Dummit & Foote Ch. 1.7: Group Actions

Scott Donaldson

Apr. 2023

1. (4/27/23)

Let F be a field. Show that the multiplicative group of nonzero elements of F (denoted by $F^\times$) acts on the set F by $g \cdot a = ga$, where $g \in F^\times, a \in F$ and ga is the usual product in F of the two field elements.

Proof. To show that $F^\times$ acts on F, we must show that $g_1 \cdot (g_2 \cdot a) = (g_1 g_2) \cdot a$ for all $g_1, g_2 \in F^\times, a \in F$, and $1 \cdot a = a$ for all $a \in F$.

First, let $g_1, g_2 \in F^\times$ and $a \in F$. By the definition of the action, $g_1 \cdot (g_2 \cdot a) = g_1 \cdot (g_2 a) = g_1 g_2 a$. By the associativity of multiplication, $g_1 g_2 a = (g_1 g_2)a$. Again by the action definition, this equals $(g_1 g_2) \cdot a$.

It follows directly from the field axiom of multiplicative identity that $1 \cdot a = a$ for all $a \in A$. Thus $F^\times$ acts on F by $g \cdot a = ga$. □

2. (4/27/23)

Show that the additive group $\mathbb{Z}$ acts on itself by $z \cdot a = z + a$ for all $z, a \in \mathbb{Z}$.

Proof. First, $z_1 \cdot (z_2 \cdot a) = z_1 \cdot (z_2 + a) = z_1 + z_2 + a = (z_1 + z_2) + a = (z_1 + z_2) \cdot a$.

Also, $0 \cdot a = 0 + a = a$ for all $a \in \mathbb{Z}$. Thus $\mathbb{Z}$ acts on itself by $z \cdot a = z + a$. □

3. (4/27/23)

Show that the additive group $\mathbb{R}$ acts on the x, y plane $\mathbb{R} \times \mathbb{R}$ by $r \cdot (x, y) = (x + ry, y)$.

Proof. First, $r_1 \cdot (r_2 \cdot (x, y)) = r_1 \cdot (x + r_2 y, y) = (x + r_2 y + r_1 y, y) = (x + (r_1 + r_2)y, y) = (r_1 + r_2) \cdot (x, y)$.

Also, $0 \cdot (x, y) = (x + 0y, y) = (x, y)$ for all $(x, y) \in \mathbb{R} \times \mathbb{R}$. Thus $\mathbb{R}$ acts on $\mathbb{R} \times \mathbb{R}$ by $r \cdot (x, y) = (x + ry, y)$. □

4. (4/27/23)

Let G be a group acting on a set A and fix some $a \in A$. Show that the following sets are subgroups of G:

(a) the kernel of the action,

Proof. The kernel of G is the set $\{g \in G \mid g \cdot a = a \text{ for all } a \in A\}$. It is closed under the binary operation of G: If g_1, g_2 are in the kernel, then $g_1 \cdot (g_2 \cdot a) = g_1 \cdot a = a$ for all $a \in A$. And, by definition of a group action, $g_1 \cdot (g_2 \cdot a) = (g_1 g_2) \cdot a$, which implies that $(g_1 g_2) \cdot a = a$, so $g_1 g_2$ is in the kernel of G.

The kernel is also closed under inverses: Let g be in the kernel of G. Then $1 \cdot a = (g^{-1} g) \cdot a = g^{-1} \cdot (g \cdot a) = g^{-1} \cdot a$. By definition, $1 \cdot a = a$, so $g^{-1} \cdot a = a$ for all a, so g^{-1} is in the kernel. Thus the kernel of the action is a subgroup of G. □

(b) $\{g \in G \mid ga = a\}$ — this subgroup is called the *stabilizer* of G.

Proof. The proof that this set of elements if a subgroup is identical to the one immediately above, but for a fixed a as opposed to all $a \in A$. □

5. (4/28/23)

Prove that the kernel of an action of the group G on the set A is the same as the kernel of the corresponding permutation representation $G \to S_A$.

Proof. Let φ be the permutation representation $G \to S_A$ corresponding to G acting on A. Let g be in the kernel of the action of G (to show that $\varphi(g)$ is in the kernel of φ). Then $g \cdot a = a$ for all $a \in A$. If σ_g is the permutation of S_A corresponding to g, then σ_g is the identity permutation, because $\sigma_g(a) = a$ for all $a \in A$. Thus $\sigma_g = \varphi(g)$ is in the kernel of φ.

