Structure, Isomorphism and Symmetry

We want to give a general definition of what is meant by a (mathematical) structure that will cover most of the structures that you will meet. It is in this setting that we will define what is meant by isomorphism and symmetry. We begin with the simplest type of structure, that of an internal structure on a set.

Definition 1 (Internal Structure). *An internal structure on a set A is any element of A or of any set that can be obtained from A by means of Cartesian products and the power set operation, e.g., $A \times A$, $\wp(A)$, $A \times \wp(A)$, $\wp((A \times A) \times A)$,... .*

Example 1 (An Element of A). $a \in A$

Example 2 (A Relation on A). $R \subseteq A \times A \implies R \in \wp(A \times A)$.

Example 3 (A Binary Operation on A). $p : A \times A \to A \implies p \in \wp((A \times A) \times A)$.

To define an external structure on a set A (e.g. a vector space structure) we introduce a second set K. The elements of K or of those sets which can be obtained from K and A by means of Cartesian products and the power set operation and which is not an internal structure on A are called K-structures on A.

Definition 2 (K-Structure). *A K-structure on a set A is any element of K or of those sets which can be obtained from K and A by means of Cartesian products and the power set operation and which is not an internal structure on A.*

Example 4 (External Operation on A). $m : K \times A \to A \implies m \in \wp((K \times A) \times A)$.

Example 5 (Distance Function or Metric on A). $d : A \times A \to \mathbb{R} \implies d \in \wp((A \times A) \times \mathbb{R})$. In addition one requires that (a) $d(x, y) \geq 0$ with equality iff $x = y$, (b) $d(x, y) = d(y, x)$, (c) $d(x, y) \leq d(x, z) + d(z, y)$ for any $z \in A$.

By a **structure** we mean either an internal or external structure.

Definition 3 (Structured Set). *A structured set is a pair (A, s), where s is a structure on the set A.*

Example 6 (Pointed Set). A points set is a pair (A, a), where a is an element of the set A.

Example 7 (Monad, Semi-group, Monoid, Group). A monad is a pair (A, p), where p is a binary operation on the set A. If p is associative, i.e., $p(x, p(y, z)) = p(p(x, y), z)$ for all $x, y, z \in A$, the monad (A, p) is called a semi-group. A semi-group is said to be a monoid if it has a neutral element, i.e., an element e such that $p(e, x) = p(x, e) = x$ for all $x \in A$. A neutral element is unique. A group is a monoid in which every element $x \in A$ has an inverse, i.e., an element $y \in A$ such that $p(x, y) = p(y, x) = e$, the neutral element. If such an inverse exists it is unique.

Example 8 (Metric Space). A metric space is a pair (A, d), where d is a metric on the set A.

Example 9 (K-set). If K is a set then a K-set is a pair (A, m), where $m : K \times A \to$ is an external operation on A.

Example 10 (Plane Geometry). A plane geometry is a pair $(A, \mathcal{L})$, where A is a set and $\mathcal{L} \in \wp^2(A) = \wp(\wp(A)$. The elements of A are called points and the elements of $\mathcal{L}$ are subsets of A called lines. In addition, the following axioms are to hold:

(PG1) Through any two distinct points there passes a unique line;

(PG2) Any line has a least two distinct points on it;

(PG3) There are at least three non-collinear points;

(PG4) Given a line and a point not on the line, there is a unique line passing through the given point and not meeting the given line.

If s is a structure on a set A and $f : A \to B$ is a mapping of A into the set B, we can obtain a structure on B by replacing each occurence of $a \in A$ in the structure s by $f(a)$. This structure is denoted by $f_*(s)$; it is called the image of s under f.

Example 11. If $s = (x, y) \in A \times A$ then $f(s) = (f(x), f(y)) \in B \times B$.

Example 12. If $s \in \wp(A\times A)$ then $f_*(s) = \{(f(x), f(y))|(x, y) \in s\} \in \wp(B\times B)$, e.g., if $A = \{0, 1, 2\}$, $B = \{a, b, c\}$, $f(0) = a, f(1) = f(2) = b$ and $s = \{(0, 1), (1, 2), (2, 1)\}$ then $f_*(s) = \{(a, b), (b, b)\}$.

