We also have

$$\begin{aligned}
(b^{-1}a^{-1})(ab) &= b^{-1}(a^{-1}(ab)) && \text{associativity} \\
&= b^{-1}((a^{-1}a)b) && \text{associativity} \\
&= b^{-1}(eb) && a^{-1} \text{ is the inverse of } a \\
&= b^{-1}b && e \text{ is the identity element} \\
&= e. && b^{-1} \text{ is the inverse of } b.
\end{aligned}$$

Therefore $b^{-1}a^{-1}$ is the inverse of ab. □

Observe that the inverse of ba is $a^{-1}b^{-1}$. Proposition 2.3 implies that the set of invertible elements of a monoid M is a group, also with identity element e.

Definition 2.2. If a group G has a finite number n of elements, we say that G is a group of *order* n. If G is infinite, we say that G has *infinite order*. The order of a group is usually denoted by $|G|$ (if G is finite).

Given a group G, for any two subsets $R, S \subseteq G$, we let

$$RS = \{r \cdot s \mid r \in R,\ s \in S\}.$$

In particular, for any $g \in G$, if $R = \{g\}$, we write

$$gS = \{g \cdot s \mid s \in S\},$$

and similarly, if $S = \{g\}$, we write

$$Rg = \{r \cdot g \mid r \in R\}.$$

From now on, we will drop the multiplication sign and write g_1g_2 for $g_1 \cdot g_2$.

Definition 2.3. Let G be a group. For any $g \in G$, define L_g, the *left translation by* g, by $L_g(a) = ga$, for all $a \in G$, and R_g, the *right translation by* g, by $R_g(a) = ag$, for all $a \in G$.

The following simple fact is often used.

Proposition 2.4. *Given a group* G*, the translations* L_g *and* R_g *are bijections.*

Proof. We show this for L_g, the proof for R_g being similar.

If $L_g(a) = L_g(b)$, then $ga = gb$, and multiplying on the left by g^{-1}, we get $a = b$, so L_g injective. For any $b \in G$, we have $L_g(g^{-1}b) = gg^{-1}b = b$, so L_g is surjective. Therefore, L_g is bijective. □

Definition 2.4. Given a group G, a subset H of G is a *subgroup of* G iff

(1) The identity element e of G also belongs to H ($e \in H$);