Dummit & Foote Ch. 4.1: Group Actions and Permutation Representations

Scott Donaldson

Dec. 2023 - Jan. 2024

Let G be a group and A be a nonempty set.

1. (12/24/23)

Let G act on the set A. Prove that if $a, b \in A$ and $b = g \cdot a$ for some $g \in G$, then $G_b = gG_ag^{-1}$ (G_a is the stabilizer of a). Deduce that if G acts transitively on A then the kernel of the action is $\cap_{g \in G}\, gG_ag^{-1}$.

Proof. We will show first that G_b, the stabilizer of b, is contained in gG_ag^{-1}, and then show the converse, which proves that they are equal.

Let $x \in G_b$, so $x \cdot b = b$. Then:

$$\begin{aligned} x \cdot g \cdot a &= g \cdot a \ (b = g \cdot a) \\ (gg^{-1}) \cdot (xg) \cdot a &= g \cdot a \ (gg^{-1} = 1, 1 \cdot a = a) \\ g \cdot (g^{-1}xg) \cdot a &= g \cdot a \\ (g^{-1}xg) \cdot a &= a, \end{aligned}$$

which implies that $g^{-1}xg \in G_a$, and therefore $x \in gG_ag^{-1}$, so $G_b \subseteq gG_ag^{-1}$.

The converse, that $gG_ag^{-1} \subseteq G_b$, can be shown by following the above proof in reverse (that is, let $x \in gG_ag^{-1}$, so $g^{-1}xg \in G_a$, which implies that $(g^{-1}xg) \cdot a = a$, and each assertion holds from bottom to top). Since each is contained in the other, we have $G_b = gG_ag^{-1}$.

Now we already know that the kernel of the group action of G on A is the intersection of the stabilizers of all the elements of A, that is, $\cap_{b \in A}\, G_b$. If G acts transitively on A, fixing $a \in A$, then for all $b \in A$, we can write $b = g \cdot a$ for some $g \in G$, which from above implies that $G_b = gG_ag^{-1}$. We deduce that the kernel can be expressed in terms of a fixed element a, namely:

$$\cap_{b \in A}\, G_b = \cap_{b \in A}\, \underbrace{gG_ag^{-1}}_{b = g \cdot a} = \cap_{g \in G}\, gG_ag^{-1}.$$

We know that $\cap_{g \in G}\, gG_ag^{-1}$ intersects all of the same conjugates as does $\cap_{b \in A}$, since G acts transitively on A. And, since $b = g \cdot a \Rightarrow G_b = gG_ag^{-1}$, it intersects no conjugates not represented by G_b for all $b \in A$. $\square$

2. (1/2/24)

Let G be a *permutation group* on the set A (i.e., $G \leq S_A$), let $\sigma \in G$ and let $a \in A$. Prove that $\sigma G_a \sigma^{-1} = G_{\sigma(a)}$. Deduce that if G acts transitively on A then

$$\bigcap_{\sigma \in G} \sigma G_a \sigma^{-1} = 1.$$

Proof. We first show that $\sigma G_a \sigma^{-1} \subseteq G_{\sigma(a)}$, and then show the converse. To begin, let $\tau \in G_a$ and consider $\sigma\tau\sigma^{-1} \in \sigma G_a \sigma^{-1}$. We note that:

$$(\sigma\tau\sigma^{-1})(\sigma(a)) = (\sigma\tau\sigma^{-1}\sigma)(a) = (\sigma\tau)(a) = \underbrace{\sigma(\tau(a)) = \sigma(a)}_{\tau \in G_a \Rightarrow \tau(a) = a},$$

and so $\sigma\tau\sigma^{-1}$ stabilizes $\sigma(a)$, which implies that $\sigma G_a \sigma^{-1} \subseteq G_{\sigma(a)}$.

For the converse, let $\tau \in G$ and suppose that $\sigma\tau\sigma^{-1} \in G_{\sigma(a)}$. Then:

$$\begin{aligned}
(\sigma\tau\sigma^{-1})(\sigma(a)) &= \sigma(a) \\
(\sigma\tau\sigma^{-1}\sigma)(a) &= \sigma(a) \\
(\sigma\tau)(a) &= \sigma(a) \\
\sigma(\tau(a)) &= \sigma(a) \\
\tau(a) &= a,
\end{aligned}$$

so τ is in the stabilizer of a, which implies that $\sigma\tau\sigma^{-1} \in \sigma G_a \sigma^{-1}$, and so $G_{\sigma(a)} \subseteq \sigma G_a \sigma^{-1}$.

