MATH 323, Algebra I, Fall 2020

Course notes, Chapter 6, The symmetric and alternating groups

Laurence Barker, Bilkent University. Version: 30 November 2020.

These notes, updated as the course progresses, are a record of the prepared text of the lectures, with a little more detail added, but they cannot cover much of the oral component of the lectures.

Summary of contents

We shall be making a study of two particular families of groups, namely, the symmetric groups and the alternating groups.

Fuller details of the material we shall be covering can be found in Judson, mostly in Chapter 5. These notes are independent of that text.

We shall be reviewing the notions of:

- a **simple group**,
- a **partition** of an integer, and the **shape** of an element of S_n,
- the **alternating groups** A_n.

We shall be discussing:

- cycle notation for elements of S_n,
- the conjugacy classes of S_n,
- the conjugacy classes of an index 2 normal subgroup and, in particular, the conjugacy classes of A_5.
- The simplicity of A_n for $n \geq 5$.

Simple groups: For a group G, we define a **strict subgroup** of G to be a subgroup H of G such that $H \neq G$. When H is a strict subgroup of G, we write $H < G$. When H is a strict normal subgroup of G, we write $H \lhd G$.

We define a **proper subgroup** of G to be a non-trivial strict subgroup of G. In other words, the proper subgroups of G are the H such that $1 < H < G$.

We call G **simple** provided G is non-trivial and has no proper normal subgroup. In other words, G is simple if and only if there does not exist H such that $1 \lhd H \lhd G$. The next remark is obvious.

Remark 6.1: *The simple abelian groups are precisely the groups that are isomorphic to a finite cyclic group C_p of prime order p.*

Suppose the group G is finite and non-simple. Choose a proper normal subgroup $1 \lhd H \lhd G$. Loosely speaking, we might view G as a group constructed by starting with

the normal subgroup H and then extending to G by gluing G/H on top of H. But there can be more than one way of accomplishing that gluing. To express the point precisely: the isomorphism classes of H and G/H do not determine the isomorphism class of G. Indeed, if $|G| = 4$, then there are two possibilities for G up to isomorphism, $G \cong C_4$ or $G \cong V_4$ yet, in both cases, G is abelian, hence any proper subgroup H of G is and satisfies $H \cong G/H \cong C_2$.

Nevertheless, for any finite group G, we can construct a chain

$$1 = H_0 \lhd H_1 \lhd ... \lhd H_{n-1} \lhd H_n = G$$

where, for each m in the range $1 \leq m \leq n$, the quotient group H_m/H_{m-1} is simple.

Review of the definition of the finite symmetric groups: Recall, given a set Ω, a bijection $\Omega \leftarrow \Omega$ is called a **permutation** of Ω. The set of permutations of Ω, denoted $\mathrm{Sym}(\Omega)$, becomes a group whose operation is composition of functions. We call $\mathrm{Sym}(\Omega)$ the **symmetric group** on Ω. Below, we shall be concerned with the case where Ω is finite.

For the rest of this chapter, we let n be a positive integer. We write $[1, n]_{\mathbb{Z}}$ to denote the set of positive integers less than or equal to n. That is, $[1, n]_{\mathbb{Z}} = \{x \in \mathbb{Z} : 1 \leq x \leq n\}$. In particular, for instance, $[1, 4]_{\mathbb{Z}} = \{1, 2, 3, 4\}$. We mention that many writers prefer the slightly simpler but occasionally ambiguous notation $\{1, ..., n\}$ instead of $[1, n]_{\mathbb{Z}}$.

The group

$$S_n = \mathrm{Sym}([1, n]_{\mathbb{Z}})$$

is called the **symmetric group with degree** n. Note that, given any finite set Ω then, putting $n = |\Omega|$, we can choose an enumeration $\Omega = \{w_1, ..., w_n\}$, whereupon there is an isomorphism

$$\theta \ : \ \mathrm{Sym}(\Omega) \leftarrow S_n$$

such that, for each $g \in S_n$ and $x \in [1, n]_{\mathbb{Z}}$, we have

$$\theta(g) w_x = w_{g(x)} \ .$$

In other words, if g sends the element $x \in [1, n]_{\mathbb{Z}}$ to an element $y \in [1, n]_{\mathbb{Z}}$, $\theta(g)$ sends the element $w_x \in \Omega$ to the element $w_y \in \Omega$. Thus, the study of S_n can be viewed as a study of $\mathrm{Sym}(\Omega)$ for any set Ω of size n. To put it another way, we can pass from $\mathrm{Sym}(\Omega)$ to S_n by replacing w_1, ..., w_n with 1, ..., n, respectively.