Next, let $\varphi(g)$ be in the kernel of φ (to show that g is in the kernel of G). Then $\varphi(g)$ is the identity permutation, so $\varphi(g) \cdot a = \sigma_g(a) = a$ for all $a \in A$. Also, by definition, $\sigma_g(a) = g \cdot a$, so $g \cdot a = a$ for all $a \in A$. Thus g is in the kernel of the action of G.

Having shown that membership in one implies membership in the other, this proves that the kernel of G acting on A is thus equal to the kernel of the permutation representation $\varphi : G \to S_A$. □

6. (4/28/23)

Prove that a group G acts faithfully on a set A if and only if the kernel of the action is the set consisting of only the identity.

Proof. First, let G act on A. Suppose that G acts on A faithfully (to show that the kernel of the action of G is the set consisting of only the identity). Consider the permutation representation $\varphi : G \to S_A$. Since G acts on A faithfully, φ is injective (that is, $g_1, g_2 \in G$ induce different permutations $\varphi(g_1), \varphi(g_2)$). Thus the identity permutation $\varphi(1)$ is the only permutation that assigns a to a for all $a \in A$. From 5., the kernel of the action of G is the same as the kernel of φ, so the identity of G is the only element in the kernel of the action of G.

Next, suppose that the kernel of the action of $G = \{1\}$ (to show that G acts on A faithfully). Suppose for some $g_1, g_2 \in G$, we have $\varphi(g_1) = \varphi(g_2)$, that is, $\sigma_{g_1}(a) = \sigma_{g_2}(a)$ for all $a \in A$. Consider the permutation obtained by composing $\varphi(g_1)^{-1} \circ \varphi(g_2)$. Applying the resulting permutation to some $a \in A$ (and saying that $\sigma_{g_1}(a) = \sigma_{g_2}(a) = b$), we obtain $(\varphi(g_1)^{-1} \circ \varphi(g_2))(a) = \sigma_{g_1}^{-1}(\sigma_{g_2}(a)) = \sigma_{g_1}^{-1}(b) = a$. This implies that $\varphi(g_1)^{-1} \circ \varphi(g_2)$ is the identity permutation. Since φ is a homomorphism, $\varphi(g_1)^{-1} \circ \varphi(g_2) = \varphi(g_1^{-1}) \circ \varphi(g_2) = \varphi(g_1^{-1} g_2)$. However, because the kernel of the action of G is $\{1\}$, and from 5., the kernel of φ is also $\{1\}$, this implies that $g_1^{-1} g_2 = 1 \Rightarrow g_1 = g_2$. □

7. (4/29/23)

Prove that the action of the multiplicative group $\mathbb{R}^\times$ on $\mathbb{R}^n$ defined by $\alpha \cdot (r_1, r_2, ..., r_n) = (\alpha r_1, \alpha r_2, ..., \alpha r_n)$ is faithful.

Proof. From 6., a group acts faithfully on a set if and only if the kernel of the action consists only of the group's identity. Therefore, to show that the given action of $\mathbb{R}^\times$ on $\mathbb{R}^n$ is faithful, it suffices to show that the kernel of the action is $\{1\}$.

By definition, the kernel of the action is the set of all $\alpha \in \mathbb{R}$ such that $\alpha \cdot (r_1, r_2, ..., r_n) = (r_1, r_2, ..., r_n)$ for all such elements of $\mathbb{R}^n$. By definition of the group action, then, for an element α of $\mathbb{R}^\times$ to be in the kernel of the action, we must have $\alpha r_1 = r_1, \alpha r_2 = r_2, ..., \alpha r_n = r_n$. The only element for which this holds is 1. Thus the kernel of the action is $\{1\}$, and so $\mathbb{R}^\times$ acts faithfully on $\mathbb{R}^n$. □

8. (4/30/23)

Let A be a nonempty set and let k be a positive integer with $k \leq |A|$. The symmetric group S_A acts on B consisting of all subsets of A of cardinality k by $\sigma \cdot \{a_1, ..., a_k\} = \{\sigma(a_1), ..., \sigma(a_k)\}$.

