Isomorphism

Definition. Let G and H be groups. A function $f: G \to H$ is called an *isomorphism* if it is one-to-one and onto, and $f(xy) = f(x)f(y)$ for all x, $y \in G$. The groups G and H are said to be *isomorphic* if there is an isomorphism from G to H.

In other words, an isomorphism is a homomorphism that is one-to-one and onto.

The definition says that G and H are isomorphic if there is a one-to-one correspondence between the elements of G and the elements of H that preserves multiplication, in the sense that if x, y, z are elements of G and x', y', z' the corresponding elements of H, then $xy = z$ if and only if $x'y' = z'$. We can regard two isomorphic groups as being two copies of the same abstract group: the multiplication is the same, but the elements have been given different names. If a group is finite then its multiplicative structure can be described by means of a multiplication table; if G and H are isomorphic then replacing each element of G by the corresponding element of H will transform a multiplication table for G into a multiplication table for H. Furthermore, any one-to-one correspondence that transforms a multiplication table for G into a multiplication table for H is necessarily an isomorphism.

For example, let $G = \mathrm{Sym}(2)$, the group of all permutations of $\{1, 2\}$. Then G has just two elements, namely, the identity permutation id, and the transposition $(1, 2)$. Let $H = \{1, -1\}$, a subgroup of the group of all nonzero real numbers under multiplication. From the multiplication tables

	id	$(1,2)$
id	id	$(1,2)$
$(1,2)$	$(1,2)$	id

	1	-1
1	1	-1
-1	-1	1

it is clear that there is a multiplication-preserving one-to-one correspondence between the elements of G and the elements of H: the identity permutation corresponds to 1, and $(1, 2)$ corresponds to -1.

For another example, let $G = \mathrm{Sym}(3) = \{\mathrm{id}, (1,2), (1,3), (2,3), (1,2,3), (1,3,2)\}$ and let H be the following set of matrices:

$$\left\{ \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \right\}.$$

Each of these matrices has the property that in each row exactly one of the entries is 1 and the other entries are 0, and in each column exactly one of the entries is 1 and the other entries are 0. Such matrices are known as *permutation matrices*, since they can be associated with permutations in a natural way. Specifically, given a permutation matrix P we can define a permutation σ as follows: for each number i, the permutation σ takes i to the unique number j such that the (i, j) entry of P is 1. Thus, for example, the permutation matrix

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

has its nonzero entries in the $(1, 2)$, $(2, 3)$ and $(3, 1)$ positions, and so the associated

permutation σ is defined by $1^\sigma = 2$, $2^\sigma = 3$ and $3^\sigma = 1$. In other words,

$$\sigma = (1, 2, 3).$$

This rule defines a one-to-one correspondence between G and H (which in fact is compatible with the order in which we listed the elements of G and the elements of H above). Note that $n \times n$ permutation matrices correspond to permutations in $\mathrm{Sym}(n)$ in just the same way as 3×3 permutation matrices correspoond to permutations in $\mathrm{Sym}(3)$.

For each permutation $\sigma \in \mathrm{Sym}(n)$, let $P(\sigma)$ be the corresponding $n \times n$ permutation matrix. For any matrix A with n columns, the matrix $AP(\sigma)$ is obtained by permuting the columns of A according to σ, in the sense that the i-th column of A becomes the i^σ-th column of $AP(\sigma)$. Thus, for example

$$\begin{pmatrix} a & b & c \\ d & e & f \end{pmatrix} \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} = \begin{pmatrix} c & a & b \\ f & d & e \end{pmatrix};$$

postmultiplying by the permutation matrix corresponding to $(1, 2, 3)$ moved column 1 to column 2, column 2 to column 3, and column 3 to column 1. Now in general, if σ, $\tau \in \mathrm{Sym}(n)$, then

$$P(\sigma)P(\tau) = (I\,P(\sigma))P(\tau)$$

is the matrix obtained from I by applying two column permutations, first σ, then τ. But by the way multiplication of permutations is defined, this is the same as applying the product $\sigma\tau$ to the columns of I. So

$$P(\sigma)P(\tau) = (I\,P(\sigma))P(\tau) = I\,P(\sigma\tau) = P(\sigma\tau). \tag{1}$$