This concludes the proof that $\sigma G_a \sigma^{-1} = G_{\sigma(a)}$.

Now if G acts transitively on A, then there is only one orbit; that is, given some $a \in A$, for all $b \in A$, there is a $\sigma \in G$ such that $b = \sigma(a)$.

From above, we conclude:

$$\bigcap_{\sigma \in G} \sigma G_a \sigma^{-1} = \bigcap_{\sigma \in G} G_{\sigma(a)} = \bigcap_{a \in A} G_a \text{ (because } G \text{ acts transitively on } A),$$

and since the only permutation that fixes every element of A is the identity, this intersection consists therefore only the identity permutation. □

3. (1/2/24)

Assume that G is an abelian, transitive subgroup of S_A. Show that $\sigma(a) \neq a$ for all $\sigma \in G - \{1\}$ and all $a \in A$. Deduce that $|G| = |A|$. [Use the preceding exercise.]

Proof. Suppose that σ_1 fixes a, so $\sigma_1(a) = a$, and let $\sigma_2(a) = b$. Then:

$$\begin{aligned}
(\sigma_1 \circ \sigma_2)(a) &= \sigma_1(\sigma_2(a)) = \sigma_1(b), \text{ and} \\
(\sigma_2 \circ \sigma_1)(a) &= \sigma_2(\sigma_1(a)) = \sigma_2(a).
\end{aligned}$$

Since G is abelian, these must be equal, and so $\sigma_1(b) = \sigma_2(a) = b$. Then σ_1 also fixes b.

Since G is transitive, for every $b \in A$, there exists a $\sigma \in G$ such that $\sigma(b) = a$, which implies that σ_1 fixes every element of A and is therefore the identity. Thus the identity is the only element of G for which $\sigma(a) = a$; equivalently, $\sigma(a) \neq a$ for all $\sigma \in G - \{1\}$ and all $a \in A$.

Now let $A = \{1, ..., n\}$. Since G is transitive, it must contain at least n permutations. For all $i \in A$, define σ_i such that $\sigma_i(1) = i$ (with σ_1 the identity permutation). Suppose that τ is another permutation in G. Since A only contains n elements, we must have $\tau(1) = i$ for some $i \in A$, so $\tau(1) = \sigma_i(1)$. Then:

$$(\tau \circ \sigma_i)(1) = \tau(\sigma_i(1)) = \tau(i), \text{ and}$$
$$(\sigma_i \circ \tau)(1) = \sigma_i(\tau(1)) = \sigma_i(i).$$

Since G is abelian, these are equal, so $\tau(i) = \sigma_i(i)$. It follows that, if $j = \tau(i) = \sigma_i(i)$, then $\tau(j) = \sigma_i(j)$, and so on for every element which σ_i permutes. Therefore $\tau = \sigma_i$, so G contains exactly n permutations. We conclude that $|G| = |A|$. □

4. (1/3/24)

Let S_3 act on the set Ω of ordered pairs: $\{(i, j) \mid 1 \leq i, j \leq 3\}$ by $\sigma((i, j)) = (\sigma(i), \sigma(j))$. Find the orbits of S_3 on Ω. For each $\sigma \in S_3$ find the cycle decomposition of σ under this action (i.e., find its cycle decomposition when σ is considered as an element of S_9 — first fix a labelling of these nine ordered pairs). For each orbit $\mathcal{O}$ of S_3 acting on these nine points pick some $a \in \mathcal{O}$ and find the stabilizer of a in S_3.

Solution. The elements $(1, 1), (2, 2)$, and $(3, 3)$ all belong to the same orbit. We see that $(1\,2) \cdot (1, 1) = (2, 2)$ and $(2\,3) \cdot (2, 2) = (3, 3)$. Further, since for any $(i, i) \in \Omega$, the action of $\sigma \in S_3$ on it results in an element with the same coordinates, there is no $(i, j) \in \Omega$ with $i \neq j$ such that $\sigma((i, i)) = (i, j)$. Therefore these three elements constitute one orbit.

