Lemma. *Suppose H and K are subgroups of G, with trivial intersection, such that each element of one commutes with each element of the other. Then $HK \cong H \times K$. Specifically, this holds if H and K are subgroups of G, with trivial intersection, that normalize each other.*

Proof. Suppose H and K are as described in the first sentence. By the second isomorphism theorem, HK is a subgroup of G (since clearly H and K normalize each other). Define $\varphi : H \times K \to HK$ by $\varphi(h, k) = hk$. The map is a homomorphism because

$$\varphi((x, y)(z, w)) = \varphi(xz, yw) = xzyw = xyzw = \varphi(x, y)\varphi(z, w).$$

If $(h, k) \in \ker \varphi$, then $hk = 1$, so $h, k \in H \cap K$, and thus $h = k = 1$. φ is clearly surjective as well, therefore it is an isomorphism.

For the latter statement, suppose H and K have trivial intersection and normalize each other. Then, for any $h \in H$ and $k \in K$, we have

$$K \ni (h^{-1}k^{-1}h)k = h^{-1}(k^{-1}hk) \in H.$$

so $h^{-1}k^{-1}hk = 1$, thus all elements of H commute with those of K. $\square$

23. Let P, P' be p-Sylow subgroups of a finite group G.

    (a) If $P' \subseteq N(P)$, then $P' = P$.

    Proof. Let $|P| = p^n$, and suppose P' normalizes P. Then by the second isomorphism theorem, $P'P$ is a subgroup of G with order $\dfrac{|P'||P|}{|P' \cap P|} = \dfrac{p^{2n}}{p^k}$ for some $k \leq n$. This is because $|P' \cap P|$ is a subgroup of P, hence its order divides p^n. If $k \neq n$, then $|P'P|$ has order p^m where $m > n$, contradicting that p^n is the highest power of p dividing $|G|$. Thus $k = n$, and so $|P' \cap P| = |P|$, hence $P' = P$. $\square$

    (b) If $N(P') = N(P)$, then $P' = P$.

    Proof. Since $P' \subseteq N(P') = N(P)$, this follows from the previous result. $\square$

    (c) We have $N(N(P)) = N(P)$.

    Proof. Clearly, $N(P) \subseteq N(N(P))$. For the reverse inclusion, suppose $g \in N(N(P))$. Then $gPg^{-1} \subseteq N(P)$, since $gN(P)g^{-1} = N(P)$ and $P \subseteq N(P)$. But gPg^{-1} is a p-Sylow subgroup, thus by part (a) we know that $gPg^{-1} = P$. So $g \in N(P)$. $\square$

24. Let p be a prime number. Show that a group of order p^2 is abelian, and that there are only two such groups up to isomorphism.

    Proof. Since G is nontrivial, it has a nontrivial center Z. If $Z = G$, then G is abelian, so suppose instead that $|Z| = p$. Then $G/Z \cong Z_p$. **We demonstrated in the previous homework (in the course of showing that if $\mathrm{Aut}(G)$ is cyclic then G is abelian) that if the quotient of a group by its center is cyclic, then the group is abelian.** Thus G is abelian (this case turns out to be vacuous, but still we have G abelian in all cases).

    Suppose $G \ncong Z_{p^2}$. Then all non-identity elements have order p. Let $x, y \in G$ be non-identity elements such that $y \notin \langle x \rangle$. Then we must have $\langle x \rangle \cap \langle y \rangle = \{1\}$, since $\langle x \rangle$ and $\langle y \rangle$ are both cyclic of prime order, so if their intersection was nontrivial then any nonidentity element would necessarily be a generator for both of them (a contradiction). Since G is abelian, $\langle x \rangle$ and $\langle y \rangle$ are normal. Also, $|\langle x \rangle\langle y \rangle| = \frac{|\langle x \rangle||\langle y \rangle|}{|\langle x \rangle \cap \langle y \rangle|} = |\langle x \rangle||\langle y \rangle| = |G|$, thus $G = \langle x \rangle\langle y \rangle$. By the lemma, then, $G \cong \langle x \rangle \times \langle y \rangle \cong \mathbb{Z}_p^2$.

    $\square$

25. Let G be a group of order p^3, where p is prime, and G is not abelian. Let Z be its center. Let C be a cyclic group of order p.

(a) Show that $Z \cong C$ and $G/Z \cong C \times C$.

Proof. Since G is a nontrivial p-group, it has a nontrivial center. But G is not abelian, so $Z \neq G$. This leaves $|Z| = p$ and $|Z| = p^2$ as possibilities. We cannot have $|Z| = p^2$, or else G/Z has order p and is thus cyclic, contradicting that G is not abelian. So Z has order p, and is thus isomorphic to C.

Now, G/Z has order p^2. By the result of the previous exercise, it is isomorphic to either C or C^2. But if $G/Z \cong C$, then again we must have that G is abelian, a contradiction. So $G/Z \cong C^2$. □

(b) Every subgroup of G of order p^2 contains Z and is normal.

