Exercise 10.7. *Let $\phi : G \to H$ and $\sigma : H \to K$ are homomorphisms. Show that $\sigma\phi : G \to K$ is homomorphism. What relationship between $\operatorname{Ker}\phi$ and $\operatorname{Ker}\sigma\phi$? If ϕ and σ are onto and G is finite, describe $[\operatorname{Ker}\sigma\phi : \operatorname{Ker}\phi]$ in terms of $|H|$ and $|K|$.*

Proof. For any $a\ b \in G$, we have $\sigma\phi(ab) = \sigma(\phi(ab)) = \sigma(\phi(a)\phi(b)) = \sigma(\phi(a))\sigma(\phi(b)) = \sigma\phi(a)\sigma\phi(b)$.

$\operatorname{Ker}\phi \subseteq \operatorname{Ker}\sigma\phi$. For any $x \in \operatorname{Ker}\phi$, $\sigma\phi(x) = \sigma(e) = e$.

Since ϕ and σ are onto, so is $\sigma\phi$. Thus $\phi(G) = H$ and $\sigma\phi(G) = K$. Then by $\dfrac{|G|}{|\operatorname{Ker}\phi|} = |\phi(G)| = |H|$ and $\dfrac{|G|}{|\operatorname{Ker}\sigma\phi|} = |\sigma\phi(G)| = |K|$ we know $|\operatorname{Ker}\phi| = \dfrac{|G|}{|H|}$ and $|\operatorname{Ker}\sigma\phi| = \dfrac{|G|}{|K|}$. Then $[\operatorname{Ker}\sigma\phi : \operatorname{Ker}\phi] = \dfrac{|\operatorname{Ker}\sigma\phi|}{|\operatorname{Ker}\phi|} = \dfrac{|G|}{|K|}\dfrac{|H|}{|G|} = \dfrac{|H|}{|K|}$. □

Exercise 10.8. *Let G be a group of permutations. For each $\sigma \in G$, define:*

$$\operatorname{sgn}(\sigma) = \begin{cases} +1 & \text{if } \sigma \text{ is even permutation} \\ -1 & \text{if } \sigma \text{ is odd permutation} \end{cases}$$

Prove that sgn is a homomorphism from G to $\{+1, -1\}$ under multiplication. What is the kernel of sgn? And why this conclude that A_n is a normal subgroup of S_n of index 2 for $n > 1$?

Proof. For any $\alpha\ \beta \in G$, if they are all even permutations or odd permutations, then $\operatorname{sgn}(\alpha\beta) = \operatorname{sgn}(\alpha)\operatorname{sgn}(\beta) = +1$. If one of them is even permutation and another one is odd permutation, $\operatorname{sgn}(\alpha\beta) = \operatorname{sgn}(\alpha)\operatorname{sgn}(\beta) = -1$.

Note that the identity of $\{+1, -1\}$ under multiplication is $+1$, so the kernel of sgn is the set of even permutations in G. Take $G = S_n$, it is easy to show that $\operatorname{Ker}\operatorname{sgn} = A_n$. Thus A_n is a normal subgroup. Then by $S_n/A_n \approx \operatorname{sgn}(S_n)$ we get $\dfrac{|S_n|}{|A_n|} = |\operatorname{sgn}(S_n)|$. It is easy to show $|\operatorname{sgn}(S_n)| = 2$ when $n > 1$. Thus the index of A_n is 2. □

Exercise 5.27. *Using* Exercise 10.8 *to show the following theorem: Let H be a subgroup of S_n where $n > 1$, either every element of H is an even permutation or exactly half of the elements of H are even permutations.*

Proof. If there is no odd permutation in H, H consists of even permutations. So we suppose $\alpha \in H$ such that α is odd permutation. Using Exercise 10.8, we take $G = H$. $\operatorname{Ker}\operatorname{sgn}$ is the set of all even permutations in H where the index of $\operatorname{Ker}\operatorname{sgn}$ is 2. Thus, half of H are even permutations. $\square$