(a) Prove that this is a group action.

Proof. The identity permutation acts on an arbitrary element of B by $(1) \cdot \{a_1, ..., a_k\} = \{a_1, ..., a_k\}$, as desired.

Further, $\sigma_1 \cdot (\sigma_2 \cdot \{a_1, ..., a_k\}) = \sigma_1 \cdot \{\sigma_2(a_1), ..., \sigma_2(a_k)\} = \{\sigma_1(\sigma_2(a_1)), ..., \sigma_1(\sigma_2(a_k))\} = \{(\sigma_1 \circ \sigma_2)(a_1), ..., (\sigma_1 \circ \sigma_2)(a_k)\} = (\sigma_1 \circ \sigma_2) \cdot \{a_1, ..., a_k\}$.

Together these two equations prove that this action of S_A on B is a group action. $\square$

(b) Describe exactly how the permutations $(1,2)$ and $(1,2,3)$ act on the six 2-element subsets of $\{1,2,3,4\}$.

- $(1,2)\cdot\{1,2\} = \{2,1\} = \{1,2\}$
- $(1,2)\cdot\{1,3\} = \{2,3\}$
- $(1,2)\cdot\{1,4\} = \{2,4\}$
- $(1,2)\cdot\{2,3\} = \{1,3\}$
- $(1,2)\cdot\{2,4\} = \{1,4\}$
- $(1,2)\cdot\{3,4\} = \{3,4\}$
- $(1,2,3)\cdot\{1,2\} = \{2,3\}$
- $(1,2,3)\cdot\{1,3\} = \{2,1\} = \{1,2\}$
- $(1,2,3)\cdot\{1,4\} = \{2,4\}$
- $(1,2,3)\cdot\{2,3\} = \{3,1\} = \{1,3\}$
- $(1,2,3)\cdot\{2,4\} = \{3,4\}$
- $(1,2,3)\cdot\{3,4\} = \{1,4\}$

9. (4/30/23)

Do both parts of the preceding exercise with "ordered k-tuples" in place of "k-element subsets," where the action on k-tuples is defined as above but with set braces replaced by parentheses (note that, for example, the 2-tuples $(1,2)$ and $(2,1)$ are different even though the sets $\{1,2\}$ and $\{2,1\}$ are the same).

(a) The proof is identical to that in 8., but with set braces replaced by parentheses. For the identity permutation, $(1)\cdot(a_1,...,a_k) = (a_1,...,a_k)$. Similarly for arbitrary σ_1, σ_2 and $(a_1,...,a_k)$, the logic holds.

(b) Describe exactly how the permutations $(1,2)$ and $(1,2,3)$ act on the twelve 2-element tuples of $(1,2,3,4)$.

- $(1,2)\cdot(1,2) = (2,1); (1,2)\cdot(2,1) = (1,2)$
- $(1,2)\cdot(1,3) = (2,3); (1,2)\cdot(3,1) = (3,2)$
- $(1,2)\cdot(1,4) = (2,4); (1,2)\cdot(4,1) = (4,2)$
- $(1,2)\cdot(2,3) = (1,3); (1,2)\cdot(3,2) = (3,1)$
- $(1,2)\cdot(2,4) = (1,4); (1,2)\cdot(4,2) = (4,1)$
- $(1,2)\cdot(3,4) = (3,4); (1,2)\cdot(4,3) = (4,3)$
- $(1,2,3)\cdot(1,2) = (2,3); (1,2,3)\cdot(2,1) = (3,2)$
- $(1,2,3)\cdot(1,3) = (2,1); (1,2,3)\cdot(3,1) = (1,2)$

- $(1,2,3)\cdot(1,4)=(2,4); (1,2,3)\cdot(4,1)=(4,2)$
- $(1,2,3)\cdot(2,3)=(3,1); (1,2,3)\cdot(3,2)=(1,3)$
- $(1,2,3)\cdot(2,4)=(3,4); (1,2,3)\cdot(4,2)=(4,3)$
- $(1,2,3)\cdot(3,4)=(1,4); (1,2,3)\cdot(4,3)=(4,1)$

10. (5/4/23)

With reference to the two preceding exercises determine:

(a) for which values of k the action of S_n on k-element subsets is faithful, and

(b) for which values of k the action of S_n on ordered k-tuples is faithful.

