Example 2–51. A simple, but illuminating, example of the Fundamental Theorem is furnished by the groups $(Z, +)$, $(\{1, -1\}, \cdot)$, and the homomorphism $f\colon Z \to \{1, \quad 1\}$, where

$$f(n) = \begin{cases} 1 & \text{if} \quad n \in Z_e, \\ -1 & \text{if} \quad n \in Z_o. \end{cases}$$

Here, the kernel of f is the set Z_e, so that

$$Z/\ker(f) = Z/Z_e = \{Z_e, Z_o\}.$$

The Fundamental Theorem then guarantees that $(\{Z_e, Z_o\}, \otimes)$ and $(\{1, -1\}, \cdot)$ are isomorphic groups indeed, this is fairly evident from an inspection of their multiplication tables:

$\otimes$	Z_e	Z_o
Z_e	Z_e	Z_o
Z_o	Z_o	Z_e

$\cdot$	1	-1
1	1	-1
-1	-1	1

Further, the proof of the theorem indicates that the function $\bar{f}$ which actually establishes this isomorphism (the induced mapping) is given by

$$\bar{f}(Z_e) = \bar{f}(0 + Z_e) = f(0) = 1,$$
$$\bar{f}(Z_o) = \bar{f}(1 + Z_e) = f(1) = -1.$$

Example 2–52. For a more penetrating example, consider an arbitrary group $(G, *)$ and a fixed element $a \in G$. Define the mapping $f\colon Z \to G$ by the rule $f(n) = a^n$, $n \in Z$. It is not difficult to check that f, so defined, is a homomorphic mapping from the additive group of integers $(Z, +)$ onto the cyclic subgroup $((a), *)$. Hence, by virtue of Theorem 2–47,

$$(Z/\ker(f), \otimes) \sim ((a), *),$$

where, in the situation at hand,

$$\ker(f) = \{n \in Z \mid a^n = e\}.$$

Now, two possibilities arise according to the magnitude of the kernel, the first being that $\ker(f) = \{0\}$; in other words, $a^n = e$ implies $n = 0$. Under the circumstances, $(Z/\ker(f), \otimes)$ is just the group $(Z, +)$ itself. On the other hand, if $\ker(f) \neq \{0\}$, there exists some least positive integer n for which $a^n = e$. One can easily deduce from this that $\ker(f) = (n)$, so we must have $(Z/\ker(f), \otimes) = (Z_n, +_n)$.

In summary, the preceding discussion reveals that (1) if the generator a is of infinite order, then $((a), *) \simeq (Z, +)$, and (2) if a is of finite order n, then

$((a), *) \simeq (Z_n, +_n)$. These facts are already familiar, of course, but the argument involved furnishes an alternative approach to Theorem 2–44.

The next theorem not only provides further evidence of the power of the Fundamental Theorem, but is of independent interest since it gives additional insight into the structure of the quotient group $(G/\text{cent } G, \otimes)$. To prepare the way, it is necessary to digress for a moment.

Given a fixed element a of the group $(G, *)$, define the mapping $\sigma_a: G \to G$ by taking

$$\sigma_a(x) = a * x * a^{-1}$$

for every x in G. Let us obtain a few of the special properties of this function. First, σ_a turns out to be a homomorphism: if $x_1, x_2 \in G$, then

$$\begin{aligned}\sigma_a(x_1 * x_2) &= a * (x_1 * x_2) * a^{-1} \\ &= (a * x_1 * a^{-1}) * (a * x_1 * a^{-1}) = \sigma_a(x_1) * \sigma_a(x_2).\end{aligned}$$

The next thing to notice is that σ_a maps the set G onto itself; specifically, for any element $x \in G$, $\sigma_a(a^{-1} * x * a) = x$. Finally, it can be proved that σ_a is actually a one-to-one function. For this purpose, assume $\sigma_a(x_1) = \sigma_a(x_2)$, so that $a * x_1 * a^{-1} = a * x_2 * a^{-1}$. The superfluous elements may be removed through the cancellation law, allowing us then to conclude that $x_1 = x_2$. All of these observations may be conveniently summarized by saying that

$$\sigma_a \in A(G).$$

Functions of the form σ_a, with $a \in G$, are usually called *inner automorphisms* of the group $(G, *)$; to be more precise, σ_a is the inner automorphism induced by the element a. For brevity, we label the set of functions arising in this way by $I(G)$:

$$I(G) = \{\sigma_a \mid a \in G\}.$$

In the case of a commutative group, $I(G)$ reduces to just the identity mapping $i_G = \sigma_e$. Thus, it is only when $(G, *)$ is noncommutative that the notion becomes meaningful.