Exercise 10.9. *Prove that the mapping from $G \oplus H$ to G given by $(g, h) \mapsto g$ is a homomorphism. What is the kernel?*

Proof. It is trivial that it is a homomorphism. The kernel is $\{e\} \oplus H$. $\square$

Exercise 10.10. *Let G be a subgroup of D_n. Define:*

$$\phi(x) = \begin{cases} +1 & \text{if } x \text{ is a rotation} \\ -1 & \text{if } x \text{ is a reflection} \end{cases}$$

Prove that ϕ is a homomorphism from G to $\{+1, -1\}$ under multiplication. What is the kernel? And use this to show that either every element of G is rotation, or exactly half element of G is rotation.

Proof. It is easy to show that ϕ is a homomorphism. Note that the identity of codomain is $+1$, so $\operatorname{Ker}\phi$ is the set of rotations of G.

If there is no reflection in G, then G consists of rotations. So we suppose $F \in G$ is a reflection. By $G/\operatorname{Ker}\phi \approx \phi(G)$ we know $\dfrac{|G|}{|\operatorname{Ker}\phi|} = |\phi(G)|$. It is easy to show $|\phi(G)| = 2$. Thus the order of $\operatorname{Ker}\phi$, the number of rotations of G is exactly $\dfrac{|G|}{2}$. $\square$

Exercise 10.11. *Prove that $(Z \oplus Z)/(\langle a\rangle \oplus \langle b\rangle)$ is isomorphic to $Z_a \oplus Z_b$.*

Proof. We claim the following function is a homomorphism:

$$\boxed{\phi((x, y)) = (x \mod a, y \mod b) : Z \oplus Z \to Z_a \oplus Z_b}$$

It is trivial that ϕ is a homomorphism. Then for any $(x, y) \in Z \oplus Z$, $\phi((x, y)) = (0, 0)$ says $x \in \langle a\rangle$ and $y \in \langle b\rangle$. Thus $(x, y) \in \langle a\rangle \oplus \langle b\rangle$. So $\operatorname{Ker}\phi = \langle a\rangle \oplus \langle b\rangle$. And obviously, $\phi(Z \oplus Z) = Z_a \oplus Z_b$, by First Isomorphism Theorem, $(Z \oplus Z)/(\langle a\rangle \oplus \langle b\rangle) \approx Z_a \oplus Z_b$. $\square$

Exercise 10.12. *Suppose k is a divisor of n. Prove that $Z_n/\langle k\rangle \approx Z_k$.*

Proof. Since k divides n, we write $n = kq$. Consider the function $\phi(x) = qx : Z_n \to Z_n$. For any $a\ b \in Z_n$:

$$\begin{aligned}\phi(a+b) &= q(a+b) \\ &= qa + qb \\ &= \phi(a)\phi(b)\end{aligned}$$

We next show that $\langle k \rangle$ is the kernel of ϕ. For any $kd \in Z_n$, $\phi(kd) = qkd = nd = 0$. And for any $x \in Z_n$, if $\phi(x) = 0$, $qx = 0$, then $n = kq$ divides qx, say $qx = kqq'$, then by cancellation, $x = kq' \in \langle k \rangle$.

Since $n = kq$, $|\langle k \rangle| = |\langle \frac{n}{q} \rangle| = q$. Then by $\dfrac{|Z_n|}{|\langle k \rangle|} = |\phi(Z_n)|$ we know $|\phi(Z_n)| = \frac{n}{q} = k$. And $\phi(Z_n)$ is cyclic since Z_n is cyclic. Thus $\phi(Z_n) \approx Z_k$. □

Exercise 10.13. *Prove that* $(A \oplus B)/(A \oplus \{e\}) \approx B$.

Proof. Consider the function $\phi((a,b)) = b$ from $A \oplus B$ to B. It is trivial that ϕ is homomorphism. $A \oplus \{e\} = \operatorname{Ker}\phi$ and $\phi(A \oplus B) = B$. □

Exercise 10.22. *Let* $\phi : G \to \overline{G}$ *is a homomorphism and* ϕ *is onto, where* G *is a finite group. For any element* $g \in \overline{G}$*, prove that* G *has an element of order* $|g|$.

