Chapter 15. Homomorphisms

There are several classes of homomorphisms that arise naturally in the study of permutation groups. They are very useful in divide-and-conquer techniques for reducing a problem in a group G to smaller, less complicated groups. The aim of this chapter is to present methods of effectively computing with these naturally arising homomorphisms.

Homomorphisms

A *homomorphism* $\phi : G \rightarrow H$ between groups G and H is a map which commutes with the operations of multiplication and inversion, and which maps the identity element of G to the identity element of H. The group G is called the *domain* and the group H is called the *codomain*. For all elements $g_1, g_2 \in G$, we have

$$\begin{aligned} \phi(g_1 \times g_2) &= \phi(g_1) \times \phi(g_2) \\ \phi(g_1^{-1}) &= \phi(g_1)^{-1} \end{aligned}$$

Hence, the homomorphism ϕ maps subgroups of G to subgroups of $\phi(G)$, and maps normal subgroups of G to normal subgroups of $\phi(G)$. The *image*, *im*ϕ, of the homomorphism ϕ is the subgroup $\phi(G) = \{ \ \phi(g) \mid g \in G \ \}$ of H. The *kernel*, *ker*ϕ, of the homomorphism ϕ is the subgroup $\{ \ g \in G \mid \phi(g) = \textit{identity} \text{ of } H \ \}$ of G. Let T be a subset of elements of *im*ϕ. The *preimage*, $\phi^{-1}(T)$, of T is the set of all elements of G which map to an element of T. That is,

$$\phi^{-1}(T) = \{ g \in G \mid \phi(g) \in T \}$$

The preimage of a subgroup of *im*ϕ is a subgroup of G, and the preimage of a normal subgroup of *im*ϕ is a normal subgroup of G. The kernel of ϕ is the preimage of the identity element of H.

The kernel of ϕ is a normal subgroup N of G and the image of ϕ is isomorphic to the quotient group G/N. Every normal subgroup N of G give rise to a natural homomorphism

$$\begin{aligned} \phi : G &\rightarrow G/N \\ g &\mapsto g \times N \end{aligned}$$

where an element is mapped to the coset of N which contains it.

A homomorphism may be defined in two ways. The first way is to give a formula or procedure which explicitly defines the image of each element of the group. For example, we can define the homomorphism ϕ between the symmetric group G of degree 4 and the cyclic group $H = < \ z \ >$ of order 2 by

$$\begin{aligned} \phi : G &\mapsto H \\ g &\mapsto z^{parity(g)} \end{aligned}$$

where the parity of a permutation g is 0 if g can be expressed as a product of an even number of transpositions, and is 1 otherwise. The second way is to define the image of each generator

s of G and allow the image of an element to be defined by expressing the element as a word in the generators. So if

$$g = s_1^{\varepsilon_1} \times \cdots \times s_t^{\varepsilon_t}$$

then the image is

$$\phi(g) = \phi(s_1)^{\varepsilon_1} \times \cdots \times \phi(s_t)^{\varepsilon_t}$$

So the homomorphism between the symmetric group of degree 4 and the cyclic group of order 2 can be defined by

$$\begin{array}{rl} \phi : & G \rightarrow H \\ (1,2,3,4) & \mapsto z \\ (1,2,3) & \mapsto \textit{identity} \end{array}$$

Overview

There are several classes of homomorphisms that arise naturally in the study of permutation groups. Let G be a permutation group acting on a set Ω. Given a G-invariant subset Δ of Ω, the *transitive constituent homomorphism* sends each g in G to its restriction on Δ. If π is a system of imprimitivity (or block system) for G, the *blocks homomorphism* sends each g in G to the permutation it induces on π.

The aim is to present methods of effectively computing with these naturally arising homomorphisms. We shall take the notion of effective computation with a homomorphism $\phi{:}G \rightarrow \overline{G}$ to mean the ability to perform the following tasks.

1. Construct the image $im\phi$ of G.
2. Construct the kernel $ker\phi$.
3. Given an element g of G, construct $\phi(g)$.
4. Given an element h of $im\phi$, construct an element g of $\phi^{-1}(h)$.
5. Given a subgroup H of G, construct $\phi(H)$.
6. Given a subgroup $\overline{H}$ of $im\phi$, construct $\phi^{-1}(\overline{H})$.

Of course, to construct a subgroup of a permutation group will mean forming a base and strong generating set of the subgroup. Also, when we given a subgroup of a permutation group we assume that a base and strong generating set of the subgroup are known.

The main issue is to determine the relationship between the homomorphism ϕ and the stabiliser chains of the domain and image. It is advantageous to choose the bases so that there is a "nice" correspondence between the homomorphism and the stabiliser chains. The first question to ask is:

> What is the preimage of a point stabiliser of the image group?

That is,

> Suppose $\overline{G}$ is the image of the homomorphism ϕ and $\overline{\alpha}$ is a point on which it acts. Which subgroup H of G is the set of all elements which map to the stabiliser $\overline{H} = \overline{G}_{\overline{\alpha}}$?