Lemma. The pair $(I(G), \circ)$ constitutes a group, known as the *group of inner automorphisms* of $(G, *)$; in fact, $(I(G), \circ)$ is a normal subgroup of $(A(G), \circ)$.

Proof. The proof that $(I(G), \circ)$ is a group presents no difficulties; it consists of nothing more than noticing that whenever $\sigma_a, \sigma_b \in I(G)$,

$$\sigma_a \circ \sigma_b = \sigma_{a*b}.$$

In addition to disposing of the closure condition, this relation also indicates σ_e is the identity element for the system and $\sigma_a^{-1} = \sigma_{a^{-1}}$.

Regarding the second assertion, it suffices to show that if $f \in A(G)$, the product $f \circ \sigma_a \circ f^{-1}$ is an inner automorphism. The argument proceeds as follows: for each element x in G,

$$\begin{aligned}(f \circ \sigma_a \circ f^{-1})(x) &= f\big(\sigma_a(f^{-1}(x))\big) \\ &= f(a * f^{-1}(x) * a^{-1}) \\ &= f(a) * f(f^{-1}(x)) * f(a^{-1}) \\ &= f(a) * x * f(a)^{-1} = \sigma_{f(a)}(x).\end{aligned}$$

The reasons for each of these steps are reasonably self-evident, and the reader should make sure he understands them. What is significant is that

$$f \circ \sigma_a \circ f^{-1} = \sigma_{f(a)} \in I(G),$$

as was to be proved.

We are now in a position to obtain the result which has been our goal. Namely, that the groups $(G/\text{cent } G, \otimes)$ and $(I(G), \circ)$ resemble each other in all essential aspects.

Theorem 2–48. For each group $(G, *)$, $(G/\text{cent } G, \otimes) \simeq (I(G), \circ)$.

Proof. To begin, consider the mapping $g: G \to I(G)$ whereby $g(a) = \sigma_a$. That this function maps G onto the set $I(G)$ is quite plain. It is equally easy to see that g is a homomorphism, since

$$g(a * b) = \sigma_{a*b} = \sigma_a \circ \sigma_b = g(a) \circ g(b), \qquad a, b \in G.$$

The crucial aspect of the proof is now to show that $\ker(g) = \text{cent } G$; once this is done, the desired conclusion will follow immediately from the Fundamental Theorem.

In the case at hand, the inner automorphism σ_e serves as the identity element for the group $(I(G), \circ)$. Accordingly, the kernel of the function g is defined by

$$\begin{aligned}\ker(g) &= \{a \in G \mid g(a) = \sigma_e\} \\ &= \{a \in G \mid \sigma_a = i_G\}.\end{aligned}$$

Referring to the definition of equality of functions, we conclude that $a \in \ker(g)$ if and only if

$$a * x * a^{-1} = x$$

for every x in G. But this is obviously equivalent to demanding the element a be such that $a * x = x * a$ for all $x \in G$, or what amounts to the same thing, that $a \in \text{cent } G$.

Returning to the general development, once again let f be a homomorphism from the group $(G, *)$ onto the group $(G', \circ)$. We have already noticed that

every subgroup $(H, *)$ of the group $(G, *)$ determines a subgroup $(f(H), \circ)$ of the group $(G', \circ)$. It goes without saying that group theory would be considerably simplified if the subgroups of $(G, *)$ were in a one-to-one correspondence with those of $(G', \circ)$ in this manner. Unfortunately, this need not be the case.

