Algebra I: Chapter 5. Permutation Groups

5.1 The Structure of a Permutation.

The **permutation group** S_n is the collection of all bijective maps $\sigma : X \to X$ of the set $X = \{1, 2, \ldots, n\}$, with composition of maps ($\circ$) as the group operation. We introduced permutation groups in Example 3.1.15 of Section 3, which you should review before proceeding. There we introduced basic notation for describing permutations. The most basic kind of permutation is a *cycle*. Recall that

5.1.1 Definition. *For $k > 1$, a k-**cycle** is a permutation $\sigma = (i_1, \ldots, i_k)$ that acts on X in the following way*

$$(1) \qquad \sigma \text{ maps } \begin{cases} i_1 \to i_2 \to \ldots \to i_k \to i_1 & \text{(a cyclic shift of list entries)} \\ j \to j & \text{for all } j \text{ not in the list } \{i_1, \ldots, i_k\} \end{cases}$$

One-cycles (k) are redundant; every one-cycle reduces to the identity map id_X, so we seldom write them explicitly, though it is permissible and sometimes useful to do so.

*The **support** of a k-cycle is the set of entries $\mathrm{supp}(\sigma) = \{i_1, \ldots, i_k\}$, in no particular order. The support of a 1-cycle (k) is the one-point set $\{k\}$.*

Recall that the order of the entries in a cycle $(i_1, \ldots, i_k)$ matters, but cycle notation is somewhat ambiguous: k different symbols obtained by cyclic shifts of the entries in σ all describe the same operation on X.

$$(i_1, \ldots, i_k) = (i_2, \ldots, i_k, i_1) = (i_3, \ldots, i_k, i_1, i_2) = \ldots = (i_k, i_1, \ldots, i_{k-1})$$

Thus $(123) = (231) = (312)$ all specify the same operation $1 \to 2 \to 3 \to 1$ in X, and likewise $(i, j) = (j, i)$ for any 2-cycle. If we mess up the cyclic order of the entries we *do not* get the same element in S_n, for example $(123) \neq (132)$ as maps because the first operation sends $1 \to 2$ while the second sends $1 \to 3$.

In Section 3.1 we also showed how to evaluate products $\sigma\tau$ of cycles, and noted the following important fact.

(2) *If $\sigma = (m_1, \ldots, m_k)$ and $\tau = (n_1, \ldots, n_r)$ are disjoint cycles, so that*

$$\mathrm{supp}(\sigma) \cap \mathrm{supp}(\tau) = \{m_1, \ldots, m_k\} \cap \{n_1, \ldots, n_r\} = \emptyset$$

then these operations commute $\sigma\tau = \tau\sigma$. If supports overlap, the cycles may or may not commute.

Since any 1-cycle (k) is the identity operator, certain cycles with overlapping supports such as (4) and (345) do commute, so property (2) only works in one direction; on the other hand an easy calculation of the sort outlined in Example 3.1.15 shows that $(23)(345) = (2345)$, which is not equal to $(345)(23) = (2453)$.

Our first task is to make good on a claim stated in 3.1.15: every permutation can be written uniquely as a product of *disjoint commuting cycles*. This is a great help in understanding how arbitrary permutations work.

5.1.2 Theorem. *Every $\sigma \in S_n$ has a factorization $\sigma = \prod_{i=1}^{r} \sigma_i$ into cycles whose supports are disjoint and fill X*

$$(3) \qquad X = \bigcup_{i=1}^{r} \mathrm{supp}(\sigma_i) \qquad \text{and} \qquad \mathrm{supp}(\sigma_i) \cap \mathrm{supp}(\sigma_j) = \emptyset \quad \text{for } i \neq j$$

Some factors may be trivial 1*-cycles, which must be written down to get the support condition* (3)*. The factors σ_i are uniquely determined, and they commute.*

Proof: If $\sigma = e$ we can write $e = (1)(2)\cdots(n)$, a product of disjoint trivial 1-cycles. So, assume $\sigma \neq e$ and consider the cyclic group it generates $H = \langle\sigma\rangle \subseteq S_n$. This finite group acts on the space X and the action $H \times X \to X$ determines various disjoint H-orbits that partition $X = (H\cdot x_1) \cup \ldots \cup (H \cdot x_r)$. Let's label the orbits $\mathcal{O}_i = H \cdot x_i$ in order of increasing size, so that $1 \leq |\mathcal{O}_1| \leq \ldots \leq |\mathcal{O}_r|$. For each orbit $\mathcal{O}_i$ we are going to define a cycle τ_i such that $\mathrm{supp}(\tau_i) = \mathcal{O}_i$. There may be some one-point orbits and for these we simply take the 1-cycles $\tau_i = (x_i)$. There must, however, be some nontrivial orbits since $\sigma \neq e$.