We conclude that our one-to-one correspondence between $\mathrm{Sym}(n)$ and the set of $n \times n$ permutation matrices preserves multiplication, and so it follows that the permutation matrices form a group isomorphic to $\mathrm{Sym}(n)$. The student should check Equation (1) by explicit calculation in at least some cases. For example,

$$P((1,2))P((2,3)) = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$$
$$= \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} = P((1,3,2)) = P((1,2)(2,3)).$$

Homomorphisms and quotients

We return now to an investigation of homomorphisms. To illustrate the ideas we shall focus on a particular homomorphism, namely, the homomorphism from $\mathrm{Sym}(4)$ to $\mathrm{Sym}(3)$ that was discussed in Tutorial 10 and Computer Tutorial 10. Let us first go through the of this homomorphism construction again.

The homomomorphism from Sym(4) to Sym(3)

Let x_1, x_2, x_3, x_4 be four variables and define three more quantities y_1, y_2, y_3 in terms of the x_i's as follows:

$$y_1 = x_1x_4 + x_2x_3$$
$$y_2 = x_2x_4 + x_1x_3$$
$$y_3 = x_3x_4 + x_1x_2.$$

If τ is any permutation of $\{1,2,3,4\}$ then one can apply τ to any expresssion in the variables x_1, x_2, x_3, x_4 and get a new expression. The process is simply to replace each x_i, wherever it occurs in the expression, by x_j, where τ takes i to j. For example, if τ is the permutation that takes 1 to 3, 3 to 4, 4 to 1 and fixes 2—that is, $\tau = (1,3,4)$—then applying τ to the expression $x_1^3x_3 + x_2x_4x_1 - x_4$ gives the expression $x_3^3x_4 + x_2x_1x_3 - x_1$.

It is easy to see that applying any permutation τ of $\{1,2,3,4\}$ to y_1, y_2 and y_3 will give y_1, y_2 and y_3 in some order. For example, applying $(1,3,4)$ to $y_1 = x_1x_4+x_2x_3$ gives $x_3x_1+x_2x_4$, which equals y_2. Applying $(1,3,4)$ to $y_2 = x_2x_4+x_1x_3$ gives $x_2x_1+x_3x_4 = y_3$, and applying $(1,3,4)$ to $y_3 = x_3x_4+x_1x_2$ gives $x_4x_1+x_3x_2 = y_1$. The point is that there are only three possible ways to split a four-element set into two two-element subsets; so any expression of the form $x_ix_j+x_kx_l$ with $\{i,j,k,l\} = \{1,2,3,4\}$ must equal y_1, y_2 or y_3.

So permuting x_1, x_2, x_3 and x_4 permutes y_1, y_2 and y_3. That is to say, if τ is any permutation of $\{1,2,3,4\}$ then there is a permutation $\phi(\tau)$ of $\{1,2,3\}$ such that replacing x_i by x_{i^τ} (for all $i \in \{1,2,3,4\}$) converts y_j into $y_{j^{\phi(\tau)}}$ (for all $j \in \{1,2,3\}$). We showed above that $x_1 \to x_3 \to x_4 \to x_1$ and $x_2 \to x_2$ gives rise to $y_1 \to y_2 \to y_3 \to y_1$. That is, if $\tau = (1,3,4)$ then $\phi(\tau) = (1,2,3)$.

Let us calculate $\phi(\tau)$ for another couple of values of τ. If τ is the 4-cycle $(1,4,2,3)$, so that

$$x_{1^\tau} = x_4, \quad x_{4^\tau} = x_2, \quad x_{2^\tau} = x_3, \quad x_{3^\tau} = x_1,$$

then we find that

$$y_{1^{\phi(\tau)}} = x_{1^\tau}x_{4^\tau} + x_{2^\tau}x_{3^\tau} = x_4x_2 + x_3x_1 = y_2,$$
$$y_{2^{\phi(\tau)}} = x_{2^\tau}x_{4^\tau} + x_{1^\tau}x_{3^\tau} = x_3x_2 + x_4x_1 = y_1,$$
$$y_{3^{\phi(\tau)}} = x_{3^\tau}x_{4^\tau} + x_{1^\tau}x_{2^\tau} = x_1x_2 + x_4x_3 = y_3,$$