Proof. Let H be such a subgroup. Clearly, H is normal because its index in G is p, which is the smallest prime dividing the order of G. Also, by exercise 24, H must be abelian.

Now, suppose that H does not contain Z. Then we must have $H \cap Z = \{1\}$, since Z is generated by any one of its nontrivial elements. So $G = HZ$ by the second isomorphism theorem (since H is normalized by Z and $|HZ| = \frac{|H||Z|}{|H \cap Z|} = p^3$). But H is abelian, and all of its elements commute with those of Z, so for any $h, k \in H$ and $x, y \in Z$ we have

$$(hx)(ky) = (hk)(xy) = (kh)(yx) = (ky)(hx)$$

contradicting that G is not abelian. So H must contain the center. □

(c) Suppose $x^p = 1$ for all $x \in G$. Show that G contains a normal subgroup $H \cong C \times C$.

Proof. We know that $G/Z \cong C^2$. C^2 has a subgroup of order p (for instance, $C \times \{0\}$), and this subgroup naturally lifts to a subgroup H of G such that $H/Z \cong C$ (by the third isomorphism theorem). So $|H| = |Z||C| = p^2$. By part (b), H is normal in G. By exercise 24, H is isomorphic to either $\mathbb{Z}_{p^2}$ or C^2. However, $\mathbb{Z}_{p^2}$ contains an element of order p^2, contradicting that $x^p = 1$ for all $x \in G$. Thus $H \cong C^2$. □

26. (a) Let G be a group of order pq, where p, q are primes and $p < q$. Assume that $q \not\equiv 1 \pmod{p}$. Prove that G is cyclic.

Proof. Let Q be a q-Sylow subgroup and P a p-Sylow subgroup. Since $p < q$, we again must have $P \cap Q = \{1\}$ since any nonidentity element in the intersection would have to generate both P and Q. The conjugation action of P on Q gives a homomorphism of P into the automorphism group of Q.

Q is a cyclic group of order q. For a fixed nonidentity element $x \in Q$, each automorphism is defined by its action on x. Specifically, there are $q - 1$ automorphisms, each sending x to a different nonidentity element of Q. The kernel K of P's action on Q must either be $\{1\}$ or P, since these are the only subgroups of P. If $K = \{1\}$ then $P \cong P/K \cong \operatorname{Im}\varphi \subseteq \operatorname{Aut} Q$, and so p divides $q - 1$. However, this contradicts that $q \not\equiv 1 \pmod{p}$, thus we must have $K = P$. So the action is trivial, meaning that $pqp^{-1} = q$ for all $p \in P$ and $q \in Q$, hence every element of P commutes with every element of Q.

By the lemma, $PQ \cong P \times Q$. Also, $G = PQ$ because $|PQ| = \frac{|P||Q|}{|P \cap Q|} = pq$. Since P and Q are cyclic with relatively prime orders, $P \times Q$ is cyclic, therefore G is cyclic. □

(b) Show that every group of order 15 is cyclic.

Proof. $15 = 3 \cdot 5$, and $5 \equiv 2 \not\equiv 1 \pmod{3}$, hence all groups of order 15 are cyclic by the result of part (a). □

27. Show that every group of order < 60 is solvable.

Proof. The trivial group is solvable by definition. Now, let $n < 60$ and consider a group G of order n. Suppose we have shown for all $m < n$ that all groups of order m are solvable. If n is prime, then G is cyclic and so is obviously solvable. Otherwise, suppose we can find a proper nontrivial normal subgroup $N \subsetneq G$. Then $|N|, |G/N| < n$, so by the inductive hypothesis we have abelian towers $1 = N_0 \subseteq N_1 \subseteq \cdots \subseteq N_j = N$ and $N/N = H_0/N \subseteq H_1/N \subseteq \cdots \subseteq H_k/N = G/N$ (the lattice isomorphism theorem tells us that the abelian tower for G/N must take this form, where $H_i \trianglelefteq H_{i+1}$ for each i). This yields an abelian tower for G:

$$1 = N_0 \subseteq N_1 \subseteq \cdots \subseteq N_j = N = H_0 \subseteq H_1 \subseteq \cdots \subseteq H_k = G.$$

Therefore, it suffices to show that G is not simple.

For many $n < 60$, we can easily verify that G is not simple unless it is cyclic. All nontrivial p-groups have nontrivial center, hence they are simple only if they are cyclic. If $|G| = pq^s$ for some primes $p < q$ and some integer $s \geq 1$, then a q-Sylow subgroup has index p, which is the smallest prime dividing $|G|$, and thus is normal.

