. Recall that $C(H) = \{g \in G \mid ghg = h, \forall h \in H\} \leq N(H) = \{g \in G \mid gHg = H\} \leq G$. **By the notes on 9/12** we have that $C_n : H \to H$ where $C_n(h) = nhn^{-1}$ is an automorphism of H if $n \in N(H)$. Now let $f : N(H) \to \mathrm{Aut}(H)$ where $f(n) = \phi_n, \forall n \in N(H)$. We show f is a group homomorphism. $\forall n_1, n_2 \in N(H)$:

$$f(n_1n_2) = \phi_{n_1n_2} \coloneqq h \mapsto (n_1n_2)h(n_1n_2)^{-1} = \phi_{n_1}(n_2hn_2^{-1}) = \phi_{n_1}(\phi_{n_2}(h)) =: \phi_{n_1} \circ \phi_{n_2} = f(n_1)f(n_2).$$

So f is a group homomorphism from $N(H)$ to $\mathrm{Aut}(H)$. Next, we show that $\ker f = C(H)$.

$(\subseteq)$: $\forall n \in \ker f$, $f(n) = id \in \mathrm{Aut}(H)$. So then $\phi_n(h) = nhn^{-1} = h = id(h), \forall h \in H$. Therefore, $n \in C(H)$ and $\ker f \subseteq C(H)$.

$(\supseteq)$: $\forall n \in C(H)$ we have that $nhn^{-1} = h, \forall h \in H$ and so $\phi_n(h) = nhn^{-1} = h = id(h), \forall h \in H$. Therefore, $f(n) = \phi_n = id$, and $n \in \ker f$. So $C(H) \subseteq \ker f$.

We have now shown that $\ker f = C(H)$.

Finally, since f is a group homomorphism from $N(H)$ to $\mathrm{Aut}(H)$, by the **First isomorphism Theorem** we have that $N(H)/\ker f = N(H)/C(H) \cong f(N(H)) \leq \mathrm{Aut}(H)$.

Thus,

$$\text{If } H \leq G, \text{ then } N(H)/C(H) \text{ is isomorphic to some subgroup of } \mathrm{Aut}(H).$$

$\square$

Problem 27.
If $G/Z(G)$ is cyclic, then G is abelian.

Proof. Since $G/Z(G)$ is cyclic, $G/Z(G) = \langle [g] \rangle$ for some $g \in G$. Therefore, for any $a, b \in G$,

$$[a] = [g]^{\alpha} = [g^{\alpha}] \text{ for some } \alpha \in \mathbb{N} \tag{1}$$

$$[b] = [g]^{\beta} = [g^{\beta}] \text{ for some } \beta \in \mathbb{N} \tag{2}$$

$$(1) \implies g^{-\alpha} a \in Z(G) \tag{3}$$

$$(2) \implies g^{-\beta} b \in Z(G) \tag{4}$$

So then $g^{-\alpha} a = z_a \implies a = g^{\alpha} z_a$ and $g^{-\beta} b = z_b \implies b = g^{\beta} z_b$ for some $z_a, z_b \in Z(G)$. Observe.

$$ab = (g^{\alpha} z_a)(g^{\beta} z_b) = g^{\alpha} g^{\beta} z_b (z_a) = g^{\beta} (g^{\alpha}) z_b z_a = g^{\beta} z_b (g^{\alpha}) z_a = (g^{\beta} z_b)(g^{\alpha} z_a) = ba.$$

Thus,

If $G/Z(G)$ is cyclic, then G is abelian.

$\square$

Problem 28.
Every group of order 28, 56, 200 must contain a normal Sylow subgroup, and hence is not simple.

Note that the justification for **(I)** is not circular, the reader may find the proof of **Problem 35** on **Page 6**

Proof.

(I): $|G| = 28 = 4(7) = 2^2(7)$. So $|G| = p^2q$ where $p = 2, q = 7$. So by **Problem 35**, G is not simple since it contains a normal Sylow subgroup.