The correspondence will be "nice" if one can establish a relationship such as

$$\phi\left[G^{(i)}\right] = \phi\left[G\right]^{(i)}$$

between the stabiliser chains and the homomorphism. That is, the correspondence is "nice" if the following diagram commutes.

$$\begin{tikzcd}
G \arrow[r, "\phi"] \arrow[d, "\text{stabiliser}"'] & \overline{G} \arrow[d, "\text{stabiliser}"] \\
G_{\alpha} \arrow[r, "\phi"] & \overline{G}_{\overline{\alpha}}
\end{tikzcd}$$

Transitive Constituent Homomorphism

Let the subset Δ of Ω be invariant under the action of G. Let Σ_{Δ} denote the symmetric group on $\{1,2,...,|\Delta|\}$. Then for each bijection ¯ between Δ and $\{1,2,...,|\Delta|\}$, there is a homomorphism

$$\phi : G \rightarrow \Sigma_{\Delta}$$

defined by restricting the action of an element g to Δ (and relabelling). Hence, for $\alpha,\beta \in \Delta$, the image of $\overline{\alpha}$ under $\phi(g)$ is $\overline{\beta}$ if and only if $\alpha^{g} = \beta$.

Consider the group G to be the symmetries of the square acting on the six pairs of points

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

The action on this set of the two generators are a=*elt*[2]=(1,4,6,3)(2,5) and b=*elt*[5]=(1,3)(4,6). Hence, the two sets $\Delta_1=\{1,3,4,6\}$ and $\Delta_2=\{2,5\}$ are invariant under the action of G. They are the edges and non-edges of the square. For the homomorphism induced by restricting to Δ_1 the relabelling ¯ can be represented by an vector l

	1	2	3	4	5	6
l	1	0	2	3	0	4

where $l[\alpha]$ is $\overline{\alpha}$, or zero when $\alpha \notin \Delta$. Then if $\alpha \in \Delta$, the entry in the permutation $\overline{g}$ is defined by $\overline{g}[l[\alpha]] = l[\alpha^{g}]$. Hence, $\overline{a} = (1,3,4,2)$ and $\overline{b} = (1,2)(3,4)$.

For $\alpha \in \Delta$, the stabilizer of $\overline{\alpha}$ in the image of G is simply the image of G_{α}, since $g \in G$ fixes α if and only if $\phi(g)$ fixes $\overline{\alpha}$. Therefore, if $\alpha_1,\alpha_2,\ldots,\alpha_r$ are points of Δ such that $G_{\alpha_1,\alpha_2,\ldots,\alpha_r}$ is the pointwise stabilizer in G of Δ, then not only is $G_{\alpha_1,\alpha_2,..,\alpha_r}$ the kernel of ϕ, but $[\overline{\alpha}_1,\overline{\alpha}_2,\ldots,\overline{\alpha}_r]$ also forms a base for the image of ϕ. Furthermore, suppose the subset S of G contains a set of generators for each subgroup in the chain

$$G \geq G_{\alpha_1} \geq G_{\alpha_1,\alpha_2} \geq \cdots \geq G_{\alpha_1,\alpha_2,\ldots,\alpha_r},$$

then $\phi(S)$ contains a set of generators of each group in the stabilizer chain of $im\phi$ relative to the base $[\bar{\alpha}_1,\bar{\alpha}_2,\ldots,\bar{\alpha}_r]$. That is, $\phi(S)$ is a strong generating set of $im\phi$ relative to $[\alpha_1,\alpha_2,\ldots,\alpha_r]$.

So, given an arbitrary base and strong generating set of G, we proceed by choosing a base

$$B = [\alpha_1,\alpha_2,\ldots,\alpha_r,\beta_1,\beta_2,\ldots,\beta_s]$$

for G such that

1. $\alpha_1,\alpha_2,\ldots,\alpha_r \in \Delta$, and
2. $G_{\alpha_1,\alpha_2,\ldots,\alpha_r}$ is the pointwise stabilizer of Δ in G.

Applying the base change algorithm if necessary, we may assume a strong generating set S of G relative to B is known.

Let us return to the above example where G is the symmetries of the square acting on pairs of points and Δ is Δ_1, the set of edges of the square. The points $\alpha_1=1$ and $\alpha_2=3$ form a base for G, so $G_{1,3} = G_{1,3,4,6} = <$ identity $>$ (and s=0). Hence, $\bar{\alpha}_1=1$ and $\bar{\alpha}_2=2$ form a base for $im\phi$. The stabiliser G_1 is generated by $b \times a$=(2,5)(3,4), so $\{a,b,b \times a\}$ is a strong generating set of G relative to the chosen base. Furthermore, the stabiliser of 1 in $im\phi$ is generated by $\overline{b \times a}$=(2,3). Hence, the set of images $\{\ \bar{a},\ \bar{b},\ \overline{b \times a}\ \}$ = { (1,3,4,2), (1,2)(3,4), (2,3) } is a strong generating set of $im\phi$ relative to the base [1,2]. The kernel of the homomorphism is the trivial subgroup, < identity >.

We may perform each of the basic tasks as follows:

1. Constructing the image of the group: Choose enough points $\alpha_1, \alpha_2, \ldots, \alpha_r \in \Delta$ such that their pointwise stabiliser fixes all points in Δ. Change the base of G to a base B which has initial segment $[\alpha_1,\alpha_2,\ldots,\alpha_r]$. Let S be the corresponding strong generating set, and let $[\beta_1,\beta_2,\ldots,\beta_s]$ complete the base B. The sequence $\bar{B} = [\bar{\alpha}_1,\bar{\alpha}_2,\ldots,\bar{\alpha}_r]$ is a base for $im\phi$, and the set $\phi(S - S^{(r+1)})$ forms a strong generating set of $im\phi$ relative to $\bar{B}$.

