Solutions

Exercise 1. The direct product of two groups G and H is the group $G \times H$ with group operation $(g, h)(g', h') = (gg', hh')$ for $g, g' \in G$ and $h, h' \in H$. Suppose $G = \langle g \rangle$ and $H = \langle h \rangle$ are cyclic of orders m and n, respectively, and that $\gcd(m, n) = 1$. Prove that $G \times H$ is cyclic of order mn.

Proof. The order of $G \times H$ is clearly mn. We compute the order of (g, h), where g and h are generators of G and H as above. First, we have $(g, h)^{mn} = (g^{mn}, h^{mn}) = ((g^m)^n, (h^n)^n) = (e, e')$, where e, e' are the identity elements of G and H, respectively. Hence the order d of (g, h) divides mn. Suppose $(g, h)^k = (e, e')$. Then $g^k = e$ and $h^k = e'$, so $m \mid d$ and $n \mid d$. Since m, n are relatively prime, this implies that $mn \mid d$. Therefore $d = mn$. Hence $G \times H$ is cyclic. □

Exercise 2. Let p be a prime. Give examples of two non-isomorphic groups of order p^2.

Solution. The groups are $\mathbb{Z}_{p^2}$ and $\mathbb{Z}_p \times \mathbb{Z}_p$. They are not isomorphic because $\mathbb{Z}_{p^2}$ has elements of order p^2, while every non-identity element of $\mathbb{Z}_p \times \mathbb{Z}_p$ has order p. □

Comment: We have proved that every group of order p^2 is abelian. Later we will show that every group of order p^2 is isomorphic to either $\mathbb{Z}_{p^2}$ or $\mathbb{Z}_p \times \mathbb{Z}_p$.

Exercise 3. Let $f : G \to G'$ be a group homomorphism. Prove that $\ker f$ is a normal subgroup of G. We denote this by $\ker f \lhd G$.

Proof. Let $k \in \ker f$ and let $g \in G$. We must show that $gkg^{-1} \in \ker G$. We compute:

$$f(gkg^{-1}) = f(g)f(k)f(g^{-1}) = f(g)ef(g)^{-1} = e,$$

so $gkg^{-1} \in \ker f$. Hence $\ker f \lhd G$. □

Comment: Conversely, every normal subgroup of G is the kernel of a homomorphism. That is, if $K \lhd G$ then there is a group G' and a homomorphism $f : G \to G'$ such that $K = \ker f$. This follows from the First Isomorphism Theorem.

Exercise 4. Recall that the center of a group G is the subgroup $Z(G) = \{a \in G : \ ab = ba \ \forall b \in G\}$. Prove that $Z(G) \lhd G$.

Proof. Let $z \in Z(G)$ and let $g \in G$. We must show that $gzg^{-1} \in Z(G)$. But $gzg^{-1} = z$, so this is clear. □

Comment: Thus, for every group G we can consider the quotient $G/Z(G)$, and this tells us something about G. For example, we proved in class that if $G/Z(G)$ is cyclic then G is abelian.

Exercise 5. The group $D_4/Z(D_4)$ has order four, so is isomorphic to either the $\mathbb{Z}_4$ or $K_4(= \mathbb{Z}_2 \times \mathbb{Z}_2)$. Decide which, with proof.

Proof. The simplest proof is to note that D_4 is nonabelian, so the quotient $D_4/Z(D_4)$ cannot be cyclic, hence must be isomorphic to K_4. Alternatively, one can compute that $g^2 \in Z(D_4)$ for all $g \in D_4$. This shows that every non-identity element of $D_4/Z(D_4)$ has order two, so $D_4/Z(D_4) \simeq K_4$. □

Exercise 6. Use the first isomorphism theorem to prove that $S_4/K_4 \simeq S_3$.

Proof. Postponed. □