The situation is reflected in the fact that if $(H, *)$ and $(K, *)$ are two subgroups of $(G, *)$ with $H \subseteq K \subseteq H * \ker(f)$, then $(f(H), *) = (f(K), *)$. The quickest way to see this is to note that

$$f(H) \subseteq f(K) \subseteq f(H * \ker(f)) = f(H) \circ f(\ker(f)) = f(H),$$

from which we infer that all the inclusions are actually equalities. In essence, we are observing that distinct subsets of G may have the same image set in G'.

The difficulty in the last paragraph could be remedied by either requiring that $\ker(f) = \{e\}$ or else by narrowing our view to consider only subgroups $(H, *)$ with $\ker(f) \subseteq H$. In either event, it follows that

$$H \subseteq K \subseteq H * \ker(f) \subseteq H,$$

yielding the subsequent equality $H = K$. The first of these aforementioned conditions has the effect of making the function f one-to-one, in which case $(G, *)$ and $(G', \circ)$ are isomorphic groups. The second possibility is the subject of the next theorem.

We pause to establish a preliminary lemma which will provide the key to later success.

Lemma. If H is any subset of G such that $\ker(f) \subseteq H$, then $H = f^{-1}(f(H))$.

Proof. Suppose the element a is in $f^{-1}(f(H))$, so that $f(a) \in f(H)$. Then $f(a) = f(h)$ for some choice of $h \in H$. As the equation $f(a) = f(h)$ is equivalent to $f(a * h^{-1}) = e'$, we have $a * h^{-1} \in \ker(f) \subseteq H$. This implies a also belongs to the set H and yields the inclusion $f^{-1}(f(H)) \subseteq H$. The opposite inclusion always holds (Theorem 1–7), whence $H = f^{-1}(f(H))$.

The relationship between the subgroups of $(G, *)$ and the subgroup of $(G', \circ)$ may be stated as follows:

Theorem 2–49. (*Correspondence Theorem*). There is a one-to-one correspondence between those subgroups $(H, *)$ of the group $(G, *)$ such that $\ker(f) \subseteq H$ and the set of all subgroups $(H', \circ)$ of the group $(G', \circ)$; specifically, H' is given by $H' = f(H)$.

Proof. Let us first check that the indicated correspondence is onto. In other words, if $(H', \circ)$ is any subgroup of $(G', \circ)$, we must produce some subgroup $(H, *)$ of $(G, *)$ with $\ker(f) \subseteq H$ for which $f(H) = H'$. To accomplish this, it is sufficient to take $H = f^{-1}(H')$. By Theorem 2-39, the pair $(f^{-1}(H'), *)$ is

a subgroup of $(G, *)$ and, since $e' \in H'$,

$$\ker(f) = f^{-1}(e') \subseteq f^{-1}(H').$$

Moreover, the function f being an onto mapping, the corollary to Theorem 1–6 indicates that $f(f^{-1}(H')) = H'$.

Next, we verify that this correspondence is also one-to-one. To this end, suppose $(H_1, *)$ and $(H_2, *)$ are both subgroups of $(G, *)$ with $\ker(f) \subseteq H_1$, $\ker(f) \subseteq H_2$ and such that $f(H_1) = f(H_2)$. According to the preceding lemma, we then must have

$$H_1 = f^{-1}(f(H_1)) = f^{-1}(f(H_2)) = H_2.$$

It follows that the correspondence $(H, *) \leftrightarrow (f(H), \circ)$ is one-to-one, thereby completing the proof.

The theorem applies, in particular, to the case in which we start with a normal subgroup $(H, *)$ of $(G, *)$ and take f to be the natural mapping $\text{nat}_H: G \to G/H$ of G onto G/H. Since $\ker(\text{nat}_H) = H$, the conclusion is modified slightly.

Corollary. Let $(H, *)$ be a normal subgroup of the group $(G, *)$. There is a one-to-one correspondence between those subgroups $(K, *)$ of $(G, *)$ such that $H \subseteq K$ and the set of all subgroups of the quotient group $(G/H, \otimes)$.

