By the definition of $e$ in $\mathscr{G}_2$,

$$b = c.$$

Similarly, from $b * a = c * a$ one can deduce that $b = c$ upon multiplication on the right by $a'$ and use of the axioms for a group. ◆

Our next proof can make use of Theorem 2.16. We show that a "linear equation" in a group has a *unique* solution. Recall that we chose our group properties to allow us to find solutions of such equations.

**2.17 Theorem** If $G$ is a group with binary operation $*$, and if $a$ and $b$ are any elements of $G$, then the linear equations $a * x = b$ and $y * a = b$ have unique solutions $x$ and $y$ in $G$.

***Proof*** First we show the existence of *at least* one solution by just computing that $a' * b$ is a solution of $a * x = b$. Note that

$$\begin{aligned} a * (a' * b) &= (a * a') * b, && \text{associative law,} \\ &= e * b, && \text{definition of } a', \\ &= b, && \text{property of } e. \end{aligned}$$

Thus $x = a' * b$ is a solution of $a * x = b$. In a similar fashion, $y = b * a'$ is a solution of $y * a = b$.

To show uniqueness of $y$, we use the standard method of assuming that we have two solutions, $y_1$ and $y_2$, so that $y_1 * a = b$ and $y_2 * a = b$. Then $y_1 * a = y_2 * a$, and by Theorem 2.16, $y_1 = y_2$. The uniqueness of $x$ follows similarly. ◆

Of course, to prove the uniqueness in the last theorem, we could have followed the procedure we used in motivating the definition of a group, showing that if $a * x = b$, then $x = a' * b$. However, we chose to illustrate the standard way to prove an object is unique; namely, suppose you have two such objects, and then prove they must be the same. Note that the solutions $x = a' * b$ and $y = b * a'$ need not be the same unless $*$ is commutative.

Because a group has a binary operation, we know from Theorem 1.15 that the identity $e$ in a group is unique. We state this again as part of the next theorem for easy reference.

**2.18 Theorem** In a group $G$ with binary operation $*$, there is only one element $e$ in $G$ such that

$$e * x = x * e = x$$

for all $x \in G$. Likewise for each $a \in G$, there is only one element $a'$ in $G$ such that

$$a' * a = a * a' = e.$$

In summary, the identity element and inverse of each element are unique in a group.

***Proof*** Theorem 1.15 shows that an identity element for any binary operation is unique. No use of the other group axioms was required to show this.

Turning to the uniqueness of an inverse, suppose that $a \in G$ has inverses $a'$ and $a''$ so that $a' * a = a * a' = e$ and $a'' * a = a * a'' = e$. Then

$$a * a'' = a * a' = e$$

and, by Theorem 2.16,

$$a'' = a',$$

so the inverse of $a$ in a group is unique. ◆

Note that in a group $G$, we have

$$(a * b) * (b' * a') = a * (b * b') * a' = (a * e) * a' = a * a' = e.$$

This equation and Theorem 2.18 show that $b' * a'$ is the unique inverse of $a * b$. That is, $(a * b)' = b' * a'$. We state this as a corollary.

**2.19 Corollary** Let $G$ be a group. For all $a, b \in G$, we have $(a * b)' = b' * a'$. ◆

For your information, we remark that binary algebraic structures with weaker axioms than those for a group have also been studied quite extensively. Of these weaker structures, the **semigroup,** a set with an associative binary operation, has perhaps had the most attention. A **monoid** is a semigroup that has an identity element for the binary operation. Note that every group is both a semigroup and a monoid.

Finally, it is possible to give axioms for a group $\langle G, * \rangle$ that seem at first glance to be weaker, namely:

1. The binary operation $*$ on $G$ is associative.
2. There exists a **left identity element** $e$ in $G$ such that $e * x = x$ for all $x \in G$.
3. For each $a \in G$, there exists **a left inverse** $a'$ in $G$ such that $a' * a = e$.

From this *one-sided definition*, one can prove that the left identity element is also a right identity element, and a left inverse is also a right inverse for the same element. Thus these axioms should not be called *weaker*, since they result in exactly the same structures being called groups. It is conceivable that it might be easier in some cases to check these *left axioms* than to check our *two-sided axioms*. Of course, by symmetry it is clear that there are also *right axioms* for a group.

## Group Isomorphisms

All our examples have been of infinite groups, that is, groups where the set $G$ has an infinite number of elements. We turn to finite groups, starting with the smallest finite sets.

Since a group has to have at least one element, namely, the identity, a minimal set that might give rise to a group is a one-element set $\{e\}$. The only possible binary operation $*$ on $\{e\}$ is defined by $e * e = e$. The three group axioms hold. The identity element is always its own inverse in every group.