The other orbit consists of the remaining six elements. Beginning with $(1, 2)$, we have:

$$(1\,2\,3)(1, 2) = (2, 3), \text{ then}$$
$$(1\,2\,3)(2, 3) = (3, 1),$$
$$(1\,2)(3, 1) = (3, 2),$$
$$(1\,2\,3)(3, 2) = (1, 3), \text{ and finally}$$
$$(1\,2\,3)(1, 3) = (2, 1).$$

Conversely to the first orbit, for no $(i, j) \in \Omega$ with $i \neq j$ do we have $\sigma((i, j)) = (i, i)$. Thus these are the two disjoint orbits of S_3 on Ω.

Next, let us label the elements of Ω:

$$\begin{array}{lll} (1,1) \to 1 & (1,2) \to 2 & (1,3) \to 3 \\ (2,1) \to 4 & (2,2) \to 5 & (2,3) \to 6 \\ (3,1) \to 7 & (3,2) \to 8 & (3,3) \to 9 \end{array}$$

Then we can describe the cycle decomposition of each permutation of S_3 by how it acts on these elements:

$$\begin{aligned} 1 &\to 1 \\ (1\,2) &\to (1\,5)(2\,4)(3\,6)(7\,8) \\ (1\,3) &\to (1\,9)(2\,8)(3\,7)(4\,6) \\ (2\,3) &\to (2\,3)(4\,7)(5\,9)(6\,8) \\ (1\,2\,3) &\to (1\,5\,9)(2\,6\,7)(3\,4\,8) \\ (1\,3\,2) &\to (1\,9\,5)(2\,7\,6)(3\,8\,4) \end{aligned}$$

For the first orbit, let us choose the point $(1,1)$ and find its stabilizer. The permutations in S_3 that fix this element must fix 1. Obviously this includes the identity. Neither of the 3-cycles fix 1. Only one of the 2-cycles, $(2\,3)$, fixes 1. Therefore the stabilizer of $(1,1)$ is the subgroup $\{1, (2\,3)\}$.

For the second orbit, we choose $(1,2)$. Since all non-identity permutations of S_3 reassign either 1 or 2 (or both), the stabilizer consists of only the identity. $\square$

5. (1/3/24)

For each of parts (a) and (b) repeat the preceding exercise but with S_3 acting on the specified set:

(a) the set of 27 triples $\{(i,j,k) \mid 1 \le i,j,k \le 3\}$

- The orbit of any point (i,j,k) consists of those other points whose coordinates are equal if i, j, or k are equal or not if they are not. For example, the orbit of $(1,1,2)$ contains all those points whose first and second coordinates are the same and whose third is different, that is:

  $$(1,1,3), (2,2,1), (2,2,3), (3,3,1), (3,3,2)$$

  (It is simple to find a 2-cycle that acts on $(1,1,2)$ to send it to any other point in this orbit.)

  For each point where at least one of the coordinates differs from the others (of the type $(i,i,j), (i,j,i), (j,i,i)$, or (i,j,k)), its orbit contains the 6 points of the same type. The three points $(1,1,1), (2,2,2)$, and $(3,3,3)$ are all in the same remaining orbit.

- Next, we label the 27 triples:

$$\begin{array}{rrrr}
(1,1,1) \to 1 & (1,1,2) \to 2 & (1,1,3) \to 3 & (1,2,1) \to 4 \\
(1,2,2) \to 5 & (1,2,3) \to 6 & (1,3,1) \to 7 & (1,3,2) \to 8 \\
(1,3,3) \to 9 & (2,1,1) \to 10 & (2,1,2) \to 11 & (2,1,3) \to 12 \\
(2,2,1) \to 13 & (2,2,2) \to 14 & (2,2,3) \to 15 & (2,3,1) \to 16 \\
(2,3,2) \to 17 & (2,3,3) \to 18 & (3,1,1) \to 19 & (3,1,2) \to 20 \\
(3,1,3) \to 21 & (3,2,1) \to 22 & (3,2,2) \to 23 & (3,2,3) \to 24 \\
(3,3,1) \to 25 & (3,3,2) \to 26 & (3,3,3) \to 27 &
\end{array}$$