Note that the restriction of an element of $S^{(r+1)}$ is the identity. Furthermore, the set $\phi(\ S - S^{(r+1)}\ )$ may contain redundant strong generators. These may be eliminated by applying Algorithm 4 of Chapter 12.

2. Constructing the kernel: The kernel of ϕ is $G_{\alpha_1,\alpha_2,\ldots,\alpha_r}$ which has $[\beta_1,\beta_2,\ldots,\beta_s]$ as a base and $S^{(r+1)}$ as a strong generating set relative to this base.

3. Constructing the image of an element: The image of an element g of G is formed by restricting its action to Δ and relabelling using the bijection $\bar{\ }: \Delta \rightarrow \{1,2,\ldots,|\Delta|\}$. This bijection is easily stored as a vector l indexed by Ω.

4. Constructing the preimage of an element: Given an element h in the image $im\phi$, we determine points $\gamma_1,\gamma_2,\ldots,\gamma_r$ in Δ such that $\bar{\alpha}_i^h = \bar{\gamma}_i$, $1 \leq i \leq r$, by using the inverse of the relabelling $\bar{\ }$. Then the base B for G and any strong generating set of G relative to B allow the computation of an element g in G which maps α_i to γ_i, $1 \leq i \leq r$. The element g belongs to $\phi^{-1}(h)$. In fact, $\phi^{-1}(h)$ is the right coset $(ker\phi)\,g$.

The inverse of $^{-}$ is readily stored as a vector l_inv indexed by $\{1,2,..., |\Delta|\}$. For our running example, the vector l_inv is

	1	2	3	4
l_inv	1	3	4	6

Algorithm 1 : Preimage of an Element

```
Input: a group $G$ acting on $\Omega$;
    an invariant subset $\Delta$ of $\Omega$;
    a corresponding base $B = [\alpha_1,\alpha_2,\ldots,\alpha_r,\beta_1,\beta_2,\ldots,\beta_s]$
        and strong generating set of $G$;
    the vector $l\_inv$;
    an element $\bar{g}$ of $im\phi$;
Output: an element $g \in G$ which maps to $\bar{g}$;
begin
  for $i$ := 1 to $r$ do
    $\gamma_i := l\_inv[\ \bar{\alpha}_i^{\bar{g}}\ ]$;
  end for;
  $g$ := an element of $G$ mapping $[\alpha_1,\alpha_2,\ldots,\alpha_r]$ to $[\gamma_1,\gamma_2,\ldots,\gamma_r]$;
end.
```

For example, the element $\bar{g}$=(1,4)(2,3) requires an element $g \in G$ mapping [1,3] to [l_inv[4],l_inv[3]]=[6,4]. Tracing the Schreier vectors would determine $g=a^2$=(1,6)(3,4).

5. Constructing the image of a subgroup: Suppose we are given a base and strong generating set of a subgroup H of G. Apply the base change algorithm to H to form a strong generating set T relative to B. Then $\bar{B}$ is a base for $\phi(H)$ and $\phi(T - T^{(r+1)})$ is a strong generating set of $\phi(H)$ relative to $\bar{B}$.

6. Constructing the preimage of a subgroup: Suppose we are given a base and strong generating set of a subgroup $\bar{H}$ of $im\phi$. Apply the base change algorithm to $\bar{H}$ and form a strong generating set $\bar{T}$ of $\bar{H}$ relative to $\bar{B}$. Using the method described in (4), form $T = \{ \phi^{-1}(t) \mid t \in \bar{T} \}$. We claim that $T \cup S^{(r+1)}$ is a strong generating set of $H = \phi^{-1}(\bar{H})$ relative to B.

Clearly B is a base for H, and $S^{(r+1)}$ is a strong generating set of $H^{(r+1)}$. If $T \cup S^{(r+1)}$ is not a strong generating set then there exists a group $H^{(i)}$, $1 \le i \le r$, in the stabilizer chain of H for which the group generated by $T^{(i)} \cup S^{(r+1)}$ is properly contained in $H^{(i)}$. But, since $S^{(r+1)}$ generates $ker\phi$, this implies that $\phi(T^{(i)})$ generates a proper subgroup of $\bar{H}^{(i)}$, thereby contradicting the fact that $\bar{T}$ is a strong generating set of $\bar{H}$ relative to $\bar{B}$.

The algorithms as implemented consist of a major routine which produces a table holding the information necessary to efficiently perform the above tasks. The table stores

a. the vector l describing the bijection $^{-}: \Delta \rightarrow \{1,2,..., |\Delta|\}$,

b. a vector l_inv for the inverse of $^{-}$,

c. the base $B = [\alpha_1, \alpha_2, \ldots, \alpha_r, \beta_1, \beta_2, \ldots, \beta_s]$,

d. the base $\bar{B} = [\bar{\alpha}_1, \bar{\alpha}_2, \ldots, \bar{\alpha}_r]$ and the strong generating set $\phi(S - S^{(r+1)})$ of $im\phi$, and

e. the base $[\beta_1, \beta_2, \ldots, \beta_s]$ and the strong generating set $S^{(r+1)}$ of $ker\phi$.