(II): $|G| = 56 = 8(7) = 2^3(7)$. By **Sylow's Theorems**, the number of distinct Sylow $7-$subgroups, n_7, is such that:

$$n_7 \equiv 1 \pmod 7 \text{ and } n_7 \mid 8 \implies n_7 \in \{1, 8\}.$$

If $n_7 = 1$, then there is a unique Sylow $7-$subgroup which is therefore normal. So G is not simple since it the Sylow subgroup is proper. If $n_7 = 8$, then there are 8 distinct Sylow $7-$subgroups $P_1, \ldots, P_8$. Since $P_i \cap P_j \leq P_i, P_j$ for any $1 \leq i < j \leq 8$, we have that $|P_i \cap P_j| \in \{1, 8\}$ but if it's 8 then the two aren't distinct. So $P_i \cap P_j = \{e\}$ for all $1 \leq i < j \leq 8$. Therefore, $|P_1 \cup \cdots \cup P_8| = 8(7) - 7 = 49$. Therefore, since by the remaining 7 non-identity elements must belong to $Q \setminus \{e\}$, where Q is a Sylow $2-$subgroup, given to exist since $2 \nmid 7$. This is formally justified as follows: Q subgroup only shares identity with any P_i since $g \in Q$ and $g \in P_i$ for all $i = 1, \ldots, 8$. Therefore, $G = P_1 \cup P_8 \cup Q$ implies that Q is a unique Sylow $2-$subgroup, which is therefore normal. So G is not simple.

(III): $|G| = 10(20) = 2(5)(4(5)) = 2^3 5^2$. By **Sylows Theorems**, the number of distinct Sylow $5-$subgroups, n_5, is such that:

$$n_5 \equiv 1 \pmod 5 \text{ and } n_5 \mid 8 \implies n_5 \in \{1, 2, 4, 8\}$$

But $2, 4, 8 \not\equiv 1 \pmod 5$. So $n_5 = 1$ and the Sylow $5-$subgroup is unique and therefore normal, as well as proper. So G is not simple.

□

Problem 30.
There is no simple group of order 24.

Proof. $|G| = 4(6) = 2^3(3)$, and so by **Sylow's Theorems**

$$n_2 \equiv 1 \pmod 2 \text{ and } n_2 \mid 3 \implies n_2 \in \{1,3\}$$

If $n_2 = 1$, then the Sylow $2-$subgroup is proper and unique and therefore normal. So G is not simple.

If $n_2 = 3$, then there are 3 distinct Sylow $2-$subgroups P_1, P_2, P_3 which must all have the trivial intersection $\{e\}$ otherwise they are not distinct. Therefore, $|P_1 \cup P_2 \cup P_3| = 3(2^3) - 2 = 22 = |G| - 2$. Therefore the remaining 2 non-identity elements must belong to the Sylow $3-$subgroup Q which exists by **Sylow's Theorems** since $3 \nmid 8$. This is formally justified via $g \in Q \cap P_i \implies |g|$ divides 2^3 and 3 which implies that $|g| = 1$ for any $i = 1,2,3$. Therefore, $|P_1 \cup P_2 \cup P_3 \cup Q| = 3(2^3) + 3 - 3 = |G| \implies G = P_1 \cup P_2 \cup P_3 \cup Q$, so Q is a unique Sylow $3-$subgroup, which is therefore normal and since it's proper, G is not simple.

□

Problem 31.
There is no simple group of order 36.

Proof. $|G| = 36 = 6(6) = 2^2 3^2$. So by **Sylow's Theorems**,

$$n_3 \equiv 1 \pmod 3 \text{ and } n_3 \mid 4 \implies n_3 \in \{1, 4\}$$

If $n_3 = 1$ then the proper Sylow $3-$subgroup is unique and therefore normal. So then G is not simple.

If $n_3 = 4$, then there are 4 distinct Sylow $3-$subgroups $P_1, \ldots, P_4$ and they all have pairwise trivial intersections otherwise they aren't distinct. So then $|P_1 \cup \cdots \cup P_4| = 4(3^2) - 3 = |G| - 3$. So then the remaining 3 non-identity elements must belong to the Sylow $2-$subgroup Q of order 4 which exists by **Sylow's Theorems** since $2 \nmid 9$. This is formally justified via $g \in Q \cap P_i \implies |g|$ divides 2^2 and 3^2 which implies that $|g| = 1$ for any $i = 1, \ldots, 4$. Therefore, $|P_1 \cup P_2 \cup P_3 \cup P_4 \cup Q| = 4(3^2) + (4) - 4 = |G| \implies G = P_1 \cup P_2 \cup P_3 \cup P_4 \cup Q$, so Q is a unique Sylow $2-$subgroup, which is therefore normal and since it's proper, G is not simple. $\square$

Problem 33.
There is no simple group of order 56.