Example 13. If $s \in \wp(A)$, so that $s \subseteq A$ then $f_*(s) = \{f(x)|x \in s\} = f(s)$.

Example 14. Let p, p' be a binary operations on A, A' respectively and let $p(x, y), p'(x', y')$ be respectively denoted by $x * y, x' *' y'$. Then

$$f_*(p) \subseteq p' \iff f(x * y) = f(x) *' f(y) \text{ for all } x, y \in A.$$

Indeed, if $f_*(p) = \{((f(x), f(y)), f(z))|((x, y), z) \in p\} \subseteq p'$ and $z = x * y$ then $((x, y), z) \in p$ so that $((f(x), f(y)), f(z)) \in p'$ which implies that $f(x * y) = f(x) *' f(y)$. Conversely, suppose that $f(x * y) = f(x) *' f(y)$ for all $x, y \in A$. If $((x', y'), z') \in f_*(p)$, there is $((x, y), z) \in p$ with $x' = f(x), y' = f(y), z' = f(z)$. Then $z' = f(z) = f(x * y) = f(x) *' f(y) = x' *' y'$ so that $((x', y'), z') \in p'$. Thus $f_*(p) \subseteq p'$. If f is surjective, we have $f_*(p) = p'$ iff $f_*(p) \subseteq p'$ since p' and $f_*(p')$ are two functions with the same domain.

Example 15. Let $m : K \times A$, $m' : K \times A \to A'$ be an external operations on the sets A, A' respectively. Then

$$f_*(m) = \{((c, f(x)), f(y))|((c, x), y) \in m\}$$

and $f_*(m) \subseteq m' \iff f(m(c, x)) = m'(c, f(x))$. The proof of this is left to the reader. If we let cx denote $m(c, x)$ and cx' denote $m'(c, x')$ then $f_*(m) \subseteq m' \iff f(cx) = cf(x)$ for all $x \in A$. If f is surjective then $f_*(m) = m' \iff f_*(m) \subseteq m'$.

The induced mapping f_* has the following important properties:

(1) If $f = 1_A$ is identity mapping of A then $f_*(s) = s$;

(2) If f is bijective and $t = f_*(s)$ then $s = (f^{-1})_*(t)$;

(3) If $f : A \to B$ and $g : B \to C$ then $(gf)_*(s) = g_*(f_*(s))$.

Definition 4 (Isomorphism). *Let s, t be structures on A, B respectively. Then (A, s) is said to be isomorphic to (B, t) if there is a bijective mapping $f : A \to B$ such that $t = f_*(s)$. The mapping f is called an isomorphism of the structured set (A, s) with the structured set (B, t). We denote this by $f : (A, s) \xrightarrow{\sim} (B, s)$. In this case, by abuse of language, we also say that s is isomorphic to t and that f is an isomorphism of s with t.*

By property (1) above, every structured set is isomorphic to itself, the isomorphism being the identity mapping. By property (2), if f is an isomorphism of (A, s) with (B, t) then f^{-1} is an isomorphism of (B, t) with (A, s). By property (3), if f is an isomorphism of (A, s) with (B, t) and g is an isomorphism of (B, t) with (C, u) then gf is an isomorphism of (A, s) with (C, u). In other words, like equality, isomorphism is reflexive, symmetric and transitive.

Example 16. Let $s : A \to A$ and let $f : A \to B$ be a bijection. Then

$$t = f_*(s) = \{(f(x), f(y)) | (x, y) \in s\}$$

is a mapping of A into A. We have $t(f(x)) = f(s(x))$ for any $x \in A$. Hence $tf = fs$ and $t = fsf^{-1}$.

Example 17. Let $(A, *)$ and $(A', *')$ be monads. A bijection $f : A \to A'$ is an isomorphism of $(A, *)$ with $(A', *')$ iff $f(x * y) = f(x) *' f(y)$ for all $x, y \in A$.

