## 0.1 $G$-sets

We introduce a part of the theory of $G$-sets, suitable for understanding the approach GAP uses to compute with permutation groups, using stabilizer chains. Rotman's book describes other results about $G$-sets, such as the Cauchy-Frobenius lemma, often known as 'Burnside's Lemma'.

Let $G$ be a group. A *$G$-set* is a set $\Omega$ with an action of $G$ by permutations. There are right and left $G$-sets and by an action of $G$ on $\Omega$ from the right we mean a mapping $\Omega \times G \to \Omega$ so that $\omega(gh) = (\omega g)h$ and $\omega \cdot 1 = \omega$ hold for all $\omega \in \Omega$ and $g, h \in G$. With the convention that functions are applied from the right, the specification of a right $G$-set is equivalent to the specification of a homomorphism $G \to S_\Omega$, the symmetric group on $\Omega$. Similarly a left $G$-set is equivalent to the specification of a homomorphism $G \to S_\Omega$ provided we adopt the convention that mappings are applied from the left. Because GAP applies mappings from the right, we will work with right $G$-sets.

For each $\omega \in \Omega$ the set $\omega G = \{\omega g \bigm| g \in G\}$ is the *orbit* of $\Omega$ that contains $\omega$. We say that $G$ acts *transitively* on $\Omega$ if there is only one orbit. We put

$$\mathrm{Stab}_G(\omega) = G_\omega = \{g \in G \bigm| \omega g = \omega\}$$

and this is the *stabilizer* of $\omega$ in $G$. For example:

- if $G$ permutes the set of its subgroups by conjugation then $\mathrm{Stab}_G(H) = N_G(H)$,
- if $G$ permutes the set of its elements by conjugation then $\mathrm{Stab}_G(x) = C_G(x)$,
- if $G$ permutes the right cosets $H\backslash G = \{Hg \bigm| g \in G\}$ by right multiplication then $\mathrm{Stab}_G(Hg) = H^g = g^{-1}Hg$. This is part 3. of the result below.

A *homomorphism* $f : \Omega \to \Psi$ of $G$-sets is a mapping with $f(\omega g) = (f(\omega))g$ always, and if this condition is satisfied we say that the mapping $f$ is *equivariant* for the action of $G$. Such a homomorphism of $G$-sets is an isomorphism if and only if it is bijective, if and only if there is a $G$-set homomorphism $f_1 : \Psi \to \Omega$ with $1_\Psi = ff_1$ and $1_\Omega = f_1 f$.

**Class Activity.** Is this obvious?

We probably already know the 'orbit-stabilizer' theorem. Part 2 of the next proposition is a more sophisticated version of this result, applying to infinite $G$-sets and containing more information.

**Proposition 0.1.1.** *1. Every $G$-set $\Omega$ has a unique decomposition $\Omega = \bigcup_{i\in I} \Omega_i$ where $I$ is some indexing set and the $\Omega_i$ are orbits of $\Omega$.*

*2. If $\Omega$ is a transitive $G$-set and $\omega \in \Omega$ then $\Omega \cong \mathrm{Stab}_G(\omega)\backslash G$ as $G$-sets. Thus if $\Omega$ is finite then $|\Omega| = |G : \mathrm{Stab}_G(\omega)|$.*

*3. When $H \le G$, the stabilizer of the element $Hg$ in the space of right cosets $H\backslash G$ is $H^g = g^{-1}Hg$.*

4. *If $H, K \leq G$, there is a $G$-set homomorphism $f : H\backslash G \to K\backslash G$ with $f(H) = Kg$ if and only if $H \subseteq K^g$.*

5. *If $H, K \leq G$ then $H\backslash G \cong K\backslash G$ as $G$-sets if and only if $K$ and $H$ are conjugate subgroups of $G$.*

6. *Every equivariant map between transitive $G$-sets is an epimorphism.*

7. $\mathrm{Aut}_{G-\mathrm{set}}(H\backslash G) \cong N_G(H)/H$.

We see from 4. that every homomorphism $H\backslash G \to K\backslash G$ is the composite of a homomorphism $H\backslash G \to K^g\backslash G$ specified by $H \mapsto K^g$ where $H \leq K^g$, followed by an isomorphism $K^g\backslash G \to K\backslash G$ specified by $K^g \mapsto Kg$.

*Proof.* 2. Given $\omega \in \Omega$, define a mapping $G \to \Omega$ by $g \mapsto \omega g$. This is a map of $G$-sets. We check that the set of elements of $G$ mapped to $\omega g$ is $\mathrm{Stab}_G(\omega)g$, so that there is induced a $G$-equivariant bijection between the two sets as claimed.

