



DISCRETE MATHEMATICS 2

ANTONIO MONTERO

*Office 5.17
FMF - University of Ljubljana*

2. GROUP ACTIONS

In the previous section we reviewed basic properties of permutation groups. In this section we will focus on a slightly more general notion, which is that of *group actions*. Informally speaking, group actions are a tool that allows us to treat any group as a permutation group. Formally speaking:

Definition 2.1. Given a group G with neutral element 1 and a set X a *(left) group action* of G on X is a function $\varphi: G \times X \rightarrow X$ that satisfies

- (a) $\varphi: (1, x) \mapsto x$ for every $x \in X$
- (b) $\varphi(gb, x) = \varphi(g, \varphi(b, x))$ for every $g, b \in G$ and $x \in X$.

We usually omit φ and think of a group action as a way to “evaluate” a group element onto an element of X . In fact, if φ is a left group action, then we usually denote by gx the element $\varphi(g, x) \in X$. With this notation, the element $\varphi(gb, x)$ should be denoted by $(gb)x$ (we first multiply the elements in the group and then evaluate), whereas the element $\varphi(g, \varphi(b, x))$ should be written as $g(bx)$ (we first evaluate b on x and then evaluate g on the resulting element). Thanks to [Item \(b\)](#) of [Definition 2.1](#), we can write gbx without the need of parentheses. If G acts on a set X we say that X is a G -set.

Words of caution: Some authors use *right* group actions, which can be defined in a similar way (see [Exercise 2.1](#)). The main difference is the order in which we evaluate the elements, if we take $g, b \in G$ and we evaluate it (on the left) in an element x we first evaluate b and then we evaluate g . While if we evaluate the same group element on a right action we first consider the action of g on x and then the action of b on the resulting element. This two operations does

E-mail address: antonio.montero@fmf.uni-lj.si.

not need to be the same. The choice of one side or another is related to the fact that we evaluate permutations on the left. As before, this choice has usually little theoretical consequences, but one needs to be careful (see [Exercise 2.1](#)).

We list several examples of group actions below.

Example 2.2. Naturally, if X is any set then the symmetric group S_X acts on the set X in the obvious way:

$$\varphi(\sigma, x) = \sigma(x).$$

Example 2.3. Both the dihedral group and the cyclic group acts on the set $[n]$ by restricting of S_n to the D_n and C_n , respectively. However, both group also act on the set of edges of a n -cycle (equivalently, a regular n -gon) when they are interpreted as symmetries.

Example 2.4. In fact, the previous examples show a obvious but important way to find actions. If G is a permutation group of S_n then G acts naturally on the set $[n]$.

If G is a permutation group, we say that G is of *degree* n if it acts on $[n]$. Some authors also require that there is no $k \in \{1, \dots, n\}$ such that $\sigma(k) = k$ for ever $\sigma \in G$, so that S_3 when interpreted as the subgroup of permutations in S_4 that fix 4 is a group of degree 3 but not of degree 4. We shall make that assumption whenever we refer to a group of degree n .

[Example 2.4](#) suggest a way to find group actions. In fact, it is not hard to see that every group action is essentially given as in this example.

Proposition 2.5. *Let G be a group acting on a set X with the action $\varphi: G \times X \rightarrow X$. The mapping $\rho_\varphi: G \rightarrow S_X$ given by $\rho_\varphi(g): x \mapsto gx$ defines a group homomorphism. Conversely, every group homomorphism $\rho: G \rightarrow S_X$ induces an action of G on X by $gx = \rho(g)(x)$.*

Proof. See [Exercise 2.2](#). □

Example 2.6. Another natural way of finding examples of group actions is by consider the *symmetry group* of geometric figures. That is, the set of symmetries of the space that preserve a given figure. For example, the symmetry group of the cube acts on the set $\{1, 2, 3, 4, 5, 6, 7, 8\}$ of vertices, the set $\{a, b, c, d, e, f, g, h, i, j, k, l\}$ of edges and the set $\{A, B, C, D, E, F\}$ of faces (just to mention some). The 3-fold rotation R on the line that connects the vertices 1 and 7 induce the following permutations the sets of vertices, edges and faces:

$$\begin{aligned} (2\ 5\ 4)(3\ 6\ 8) & \text{ on vertices,} \\ (a\ d\ e)(i\ b\ h)(f\ c\ l)(j\ g\ k) & \text{ on edges,} \\ (A\ B\ C)(D\ E\ F) & \text{ on faces.} \end{aligned}$$