For a nontrivial orbit $\mathcal{O} = H{\cdot}x$ we observe that in the ordered list $\{x, \sigma(x), \sigma^2(x), \ldots\}$ there will be a first index $k \geq 2$ such that $\sigma^k(x)$ is a repeat of some previous entry $\sigma^\ell(x)$, $0 \leq \ell < k$. This can only happen if $\{x, \sigma(x), \ldots, \sigma^{k-1}(x)\}$ are distinct and $\sigma^k(x) = x$. [If $0 < \ell < k$ the definition of k is violated because $\sigma^k(x) = \sigma^\ell(x) \Rightarrow \sigma^{k-\ell}(x) = x$ and $k - \ell < k$.] The list $\tau = (x, \sigma(x), \ldots, \sigma^{k-1}(x))$ enumerates the points in $\mathcal{O}$ in a particular cyclic order, which determines a k-cycle τ with $\mathrm{supp}(\tau) = \mathcal{O}$. The resulting cycle does not depend of the base point $x \in \mathcal{O}$ we choose to start our list: a different base point $x' = \sigma^j(x)$ yields the ordered list

$$\sigma^j(x), \sigma^{j+1}(x), \ldots, \sigma^{k-1}(x), x, \sigma(x), \ldots, \sigma^{j-1}(x)$$

which is a cyclically shifted version of $x, \sigma(x), \sigma^2(x), \ldots \sigma^{k-1}(x)$ and determines the same k-cycle in S_n. Thus τ is uniquely determined by the orbit $\mathcal{O}$ and iterated action of σ upon it.

The cycles $\tau_1, \ldots, \tau_r$, one for each orbit, are disjoint. Their supports partition $X = \mathrm{supp}(\tau_1) \cup \ldots \cup \mathrm{supp}(\tau_r)$, and the τ_i commute because their supports are disjoint. Furthermore for each i,

(i) σ and τ_i have the same actions on the orbit $\mathcal{O}_i$: they both act as cyclic "1-shifts" that send $\sigma^i(x) \to \sigma^{i+1}(x)$ and $\sigma^{k-1}(x) \to x$.

(ii) $\tau_i(y) = y$ for all $y \notin \mathcal{O}_i$

It is now apparent that σ and $\prod_{i=1}^r \tau_i$ have the same actions throughout X.

Uniqueness of the cycles τ_i is built into the above construction, since they depend on the H-orbits in X, which are completely determined once σ is specified. $\square$

One-point orbits must be taken into account in partitioning X if the support condition (3) is to hold, so the corresponding 1-cycles must be included in the factorization of σ. Thus in S_5 the disjoint cycle decomposition of (123) would be written (123)(4)(5).

***5.1.3 Exercise.** A power τ^j of a cycle need not be a cycle.

(a) Verify that $\tau = (1234) \in S_5$ has $\tau^2 = (13)(24)$.

(b) What is the order $o(\tau)$ of this element in S_5?

(c) If $H = \langle\tau\rangle$, what are the possible cardinalities of the H-orbits in $X = \{1, 2, 3, 4, 5\}$?

(d) Determine all orbits in X under the iterated action of τ.

Hint: Recall 4.2.3 is transitive (see Section 4.2). $\square$

***5.1.3A Exercise.** In S_n

(a) If σ, τ are disjoint cycles with lengths $o(\sigma) = m, o(\tau) = k$. Prove that the order of their product ab is the least common multiple $\mathrm{lcm}\big(o(\sigma), o(\tau)\big) = \mathrm{lcm}(m, k)$.

(b) If $\sigma_1, \ldots, \sigma_r$ are disjoint commuting cycles in S_n prove that the order of $\sigma = \sigma_1 \cdot \ldots \cdot \sigma_r$ is $o(\sigma) = \mathrm{lcm}\big(o(\sigma_1), \ldots, o(\sigma_r)\big)$.

Note: The crucial point is that σ and τ act on disjoint subsets of $[1, n]$, so the cyclic subgroups generated by these elements satisfy $\langle\sigma\rangle \cap \langle\tau\rangle = (e)$. In Chapter 2 we proved that $\text{lcm}(a, \text{lcm}(b, c)) = \text{lcm}(a, b, c)$, etc. $\square$

5.1.3B Exercise. Let a, b be *commuting* elements in an arbitrary group. If these elements have finite orders $o(a)$ and $o(b)$,

(a) Prove that ab must have finite order and show that $o(ab)$ must be a divisor of the least common multiple $\text{lcm}\big(o(a), o(b)\big)$.