For the action of S_n on k-element subsets, the action is faithful if $n > 1$ and $k < n$.

Proof. In the case where $n = 1$, then the action is trivially faithful (because the symmetric group S_n consists only of the identity).

So suppose that $n > 1$ and let $k < n$, with B the set of all k-element subsets of $A = \{1, 2, ..., n\}$. Let $\sigma \in S_n$ be a non-identity permutation. Then σ assigns at least one element of A to a different element of A. Suppose that $\sigma(a_1) = a_2$ for some $a_1, a_2 \in A$. Because $k < n$, there exists a subset $b \in B$ such that $a_1 \in b$ and $a_2 \notin b$. Then $\sigma \cdot b = \{\sigma(a_1), ...\} = \{a_2, ...\} \neq b$, and so σ is not in the kernel of the action. Therefore the kernel of the action consists only of the identity permutation, and so the action is faithful.

Now, let $n > 1$ and let $k = n$. Then B, the set of all k-element subsets of $A = \{1, 2, ..., n\}$, consists only of A itself. Now let $\sigma \in S_n$ and let $a_1, a_2 \in A$ with $\sigma(a_1) = a_2$. For all $b \in B$ (because $b = A$), $a_1, a_2 \in b \Rightarrow \sigma(a_2) \in b$. Therefore $\sigma \cdot b = b$ for all $b \in B$. Thus every permutation of S_n is in the kernel of the action, and so the action is not faithful.

This proves that the action of S_n on k-element subsets is faithful if and only if $n > 1$ and $k < n$. □

For the action of S_n on ordered k-tuples, the action is faithful for all values of k (if $n > 1$).

Proof. As above, the action is trivially faithful if $n = 1$, so suppose that $n > 1$, let σ be a non-identity permutation in S_n, and let $1 \leq k \leq n$, such that B is the set of all k-element tuples of $A = \{1, 2, ..., n\}$ (ex. $(1, 2)$ and $(2, 1) \in B$). Let $a_1 \in A$ and let $a_2 = \sigma(a_1)$. Let b be the k-tuple consisting only of a_1, that is, $\underbrace{(a_1, ..., a_1)}_{k \text{ times}}$. Then $\sigma \cdot b = \sigma \cdot (a_1, ..., a_1) = (\sigma(a_1), ..., \sigma(a_1)) = (a_2, ..., a_2)$. Then for all non-identity $\sigma \in S_n$, there exists a $b \in B$ such that $\sigma \cdot b \neq b$. Therefore the only permutation in the kernel of the action is the identity permutation, and so the action is faithful for all values of k. □

11. (5/4/23)

Write out the cycle decomposition of the eight permutations in S_4 corresponding to the elements of D_8 given by the action of D_8 on the vertices of a square.

- $1 : (1)$
- $r : (1, 2, 3, 4)$
- $r^2 : (1, 3)(2, 4)$
- $r^3 : (1, 4, 3, 2)$
- $s : (2, 4)$
- $sr : (1, 4)(2, 3)$
- $sr^2 : (1, 3)$
- $sr^3 : (1, 2)(3, 4)$

12. (5/5/23)

Assume n is an even positive integer and show that D_{2n} acts on the set consisting of pairs of opposite vertices of a regular n-gon. Find the kernel of this action.

Proof. Let A be the set of pairs of opopsite vertices of a regular n-gon:

$$\big\{\{1, \frac{n}{2}+1\}, \{2, \frac{n}{2}+2\}, ..., \{\frac{n}{2}-1, n-1\}\big\}.$$

We will show that the following is an action of D_{2n} on the element $\{k, \frac{n}{2}+k\} \in A, 1 \leq k < \frac{n}{2}$ defined on the generators of D_{2n}:

- $s \cdot \{k, \frac{n}{2}+k\} = \{n-k+1, \frac{n}{2}-k+1\}$, and
- $r \cdot \{k, \frac{n}{2}+k\} = \{k+1, \frac{n}{2}+k+1\}$, where all values are taken mod n.

