7.3 The alternating group A_n

Definition 7.3.1. The *alternating group of degree n*, denoted A_n, is the group of all even permutations in S_n. In other words, $A_n = \{g \in S_n : \sigma(g) = 1\}$. (We should prove this is a group - we do this in the handout).

Theorem 7.3.2. *If $n \geq 2$, then* $|A_n| = \dfrac{|S_n|}{2} = \dfrac{n!}{2}$.

Here is a short proof using the First Isomorphism Theorem.

Proof. Suppose $n \geq 2$. Recall Proposition 7.2.2: the map $\sigma : S_n \to \{1, -1\}$ is a homomorphism. Note that $\sigma(e) = 1$ and $\sigma((1\ 2)) = -1$, so the image of σ is $\{1, -1\}$. The kernel of σ is $\{g \in S_n : \sigma(g) = 1\}$ — however, this is the precise definition of A_n. Therefore,

$$\text{Im}(\sigma) = \{1, -1\} \quad \text{and} \quad \text{Ker}(\sigma) = \text{A}_\text{n}.$$

By the First Isomorphism Theorem,

$$S_n \,/\, \text{Ker}(\sigma) \cong \text{Im}(\sigma).$$

Isomorphic groups have the same size, so $\dfrac{|S_n|}{|\text{Ker}(\sigma)|} = |\text{Im}(\sigma)|$. Therefore $|A_n| = |S_n|/2$. □

Example 7.3.3. Let's list all elements of A_3. We could list all elements in S_3 and then calculate their signatures, throwing out those with signature -1. However, this doesn't work well for larger groups like A_5, A_6, etc because it gets too complicated. Instead we analyse the possible cycle shapes, like we did in Question 7.1.3. Then we need only list all permutations with the correct cycle shape.

Consider the following table of cycle shapes in S_3.

Cycle shape	Example of this cycle shape	Signature	In A_3?
$\varnothing$	e	1	Yes
(2)	(1 2)	-1	No
(3)	(1 2 3)	1	Yes

To list all elements in A_3 we only need to list all permutations in S_3 with cycle shapes $\varnothing$ and (3). This is the identity plus all possible 3-cycles. Hence:

$$A_3 = \{e, (1\ 2\ 3), (1\ 3\ 2)\} = C_3.$$

Example 7.3.4. The cycle shapes in S_4 are $\varnothing, (2), (2,2), (3)$ and (4). The cycle shapes whose signature is 1 are $\varnothing$, $(2,2)$ and (3). All permutations with this cycle shape therefore lie in A_4. One could then use this to list all elements in A_4. On a problem sheet you will list all elements of A_5 using this method.

Theorem 7.3.5. $A_n \trianglelefteq S_n$

Proof. Fix $g \in S_n$ and $h \in A_n$. Recall that the signature function σ is a homomorphism and $\sigma(h) = 1$. Hence,

$$\sigma(g^{-1}hg) = \sigma(g^{-1})\sigma(h)\sigma(g) = \sigma(g^{-1})\sigma(g) = \sigma(g^{-1}g) = \sigma(e) = 1.$$

Therefore $g^{-1}hg \in A_n$. □

Remark 7.3.6. Recall that a group G is simple if it has no normal subgroups other than the trivial group $\langle e \rangle$ and G itself. The groups A_1 and A_2 are $\langle e \rangle$ and so they are simple. As we saw in Example 7.3.3, $A_3 = C_3$ and so A_3 is also simple. Now A_4 is not simple ($K_4 \trianglelefteq A_4$), but as we shall see A_n is simple for $n \geq 5$.

Theorem 7.3.7. A_n *is simple for* $n \geq 5$.

7.3.1 Handout for Section 7.3

Proof that A_n is a group. By definition $A_n \subseteq S_n$, so we can use the Quick Subgroup Test.

Identity: It's easy to see that $e\Delta = \Delta$, so $\sigma(e) = 1$. The identity is therefore an even permutation. Hence $e \in A_n$.

Closure: If $g, h \in A_n$ then $\sigma(g) = 1$ and $\sigma(h) = 1$. Since σ is a homomorphism, we have $\sigma(gh) = \sigma(g)\sigma(h) = 1$. Hence $gh \in A_n$.

Inverse: If $g \in A_n$, then $\sigma(g) = 1$. We know $\sigma(g) = \sigma(g^{-1})$ by Proposition 7.2.5. Hence $\sigma(g^{-1}) = 1$, so $g^{-1} \in A_n$.