(b) Provide an example showing that the order $o(ab)$ can be *less than* $\text{lcm}\big(o(a), o(b)\big)$.

Hint: $H = \langle a, b\rangle$ is an abelian group. In (b) try a really simple group such as $G = \mathbb{Z}_n$ with n non-prime.

5.1.3C Exercise. If $\sigma = (i_1, \ldots, i_k)$ is a k-cycle in S_n it has order $o(\sigma) = k$. Show that the power σ^j is again a k-cycle $\Leftrightarrow j \in \mathrm{U}_k$ (multiplicative units in $\mathbb{Z}_k$).
Hints: By relabeling points in $X = [1, n]$ we may assume σ is the particular k-cycle $\sigma = (1, 2, \ldots, k)$. Note that σ^j is a "j-shift" on the cyclic ordered list $(1, 2, \ldots, k)$, with $\sigma^j(s) \equiv s + j \pmod{k}$ for all $1 \leq s \leq k$. $\square$

5.1.4 Exercise. If σ and τ are nontrivial cycles in S_n they commute if their supports are disjoint. But disjointness is not a *necessary* condition in order to have $\sigma\tau = \tau\sigma$. Can you find a *necessary and sufficient condition* for the cycles to commute?
Note: This is not an easy problem. The answer has the form $\sigma\tau = \tau\sigma \Leftrightarrow$ (disjoint) OR (....). Start by asking: *If* $\text{supp}(\sigma) = \text{supp}(\tau)$*, does that make the cycles commute? What happens if neither support includes the other?* $\square$

Cycle Types of Permutations. The cardinalities of orbits in X under the action of $H = \langle\sigma\rangle$ provide us with a natural way to classify permutations.

5.1.5 Definition. *If* $\sigma \in S_n$ *and* $H = \langle\sigma\rangle$ *the* **cycle type** *of* σ *is the list of integers*

$$1 \leq n_1 \leq n_2 \leq \ldots \leq n_r \qquad \textit{such that} \qquad n_1 + \ldots + n_r = n \tag{4}$$

determined by listing the H*-orbits in* X *in order of increasing size and taking* $n_i = |\mathcal{O}_i|$*. The* n_i *are just the lengths of the cycles in the unique disjoint cycle decomposition of* σ*.*

Any sum of integers $n_i \in \mathbb{N}$ having the properties (4) is known to number theorists as a **partition** of the integer n. Every possible partition is accounted for in the list of cycle types found in S_n. For example in S_5 we have the cycle types shown in Table 1.

Cycle Type	**Example**	**#(Elements in $\mathbf{S_5}$)**
11111	e	1
1112	(12)	10
113	(123)	20
122	(12)(34)	15
14	(1234)	30
23	(12)(345)	20
5	(12345)	24

Table 1. Cycle types in S_5.

Notice that we have listed the cycle types in "alphabetical" order (think: $1 = A, 2 = B, \ldots$), which makes it easy to enumerate all the types.

For a given group element σ the action $H \times \mathcal{O} \to \mathcal{O}$ on an orbit is *transitive*, so by 4.2.3 the indices $n_i = |\mathcal{O}_i|$ always divide the order $|H| = o(\sigma)$. Thus there are number-theoretic connections between the cycle-type indices n_i and the order of σ as an element of S_n.

Enumerating the elements of a particular cycle type in S_n is a fairly straightforward combinatorial problem, but there is no general formula. In doing the count you must keep in mind that k different symbols $(i_1, \ldots, i_k)$, $(i_2, \ldots, i_k, i_1), \ldots$ represent the same k-cycle in S_n; there can be other complications.

5.1.6 Example. To illustrate the idea we shall count the number of elements in S_6 of the following cycle types.

Cycle Type	**#(Elements in S_6)**
1113	40
123	120
1122	45

Discussion: For cycle type 1113 (3-cycles in S_6) we first select distinct entries from $\{1, 2, \ldots, 6\}$ to fill the spots in the ordered list $\square\square\square$ and create a 3-cycle. There are $6{\cdot}5{\cdot}4$ way to do this, but 3 lists of this type collapse to a single element of S_6, so #(3-cycles) $= \frac{1}{3}(6{\cdot}5{\cdot}4) = 40$.