In order to prove that this is a group action, we will show that the relations of D_{2n} hold when acting on elements of A, that is, for all $a \in A$, we have $a = 1 \cdot a = (s^2) \cdot a = s \cdot s \cdot a$, that $a = 1 \cdot a = (r^n) \cdot a = \underbrace{r \cdot ... \cdot r}_{n \text{ times}} \cdot a$, and finally, that $s \cdot r \cdot a = r^{-1} \cdot s \cdot a$.

First, $s \cdot s \cdot \{k, \frac{n}{2}+k\} = s \cdot \{n-k+1, \frac{n}{2}-k+1\}$ by definition. In turn, this equals $\{n-(n-k+1)+1, \frac{n}{2}-(n-k+1)+1\} = \{k, -\frac{n}{2}+k\}$. Since all values are taken mod n, $-\frac{n}{2}+k = \frac{n}{2}+k$, and so $s \cdot s \cdot \{k, \frac{n}{2}+k\} = \{k, \frac{n}{2}+k\}$. Therefore $s \cdot s \cdot a = a$ for all $a \in A$.

Next, to show that $\underbrace{r \cdot ... \cdot r}_{n \text{ times}} \cdot a = a$, we will first prove by induction that $\underbrace{r \cdot ... \cdot r}_{m \text{ times}} \cdot \{k, \frac{n}{2}+k\} = \{k+m, \frac{n}{2}+m\}, m \geq 0$. The base case $r \cdot \{k, \frac{n}{2}+k\} =$

$\{k{+}1, \frac{n}{2}{+}k{+}1\}$ holds by definition. So suppose for some m, $\underbrace{r \cdot \ldots \cdot r}_{m \text{ times}} \cdot \{k, \frac{n}{2}{+}k\} = \{k+m, \frac{n}{2}+m\} \pmod{n}$. Then:

$$\underbrace{r \cdot \ldots \cdot r}_{m+1 \text{ times}} \cdot \{k, \frac{n}{2}+k\} = r \cdot \underbrace{r \cdot \ldots \cdot r}_{m \text{ times}} \cdot \{k, \frac{n}{2}+k\} = r \cdot \{k+m, \frac{n}{2}+k+m\} = \{k+(m+1), \frac{n}{2}+k+(m+1)\}.$$

Thus the induction case holds, and so:

$$\underbrace{r \cdot \ldots \cdot r}_{n \text{ times}} \cdot a = \underbrace{r \cdot \ldots \cdot r}_{n \text{ times}} \cdot \{k, \frac{n}{2}+k\} = \{k+n, \frac{n}{2}+k+n\} = \{k, \frac{n}{2}+k\} = a \text{ for all } a \in A.$$

Finally, to show that $s \cdot r \cdot a = r^{-1} \cdot s \cdot a$, we first note that $r^{-1} \cdot a = \{k-1, \frac{n}{2}+k-1\}$. Now:

$$\begin{aligned} s \cdot r \cdot \{k, \tfrac{n}{2}+k\} &= & r^{-1} \cdot s \cdot \{k, \tfrac{n}{2}+k\} &= \\ s \cdot \{k+1, \tfrac{n}{2}+k+1\} &= & r^{-1} \cdot \{n-k+1, \tfrac{n}{2}-k+1\} &= \\ \{n-(k+1)+1, \tfrac{n}{2}-(k+1)+1\} &= & \{n-k, \tfrac{n}{2}-k\}. & \\ \{n-k, \tfrac{n}{2}-k\}, \text{ and} & & & \end{aligned}$$

Therefore $s \cdot r \cdot a = r^{-1} \cdot s \cdot a$ for all $a \in A$. Together, these relations show that the above is a group action.

We will now consider the kernel of this action. This consists of elements $s^{\{0,1\}}r^m$ of D_{2n} such that $s^{\{0,1\}}r^m \cdot a = a$ for all $a \in A$. We will consider the two cases r^m and sr^m separately.

- r^m: From above, $r^m \cdot \{k, \frac{n}{2}+k\} = \{k+m, \frac{n}{2}+k+m\}$ for all $m \geq 0$. Clearly $m = 0 \Rightarrow r = 1$ satisfies this equality. Since values are taken mod n and these are sets, not tuples, also note that $k = \frac{n}{2}+k+m \Rightarrow 0 = \frac{n}{2}+m \Rightarrow m = \frac{n}{2}$. So among elements of the form r^m, only 1 and $r^{n/2}$ are in the kernel of the action.