Proof. Since ϕ is onto, $\phi(G) = \overline{G}$, then $G/\operatorname{Ker}\phi \approx \overline{G}$. For any element of $g \in \overline{G}$, there is an element of order $|g|$ in $G/\operatorname{Ker}\phi$. Then by Lemma 9.1, G also has an element of order $|g|$. □

Exercise 10.29. *Suppose that* ϕ *is a homomorphism from finite* G *onto* Z_{10}*. Prove that* G *has normal subgroups of index* 2 *and* 5.

Proof. By Exercise 10.12, there is a homomorphism f from Z_{10} onto Z_2 and g from Z_{10} onto Z_5.

Thus, $\operatorname{Ker} f\phi$ is a normal subgroup of G of index 2 and $\operatorname{Ker} g\phi$ is a normal subgroup of G of index 5. □

Exercise 10.48 ($\star$)**.** *Let* ϕ *a homomorphism from* G *to some group, where* $G = \langle S \rangle$ *and* $\langle S \rangle = \{\ s_0^{d_0} s_1^{d_1} \cdots s_n^{d_n} \mid s_i \in S, d_i \in \mathbb{Z}\ \}$*. Prove that* $\phi(G) = \langle \phi(S) \rangle$.

Proof. For any $\phi(x) \in \phi(G)$, since G is generated by S:

$$\begin{aligned}\phi(x) &= \phi(s_0^{d_0} s_1^{d_1} \cdots s_n^{d_n}) \\ &= \phi(s_0^{d_0})\phi(s_1^{d_1}) \cdots \phi(s_n^{d_n}) \\ &= \phi(s_0)^{d_0}\phi(s_1)^{d_1} \cdots \phi(s_n)^{d_n}\end{aligned}$$

where $\phi(s_i) \in \phi(S)$, thus $\phi(x) \in \langle \phi(S) \rangle$.

And for any $x \in \langle \phi(S) \rangle = \{\ t_0^{d_0} t_1^{d_1} \cdots t_m^{d_m} \mid t_i \in \phi(S), d_i \in \mathbb{Z}\ \}$, since it is generated by $\phi(S)$:

$$\begin{aligned}x &= t_0^{d_0} t_1^{d_1} \cdots t_m^{d_m} \\ &= \phi(s_0)^{d_0}\phi(s_1)^{d_1} \cdots \phi(s_m)^{d_m} \\ &= \phi(s_0^{d_0})\phi(s_1^{d_1}) \cdots \phi(s_m^{d_m}) \\ &= \phi(s_0^{d_0} s_1^{d_1} \cdots s_m^{d_m})\end{aligned}$$

where $s_0^{d_0} s_1^{d_1} \cdots s_m^{d_m} \in \langle S \rangle = G$, $\phi(s_0^{d_0} s_1^{d_1} \cdots s_m^{d_m}) \in \phi(G)$. □

Exercise 10.49 (Second Isomorphism Theorem)**.** *If $K \leq G$ and $N \lhd G$, show that $K/(K \cap N) \approx KN/N$.*

Proof. Let $\phi(k) = kN$ a mapping from K to KN/N. For any $a\ b \in K$, $\phi(ab) = abN = aNbN = \phi(a)\phi(b)$, thus ϕ is a homomorphism.

For any $k \in K$, if $k \in N$, $\phi(k) = N$, thus $\operatorname{Ker}\phi = K \cap N$.

For any $aN \in KN/N$ where $a \in KN$, thus $a = kn$ for some $k \in K$ and $n \in N$. Then $aN = (kn)N = kNnN$, since $n \in N$, so $kNnN = kN$ and $aN = kN$. Then $\phi(k) = kN = aN$, ϕ is onto.