To create 2,3-cycles we first select distinct entries for the ordered list $\square\square\,|\,\square\square\square$; there are $6\cdot 5\cdot \ldots \cdot 2$ to make such a list. The $6\cdot 5$ ways to fill the first two slots yield $\frac{1}{2}(6 \cdot 5) = 15$ possible 2-cycles; the $4 \cdot 3 \cdot 2$ possibilities in the last three spots yield $\frac{1}{3}(4 \cdot 3 \cdot 2) = 8$ distinct 3-cycles. The number of pairs is therefore

$$\#(\text{2,3-cycles in } S_6) = \frac{(6{\cdot}5){\cdot}(4{\cdot}3{\cdot}2)}{2{\cdot}3} = 120$$

For cycle type 1122 (the 2,2-cycles) there are $6{\cdot}5{\cdot}4{\cdot}3$ ways to fill the list $\square\square\,|\,\square\square$. The first two entries yield $\frac{1}{2}(6{\cdot}5) = 15$ two-cycles; the second two yield $\frac{1}{2}(4{\cdot}3) = 6$ two-cycles disjoint from the first. So it would appear that

$$\#(\text{2,2-cycles in } S_6) \;=\; \frac{6{\cdot}5{\cdot}4{\cdot}3}{2{\cdot}2} = 90$$

But a hidden symmetry has been overlooked. If $\sigma_1\sigma_2$ is a 2,2-cycle, we get the same element in S_6 if we switch $\sigma_1 \leftrightarrow \sigma_2$, because disjoint cycles commute. So we must divide this preliminary count by 2 to get the correct result

$$\#(\text{2,2-cycles in } S_6) \;=\; \frac{6{\cdot}5{\cdot}4{\cdot}3}{(2{\cdot}2){\cdot}2} = 45$$

By invoking Exercise 5.1.3A we can determine the orders $o(\sigma)$ of elements of each cycle type: If σ is of type 113 (a 3-cycle) its order is clearly $o(\sigma) = 3$. If σ is a 2,3-cycle its order is $o(\sigma) = \mathrm{lcm}(2, 3) = 6$, and if σ is a 2,2-cycle its order is clearly $o(\sigma) = 2$. In fact one can determine the orders of elements of each cycle type without having to count the number of such elements. For instance all 2,4-cycles (whatever their number) have order $\mathrm{lcm}(2, 4) = 4$, while all 3,3-cycles have order 3. $\square$

5.1.7 Exercise. List all possible cycle types for elements of S_6. Then

(a) Explain why all elements of the same cycle type have the same order.

(b) Compute the orders of elements for each cycle type. $\square$

5.1.8 Exercise. Here is a permutation in S_9, described by telling where each element in $X = [1, 9]$ ends up

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 4 & 7 & 5 & 1 & 6 & 3 & 9 & 8 \end{pmatrix}$$

Determine the decomposition into disjoint cycles, the cycle type and the order $o(\sigma)$. $\square$

5.1.9 Exercise. If $\sigma \in S_n$ has one of the following cycle types

(i) Cycle Type: 3211 in S_7 (ii) Cycle Type: 421 in S_7

(iii) Cycle Type: 22111 in S_7 (iv) Cycle Type: 8631 in S_{18}

what is the order of the cyclic group $H = \langle\sigma\rangle$? $\square$

5.2. Parity of a Permutation.

We now show that S_n is generated by its 2-cycles (i, j), so every $\sigma \in S_n$ can be factored as a product $\sigma_1 \cdot \sigma_2 \cdot \ldots \cdot \sigma_m$ of (not necessarily commuting) 2-cycles. This factorization is far from unique. For instance the identity element e can be factored as $e = (12)(12) = (13)(13) = \ldots$, and the number of factors isn't unique either since $e = (12)^2 = (35)^2$, etc. Nevertheless, there *is* something important that all such decompositions of σ have in common, as we shall see.

5.2.1 Lemma. *For $n \geq 2$, every $\sigma \in S_n$ can be written as a product of finitely many 2-cycles.*

Proof: Factor $\sigma = \sigma_1 \cdots \sigma_r$ into disjoint commuting cycles, which may have various lengths. It suffices to show that any k-cycle can be written as a product of 2-cycles. By relabeling entries in $\sigma = (i_1, \ldots, i_k)$, we may as well assume that we are dealing with the particular k-cycle $\sigma = (1, 2, \ldots, k)$. (Once you see how to factor the latter it is easy to see how to factor the general k-cycle.) By hand one easily verifies that

$$(1, 2, \ldots, k) = (1, k)(1, k-1) \cdots (1, 3)(1, 2) \tag{5}$$

Done. $\square$

The factorization (5) is worth remembering. It's not so easy to prove the lemma until you hit upon this idea.