Hence A_n satisfies the Quick Subgroup Test, so $A_n \leq S_n$. □

Outline of the proof that A_n is simple for $n \geq 5$. We only give a sketch proof here, since the full proof is very long. This proof is not examinable of course.

- First show that every element of A_n can be written as a product of 3-cycles. Hence A_n is the group generated by all 3-cycles in S_n.
  - (i) Every element in A_n is a product of 2-cycles, and moreover must be the product of an even number of 2-cycles because $\sigma(g) = 1$.
  - (ii) One uses induction to prove that if $g \in A_n$ is the product of $2k$ 2-cycles, then g can also be written as a product of 3-cycles.
  - (iii) The induction step is to write $g = (a_1\ b_1)(a_2\ b_2)h$, where $h \in A_n$ is the product of $2(k-1)$ 2-cycles, then examine the cases where $|\{a_1, b_1\} \cap \{a_2, b_2\}| = 0, 1, 2$ separately, showing that in each case $g = \rho h$ where ρ is e or a product of 3-cycles.
- Second show that if $H \trianglelefteq A_n$ contains a 3-cycle, then it contains all 3-cycles (and hence equals A_n).
  - (i) Suppose $(a_1\ a_2\ a_3) \in H$ and recall that A_n contains every 3-cycle.
  - (ii) Choose $b \notin \{a_1, a_2, a_3\}$ and $z \neq \{a_1, a_2, a_3, b\}$ (which we can do because $n \geq 5$).
  - (iii) Now $(a_1\ z\ b) \in A_n$ because it is a 3-cycle and so $(a_1\ z\ b)^{-1}(a_1\ a_2\ a_3)(a_1\ z\ b) \in H$ because $H \trianglelefteq A_n$
  - (iv) Hence $(a_1\ z\ b)^{-1}(a_1\ a_2\ a_3)(a_1\ z\ b) = (b\ a_2\ a_3) \in H$
  - (v) Of course $(b\ a_2\ a_3) = (a_2\ a_3\ b)$; hence we can repeat above trick to show any 3-cycle $(b\ c\ d)$ lies in H
- Third show that if $\langle e \rangle \neq H \trianglelefteq A_n$ then H contains a 3-cycle.
  - (i) Choose $h \in H$ with $h \neq e$ and write h as a product of disjoint cycles $h = c_1 c_2 \cdots c_m$.
  - (ii) If one cycle in h is a 3-cycle and all others are 2-cycles then $h^2 \in H$ is a 3-cycle
  - (iii) If the longest cycle in h has length at least 4, then one can find a 3-cycle ρ such that $\rho h \rho^{-1} h^{-1} \in H$ is a 3-cycle.
  - (iv) If this is not the case, then one can always find a 3-cycle ρ such that $\rho h \rho^{-1} h^{-1} \in H$ is a 5-cycle. Hence we can take h now to be this 5-cycle and then by the previous step (iii) we have that H contains a 3-cycle.
- Summary: if $\langle e \rangle \neq H \trianglelefteq A_n$, then H contains a 3-cycle and therefore it contains all 3-cycles. Hence $H = A_n$. Thus the only normal subgroups of A_n are $\langle e \rangle$ and A_n, so A_n is simple.

□

8 Group Actions

8.1 G-sets

Motivation. Every group is a permutation group! Often in more than one way!

Definition 8.1.1. Let G be a group and X be a set. An *action* of G on X is a function λ such that for all $g \in G$ and all $x \in X$ there is an element $\lambda(g)x \in X$ that satisfies:

1. $\lambda(e_G)x = x \quad \forall x \in X$;
2. $\lambda(fg)x = \lambda(f)(\lambda(g)x) \quad \forall f, g \in G$ and $\forall x \in X$

If there exists an action of G on X, we say that G *acts on* X, and we call X a G-set.

Example 8.1.2. If $X = \{1, 2, \ldots, n\}$ and $G = S_n$, then X is a G-set, where the action is given by $\lambda(g)x = gx$ for all $g \in G$ and $x \in X$. E.g. $\lambda((123))3 = 1$.

Example 8.1.3. If X is any set and G is any group, then X is a G-set via the *trivial action*, where $\lambda(g)x = x$ for all $g \in G$ and all $x \in X$.

Proposition 8.1.4. *If X is a G-set and $g \in G$, then $\lambda(g)$ is a permutation of X. Moreover, λ is a homomorphism from G to* $\mathrm{Sym}(X)$.