By $K/\operatorname{Ker}\phi \approx \phi(K)$ we get $K/(K \cap N) \approx KN/N$. □

Exercise 10.50 (Third Isomorphism Theorem)**.** *Let M and N are normal subgroups of G, and $N \leq M$. Prove that $(G/N)/(M/N) \approx G/M$.*

Proof. Consider $\phi(gN) = gM$ from G/N to G/M. We need to show that it **is** a function. For any $aN\ bN \in G/N$ where $aN = bN$, then $a^{-1}b \in N$, thus $a^{-1}b \in M$ since $N \leq M$. Then $aM = bM$ and $\phi(aN) = \phi(bN)$.

For any $mN \in M/N$ where $m \in M$, $\phi(mN) = mM = M$ since $m \in M$. Thus $M/N \subseteq \operatorname{Ker}\phi$. For any $gN \in G/N$ such that $\phi(gN) = M$, then $gM = M$ and $g \in M$, therefore $gN \in M/N$. Thus $\operatorname{Ker}\phi \subseteq M/N$.

For any $gM \in G/M$, we have $\phi(gN) = gM$, therefore ϕ is onto. And by First Isomorphism Theorem, $(G/N)/\operatorname{Ker}\phi = (G/N)/(M/N) \approx \phi(G/N) = G/M$. $\square$

Exercise 10.59. *Using* Lemma 10.17 *to answer the following question: Let N be a normal subgroup of G, show that every subgroup of G/N has form (is isomorphic to) H/N, where $H \leq G$.*

Proof. We have natural mapping $\gamma(g) = gN$. Let $\overline{H}$ a subgroup of G/N, and let $H = \gamma^{-1}(\overline{H})$. By Lemma 10.17, H is a subgroup of G. Since $\gamma^{-1}(e) = \operatorname{Ker}\gamma$ and $e \in \overline{H}$, then $\operatorname{Ker}\gamma = N \subseteq \gamma^{-1}(\overline{H}) = H$.

Now let $\psi(h) = \gamma(h)$ a homomorphism from H to G/N. Since $H/N \approx \psi(H) = \gamma(H) = \gamma(\gamma^{-1}(\overline{H})) = \overline{H}$. We conclude that every subgroup $\overline{H}$ has form H/N. $\square$

Exercise 10.60. *Let $S = \langle a \rangle$, ϕ and ψ are homomorphism from S to some group, show that if $\phi(a) = \psi(a)$, $\phi = \psi$.*

Proof. For any $a^k \in S$, $\phi(a^k) = \phi(a)^k = \psi(a)^k = \psi(a^k)$. $\square$

Exercise 10.61. *Using First Isomorphism Theorem to prove the theorem in Chapter 9: For any group G, $G/Z(G) \approx \operatorname{Inn}(G)$*

Proof. Let $\phi(g) = \phi_g$ a mapping from G to $\operatorname{Inn}(G)$, where $\phi_g(x) = gxg^{-1}$ is inner isomorphism.

For any $a\ b \in G$, $\phi(ab) = \phi_{ab} = \phi_a \circ \phi_b = \phi(a) \circ \phi(b)$. Thus ϕ is a homomorphism.

For any $g \in Z(G)$, $\forall x \in G, \phi(g)(x) = \phi_g(x) = gxg^{-1} = xgg^{-1} = x$ tells us $\phi(g) = \phi_g = \phi_e$. And for any $g \in G$ where $\phi(g) = \phi_g = \phi(e) = \phi_e$, then $\forall x \in G, \phi_g(x) = \phi_e(x) \to gxg^{-1} = x$ therefore $gx = xg$, this tells us $g \in Z(G)$. Thus the kernel of ϕ is $Z(G)$.

For any $\phi_g \in \operatorname{Inn}(G)$ for some g, $\phi(g) = \phi_g$, thus ϕ is onto.

And by First Isomorphism Theorem, $G/\operatorname{Ker}\phi = G/Z(G) \approx \phi(G) = \operatorname{Inn}(G)$. $\square$

Exercise 10.66. *If H and K are normal subgroups of G and $H \cap K = \{e\}$. Prove that G is isomorphic to some subgroup of $G/H \oplus G/K$.*

Proof. Consider the mapping $\phi(g) = (gH, gK)$ from G to $G/H \oplus G/K$. It is obviously a homomorphism by $\forall a\ b \in G, abH = aHbH$.

