Problem 1 (Ch. 4.6)

Show that an abelian group has a composition series if and only if it is finite.

Solution. Let G be an abelian group. Assume G is finite. Let $G = G_1$. Consider the largest subgroup of G_1, H, such that $H \subsetneq G_1$. Since G is abelian, H must be normal (i.e. $gHg^{-1} = gg^{-1}H = H$). Thus, H is maximal normal in G_1. Let $G_2 = H$. Since G is finite, G_2 is finite as well, and $|G_2|$ is strictly less than $|G_1|$. We repeat this process, taking the largest subgroup of G_i, this is normal, hence G_{i+1} is maximal normal. Note that at most, we can only repeat this process $|G_1|$ times before $G_s = \{1\}$, since the order at each iteration is strictly decreasing. Thus, we get a series $G = G_1 \triangleright G_2 \cdots \triangleright G_s = 1$ where each G_{i+1} is maximal normal in G_i, thus G has a composition series.

Now assume that G has a composition series, say $G = G_1 \triangleright G_2 \triangleright \cdots \triangleright G_s = \{1\}$. For the sake of contradiction, assume that G is infinite. We claim that the maximal normal subgroup of an infinite group is also infinite. To see this, assume the opposite, that is that the maximal normal subgroup is finite, call the group H. Now if $g \in G$ but $g \notin H$ (which of course must exist, otherwise H would be infinite as well), then consider the group generated by g and all the elements of H, call this new group K. Obviously, $|K| > |H|$ ($H \subseteq K$ but $g \notin H$), and furthermore, since G is abelian, any subgroup of G is normal, thus K is normal with a greater order than H, contradicting that H was maximal normal. Thus, the maximal normal subgroup of G is also of infinite order. Thus, if G_2 is of infinite order. Applying this iteratively s times, this gives us that G_s is of infinite order. But $\{1\}$ is a finite group, thus contradiction. Therefore, G must be finite.

Hence, we have proven both directions, so if G is abelian, G has a composition series $\iff$ G is finite.

Problem 2 (Ch. 4.6)

Let G be cyclic of order n ($< \infty$) and let $G = G_1 \triangleright G_2 \triangleright \cdots \triangleright G_{s+1} = 1$ be a composition series. Put $|G_i| = n_i$. Show that $p_i = n_i/n_{i+1}$ is a prime, and conversely, if $n = n_1, n_2, \ldots, n_{s+1} = 1$ is a sequence of integers such that n_i/n_{i+1} is a prime, then we have a composition series for which $|G_i| = n_i$.

Solution. Let G be a finite cyclic group of order n. Assume we have a composition series $G = G_1 \triangleright G_2 \triangleright \cdots \triangleright G_{s+1} = 1$, and $n_i = |G_i|$.

Note that the smallest value that divides $|G|$ is a prime. If it were not prime, then it is composite, and so then a smaller value divides it and also divides $|G|$, a contradiction. So call the smallest value that divides $|G|$, p. Note that since $|G|/p \mid |G|$, we have a group of order $|G|/p$ by Theorem 1.3 and the fact G is cyclic. This is the largest possible divisor of G, and so is the largest possible subgroup (by Lagrange's). If this largest subgroup of $|G|$ is H, then Lagrange's gives $|G| = |H|p$. By Problem 5 from Ch. 1.12, we then have H is normal as well. Thus, H is maximal normal. So if $G = G_1$, we have that $H = G_2$. Furthermore, $|G_1|/|G_2| = n_1/n_2 = p$ is prime. We can repeat this argument at each step (since subgroups of cyclic groups are also cyclic), starting with G_i and the maximal subgroup of G_i has prime index, and so is normal, so our subgroup is G_{i+1}; then, $|G_i|/|G_{i+1}| = n_i/n_{i+1} = p_i$ is prime.

Now assume that $n = n_1, n_2, \ldots, n_{s+1} = 1$ is a sequence of integers where n_i/n_{i+1} is prime. Since we have $n_{i+1} \mid n_i$ (since their quotient is an integer), we can see that $n_{s+1} \mid n_s \mid \cdots \mid n_2 \mid n_1 = n$. Thus, since G is cyclic, we have that there exists subgroups of G, G_i such that $|G_i| = n_i$ (by Theorem 1.3). Furthermore, since n_i must be decreasing (to ensure divisibility), we have that the group of order n_{i+1} is the maximal subgroup, and so it's index must then be the smallest value that divides n_i (since the groups are cyclic, so each divisor has a subgroup), and the index is prime, so we have that it is normal. Thus, G_{i+1} is maximal normal for G_i, and so $G = G_1 \triangleright G_2 \triangleright \cdots \triangleright G_{s+1} = 1$ forms a composition series.