Definition 5 (Homomorphism of Monads). *A mapping $f : A \to A'$ is said to be a homomorphism of the monad $(A, *)$ to the monad $(A', *')$ if $f(x * y) = f(x) *' f(y)$ for all $x, y \in A$. We denote this by $f : (A, *) \to (A, *')$.*

Definition 6 (Homomorphism of K-sets). *A mapping $f : A \to A'$ is said to be a homomorphism of the K-set (A, m) to the K-set A' if $f(m(c, x)) = m'(c, f(x))$ for all $x \in A$. We denote this by $f : (A, m) \to (A', m')$.*

A homomorphism of monads or K-sets is an isomorphism iff it is bijective.

Theorem 1. *Let $f : (A, *) \to (A', *')$ be a surjective homomorphism of monads. Then*

(1) If e is a neutral element for $*$ then $f(e)$ is a neutral element for $*'$;

(2) If $*$ is associative then $*'$ is associative;

(3) If $*$ is commutative then $*'$ is commutative;

(4) If $(A, *)$ is a monoid and $x \in A$ is invertible with inverse y then $f(x) \in A'$ is invertible with inverse $f(y)$.

If $f : (A, *) \to (A', *')$ is a homomorphism of monads and $(A, *)$, $(A', *')$ have respectively the neutral elements e, e', it is not always the case that $f(e) = e'$. For example, $\mathbb{N}$ under ordinary multiplication is a monoid with neutral element 1 while $\mathbb{N} \times \mathbb{N}$ is a monoid under the operation $(a, b)(c, d) = (ac, bd)$ with neutral element $(1, 1)$. The mapping $f : \mathbb{N} \to \mathbb{N} \times \mathbb{N}$ defined by $f(n) = (n, 0)$ is a homomorphism of monads but $f(1) \neq (1, 1)$. However, we have

Theorem 2. *If $f : (A, *) \to (A', *')$ is a homomorphism of monads with $(A', *')$ a group and $(A, *)$ a monoid with neutral element e then $f(e) \in A'$ is the neutral element for $*'$.*

Proof. We have $f(e) = f(e * e) = f(e) * f(e)$. If we multiply both sides by the inverse of $f(e)$, we get $e' = f(e)$, where $e' \in A'$ is the neutral element for $*'$. □

If we want homomorphisms to send neutral elements to neutral elements in general, we have to make them part of the structure. We there modify our definition of a monoid by including the neutral element as part of the structure.

Definition 7 (Monoid). *A monoid is a pair $(A, (*, e))$, where $(A, *)$ is a semi-group and $e \in A$ is a neutral element for $*$.*

Definition 8 (Homomorphism of Monoids). *A homomorphism of the monoid $(A, *, e)$ to the monoid $(A', *', e')$ is a homomorphism of $(A, *)$ to $(A', *')$ such that $f(e) = e'$.*

Since we want a group to be a monoid we also include the neutral element of a group as part of its structure.

Definition 9 (Group). *A group is a monoid in which every element is invertible.*

Definition 10 (Homomorphism of Groups). *A homomorphism of groups is the same as a homomorphism of monoids.*

Since homomorphisms of groups preserve neutral elements, $f : (G, *, e) \to (G', *', e')$ is a homomorphism of groups iff $f(x * y) = f(x) *' f(y)$ for all $x, y \in G$.