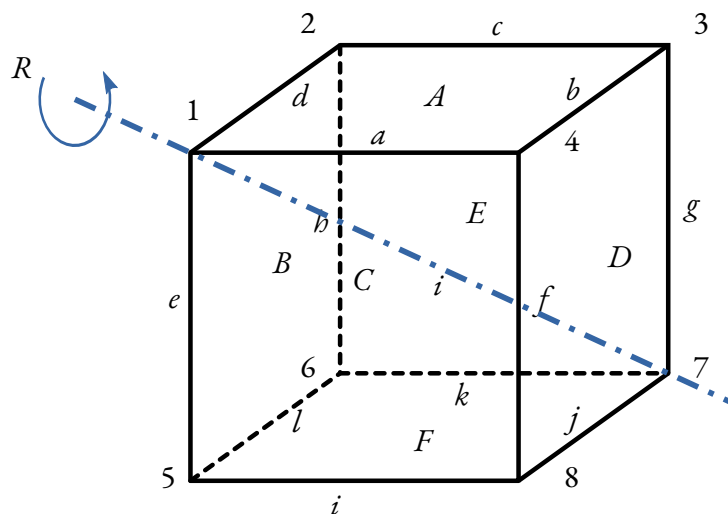


FIGURE 1. A rotation of the cube

Example 2.7. Every group G acts on itself by left multiplication. That is, the action is given by $(g, x) \mapsto gx$ for every $g, x \in G$. If G is finite, say $|G| = n$ the representation $\mu_l: G \rightarrow S_n$ defined by $\mu_l(g) = \gamma_g$ where $\gamma_g: G \rightarrow G$ is given by $\gamma_g(x) = gx$. Yet again, observe that the side for which we multiply is relevant so that μ_l is actually a group-homomorphism, i.e.

$$\gamma_{hg} = \mu_l(hg) = \mu_l(h)\mu_l(g) = \gamma_h\gamma_g.$$

The left-most permutation of G in the equation above maps x to $(hg)x$ while the right-most maps x to $\gamma_h(gx) = h(gx)$.

Observe that μ_l is injective. In fact if $\mu_l(g) = \varepsilon$, then $gx = \gamma_g(x) = x$ for every x , which implies that $g = 1$.

The G acts on a set X , the *kernel* of the action is the kernel of the induced representation of G in S_X . We say that an action is *faithful* whenever the its kernel is the trivial subgroup. Equivalently, when the associated representation is injective.

The group homomorphism μ_l in [Example 2.7](#) is often called the (left) Cayley representation of G . This homomorphism proves the following theorem.

Theorem 2.8 (Cayley, 1854). *Every finite group with n elements is isomorphic to a subgroup of S_n .*

Even though [Theorem 2.8](#) is more than one hundred years old, it has current relevance. Permutation groups are concrete objects compared to an abstract group. In particular, permutation groups can be understood by a programming language. Unfortunately, the theorem as it is has little practical applications. If a group G is relatively large, the symmetric group on $|G|$ symbols is extremely

complicated. However, the truth is that every faithful action induces an injective homomorphism, so in order to find a representation of an abstract group as a permutation group we only need to find a faithful action. For example, the group G of symmetries of the cube has 48 elements, [Theorem 2.8](#) says that G is isomorphic to a subgroup of S_{48} , which has size $48!$. Yet, the action of G on the set of vertices is faithful so G has a representation in S_8 . Moreover, the action on the set of faces is also faithful, which implies that G has a representation of degree 6. It is an active research area to find small (minimal) permutation representations of relevant families of finite groups.

Unfortunately, most actions are not faithful. Let us show an example of it.