Blocks Homomorphism

The homomorphisms of this section were originally defined in terms of systems of imprimitivity, however, all that is required is a partition of the set of points which is invariant under the action of the group. It is not even necessary for the action to be transitive.

A partition $\pi = \{B_1 \mid B_2 \mid \cdots \mid B_t\}$ of Ω is G-invariant if G permutes the subsets $B_1, B_2, \ldots, B_t$ amongst themselves. (The subsets $B_1, B_2, \ldots, B_t$ are also called *blocks*.) Let Σ_t be the symmetric group on $\{1,2,...,t\}$. There is a homomorphism

$$\phi : G \rightarrow \Sigma_t$$

where the image $\phi(g)$ of a permutation g maps i to j if and only if $B_i^g = B_j$.

As an example consider the group G of the symmetries of the square acting on the 4 vertices of the square. Then π=$\{1,3|2,4\}$ is an invariant partition. The partition could be represented by a vector π mapping the points of Ω to an integer in $\{1,2\}$ indicating whether the point was in the first or second subset of the partition:

	1	2	3	4
π	1	2	1	2

We also need to know a representative point b_i of each block B_i of the partition. A vector b indexed by $\{1,2,..,t\}$ can represent this information:

	1	2
b	1	2

Given an element $g \in G$ the image $\bar{g}$ is computed by setting $\bar{g}[i] = \pi[b[i]^g]$, for each $i \in \{1,2,...,t\}$. So the image of a=(1,2,3,4) is $\bar{a}$=(1,2).

A permutation $\phi(g)$ stabilizes i if and only if g fixes the block B_i as a set. Let G_{B_i} denote the setwise stabilizer of the block B_i. Then the image of G_{B_i} is the stabilizer of i in $im\phi$. Furthermore, the image of a set of generators of G_{B_i} will generate the stabilizer of i in $im\phi$. We therefore choose blocks $B_{i_1}, B_{i_2}, \ldots, B_{i_r}$ in π such that any permutation which stabilizes each of the blocks $B_{i_1}, B_{i_2}, \ldots, B_{i_r}$ stabilizes every block of π. That is,

$$G_{B_{i_1}, B_{i_2}, \ldots, B_{i_r}} = \bigcap_{B \in \pi} G_B = ker\phi.$$

Then $[i_1, i_2, \ldots, i_r]$ is a base for $im\phi$. A strong generating set of $im\phi$ relative to this base may be computed by taking the images of the sets of generators of each group in the chain

$$G \geq G_{B_{i_1}} \geq G_{B_{i_1}, B_{i_2}} \geq \cdots \geq G_{B_{i_1}, B_{i_2}, \ldots, B_{i_r}}.$$

The first problem then is to compute a base and strong generating set of the stabilizer G_B of a block B. We assume that a base and strong generating set of G are known. Once such an algorithm is known, it may be applied repeatedly to form each group in the chain.

Let $B \in \pi$ and let b be any point in the block B. It follows from the definition of G-invariant that if a permutation g maps b to a point in B then g fixes B setwise. That is, $g \in G_B$. An immediate consequence is that $G_b \leq G_B$. Furthermore, G_b is the stabilizer of b in G_B. Another consequence is that the orbit of b under G_B is precisely the intersection of B with the orbit b^G. These facts may be used in conjunction with the following lemma to prove the correctness of the algorithm that we present below.

Lemma

Let T be a subset of a permutation group H. If T contains a strong generating set of H_b, for some point b, and if the orbit of b under H is the same as the orbit of b under $< T >$, then T is a strong generating set of H (relative to some base beginning with b).

A block B is fixed by $G_{B_{i_1}}$ if and only if the orbit of b under $G_{B_{i_1}}$ is contained in B for any point b in B. These facts lead to an algorithm, which we call *blocks_image*, to produce a base and strong generating set of $im\phi$ and also a base and strong generating set of $ker\phi$.

Algorithm 2 : Blocks Image

```
Input: a base and strong generating set of a group $G$ acting on $\Omega$;
    an invariant partition $\pi = \{B_1 | B_2 | \ldots | B_t\}$ of $\Omega$;

Output: a base $\bar{B}$ and a strong generating set $\bar{S}$ of $im\phi$;
    a base and strong generating set T of K = $ker\phi$, for blocks homomorphism $\phi$;

begin (* blocks_image *)
  $K := G$; $T :=$ strong generators of $G$; $\bar{B} := [\,]$; $\bar{S} :=$ empty set;
  for $i := 1$ to $t$ do (* K is $G_{B_1, B_2, \ldots, B_{i-1}}$ *)
    choose a point $b$ in $B_i$; form $\Gamma := b^K - \{b\}$;
    if not ( $\Gamma \subseteq B_i$ ) then (* non-redundant block to stabilize *)
      change base of $K$ to start with $b$;
      $T :=$ strong generating set of $K_b$; $\Gamma := \Gamma \cap B_i$;
      (* extend $T$ to generate $K_{B_i}$ *)
      while $\Gamma \neq$ empty set do
        choose $\gamma \in \Gamma$;
        take $g = u^{(1)}(\gamma)$ of $K$ as an element mapping $b$ to $\gamma$;
        $T := T \cup \{g\}$; $\Gamma := \Gamma - b^{<T>}$;
      end while;
      (* add next group to stabilizer chain of $im\phi$ *)
      append $i$ to $\bar{B}$;
      add $\{ \phi(g) \mid g \in T \}$ to $\bar{S}$;
      $K := < T >$; (* $T$ is strong generating set of $K$ relative to present base for $K$ *)
    end if;
  end for;
end. (* blocks_image *)
```

Note that the transitivity of G is not required for the algorithm to be correct. It is only necessary that the group G permute the blocks amongst themselves.