Remark 6.2: *The order of S_n is $|S_n| = n!$.*

Proof: To choose an element g of S_n, there are n choices for $g(1)$, then $n - 1$ choices for $g(2)$, and so on, finally 2 choices for $g(n - 1)$ and 1 choice for $g(n)$. $\square$

Cycle notation: We shall establish some notation for expressing elements of the symmetric group S_n.

For distinct elements $x_1, ..., x_m$ of $[1, n]_{\mathbb{Z}}$, we write $(x_1, ..., x_m)$ to denote the element of S_n such that, given $x \in [1, n]_{\mathbb{Z}}$, then

$$(x_1, ..., x_m)(x) = \begin{cases} x_{i+1} & \text{if } x = x_i \text{ with } 1 \leq i \leq m-1, \\ x_1 & \text{if } x = x_m, \\ x & \text{otherwise.} \end{cases}$$

The first two conditions can be neatly combined by saying that $(x_1, ..., x_m)(x_i) = x_{i+1}$ for any $i \in [1, m]_{\mathbb{Z}}$, where $i + 1$ is to be interpreted modulo m. We mean, x_{m+1} is to be interpreted as x_1. We call the element $(x_1, ..., x_m)$ a **cycle** or an m**-cycle**.

Two cycles $(x_1, ..., x_m)$ and $(x'_1, ..., x'_{m'})$ are said to be **disjoint** provided the sets $\{x_1, ..., x_m\}$ and $\{x'_1, ..., x'_{m'}\}$ are disjoint. Plainly,

$$(x_1, ..., x_m)(x'_1, ..., x'_{m'})(x'_1, ..., x'_{m'})(x_1, ..., x_m)$$

when we have disjointness $\{x_1, ..., x_m\} \cap \{x'_1, ..., x'_{m'}\} = \emptyset$. That is to say, mutually disjoint cycles commute.

To give some examples, in S_6, consider the cycle $a = (2, 4, 5)$. Then

$$a(1) = 1\ , \quad a(2) = 4\ , \quad a(3) = 3\ , \quad a(4) = 5\ , \quad a(5) = 2\ , \quad a(6) = 6\ .$$

The cycle $b = (3, 6)$ is such that $b(3) = 6$ and $b(6) = 3$ and $b(x) = x$ for all $x \in \{1, 2, 4, 5\}$. The sets $\{2, 4, 5\}$ and $\{3, 6\}$ are disjoint. Thus, a and b are disjoint cycles and $ab = ba$.

Below, we shall show that any element of S_n can be expressed as a product of mutually disoint cycles. First, let us give another example. Take g to be the element of S_8 specified by the following table.

x	1	2	3	4	5	6	7	8
$g(x)$	3	6	7	4	8	2	1	5

Thus, for instance, $g(1) = 3$ and $g(2) = 6$. Let us construct, in a step-by-step way, an expression for g as a product of mutually disjoint cycles. The process can be viewed as a template which can be applied to any explicitly specified element of S_n, for any positive integer n.

- First, without even looking at the specification of g, we write: "(1,".
- Noting that g sends 1 to 3, we write "(1, 3,".
- Noting that $g(3) = 7$, we write: "(1, 3, 7".
- Noting that $g(7) = 1$, we write: "(1, 3, 7)".
- The smallest of the remaining numbers is 2, and $g(2) = 6$. We write "(1, 3, 7)(2,".
- Noting that $g(2) = 6$, we write: "(1, 3, 7)(2, 6".
- Noting that $g(6) = 2$, we write: "(1, 3, 7)(2, 6)".
- The smallest remaining number is 4, and $g(4) = 4$. We write "(1, 3, 7)(2, 6)(4)".
- The smallest remaining number is 5, and $g(5) = 8$. We write "(1, 3, 7)(2, 6)(4)(5, 8".
- We have $g(8) = 6$. We write "(1, 3, 7)(2, 6)(4)(5, 8)".