Example 2.9. Let G be a group and H a subgroup of G . The set X of left cosets of H is a G -set. The action is given by

$$g(xH) = gxH.$$

This action is generally not faithful. If K is a normal subgroup of H then $x^{-1}kx \in K \subseteq H$ for every $k \in K$, which implies that

$$kxH = xH \text{ for every } k \in K$$

Definition 2.10. If $H \leq G$ are groups, then the *normal core* (or simply, the *core*) of H in G is the largest normal subgroup of G contained in H , that is

$$\text{Core}_G(H) = \bigcap_{g \in G} g^{-1}Hg$$

Example 2.11. If G is a group, then G is itself a G -set where the action is given by (left) conjugation, that is, the action of a given element g on x is given by

$$g : x \mapsto gxg^{-1}.$$

The kernel of this action is the *centre* $Z(G)$.

Example 2.12. Similarly, G acts on the set $X = \{H : H \text{ is subgroup of } G\}$ by $g : H \mapsto gHg^{-1}$.

The intuitive idea of a group G acting on a set X is that every element of G move the elements of X . It makes sense to consider the following important concepts.

Definition 2.13. Assume that G acts on a set X . Given $x \in X$, the *orbit* of x is the set

$$Gx = \{gx : g \in G\}.$$

The *stabiliser* of x is the subgroup (see [Exercise 2.5](#))

$$\text{Stab}_G(x) = \{g \in G : gx = x\}.$$

For a given $g \in G$ the set of *fixed points* is the set

$$\text{Fix}(g) = \{x \in X : gx = x\}.$$

The set of *fixed points* of G is the set

$$\text{Fix}(G) = \{x \in X : gx = x \text{ for all } g \in G\} = \bigcap_{g \in G} \text{Fix}(g)$$

It is important to remark that some authors denote these sets differently. A common notation for the orbit of x is $O(x)$ and the stabiliser is sometimes denoted G_x (see [Rot96], for example). The set of fixed points of an element g and of the group G are sometimes denoted X_g and X_G , respectively.

Observe that the relation $\sim$ in X given by $x \sim y$ if and only if $Gx = Gy$ is an equivalence relation (Exercise 2.4). Therefore this relation defines a partition of X in equivalence classes given by the orbits. The latter implies the following straightforward result.

Proposition 2.14. *The set of orbits induces a partition of X . If $R \subseteq X$ is a set of representatives containing exactly one element for each non-trivial orbit, then*

$$X = \text{Fix}(G) \cup \left(\bigcup_{x \in R} Gx \right)$$

In particular, if X is finite, then

$$|X| = |\text{Fix}(G)| + \left(\sum_{x \in R} |Gx| \right).$$

Let X and Y be two G sets with actions φ_X and φ_Y , respectively. We say that X and Y are *equivalent* (as G -sets) if there exists a bijection $\eta : X \rightarrow Y$ such that the following diagram commutes:

$$\begin{array}{ccc} G \times X & \xrightarrow{(\varepsilon, \eta)} & G \times Y \\ \downarrow \varphi_X & & \downarrow \varphi_Y \\ X & \xrightarrow{\eta} & Y \end{array}$$

That is, if

$$\eta(\varphi_X(g, x)) = \varphi_Y(g, \eta(x))$$

Observe that if X is a G -set and $Z \subseteq X$ is such that $gz \in Z$ for ever $g \in G$, then Z is a G -set. In particular, the orbit of every element of a G -set X is a G -set itself.

Now we present a straightforward but very useful result, sometimes even called the *fundamental theorem of group actions*.

Theorem 2.15 (Orbit-Stabiliser Theorem). *Let G be a group acting on a set X and let $x \in X$. The orbit Gx of x and the set of left cosets of $\text{Stab}_G(x)$ are equivalent as G -sets. In particular,*

$$|Gx| = [G : \text{Stab}_G(x)].$$

If G is finite, then

$$|Gx| = \frac{|G|}{|\text{Stab}_G(x)|}$$

Proof. Let S denote the subgroup $\text{Stab}_G(x)$. Consider the mapping $\phi : G/S \rightarrow Gx$ given by $\phi(gS) = gx$. First notice that ϕ is well-defined. Indeed if $gS = hS$ then $h^{-1}g \in S$, that is $h^{-1}gx = x$, which implies that $gx = hx$.

