1. (DF3.4.4) Use Cauchy's Theorem and induction to show that a finite abelian group has a subgroup of order n for each positive divisor n of its order.

   Proof. Let G be an arbitrary finite abelian group. We proceed by induction on the order of G; that is, we assume that for any finite abelian group H such that $1 \leq |H| < |G|$, the group H has a subgroup of order d for every positive divisor d of $|H|$. It suffices to show that G has a subgroup of order n for every positive divisor n of $|G|$. Whenever n is prime, we already have by Cauchy's theorem the existence of a subgroup of prime order n. So without loss of generality, let n be composite.

   Let p be any prime which divides n, so that for some positive integer $k > 1$ (as n is composite), $n = pk$. By Cauchy's Theorem, it follows that G has a subgroup N of order p. Then because all subgroups of abelian groups are abelian, it follows that N is normal in G and so the quotient group G/N is well defined.

   Because $n \mid |G|$, there exists a positive integer q such that $|G| = nq$. So by Lagrange's theorem, the order of the quotient group G/N is $|G|/|N| = nq/p = pkq/p = kq$, which because $k > 1$, the quotient group is not trivial. Furthermore, because $k > 1$ and p is a prime number, it follows that $|G/N| = kq < n$. Then by the inductive hypothesis, it follows that G/N contains a subgroup of order k, which by the Lattice Isomorphism Theorem we may write as A/N for some $N \trianglelefteq A \trianglelefteq G$ (all subgroups of G are normal in larger subgroups of G containing them because all subgroups of G are abelian).

   Then again using Lagrange's theorem we have that $|A/N| = |A|/|N| = |A|/p = k$, which means $|A| = pk = n$, so A is a subgroup of G with order n. $\square$

2. (DF3.4.1) Prove that if G is an abelian simple group then $G \cong Z_p$ for some prime p. (not a homework problem, but needed for DF3.4.8, the next exercise)

   Proof. Let G be an abelian simple group. Then there are no normal subgroups outside of the trivial subgroup and G itself. This means that for some element $x \neq 1$ in G, the subgroup $\langle x \rangle$ is normal in G because G is abelian, but because $x \neq 1$, this normal subgroup is equal to G. Hence G is cyclic.

   Then suppose that G is an infinite cyclic group. Then $\langle x \rangle = \{x, x^2, \dots\} = G$ but since $x^2 \neq 1$ (infinite order), $\langle x^2 \rangle = \{x^2, x^4, \dots\} \neq G$ but $\langle x^2 \rangle$ is normal in G because G is abelian. This is in contradiction to the assumption that G was simple. So G has finite order.

   Suppose that the order of G is composite. Then $|G| = pk$ for some prime p and some positive integer $k > 1$ ($|G|$ is composite). But by Cauchy's theorem, we know that there is a subgroup of G of order p, which is strictly less than $|G|$ and strictly greater than 1, which again is in contradiction to the assumption that G was simple. Hence the order of G is not composite; that is, the order of G is a prime number.

   Groups with prime order are known to be cyclic due to Lagrange's theorem. Therefore $G \cong Z_p$ for some prime p. $\square$

3. (DF3.4.8) Let G be a finite group. Prove that the following are equivalent:

(i) G is solvable (there is a chain of subgroups $1 = G_0 \trianglelefteq G_1 \trianglelefteq G_2 \trianglelefteq \cdots \trianglelefteq G_s = G$ such that G_{i+1}/G_i is abelian for $i = 0, 1, \ldots, s-1$)

(ii) G has a chain of subgroups: $1 = H_0 \trianglelefteq H_1 \trianglelefteq H_2 \trianglelefteq \cdots \trianglelefteq H_s = G$ such that H_{i+1}/H_i is cyclic, $0 \leq i \leq s-1$

(iii) all composition factors of G are of prime order

(iv) G has a chain of subgroups: $1 = N_0 \trianglelefteq N_1 \trianglelefteq N_2 \trianglelefteq \cdots \trianglelefteq N_t = G$ such that each N_i is a normal subgroup of G and N_{i+1}/N_i is abelian, $0 \leq i \leq t-1$.

Proof. We show that **(i)** is equivalent to **(ii)**, **(i)** is equivalent to **(iii)**, and that **(i)** is equivalent to **(iv)**.

From **(i)**, let G be a group with a chain of subgroups $1 = G_0 \trianglelefteq G_1 \trianglelefteq G_2 \trianglelefteq \cdots \trianglelefteq G_s = G$ such that G_{i+1}/G_i is abelian for $i = 0, 1, \ldots, s-1$). The factor groups G_{i+1}/G_i may not be simple, so we must insert intermediate subgroups within the chain which make simple and abelian subgroups.