whence $\phi(\tau)$ is the transposition $(1,2)$. Similarly, if τ is the 3-cycle $(2,3,4)$, so that

$$x_{1^\tau} = x_1, \quad x_{2^\tau} = x_3, \quad x_{3^\tau} = x_4, \quad x_{4^\tau} = x_2,$$

then we find that

$$y_{1^{\phi(\tau)}} = x_{1^\tau}x_{4^\tau} + x_{2^\tau}x_{3^\tau} = x_1x_2 + x_3x_4 = y_3,$$
$$y_{2^{\phi(\tau)}} = x_{2^\tau}x_{4^\tau} + x_{1^\tau}x_{3^\tau} = x_3x_2 + x_1x_4 = y_1,$$
$$y_{3^{\phi(\tau)}} = x_{3^\tau}x_{4^\tau} + x_{1^\tau}x_{2^\tau} = x_4x_2 + x_1x_3 = y_2,$$

So $\phi((2,3,4)) = (1,3,2)$. As a final example, observe that if $\tau = (1,2)(3,4)$ then applying τ takes $y_1 \to x_2x_3 + x_1x_4 = y_1$, takes $y_2 \to x_1x_3 + x_2x_4 = y_2$ and takes $y_3 \to x_4x_3 + x_2x_1 = y_3$. So $\phi((1,2)(3,4))$ is the identity permutation of $\{1,2,3\}$.

The complete list of values of ϕ is as follows:

$$\begin{array}{rrr}
\phi(\mathrm{id}) = \mathrm{id} & \phi((1,2,3)) = (1,2,3) & \phi((1,3,2)) = (1,3,2) \\
\phi((1,2)(3,4)) = \mathrm{id} & \phi((2,4,3)) = (1,2,3) & \phi((1,4,3)) = (1,3,2) \\
\phi((1,3)(2,4)) = \mathrm{id} & \phi((1,4,2)) = (1,2,3) & \phi((2,3,4)) = (1,3,2) \\
\phi((1,4)(2,3)) = \mathrm{id} & \phi((1,3,4)) = (1,2,3) & \phi((1,2,4)) = (1,3,2)
\end{array}$$

$$\begin{array}{rrr}
\phi((1,2)) = (1,2) & \phi((1,3)) = (1,3) & \phi((2,3)) = (2,3) \\
\phi((3,4)) = (1,2) & \phi((1,4,3,2)) = (1,3) & \phi((1,2,4,3)) = (2,3) \\
\phi((1,4,2,3)) = (1,2) & \phi((2,4)) = (1,3) & \phi((1,3,4,2)) = (2,3) \\
\phi((1,3,2,4)) = (1,2) & \phi((1,2,3,4)) = (1,3) & \phi((1,4)) = (2,3)
\end{array}$$

The student should check at least a few of these.

To show that the map ϕ is a homomorphism from Sym(4) to Sym(3) we must show that

$$\phi(\sigma\tau) = \phi(\sigma)\phi(\tau)$$

for all σ, τ in Sym(4). This proof was not done in lectures, and is included here only for completeness.

It is helpful to make use of the notation and terminology we used in the notes for Week 5: given a polynomial f in the variables x_1, x_2, x_3, x_4 and a permutation σ of $\{1,2,3,4\}$, let f^σ be the polynomial defined by

$$f^\sigma(x_1, x_2, x_3, x_4) = f(x_{1^\sigma}, x_{2^\sigma}, x_{3^\sigma}, x_{4^\sigma}).$$

We showed in Week 5 that with this definition the equation $f^{\sigma\tau} = (f^\sigma)^\tau$ holds for all σ, $\tau \in \mathrm{Sym}(4)$ and all polynomials f.

