Exercise 1.5.14

If $N_1 \triangleleft G_1$, $N_2 \triangleleft G_2$, then $(N_1 \times N_2) \triangleleft (G_1 \times G_2)$ and $(G_1 \times G_2)/(N_1 \times N_2) \cong (G_1/N_1) \times (G_2/N_2)$.

Proof. Let $(n_1, n_2) \in N_1 \times N_2$ and $(g_1, g_2) \in G_1 \times G_2$. Then

$$(g_1, g_2)(n_1, n_2)(g_1, g_2)^{-1} = (g_1 n_1 g_1^{-1}, g_2 n_2 g_2^{-1}) \in N_1 \times N_2$$

since $N_i \triangleleft G_i$ for $i = 1, 2$. Thus $N_1 \times N_2 \triangleleft G_1 \times G_2$.

Now define $\varphi : G_1 \times G_2 \to (G_1/N_1) \times (G_2/N_2)$ by $\varphi(g_1, g_2) = (g_1 N_1, g_2 N_2)$. This is a homomorphism since

$$\begin{aligned}\varphi((g_1, g_2)(h_1, h_2)) &= \varphi(g_1 h_1, g_2 h_2) = (g_1 h_1 N_1, g_2 h_2 N_2) \\ &= (g_1 N_1, g_2 N_2)(h_1 N_1, h_2 N_2) = \varphi(g_1, g_2)\varphi(h_1, h_2)\end{aligned}$$

for all $(g_i, h_i) \in G_i$, $i = 1, 2$. It is surjective since for any $(g_1' N_1, g_2' N_2) \in (G/N_i)$ we have $\varphi(g_1', g_2') = (g_1' N_i, g_2' N_i)$.

Finally,

$$\ker(\varphi) = \{(g_1, g_2) : (g_1 N_i, g_2 N_i) = (N_i, N_i)\} = \{(g_1, g_2) : g_1 \in N_1, g_2 \in N_2\} = N_1 \times N_2$$

Thus by the First Isomorphism Theorem,

$$(G_1 \times G_2)/(N_1 \times N_2) \cong (G_1/N_1) \times (G_2/N_2)$$

as desired. $\square$

1.6.11

Find all normal subgroups of D_n.

For notation, let a be a rotation of order n and b be a reflection of order 2. Then $D_n = \langle a, b : a^n = e, b^2 = e, bab = a^{-1} \rangle$. If n is odd then we have that $\langle a^i \rangle \triangleleft D_n$ for all i dividing n, and these are the only normal subgroups. If n is even then we have that $\langle a^i \rangle \triangleleft D_n$ for all i dividing n, as well as $\langle a^2, b \rangle \triangleleft D_n$ and $\langle a^2, ab \rangle \triangleleft D_n$, and these are the only normal subgroups. This is because the rotations form a cyclic subgroup which is normal, and the conjugacy classes of reflections depend on the parity of n.

1.8.2

Give an example of groups H_i, K_j such that $H_1 \times H_2 \cong K_1 \times K_2$ and no H_i is isomorphic to any K_j.

Consider $H_1 = \mathbb{Z}_4, H_2 = \mathbb{Z}_3, K_1 = \mathbb{Z}_6, K_2 = \mathbb{Z}_2$. Then $H_1 \times H_2 \cong \mathbb{Z}_{12} \cong K_1 \times K_2$, but no H_i is isomorphic to any K_j.

1.8.3

Let G be an (additive) abelian group with subgroups H and K. Show that $G \cong H \oplus K$ if and only if there are homomorphisms $H \leftrightarrows_{\iota_1}^{\pi_1} G \leftrightarrows_{\iota_2}^{\pi_2} K$ such that $\pi_1\iota_1 = 1_H, \pi_2\iota_2 = 1_K, \pi_1\iota_2 = 0$, and $\pi_2\iota_1 = 0$, where 0 is the map sending every element onto the zero (identity) element, and $\iota_1\pi_1(x) + \iota_2\pi_2(x) = x$ for all $x \in G$.

