2–2 CERTAIN ELEMENTARY THEOREMS ON GROUPS

As we remarked earlier, our approach to the subject matter in this text is characterized by the abstract axiomatic development of modern mathematics. Thus each system to be investigated consists of a set of elements and one or more operations which are undefined except that they are assumed to obey certain rules known as *axioms* or *postulates*. Once the axioms are granted, all else is obtained by careful logical argument. Each new theorem is deduced from the definitions, the axioms, and the theorems previously proved. The great advantage of the axiomatic method is that any particular example we encounter which satisfies the axioms of a given mathematical system will also satisfy all the theorems which are true for that system. While the uninitiated reader may find this approach uncomfortably abstract at first, the feeling will disappear as he progresses further into the text. In the process, we hope that he will gain an appreciation of mathematics as an exacting, logical discipline.

In proving the following theorems on groups, it is essential to understand that we know nothing whatever about the actual nature of either the set G or the operation $*$; both are completely abstract and unspecified. Our knowledge of G and its associated operation is strictly confined to the information contained in the definition of group given earlier. The reader would be well advised at this point to review Definition 2–11, Section 2–1, before proceeding. We shall begin with a simple, yet highly important result.

Theorem 2–2. The identity element of a group $(G, *)$ is unique, and each element of a group has precisely one inverse element.

Proof. Theorem 2–1 may be used to establish that the identity is unique. To show that an element has exactly one inverse in G, we proceed as in Theorem 2–1 by showing that two supposedly distinct inverses are actually equal. To this end, assume the element $a \in G$ has two inverses, a_1' and a_2'. Then according to the definition of inverse,

$$a * a_1' = a_1' * a = e, \qquad a * a_2' = a_2' * a = e.$$

But, the identity element is the same in both cases (there is only one identity as we have already seen), so that

$$a * a_1' = a * a_2'.$$

Multiply both sides of this equation on the left by a_1' (or by a_2') to get

$$a_1' * (a * a_1') = a_1' * (a * a_2').$$

Using the associative law, we have $(a_1' * a) * a_1' = (a_1' * a) * a_2'$, and so

$$e * a_1' = e * a_2' \qquad \text{or} \qquad a_1' = a_2',$$

which proves that a has only one inverse.

An inspection of the proof shows that we have established a little more than is indicated by the statement of the theorem. We have, in fact, shown that if an element of a semigroup with identity has an inverse, then it must be unique.

Corollary. Each element of a semigroup with identity has at most one inverse.

A further useful conclusion to be drawn from Theorem 2–2 is that $(a^{-1})^{-1} = a$. This stems from the observation that $(a^{-1})^{-1}$ is an element of G for which

$$a^{-1} * (a^{-1})^{-1} = (a^{-1})^{-1} * a^{-1} = e.$$

Since a itself has this property, and since inverses have just been seen to be unique, the element a must be the inverse of a^{-1}. For the proof of the next theorem, we shall require a preliminary lemma.

Lemma. If $a, b, c, d \in G$ and $(G, *)$ is a semigroup, then

$$(a * b) * (c * d) = a * ((b * c) * d).$$

Proof. Let us temporarily denote the product $c * d$ by x. Then, since the operation $*$ is associative, we have

$$\begin{aligned} a * ((b * c) * d) &= a * (b * (c * d)) \\ &= a * (b * x) \\ &= (a * b) * x \\ &= (a * b) * (c * d). \end{aligned}$$

Theorem 2–3. If $(G, *)$ is a group and $a, b \in G$, then $(a * b)^{-1} = b^{-1} * a^{-1}$. That is, the inverse of a product of group elements is the product of their inverses in reverse order.

Proof. According to the definition of inverse, all we need to show is that

$$(a * b) * (b^{-1} * a^{-1}) = (b^{-1} * a^{-1}) * (a * b) = e,$$

where e is the group identity. From the uniqueness of the inverse of $a * b$, we would then conclude that

$$(a * b)^{-1} = b^{-1} * a^{-1}.$$

Using the above lemma, we have

$$\begin{aligned} (a * b) * (b^{-1} * a^{-1}) &= a * ((b * b^{-1}) * a^{-1}) \\ &= a * (e * a^{-1}) = a * a^{-1} \\ &= e. \end{aligned}$$

A similar argument establishes that $(b^{-1} * a^{-1}) * (a * b) = e$.