  So we can describe each permutation in S_3 by how it acts on these elements:

$$\begin{aligned}
1 &\to 1 \\
(1\,2) &\to (1\,14)(2\,13)(3\,15)(4\,11)(5\,10)(6\,12)(7\,17) \\
&\quad (8\,16)(9\,18)(19\,23)(20\,22)(21\,24)(25\,26) \\
(1\,3) &\to (1\,27)(2\,26)(3\,25)(4\,24)(5\,23)(6\,22)(7\,21) \\
&\quad (8\,20)(9\,19)(10\,18)(11\,17)(12\,16)(13\,15) \\
(2\,3) &\to (2\,3)(4\,7)(5\,9)(6\,8)(10\,19)(11\,21)(12\,20) \\
&\quad (13\,25)(14\,27)(15\,26)(16\,22)(17\,24)(18\,23) \\
(1\,2\,3) &\to (1\,14\,27)(2\,15\,25)(3\,13\,26)(4\,17\,21)(5\,18\,19) \\
&\quad (6\,16\,20)(7\,11\,24)(8\,12\,22)(9\,10\,23) \\
(1\,3\,2) &\to (1\,27\,14)(2\,25\,15)(3\,26\,13)(4\,21\,17)(5\,19\,18) \\
&\quad (6\,20\,16)(7\,24\,11)(8\,22\,12)(9\,23\,10)
\end{aligned}$$

- Finally, for each orbit, we choose an element from it and find its stabilizer:

  $(1,1,1)$ has stabilizer $\{1,(2,3)\}$.

  For each remaining orbit, since an element from has at least two coordinates that are different, each non-identity element of S_3 reassigns it, so the stabilizer of all elements from the other orbits is simply the identity.

(b) the set $\mathcal{P}(\{1,2,3\}) - \{\emptyset\}$ of all 7 nonempty subsets of $\{1,2,3\}$.

- There are three orbits, which partition the power set by how many elements each child set contains (ex. one orbit consists of the three singleton sets, namely $\{\{1\},\{2\},\{3\}\}$).
- We label each element:

$$\begin{array}{rrr}
\{1\} \to 1 & \{2\} \to 2 & \{3\} \to 3 \\
\{1,2\} \to 4 & \{1,3\} \to 5 & \{2,3\} \to 6 \\
\{1,2,3\} \to 7 & &
\end{array}$$

So we can describe each permutation in S_3 by how it acts on these elements:

$$\begin{aligned} 1 &\to 1 \\ (1\,2) &\to (1\,2)(5\,6) \\ (1\,3) &\to (1\,3)(4\,6) \\ (2\,3) &\to (2\,3)(4\,5) \\ (1\,2\,3) &\to (1\,2\,3)(4\,6\,5) \\ (1\,3\,2) &\to (1\,3\,2)(4\,5\,6) \end{aligned}$$

- Finally, for each orbit, we choose an element from it and find its stabilizer. In the orbit of singletons, the stabilizer of $\{1\}$ is $\{1, (2\,3)\}$. In the orbit of doubles, the stabilizer of $\{1, 2\}$ is $\{1, (1\,2)\}$. In the orbit that consists only of the triple $\{1, 2, 3\}$, the stabilizer is all of S_3.

6. (1/18/24)

As in Exercise 12 of Section 2.2 let R be the set of all polynomials with integer coefficients in the independent variables x_1, x_2, x_3, x_4 and let S_4 act on R by permuting the indices of the four variables:

$$\sigma \cdot p(x_1, x_2, x_3, x_4) = p(x_{\sigma(1)}, x_{\sigma(2)}, x_{\sigma(3)}, x_{\sigma(4)})$$

for all $\sigma \in S_4$.