Proof. Fix $g \in G$ and note that $\lambda(g) : X \to X$ is a function, so we just need to check it is a bijection.

One-to-one: if $\lambda(g)x = \lambda(g)y$ then $\lambda(g^{-1})(\lambda(g)x) = \lambda(g^{-1})(\lambda(g)y)$. By property 2 of the action, this implies that $\lambda(e_G)x = \lambda(e_G)y$. Property 1 of the action now implies that $x = y$.

Onto: fix $y \in X$, and let $x := \lambda(g^{-1})y \in X$. Now $\lambda(g)x = \lambda(g)(\lambda(g^{-1})y) = y$.

We have shown that $\lambda(g)$ is one-to-one and onto, so it is a bijection from X to X; in other words it is a permutation of X.
Hence λ is a function from G to $\mathrm{Sym}(X)$. It is a homomorphisms because for all $f, g \in G$ we have that $\lambda(fg)$ and $\lambda(f)\lambda(g)$ give the same permutation of X. In other words, $\lambda(fg) = \lambda(f)\lambda(g)$. □

Remark 8.1.5. We have just seen that every action λ of G on a set X is a homomorphism from G to $\mathrm{Sym}(X)$. This means we can talk about the kernel and image of an action.

Notation. Often we drop the symbol λ, and write gx instead of $\lambda(g)x$.

What is the point?!. A group action describes precisely how a group behaves as a collection of symmetries (i.e. permutations) of a set. It allows us to turn every group into a permutation group!

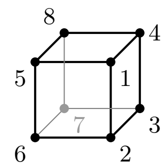
Example 8.1.6. When we think of D_8 and the way it permutes the corners of a square, that is an example of a group action where $\lambda(\rho)1 = 2$ and $\lambda(\rho)2 = 3$ and $\lambda(\rho)3 = 4$ and $\lambda(\rho)4 = 1$ for example.

Example 8.1.7 (Important example)**.** Every group acts on itself by left multiplication. This is called a *regular action.* In this setting, $X = G$ and $\lambda(g)x = gx$ for all $g \in G$ and all $x \in X = G$.

Example 8.1.8 (Important example)**.** Every group acts on itself by *conjugation.* This is called the *(left) conjugation action.* In this setting, $X = G$ and $\lambda(g)x = gxg^{-1}$, for all $g \in G$ and all $x \in X = G$.

8.1.1 Handout for Section 8.1

Example 8.1.9. (Easy example). Consider $G = D_8$, the group of symmetries of a square. Also consider the cube $\mathcal{C}$ below.



As we know, D_8 is the group of symmetries of the square with corners 1–2–3–4. However, one can also see how any symmetry of the square 1–2–3–4 moves the rest of the cube in a natural way. This is D_8 acting on the cube.

Formally, recall $D_8 = \{e, \rho, \rho^2, \rho^3, \sigma, \sigma\rho, \sigma\rho^2, \sigma\rho^3\}$, where $\rho = (1\ 2\ 3\ 4)$ and $\sigma = (1\ 4)(2\ 3)$. Now define an action λ of D_8 on the corners $\{1, 2, 3, 4, 5, 6, 7, 8\}$ of $\mathcal{C}$ by,

$$\lambda(\rho) = (1\ 2\ 3\ 4)(5\ 6\ 7\ 8) \quad \text{and} \quad \lambda(\sigma) = (1\ 4)(2\ 3)(5\ 8)(6\ 7) \quad \text{and} \quad \lambda(\sigma^i\rho^j) = \lambda(\sigma)^i\lambda(\rho)^j.$$

It is easy to check that λ is an action of D_8 on $\mathcal{C}$ by simply checking that conditions (1) and (2) from Definition 8.1.1 hold.

Non-Example 8.1.10. Let G be a group and $X = G$ be a set. The following is *not* in general an action: $\lambda(g)x = g^{-1}xg$ for all $g \in G$ and $x \in X$.

To see why, notice that on one hand $\lambda(gf)x = (gf)^{-1}x(gf) = f^{-1}g^{-1}xgf$, but on the other hand $\lambda(g)(\lambda(f)x) = \lambda(g)(f^{-1}xf) = g^{-1}f^{-1}xfg$.
For some groups, $g^{-1}f^{-1}xfg$ might equal $f^{-1}g^{-1}xgf$ (can you think of an example?) but in general these two terms will not be equal.