4. We first observe that if $f : \Omega \to \Psi$ is a map of $G$ sets then $\mathrm{Stab}_G(\omega) \subseteq \mathrm{Stab}_G(f(\omega))$. From this, the implication '$\Rightarrow$' follows. Conversely, if $H \subseteq K^g$ we show that the specification $f : H\backslash G \to K\backslash G$ by $f(Hx) = Kgx$ is well defined. This is because if $Hx = Hy$ the $xy^{-1} \in H$ so $xy^{-1} \in K^g$ and $x = g^{-1}kgy$ for some $k \in K$. Thus $Kgx = Kgg^{-1}kgy = Kgy$. The mapping $f$ is $G$-equivariant, so we have a homomorphism as claimed.

7. The mapping $N_G(H) \to \mathrm{Aut}_{G-\mathrm{set}}(H\backslash G)$ given by $g \mapsto (H \mapsto Hg)$ is a surjective homomorphism of groups. Its kernel is $H$. □

Let $H$ be a subgroup of a group $G$. A *right transversal* to $H$ in $G$ is the same thing as a set of right coset representatives for $H$ in $G$, that is: a set of elements $g_1, \ldots, g_t$ of $G$ so that $G = Hg_1 \cup \cdots \cup Hg_t$.

**Proposition 0.1.2.** *Let $G$ act transitively on a set $\Omega$ and let $\omega \in \Omega$ be an element with stabilizer $G_\omega$. Then elements $\{g_i \bigm| i \in I\}$ of $G$ form a right transversal to $G_\omega$ in $G$ if and only if $\Omega = \{\omega g_i \bigm| i \in I\}$ and the $\omega g_i$ are all distinct.*

*Proof.* This comes from the isomorphism of $G$-sets $\Omega \cong G_\omega\backslash G$ under which $\omega g \leftrightarrow G_\omega g$. □

**Algorithm 0.1.3.** This observation provides a way to compute a transversal for $\mathrm{Stab}_G(\omega)$ in $G$. Take the generators of $G$ and repeatedly apply them to $\omega$, obtaining various elements of the form $\omega g_{i_1} g_{i_2} \cdots g_{i_r}$ where the $g_{i_j}$ are generators of $G$. Each time we get an element we have seen previously, we discard it. Eventually we obtain the orbit $\omega G$, and the various elements $g_{i_1} g_{i_2} \cdots g_{i_r}$ are a right transversal to $\mathrm{Stab}_G(\omega)$ in $G$.

There is an example below with a group of permutations of six points.

The elements of this transversal come expressed as words in the generators of $G$. It is what GAP does, except that it does the above with the inverses of the generators of

$G$. If an inverse generator $g^{-1}$ sends an already-computed element $u$ to a new element $v$, the generator $g$ is stored in position $v$ in a list. This means that applying $g$ to $v$ gives $u$. By repeating this we eventually get back to the first element of the orbit. It is this list of generators that GAP stores in the field ‘ `transversal`’ of a stabilizer chain. Elements of a right transversal are obtained by multiplying the inverses of the generators in reverse sequence.

### 0.1.1 Stabilizer chains

Computing chains of stabilizers is the most important technique available in computations with permutation groups. The idea of doing this in the context of computational group theory is due to Charles Sims. The following theorem of Schreier allows us to compute generators for stabilizer subgroups and the whole approach is known as the *Schreier-Sims algorithm.*

**Theorem 0.1.4** (Schreier)**.** *Let $X$ be a set of generators for a group $G$, $H \leq G$ a subgroup, and $T$ a right transversal for $H$ in $G$ such that the identity element of $G$ represents the coset $H$. For each $g \in G$ let $\overline{g} \in T$ be such that $H\overline{g} = Hg$. Then*

$$\{tg(\overline{tg})^{-1} \mid t \in T, g \in X\}$$

*is a set of generators for $H$.*

Note that since $Htg = H\overline{tg}$, the elements $tg(\overline{tg})^{-1}$ lie in $H$ always. Also $\overline{\overline{a}} = \overline{a}$ and $\overline{\overline{a}b} = \overline{ab}$. The generators in the set are called *Schreier generators.* Not only do they generate $H$ but, if the elements of the transversal are expressed as words in the generators of $G$, then the generators of $H$ are also expressed as words in the generators of $G$.

