**Section 3: Fundamental Theorems about Groups**

We gave their usual names to the elements the "identity" of $G$ and the "inverse" of $g$ in $G$ mentioned in this definition; but we probably unwise to do so, because they might be ambiguous — just as "the square root" can be ambiguous: A positive real number has not one but two square roots, so to which does "the square root" refer? (There are several algebraic tricks based on this ambiguity.) Even to give a notation like $g^{-1}$ almost assumes there can only be one such inverse for a given $g$, i.e., one element represented by that symbol. (The square root symbol means the nonnegative square root — $\sqrt{4} = 2$, not $\pm 2$, — so it is not used in the context of complex numbers, where "positive" and "negative" are meaningless.) So let us prove that there is no ambiguity in this case:

**Prop:** In a group $G$, there is only one element $e$ that satisfies the condition in (i) of the definition, and for each $g$ in $G$ there is only one element $g^{-1}$ that satisfies the condition in (ii) of the definition.

*Pf:* The natural way to prove that there is only one of something is to assume that there are two and show they are the same. So suppose first that $e$ and $f$ both satisfy the condition of (i). Here is the big trick: What happens if we "star" them together? Well, because $e$ is an element of $G$ and $f$ has the condition in (i), $e * f = e$. But also, because $f$ is an element of $G$ and $e$ satisfies the condition in (i), we have $e * f = f$. So $e = f$.

Similarly, suppose $s$ and $t$ are both elements of $G$ that have the property ascribed to $g^{-1}$ in (ii). This time, "starring" them doesn't give much, but we can put their $g$ in the middle — and because the operation is associative, the two possible ways that the resulting three-fold "star" might be grouped into two binary operations must be equal: $s * g * t = s * (g * t) = s * e = s$, but also $s * g * t = (s * g) * t = e * t = t$, so $s = t$.//

Now we know that the terminology "the identity of $G$" and "the inverse of $g$ in $G$" and the symbol $g^{-1}$ are safe and unambiguous to use.

You may have noticed that in the proof we needed to use both equalities in (i) to prove that there is only one identity, and both equalities in (ii) to prove there is only one inverse for a given $g$. There are semigroups in which only one equality of (i) holds, i.e., the semigroup has a "left identity" that is not a "right identity" (or vice versa); or in which only one equality of (ii) holds, i.e., an element of the semigroup has a "left inverse" but not a "right inverse" (or vice versa). If an element $e$ satisfies $e * x = x$ for all $x$ in $S$, we'll call it a left identity, and if $y * x$ is an identity, then $y$ is a left inverse for $x$; but other books may call it a right identity and inverse, so I won't hold you to this terminology. The text gives the example $x * y = x$ on $\mathbb{Z}$ to show that we can have a right identity which is not unique. In fact, every integer $y$ — not just 1, which the text picks out, but also, say, 57 — works as a right identity: $x * 57 = x$ for every $x$. So there are infinitely many left identities. in this semigroup. Moreover, in this example, 57 is a left "inverse" (the quotes because 57 is not a real identity) for every element of $\mathbb{Z}$: $57 * x = 57$ for every $x$ in $\mathbb{Z}$.

Here is an example where there is a real (two-sided) identity, but some elements have only one-sided inverses: in the family $S$ of functions $\mathbb{Z}^+ \to \mathbb{Z}^+$, with the operation of composition, define $g$ to be the function $x \mapsto x + 1$, and for each $n$ in $\mathbb{Z}^+$ define $g_n$ by $g_n(1) = n$ and $g_n(x) = x - 1$ if $x > 1$. Then for each $n$, the composite function $g_n \circ g$ is the identity function $x \mapsto x$ on $\mathbb{Z}^+$, which is the identity in the semigroup $S$; so $g$ has infinitely many one-sided (Left? Right? Your choice.) inverses $g_n$. But it has no "other-sided" inverse, i.e., there is no $f$ in $S$ for which $g \circ f$ is the identity — because, if it did, we could use the proof above to show that all the $g_n$'s are equal to $f$ and hence to each other, which isn't true.

Enough ugly technicalities! Let's note some basic facts about groups:

**Prop:** Let $(G, *)$ be a group.

(i) For any element $x$ of $G$, $(x^{-1})^{-1} = x$.