Finally, we have arrived at an expression for g as a product of mutually disjoint cycles,

$$g = (1, 3, 7)(2, 6)(4)(5, 8)\ .$$

The 1-cycle (4) is the identity element. So, more briefly,

$$g = (1,3,7)(2,6)(5,8) \ .$$

Of course, to achieve the stated aim, there is no need for the rule that we start with 1, nor for the rule that we choose the smallest remaining number whenever freedom of choice arises. A minor benefit in following those two rules is that it yields g a standard form, with smallest numbers first wherever possible. When two elements of a symmetric group are written in that standard form, it becomes very easy to see whether or not they are equal. Another way of expressing g as a product of cycles is

$$g = (2,6)(8,5)(3,7,1) \ .$$

Before describing the process in general, it will be helpful to first establish some notation.

Consider a subgroup $H \leq S_n$. We define a relation $\equiv_H$ on $[1,n]_{\mathbb{Z}}$ such that, given $x, y \in [1,n]_{\mathbb{Z}}$, then $x \equiv_H y$ provided $x = hy$ for some $h \in H$. Trivially, $\equiv_H$ is reflexive. Since H is closed under inversion, $\equiv_H$ is symmetric. Since H is closed under multiplication, $\equiv_H$ is transitive. We have proved that $\equiv_H$ is an equivalence relation. The equivalence class of x under $\equiv_H$ is called the **H-orbit** of x. By a general property of equivalence relations, $[1,n]_{\mathbb{Z}}$ is the disjoint union of the H-orbits.

Lemma 6.3: *Let $g \in S_n$ and $x \in [1,n]_{\mathbb{Z}}$. Let m be the smallest integer such that x, gx, g^2x, ..., $g^{m-1}x$ are mutually distinct. Then $g^m x = x$, and $\{x, gx, g^2x, ..., g^{m-1}x\}$ is the $\langle g \rangle$-orbit of x.*

Proof: By the hypothesis on m, we have $g^m x = g^i x$ for some $0 \leq i \leq m-1$. If $i \neq 0$, then $g^{i-1}x = g^{m-1}x$, which contradicts the mutual distinctness. Therefore $i = 0$, in other words, $g^m = x$. The rider follows. □

For any $g \in S_n$, we can write

$$[1,n]_{\mathbb{Z}} = \{x_{1,1}, ..., x_{1,m_1}\} \sqcup \{x_{2,1}, ..., x_{2,m_2}\} \sqcup ... \sqcup \{x_{r,1}, ..., x_{r,m_r}\}$$

as a disjoint union where, for each $1 \leq i \leq r$, the set $\{x_{i,1}, ..., x_{i,m_i}\}$ is a $\langle g \rangle$-orbit. By the latest lemma, we can choose the enumerations such that each $gx_{i,j} = x_{i,j+1}$, where j is interpreted as a modulo m_i congruence class. Then

$$g = (x_{1,1}, ..., x_{1,m_1})(x_{2,1}, ..., x_{2,m_2})...(x_{r,1}, ..., x_{r,m_r})$$

as a product of disjoint cycles. We have proved the following result.

Proposition 6.4: *Any element of S_n can be expressed as the product of mutually disjoint cycles.*

The conjugacy classes of S_n: We define **partition** of the positive integer n to be a tuple $(m_1, m_2, ..., m_r)$ of positive integers m_1, m_2, ..., m_r such that $m_1 \geq m_2 \geq ... \geq m_r$ and $m_1 + m_2 + ... + m_r = n$. Throughout most of the literature, partitions are written

with the brackets omitted and the commas replaced by + signs. Thus, we speak of the partition

$$m_1 + m_2 + ... + m_r = (m_1, m_2, ..., m_r) \ .$$

Of course, this is a dire abuse of notation. The sum $m_1 + ... + m_r$ and the partition $m_1 + ... + m_r$ are two quite different things. We rely on context to resolve any ambiguity.

Warning: when a writer uses the standard phrase "we rely on context to resolve the ambiguity", it means that he or she will take care to ensure that the meaning of an expression will be clear from the surrounding words. When you employ the notation $m_1 + ... + m_r$ for a partition, you must compose the accompanying text in such a way as to let the reader know you are referring to a partition, not a sum. If you are not writing in complete sentences, then you are likely to get into trouble here!

Again, let $g \in S_n$, and write

$$g = (x_{1,1}, ..., x_{1,m_1})(x_{2,1}, ..., x_{2,m_2})...(x_{r,1}, ..., x_{r,m_r})$$

as a product of disjoint cycles, including all the 1-cycles. Then $m_1 + ... + m_r = n$. Since mutually disjoint cycles commute, we can choose the numbering such that $m_1 \geq ... \geq m_r$. Then the partition $m_1 + ... + m_r$ is called the **shape** of g. Thus, the shape of g is the partition consisting of the sizes of the $\langle g \rangle$-orbits, arranged in non-increasing order.

