The Regular Representation

Let $(G, \cdot)$ be a monad. For any $g \in G$ let $g_L : G \to G$ be the mapping defined by $g_L(x) = gx$; this mapping is called **left translation** by g. If we let $M(G)$ denote the set of all mappings of G into itself then $M(G)$ is a monoid under composition of mappings, the neutral element being the identity mapping of G. Let $\rho_L : G \to M(G)$ be the mapping defined by $\rho_L(g) = g_L$. This mapping is called the **left regular representation** of G. If we replace left translations g_L by right translations g_R, where $g_R(x) = xg$, we get the **right regular representation** ρ_R of G.

If G has an identity element then both the left and right regular representation are injective. Indeed, if $g_L = h_L$ then $g \cdot 1 = h \cdot 1$ which gives $h = g$; similarly, $g_R = h_R$ implies $eg = eh$ and hence $h = g$.

Theorem 1. *The monad $(G, \cdot)$ is a semi-group iff $(gh)_L = g_L h_L$ for all $g, h \in G$.*

Proof. We have $(gh)_L = g_L h_L$ iff $gh(x) = g(hx)$ for all $x \in G$. □

Let $G_L = \rho_L(G) = \{g_L | g \in G\}$.

Corollary 2. *If the monad G has a neutral element then G is a monoid iff G_L is closed under composition of mappings, i.e., $g_L h_L \in G_L$ for all $g, h \in G$.*

Proof. If $g_L h_L = k_L$ then $gh = g(h \cdot 1) = k \cdot 1 = k$. □

Thus, if $(G, \cdot, 1)$ is a monoid, G_L is a subset of $M(G)$ containing 1_G and the product of any two elements in G_L. Such a subset of $M(G)$ is called a **monoid of transformations** of G. It is a monoid under composition of mappings, with neutral element 1_G. Moreover $\rho_L : (G, \cdot, 1) \xrightarrow{\sim} (G_L, \circ, 1_G)$. We thus get the following result:

Theorem 3 (Cayley's Theorem for Monoids). *Every monoid is isomorphic to a monoid of transformations.*

If G is a group, G_L is a permutation group on G and so is a group under composition of mappings. This gives

Theorem 4 (Cayley's Theorem). *Every group is isomorphic to a permutation group.*

The following theorem is a sharpening of Cayley's Theorem:

Theorem 5. *Every group is the group of symmetries of some structured set.*

Our proof rests on the following Lemma:

Lemma 6. *Let $(G, \cdot, 1)$ be a monoid. Then $G_L = \{f \in M(G) | f g_R = g_R f$ for all $g \in G\}$.*

Proof of Lemma. Let $(G, \cdot, 1)$ be a monoid. If $g, h \in G$ then $g_L h_R = h_R g_L$, i.e., left translations commute with right translations. Indeed, $g_L h_R(x) = g(xh) = (gx)h = h_R g_L(x)$ for any $x \in G$. Conversely, if $f \in M(G)$ and $f g_R = g_R f$ for all $g \in G$ then $f(xg) = f(x)g$ for all $x, g \in G$. Setting $x = 1$, we get $f(g) = f(1)g$ for all $g \in G$. Thus $f = h_L$ with $h = f(1)$. □

Proof of Theorem. Let s be the family $(g_R)_{g \in G}$. Then $s \in \wp(G \times \wp(G \times G))$. However, we want the first occurence of G in this structure to be external so that $f \in M(G)$ implies that $f_*(g, (h, k)) = (g, (f(h), f(k))$. Then, if $f \in S_G$, we have $f_*(s) = s \iff f_*(g_R) = g_R$. But $f_*(g_R) = f g_R f^{-1}$, so that $f_*(s) = s$ iff $f g_R f^{-1} = g_R$ for all $g \in G$, i.e., iff $f g_R = g_R f$ for all $g \in G$. By the lemma, this is equivalent to $f \in G_L$. □

Remark (The Graph of a Group). If s is the structure in the above proof and $(a,(b,c))$ is an element of s, then (b,c) can be viewed as an oriented edge joining the points b,c of G and a as a label for this edge. Thus (G,s) can be viewed as an graph whose edges are labeled by the elements of G. The symmetries of this graph are the permutations of G which send oriented edges to oriented edges and which do not change the label of an edge. If G is generated by a subset S of G, i.e, every element of G is a products of elements of S and their inverses, we can reduce the number of edges by taking only those edges labeled by an element of S. This does not change the group of symmetries (why?). This graph is called the graph of G with respect to the generating set S and is denoted by $\Gamma(G,S)$.

We now give an example of the use of the regular representation to show that an operation on a set is associative. By Theorem 1, it suffices to show that $g_L h_L = (gh)_L$ for all $g,h \in G$. If $|G| = n$, this requires $4n^3$ multiplications in G. If there is a neutral element, this reduces to $4(n-1)^3$ and to $2(n-1)^3$ if, in addition, the operation is commutative. However, one can reduces the number of multiplications required by reducing the number of products $g_L h_L$. This is due to the fact that one can associativity in $M(G)$ and any identities in G_L to great advantage. This is illustrated in the following problem.