Proof. $|G| = 56 \implies G$ is not simple by **Problem 28**.

$\square$

Problem 35.
Let G be a group of order p^2q where p,q are distinct primes. Show that G is not simple.

Proof. Since p,q are distinct primes, we have two cases.

$(\mathbf{q} < \mathbf{p}) \implies n_p \equiv 1 \pmod p$ and $n_p \mid q \implies n_p \in \{1,q\}$. But $2 \leq q < p \implies q \not\equiv 1 \pmod p$. So $n_p = 1$ and G is not simple.

$(\mathbf{p} < \mathbf{q}) \implies n_q \equiv 1 \pmod q$ and $n_q \mid p^2 \implies n_q \in \{1, p, p^2\}$. If $n_q = 1$, G is not simple. Next, since $p < q$ we have that $p \not\equiv 1 \pmod q$. Lastly, if $n_p = p^2$, then there are p^2 Sylow $q-$subgroups $Q_1, \ldots, Q_{p^2}$ of order q in G. Therefore, for any $1 \leq i < j < p^2$, since $Q_i \cap Q_j \leq Q_i, Q_j$, we have that $|Q_i \cap Q_j| \in \{1,q\}$. But if $|Q_i \cap Q_j| = q$, then $Q_i = Q_j$ and they are not distinct, a contradiction. So then $Q_i \cap Q_j = \{e\}$ and $Q_1 \cap \cdots \cap Q_{p^2} = \{e\}$. Therefore, $|Q_1 \cup \cdots Q_{p^2}| = p^2q - (p^2 - 1)$. So then the remaining $p^2 - 1$ non-identity elements must belong to the Sylow $p-$subgroup P of order p^2, given to exist by **Sylow's Theorems**. This is formally justified as follows: For any $i = 1, \ldots, p^2$, $Q_i \cap P = \{e\}$ since $g \in Q_i \cap P \implies |g|$ divides q and p^2, which have $\gcd(q, p^2) = 1$ otherwise $q|p^2 \implies q \in \{1, p, p^2\}$ all contradictions since q is prime and $q \nmid p$. So then,

$$|Q_1 \cup Q_{p^2} \cup P| = [p^2(q) - (p^2 - 1)] + p^2 - 1 = p^2q \implies G = Q_1 \cup \cdots Q_{p^2} \cup P.$$

Therefore P is a proper and unique Sylow p subgroup, and therefore it is normal. So then $P \triangleleft G$ and G is not simple.

Thus,

A group of order p^2q where p,q are distinct primes is not simple.

$\square$

Problem 36.
If every Sylow p-subgroup of a finite group G is normal for every prime p, then G is isomorphic to the direct product of its Sylow subgroups.

We begin by proving a Lemma.

Lemma 1. *$P \trianglelefteq G$ is a Sylow $p-$subgroup $\iff$ P is a unique Sylow $p-$subgroup in G.*

Proof. Let P be a Sylow $p-$subgroup of G. If P is normal, then $gPg^{-1} = P, \forall g \in G$. Well, for any Sylow $p-$subgroup Q, we have that there exists $g_* \in G$ such that $Q = g_*Pg_*^{-1} = P$. So P is unique. $\square$

Now we solve the problem.

Proof. To begin, we use $[n]$ to denote $\{1,\ldots,n\}$ throughout here.

Now, since G is finite, it's order has some prime decomposition $|G| = \prod_{i=1}^{n} p_i^{a_i}$ where $p_1,\ldots,p_n$ are distinct primes and $a_a \in \mathbb{Z}^+$ for all $i = 1,\ldots,n$. Notice that for any $k \in \{1,\ldots,n\}$, we have that $p_k^{a_k} \nmid p_i^{a_i}$ for all $i \in \{1,\ldots,n\} \setminus \{k\}$ otherwise p_k is 1 or a multiple of some prime p_i in our prime decomposition and therefore not prime, a contradiction. So then for each $k \in [n]$, $p_i \nmid \prod_{i\in[n]\setminus\{k\}} p_i^{a_i}$. Therefore, by **Sylow's Theorems** there exists a Sylow p_i-subgroup P_i of order $p_i^{a_i}$ for each $i \in [n]$.