If a factor group G_{i+1}/G_i is not simple, there exists a nontrivial proper normal subgroup of G_{i+1}/G_i, which because G_{i+1}/G_i is abelian, is also abelian. So by the Lattice Isomorphism Theorem, there exists a nontrivial proper normal subgroup A/G_i such that $G_i \leq A \trianglelefteq G_{i+1}$. Furthermore, because G_i is a normal subgroup of G_{i+1}, it follows that G_i is a normal subgroup of A.

So $G_i \trianglelefteq A \trianglelefteq G_{i+1}$, and A/G_i is abelian. We need to show that G_{i+1}/A is abelian. Because G_{i+1}/G_i is abelian, the multiplication of members xG_i, yG_i (with any $x, y \in G_{i+1}$) commute:

$$xG_iyG_i = xyG_i = yxG_i = yG_ixG_i$$

So $(yx)^{-1}xy \in G_i$, and by inclusion, $(yx)^{-1}xy \in A$, which means that $xAyA = xyA = yxA = yAxA$, so that the factor group G_{i+1}/A is abelian. It is possible for A/G_i or G_{i+1}/A or both to not be simple.

Therefore, it is possible to form a new chain of subgroups from the chain

$$1 = G_0 \trianglelefteq G_1 \trianglelefteq G_2 \trianglelefteq \cdots \trianglelefteq G_i \trianglelefteq G_{i+1} \trianglelefteq \cdots \trianglelefteq G_s = G$$

by replacing $G_i \trianglelefteq G_{i+1}$ with $G_i \trianglelefteq A \trianglelefteq G_{i+1}$ when G_{i+1}/G_i is not simple, to form

$$1 = G_0 \trianglelefteq G_1 \trianglelefteq G_2 \trianglelefteq \cdots \trianglelefteq G_i \trianglelefteq A \trianglelefteq G_{i+1} \trianglelefteq \cdots \trianglelefteq G_s = G.$$

Of course, we can keep expanding out the non-simple factors of this new series that we obtained, but because G is finite, by the Jordan-Hölder theorem, we will arrive at the composition series for G. By repeating the above procedure until all of the abelian factor groups N_{i+1}/N_i for $0 \leq i \leq t-1$ are simple in the final chain $1 = N_0 \trianglelefteq N_1 \trianglelefteq N_2 \trianglelefteq \cdots \trianglelefteq N_t = G$, we arrive at the composition series for G.

Then by the previous theorem which states that abelian simple groups are isomorphic to a cyclic group of prime order, all of these factor groups N_{i+1}/N_i are cyclic groups, so **(i)** implies **(ii)**. Because cyclic groups are abelian by exponent rules, **(ii)** implies **(i)**. Hence **(i)** is equivalent to **(ii)**.

Furthermore, by the same theorem, these factor groups (composition factors) N_{i+1}/N_i are of prime order, so **(i)** implies **(iii)**. Then if all of the composition factors of G are of prime order, then necessarily they are cyclic and hence abelian. So **(iii)** implies **(i)**. Hence **(i)** is equivalent to **(iii)**.

What remains is to show that **(i)** is equivalent to **(iv)**. It is clear that **(iv)** implies **(i)** because **(iv)** is a stronger statement:

(iv) G has a chain of subgroups: $1 = N_0 \trianglelefteq N_1 \trianglelefteq N_2 \trianglelefteq \cdots \trianglelefteq N_t = G$ such that each N_i is a normal subgroup of G and N_{i+1}/N_i is abelian, $0 \leq i \leq t-1$.

So not only are the subgroups N_i normal in N_{i+1} for $0 \leq i \leq t-1$, but they are normal in G. Conversely, assume **(i)** is true. Then let M be a minimal nontrivial normal subgroup of G, so that M does not contain any nontrivial proper subgroups which are normal in G. Let $N \trianglelefteq M$ be a normal subgroup of M of prime index, which exists because G has a composition series and so M has one as well (subgroups of solvable groups are solvable), so by **(iii)**, N exists.

Then the quotient M/N is cyclic, so it is abelian. This means that for any $x, y \in M$, $xNyN = xyN = yxN = yNxN$, which implies that $(yx)^{-1}xy \in N$. Similarly, consider gNg^{-1} for $g \in G$. This is a subgroup of G that is also a normal subgroup of M because for any $m \in M$, $mgNg^{-1}m^{-1} \subseteq gNg^{-1}$ is equivalent to showing that $g^{-1}mgN(g^{-1}mg)^{-1} \subseteq N$. But $M \trianglelefteq G$, so $g^{-1}mg, (g^{-1}mg)^{-1} \in M$, and we know that $N \trianglelefteq M$, so $g^{-1}mgN(g^{-1}mg)^{-1} \subseteq N$ is true. Then $mgNg^{-1}m^{-1} \subseteq gNg^{-1}$ is true, which means that gNg^{-1} is a normal subgroup of M.