**2.20 Table**

| $\times$ | 1 | $-1$ |
|---|---|---|
| 1 | 1 | $-1$ |
| $-1$ | $-1$ | 1 |

There is a group with only two elements, namely $G = \{1, -1\}$ with operation the usual multiplication. It is clear that $G$ is closed under multiplication and we know that multiplication is associative. Furthermore, 1 is the identity, the inverse of 1 is 1, and the inverse of $-1$ is $-1$. Table 2.20 is the group table for $G$.

Is this the only group with exactly two elements? To see, let us try to put a group structure on a set with two elements. Since one of the elements must be the identity, we will label the identity element $e$ and we will label the other element $a$. Following tradition, we place the identity first both on the top and to the left as in the following table.

| $*$ | $e$ | $a$ |
|---|---|---|
| $e$ | | |
| $a$ | | |

Since $e$ is to be the identity,

$$e * x = x * e = x$$

for all $x \in \{e, a\}$. We are forced to fill in the table as follows, if $*$ is to give a group:

| $*$ | $e$ | $a$ |
|---|---|---|
| $e$ | $e$ | $a$ |
| $a$ | $a$ | |

Also, $a$ must have an inverse $a'$ such that

$$a * a' = a' * a = e.$$

**2.21 Table**

| $*$ | $e$ | $a$ |
|---|---|---|
| $e$ | $e$ | $a$ |
| $a$ | $a$ | $e$ |

In our case, $a'$ must be either $e$ or $a$. Since $a' = e$ obviously does not work, we must have $a' = a$, so we have to complete the table as shown in Table 2.21.

All the group axioms are now satisfied, except possibly associativity. But if we relabel 1 as $e$ and $-1$ as $a$ in Table 2.20 we obtain Table 2.21. Therefore, the table we constructed for $\{e, a\}$ must also satisfy $\mathscr{G}_1$, the associative property. The table also shows clearly that properties $\mathscr{G}_2$ and $\mathscr{G}_3$ are satisfied, so $\langle \{e, a\}, * \rangle$ is a group. The groups $\{1, -1\}$ and $\{e, a\}$ are not the same, but they are essentially the same since by relabeling elements of one with the names of the other, the operations match. When the elements of one group can be matched with another in such a way that the operations are the same, we say that the groups are **isomorphic** and the matching is called a **group isomorphism**. We showed that any group with two elements is isomorphic with $\{1, -1\}$ under multiplication. The notation used to indicate isomorphism is $\simeq$, so we could write $\langle \{1, -1\}, \times \rangle \simeq \langle \{e, a\}, * \rangle$. Of course the matching is a one-to-one function from one group onto the other. If we were only interested in groups whose tables are easy to compute, then we would not need a more precise definition for isomorphism. We would simply see if we can relabel one group table to make it look like the other. However, in the case of infinite groups or even groups with more than a few elements, we need a better way to verify that groups are isomorphic. We now give a more precise definition of a group isomorphism.

**2.22 Definition** Let $\langle G_1, *_1 \rangle$ and $\langle G_2, *_2 \rangle$ be groups and $f : G_1 \to G_2$. We say that $f$ is a **group isomorphism** if the following two conditions are satisfied.

1. The function $f$ is one-to-one and maps onto $G_2$.
2. For all $a, b \in G_1, f(a *_1 b) = f(a) *_2 f(b)$. ■

Note that Condition 1 simply gives a way to relabel the elements of $G_1$ with elements in $G_2$. Condition 2, which we will refer to as the **homomorphism property**, says that with this relabeling, the operations $*_1$ on $G_1$ and $*_2$ on $G_2$ match. If we are in the context of groups, we will often use the term isomorphism to mean group isomorphism. If there is an isomorphism from a group $G_1$ to $G_2$, we say that $G_1$ is **isomorphic** with (or to) $G_2$. In Exercise 44, you are asked to show that if $f : G_1 \to G_2$ is an isomorphism, then $f^{-1} : G_2 \to G_1$, the inverse function, is also an isomorphism. So if $G_1$ is isomorphic with $G_2$, then $G_2$ is isomorphic with $G_1$. If you wish to verify that two groups, $G_1$ and $G_2$, are isomorphic, you can either construct an isomorphism mapping $G_1$ to $G_2$ or one mapping $G_2$ to $G_1$.

**2.23 Example** In Exercise 10 you will be asked to show that $2\mathbb{Z}$, the even integers, forms a group under addition. Here we show $\mathbb{Z}$ and $2\mathbb{Z}$ are isomorphic groups. In this case, the operations on the groups are both addition. We need a function $f : \mathbb{Z} \to 2\mathbb{Z}$ that is both one-to-one and onto $2\mathbb{Z}$. Let $f : \mathbb{Z} \to 2\mathbb{Z}$ be given by $f(m) = 2m$. We need to verify Condition 1 for an isomorphism, which says that $f$ is one-to-one and onto. Suppose that $a, b \in \mathbb{Z}$ and $f(a) = f(b)$. Then $2a = 2b$, which implies that $a = b$, so $f$ is one-to-one. We now show $f$