Proof. ($\Rightarrow$) Suppose $G \cong H \oplus K$. Then every $g \in G$ can be uniquely written as $g = h + k$ for some $h \in H, k \in K$. Define $\pi_1 : G \to H$ by $\pi_1(g) = h$ and $\pi_2 : G \to K$ by $\pi_2(g) = k$. Also define $\iota_1 : H \to G$ by $\iota_1(h) = h + 0_K$ and $\iota_2 : K \to G$ by $\iota_2(k) = 0_H + k$. Then for any $h \in H, k \in K, g \in G$ we have

$$\begin{aligned} \pi_1\iota_1(h) &= \pi_1(h + 0_K) = h, & \pi_2\iota_2(k) &= \pi_2(0_H + k) = k, \\ \pi_1\iota_2(k) &= \pi_1(0_H + k) = 0_H, & \pi_2\iota_1(h) &= \pi_2(h + 0_K) = 0_K, \\ \iota_1\pi_1(g) + \iota_2\pi_2(g) &= (h + 0_K) + (0_H + k) = h + k = g. \end{aligned}$$

Thus the desired homomorphisms exist.

($\Leftarrow$) Suppose the homomorphisms π_i, ι_i exist as described. Then for any $g \in G$, we have

$$g = \iota_1\pi_1(g) + \iota_2\pi_2(g)$$

where $\iota_1\pi_1(g) \in H$ and $\iota_2\pi_2(g) \in K$. Thus every element of G can be written as a sum of an element of H and an element of K. Now suppose $h + k = h' + k'$ for some $h, h' \in H$ and $k, k' \in K$. Then

$$\begin{aligned} h + k &= h' + k' \\ \iota_1\pi_1(h + k) + \iota_2\pi_2(h + k) &= \iota_1\pi_1(h' + k') + \iota_2\pi_2(h' + k') \\ \iota_1(\pi_1(h) + \pi_1(k)) + \iota_2(\pi_2(h) + \pi_2(k)) &= \iota_1(\pi_1(h') + \pi_1(k')) + \iota_2(\pi_2(h') + \pi_2(k')) \\ \iota_1(\pi_1(h) + 0_H) + \iota_2(0_K + \pi_2(k)) &= \iota_1(\pi_1(h') + 0_H) + \iota_2(0_K + \pi_2(k')) \\ \iota_1\pi_1(h) + \iota_2\pi_2(k) &= \iota_1\pi_1(h') + \iota_2\pi_2(k') \\ h + k &= h' + k' \end{aligned}$$

Thus the representation of elements in G as sums of elements from H and K is unique, and $G \cong H \oplus K$. □

1.8.5

Let G, H be finite cyclic groups. Then $G \times H$ is cyclic if and only if $(|G|, |H|) = 1$.

Proof. ($\Rightarrow$) Suppose $G \times H$ is cyclic. Then there exists some $(g, h) \in G \times H$ such that $\langle (g, h) \rangle = G \times H$. Thus $|\langle (g, h) \rangle| = |G \times H| = |G||H|$. But $|\langle (g, h) \rangle| = \operatorname{lcm}(|g|, |h|)$, so $\operatorname{lcm}(|g|, |h|) = |G||H|$. Since $|g|$ divides $|G|$ and $|h|$ divides $|H|$, we have that $\operatorname{lcm}(|g|, |h|)$ divides $\operatorname{lcm}(|G|, |H|)$. Thus $\operatorname{lcm}(|G|, |H|)$ must be equal to $|G||H|$, which implies that $(|G|, |H|) = 1$.

($\Leftarrow$) Suppose $(|G|, |H|) = 1$. Let g be a generator of G and h be a generator of H. Then consider the element $(g, h) \in G \times H$. We have that $|(g, h)| = \operatorname{lcm}(|g|, |h|) = \operatorname{lcm}(|G|, |H|) = |G||H|$ since $(|G|, |H|) = 1$. Thus $|(g, h)| = |G \times H|$, so $\langle (g, h) \rangle = G \times H$ and $G \times H$ is cyclic. □

1.8.9

If a group G is the (internal) direct product of its subgroups H, K, then $H \cong G/K$ and $G/H \cong K$.

