3.1.1) Let $\varphi : G \to H$ be a homomorphism and let $E \leq H$. Prove that $\varphi^{-1}(E) \leq G$. If $E \trianglelefteq H$ prove that $\varphi^{-1}(E) \trianglelefteq G$. Deduce that $\ker\varphi \trianglelefteq G$

Proof
Notice that since E is a subgroup of H, then $\mathbb{1}_H \in E$, so it is clear that $\mathbb{1}_G \in \varphi^{-1}(E)$ since $\varphi(\mathbb{1}_G) = \mathbb{1}_H$. Now let $a, b \in \varphi^{-1}(E)$. Then, there exist $c, d \in E$ such that $\varphi(a) = c$ and $\varphi(b) = d$. Thus, since $cd \in E$, we have that $\varphi(a)\varphi(b) = \varphi(ab) = cd \in E$, or $ab \in \varphi^{-1}(E)$. Finally, we let $\varphi(a) = c \in E$. Then $\varphi(a)^{-1} = \varphi(a^{-1}) = c^{-1} \in E$ or $a \in \varphi^{-1}(E)$. This means that $\varphi^{-1}(E)$ is a subgroup of G if G and H are homomorphic and E is a subgroup of H.

Furthermore, let us suppose that E is a normal subgroup of H. Let $g \in G$ and $a \in \varphi^{-1}(E)$. Then consider gag^{-1}. We want to show that this is in $\varphi^{-1}(E)$. Notice that $\varphi(gag^{-1}) = \varphi(g)\varphi(a)\varphi(g^{-1})$. Obviously, $\varphi(g), \varphi(g^{-1}) \in H$ and $\varphi(a) \in E$. Thus, $\varphi(gag^{-1}) \in hEh^{-1} = E$ if we denote $h = \varphi(g)$. Hence, it immediately follows that $gag^{-1} \in \varphi^{-1}(E)$ and that $\varphi^{-1}(E) \trianglelefteq G$.

■

$\to$ As a corollary: It is trivially true that $\{\mathbb{1}_H\} \trianglelefteq H$, so $\ker\varphi = \varphi^{-1}(\{\mathbb{1}_H\}) \trianglelefteq G$.

3.1.3) Let A be an abelian group and $B \leq A$. Prove that A/B is abelian. Give an example of a non-abelian group G containing a proper normal subgroup N such that G/N is abelian.

Proof
Recall the definition of a quotient group: $A/B = \{aB | a \in A\}$. Suppose that $a, a' \in A$, then $aB \cdot a'B = aa'B$ and $a'B \cdot aB = a'aB$. Obviously, since A is abelian, it follows that $a'aB = aa'B$, or that A/B is abelian.

■

Example: Consider the dihedral group for symmetries of a triangle $G = D_6$ where $N = \langle r \rangle$. Obviously G is not abelian and N is a normal subgroup of G. We then see that G/N has two elements $s\langle r \rangle$ and $\langle r \rangle$, which is abelian.

3.1.4) Prove that in the quotient group G/N, $(gN)^\alpha = g^\alpha N$ for all $\alpha \in \mathbb{Z}$.

Proof
This is a fairly simple proof by induction. By definition, if $\alpha = 0$, then we get $N = N$, and if $\alpha = 1$, then $(gN)^1 = gN$. Next, suppose that $(gN)^\alpha = g^\alpha N$ for some positive integer α. Then $(gN)^{\alpha+1} = gN \cdot (gN)^\alpha = gN \cdot g^\alpha N = gg^\alpha N = g^{\alpha+1}N$.

Reversing the proof is simple for negative integers α. Notice that if we let $g = g_1^{-1}$ (since g must have an inverse in the group G), then we get negative powers from the above for the element g_1.

■

3.1.5) Use the preceding exercise to prove that the order of the element gN in G/N is n, where n is the smallest positive integer such that $g^n \in N$. Give an example to show that the order of gN in G/N may be strictly smaller than the order of g in G.