Before proceeding, it should be remarked that the Correspondence Theorem remains valid if we replace the term "subgroup" throughout by "normal subgroup." That is to say, there is also a one-to-one correspondence between those normal subgroups of $(G, *)$ which contain $\ker(f)$ and the set of all normal subgroups of $(G', \circ)$. The additional argument needed to establish this fact is left for the reader to supply.

Example 2–53. As an application of these ideas, consider the following statement: if $(G, *)$ is a finite cyclic group of order n, then $(G, *)$ has exactly one subgroup of order m for each positive divisor m of n and no other proper subgroups. Although there is nothing very surprising about this assertion, our aim is to demonstrate its validity by using the corollary to the Correspondence Theorem.

First observe that, since the groups $(G, *)$ and $(Z_n, +_n)$ are isomorphic, there is no loss in generality in working with $(Z_n, +_n)$. Furthermore, as we have pointed out on several occasions, $(Z_n, +_n) = (Z/(n), \otimes)$. By the corollary, we learn there is a one-to-one correspondence between those subgroups of the group $(Z, +)$ which contain the set (n) and the subgroups of $(Z_n, +_n)$.

But, the subgroups of $(Z, +)$ are just the cyclic subgroups $((m), +)$, where m is a nonnegative integer. Combining these results, we arrive at the conclusion there is a one-to-one correspondence between the subgroups of $(Z_n, +_n)$

and those subgroups $((m), +)$ of $(Z, +)$ such that $(m) \supseteq (n)$. This last inclusion occurs if and only if m divides n.

The two concluding theorems of this section are somewhat deeper results than usual and require the full force of our accumulated machinery; they comprise what are often called the First and Second Isomorphism Theorems for Groups and are of great importance in the study of group structure.

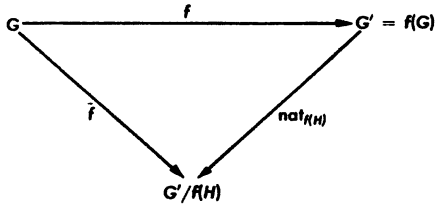
Theorem 2-50. If $(H, *)$ is any normal subgroup of the group $(G, *)$ such that $\ker(f) \subseteq H$, then $(G/H, \otimes) \simeq (G'/f(H), \otimes')$.

Proof. As a prefatory remark, we might point out that the corollary to Theorem 2-39 implies the pair $(f(H), \circ)$ is a normal subgroup of $(G', \circ)$, so that it is certainly permissible to form the quotient group $(G'/f(H), \otimes')$.

Let us now define the function $\bar{f}: G \to G'/f(H)$ by

$$\bar{f} = \text{nat}_{f(H)} \circ f,$$

where $\text{nat}_{f(H)}: G \to G'/f(H)$ designates the natural mapping. The following diagram helps to visualize the situation:



Observe that $\bar{f}$ merely assigns to each element $a \in G$ the coset $f(a) \circ f(H)$ of $G'/f(H)$. Since both the functions f and $\text{nat}_{f(H)}$ are onto and operation-preserving, the composition of these gives us a homomorphic mapping from the group $(G, *)$ onto the group $(G'/f(H), \otimes')$.

The main line of the argument is to show that $\ker(\bar{f}) = H$, for then the desired result would be a simple consequence of the Fundamental Theorem. Now the identity element of $(G'/f(H), \otimes')$ is just the coset $f(H) = e' \circ f(H)$. This means the kernel of $\bar{f}$ consists of those members of G which are mapped by $\bar{f}$ onto $f(H)$; that is,

$$\begin{aligned} \ker(\bar{f}) &= \{a \in G \mid \bar{f}(a) = f(H)\} \\ &= \{a \in G \mid f(a) \circ f(H) = f(H)\} \\ &= \{a \in G \mid f(a) \in f(H)\} = f^{-1}(f(H)). \end{aligned}$$

As we are given that $\ker(f) \subseteq H$, the lemma preceding Theorem 2-49 may be invoked to conclude $H = f^{-1}(f(H))$. Hence, $\ker(\bar{f}) = H$, which completes the proof.

In applications of this theorem, we frequently start with an arbitrary normal subgroup of $(G', \circ)$ and utilize inverse images rather than direct images.