Proof. Let $\pi : G \to G/H$ be the natural projection. Then $\ker(\pi) = H$, so by the first isomorphism theorem we have $G/H \cong \pi(G)$. But $\pi(G) = \{gH \mid g \in G\} = \{gH \mid g \in H\} \cup \{gH \mid g \in K\} = H \cup K$. Thus $G/H \cong H \cup K$. But since $H \cap K = \{e\}$ and every element of G can be uniquely written as hk for some $h \in H, k \in K$, we have that $H \cup K \cong K$. Thus $G/H \cong K$. Similarly, let $\rho : G \to G/K$ be the natural projection. Then $\ker(\rho) = K$, so by the first isomorphism theorem we have $G/K \cong \rho(G)$. But $\rho(G) = \{gK \mid g \in G\} = \{gK \mid g \in H\} \cup \{gK \mid g \in K\} = H \cup K$. Thus $G/K \cong H \cup K$. But since $H \cap K = \{e\}$ and every element of G can be uniquely written as hk for some $h \in H, k \in K$, we have that $H \cup K \cong H$. Thus $G/K \cong H$. □

1.9.1

Every nonidentity element in a free group F has infinite order.

Proof. Let F be a free group on the set X. Then every nonidentity element of F can be uniquely written as a reduced word in the elements of X and their inverses. Suppose $w \in F$ is a nonidentity element. Then $w = x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n}$ where $x_i \in X$, $a_i \in \mathbb{Z} \setminus \{0\}$, and $x_i \neq x_{i+1}$ for all $1 \leq i < n$. Then for any integer $m > 0$, we have

$$w^m = (x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n})^m = x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n} x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n} \cdots x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n}$$

which is a reduced word since $x_n \neq x_1$. Thus w^m is not the identity element for any integer $m > 0$. Similarly, for any integer $m < 0$, we have

$$w^m = (x_n^{-a_n} x_{n-1}^{-a_{n-1}} \cdots x_1^{-a_1})^{-m} = x_n^{-a_n} x_{n-1}^{-a_{n-1}} \cdots x_1^{-a_1} x_n^{-a_n} x_{n-1}^{-a_{n-1}} \cdots x_1^{-a_1} \cdots x_n^{-a_n} x_{n-1}^{-a_{n-1}} \cdots x_1^{-a_1}$$

which is also a reduced word since $x_1 \neq x_n$. Thus w^m is not the identity element for any integer $m < 0$. Therefore, the only integer m such that w^m is the identity element is $m = 0$, so w has infinite order. Thus every nonidentity element in a free group has infinite order. □

1.9.4

Let F be the free group on the set X, and let $Y \subset X$. If H is the smallest normal subgroup of F containing Y, then F/H is a free group.

Proof. Let F be the free group on the set X, and let $Y \subset X$. Let H be the smallest normal subgroup of F containing Y. Then H is the normal closure of Y in F, which is the intersection of all normal subgroups of F containing Y. Thus H is generated by all conjugates of elements of Y in F.

Now consider the quotient group F/H. The elements of F/H are the cosets of H in F, which can be represented as gH for some $g \in F$. Since H is normal in F, the group operation on F/H is well-defined.

To show that F/H is a free group, we need to show that it has a basis, i.e., a set of elements such that every element of the group can be uniquely expressed as a reduced word in these elements and their inverses.

Let $Z = X \setminus Y$. Then every element of F/H can be uniquely expressed as a reduced word in the elements of Z and their inverses. This is because any element of Y is in H, so it becomes the identity element in the quotient group. Thus, the only elements that remain are those from Z.

Therefore, the set Z forms a basis for the free group F/H, and hence, we conclude that F/H is indeed a free group. □