Similarly, if g and h are elements in G such that $gx = hx$, then $gS = hS$. In other words, ϕ is injective. Clearly ϕ is surjective. The bijection ϕ defines an equivalence of G -sets. $\square$

We finish this section with some important definitions.

Definition 2.16. Let G be a group acting on a set X . We say that the action is *transitive* if there is only one orbit. That is, if for every two elements $x, y \in X$ there exists a group element g such that $gx = y$.

We say that the action is *free* or *semiregular* if the stabiliser of every element is the trivial group. Finally, we say that an action is *regular* if it is both transitive and semiregular.

Exercises.

2.1 A *right action* of a group G on a set X is mapping $\psi : X \times G \rightarrow X$ such that

- $\psi : (x, 1) \mapsto x$ for every $x \in X$
- $\psi(x, gh) = \psi(\psi(x, g), h)$.

We usually denote $\psi(x, g)$ by xg .

- (a) Prove that if $\phi : G \times X \rightarrow X$ is a left action, then the mapping $\psi : X \times G \rightarrow X$ defined by $\psi(x, g) = \phi(g^{-1}, x)$ defines a right action.
 - (b) Conversely, if $\psi : X \times G \rightarrow X$ is a right action, the mapping $\phi : G \times X \rightarrow X$ given by $\phi(g, x) = \psi(x, g^{-1})$ defines a left action.
 - (c) Give an example of a left action ϕ such that the mapping $\psi : X \times G \rightarrow X$ given by $\psi(x, g) = \phi(g, x)$ is not a right action.
- 2.2 Proof that every action of a group G on a set X induces a group homomorphism $G \rightarrow S_X$ and conversely, that every such homomorphism induces an action of G on X .
- 2.3 Let G and H be groups. A *group antimorphism* is a function $\phi : G \rightarrow H$ that satisfies that

$$\phi(g_1g_2) = \phi(g_2)\phi(g_1),$$

for every $g_1, g_2 \in G$.

- (a) Prove that if $\phi_1 : G \rightarrow H$ and $\phi_2 : H \rightarrow K$ are group antimorphisms, then $\phi_2 \circ \phi_1 : G \rightarrow K$ is a group homomorphism.
- (b) Show that $(\)^{-1} : G \rightarrow G$ given by $g \mapsto g^{-1}$ is a group antimorphism.

- (c) Conclude that right actions of G to X are incorrespondence with group antimorphisms $G \rightarrow S_X$.
- 2.4 If G is a set acting on a set X , then the relation on X defined by $x \sim y$ if and only if $Gx = Gy$ defines an equivalence relation on X .
- 2.5 Prove that the stabiliser of a point is a subgroup of G .
- 2.6 Let X and Y two G -sets. Prove that $X \times Y$ is a G set with the action $g(x, y) = (gx, gy)$. Prove that the stabiliser of (x, y) is $\text{Stab}_G(x) \cap \text{Stab}_G(y)$. Show an example where X and Y are transitive but $X \times Y$ is not.
- 2.7 Show that if $x, y \in X$ belong to the same orbit, then $\text{Stab}_G(x)$ and $\text{Stab}_G(y)$ are conjugate.
- 2.8 Let X be a transitive G -set. Let S denote the subgroup $\text{Stab}_G(x)$ of a point x . Prove that the core of S on G is precisely the kernel of the action. Prove that this is not necessarily true if X is not transitive.
- 2.9 If G is a group, a *core-free* subgroup of G is a subgroup H such that $\text{Core}_G(H)$ is trivial. Show that every transitive faithful action of G is equivalent to the left-coset action of a core-free subgroup of G .
- 2.10 Let H and K subgroup of G , then G is a union of disjoint *double cosets*
- $$HgK = \{h g k \in G : h \in H, k \in K\}.$$
- 2.11 If G is finite, then the size of a double coset HgK is $|K| \times [H : (gKg^{-1} \cap H)]$.
Let G be a group acting transitively on a set X . Let H be a subgroup of G and let S denote the subgroup $\text{Stab}_G(x)$. Prove that the following statements are equivalent
- (a) $G = SH$,
 - (b) $G = HS$,
 - (c) H is transitive.
- In particular, the only transitive subgroup of G containing S is G itself.
- 2.12 If G contains a subgroup H of index n , then it contains a normal subgroup $K \leq H$ such that $[G : K]$ is finite and divides $n!$.
- 2.13 if G is a finite group of order m , and p is the smallest prime which divides m , then any group of index p is normal in G .
- 2.14 Let $n \geq 5$, then the only proper subgroup of index less than n in the symmetric group S_n is the alternating group A_n of index 2.
- 2.15 Prove that there is no simple group of order 56.
- 2.16 Prove that there is no simple noncyclic group of order $2^m p^n$ where $m \in \{1, 2, 3\}$ and p is an odd prime.
- 2.17 For $n \geq 2$, $n - 2$ transposition cannot generate a transitive group of degree n (Compare with Exercise 1.8)
- 2.18 Let G be a group acting faithfully on a set X . Assume that G has finitely many orbits $X_1, \dots, X_k$. Notice that G acts transitively on each subset X_i ($i \in \{1, \dots, k\}$). Prove that G is isomorphic to a subgroup of $S_{X_1} \times \dots \times S_{X_k}$.