Let us return to our example of the group G, the symmetries of the square acting on the 4 vertices, and the invariant partition $\{1,3|2,4\}$. The first block is $\{1,3\}$ with representative point 1. The stabiliser G_1 is generated by b, and the set Γ is $\{3\}$, so we find an element g mapping 1 to 3. Such an element is a^2=(1,3)(2,4), so the block stabiliser $G_{\{1,3\}}$ is $< a^2, b >$. This subgroup also stabilises the other block $\{2,4\}$. Hence, it is the kernel of the homomorphism. The kernel has a base [2] and strong generating set $\{a^2,b\}$. Therefore, the image $im\phi$ has a base [1] and strong generating set $\{(1,2)\} = \{\bar{a}\}$, since $b \in ker\phi$.

The inverse problem arises during the determination of preimages of subgroups. In this situation we know a base and strong generating set of G_B, for some block B, and we know a set of generators of G. The problem is to determine a base and strong generating set of G. Equivalently, we require a base and strong generating set for some point stabilizer G_α in G. The solution is to choose a point b in B as the point α. Then the stabilizer G_b is precisely the stabilizer of b in G_B, which can be determined by applying the base change algorithm to G_B. Inserting the point b at the start of the base for G_b, and adding the generators of G to the strong generating set of G_b gives the desired base and strong generating set of G.

Before presenting methods to perform the six basic tasks, we will relate the blocks homomorphism to a transitive constituent homomorphism.

We may regard G as acting on the set $\pi \cup \Omega$. Then π is invariant under G, and the blocks homomorphism is precisely the transitive constituent homomorphism. We form a base $[B_{i_1}, B_{i_2}, \ldots, B_{i_r}, \beta_1, \beta_2, \ldots, \beta_s]$ where

$$G_{B_{i_1}, B_{i_2}, \ldots, B_{i_r}} = \bigcap_{B \in \pi} G_B$$

and form the corresponding strong generating set. Here, however, we work with the representation of G on Ω and use the algorithms of this section to convert from block stabilizers to point stabilizers, and vice versa.

1. Constructing the image of the group: Algorithm *blocks_image* computes a base and strong generating set of $im\phi$.

2. Constructing the kernel: Algorithm *blocks_image* computes a base and strong generating set of $ker\phi$.

3. Constructing the image of an element: If we store a list of representative points $b_1, b_2, \ldots, b_t$ for the blocks $B_1, B_2, \ldots, B_t$, and also store a vector indexed by Ω which gives the number of the block containing a given point, then it is straightforward to determine $\phi(g)$ from an element g of G.

4. Constructing the preimage of an element: Given an element h in $im\phi$, its preimage is determined by working in the representation of G on Ω rather than on $\pi \cup \Omega$, which complicates matters slightly. For each group $G_{B_{i_1}, B_{i_2}, \ldots, B_{i_{m-1}}}$, $1 \le m \le r$, we store a set of generators and the Schreier vector of the orbit of b_{i_m}. In order to find an element mapping B_{i_m} to B_j, we choose a point γ in the intersection of B_j and the orbit of b_{i_m}, and take the element mapping b_{i_m} to γ as determined by the Schreier vector.

Algorithm 3 : Preimage of an Element

```
Input: a group $G$ acting on $\Omega$;
    an invariant partition $\pi$ of $\Omega$ with vectors $\pi$ and $b$;
    the corresponding blocks homomorphism $\phi$;
    a corresponding base $\overline{B} = [i_1, i_2, \ldots, i_r]$ of $im\phi$;
    generators of $G_{B_{i_1}, B_{i_2}, \ldots, B_{i_{m-1}}}$, $1 \le m \le r$;
    the orbit $\Delta^{(m)}$ and Schreier vector $v^{(m)}$ of $b_{i_m}$ under the
        subgroup $G_{B_{i_1}, B_{i_2}, \ldots, B_{i_{m-1}}}$, $1 \le m \le r$;
    an element $\overline{g}$ of $im\phi$;
Output: an element $g \in G$ which maps to $\overline{g}$;
begin
  for $m := 1$ to $r$ do
    $\gamma_m := b[\, i_m^{\overline{g}}\, ]$;
  end for;

  $g :=$ identity of $G$;

  for $m := 1$ to $r$ do
    $j := \pi[\, \gamma_m\, ]$;
    find a point $\gamma \in B_j \cap \Delta^{(m)}$;
    $u_m := trace(\, \gamma, v^{(m)}\, )$;
    $g := u_m \times g$;
    $[\gamma_1, \gamma_2, \ldots, \gamma_r] := [\gamma_1, \gamma_2, \ldots, \gamma_r]^{u_m^{-1}}$;
  end for;
end.
```

5. Constructing the image of a subgroup: Given a base and strong generating set of a subgroup H of G, then algorithm *blocks_image* will determine a base and strong generating set of $\phi(H)$ since the blocks of π are permuted amongst themselves by H.