Since y_1, y_2 and y_3 are polynomials in the x_i's, we can employ the notation above. We find that the rule for determining $\phi(\sigma)$, for $\sigma \in \mathrm{Sym}(4)$, is as follows: for i, $j \in \{1,2,3\}$,

$$i^{\phi(\sigma)} = j \quad \text{if and only if} \quad y_i^\sigma = y_j.$$

So if σ, $\tau \in \mathrm{Sym}(4)$ and $i \in \{1,2,3\}$ then, writing $j = i^\sigma$, we find that

$$i^{\phi(\sigma)\phi(\tau)} = (i^{\phi(\sigma)})^{\phi(\tau)} = j^{\phi(\tau)} = k,$$

where k is such that $y_j^\tau = y_k$. But $y_j = y_i^\sigma$; so

$$y_k = y_j^\tau = (y_i^\sigma)^\tau = y_i^{\sigma\tau},$$

and hence $i^{\phi(\sigma\tau)} = k$. So we conclude that

$$i^{\phi(\sigma)\phi(\tau)} = i^{\phi(\sigma\tau)}$$

for all $i \in \{1,2,3\}$, which shows that $\phi(\sigma\tau) = \phi(\sigma)\phi(\tau)$, as required.

The above proof will not be considered examinable, since it was not done in lectures. However, from the right intuitive viewpoint it can almost be regarded as obvious.

Permuting x_1, x_2, x_3, x_4 via the permutation σ permutes y_1, y_2, y_3 via $\phi(\sigma)$. So permuting x_1, x_2, x_3, x_4 via $\sigma\tau$ permutes y_1, y_2, y_3 via $\phi(\sigma\tau)$. But applying the product $\sigma\tau$ to x_1, x_2, x_3, x_4 means first applying σ and then applying τ, and the effect of this on y_1, y_2, y_3 is to first apply $\phi(\sigma)$ and then apply $\phi(\tau)$. So $\phi(\sigma\tau)$ equals the product $\phi(\sigma)\phi(\tau)$.

The equivalence relation obtained from a function

We shall continue discussing the above example shortly, but let us first investigate a much more general situation. Let $f\colon A \to B$ be any function at all. Recall that the sets A and B are called the *domain* and *codomain* of f. Since we have imposed no restrictions at all on f, the sets A and B are also completely arbitrary. Recall that the *image* (or *range*) of f is the set

$$\operatorname{im} f = \{\, f(a) \mid a \in A \,\},$$

a subset of B.

If f were a one-to-one function then for each $b \in \operatorname{im} f$ there would be a unique $a \in A$ with $f(a) = b$. In the general situation, though, for each $b \in \operatorname{im} f$ there could be many different $a \in A$ with $f(a) = b$. Each $a \in A$ gives rise to some $b \in \operatorname{im} f$, defined by $b = f(a)$, but for each $b \in \operatorname{im} f$ the subset of A consisting of those a with $f(a) = b$ could have any number of elements. The subsets of A obtained in this way, for the various elements $b \in \operatorname{im} f$, partition A up into non-overlapping pieces. The function f takes a constant value on each piece, and there is one piece for each value that arises.

This idea can also be described using the language of equivalence relations: we can regard elements a, $a' \in A$ as equivalent if $f(a) = f(a')$, and then the "pieces" referred to above are just the equivalence classes. More formally, we define a relation $\equiv_f$ on the set A by the rule that $a \equiv_f a'$ if and only if $f(a) = f(a')$; it is trivial to check that this relation is reflexive, symmetric and transitive, and hence partitions A into equivalence classes.

In the case of the function ϕ from Sym(4) to Sym(3) constructed above, we see from the table of values taken by ϕ that there are six equivalence classes, each with four elements. The sets are

$$\begin{aligned}
S_1 &= \{\mathrm{id}, (1,2)(3,4),\ (1,3)(2,4),\ (1,4)(2,3)\},\\
S_2 &= \{(1,2),\ (3,4),\ (1,4,2,3),\ (1,3,2,4)\},\\
S_3 &= \{(2,3),\ (1,2,4,3),\ (1,3,4,2),\ (1,4)\},\\
S_4 &= \{(1,3),\ (1,4,3,2),\ (2,4),\ (1,2,3,4)\},\\
S_5 &= \{(1,2,3),\ (2,4,3),\ (1,4,2),\ (1,3,4)\},\\
S_6 &= \{(1,3,2),\ (1,4,3),\ (2,3,4),\ (1,2,4)\}.
\end{aligned}$$