*Proof.* Suppose that $g_1 \cdots g_n \in H$ where the $g_i$ lie in $X$. Then

$$g_1 \cdots g_n = (g_1\overline{g_1}^{-1})(\overline{g_1}g_2\overline{g_1g_2}^{-1})(\overline{g_1g_2}g_3\overline{g_1g_2g_3}^{-1}) \cdots (\overline{g_1 \cdots g_{n-1}}g_n)$$

is a product of the Schreier generators. Note that $g_1 \cdots g_n \in H$ so that $\overline{g_1 \cdots g_n} = 1$. □

If $G$ permutes $\Omega$, a *base* for $G$ on $\Omega$ is a list of elements $\omega_1, \omega_2, \ldots, \omega_s$ of $\Omega$ so that the stabilizer $G_{\omega_1,\omega_2,\ldots,\omega_s}$ equals 1. Here $G_{\omega_1,\omega_2,\ldots,\omega_r}$ is the stabilizer inside the subgroup $G_{\omega_1,\omega_2,\ldots,\omega_{r-1}}$ of $\omega_r$, for each $r$. Let us write $G_r$ instead of $G_{\omega_1,\omega_2,\ldots,\omega_r}$ and $G_0 = G$. In this situation the chain of subgroups

$$G = G_0 \geq G_1 \geq \cdots \geq G_s = 1$$

is called a *stabilizer chain* (for $G$, with respect to the given base). We will consider for each $r$ the subset $\Omega_r$ of $\Omega$ which is defined to be the $G_r$-orbit containing $\omega_{r+1}$. Thus $\Omega_0 = \omega_1 G$, $\Omega_1 = \omega_2 G_1$ etc. A *strong generating set* for $G$ (with respect to the base) is a set of generators for $G$ which includes generators for each of the subgroups $G_r$. Thus in a strong generating set, $G_r$ is generated by those generators that happen to fix each of $\omega_1, \ldots, \omega_r$.

**Proposition 0.1.5.** *Each $\Omega_i$ is acted on transitively by $G_i$. As $G_i$-sets, $\Omega_i \cong G_{i+1}\backslash G_i$. Hence $|G| = |\Omega_0| \cdots |\Omega_{s-1}|$.*

*Proof.* We have $\omega_{i+1} \in \Omega_i$ and $\mathrm{Stab}_{G_i}(\omega_{i+1}) = G_{i+1}$. □

Given a set of generators $G = \langle g_1, \dots, g_d \rangle$ and a subgroup $H \leq G$ a *right Schreier transversal* for $H$ in $G$ is a right transversal with elements expressed as words in the generators, as suggested by the following $1, g_{i_1}, g_{i_1}g_{i_2}, g_{i_3}, \dots$ so that each initial segment of a word appears (earlier) in the list. Schreier transversals correspond to rooted trees.

**Example 0.1.6.** Let $G = \langle (1,5)(2,6), (1,3)(4,6), (2,3)(4,5) \rangle$ and write these generators as $a = (1,5)(2,6)$, $b = (1,3)(4,6)$, $c = (2,3)(4,5)$. Find a set of coset representatives for $\mathrm{Stab}_G(1)$.

Solution: We construct a Schreier tree:

$$\begin{tikzcd}
1 \arrow[r, "a"] \arrow[d, "b"'] & 5 \arrow[r, "c"] & 4 \\
3 \arrow[r, "c"] & 2 \arrow[r, "a"] & 6
\end{tikzcd}$$

giving coset representatives $1, a, b, ac, bc, bca$. These form a Schreier transversal: every initial segment of a word is in the transversal. These generators have order 2, and GAP stores their inverses in the list $[1, c, b, c, a, a]$.

**Class Activity.** Given that the element $abc = (1,4,6,3)(2,5) = x$ lies in $G$, find the coset representative that represents $\mathrm{Stab}_G(1)x$.

Table of $\overline{tg}$:

| $1$ | $a$ | $b$ | $ac$ | $bc$ | $bca$ | |
|---|---|---|---|---|---|---|
| $a$ | $1$ | $b$ | $ac$ | $bca$ | $bc$ | $a$ |
| $b$ | $a$ | $1$ | $bca$ | $bc$ | $ac$ | $b$ |
| $1$ | $ac$ | $bc$ | $a$ | $b$ | $bca$ | $c$ |

Table of $tg\overline{tg}^{-1}$:

| $1$ | $a$ | $b$ | $ac$ | $bc$ | $bca$ | |
|---|---|---|---|---|---|---|
| $1$ | $a^2$ | $bab^{-1}$ | $acac^{-1}a^{-1}$ | $1$ | $bca^2c^{-1}b^{-1}$ | $a$ |
| $1$ | $aba^{-1}$ | $b^2$ | $acba^{-1}c^{-1}b^{-1}$ | $bcbc^{-1}b^{-1}$ | $bcabc^{-1}a^{-1}$ | $b$ |
| $c$ | $1$ | $1$ | $ac^2a^{-1}$ | $bc^2b^{-1}$ | $bcaca^{-1}c^{-1}b^{-1}$ | $c$ |

