7.7.2 Show that $\mathbb{Z}_6/N \cong \mathbb{Z}_3$, where N is the suibgroup $\{0, 3\}$.

Note that if G is a finite group and H is a normal subgroup of G, then $|G/H| = [G : H]$. So by Lagrange's Theorem $|\mathbb{Z}_6/N| = |\mathbb{Z}_|/|N| = 6/2 = 3$. Since every group of prime order is cyclic (and 3 is a prime), $\mathbb{Z}_6/N$ is cyclic of order 3 and so by Theorem 7.18, $\mathbb{Z}_6/N \cong \mathbb{Z}_3$ as required. ◆

7.7.4 Let $G = \mathbb{Z}_4 \times \mathbb{Z}_4$ and let N be the cyclic subgroup generated by $(3, 2)$. Show that $G/N \cong \mathbb{Z}_4$.

Note that $N = \langle(3, 2)\rangle = \{(0, 0),(3, 2),(2, 0),(1, 2)\}$; so $|N| = 4$ and therefore (arguing as in 7.2.2) by Lagrange's Theorem we have $|G/N| = |\mathbb{Z}_4 \times \mathbb{Z}_4|/|N| = 16/4 = 4$. Note that G/N consists of the four cosets:

$$\begin{aligned} N + (0, 0) &= \{(0, 0),(3, 2),(2, 0),(1, 2)\} \\ N + (0, 1) &= \{(0, 1),(3, 3),(2, 1),(1, 3)\} \\ N + (0, 2) &= \{(0, 2),(3, 0),(2, 2),(1, 0)\} \\ N + (0, 3) &= \{(0, 3),(3, 1),(2, 3),(1, 1)\}. \end{aligned}$$

We see that the element $N + (0, 1)$ has order 4 in G/N, since

$$\begin{aligned} 4(N + (0, 1)) &= N + (0, 0) = 0_{G/N} \qquad \text{but} \\ 2(N + (0, 1)) &= N + (0, 2) \neq 0_{G/N}. \end{aligned}$$

Hence, $G/N \cong \mathbb{Z}_4$ (by Theorem 7.18). This can also be shown by constructing the operation table of G/N as in the examples given in the section. ◆

7.7.17 Let G and H be groups and let G^* be the subset of $G \times H$ consisting of all (a, e) with $a \in G$,

(a) Show that G^* is isomorphic to G.

Define $f : G \to G \times H$ by $f(a) = (a, e)$. Then for $a, b \in G$, we have

$$f(ab) = (ab, e) = (a, e)(b, e) = f(a)f(b).$$

Hence, f is a homomorphism which is evidently injective. Since $\operatorname{Im} f = G^*$, it follows by Theorem 7.19 that G^* is a subgroup of $G \times H$ and that G^* is isomorphic to G. ◆

(b) Show that G^* is a normal subgroup of $G \times H$.

As noted in part (a), since G^* is the image of a homomorphism it is a subgroup of $G \times H$ (by Theorem 7.19). Let $x \in G \times H$ and let $y \in G^*$. Then $x = (a, b)$ and $y = (c, e)$ for some $a, c \in G$ and $b \in H$. We have

$$xyx^{-1} = (a, b)(c, e)(a, b)^{-1} = (ac, b)(a^{-1}, b^{-1}) = (aca^{-1}, bb^{-1}) = (aca^{-1}, e) \in G^*$$

since $aca^{-1} \in G$. Hence, G^* is a normal subgroup of $G \times H$ by Theorem 7.34. ◆

(c) Show that $(G \times H)/G^* \cong H$.

First note that $(G \times H)/G^* = \{G^*(e, h) \mid h \in H\}$, since $(g, h) = (g, e)(e, h) \in G^*(e, h)$ for every $(g, h) \in G \times H$. Moreover, fpr $h_1, h_2 \in H$, $G^*(e, h_1) = G^*(e, h_2)$ only if $h_1 = h_2$. This follows from the Theorem 7.23 which asserts that $G^*(e, h_1) = G^*(e, h_2)$ iff $(e, h_1)(e, h_2)^{-1} \in G^*$. But $(e, h_1)(e, h_2)^{-1} = (e, h_1h_2^{-1})$, so $(e, h_1)(e, h_2)^{-1} \in G^*$ only if $h_1h_2^{-1} = e$, that is, $h_1 = h_2$.
Next, we define a map $\varphi : H \to (G \times H)/G^*$ by $\varphi(h) = G^*(e, h)$. Then, by the above observations, φ is a bijection so it remains to show that φ is a homomorphism. Let $h_1, h_2 \in H$ be given; then we have

$$\varphi(h_1h_2) = G^*(e, h_1h_2) = G^*(e, h_1)(e, h_2) = G^*(e, h_1)G^*(e, h_2) = \varphi(h_1)\varphi(h_2)$$

by definition of coset multiplication. Hence, φ is an isomorphism and thus $(G \times H)/G^* \cong H$. ◆

7.7.21 Let G be a group of order pq, with p and q (not necessarily distinct) primes. Prove that the center $Z(G)$ is either $\langle e\rangle$ or G.

We apply Theorem 7.38 and prove the statement by contradiction. Suppose that the center $Z(G)$ is neither $\langle e\rangle$ nor G. Then since the order of the center must divide $|G| = pq$ and p and q are primes, we must have $|Z(G)| = p$ or $|Z(G)| = q$ (note that we have ruled out $|Z(G)| = pq$ and $|Z(G)| = 1$).

Suppose $|Z(G)| = p$; since $Z(G)$ is normal we may form the quotient group $G/Z(G)$ which by Lagrange's Theorem must have order $|G|/|Z(G)| = pq/p = q$. Since q is prime, $G/Z(G)$ is cyclic (by Theorem 7.28). Hence, by Theorem 7.38, G is abelian. But in this case $Z(G) = G$. This results in a contradiction. If $|Z(G)| = q$, the argument proceeds in exactly the same way with the roles of p and q reversed. In either case a contradiction results. Hence, $Z(G)$ is either $\langle e\rangle$ or G. ◆