Elements σ, $\tau \in \mathrm{Sym}(4)$ lie in the same set S_i if $\sigma \equiv_\phi \tau$, which by definition means $\phi(\sigma) = \phi(\tau)$. The six sets S_i correspond to the six elements of $\operatorname{im}\phi = \mathrm{Sym}(3)$, as follows:

$$\begin{aligned}
S_1 &\leftrightarrow \mathrm{id}, & S_4 &\leftrightarrow (1,3),\\
S_2 &\leftrightarrow (1,2), & S_5 &\leftrightarrow (1,2,3),\\
S_3 &\leftrightarrow (2,3), & S_6 &\leftrightarrow (1,3,2).
\end{aligned} \tag{2}$$

Every element τ in S_1 satisfies $\phi(\tau) = \mathrm{id}$, every τ in S_2 satisfies $\phi(\tau) = (1,2)$, and so on.

Defining multiplication of equivalence classes

As we have pointed out, one-to-one correspondences like the one above can be obtained for any function at all. However, the function ϕ in the example above is a homomorphism, and this gives us some additional information. Specifically, it tells us that the one-to-one correspondence in the table (2) above respects the multiplication in the groups Sym(4) and Sym(3), in the following sense. Let α, $\beta \in \mathrm{Sym}(3)$ and suppose that $S_i \leftrightarrow \alpha$ and $S_j \leftrightarrow \beta$ in table (2). Let S_k be the set that corresponds to the product $\alpha\beta$. Then for any σ in S_i and τ in S_k the product $\sigma\tau$ will lie in S_k.

$$\sigma \in S_i \leftrightarrow \alpha$$
$$\tau \in S_j \leftrightarrow \beta$$
$$\sigma\tau \in S_k \leftrightarrow \alpha\beta$$

To put it another way, if σ, $\tau \in \mathrm{Sym}(4)$ lie in the sets that correspond to $\alpha\,\beta \in \mathrm{Sym}(3)$ then the product $\sigma\tau$ lies in the set corresponding to the product $\alpha\beta$.

For example, let $\alpha = (1,3,2)$ and $\beta = (2,3)$. Then $\alpha\beta = (1,3,2)(2,3) = (1,2)$. So the product of any σ in the set corresponding to $(1,3,2)$ by any τ in the set corresponding to $(2,3)$ should lie in the set corresponding to $(1,2)$. That is, if $\sigma \in S_6$ and $\tau \in S_3$ then $\sigma\tau \in S_2$. There are four possible choices for each of σ and τ, and it is straightforward to evaluate all sixteen possible products to confirm the assertion. The following table, which the student should check, gives all the sixteen products.

	(2,3)	(1,2,4,3)	(1,3,4,2)	(1,4)
(1,3,2)	(1,2)	(3,4)	(1,4,2,3)	(1,3,2,4)
(1,4,3)	(1,4,2,3)	(1,3,2,4)	(1,2)	(3,4)
(2,3,4)	(3,4)	(1,2)	(1,3,2,4)	(1,4,2,3)
(1,2,4)	(1,3,2,4)	(1,4,2,3)	(3,4)	(1,2)

In all cases the product is indeed in S_2.

It is not hard to see why this works. If $\sigma \in S_6$ then $\phi(\sigma) = (1,3,2)$ (because this is how S_6 was defined). Similarly, $\tau \in S_3$ means $\phi(\tau) = (2,3)$. Now, since ϕ is a homomorphism, if $\sigma \in S_6$ and $\tau \in S_3$ then

$$\phi(\sigma\tau) = \phi(\sigma)\phi(\tau) = (1,3,2)(2,3) = (1,2),$$

and therefore $\sigma\tau \in S_2$.

Since the product of any element of S_6 by any element of S_3 gives an element of S_2, it is reasonable to define the product of the sets S_6 and S_3 to be the set S_2. More generally, we define S_iS_j to be S_k if $\sigma\tau \in S_k$ whenever $\sigma \in S_i$ and $\tau \in S_j$. In this way we obtain an operation on the set $\{S_1, S_2, S_3, S_4, S_5, S_6\}$. From the discussion above we see that if $S_i \leftrightarrow \alpha$ and $S_j \leftrightarrow \beta$ then $S_iS_j \leftrightarrow \alpha\beta$.