Then the quotient M/gNg^{-1} is well defined, and because $\left|gNg^{-1}\right| = |N|$, this quotient has prime order as well, which means it is cyclic and hence abelian. Similarly, for any $x, y \in M$, $xgNg^{-1}ygNg^{-1} = xygNg^{-1} = yxgNg^{-1} = ygNg^{-1}xgNg^{-1}$, so that $(yx)^{-1}xy \in gNg^{-1}$. Since g was arbitrary, the following is true: $(yx)^{-1}xy \in \cap_{g\in G} gNg^{-1}$.

But observe that $\cap_{g\in G} gNg^{-1}$ is a subgroup of N since it contains only those elements of N which appear in each gNg^{-1}, and this set is a subgroup because the intersection of subgroups is a subgroup. Furthermore, $\cap_{g\in G} gNg^{-1}$ is also a normal subgroup of G: Let $h \in G$. We must show that

$$h\left(\bigcap_{g\in G} gNg^{-1}\right)h^{-1} \subseteq \bigcap_{g\in G} gNg^{-1},$$

but this is clear from the fact that any of the elements on the left hand side take on the form $g'n'(g')^{-1}$ for every $g' \in G$ and some $n' \in N$. Then $hg'n'(g')^{-1}h^{-1} = (g'h)n'(g'h)^{-1} \in \cap_{g\in G} gNg^{-1}$ since $g'h$ takes on any element of G. Hence the intersection is a normal subgroup of G.

But the minimality of M suggests that this subgroup of N (and hence a proper subgroup of M) should be the trivial subgroup, and since for every $x, y \in M$, $(yx)^{-1}xy \in \cap_{g\in G} gNg^{-1} = \{1\}$, we must have that $(yx)^{-1}xy = 1$ so that $xy = yx$. So M is abelian, and M was a minimal nontrivial normal subgroup of G. Furthermore, this means that $M/1$ is abelian as well.

Suppose by induction that for all groups of a strictly lower order than G which are solvable, there exists a chain of the form given in **iv** for the lower order groups, where G is solvable. Then consider the quotient group G/M, where M was a minimal nontrivial normal subgroup of G. This group is solvable because any chain of subgroups of the form $1 = \overline{G_0} \trianglelefteq \overline{G_1} \trianglelefteq \overline{G_2} \trianglelefteq \cdots \trianglelefteq \overline{G_r} = G/M$, which by the Lattice Isomorphism Theorem we can write $\overline{G_i} = A_i/M$ for some subgroup A_i containing M ($M \trianglelefteq A_i$). Then by the Third Isomorphism Theorem, we have that $\overline{G_{i+1}}/\overline{G_i} = (A_{i+1}/M)/(A_i/M) \cong A_{i+1}/A_i$, which are abelian since G is solvable. Hence the quotient group is solvable, furthermore, because M is nontrivial, the order of the quotient group G/M is strictly lower than the order of G and by the inductive hypothesis G/M has a series as given in **(iv)**, say $1 = \overline{G_0} \trianglelefteq \overline{G_1} \trianglelefteq \overline{G_2} \trianglelefteq \cdots \trianglelefteq \overline{G_r} = G/M$, with each $\overline{G_i} \trianglelefteq G/M$ where by the Lattice Isomorphism Theorem we can write $\overline{G_i} = G_i/M$ for some subgroup G_i containing M ($M \trianglelefteq G_i$). Furthermore, by the Lattice Isomorphism Theorem, each $G_i \trianglelefteq G$; and so by the Third Isomorphism Theorem it follows that $\overline{G_{i+1}}/\overline{G_i} = (G_{i+1}/M)/(G_i/M) \cong G_{i+1}/G_i$ we can form the chain of subgroups for G: $1 \trianglelefteq M = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_{r+1} = G$ where each G_i is normal in G as well. Each of the factors G_{i+1}/G_i (and $M/1$) will be abelian as well since $\overline{G_{i+1}}/\overline{G_i}$ is abelian by assumption, and M is abelian. Thus **(i)** implies **(iv)**, so that **(i)** is equivalent to **(iv)**.

Therefore, all four statements are equivalent to each other. □

4. (DF3.5.12) Prove that A_n contains a subgroup isomorphic to S_{n-2} for each $n \geq 3$.

Proof. Let $n \geq 3$, since A_1 and A_2 are both the trivial group. View S_n as the group of permutations of $\{1, 2, \ldots, n\}$, so that we can view S_{n-2} as the group of permutations of $\{1, 2, \ldots, n-2\}$, which are all the permutations of S_n which fix n and $n-1$. Let τ be the transposition in S_n which interchanges n and $n-1$; i.e. $\tau = ((n-1)\, n)$. Note that τ has order 2, and commutes with all elements of S_{n-2} which appear in S_n.