Problem 3 (Ch. 4.6)

If g and h are elements of a group we write g^h for $h^{-1}gh$. Then $g^{hk} = (g^h)^k$ and by definition of $(g,h) = g^{-1}h^{-1}gh$ we have $g^h = g(g,h)$. Verify that

$$(\alpha)(g, hk) = (g,k)(g,h)^k$$
$$(\beta)(gh, k) = (g,k)^h(h,k)$$
$$(\gamma)(g^h, (h,k))(h^k, (k,g))(k^g, (g,h)) = 1.$$

Solution. (α):

$$\begin{aligned}
(g, hk) &= g^{-1}(hk)^{-1}ghk \\
&= g^{-1}k^{-1}h^{-1}ghk \\
&= g^{-1}k^{-1}gg^{-1}h^{-1}ghk \\
&= g^{-1}k^{-1}gkk^{-1}g^{-1}h^{-1}ghk \\
&= (g, k)(g, h)^k
\end{aligned}$$

(β):

$$\begin{aligned}
(gh, k) &= (gh)^{-1}k^{-1}ghk \\
&= h^{-1}g^{-1}k^{-1}gkk^{-1}hk \\
&= h^{-1}g^{-1}k^{-1}gkhh^{-1}k^{-1}hk \\
&= (g, k)^h(h, k)
\end{aligned}$$

(γ): Note that

$$(a^b, (b, c)) = (b^{-1}ab)^{-1}(b^{-1}c^{-1}bc)^{-1}(b^{-1}ab)(b^{-1}c^{-1}bc) = b^{-1}a^{-1}bc^{-1}b^{-1}cbb^{-1}abb^{-1}c^{-1}bc = b^{-1}a^{-1}bc^{-1}b^{-1}cac^{-1}bc$$

Plugging this in, we get

$$\begin{aligned}
(g^h, (h, k))(h^k, (k, g))(k^g, (g, h)) &= h^{-1}g^{-1}hk^{-1}h^{-1}kgk^{-1}hkk^{-1}h^{-1}kg^{-1}k^{-1}ghg^{-1}kgg^{-1}k^{-1}gh^{-1}g^{-1}hkh^{-1}gh \\
&= h^{-1}g^{-1}hk^{-1}h^{-1}kgk^{-1}hh^{-1}kg^{-1}k^{-1}ghg^{-1}kk^{-1}gh^{-1}g^{-1}hkh^{-1}gh \\
&= h^{-1}g^{-1}hk^{-1}h^{-1}kgk^{-1}kg^{-1}k^{-1}ghg^{-1}gh^{-1}g^{-1}hkh^{-1}gh \\
&= h^{-1}g^{-1}hk^{-1}h^{-1}kgg^{-1}k^{-1}ghh^{-1}g^{-1}hkh^{-1}gh \\
&= h^{-1}g^{-1}hk^{-1}h^{-1}kk^{-1}gg^{-1}hkh^{-1}gh \\
&= h^{-1}g^{-1}hk^{-1}h^{-1}hkh^{-1}gh \\
&= h^{-1}g^{-1}hk^{-1}kh^{-1}gh \\
&= h^{-1}g^{-1}hh^{-1}gh \\
&= h^{-1}g^{-1}gh \\
&= h^{-1}h \\
&= 1
\end{aligned}$$

Problem 4 (Ch. 1.13)

If $H \triangleleft G$ and $K \triangleleft G$ define (H, K) to be the subgroup generated by the commutators $(h, k), h \in H, k \in K$. Show that $(H, K) = (K, H) \triangleleft G$.

Solution. Let $a \in (H, K)$. Then $a = h_{i_1}^{-1}k_{i_1}^{-1}h_{i_1}k_{i_1} \cdots h_{i_s}^{-1}k_{i_s}^{-1}h_{i_s}k_{i_s}$ where $h_{i_r} \in H$, $k_{i_r} \in K$, and h_{i_r} and $h_{i_{r'}}$ are not necessarily distinct (and similarily with k_{i_r}). Note $k_{i_1}h_{i_1}k_{i_1}^{-1} \in H$ since H is normal in G, thus let $h_{i_1}' = k_{i_1}h_{i_1}k_{i_1}^{-1}$, so $(h_{i_1}')^{-1} = k_{i_1}h_{i_1}^{-1}k_{i_1}^{-1}$. Then $a = k_{i_1}^{-1}(h_{i_1}')^{-1}k_{i_1}k_{i_1}^{-1}h_{i_1}k_{i_1} \cdots = k_{i_1}^{-1}(h_{i_1}')^{-1}h_{i_1}k_{i_1} \cdots = k_{i_1}^{-1}(h_{i_1}')^{-1}k_{i_1}h_{i_1}'k_{i_1}^{-1}k_{i_1} \cdots = k_{i_1}^{-1}(h_{i_1}')^{-1}k_{i_1}h_{i_1}' \cdots$. We can repeat this process for each i_r where $1 \leq r \leq s$, so we get $k_{i_1}^{-1}(h_{i_1}')^{-1}k_{i_1}h_{i_1}' \cdots k_{i_s}^{-1}(h_{i_s}')^{-1}k_{i_s}h_{i_s}'$. Thus, $a \in (K, H)$. Since a was arbitrary, we get that $(H, K) \subseteq (K, H)$.