6. Constructing the preimage of a subgroup: Let $\overline{H}$ be a subgroup of $im\phi$, and let $H = \phi^{-1}(\overline{H})$. As in the case of the transitive constituent homomorphism, we can form generators for each group in the chain

$$H \ge H_{B_{i_1}} \ge H_{B_{i_1}, B_{i_2}} \ge \cdots \ge H_{B_{i_1}, B_{i_2}, \ldots, B_{i_r}}$$

by changing the base of $\overline{H}$ to $[i_1, i_2, \ldots, i_r]$ and using the methods in (4) above. The problem is to use this information to form generators for a chain of point stabilizers in H; that is, form a base and strong generating set of H. Since $H_{B_{i_1}, B_{i_2}, \ldots, B_{i_r}}$ is $ker\phi$ (and we know a base and strong generating set of $ker\phi$ by (2) above), the problem is to work up the chain of block stabilizers forming a base and strong generating set of $H_{B_{i_1}, B_{i_2}, \ldots, B_{i_{m-1}}}$ using a base and strong generating set of $H_{B_{i_1}, B_{i_2}, \ldots, B_{i_m}}$ and the generators of $H_{B_{i_1}, B_{i_2}, \ldots, B_{i_{m-1}}}$. This is precisely the inverse problem solved above.

The complete process is presented as algorithm *blocks_preimage*. The strong generating set of H produced may contain redundancies.

Algorithm 4 : Blocks Preimage

```
Input: a group $G$ acting on $\Omega$;
        an invariant partition $\pi = \{B_1 | B_2 | \ldots | B_t\}$ of $\Omega$;
        the corresponding blocks homomorphism $\phi$;
        a base $\bar{B} = [i_1, i_2, \ldots, i_r]$ of $im\phi$;
        a strong generating set $\bar{T}$ of a subgroup $\bar{H}$ of $im\phi$ relative to the base $\bar{B}$;
        a base and strong generating set of $ker\phi$;

Output: a base and strong generating set $T$ of $H = \phi^{-1}(\bar{H})$;

begin (* blocks_preimage *)

  (* form a base and strong generating set of $H_{B_{i_1}, B_{i_2}, \ldots, B_{i_r}}$ *)
  $H := ker\phi$;

  (* work up the chain of block stabilizers *)
  for $m := r$ downto 1 do
    (* form a base and strong generating set of $H_{B_{i_1}, B_{i_2}, \ldots, B_{i_{m-1}}}$ *)
    choose a point $b$ in $B_{i_m}$; change base of $H$ to start with $b$;
    $T := \phi^{-1}(\bar{T}^{(m)}) \cup$ strong generators of $H_b$;
    $H := < T >$; (* with base of previous $H$ and strong generating set $T$ *)
  end for;

end. (* blocks_preimage *)
```

The table of information required by the blocks homomorphism routines is as follows.

a. a list of representative points $b_1, b_2, \ldots, b_t$ of the blocks,

b. a vector giving the partition π of Ω; that is a map from Ω to $\{1,2,\ldots,t\}$,

c. a base $[i_1, i_2, \ldots, i_r]$ and strong generating set of $im\phi$,

d. a base $[\beta_1, \beta_2, \ldots, \beta_s]$ and strong generating set of $ker\phi$, and

e. for each m, $1 \le m \le r$, generators of $G_{B_{i_1}, B_{i_2}, \ldots, B_{i_{m-1}}}$ and the Schreier vector of the orbit of b_{i_m} under the action of this group.

Other Homomorphisms

General homomorphisms may be defined by specifying the image of each generator of the group G. This section looks at such homomorphisms. Let G be a permutation group acting on $\Omega_1 = \{1,2,\ldots,n\}$ and generated by the set S. Let H be a permutation group acting on $\Omega_2 = \{n+1, n+2, \ldots, n+m\}$. Let $f : S \rightarrow H$ be a map specifying the image of each generator of G. The map f may determine a homomorphism ϕ defined by

$$\begin{array}{c} \phi : G \rightarrow H \\ s_1^{\varepsilon_1} \times \cdots \times s_t^{\varepsilon_t} \mapsto f(s_1)^{\varepsilon_1} \times \cdots \times f(s_t)^{\varepsilon_t} \end{array}$$

The first problem is that not all maps $f : S \rightarrow H$ determine a homomorphism. It may be the case that if we express an element g as a word in two different ways - say as w_1 and w_2- then the "image" of g will be different. That is, $f(w_1) \neq f(w_2)$. Then the homomorphism is not even well-defined. In this case we have that the word $w_1 \times w_2^{-1}$ represents the identity element - that is, it is a relator - but it does not get mapped to the identity under f. Actually, f determines a homomorphism if and only if every relator of G is mapped to the identity element of H.

The computations with the map f and the homomorphism ϕ are carried out in the direct product

$$G \times H = \{ (g,h) \mid g \in G, h \in H \}$$

which is the group of all pairs (g,h). The multiplication of these pairs is defined componentwise

$$(g_1,h_1) \times (g_2,h_2) = (g_1 \times g_2, h_1 \times h_2)$$

and so is inversion

$$(g,h)^{-1} = (g^{-1}, h^{-1})$$

The identity element of the direct product is $(identity_G, identity_H)$. The direct product acts on the set $\Omega = \Omega_1 \cup \Omega_2 = \{1,2,...n+m\}$ by defining the image of a point i under (g,h) to be i^g if $1 \leq i \leq n$, and to be i^h if $n+1 \leq i \leq n+m$.