For a more specific case, suppose $n = p^2q$ for some primes $p < q$. We know that $n_p \mid q$ and $n_q \mid p^2$. If either $n_p = 1$, then the p-Sylow subgroup P is stabilized by conjugation, hence is normal (and similarly if $n_q = 1$). So we may assume $n_p = q$ and $n_q = p$ or p^2. If $n_q = p^2$, we have a combinatorial issue regarding the size of G. Since the q-Sylows are cyclic, their pairwise intersections must be trivial. Similarly, they must have trivial intersection with each p-Sylow as well, else their intersection would generate an order q subgroup of a p-Sylow, contradicting that $q \nmid p$. So these q-Sylows, along with just one of the p-Sylows, account for $p^2(q-1) + (p^2-1) + 1 + p^2q = |G|$ elements of the group. This leaves no room for any more p-Sylows, contradicting that $n_p = 1$. Therefore, G contains a normal subgroup (either a p-Sylow or a q-Sylow).

Next, suppose p divides n with multiplicity s, and that $p > \frac{n}{p^s}$. Since $n_p \mid \frac{n}{p^2} < p$ and $n_p \equiv 1 \pmod{p}$, we must have $n_p = 1$. Therefore, the single p-Sylow is stabilized by conjugation, and thus is normal.

Again, suppose p divides n with multiplicity s. Consider the action of G on the set S of cosets of a p-Sylow subgroup P by conjugation. Assume that G is simple. Then the kernel K of the action is either $\{1\}$ or G. If $K = G$, however, then every element of G stabilizes every coset of P. In particular, they all stabilize P itself, thus P is normal - a contradiction. Therefore, $K = \{1\}$. This gives an embedding of G into $\mathrm{Perm}(S)$, which has order $(\frac{n}{p^s})!$. Therefore, if $(\frac{n}{p^s})! < n$, then G cannot be simple.

After applying each of these results to as many cases as possible, we have eliminated all cases except for $n = 30, 40$, and 56 (see the table below). For $n = 30$, we have $n_5 \mid 6$ and $n_5 \equiv 1 \pmod{5}$, so we may assume $n_5 = 6$. $n_3 \mid 10$ and $n_3 \equiv 1 \pmod{3}$, so we may assume $n_3 = 10$. Since 5 and 3 each divide n with multiplicity 1, all pairwise intersections between any two 3- or 5-Sylows must be trivial. So these alone must account for $6(5-1) + 10(3-1) + 1 = 45$ elements of G, a contradiction. For $n = 40$, we know n_5 divides 8 and is congruent to 1 (mod 5), leaving $n_5 = 1$ as the only possibility. For $n = 56$, we have $n_7 \mid 8$ and $n_7 \equiv 1 \pmod{7}$. So $n_7 = 8$. There is also at least one 2-Sylow of size 8. But these together account for $8(7-1) + (8-1) + 1 = 56$ elements of the group, leaving no room for any more 2-Sylows (since another would have to have at least one element not yet accounted for).

n	**Factorization**	**Reason**	30	$2 \cdot 3 \cdot 5$	
1		trivial	31	31	cyclic
2	2	cyclic	32	2^5	p-group
3	3	cyclic	33	$3 \cdot 11$	pq^s
4	2^2	p-group	34	$2 \cdot 17$	pq^s
5	5	cyclic	35	$5 \cdot 7$	pq^s
6	$2 \cdot 3$	pq^s	36	$2^2 \cdot 3^2$	$n > \frac{n}{p^s}!$
7	7	cyclic	37	37	cyclic
8	2^3	p-group	38	$2 \cdot 19$	pq^s
9	3^2	p-group	39	39	cyclic
10	$2 \cdot 5$	pq^s	40	$2^3 \cdot 5$	
11	11	cyclic	41	41	cyclic
12	$2^2 \cdot 3$	p^2q	42	$2 \cdot 3 \cdot 7$	$p > \frac{n}{p^s}$
13	13	cyclic	43	43	cyclic
14	$2 \cdot 7$	pq^s	44	$2^2 \cdot 11$	$p > \frac{n}{p^s}$
15	$3 \cdot 5$	pq^s	45	$3^2 \cdot 5$	p^2q
16	2^4	p-group	46	$2 \cdot 23$	pq^s
17	17	cyclic	47	47	cyclic
18	$2 \cdot 3^2$	pq^s	48	$2^4 \cdot 3$	$n > \frac{n}{p^s}!$
19	19	cyclic	49	7^2	p-group
20	$2^2 \cdot 5$	$p > \frac{n}{p^s}$	50	$2 \cdot 5^2$	pq^s
21	$3 \cdot 7$	pq^s	51	$3 \cdot 17$	pq^s
22	$2 \cdot 11$	pq^s	52	$2^2 \cdot 13$	$p > \frac{n}{p^s}$
23	23	cyclic	53	53	cyclic
24	$2^3 \cdot 3$	$n > \frac{n}{p^s}!$	54	$2 \cdot 3^3$	pq^s
25	5^2	p-group	55	$5 \cdot 11$	pq^s
26	$2 \cdot 13$	pq^s	56	$2^3 \cdot 7$	
27	3^3	p-group	57	$3 \cdot 19$	pq^s
28	$2^2 \cdot 7$	$p > \frac{n}{p^s}$	58	$2 \cdot 29$	pq^s
29	29	cyclic	59	59	cyclic

$\square$