- sr^m: From above, $sr^m \cdot \{k, \frac{n}{2}+k\} = s \cdot \{k+m, \frac{n}{2}+k+m\} = \{n-(k+m)+1, \frac{n}{2}-(k+m)+1\}$. Considering the first elements of each set together, we have $k = n-(k+m)+1 \Rightarrow 2k = n-m+1 \Rightarrow m = 1-2k$. Since k is variable, we cannot fix m, and so there is no value of m for which $sr^m \cdot a = a$ for all $a \in A$.

Thus the kernel of this action is $\{1, r^{n/2}\}$. $\square$

13. (5/5/23)

Find the kernel of the left regular action.

Proof. The left regular action of G on itself is defined by $g \cdot a = ga$ for $g, a \in G$. The kernel of this action consists of all $g \in G$ such that $ga = a$ for all $a \in G$. Let $a \in G$ and suppose that $ga = a$ for some $g \in G$. By definition of the group identity, $1 \cdot a = a$, so $ga = 1 \cdot a$. We right-multiply both sides by a^{-1} to obtain $g = 1$. Then the kernel of the left regular action is $\{1\}$, and so the action is faithful. □

14. (5/5/23)

Let G be a group and let $A = G$. Show that if G is non-abelian then the maps defined by $g \cdot a = ag$ for all $g, a \in G$ do *not* satisfy the axioms of a (left) group action of G on itself.

Proof. Since G is non-abelian, there exist $g_1, g_2 \in G$ such that $g_1 g_2 \neq g_2 g_1$. Then for all $a \in G$:

$$g_1 \cdot g_2 \cdot a = g_1 \cdot (ag_2) = ag_2 g_1 \neq ag_1 g_2 = (g_1 g_2) \cdot a.$$

Thus this map is not a group action for non-abelian groups. □

15. (5/12/23)

Let G be any group and let $A = G$. Show that the maps defined by $g \cdot a \mapsto ag^{-1}$ for all $g, a \in G$ *do* satisfy the axioms of a (left) group action of G on itself.

Proof. For the identity, $1 \cdot a = a(1^{-1}) = a$ for all $a \in G$.

Then, for all $g_1, g_2 \in G$, $g_1 \cdot g_2 \cdot a = g_1 \cdot (ag_2^{-1}) = ag_2^{-1}g_1^{-1} = a(g_1 g_2)^{-1} = (g_1 g_2)^{-1} \cdot a$.

Therefore this satisfies the axioms of a group action of G on itself. □

16. (5/12/23)

Let G be any group and let $A = G$. Show that the maps defined by $g \cdot a \mapsto gag^{-1}$ for all $g, a \in G$ *do* satisfy the axioms of a (left) group action of G (this action of G on itself is called *conjugation*).

Proof. As in 15., the requirement for identity is trivial, since $1 = 1^{-1}$.

Then, for all $g_1, g_2 \in G$, we have:

$$g_1 \cdot g_2 \cdot a = g_1 \cdot (g_2 a g_2^{-1}) = g_1 g_2 a g_2^{-1} g_1^{-1} = (g_1 g_2) a (g_1 g_2)^{-1} = (g_1 g_2) \cdot a,$$

as desired. Therefore conjugation satisfies the axioms of a group action of G on itself. □

17. (5/12/23)

Let G be a group and let G act on itself by left conjugation, so each $g \in G$ maps G to G by $x \mapsto gxg^{-1}$. For fixed $g \in G$, prove that conjugation by g is an isomorphism from G onto itself. Deduce that x and gxg^{-1} have the same order for all $x \in G$ and that for any subset A of G, $|A| = |gAg^{-1}|$ (here $gAg^{-1} = \{gag^{-1} \mid a \in A\}$).

Proof. Let $g \in G$ and let $\varphi_g : G \to G$ be defined by $\varphi_g(x) = gxg^{-1}$. We will show that φ_g is a homomorphism, is injective, and is surjective; it follows then that φ_g is an automorphism of G.

Let $x, y \in G$. Then $\varphi_g(x)\varphi_g(y) = gxg^{-1}gyg^{-1} = gxyg^{-1} = \varphi_g(xy)$. Thus φ_g is a homomorphism.