Then there is a homomorphism $\varphi\colon S_{n-2} \to A_n$ given by

$$\varphi(\sigma) = \begin{cases} \sigma, & \text{if } \sigma \text{ is an even permutation} \\ \sigma\tau, & \text{if } \sigma \text{ is an odd permutation} \end{cases}.$$

In both cases we obtain an even permutation (we make odd permutations even by appending τ on the right), so the image of the homomorphism is indeed a subgroup of A_n. We should check that this is a homomorphism. For permutations $\sigma, \pi \in S_{n-2}$, we investigate $\varphi(\sigma\pi)$ for each of the four ways we choose the parity of σ and π, remembering that $\tau^2 = 1$, and that τ commutes with all elements of S_{n-2} which appear in S_n.

σ	π	$\sigma\pi$	$\varphi(\sigma\pi) \overset{?}{=} \varphi(\sigma)\varphi(\pi)$
even	even	even	$\varphi(\sigma\pi) = \sigma\pi = \varphi(\sigma)\varphi(\pi)$
even	odd	odd	$\varphi(\sigma\pi) = \sigma\pi\tau = (\sigma)(\pi\tau) = \varphi(\sigma)\varphi(\pi)$
odd	even	odd	$\varphi(\sigma\pi) = \sigma\pi\tau = (\sigma\tau)(\pi) = \varphi(\sigma)\varphi(\pi)$
odd	odd	even	$\varphi(\sigma\pi) = \sigma\pi = \sigma\pi\tau^2 = (\sigma\tau)(\pi\tau) = \varphi(\sigma)\varphi(\pi)$

So φ is a homomorphism from S_{n-2} to A_n.

It is also true that φ is injective. Let $\varphi(\sigma) = \sigma\tau^a = \pi\tau^b = \varphi(\pi)$, for $a, b \in \{0, 1\}$. We reach a contradiction when $a \neq b$, because σ and τ were permutations in S_{n-2}, so they fix n and $n-1$. It is not possible to write

$\sigma = \pi\tau$ or $\pi = \sigma\tau$ as a result. Therefore, $a = b$, and by right cancellation $\sigma = \pi$. Hence φ is an injective homomorphism, which means $\ker\varphi$ is the trivial subgroup. Then by the First Isomorphism Theorem,

$$\frac{S_{n-2}}{\ker\varphi} = \frac{S_{n-2}}{\{1\}} \cong S_{n-2} \cong \varphi(S_{n-2}) \leq A_n.$$

Hence for all $n \geq 3$, A_n contains a subgroup isomorphic to S_{n-2}. □

5. (DF3.1.36) Prove that if $G/Z(G)$ is cyclic then G is abelian.

Proof. Let G be a group such that $G/Z(G)$ is cyclic as given. Then by definition, $G/Z(G)$ has a generator. We may choose a representative $x \in G$ so that $xZ(G)$ is a generator for $G/Z(G)$. Then because the left cosets of $Z(G)$ partition G, it follows that for any element $g \in G$, g lies in one of the left cosets of $Z(G)$. In particular, g lies in $gZ(G)$, which is an element of $G/Z(G)$. Since $xZ(G)$ generates $G/Z(G)$, there exists $n \in \mathbb{Z}$ such that $gZ(G) = (xZ(G))^n = x^nZ(G)$. Thus there exists $z_1, z_2 \in Z(G)$ such that $gz_1 = x^nz_2$, which by right multiplication we have that $g = x^nz_2z_1^{-1}$. Let $z = z_2z_1^{-1}$, and because $Z(G)$ is a subgroup of G, $z_2z_1^{-1} = z \in Z(G)$.

Hence any element $g \in G$ can be written as $g = x^nz$, where $n \in \mathbb{Z}$ and $z \in Z(G)$. Then let $a, b \in G$ so that $a = x^jz_1$ and $b = x^kz_2$ for $j, k \in \mathbb{Z}$ and $z_1, z_2 \in Z(G)$. Due to exponent rules and the fact that z_1, z_2 lie in the center of G,

$$\begin{aligned} ab &= (x^jz_1)(x^kz_2) \\ &= (z_1x^j)(x^kz_2) \\ &= z_1(x^jx^k)z_2 \\ &= z_2(x^kx^j)z_1 \\ &= (z_2x^k)(x^jz_1) \\ &= (x^kz_2)(x^jz_1) = ba. \end{aligned}$$

Because a, b were arbitrary elements of G it follows that G is abelian. □