(ii) (Cancellation) If $x * y = x * z$ [or if $y * x = z * x$] for some $x, y, z$ in $G$, then $y = z$.

(iii) If $x * y = x$ [or if $y * x = x$] for some $x, y$ in $G$, then $y = e$ (the identity).

(iv) If $x * y = e$ [or if $y * x = e$] for $x, y$ in $G$, then $y = x^{-1}$.

(v) If $x, y$ are elements of $G$, then there is exactly one element $z$ of $G$ for which $x * z = y$ [respectively $z * x = y$], namely $z = x^{-1} * y$ [respectively $z = y * x^{-1}$].

*Pf:* (i) Although high school algebra students have a hard time with this, it is really an obvious use of words — a "tautology", in the terminology of logic: An inverse of "Fred" is an element that, when it is "starred" with "Fred", the result is the identity, and $x$ plays that role for $x^{-1}$, so $x$ is the inverse of $x^{-1}$.

(ii) Suppose $x * y = x * z$. (The bracketed part is similar.) Then because the ordered pairs $(x^{-1}, x*y)$ and $(x^{-1}, x*z)$ are identical and $*$ is a function $S \times S$ to $S$, the images of these ordered pairs are equal, i.e., $x^{-1} * (x * y) = x^{-1} * (x * z)$ — this is just to explain why it is legal to "do the same thing to both sides of the equal sign" — and it follows easily, using associativity, that $y = z$.

(iii) and (iv) These are immediate from (ii): If $x*y = x = x*e$, then $y = e$. If $x*y = e = x*x^{-1}$, then $y = x^{-1}$. And similarly for the bracketed versions.

(v) It is easy to check that $z = x^{-1} * y$ satisfies $x * z = y$, and by cancellation it is the only solution. Similarly for the bracketed statement.//

In the following corollary, we use the Greek equivalents to the letters "l" for "operating" on the left, and "r" for "operating" on the right, by a fixed element of a group.

**Cor:** If $(G, *)$ is a group and $g \in G$, then the functions $\lambda_g : G \to G : x \mapsto g * x$ and $\rho_g : G \to G : x \mapsto x * g$ are one-to-one functions from $G$ onto $G$, i.e., they are elements of the group $\mathcal{S}(G)$.

*Pf:* They are one-to-one by (ii) (cancellation) and onto $G$ by (v).//

**Cor:** If $(G, *)$ is a finite group, then every element of $G$ appears exactly once in every row and column of the operation table for $*$.

*Pf:* The row of the operation that is headed by $x$ is a list of the elements $x * y$ in $G$. Because all the column heads are different, cancellation says that all the entries in that row are different, so every element of $G$ appears at most once in that row. But there are the same number of entries in that row as there are elements of $G$, so every element of $G$ must be there. (Or, we could have said, by (v) above, every element of $G$ appears in that row at least once, but the number of entries in the row is the same as the number of elements of $G$, so each element appears only once.)//

**Ex:** The operation table below makes the set $G = \{m, n, o, p, q, r\}$ into a group. Find the missing entries, justifying your answers:

| $*$ | $m$ | $n$ | $o$ | $p$ | $q$ | $r$ |
|---|---|---|---|---|---|---|
| $m$ | $m$ | $n$ | $o$ | $p$ | $q$ | $r$ |
| $n$ | $\boxed{1}$ | $p$ | $q$ | $\boxed{3}$ | $r$ | $o$ |
| $o$ | $\boxed{2}$ | $r$ | $m$ | $\boxed{5}$ | | $\boxed{6}$ |
| $p$ | | $\boxed{4}$ | $r$ | | | |
| $q$ | | | $n$ | | | |
| $r$ | | $q$ | $p$ | | | |

By the $o$-column, only $m$ could be the identity in this group. So $\boxed{1} = n * m = n$ and $\boxed{2} = o * m = o$.

The element $n$ must have an inverse, but no other element of its row is the identity $m$. So we have $\boxed{3} = n * p = m$. And because an inverse in a group must be 2-sided, $\boxed{4} = p * n = m$.

By associativity, $\boxed{5} = o * p = o * (n * n) = (o * n) * n = r * n = q$, and $\boxed{6} = o * r = o * (p * o) = (o * p) * o = q * o = n$.

The rest of the table is left to the class.