Observe that 5 of these entries are necessarily 1. Upon evaluation of these expressions in $G$ the last table becomes the following:

| $1$ | $a$ | $b$ | $ac$ | $bc$ | $bca$ | |
|---|---|---|---|---|---|---|
| $1$ | $1$ | $(2,4)(3,5)$ | $(2,3)(4,5)$ | $1$ | $1$ | $a$ |
| $1$ | $(2,4)(3,5)$ | $1$ | $(2,5)(3,4)$ | $(2,3)(4,5)$ | $(2,5)(3,4)$ | $b$ |
| $(2,3)(4,5)$ | $1$ | $1$ | $1$ | $1$ | $(2,4)(3,5)$ | $c$ |

We see that, in the stabilizer chain, $G_0$ acts on $\Omega$ of size 6, $G_1 = \langle (2,3)(4,5), (2,4)(3,5) \rangle$ acts on $\{2,3,4,5\}$ of size 4, and $G_{12} = 1$, so that $|G| = 4 \cdot 6 = 24$. The fact that $G_{12} = 1$ we can see by inspection, because the group is so small, but to continue the algorithm properly we go through Schreier's theorem.

**Theorem 0.1.7** (Schreier)**.** *Let $G$ have $d$ generators and let $H \leq G$ have finite index. Then $H$ can be generated by $|G : H|(d-1)+1$ elements.*

*Proof.* Consider the generators $tg(\overline{tg})^{-1}$ for $H$, and write $n = |G : H|$. The number of edges in the Schreier tree is $n-1$. Each gives an entry 1 in the table of generators. The number of table entries which are not 1 is at most $dn - n + 1 = n(d-1)+1$. □

Write $d(G)$ for the smallest size of a set of generators of $G$. The last result can be written $d(H) - 1 \leq |G : H|(d(G)-1)$. When $G$ is a free group it turns out that we always get equality in this bound. We will see this when we come to the section on free groups and, more generally, groups acting on trees. In the example, there were 5 edges in the Schreier tree, and these accounted for the 5 identity elements in the first table.

**Algorithm 0.1.8.** Given a stabilizer chain with a transversal for each stabilizer group in the next, we can test whether a permutation belongs to a group. If it does, and the transversal elements are words in the generators, we can express the permutation as a word in the generators. This algorithm solves problems such as restoring Rubik's cube to its initial position, given a random permutation of its faces.

Given a permutation $\pi$ find the coset representative $x_1$ of the coset $G_1\pi$ by computing the action of $\pi$ on $\Omega$. We compute $(\omega_1)\pi$. If $\pi \in G$ this must equal $(\omega_1)g$ for some unique $g$ in a right transversal for $G_1$ in $G_0$ and so $\pi g^{-1} \in G_1$. In fact, $\pi \in G$ if and only if $(\omega_1)\pi = (\omega_1)g$ for some $g$ in the transversal and $\pi g^{-1} \in G_1$. We now continue to test whether $\pi g^{-1} \in G_1$ by repeating the algorithm.

**Example 0.1.9.** Continuing the previous example: is $(1,2,3)$ in $G$? Since $(1,2,3)c^{-1}b^{-1} = (4,5,6) \notin G_1$, the answer is No.

**Class Activity.** Is $(1,3,5)(2,6,4)$ in $G$? If it is, write this permutation as a word in the given generators of $G$.

**Algorithm 0.1.10.** We give an algorithm for listing the elements of $G$. We start by listing elements in the subgroups at the small end of the stabilizer chain, at each stage listing them by cosets in the next biggest stabilizer. Thus, if the elements of $G_{i+1}$ have been listed and $t_1, \ldots, t_s$ is a transversal for $G_{i+1}$ in $G_i$ then $G_i = G_{i+1}t_1 \cup \cdots \cup G_{i+1}t_s$. In the example we get

$$[(), (3,5)(2,4), (2,3)(4,5), (3,4)2,5), a, (3,5)(2,4)a, (2,3)(4,5)a, \ldots,$$

starting with the 4 elements of $G_1$, and continuing with the cosets of $G_1$ put in the order given by the Schreier transversal. This puts an ordering on the elements of $G$. GAP orders everything.

**Class Activity.** Examine the list of elements of some groups, such as $S_4$ to see the coset structure in the list.

Other algorithms, such as computing generators for a Sylow $p$-subgroup of a group, or for the normalizer of a subgroup, depend on computing a stabilizer chain. This approach to computation within permutation groups is due to Charles Sims.