(a) Find the polynomials in the orbit of S_4 on R containing $x_1 + x_2$ (recall from Exercise 12 in Section 2.2 that the stabilizer of this polynomial has order 4).

$$\begin{array}{lll} x_1 + x_2 & x_1 + x_3 & x_1 + x_4 \\ x_2 + x_3 & x_2 + x_4 & x_3 + x_4 \end{array}$$

(b) Find the polynomials in the orbit of S_4 on R containing $x_1x_2 + x_3x_4$ (recall from Exercise 12 in Section 2.2 that hte stabilizer of this polynomial has order 8).

$$x_1x_2 + x_3x_4 \qquad x_1x_3 + x_2x_4 \qquad x_1x_4 + x_2x_3$$

(c) Find the polynomials in the orbit of S_4 on R containing $(x_1+x_2)(x_3+x_4)$.

$$(x_1 + x_2)(x_3 + x_4) \qquad (x_1 + x_3)(x_2 + x_4) \qquad (x_1 + x_4)(x_2 + x_3)$$

7. (1/30/24)

Let G be a transitive permutation group on the finite set A. A *block* is a nonempty subset B of A such that for all $\sigma \in G$ either

$$\sigma(B) = B \text{ or } \sigma(B) \cap B = \emptyset$$

(here $\sigma(B)$ is the set $\{\sigma(b) \mid b \in B\}$).

(a) Prove that if B is a block containing the element a of A, then the set G_B defined by $G_B = \{\sigma \in G \mid \sigma(B) = B\}$ is a subgroup of G containing G_a.

Proof. Let $\sigma_1, \sigma_2 \in G_B$. Then $\sigma_1(B) = \sigma_2(B) = B$. We also know that $\sigma_2^{-1}(B) = B$. It follows that:

$$(\sigma_1 \circ \sigma_2^{-1})(B) = \sigma_1(\sigma_2^{-1}(B)) = \sigma_1(B) = B,$$

so by the subgroup criterion, $G_B \leq G$.

Next, for some $a \in B$, let $\tau \in G_a$, so $\tau(a) = a$. Since B is a block, either $\tau(B) = B$ or else $\tau(B) \cap B = \emptyset$. Now $a \in B$ and $\tau(a) = a$. Therefore $\tau(a)$ lies in B, so the intersection of $\tau(B)$ and B is not empty, which implies that $\tau(B) = B$. Therefore $\tau \in G_B$, and so $G_a \subseteq G_B$; since they are both subgroups, we have $G_a \leq G_B$. □

(b) Show that if B is a block and $\sigma_1(B), \sigma_2(B), ..., \sigma_n(B)$ are all the distinct images of B under the elements of G, then these form a partition of A.

Proof. Let $b \in B$ and $\sigma, \tau \in G$. We consider the two cases:

(i) Suppose $b \in \sigma(B)$. If $b \in \tau(B)$, then we have $\sigma(B) = \tau(B) = B$. Otherwise, $\sigma(B) = B$ and $\tau(B) \cap B = \emptyset$, so $\sigma(B)$ and $\tau(B)$ are also disjoint.

(ii) Suppose $b \notin \sigma(B)$. If $b \in \tau(B)$, then as above, $\sigma(B)$ and $\tau(B)$ are disjoint. If $b \notin \tau(B)$, then choose a $c \in \sigma(B)$, and as above, either $\sigma(B) = \tau(B)$ or they are disjoint.

Therefore the images of B form a partition of A. □

(c) A (transitive) group G on a set A is said to be *primitive* if the only blocks in A are the trivial ones: the sets of size 1 and A itself. Show that S_4 is primitive on $A = \{1, 2, 3, 4\}$. Show that D_8 is not primitive as a permutation group on the four vertices of a square.

Proof. Let $G = S_4$ act on $A = \{1, 2, 3, 4\}$, and let B be a block in A. Since blocks form a partition of sets, the order of B must divide A (must be 1, 2, or 4). Without loss of generality, let $4 \in B$. The stabilizer of 4, $G_4 \leq S_4$ is S_3 (from Chapter 3.2, Exercise 15). From part (a), $G_4 \leq G_B \leq G$, so the order of G_B must be greater than or equal to 6 and must divide 24 (must be 6, 12, or 24). We consider these cases separately:

(i) $|G_B| = 6$. Then $|G_4| = |G_B| = 6$, so $G_B = S_3$. Since S_3 contains all transpositions of 1, 2, and 3, it does not fix any of them, and so $B = \{4\}$.

