CS21201 Discrete Structures

About Identities

Why is it necessary to check whether an identity is both a left identity and a right identity?

In what follows, we let $*$ be an associative operation on a set S.

Theorem: If S contains a left identity L and a right identity R, then $L = R$, and this element is unique.

Proof By closure, $a = L * R \in S$. Since L is a left identity, we have $a = R$. Since R is a right identity, we have $a = L$. Therefore $a = L = R$. If L, L' are two left identities, then by the result just proved, we have $L = R$ and $L' = R$, that is, $L = L'$, that is, the left identity is unique. Analogously, the right identity is unique. ◄

From this result, it appears that checking both is not needed. But note that the theorem has a condition "if L and R both exist". Now, is it possible that this condition fails to hold?

The answer is yes. Consider the set S of all 2×2 matrices of the form

$$\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix},$$

where a, b are non-negative integers with $a > b$ (so $b \geqslant 0$, and $a > 0$). Take $*$ as normal matrix multiplication.

[Closure] We have the product

$$\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \begin{pmatrix} c & d \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} ac & ad \\ 0 & 0 \end{pmatrix}.$$

Since $a > 0$ and $c > d \geqslant 0$, we have $ac > ad \geqslant 0$.

[Associativity] Matrix multiplication is associative.

[Left identity] Consider the condition

$$\begin{pmatrix} \alpha & \beta \\ 0 & 0 \end{pmatrix} \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}.$$

We then have $\alpha a = a$ and $\alpha b = b$. Since this holds for any a, b, we should have $\alpha = 1$. This immediately does not put any restriction on β. But we should have $1 = \alpha > \beta \geqslant 0$, so this forces $\beta = 0$. Therefore

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$$

is the unique left identity in the structure.

[Right identity] Consider the condition

$$\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \begin{pmatrix} \alpha & \beta \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}.$$

We then have $a\alpha = a$ and $a\beta = b$. Since $a > 0$, we have $\alpha = 1$. But for any fixed β, the condition $a\beta = b$ cannot be satisfied by all a, b. It follows that a right identity in this structure does not exist.

Note: If we do not impose the restriction $a > b$ in the definition, that is, if we allow a, b to be arbitrary integers (non-negative if you prefer), then any element of the form

$$\begin{pmatrix} 1 & \beta \\ 0 & 0 \end{pmatrix}$$

is a left identity. So the left identity need not be unique. A right identity still does not exist anyway.

Therefore if you suspect some element as the identity, you should check that it is both a left identity and a right identity. If yes, then by the above theorem, that element will be the unique identity in the structure.

Likewise, check for both left and right inverses.