We can repeat an identical argument with the k's and h's swapped to get the result $(K, H) \subseteq (H, K)$. Hence, $(H, K) = (K, H)$.

We now show that $(H, K) = (K, H) \triangleleft G$. Let $a \in (H, K)$ so $a = h_{i_1}^{-1}k_{i_1}^{-1}h_{i_1}k_{i_1} \cdots h_{i_s}^{-1}k_{i_s}^{-1}h_{i_s}k_{i_s}$. If $g \in G$, then $g^{-1}h_{i_r}g \in H$ by the normality of G, so define $h_{i_r}' = g^{-1}h_{i_r}g$ which means $(h_{i_r}')^{-1} = (g^{-1}h_{i_r}g)^{-1} = g^{-1}h_{i_r}^{-1}g$.

Similarily, we have $k'_{i_r} = g^{-1}k_{i_r}g \in K$ and $k'_{i_r})^{-1} = g^{-1}k_{i_r}^{-1}g$. Thus,

$$
\begin{aligned}
g^{-1}ag &= g^{-1}h_{i_1}^{-1}k_{i_1}^{-1}h_{i_1}k_{i_1}\cdots h_{i_s}^{-1}k_{i_s}^{-1}h_{i_s}k_{i_s}g \\
&= g^{-1}h_{i_1}^{-1}gg^{-1}k_{i_1}^{-1}gg^{-1}h_{i_1}gg^{-1}k_{i_1}g\cdots g^{-1}h_{i_s}^{-1}gg^{-1}k_{i_s}^{-1}gg^{-1}h_{i_s}gg^{-1}k_{i_s}g \\
&= (h'_{i_1})^{-1}(k'_{i_1})^{-1}h'_{i_1}k'_{i_1}\cdots (h'_{i_s})^{-1}(k'_{i_s})^{-1}h'_{i_s}k'_{i_s} \in (H,K)
\end{aligned}
$$

Thus, since g and a were arbitrary, we have $(H,K) \triangleleft G$.

Problem 11(a) (Herstein p. 102)

If $o(G) = pq$, p and q distinct primes, $p < q$, show if $p \nmid (q-1)$, then G is cyclic.

Solution. Note that by Sylow's theorems, if n_p is the number of Sylow p-subgroups and n_q is the number of Sylow q-subgroups, we have $n_p \equiv 1 \pmod{p}$ and and $n_q \equiv 1 \pmod{q}$, and $n_p \mid q$ and $n_q \mid p$. Since $q > p$, $n_q = 1$ (since we can't have $n_q \geq q+1 > p$). Furthermore, $n_p = 1$, since if $n_p = mp+1 \mid q$ where $m > 0$, $mp \mid q-1 \implies p \mid (q-1)$, which we assumed was not true.

Note that each non-identity element in the Sylow p-subgroup must be of order p, otherwise if there were some element a with order $r < p$, $\langle a \rangle$ generates a subgroup of order r, but by Lagrange's theorem, prime order groups don't have subgroups. Similarly, each non-identity element in the Sylow q-subgroup must be of order q. Thus the elements in the two subgroups are distinct (besides the identity). Thus, there are $p-1$ elements of order p and $q-1$ elements of order q. Hence, we have at least $p-2+q-2+1 = p+q-1$ elements in G.

We now prove that $|G| > p+q-1$. It is sufficient to prove that $|G| \neq p+q-1$. For the sake of contradiction, assume $|G| = pq = p+q-1$. Dividing out by p, we have $q = 1 + (q-1)/p$. But since $p \nmid q-1$, $(q-1)/p$ is not an integer, and so $q-1$ is not an integer, a contradiction. Thus $|G| > p+q-1$. So there exists elements in G that are not in the Sylow p-subgroup or the Sylow q-subgroup. Consider one such element, a. We must have the order of a be pq, since $\langle a \rangle$ is a subgroup of G, and by Lagrange's $|\langle a \rangle| \mid |G|$, so $|\langle a \rangle| = 1, p, q, pq$. But since we are assuming a is not the identity, or in either the Sylow p-subgroup or q-subgroup, we must then have $|\langle a \rangle| = pq$. But then $\langle a \rangle = G$. Thus G is cyclic.