Lemma 6.5: *Let x_1, ..., x_m be mutually distinct elements of $[1, n]_{\mathbb{Z}}$. Let $t \in S_n$. Then, as cycles in S_n, we have $t(x_1, ...x_m)t^{-1} = (t(x_1), ..., t(x_m))$.*

Proof: Write $g = (x_1, ..., x_m)$. Let $y \in [1, n]_{\mathbb{Z}}$. If $y = tx_i$ for some $i \in [1, m]_{\mathbb{Z}}$, then $tgt^{-1}y = tgx_i = tx_{i+1}$, with the index i interpreted modulo m. If y is not of the form tx_i, then $t^{-1}y$ is not of the form x_i, hence $tgt^{-1}y = tt^{-1}y = y$. $\square$

Proposition 6.6: *Let $g, h \in S_n$. Then g and h are conjugate if and only if g and h have the same shape.*

Proof: Write

$$g = (x_{1,1}, ..., x_{1,m_1})(x_{2,1}, ..., x_{2,m_2})...(x_{r,1}, ..., x_{r,m_r})$$

with $m_1 + ... + m_r = n$ and $m_1 \geq ... \geq m_r$. Thus, the shape of g is the partition $m_1 + ... + m_r$. Suppose h is conjugate to g, say, $h = tgt^{-1}$ with $t \in S_n$. Using the previous lemma,

$$tgt^{-1} = t(x_{1,1}, ..., x_{1,m_1})t^{-1}.t(x_{2,1}, ..., x_{2,m_2})t^{-1}...t(x_{r,1}, ..., x_{r,m_r})t^{-1}$$

$$= (tx_{1,1}, ..., tx_{1,m_1})(tx_{2,1}, ..., tx_{2,m_2})...(tx_{r,1}, ..., tx_{r,m_r}) \ .$$

Hence h has shape $m_1 + ... + m_r$.

Conversely, suppose h has shape $m_1 + ... + m^r$. Then

$$h = (y_{1,1}, ..., y_{1,m_1})(y_{2,1}, ..., y_{2,m_2})...(y_{r,1}, ..., y_{r,m_r})$$

where the $y_{i,j}$ are the elements of $[1, n]_{\mathbb{Z}}$, each element appearing exactly once. Let t be the element of S_n such that $y_{i,j} = tx_{i,j}$ for all i and j. The calculation in the previous paragraph shows that $h = tgt^{-1}$. $\square$

For any $g \in S_n$, we define the **shape** of the conjugacy class $[g]_{S_n}$ to be the shape of g. The latest proposition says that all the elements of $[g]_{S_n}$ have the same shape, in other words, the shape of $[g]_{S_n}$ is well-defined. The next result is just a reformulation of the latest proposition.

Theorem 6.7: *There is a bijective correspondence between the partitions $m_1 + ... + m_r$ of n and the conjugacy classes $[g]_{S_n}$ of the elements g of S_n whereby $m_1 + ... + m_r \leftrightarrow [g]_{S_n}$ if and only if $m_1 + ... + m_r$ is the shape of $[g]_{S_n}$.*

To illustrate the material above in this section, let g and t be the elements of S_8 specified by the following table.

x	1	2	3	4	5	6	7	8
$g(x)$	3	6	7	4	8	2	1	5
$t(x)$	5	1	8	6	4	3	2	7

In the previous section, we saw that $g = (1,3,7)(2,6)(5,8)$. Including the 1-cycle,

$$g = (1,3,7)(2,6)(5,8)(4) \ .$$

So g has shape $3+2+2+1$. We shall make a comparison with tgt^{-1}. To calculate tgt^{-1}, we first determine t^{-1}, then gt^{-1}, then finally tgt^{-1}, as shown in the next table.

x	1	2	3	4	5	6	7	8
$t^{-1}(x)$	2	7	6	5	1	4	8	3
$gt^{-1}(x)$	6	1	2	8	3	4	5	7
$tgt^{-1}(x)$	3	5	1	7	8	6	4	2

Applying the method above,

$$tgt^{-1} = (1,3)(2,5,8)(4,7)(6)$$

which has shape, again, $3 + 2 + 2 + 1$.

