Tutorial 3

Understanding the various interpretations of objects of study is the key to developing intuition in mathematics. You have seen the equivalence between partitions and equivalence relations, and how orbits of group actions give rise to them both. In Tutorial 1, you saw how every surjective function can seen as a composition of the collapse function on equivalence classes and bijections. In today's tutorial we give a new look at binary operations and Lagrange's theorem.

Binary operations

Recall that we describe the set of all functions from set A to set B as B^A., For example, we may have $f : \{1, \dots, n\} \to \mathbb{R}$ as a function in $\mathbb{R}^{\{1,\dots,n\}}$. [Can you see why the power set of S is often written as 2^S? Can you relate it to $\{1, 2\}^S$?]

Let S be a set, recall that binary operations are elements of

$$S^{S\times S}.$$

Problem 1. If $(S, \star)$ is a binary operation on S, then consider the map $F : S \longrightarrow S^S$ given by

$$s \mapsto f_s$$

where for $t \in S$, we have

$$f_s(t) = s \star t.$$

a) Show that $\star$ is a composition law if and only if $\forall s, t \in S : f_{s\star t} = f_s \circ f_t$.

b) Construct a bijection between binary operations on S and the set $(S^S)^S$.

Solution

a)

$$\begin{aligned}
& \star \text{ is a composition law} \\
\iff\ & \forall s, t, u \in S : s \star (t \star u) = (s \star t) \star u \\
\iff\ & \forall s, t, u \in S : s \star (f_t(u)) = f_{s\star t}(u) \\
\iff\ & \forall s, t, u \in S : f_s(f_t(u)) = f_{s\star t}(u) \\
\iff\ & \forall s, t, u \in S : (f_s \circ f_t)(u) = f_{s\star t}(u) \\
\iff\ & \forall s, t \in S : f_s \circ f_t = f_{s\star t}
\end{aligned}$$

b) The bijection is given by

$$\star \longrightarrow F$$

given in the question. We simply check that this is a bijection. This is easy to observe as the process of constructing F from $\star$ is a reversible process. Given F, we may construct $\star$ by

$$s \star t := F(s)(t).$$

Here $F(s) : S \to S$ is a function which we apply to $t \in S$. Think of this in terms of construction of a Cayley table by construction each row as a function associated to the name of the row.

This procedure clearly reverses the procedure given in the question.

Problem 2. For this problem, assume $\star$ is a composition law.

a) Show that if $(S, \star)$ contains some right identity e, then F is injective. [Hint: What does $f_s = f_t$ mean?]

b) Show that ~~if s has a right inverse under $\star$, then f_s is a bijection.~~ (This problem is incorrect. Credits: Hymn) Correction: if $(S, \star)$ also has the right inverse property, then for all $s \in S$, f_s is a bijection.

c) Show that if $(S, \star)$ has the right identity and right inverse axioms, then $F(S)$ is a subgroup of

$$\mathrm{Sym}(S) := \{f \in S^S : f \text{ is bijective}\}.$$

~~Conclude that S is a group. [Hint: If $F : X \to Y$ is injective, then $F : X \to F(X)$ is bijective.]~~ Correction: Show that S and $F(S)$ are isomorphic.

Solution

a) Observe that $f_s = f_t$ means $f_s(e) = f_t(e)$, so $s \star e = t \star e$ and hence $s = t$.

b) We note first that $f_s \circ f_{s^{-1}} = f_e$.

Suppose that for some $i \in S$, $f_i \circ f_i = f_i$. Then $f_e = f_i \circ f_{i^{-1}} = f_i \circ f_i \circ f_{i^{-1}} = f_i$. By a) we know $i = e$.

Now consider $f_{s^{-1} \star s}$. We have $f_{s^{-1} \star s} \circ f_{s^{-1} \star s} = f_{s^{-1} \star s}$, so by the above reasoning, we know $s^{-1} \star s = e$. Then $f_e = f_{s^{-1} \star s} = f_{s^{-1}} \circ f_s$.

It remains to show that f_e is the identity map. For any s, we have that $f_e(s) = e \star s = f_{s \star s^{-1}}(s) = f_s(e) = s$. So $f_e = \mathrm{id}$ and f_s has $f_{s^{-1}}$ as its two-sided inverse.

Remark. Note that the original version of this problem is wrong because:

- We do not immediately know that f_e is the identity map, and
- For infinite sets S, we need both $f_s \circ f_{s^{-1}}$ *and* $f_{s^{-1}} \circ f_s = \mathrm{id}$ to conclude that f_s is bijective.

c) From part b we know that $f_s \in \mathrm{Sym}(S)$. We check subgroup criterion. Since $f_{s\star t} = f_s \circ f_t$ we have that $F(S)$ is closed under composition. Furthermore, since s has a right inverse, say t, then $f_s \circ f_t = \mathrm{id}$ and thus f_t is the inverse of f_s sitting inside $F(S)$.

We proved in the process of b) that S is also a group [Why?]. So $F : S \to F(S)$ is a map between groups. From a), F is bijective. We also know from Problem 1a) that $F(st) = F(s) \circ F(t)$, so F is an isomorphism.

In other words, every composition law defining a group is equivalent to the composition of a certain set of functions on the same set.

Lagrange's Theorem

Problem 3. Given a group G and its subgroup H, define a group action by G on the left cosets G/H by

$$g' . gH = (g'g)H.$$

a) Show that this is indeed a group action.

b) Given $g \in G$, let S_g be the set of elements that send gH to itself. What is S_g?

c) Show that S_g is a subgroup of G in two ways:

   i) Checking the subgroup criterion.

   ii) Constructing an isomorphism with another group.

Remark. S_g is called the *stabilizer* of gH under the given group action.

Solution

a) For any g, $e . gH = (eg)H = gH$. For any g', g'', we have

$$g'' . (g' . gH) = g'' . (g'gH) = g''g'gH = (g''g') . gH.$$

So the identity and compatibility axioms hold.

b) For any $g' \in S_g$, we know that $g'gH = gH$, which is to say, for any $h \in H$, there is some $h' \in H$ such that $g'gh = gh'$. In other words, $g' = gh'h^{-1}g^{-1}$.

We define the set $gHg^{-1} = \{ghg^{-1} : h \in H\}$. Then $S_g \subset gHg^{-1}$. We wish to show that $gHg^{-1} \subset S_g$ as well. This is true as $ghg^{-1} . gH = (gh)H$, and $gh \in gH$ so $(gh)H = gH$ [since cosets are either equal or disjoint].

c) i) For any two elements ghg^{-1} and $gh'g^{-1} \in S_g$, we have

$$ghg^{-1}(gh'g^{-1})^{-1} = ghg^{-1}gh'g^{-1} = ghh'g^{-1},$$

which is in S_g.

ii) Consider the map $\varphi : H \to gHg^{-1}$ defined by $h \mapsto ghg^{-1}$. This map is a bijection because we can construct its inverse $\varphi^{-1} : gHg^{-1} \to H$, $ghg^{-1} \mapsto h$. It is an isomorphism as $\varphi(hh') = ghh'g^{-1} = ghg^{-1}(gh'g^{-1})^{-1} = \varphi(h)\varphi(h')$. So S_g must be a group.

Remark. S_g is also called the *conjugate subgroup* of H by g. We will relate these two names soon.