Next, by **Lemma 1** each of these subgroups is unique since they are all normal by assumption. Also recall that by **Problem 10**, $HK = KH \iff HK \leq G$. Observe.

Since $P_1, P_2 \trianglelefteq G$, $P_1P_2 = P_2P_1 \implies P_1P_2 \leq G$ by **Problem 10**. Suppose $\prod_{i=1}^{k} P_i \leq G$ for some $2 \leq k < n$, and consider $\prod_{i=1}^{k+1} P_i$. Well, $\prod_{i=1}^{k+1} P_i = (\prod_{i=1}^{k} P_i)P_{k+1}$. Then, since $\prod_{i=1}^{k} P_i \leq G$ and $P_{k+1} \trianglelefteq G$, we have that $P_{k+1}(\prod_{i=1}^{k} P_i) = (\prod_{i=1}^{k} P_i)P_{k+1} \implies \prod_{i=1}^{k+1} P_i \leq G$. So then recursively we have that $|P_1 \cdots P_n| = \frac{|P_1|\cdots|P_n|}{|P_1\cap\cdots\cap P_n|}$.

Lastly, consider $P_i \cap P_j \leq P_i, P_j$ for $1 \leq i < j \leq n$. Well, $g \in P_i \cap P_j \implies |g|$ divides $p_i^{a_i}$ and $p_j^{a_j}$. So $|g| = p_i^m = p_j^n$ for some $(m,n) \in \mathbb{Z}_{a_i+1} \times \mathbb{Z}_{a_j+1}$. Therefore, $(m,n) = (0,0)$ otherwise once more p_i and p_j are not distinct primes. So then $P_i \cap P_j = \{e\}$ and we have that $P_1 \cap \cdots \cap P_n = \{e\}$.

Therefore, $|P_1 \cdots P_n| = \frac{|P_1|\cdots|P_n|}{|P_1\cap\cdots\cap P_n|} = \frac{\prod_{i=1}^{n} p_i^{a_i}}{1} = |G|$ and so $G = P_1 \cdots P_n$. Well, since $P_i \trianglelefteq G, \forall i \in [n]$, G is an internal direct product and finally we have that $P_1 \cdots P_n = G \cong P_1 \oplus \cdots \oplus P_n$.

$\square$

Problem 37.
If P is a normal Sylow p-subgroup of a finite group G and $f : G \to G$ is a group homomorphism, then $f(P) \subseteq P$.

Proof. Since P is a Sylow $p-$subgroup of G, $|G| = p^n m$ for some $m \in \mathbb{Z}^+$ where $p \nmid m$.

Next, let f_p be f whose domain is restricted to P. f_p is a group homomorphism since for any $a, b \in P$, we have that $f_p(ab) = f(ab) = f(a)f(b) = f_p(a)f_p(b)$. So by the **First Isomorphism Theorem**,

$$P/\ker f_p \cong f_p(P) = f(P).$$

Therefore, $|P/\ker f_p| = \frac{|P|}{|\ker f_p|} = |f(P)| \implies \frac{|P|}{|f(P)|} = |\ker f_p|$ and so $|f(P)|$ divides $|P| = p^n \implies |f(P)| = p^k$ for some $0 \leq k \leq n$. Observe.

$P \trianglelefteq G$ and $f(P) \leq G \implies gP = Pg, \forall g \in G \implies f(P)P = Pf(P) \implies f(P)P \leq G$ by **Problem 10**. Notice that $P \cap f(P)$ must be a $p-$subgroup of G since it is a subgroup of both P and $f(P)$. Therefore, $|f(P)P| = \frac{|f(P)||P|}{|f(P)\cap P|}$ must be some power of p and $f(P)P$ is a $p-$subgroup of G. Lastly, notice that $P \subseteq f(P)P$. Well, $P \not\subset f(P)P$, otherwise $f(P)P$ is a higher order $p-$subgroup of G than the Sylow $p-$subgroup P of G, a contradiction. Therefore $P = f(P)P$ and we must have that $f(P) \subseteq P$.