Problem 1. *Show that the following table defines a group structure on $G = \{a,b,c,d,e,f,g,h\}$.*

	a	b	c	d	e	f	g	h
a	a	b	c	d	e	f	g	h
b	b	h	d	f	a	g	c	e
c	c	g	h	b	d	a	e	f
d	d	c	e	h	f	b	a	g
e	e	a	g	c	h	d	f	b
f	f	d	a	e	g	h	b	c
g	g	f	b	a	c	e	h	d
h	h	e	f	g	b	c	d	a

Solution. From the table we see that a is a neutral element and that $G_L \subseteq S_G$. One also sees immediately that each element is invertible. It remains to check the associative law. We have

$$a_L = 1,\ b_L = \begin{pmatrix} a & b & c & d & e & f & g & h \\ b & h & d & f & a & g & c & e \end{pmatrix},\ b_L^2 = \begin{pmatrix} a & b & c & d & e & f & g & h \\ h & e & f & g & b & c & d & a \end{pmatrix} = h_L,$$

$$b_L^3 = h_L b_L = \begin{pmatrix} a & b & c & d & e & f & g & h \\ e & a & g & c & h & d & f & b \end{pmatrix} = e_L,\ b_L^4 = e_L b_L = 1,$$

$$c_L = \begin{pmatrix} a & b & c & d & e & f & g & h \\ c & g & h & b & d & a & e & f \end{pmatrix},\ c_L^2 = \begin{pmatrix} a & b & c & d & e & f & g & h \\ h & e & f & g & b & c & d & a \end{pmatrix} = h_L,$$

$$c_L^3 = h_L c_L = \begin{pmatrix} a & b & c & d & e & f & g & h \\ f & d & a & e & g & h & b & c \end{pmatrix} = f_L,\ c_L^4 = f_L c_L = 1.$$

This yields the six elements of G_L

$$a_L,\ b_L,\ b_L^2 = c_L^2 = h_L,\ b_L^3 = e_L,\ c_L,\ c_L^3 = f_L.$$

We now multiply these elements on the left by $b_L, b_L^2 = h_L, b_L^3 = e_L$ and get the following elements

$$a_L,\ b_L,\ b_L^2 = c_L^2 = h_L,\ b_L^3 = e_L,\ c_L,\ c_L^3 = f_L,$$

$$b_L c_L = \begin{pmatrix} a & b & c & d & e & f & g & h \\ d & c & e & h & f & c & b & g \end{pmatrix} = d_L,\ b_L c_L^3 = \begin{pmatrix} a & b & c & d & e & f & g & h \\ g & f & b & a & c & e & h & d \end{pmatrix} = g_L,$$

$$b_L^2 c_L = \begin{pmatrix} a & b & c & d & e & f & g & h \\ f & d & a & e & g & h & b & c \end{pmatrix} = f_L,\ b_L^2 c_L^3 = \begin{pmatrix} a & b & c & d & e & f & g & h \\ c & g & h & b & d & a & e & f \end{pmatrix} = c_L,$$

$$b_L^3 c_L = \begin{pmatrix} a & b & c & d & e & f & g & h \\ g & f & b & a & c & e & h & d \end{pmatrix} = g_L,\ b_L^3 c_L^3 = \begin{pmatrix} a & b & c & d & e & f & g & h \\ d & c & e & h & f & b & a & g \end{pmatrix} = d_L$$

which is equal to G_L. Since G_L consists precisely of the elements of the form $b_L^i c_L^j$, we have G_L closed under composition iff G_L is closed under left translation by c_L. But

$$c_L b_L = \begin{pmatrix} a & b & c & d & e & f & g & h \\ g & f & b & a & c & e & h & d \end{pmatrix} = g_L = b_L c_L^3$$

which implies by induction that

$$c_L b_L^i = b_L^i c_L^{3^i}.$$

This is true in any monoid and the proof is left to the reader. Thus

$$c_L b_L^i c_L^j = b_L^i c_L^{j+3^i}.$$

Hence G_L is closed under composition and G is a group. The reader will verify that only 208 multiplications in G were required as opposed to the $1,372$ multiplications which would have been required to verify the associative law directly. □

Remark. The group G in the above example is the quaternion group and G_L is denoted by Q_8. The subscript 8 refers to the fact that it is a permutation group of degree 8, i.e., a subgroup of S_8. The reader is invited to construct the graph of this group using the generating set $S = \{b, c\}$. The reader is also invited to prove that Q_8 is not isomorphic to a subgroup of S_n if $n < 8$, which shows that the above graph is the simplest one whose group of symmetries is isomorphic to Q_8.

September 11, 1997
Revised September 28, 1997