Solution to Exercise 15

We worked in class on Exercise 15 on page 149: If $*$ is a binary operation on a set A, and $*$ is associative, and there exists an identity element e, then define a relation R on A by saying that aRb when there exists an invertible element c such that $b = c^{-1} * a * c$. The goal is to show that R is an equivalence relation, that is, R is reflexive and symmetric and transitive.

The first point to notice is that in view of the existential quantifier, the element c may depend on a and b. The discussion below therefore uses subscripts to distinguish different instances of the element c. A second point to notice: multiplying by c shows that

$$b = c^{-1} * a * c \qquad \text{if and only if} \qquad c * b = a * c. \tag{1}$$

Proof of reflexivity The definition of identity element shows that $e * a = a * e$ (both sides are equal to a). Therefore property (1) shows that $a = e^{-1} * a * e$. In other words, aRa, for the required element c can be taken to be equal to e in this case. Since this argument holds for an arbitrary element a, the relation is reflexive.

Proof of symmetry If aRb, then there is an element c_1 such that $b = c_1^{-1} * a * c_1$. Multiplying on the right by c_1^{-1} shows that $b * c_1^{-1} = c_1^{-1} * a$. Rename c_1^{-1} as c_2 and switch the two sides of the equation to obtain that $c_2 * a = b * c_2$. In view of property (1), this equation means that bRa.

Thus aRb implies bRa for arbitrary elements a and b, so the relation is symmetric.

Proof of transitivity Usually the property of transitivity is written for elements a, b, and c, but the letter c is reserved in this problem, so consider instead three elements named a, b, and d.

Suppose aRb and bRd. Then there exists an element c_1 such that $b = c_1^{-1} * a * c_1$, and there exists an element c_2 such that $d = c_2^{-1} * b * c_2$. Substitute the first equation into the second equation to see that $d = c_2^{-1} * (c_1^{-1} * a * c_1) * c_2$. Since $*$ is associative, the grouping can be changed to write that $d = (c_2^{-1} * c_1^{-1}) * a * (c_1 * c_2)$.

Associativity also implies that

$$(c_2^{-1} * c_1^{-1}) * (c_1 * c_2) = c_2^{-1} * (c_1^{-1} * c_1) * c_2 = c_2^{-1} * e * c_2 = c_2^{-1} * c_2 = e,$$

so the inverse of $(c_1 * c_2)$ is $(c_2^{-1} * c_1^{-1})$. Give $(c_1 * c_2)$ the shorthand name c_3. The final equation of the preceding paragraph can then be rewritten as the statement that $d = c_3^{-1} * a * c_3$. In other words, aRd.

What has been shown is that $aRb \wedge bRd \implies aRd$ for arbitrary elements a, b, and d. Thus the relation is transitive.

Remark This relation is not just a made-up problem for practice. If you take linear algebra (Math 304 or Math 323), then you will encounter this equivalence relation under the name of *similarity*. And if you take modern algebra (Math 415), then you will encounter this equivalence relation under the name of *conjugacy*.