Thus,

If G is finite, and $P \trianglelefteq G$ is a Sylow p-subgroup and $f : G \to G$ is a group homomorphism, then $f(P) \subseteq P$.

□

Problem 38.
Let G be a cyclic group of order n. Let d be a divisor of n. Prove that G has a unique subgroup with d elements.

Proof. If $H = \{e\}$ it is cyclic. If H is non-trivial, then it contains some $h \neq e$. Well, since $h \in H \leq G$, $h = g^k$ for some $k \in \mathbb{Z}^+$. So then there exists some minimal non-trivial power $\mu = \min\{i \in \mathbb{Z}^+ \mid g^i \in H \setminus \{e\}\}$ of g present in $H \setminus \{e\}$. Observe.

By the division algorithm, $\forall m \in \{i \in \mathbb{Z}^+ \mid g^m = H \setminus \{e\}\}$, there exists a unique pair of naturals (q, r) with $0 \leq r < \mu$ such that

$$m = \mu q + r \implies g^m = g^{\mu q + r} = g^{\mu q} g^r \implies g^{m - \mu q} = g^r \in H.$$

Suppose $r \neq 0$. But then $g^r \in H$ for some $0 < r < \mu$ and μ is not minimal, a contradiction. So then $r = 0$ and for any $m \in \mathbb{Z}^+,$ such that $g^m \in H,$ $g^m = g^{\mu q_*} = (g^\mu)^{q_*}$ for some $q_* \in \mathbb{N}$. Therefore, $H = \langle g^\mu \rangle$, a cyclic group. So any subgroup of a cyclic group is cyclic.

Next, if G is finite and of order n, consider any divisor d of $|G| = n$. Since $G = \langle g \rangle$, $|g| = n$. Well, since $d|n$, $\exists! q \in \mathbb{Z}^+$ such that $dq = n$. So we see $g^{dq} = g^n \implies (g^q)^d = e$. Such a d is necessarily a minimal power that gives identity here since $0 < q, d$ and otherwise there exists $0 < k < n$ such that $k = d'q < dq = n$, and so $g^k = e$ and $|g| = k$, a contradiction. So $|g^q| = d$. Suppose $|g^{q'}| = d$ for some $q' \leq n$ with $q' \neq q$. But then $n = q'd < qd = n$, a contradiction. So there is only one power q of g with order d. Since any $d-$ordered subgroup H_d of G is cyclic, it must be generated by some power of G, of which there is only one and so $H_d = \langle g^d \rangle$ is the only subgroup of order d which divides n.

$\square$

Problem 39.
A semidirect product $H \rtimes_\varphi K$ is unchanged up to isomorphism if the action $\varphi : K \to \mathrm{Aut}(H)$ is composed with an automorphism of K. More precisely, for automorphisms $f : K \to K$, prove that $H \rtimes_{\varphi \circ f} K \cong H \rtimes_\varphi K$.

Proof. Let $\phi : H \rtimes_\varphi K \to H \rtimes_{\varphi \circ f} K$ be defined via $(h,k) \mapsto (h, f^{-1}(k))$. Since $\phi^{-1} := (h,k) \mapsto (h, f(k))$ is such that $\phi^{-1}(\phi((h,k))) = \phi^{-1}((h, f^{-1}(k))) = (h, f(f^{-1}(k))) = (h,k)$ and $\phi(\phi^{-1}(h,k)) = \phi((h, f(k))) = (h, f^{-1}(f(k))) = (h,k)$, ϕ has an inverse and is a bijection. We now show ϕ is a group homomorphism.

$$\phi((h_1,k_1)(h_2,k_2)) = \phi(h_1\varphi_{k_1}(h_2), k_1k_2) = (h_1\varphi_{k_1}(h_2), f^{-1}(k_1k_2)) = (h_1\varphi_{k_1}(h_2), f^{-1}(k_1k_2)) =$$
$$(h_1\varphi_{f(f^{-1}(k_1))}(h_2), f^{-1}(k_1)f^{-1}(k_2)) = (h_1, f^{-1}(k_1))(h_2, f^{-1}(k_2)) = \phi((h_1,k_1))\phi((h_2,k_2)).$$

Thus, ϕ is a group isomorphism and $H \rtimes_{\varphi \circ f} K \cong H \rtimes_\varphi K$.

$\square$