- 2.19 Let G be a group of order p^k with p prime and $k \in \mathbb{N}$. Assume that G acts faithfully on a set X with $|X| = n$ where $n \leq p^2$. Prove that $G \cong \mathbb{Z}_p \times \cdots \times \mathbb{Z}_p$.
- 2.20 Let G be an abelian group. Prove that if G acts transitively on a set X , then the action is regular.
- 2.21 Find the order of the symmetry group of the cube and the order of the symmetry group of a regular icosahedron.
- 2.22 If G is a finite non-trivial p -group (that is, a group such that $|G| = p^k$ for some $k \in \mathbb{N}$), then $Z(G)$ is not trivial. **Hint:** consider the action in [Example 2.11](#).
- 2.23 Let p be a prime such that $p \equiv 1 \pmod{4}$. Consider the set

$$X = \{(x, y, z) \in \mathbb{N}^3 : x + 4yz = p\}.$$

Consider the mapping

$$\phi : (x, y, z) \mapsto \begin{cases} (x + 2z, z, y - x - z) & \text{if } x < y - z \\ (2y - x, y, x - y + z) & \text{if } y - z < x < 2y \\ (x - 2y, x - y + z, y) & \text{if } x > 2y \end{cases}$$

- (a) Prove that ϕ is a permutation of order 2 on X with exactly one fixed point.
- (b) Prove that the permutation $\psi : (x, y, z) \mapsto (x, z, y)$ must also have at least one fixed point.
- (c) Prove a famous theorem in number theory: An odd prime p is a sum of two squares if and only if $p \equiv 1 \pmod{4}$.

REFERENCES

- [Arm88] Mark A. Armstrong. *Groups and Symmetry*. en. Undergraduate Texts in Mathematics. New York: Springer-Verlag, 1988. ISBN: 9780387966755. DOI: [10.1007/978-1-4757-4034-9](https://doi.org/10.1007/978-1-4757-4034-9). URL: <https://www.springer.com/gp/book/9780387966755> (visited on 08/16/2021).
- [BW79] Norman L. Biggs and A. T. White. *Permutation Groups and Combinatorial Structures*. Cambridge University Press, Aug. 1979. DOI: [10.1017/cbo9780511600739](https://doi.org/10.1017/cbo9780511600739).
- [Cam99] Peter J. Cameron. *Permutation Groups*. Cambridge University Press, Feb. 1999. DOI: [10.1017/cbo9780511623677](https://doi.org/10.1017/cbo9780511623677).
- [DM96] John D. Dixon and Brian Mortimer. *Permutation groups*. Vol. 163. Graduate Texts in Mathematics. Springer-Verlag, New York, 1996, pp. xii+346. ISBN: 0-387-94599-7. DOI: [10.1007/978-1-4612-0731-3](https://doi.org/10.1007/978-1-4612-0731-3). URL: <http://dx.doi.org/10.1007/978-1-4612-0731-3>.

- [Rot96] Joseph J. Rotman. *A first course in abstract algebra*. Prentice Hall, Inc., Upper Saddle River, NJ, 1996, pp. xiv+265. ISBN: 0-13-311374-4.