Proof
The order of $gN \in G/N$ is the smallest $n \in \mathbb{Z}^+$ such that $(gN)^n = g^nN = \mathbb{1}N = N$. At this point, it may be tempting to say that $g^n = \mathbb{1}$, and while this may hold true for some n, it does not necessarily produce the smallest possible value of n. We simply need N, which is a subgroup of G such that $g^nN = N$. Since N is a subgroup, it is closed under multiplication (i.e. for any $m \in N$ then $g^nm \in N$). Hence, we need $g^n \in N$, or alternatively, n, the order of gN, is the smallest positive integer such that $g^n \in N$.

■

3.1.24) Prove that if $N \trianglelefteq G$ and H is any subgroup of G then $N \cap H \trianglelefteq H$.

Proof
We have previously proven that if $N, H \leq G$ that $N \cap H \leq H$. Thus, it remains to show that $h(N \cap H)h^{-1} \subseteq N \cap H$ for any $h \in H$. Let $n \in N \cap H$, then obviously, $n \in H$ and $hnh^{-1} \in H$. Hence, $N \cap H$ is a normal subgroup of H.

■

3.1.36) Prove that if $G/Z(G)$ is cyclic then G is abelian.

Proof
Recall $Z(G) = \{g \in G | \forall x \in G,\ gx = xg\}$ and $G/Z(G) = \{gZ(G) | g \in G\}$. Suppose that $G/Z(G)$ is cyclic. Then, if $z \in Z(G)$ any element of $G/Z(G)$ can be written as x^az. Now, let $g, h \in G$. Then $gz = x^az$ and $hz = x^bz$ for some integers a, b. Notice since $G/Z(G)$ is abelian, then $(x^az)(x^bz) = (x^bz)(x^az)$. Thus, $x^ax^bz = x^bx^az$ or $x^ax^b = gh = hg = x^bx^a$, implying that G is abelian.

■

3.2.1) Which of the following are permissible orders for subgroups of a group of order 120: 1, 2, 5, 7, 9, 15, 60, 240? For each permissible order give the corresponding index.

$\rightarrow$ If H is a subgroup of G, then it must be true that $|H| \,\big|\, |G|$. The permissible orders of subgroups are then as follows: 1(trivially), 2, 5, 15, and 60. The indices for each corresponding order is defined to be $|G|/|H|$, and are given as follows, respectively: 120, 60, 24, 8, and 2.

3.2.4) Show that if $|G| = pq$ for some primes p and q (not necessarily distinct) then either G is abelian or $Z(G) = 1$.

Proof
Recall that $Z(G)$ is a subgroup of G, so $|G| = |G/Z(G)||Z(G)|$. Thus, $|G/Z(G)| \in \{1, p, q, pq\}$. If $|G/Z(G)| = 1$, then $Z(G) = G$, implying that G is abelian. Next, if $|G/Z(G)| \in \{p, q\}$ (a set of prime numbers), then it is a cyclic group, and furthermore, it follows that G is an abelian group. Finally, suppose that $|G/Z(G)| = pq$, then $|Z(G)| = 1$, and since $\mathbb{1} \in Z(G)$ for all groups G, it follows that $Z(G)$ is the trivial subgroup.

■

3.2.8) Prove that if H and K are finite subgroups of G whose orders are relatively prime then $H \cap K = 1$.

Proof
Suppose that H, K are finite subgroups of G with $\gcd(|H|, |K|) = 1$. Recall that if $x \in G$, which is finite, then $|G| = n|\langle x \rangle|$. Then for each $h \in H$ and $k \in K$, we have $|H| = m_h|\langle h \rangle|$ and $|K| = l_k|\langle k \rangle|$ for some integers m_h, l_k. It is clear that since H, K are subgroups of G that they both contain the identity. If $h, k \neq \mathbb{1}$, then $\gcd(|\langle h \rangle|, |\langle k \rangle|) = 1$. Hence h and k are distinct. Thus, $H \cap K$ only contains the identity of G.

■