To illustrate the proof of Proposition 6.6, let us also note that, since disjoint cycles commute,

$$tgt^{-1} = (2,5,8)(1,3)(4,7)(6)$$

and, since $(2,5,8) = (5,8,1)$, we have

$$tgt^{-1} = (5,8,1)(1,3)(4,7)(6) = (t(1),t(3),t(7))(t(2),t(6))(t(5),t(8))(t(4)) \ .$$

The latest expression for tgt^{-1} is the same as an above expression for g, but with each element x of $[1,8]_{\mathbb{Z}}$ replaced by $t(x)$.

Details of the conjugacy classes of S_n for $n \leq 5$: We shall describe the conjugacy classes of S_n for all positive integers n less than or equal to 5.

The first two cases are quite banal but, to be comprehensive, let us cover them. There is exactly 1 partition of 1, and there is exactly one conjugacy class of S_n, namely, $\{1\}$. The partitions of 2 are $1+1$ and 2. The corresponding conjugacy classes of S_2 are $[1]_{S_2} = \{1\}$ and $[(1,2)]_{S_2} = \{(1,2)\}$, respectively.

The case $n = 3$ is very easy too. The partitions of 3 are $1 + 1 + 1$ and $2 + 1$ and 3. The conjugacy classes corresponding to those partitions are

$$[1]_{S_3} = \{1\} \ , \quad [(1,2)]_{S_3} = \{(1,2),(1,3),(2,3)\} \ , \quad [(1,2,3)]_{S_3} = \{(1,2,3),(1,3,2)\}$$

respectively. The correspondence is summarized in the next table.

partition	conjugacy class	size of class
$1+1+1$	$[1]_{S_3}$	1
$2+1$	$[(1,2)]_{S_3}$	3
3	$[(1,2,3)]_{S_3}$	2

To construct similar tables for S_4 and S_5 is not much harder. Any element of S_4 with shape $2 + 1 + 1$ has the form $(a, b) = (b, a)$ where $a, b \in \{1, 2, 3, 4\}$. So the number of such (a, b) is the number of subsets $\{a, b\} \subset \{1, 2, 3, 4\}$. That number is $4.3/2 = 6$. So $|[(1,2)]_{S_4}| = 6$. Similar arguments yield the sizes of the other conjugacy classes. Note that

$$[(1,2)(3,4)]_{S_4} = \{(1,2)(3,4),(1,3)(2,4),(1,4)(2,3)\} \ .$$

We obtain the following table for S_4.

partition	conjugacy class	size of class
$1+1+1+1$	$[1]_{S_4}$	1
$2+1+1$	$[(1,2)]_{S_4}$	6
$2+2$	$[(1,2)(3,4)]_{S_4}$	3
$3+1$	$[(1,2,3)]_{S_4}$	8
4	$[(1,2,3,4)]_{S_4}$	6

As a check, we note the the sum of the sizes of the conjugacy classes of S_4 is

$$|S_4| = 4! = 24 = 1 + 6 + 3 + 8 + 6 \ .$$

The same techniques yield the following table for the conjugacy classes of S_5. For instance, any 5-cycle in S_5 can be written uniquely in the form $(1, b, c, d, e)$ where $\{b, c, d, e\} = \{2, 3, 4, 5\}$, so the number of 5-cycles in S_5 is $4.3.2.1 = 24$.

partition	conjugacy class	size of class
$1+1+1+1+1$	$[1]_{S_5}$	1
$2+1+1+1$	$[(1,2)]_{S_5}$	10
$2+2+1$	$[(1,2)(3,4)]_{S_5}$	15
$3+1+1$	$[(1,2,3)]_{S_5}$	20
$3+2$	$[(1,2,3)(4,5)]_{S_5}$	20
$4+1$	$[(1,2,3,4)]_{S_5}$	30
5	$[(1,2,3,4,5)]_{S_5}$	24

Again, as a check, $|S_5| = 5! = 120 = 1 + 10 + 15 + 20 + 20 + 30 + 24$.

Transpositions: A 2-cycle in the group S_n is called a **transposition**. Thus, the transpositions in S_n are the elements having the form (a, b), in cycle notation, where a

and b are distinct elements of $[1,n]_{\mathbb{Z}}$. For $x \in [1,n]_{\mathbb{Z}}$, we have

$$(a,b)(x) = \begin{cases} b & \text{if } x = a, \\ a & \text{if } x = b, \\ x & \text{otherwise.} \end{cases}$$

Of course $(a,b) = (b,a)$. Plainly, set of transpositions in S_n is a conjugacy class in S_n.