Define the subgroup $F = < (s,f(s)) \mid s \in S >$ of $G \times H$. We can rephrase the criterion that f maps every relator to the identity as

Lemma

The map f determines a homomorphism if and only if

$$F \cap \left[\{ identity_G \} \times H \right] = \{ identity_{G \times H} \}$$

Similarly, the definition of the kernel as the subgroup of G of all the elements which map to the identity can be rephrased as

Lemma

If the map f determines a homomorphism ϕ, then

$$ker\phi = F \cap \left[G \times \{ identity_H \} \right]$$

The definition of a base as being a sequence of points whose stabiliser is the identity allows us to rephrase the above lemmas as

Theorem

Let B be a base for G acting on Ω_1, and let C be a base for H acting on Ω_2. Then

(a) the map f determines a homomorphism if and only if B is a base for F.

(b) if the map f determines a homomorphism ϕ, then $ker\phi$ is the pointwise stabiliser of C in F.

As an example, consider the group G to be the symmetric group of degree 4 acting on $\Omega_1 = \{1,2,3,4\}$ and generated by a=(1,2,3,4) and b=(1,2,3). So $S=\{a,b\}$. Let H be the cyclic group of order 2 acting on the set $\Omega_2 = \{5,6\}$ and generated by z=(5,6). Define $f : S \rightarrow H$ by $a \mapsto z$ and $b \mapsto$ *identity*. Then $G \times H$ acts on $\Omega = \{1,2,3,4,5,6\}$ and is generated by

$$(a,\text{identity})=(1,2,3,4)(5)(6)$$
$$(b,\text{identity})=(1,2,3)(4)(5)(6)$$
$$(\text{identity},z)=(1)(2)(3)(4)(5,6)$$

The subgroup F is generated by

$$(a,z)=(1,2,3,4)(5,6)$$
$$(b,\text{identity})=(1,2,3)(4)(5)(6)$$

A base B for G is [1,2,3] and a base C for H is [5]. Using the Schreier-Sims method, we can verify that B is a base for F, and that $ker\phi$ is $< b,a^2 >$, the stabiliser F_5.

We now turn to how we can perform each of the basic tasks. We will assume we know a base B and strong generating set T for G, that we know a generating set S of G, and that we know a base C for H. The map f is defined on S, though it is useful if f is defined on T.

0. Checking that f determines a homomorphism: Form the subgroup F and using the Schreier-Sims method verify that B is a base for F.

If we already know that f determines a homomorphism ϕ then we can directly form a strong generating set of F relative to B by taking the set $\{ (t,\phi(t)) \mid t \in T \}$, where T is a strong generating set of G relative to B.

In either case, we can assume that we know a base and strong generating set for F after we have confirmed that f determines a homomorphism ϕ.

1. Constructing the image of the group: A base C and strong generating set of $im\phi$ acting on Ω_2 can be constructed by changing the base of F to begin with C and restricting each element of the resulting strong generating set of F to Ω_2.

2. Constructing the kernel: The kernel is the stabiliser of C in F, so changing the base of F to begin with C will determine a base and strong generating set of $ker\phi$ acting on Ω. We can restrict to Ω_1 if we so desire.

3. Constructing the image of an element: Given an element $g \in G$ we take its base image B^g and determine the element of F which maps its base B to B^g. The restriction of this element to Ω_2 is $\phi(g)$.

4. Constructing the preimage of an element: Given an element $h \in im\phi$ we take its base image C^h and determine an element of F which maps C to C^h using a base D for F which has C as an initial segment. The restriction of this element to Ω_1 is $\phi^{-1}(h)$.

5. Constructing the image of a subgroup: Given a subgroup L of G with a strong generating set X relative to B, we form the subgroup L_F of $G \times H$ which has base B and strong generating set $\{ (x,\phi(x)) \mid x \in X \}$. We change the base of L_F to begin with C and restrict the elements of the resulting strong generating set to Ω_2. The set of these restricted elements is a strong generating set of $\phi(L)$ relative to the base C.

6. Constructing the preimage of a subgroup: Given a subgroup L of $im\phi$ with a strong generating set X relative to C, we form the subgroup L_F of $G \times H$ with a base D (the base for F which begins with C) and a strong generating set which is the union of $\{ (x,\phi(x)) \mid x \in X \}$ and a strong generating set of the stabiliser of C in F (relative to D). We change the base of L_F to be B and restrict the elements of the resulting strong generating set to Ω_1. The set of these restricted elements is a strong generating set of $\phi^{-1}(L)$ relative to the base B.

Summary

This chapter has considered the tasks of computing images and preimages of elements and subgroups under homomorphisms. In particular, it deals with the task of computing the kernel of the homomorphism. Most attention is given to the natural homomorphisms of a permutation group that arise from invariant subsets and partitions of the points, but the chapter also considers general homomorphisms defined in terms of the images of the group generators.