For any $g \in \operatorname{Ker}\phi$, $\phi(g) = (H, K)$ implies $g \in H$ and $g \in K$, thus $g \in H \cap K$, but the only element in $H \cap K$ is e, thus $g = e$. Then $\operatorname{Ker}\phi \subseteq \{e\}$, and $\{e\} \subseteq \operatorname{Ker}\phi$ since $\operatorname{Ker}\phi$ is a subgroup.

Thus $G/\operatorname{Ker}\phi = G/\{e\} \approx G \approx \phi(G)$ where $\phi(G)$ is a subgroup of $G/H \oplus G/K$. □

69

Exercise 10.68. *If G is a non-Abelian group of order 55. Prove that G has exactly 11 subgroups of order 5, and they have form a^iKa^{-1} for $i = 0, 1, \ldots, 10$ for some element a in G and some subgroup K of G.*

Proof. If G has no element of order 11, then G has to have 54 non-identity elements of order 5. But $|\phi(5)| = 4$ doesn't divides 54 (ϕ is Eular's totient function), thus G has at least one element of order 11. Suppose H and K are subgroups of G of order 11, then $|HK| = \dfrac{|H||K|}{|H \cap K|} = \dfrac{11 \times 11}{1} = 121$. But $HK \subseteq G$ where $|G| = 55$. Thus G has only one subgroup of order 11, and G has at least one element of order 5.

We denote the subgroup of G of order 11 as H, and a subgroup of G of order 5 as K.

Let $\phi(k) = aka^{-1}$ (and forget the last ϕ we use) from K to G, where $a \in H$. It is obviously a homomorphism.

We will show that $\phi \neq \mathrm{id}$. Suppose $\forall k \in K, \phi(k) = aka^{-1} = k$. Then $a \in C(k)$. Obviously, $K \subseteq C(k)$ since K is Abelian. If $a \in C(k)$, then $H \subseteq C(k)$ since a is the generator of H. Then $HK \subseteq C(k)$ where $|HK| = \dfrac{|H||K|}{|H \cap K|} = \dfrac{11 \times 5}{1} = 55$. Thus $C(k) = G$, therefore $k \in Z(G)$, and $\langle k \rangle = K \subseteq Z(G)$. But now the index of K is prime, which indicates G is Abelian. So $\phi \neq id$. Then by $\phi^{11}(k) = a^{11}ka^{-11} = eke = k$, $|\phi| = 11$.

For any $i\ j \in Z_{11}$, $s\ t \in K$, and suppose $i \neq j$, s and t are non-identity and $\phi^i(s) = \phi^j(t)$. Then $\phi^{i-j}(s) = t$, therefore $\phi^{i-j}(K) = K$ since s and t are generators of K, which means $a^{i-j} \in N(K)$, therefore $H \subseteq N(K)$ since a^{i-j} generates H. Obviously, $K \subseteq N(K)$, thus $N(K) = G$ since $HK \subseteq N(K)$ and $|HK| = 55$. And by $|\phi| = 11$, $H \nsubseteq C(K)$ unless $|\phi| = 1$. By $K \subseteq C(K)$ (since K is Abelian), $|C(K)|$ divides 55 and $H \nsubseteq C(K)$, we know $|C(K)| = 5$ therefore $C(K) = K$. Then by N/C Theorem, $N(K)/C(K) \approx$ a subgroup of $\operatorname{Aut}(K)$, where the order of left hand side is $\frac{|G|}{|K|} = 11$ and the order of right hand side is $|\operatorname{Aut}(K)| = |\operatorname{Aut}(Z_5)| = |U(5)| = 4$. 11 doesn't divides 4, thus $N(K)/C(K)$ can not isomorphic to a subgroup of $\operatorname{Aut}(K)$. If s is identity, then $\phi^i(s) = e$, therefore t has to be e, since the kernel of $\phi^j = \{e\}$. So the intersection of the image of ϕ^i and ϕ^j is $\{e\}$.