Lemma 6.8: *For any integer m with $m \geq 2$, any m-cycle in S_n can be expressed as a product of transpositions.*

Proof: We have $(x_1, ..., x_m) = (x_1, x_2)(x_2, x_3)...(x_{m-1}, x_m)$ for mutually distinct elements $x_1, ..., x_m \in [1,n]_{\mathbb{Z}}$. □

For any group G and a subset $S \subseteq G$, we write $\langle S \rangle$ for the subgroup of G that is minimal subject to the condition that $S \subseteq \langle S \rangle$. Thus, given $H \leq G$, we have $\langle S \rangle \leq H$ if and only if $S \leq H$. It is not hard to see that S consisting of those elements of G that can be written as a product $g_1...g_r$ where, for each index i, we have $g_i \in S$ or $g_i^{-1} \in S$. It is to be understood that $\langle \emptyset \rangle$ is the trivial subgroup $\{1\}$ of G. Of course, we also have $\{1\} = \langle 1 \rangle$. Observe that, more generally, the subgroups of G with a singleton generating set are precisely the cyclic subgroups of G, and $\langle g \rangle = \langle \{g\} \rangle$ for any $g \in G$.

Proposition 6.9: *When $n \geq 2$, the set of transpositions is a generating set for S_n.*

Proof: This follows from Proposition 6.4 and Lemma 6.8. □

In a trivial way, the proposition also makes sense in the case $n = 1$. Indeed, the empty set is a generating set for the trivial group S_1, and the trivial element of S_1 can be viewed as a product of 0 transpositions.

The proof shows how to express an explicitly given element of S_n as a product of transpositions. For example, consider the element $g \in S_{10}$ specified by the table

x	1	2	3	4	5	6	7	8	9	10	11
$g(x)$	5	3	2	1	7	11	4	8	6	10	9

Employing a technique discussed earlier, we quickly obtain

$$g = (1,5,7,4)(2,3)(6,11,9)\ .$$

Now using Lemma 6.8, $g = (1,5)(5,7)(7,4)(2,3)(6,11)(11,9)$.

The alternating groups: In this section, we assume that $n \geq 2$. We define A_n to be the subset of S_n consisting of those elements g such that g is a product of an even number of transpositions. It is obvious that A_n is a normal subgroup of S_n.

An even integer is said to have **even parity**. An odd integer is said to have **odd parity**. When two integers are both even or both odd, we say that they have the *same parity*, otherwise we say that they have **opposite parity**.

Lemma 6.10: *Let s_1, ..., s_u, t_1, ..., t_v be transpositions in S_n such that $s_1...s_u = t_1...t_v$. Then u and v have the same parity.*

Proof: Let Π be the set consisting of the subsets of $[1,n]_{\mathbb{Z}}$ that have size 2. Given $g \in S_n$ and $\{i,j\} \in \Pi$, we say that g reverses $\{i,j\}$ provided exactly one of the conditions $i<j$ and $gi<gj$ holds. Let $\Pi(g)$ be the set consisting of those elements of Π that are reversed by g. Let $t=(a,b)$ be a transposition in S_n with $a<b$. The elements of Π reversed by t are $\{a,b\}$ together with the sets having the form $\{a,c\}$ or $\{c,b\}$ where $a<c<b$. Observe that t reverses exactly $2b-2a+1$ elements of Π. So there are exactly $2b-2a+1$ elements of Π that belong to exactly one of the sets $\Pi(g)$ and $\Pi(tg)$. Therefore, $|\Pi(g)|$ and $|\Pi(tg)|$ have opposite parity. An inductive argument now shows that $\Pi(g)$ has the same parity as u. Similarly, $\Pi(g)$ has the same parity as v. $\square$

The subset $\{\pm 1\} = \{1,-1\}$ of $\mathbb{Z}$ is a group under multiplication. The lemma implies that there is a well-defined group homomorphism $\mathrm{sgn} : \{\pm 1\} \leftarrow S_n$ such that, given $g \in S_n$, then $\mathrm{sgn}(g)=1$ if and only if $g \in A_n$. Thus, if g is a product of u transpositions, then $\mathrm{sgn}(g)=(-1)^u$. We call $\mathrm{sgn}(g)$ the **signature** of g. We have

$$A_n = \ker(\mathrm{sgn}) \ .$$

The next theorem now follows via the First Isomorphism Theorem.

Theorem 6.11: *The subgroup A_n of S_n has index 2. In other words, $|A_n| = n!/2$.*

Let us point out that, to obtain the theorem, the use of the lemma was crucial. The lemma was needed to establish the well-definedness of the signature homomorphism.