(ii) $|G_B| = 12$. We know that $G_4 = S_3 \leq G_B$. It can be verified that $\langle S_3, \sigma \rangle$ (where $\sigma \in S_4, \sigma \notin S_3$) is all of S_4. Therefore $|G_B|$ cannot have order 12.

(iii) $|G_B| = 24$. Then G_B is all of S_4, and so B must be all of A.

Since B must be a singleton or else all of A, S_4 is primitive on A.

Next, suppose that D_8 acts on the four vertices of a square 1, 2, 3, 4:

$$\begin{array}{llll} r \cdot 1 = 2 & r \cdot 2 = 3 & r \cdot 3 = 4 & r \cdot 4 = 1 \\ s \cdot 1 = 1 & s \cdot 2 = 4 & s \cdot 3 = 3 & s \cdot 4 = 2 \end{array}$$

We claim that the subset $\{1, 3\}$ is a block. We see that $r \cdot \{1, 3\} = \{2, 4\}$, and $s \cdot \{1, 3\} = \{1, 3\}$. So the generators of D_8 either assign $\{1, 3\}$ to a disjoint set or keep it fixed. Then for any element $s^a r^b \in D_8$, we have:

$$(s^a r^b) \cdot \{1, 3\} = s^a \cdot (r^b \cdot \{1, 3\}) = \begin{cases} s^a \cdot \{1, 3\} = \{1, 3\} & \text{if } b \text{ is even} \\ s^a \cdot \{2, 4\} = \{2, 4\} & \text{if } b \text{ is odd} \end{cases}.$$

Therefore any element of D_8 acting on $\{1, 3\}$ satisfies the conditions for it to be a block, and since its size is 2, it is not a trivial block. Therefore D_8 is not primitive on the four vertices of a square. □

(d) Prove that the transitive group G is primitive on A if and only if for each $a \in A$, the only subgroups of G containing G_a are G_a and G (i.e., G_a is a *maximal* subgroup of G, cf. Exercise 16, Section 2.4). [Use part (a).]

Proof. □

8. (1/19/24)

A transitive permutation group G on a set A is called *doubly transitive* if for any (hence all) $a \in A$ the subgroup G_a is transitive on the set $A - \{a\}$.

(a) Prove that S_n is doubly transitive on $\{1, 2, ..., n\}$ for all $n \geq 2$.

Proof. From Chapter 3.2, Exercise 15, the stabilizer of any element of $\{1, 2, ..., n\}$ in S_n is isomorphic to S_{n-1} and consists of all the permutations (in particular, transpositions) of the remaining $n - 1$ elements. Therefore the stabilizer acts transitively on the remaining elements, and S_n is thus doubly transitive. □

(b) Prove that a doubly transitive group is primitive. Deduce that D_8 is not doubly transitive in its action on the 4 vertices of a square.

Proof. Let G be doubly transitive on A. Suppose that $B \subseteq A$ is a block and $a, b \in B$.

Now suppose that $c \in A$ is not in the block B. Since G is doubly transitive, G_a acts transitively on $A - \{a\}$. Therefore there exists $g \in G_a$ such that $c = g \cdot b$. However, since $g \in G_a$, we know that $g \cdot a = a \in B$, which implies that $g \cdot b$ also lies in B, contradicting $c = g \cdot b \notin B$. Then c must *also* lie in the block B, and so B is all of G.

Since any block containing at least two elements must be the entire group, this proves that a doubly transitive group is primitive.

Next, suppose that D_8 acts on the 4 vertices of a square $1, 2, 3, 4$ as in part (c) of the previous exercise. Then the stabilizer of 1 in D_8 — the subgroup $\langle s \rangle$ — is not transitive on $\{2, 3, 4\}$, because there is no element $x \in \langle s \rangle$ such that $2 = x \cdot 3$ (in fact, 3 is a fixed point). Therefore D_8 is not doubly transitive in its action on the 4 vertices of a square. □

9. (2/6/24)

Assume G acts transitively on the finite set A and let H be a normal subgroup of G. Let $\mathcal{O}_1, \mathcal{O}_2, ..., \mathcal{O}_r$ be the distinct orbits of H on A.