The algorithms determine a base and strong generating set of the subgroups constructed as kernels, images, or preimages. They are efficient, and the most expensive component in their execution is the base change algorithm.

Homomorphisms play an important role in divide-and-conquer algorithms for permutation groups, as the reader will see in the following chapters.

Exercises

(1/Easy) Consider the group G to be the symmetries of the square acting on the pairs of points. Take the set Δ to be the set Δ_2 of non-edges of the square. Let ϕ be the corresponding transitive constituent homomorphism. Determine an appropriate base of G, a base and strong generating set of $im\phi$, and a base and strong generating set of $ker\phi$.

(2/Moderate) Let G be the symmetries of the square acting on the 6 pairs of points. The partition $\{1,6|2,5|3,4\}$ is invariant under the action of G. Determine the block stabiliser K of $\{1,6\}$, and then the block stabiliser of $\{2,5\}$ in K. Hence, give a base and strong generating set for $im\phi$, where ϕ is the corresponding blocks homomorphism.

(3/Moderate) Consider the sixth group G of Chapter 10. The group has degree 14 and is generated by

$$a=(1,2)(3,4)(5,6)(7,8)(9,10)(11,12)$$
$$b=(1,13)(2,3,7,5)(6,9,11,8)(10,14)$$

The following partition is invariant under G.

$$\{1,10|2,9|3,11|4,12|5,6|7,8|13,14\}$$

Form the successive block stabilisers of $\{1,10\}$, $\{2,9\}$, $\{3,4\}$ and show that $K = G_{\{1,10\},\{2,9\},\{3,4\}}$ is the kernel of the blocks homomorphism ϕ.

Furthermore, show that K has a base [3,2,1,4,7,8] and strong generating set

$$\begin{gathered}(1,10)(2,9)(3,11)(5,6)\\(1,10)(2,9)(5,6)(7,8)\\(1,10)(4,12)(7,8)(13,14)\\(4,10)(13,14)\\(2,8)(13,14)\\(5,6)(13,14)\end{gathered}$$

Hence, K has order 2^6.

Furthermore, show that the block stabilisers are generated as follows:

$$\begin{aligned}G_{\{1,10\},\{2,9\}} &= < K, (1,10)(3,8)(4,13)(5,6)(7,11)(12,14), (3,14)(4,8)(7,12)(11,13) >\\G_{\{1,10\}} &= < G_{\{1,10\},\{2,9\}}, (2,4)(3,11)(5,13)(6,14)(7,8)(9,12) >\end{aligned}$$

Hence, show that $im\phi$ has a base [1,2,3] and strong generating set

$$\begin{gathered}(1,2)(3,4)\\(1,7)(2,3,6,5)\\(2,4)(5,7)\\(3,6)(4,7)\\(3,7)(4,6)\end{gathered}$$

(The image is isomorphic to the symmetries of the projective plane of order two.)

(4/Easy) Consider the group G to be the symmetric group of degree 4 acting on $\Omega_1 = \{1,2,3,4\}$ and generated by a=(1,2,3,4) and b=(1,2,3). So $S=\{a,b\}$. Let H be the cyclic group of order 2 acting on the set $\Omega_2 = \{5,6\}$ and generated by z=(5,6). A base B for G is [1,2,3] and a base C for H is [5].

(a) Define $f : S \rightarrow H$ by $a \mapsto z$ and $b \mapsto z$. The subgroup F is generated by

$$\begin{gathered}(a,z)=(1,2,3,4)(5,6)\\(b,z)=(1,2,3)(4)(5,6)\end{gathered}$$

Using the Schreier-Sims method - or otherwise - verify that B is not a base for F, and that f does not determine a homomorphism. Find a relator of G in terms of a and b which is not mapped to the identity by f.

(b) Let c=(1,2) of G and take the set S of generators of G to be $\{a,c\}$. Define $f : S \rightarrow H$ by $a \mapsto z$ and $c \mapsto z$. The subgroup F is generated by

$$\begin{gathered}(a,z)=(1,2,3,4)(5,6)\\(c,z)=(1,2)(3)(4)(5,6)\end{gathered}$$

Using the Schreier-Sims method - or otherwise - verify that B is a base for F, and that f determines a homomorphism ϕ. Compute the stabiliser F_5 and determine $ker\phi$.

Bibliographical Remarks

The natural homomorphisms for permutation groups have been used extensively in the theoretical literature on permutations groups. It has long been clear how to determine images of elements, and hence generators for the image of a subgroup. It was also known that the kernel of the transitive constituent homomorphism defined by a subset Δ is the pointwise stabiliser of Δ. With the development of the Schreier-Sims method and the base change algorithm, people knew how to compute (a base and strong generating set for) the kernel of a transitive constituent homomorphism. Algorithms to perform the remaining tasks for the natural homomorphisms of permutation groups were first developed in the author's thesis G. Butler, **Computational Approaches to Certain Problems in the Theory of Finite Groups**, Ph. D. Thesis, University of Sydney, 1980, and published in G. Butler, *"Effective computation with group homomorphisms"*, Journal of Symbolic Computation **1**, 2 (1985) 143-157.

The results of the last section dealing with general homomorphisms defined by the generator images is due to C.R. Leedham-Green, C.E. Praeger, and L.H. Soicher, *"Computing with group homomorphisms"*, to appear in Journal of Symbolic Computation.