This multiplication operation makes the set $\{S_1, S_2, S_3, S_4, S_5, S_6\}$ into a group: it is an example of what is called a *quotient group*. In general, if one can define an equivalence relation on the elements of a group G in such a way that gh is equivalent to $g'h'$ whenever g is equivalent to g' and h is equivalent to h', then multiplication of equivalence classes can be defined in the same way as we defined it for the set $\{S_1, S_2, S_3, S_4, S_5, S_6\}$ above. That is, if X and Y are equivalence classes then XY is defined to be the equivalence class

containing all the products xy, where $x \in X$ and $y \in Y$. This operation makes the set of equivalence classes into a group, known as a quotient group of G.

In fact it is clear from our discussion above that the quotient group of Sym(4) formed by the sets S_1, S_2, S_3, S_4, S_5 and S_6 is isomorphic to Sym(3). Table (2) above gives a one-to-one correspondence between the sets S_i and the elements of Sym(3), and this correspondence preserves multiplication because of the way we defined multiplication for the sets S_i.

Exactly the same procedure works for any group homomorphism $\phi\colon G \to H$. We can define an equivalence relation $\equiv_\phi$ on G by $g \equiv_\phi g'$ if and only if $\phi(g) = \phi(g')$. The equivalence classes then form a quotient group of the group G. Furthermore, there is a one-to-one correspondence between the set of equivalence classes and the image of ϕ (which is a subgroup of H). This one-to-one correspondence is an isomorphism.

The equivalence classes are the cosets of the kernel

We continue with the hypotheses of the preceding paragraph: $\phi\colon G \to H$ is a group homomorphism, and $\equiv_\phi$ is the equivalence relation on G such that $g \equiv_\phi g'$ if and only if $\phi(g) = \phi(g')$. Let e_G, e_H be the identity elements of G and H.

We proved last week that $\phi(e_G) = e_H$; so if $g \in G$ then $g \equiv_\phi e_G$ if and only if $\phi(g) = e_H$. The $\equiv_\phi$ equivalence class containing ϕ is therefore the set

$$K = \{\, g \in G \mid \phi(g) = e_H \}.$$

We have proved that this set is a subgroup of G.

Definition. The set $K = \{\, g \in G \mid \phi(g) = e_H\}$ is called the *kernel* of the homomorphism ϕ.

Suppose now that g, $g' \in G$ and $g' \equiv_\phi g$. Then $\phi(g') = \phi(g)$. Put $x = g'g^{-1}$, so that

$$xg = (g'g^{-1})g = g'(g^{-1}g) = g'e_G = g'.$$

Since ϕ is a homomorphism,

$$\phi(x) = \phi(g'g^{-1}) = \phi(g')\phi(g^{-1}) = \phi(g')\phi(g)^{-1} = \phi(g)\phi(g)^{-1} = e_H$$

since $\phi(g') = \phi(g)$. It follows that x is in K, the kernel of ϕ. So $g' = xg \in Kg$. We conclude that every $g' \in G$ with $g' \equiv_\phi g$ lies in the coset Kg. Conversely, every element of the coset Kg has the form xg for some $x \in K$, and then we have that

$$\phi(xg) = \phi(x)\phi(g) = e_H\phi(g) = \phi(g).$$

So every element of the coset Kg is equivalent to g. The conclusion is that the equivalence classes for the relation $\equiv_\phi$ are precisely the cosets of K, the kernel of ϕ.

In the example we considered above, the kernel K is

$$\{\, \sigma \in \mathrm{Sym}(4) \mid \phi(\sigma) = \mathrm{id}\,\} = \{\mathrm{id}, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}$$

(which is just the same as the set S_1). The right cosets of K in Sym(4) are precisely the sets S_1, S_2, S_3, S_4, S_5 and S_6. Indeed, it is easily verified that

$$\begin{aligned} S_1 &= K\mathrm{id}, & S_4 &= K(1,3), \\ S_2 &= K(1,2), & S_5 &= K(1,2,3), \\ S_3 &= K(2,3), & S_6 &= K(1,3,2). \end{aligned}$$