(a) Prove that G permutes the sets $\mathcal{O}_1, \mathcal{O}_2, ..., \mathcal{O}_r$ in the sense that for each $g \in G$ and each $i \in \{1, ..., r\}$ there is a j such that $g\mathcal{O}_i = \mathcal{O}_j$, where $g\mathcal{O} = \{g \cdot a \mid a \in \mathcal{O}\}$ (i.e., in the notation of Exercise 7 the sets $\mathcal{O}_1, \mathcal{O}_2, ..., \mathcal{O}_r$ are blocks). Prove that G is transitive on $\{\mathcal{O}_1, \mathcal{O}_2, ..., \mathcal{O}_r\}$. Deduce that all orbits of H have the same cardinality.

Proof. Let $g \in G$, let $a \in \mathcal{O}_i$ for some $i \in \{1, ..., r\}$, and suppose that $g \cdot a \in \mathcal{O}_j$.

First, let $b \in \mathcal{O}_j$. Then there exists $h \in H$ such that $b = h \cdot g \cdot a$. This implies that:

$$b = h \cdot g \cdot a = (hg) \cdot a = g \cdot (g^{-1}hg) \cdot a.$$

Now since $H \trianglelefteq G$, we know that $g^{-1}hg \in H$, so $(g^{-1}hg) \cdot a$ lies in $\mathcal{O}_i$. Therefore $b = g \cdot c$ for some $c \in \mathcal{O}_i$, so $b \in g\mathcal{O}_i$, and $\mathcal{O}_j \subseteq g\mathcal{O}_i$.

Next, let $b = g \cdot c \in g\mathcal{O}_i$. There exists $h \in H$ such that $c = h \cdot a$, so $b = g \cdot h \cdot a$. Then:

$$b = g \cdot h \cdot a = (gh) \cdot a = (ghg^{-1}) \cdot g \cdot a.$$

Now since $g \cdot a \in \mathcal{O}_j$, and $ghg^{-1} \in H$ acting on $g \cdot a$ gives a result that remains in the same orbit, we have $b \in \mathcal{O}_j$, and $g\mathcal{O}_i \subseteq \mathcal{O}_j$.

Thus for each $g \in G$ and each $i \in \{1, ..., r\}$ there is a j such that $g\mathcal{O}_i = \mathcal{O}_j$. This further implies that all orbits of a normal subgroup have the same cardinality, since $g\mathcal{O}_i = \mathcal{O}_j$ implies that $|\mathcal{O}_i| = |\mathcal{O}_j|$. □

(b) Prove that if $a \in \mathcal{O}_1$ then $|\mathcal{O}_1| = |H : H \cap G_a|$ and prove that $r = |G : HG_a|$.

Proof. Note that $H \cap G_a$ consists of those elements of H that are in the stabilizer of a in G, that is, the subgroup of elements of H that stabilize a, denoted H_a. From Proposition 2, the number of elements in any orbit of H is $|H : H \cap G_a$.

Next, let $g \in G$, let $a \in \mathcal{O}_i$ and as in part (a) suppose that $g \cdot a \in \mathcal{O}_j$. Now let $x, y \in gHG_a$. So $x = gh_1g_1$ and $y = gh_2g_2$ for some $h_1, h_2 \in H$ and $g_1, g_2 \in G_a$. Then:

$$x \cdot a = (gh_1g_1) \cdot a = (gh_1) \cdot g_1 \cdot a = (gh_1) \cdot a = g \cdot h_1 \cdot a, \text{ and}$$
$$y \cdot a = (gh_2g_2) \cdot a = (gh_2) \cdot g_2 \cdot a = (gh_2) \cdot a = g \cdot h_2 \cdot a.$$

Since $h_1 \cdot a$ and $h_2 \cdot a$ both lie in $\mathcal{O}_i$, we conclude that $x = g \cdot h_1 \cdot a$ and $y = g \cdot h_2 \cdot a$ both lie in $g\mathcal{O}_i = \mathcal{O}_j$. This shows that r, the number of distinct orbits of H on A, is determined by the number of distinct left cosets of HG_a in G, so $r = |G : HG_a|$. □