Definition 11 (Symmetry). *If s is a structure on a set A, a symmetry of s or of (A, s) is a bijection $f : A \to A$ such that $f_*(s) = s$.*

Thus a symmetry of a stuctured set is an isomorphism of the structured set with itself. We let Sym(A, s) denote the symmetries of the structured set (A, s). Then $S_A = \mathrm{Sym}(A, \emptyset)$ is the set of all bijections of A with itself. Such bijections are also called **permutations** of A. The set Γ of symmetries of a set A has the following properties:

$$
\begin{aligned}
&(S1) \quad \Gamma \subseteq S_A;\\
&(S2) \quad 1_A \in \Gamma;\\
&(S3) \quad f, g \in \Gamma \implies fg \in \Gamma;\\
&(S4) \quad f \in \Gamma \implies f^{-1} \in \Gamma.
\end{aligned}
$$

These properties are equivalent to

$$
\begin{aligned}
&(S1') \quad \Gamma \text{ is a non-empty subset of } S_A;\\
&(S2') \quad f, g \in \Gamma \implies fg^{-1} \in \Gamma.
\end{aligned}
$$

Definition 12 (Permutation Group). *A permutation group on the set A is any subset Γ of S_A satisfying $(S1) - (S4)$ or, equivalently, $(S1'), (S2')$.*

The permutation group Sym(A, s) is a group under composition of mappings. The set S_A is a permutation group on A called the **symmetric group** on A. If $A = \{1, 2, \ldots, n\}$, we denote S_A by S_n. If $f \in S_n$, we denote it by

$$
\begin{pmatrix} 1 & 2 & \cdots & i & \cdots & n \\ a_1 & a_2 & \cdots & a_i & \cdots & a_n \end{pmatrix},
$$

where $a_i = f(i)$. The cardinality (number of elements) of a set A is denoted by $|A|$. We have $|S_n| = n!$. The cardinality of a group or monoid is called its **order**.

Problem 1. *Find the group of symmetries of the structured set (A, s), where $A = \{1, 2, 3, 4, 5, 6\}$ and*

$$
s = \{\{1, 2\}, \{1, 4\}, \{2, 3\}, \{3, 6\}, \{2, 5\}, \{4, 5\}, \{5, 6\}\}.
$$

Find a multiplication table for this group.

Solution. The elements $2, 5$ are distinguished in that they are the only two elements of A that belong to three distinct members of s. Hence, if $f \in \mathrm{Sym}(A, s)$, we must have $f(\{2, 5\}) = \{2, 5\}$.

Case 1: If $f(2) = 2$ we must have $f(5) = 5$. Then f permutes the sets $\{1, 2\}$, $\{2, 3\}$ and the sets$\{4, 5\}$, $\{5, 6\}$. If $f \neq 1_A$, we must have $f(1) = 3$, $f(3) = 1$, $f(4) = 6$, $f(6) = 4$ since $f(1) = 1$ implies $f(4) = 4$ as $f(\{1, 4\}) = \{1, 4\}$ and $f(4) = 4$ implies $f(\{4, 5\}) = \{4, 5\}$.

Case 2: If $f(2) = 5$ we must have $f(5) = 2$. Then $f(\{1, 2\}) = \{4, 5\}$ or $\{5, 6\}$. In the first case we have $f(1) = 4$ and $f(4) = 1$ since otherwise $f(4) = 3$ and we would have $f(\{1, 4\}) = \{3, 4\} \in s$

which is not the case. Then $f(3) = 6$ and $f(6) = 3$. In the second case, $f(1) = 6$ and so $f(4) = 3$ since $f(\{1,4\}) = \{3,6\}$ or $\{5,6\}$ and $f(\{1,4\}) = \{5,6\}$ is not possible as that would imply that $f(4) = 5$. Then $f(3) = 4$ and $f(4) = 3$.

Thus Sym(A, s) consists of the permutations

$$1_A, \quad \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 1 & 6 & 5 & 4 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 5 & 6 & 1 & 2 & 3 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 4 & 3 & 2 & 1 \end{pmatrix}.$$

If e, a, b, c are respectively the above permutations the multiplication table of Sym(A, s) is

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

□

Remark. The definition of structure can be extended by replacing A by a sequence of sets $(A_1, A_1, \ldots)$ or, in the case of a K-structure, K by a sequence of sets $(K_1, K_2, \ldots)$. To define isomorphisms, we replace f by a sequence of mappings $(f_1, f_2, \ldots)$ with $f_i : A_i \to B_i$. The details are left to the reader.

September 9, 1997