Finally, the image of each ϕ^i corresponds a subgroup of G, and they are distinct. Also, they have form $a^i K a^{-i}$ for $i \in Z_{11}$.

Then G has at least 11×4 elements of order 5, 10 elements of order 11, 1 element of order 1, where $44 + 10 + 1 = 55$. Thus G has exactly 11 subgroups of order 5. □

Exercise 10.74. *If m and n are positive integers, prove that the mapping $\phi(x) = x \bmod n$ from Z_m to Z_n is a homomorphism if and only if n divides m.*

Proof. Suppose ϕ is a homomorphism, then divide m by n, we get $m = nq + r$ where $0 \leq r < n$. If n doesn't divide m, that is, $r \neq 0$, then $\phi(m) = \phi(nq+r) = q\phi(n) + \phi(r) = \phi(r) = r \bmod n$. Since $r < n$, therefore $r \bmod n = r$. But $r \neq 0$ and $\phi(m) = \phi(0) = 0$. Thus n has to divide m.

Suppose n divides m, then $m = nq$. For any $x\ y \in Z_m$, $\phi(x+y) = (x + y \bmod m) \bmod n = (x + y \bmod nq) \bmod n$. Divide $x + y$ by nq, we get $x + y = (nq)p + s$, then divide s by n, we get $s = nr + t$, then $x + y = nqp + nr + t$. Therefore:

$$\begin{aligned}
&(x + y \bmod nq) \bmod n \\
=&(nqp + nr + t \bmod nq) \bmod n \\
=&nr + t \bmod n \\
=&t
\end{aligned}$$

where

$$\begin{aligned}
&x + y \bmod n \\
=&nqp + nr + t \bmod n \\
=&t
\end{aligned}$$

Then $\phi(x+y) = x + y \bmod n = ((x \bmod n) + (y \bmod n)) \bmod n = \phi(x) + \phi(y)$. □

Lemma. *Let H a normal subgroup of G, and let $\overline{G}$ be any group. the number of isomorphisms between G/H and $\overline{G}$ is equal to the number of homomorphism from G onto $\overline{G}$ where the kernel is H.*

Proof. The mapping f given by $\phi \mapsto (gH \mapsto \phi(g))$ from $(\Sigma[\phi \in G \to \overline{G}] \operatorname{Ker}\phi = H)$ to $G/H \approx \overline{G}$ ($gH \mapsto \phi(g)$ is a isomorphism by First Isomorphism Theorem) is bijective:

- One-to-one: For any $\phi\ \psi : G \to \overline{G}$, if $f(\phi) = f(\psi)$, then for any $g \in G$:

$$f(\phi)(gH) = f(\psi)(gH)$$
$$\phi(g) = \psi(g)$$

  which implies $\phi = \psi$

- Onto: For any $g : G/H \approx \overline{G}$, consider the homomorphism $\phi(a) = g(aH)$, for any $aH \in G/H$, $f(\phi)(aH) = \phi(a) = g(aH)$, thus $f(\phi) = g$.

□

Exercise 10.76. *Let p be a prime. Determine the number of homomorphisms from $Z_p \oplus Z_p$ to Z_p.*

Proof. For any homomorphism that maps to Z_p, the image of it can be $\{e\}$ or Z_p, we focus on the later one.

For each subgroup H of $Z_p \oplus Z_p$ of order p, we have $|(Z_p \oplus Z_p)/H \approx Z_p| = |Z_p \approx Z_p| = |Aut(Z_p)| = |U(p)| = \phi(p) = p - 1$ homomorphisms from $Z_p \oplus Z_p$ onto Z_p where the kernel is H.

And $Z_p \oplus Z_p$ has $\dfrac{p^2 - 1}{p - 1} = (p + 1)$ subgroups of order p. Thus there are $(p + 1)(p - 1) + 1 = p^2 - 1 + 1 = p^2$ homomorphisms from $Z_p \oplus Z_p$ to Z_p. □