Next, to show that φ_g is one-to-one, let $\varphi_g(x) = \varphi_g(y)$. Then $gxg^{-1} = gyg^{-1}$. Right-multiplying by g^{-1} and then left-multiplying by g, we obtain $x = y$, so φ_g is injective.

Lastly, to show that φ_g is onto, let $z \in G$. Let $x = g^{-1}zg$. Then $\varphi_g(x) = gxg^{-1} = gg^{-1}zgg^{-1} = z$, so φ_g is surjective. Since it is a bijective homomorphism, φ_g is thus an automorphism of G.

Since φ is an automorphism that uniquely maps x to gxg^{-1}, we deduce that $|x| = |gx^{-1}|$ (from Ch. 1.6, exercise 2.). It follows that, for any $A \subseteq G$, $gAg^{-1} \subseteq G$ contains as many elements (of equal order) as does A. □

18. (5/12/23)

Let H be a group acting on a set A. Prove that the relation $\sim$ on A defined by

$$a \sim b \text{ if and only if } a = hb \text{ for some } h \in H$$

is an equivalence relation. (For each $x \in A$ the equivalence class of x under $\sim$ is called the *orbit* of x under the action of H. The orbits under the action of H partition the set A.)

Proof. In order to show that $\sim$ is an equivalence relation on A, we must show that, for all $a, b, c \in A$, i) $a \sim a$; ii) $a \sim b \Rightarrow b \sim a$, and iii) $a \sim b, b \sim c \Rightarrow a \sim c$.

First, for all $a \in A$, $1_H \cdot a = a$ (by definition of a group action), so $a \sim a$.

Next, suppose that $a \sim b$. Then $a = hb$ for some $h \in H$. This implies that $b = h^{-1}a$, and since h^{-1}, it follows that $b \sim a$ as well.

Finally, suppose that $a \sim b$ and $b \sim c$. Then $a = h_1 b, b = h_2 c$ for some $h_1, h_2 \in H$. Then $a = h_1 h_2 c$, and since H is closed under its group operation, the product $h_1 h_2 \in H$, so $a \sim c$.

Thus $\sim$ is an equivalence relation on A. □

19. (5/15/23)

Let H be a subgroup of the finite group G and let H act on G by left multiplication. Let $x \in G$ and let $\mathcal{O}$ be the orbit of x under the action of H. Prove that the map $H \to \mathcal{O}$ defined by $h \mapsto hx$ is a bijection (hence that all orbits have cardinality $|H|$). From this and the preceding exercise deduce *Lagrange's Theorem*:

if G is a finite group and H is a subgroup of G then $|H|$ divides $|G|$.

Proof. To show that the map from the subgroup H to the orbit $\mathcal{O}$ of $x \in G$ defined by left multiplication is a bijection, let $\varphi : H \to \mathcal{O}$ be defined by $\varphi(h) = hx$. We will show that φ is injective and surjective.

First, to show that φ is one-to-one, let $\varphi(y_1) = \varphi(y_2)$ for $y_1, y_2 \in H$. Then $y_1x = y_2x$, which implies that $y_1 = y_2$, so φ is injective.

Next, to show that φ is onto, let $z \in \mathcal{O}$ (to show that $z = \varphi(y)$ for some $y \in H$). Since z is in the orbit of the given element x, $x = hz$ for some $h \in H$. Then $z = h^{-1}x$, which implies that $z = \varphi(h^{-1})$, and since H is a subgroup of G and is therefore closed under inverses, φ is surjective.

Since φ is a bijection from the subgroup H to $\mathcal{O}$, the orbit of x, the two have the same cardinality. From 18., the orbits of the elements of G partition G; that is, the orbits of x and y under the action of H are either disjoint or equal. Let $|H| = |\mathcal{O}| = n$. There are $|G| - n$ elements in G not in the orbit of x under the action of H. For another element $y \in G$, either the orbit of y is equal to the orbit of x, or it contains $|H| = n$ elements, and in the case of the latter, there are $|G| - 2n$ elements in G not in the orbits of x and y. Continuing this process for each element of G, the orbit of each element must contain n elements and we must eventually arrive at 0 remaining elements, so $|G| = kn$, that is, the order of the subgroup H divides the order of G. □