The next result tells us how to tell, from the shape of an element of S_n, whether or not the element belongs to A_n.

Proposition 6.12: *Given a positive integer m, then an m-cycle in S_n belongs to A_n if and only if m is odd. More generally, given $g \in S_n$, writing $m_1 + ... + m_r$ for the shape of g, then $g \in A_n$ if and only there is an even number of indices i such that m_i is even.*

Proof For the first part, the case $m=1$ is trivial. Suppose $m \geq 2$. Given distinct elements x_1, ..., x_m of $[1,n]_{\mathbb{Z}}$, then $(x_1,...,x_m) = (x_1,x_2)(x_2,x_3)...(x_{m-1},x_m)$. In particular, the m-cycle $(x_1,...,x_m)$ is a product of $m-1$ transpositions. The first part is now established. The second part follows immediately. $\square$

For example, the elements of S_5 with shape $2+2+1$ belong to A_5 since exactly 2 of the terms of the partition are even. The elements of S_5 with shape $2+3$ do not belong to A_5, since exactly 1 of terms of the partition is even. Applying similar observations to the other 5 partitions of 5, we find that the elements of A_5 are precisely those which have one of the shapes

$$1+1+1+1+1 \ , \qquad 2+2+1 \ , \qquad 3+1+1 \ , \qquad 5 \ .$$

The conjugacy classes of a subgroup with index 2: Recall that, given a finite group G and a subgroup $H<G$ with index $|G:H|=2$, then $H \lhd G$. That is to say, H is the union of some of the conjugacy classes of G. However, given $h \in H$, then the G-conjugacy class $[h]_G$ is not necessarily the same as the H-conjugacy class $[h]_H$.

The next result gives a necessary and sufficient criterion for $[h]_G$ to be an H-conjugacy class. The result also describes the situation that arises when that criterion fails.

Proposition 6.13: *Let G be a finite group. Let $H < G$ with $|G : H| = 2$, whereupon $H \lhd G$. Let $h \in H$. Then exactly one of the following two conditions holds:*
Stable case: *We have $|C_G(h) : C_H(h)| = 2$ and $[g]_H = [h]_H$.*
Fusion case: *We have $C_G(h) = C_H(h)$ and $[g]_G = [h]_H \sqcup [h']_H$ as the disjoint union of two H-conjugacy classes with equal size, $|[h]_H| = |[h']_H| = |[g]_H|/2$.*

Proof: We have $H \lhd G$ because $G - H$ is both a left coset and a right coset. So we can form the subgroup $HC_G(h)$. Either $HC_G(h) = G$ or else $HC_G(h) = H$. In the former case, the Second Isomorphism Theorem implies that $C_G(h)/C_H(h) \cong G/H$, hence $|C_G(h)| = 2|C_H(h)|$, whereupon the Orbit-Stabilizer Equation yields $|[h]_G| = |G : C_G(h)| = |H : C_H(h)| = |[h]_H|$ and we deduce that $[h]_G = [h]_H$. In the latter case, $C_G(h) = C_H(h)$, the Orbit-Stabilizer Equation yields $|[h]_G| = 2|[h]_H|$ and, replacing h with any element $h' \in [h]_G - [h]_H$, we also have $|[h]_G| = 2|[h']_G|$. □

The simplicity of A_5: We shall determime the conjuacy classes of the alternating group A_5. Using that information, we shall prove that A_5 is simple.

Above, we determined which of the partitions of 5 are the shapes of elements of A_5. Hence, the S_5-conjugacy classes contained in A_5 are

$$[1]_{S_5} \ , \qquad [(1,2)(3,4)]_{S_5} \ , \qquad [(1,2,3)]_{S_5} \ , \qquad [(1,2,3,4,5)]_{S_5} \ .$$

We also found, above, that the sizes of those S_5-conjugacy classes are 1, 15, 20, 24, respectively. Since each of the elements 1 and $(1,2)(3,4)$ and $(1,2,3)$ is centralized by a transposition, Proposition 6.3 tells us that the first three of those S_5-conjugacy classes are also A_5-conjugacy classes. But 24 does not divide the order $|A_5| = 60$. So, by Proposition 6.13 again, $[(1,2,3,4,5)]_{S_5}$ is the disjoint union of two A_5-conjugacy classes. Noting that $(1,3,5,2,4) = (2,3,5,4)(1,2,3,4,5)(2,3,5,4)^{-1}$ and that $(2,3,5,4) \notin A_5$, we see that the A_5-conjugacy classes are

$$[1]_{A_5} \ , \quad [(1,2)(3,4)]_{A_5} \ , \quad [(1,2,3)]_{A_5} \ , \quad [(1,2,3,4,5)]_{A_5} \ . \quad [(1,3,5,2,4)]_{A_5}$$

with sizes 1, 15, 20, 12, 12, respectively.

Theorem 6.14: *The group A_5 is simple.*

Proof: Let H be a non-trivial normal subgroup of A_5. Then H is the union of $\{1\}$ and some or all of the other 4 conjugacy classes. So $|H| \geq 13$. On the other hand, by Lagrange's Theorem, $|H|$ divides 60. So $|H| \in \{15, 20, 30, 60\}$. But none of the integers 15 or 20 or 30 can be expressed as 1 plus some of the numbers among 15, 20, 12, 12. Therefore, $|H| = 60$ and $H = A_5$. □

The simplicity of most of the alternating groups: We shall show that A_n is simple when $n \geq 5$. The following lemma will be needed.

Lemma 6.16: *For any integer $n \geq 3$, the set of 3-cycles in A_n is a generating set for A_n.*

Proof: The definition of A_n implies that A_n has a generating set consisting of the elements that can be expressed as the product $(a,b)(c,d)$ of two distinct transpositions. When a, b, c, d are mutually distinct, we have $(a,b)(c,d)(a,b,c)(b,c,d)$. When a, b, c, d are not mutually distinct, one of a or b must be the same as c or d. We have $(a,b)(b,c) = (a,b,c)$. □

The alternating group A_2 is trivial, hence not simple. We have $A_3 \cong C_3$, which is simple. It is easy to see that A_4 has a normal subgroup isomorphic to V_4 and, in particular, A_4 is not simple. Having disposed of those easy cases, let us now generalize the latest theorem.

Theorem 6.17: *For each integer $n \geq 5$, the group A_n is simple.*

Proof: Let H be a non-trivial normal subgroup of A_n. We must show that $H = A_n$. Consider a subset $\Gamma \subseteq [1,n]_{\mathbb{Z}}$ such that $|\Gamma| = 5$. Let A_Γ be the subgroup of A_n consisting of the elements g such that $gx = x$ for all $x \in [1,n]_{\mathbb{Z}} - \Gamma$. We have $A_\Gamma \cong A_5$ and, by Theorem 16.15, A_Γ is simple.

Suppose that $H \cap A_\Gamma$ is non-trivial. Since $H \cap A_\Gamma$ is a non-trivial normal subgroup of the simple group A_Γ, we have $H \geq A_\Gamma$. In particular, H owns a 3-cycle. Bearing in mind that $n \geq 5$, we see that any 3-cycle in A_n commutes with some transposition in A_n. So, by Proposition 6.13, the 3-cycles in A_n comprise a single A_n-conjugacy class. Therefore, H owns all the 3-cycles in A_n. Using the latest lemma, we deduce that, in this case, $H = A_n$. Thus, it suffices to show that $H \cap A_\Gamma \neq \{1\}$ for some subset Γ of $[1,n]_{\mathbb{Z}}$ with size 5, then

Let $h \in H - \{1\}$. Let c be any 3-cycle $c \in A_n$. The element $g = hch^{-1}c^{-1}$ is the product of two elements of H, so $g \in H$. But g is also the product of the three cycles $u = hch^{-1}$ and $v = c^{-1}$. Let Δ be the set of elements x of $[1,n]_{\mathbb{Z}}$ such that $ux \neq x$ or $vx \neq x$. Then $|\Delta| \leq 6$.

If $|\Delta| \leq 5$, then we can apply the comments above by taking Γ to be any subset of $[1,n]_{\mathbb{Z}}$ containing Δ. So we may assume that $|\Delta| = 6$. For any $f \in S_n$, we can replace H with ${}^fH$, and we can replace u and v with ${}^fu$ and ${}^fv$. So we may assume that $u = (1,2,3)$ and $v = (4,5,6)$. Hence $g = (1,2,3)(4,5,6)$. Let $s = (3,4)(5,6)$. Then ${}^sg = (1,2,4)(3,6,5)$. So $g.{}^sg = (1,3,4,2,5)$. But $g \in H$ and ${}^sg \in H$, hence $g{}^sg \in H$. Putting $\Gamma = \{1,2,3,4,5\}$, then $H \cap A_\Gamma$ is non-trivial, as required. □