***5.2.2 Exercise.** Use the idea in (5) to factor the 5-cycles $\sigma = (12345)$ and $\tau = (i_1, \ldots, i_5) = (13582)$ as products of 2-cycles. $\square$

5.2.2A Exercise. Using the idea of "proof by relabeling" explain why

$$(i_1, i_2, \ldots, i_k) = (i_1, i_k)(i_1, i_{k-1}) \ldots (i_1, i_3)(i_1, i_2)$$

for any ordered list of k distinct indices $\{i_1, \ldots, i_k\} \subseteq [1, n]$. $\square$

We now show that these nonunique factorizations all assign the same *parity* to a permutation.

5.2.3 Theorem (The Parity sgn(σ) of a Permutation). *If $\sigma \in S_n$ is decomposed as a product $\sigma = \sigma_1 \cdots \sigma_r$ of 2-cycles, then the*

$$\text{Parity:} \quad \operatorname{sgn}(\sigma) = (-1)^r \qquad (r = \textit{number of factors}) \tag{6}$$

is uniquely determined. Furthermore, $\operatorname{sgn}(e) = 1$ *and parity is multiplicative*

$$\operatorname{sgn}(\sigma\tau) = \operatorname{sgn}(\sigma) \cdot \operatorname{sgn}(\tau) \qquad \textit{for all} \quad \sigma, \tau \in S_n \tag{7}$$

Thus the **parity map** $\operatorname{sgn} : S_n \to \{\pm 1\}$ *is a homomorphism from the group of operators* $(S_n, \circ)$ *to the 2-element multiplicative group* $(\{\pm 1\}, \cdot)$.

$$
\begin{bmatrix}
1 & & & 0 & & & & 0 & & & 0 \\
& \ddots & & \vdots & & & & \vdots & & & \\
& & 1 & & & & & & & & \\
0 & \cdots & & \boxed{0} & & \cdots & & \boxed{1} & & \cdots & 0 \\
& & & & 1 & & & & & & \\
& & & \vdots & & \ddots & & \vdots & & & \\
& & & & & & 1 & & & & \\
0 & \cdots & & \boxed{1} & & \cdots & & \boxed{0} & & \cdots & 0 \\
& & & & & & & & 1 & & \\
& & & \vdots & & & & \vdots & & \ddots & \\
0 & & & 0 & & & & 0 & & & 1
\end{bmatrix}
$$

Figure 5.1. Permutation matrix associated with the 2-cycle $\sigma = (i, j)$ differs from the identity matrix only in rows/columns i and j.

Proof: There are combinatorial proofs based on induction, but we shall prove this using ideas from linear algebra, especially the theory of determinants. We start by providing a different interpretation of $\mathrm{sgn}(\sigma)$. Each $\sigma \in S_n$ can be thought of as a permutation of vectors in the standard orthonormal basis $\mathfrak{X} = \{\mathbf{e}_1, \ldots, \mathbf{e}_n\}$ in $\mathbb{R}^n$, with $\sigma : \mathbf{e}_k \mapsto \mathbf{e}_{\sigma(k)}$. That action induces a linear operator $\tilde{\sigma} : \mathbb{R}^n \to \mathbb{R}^n$ given by

$$\tilde{\sigma}\left(\sum_{k=1}^{n} a_k \mathbf{e}_k\right) = \sum_{k=1}^{n} a_k \mathbf{e}_{\sigma(k)} \qquad \text{where } a_k \in \mathbb{R},\ 1 \leq k \leq n$$

The matrix $[\tilde{\sigma}] = [\tilde{\sigma}]_{\mathfrak{X}}$ of $\tilde{\sigma}$ with respect to the standard basis is called a *permutation matrix*. These matrices are characterized by the following special properties

(i) Each entry is 0 or 1.

(ii) Each column contains exactly one "1"

(iii) Each row contains exactly one "1"

To illustrate, we show the permutation matrix corresponding to the 2-cycle $\sigma = (i, j)$ in Figure 5.1.

The correspondence $\Phi : \sigma \to \tilde{\sigma}$ is a homomorphism mapping S_n into the group $(\mathrm{GL}(n), \circ)$ of invertible linear operators on $\mathbb{R}^n$, so that $\Phi(\sigma\tau) = \Phi(\sigma) \circ \Phi(\tau) = \tilde{\sigma} \circ \tilde{\tau}$. Since determinants are multiplicative, it follows that

(i) $\det \Phi(e) = 1$

(ii) $\det \Phi(i, j) = -1$ for any 2-cycle $(i \neq j)$

(iii) $\det(\Phi(\sigma)) = \prod_{i=1}^{r} \det \Phi(\sigma_i) = (-1)^r = \mathrm{sgn}(\sigma)$ if σ is a product $\sigma = \sigma_1 \cdots \sigma_r$ of 2-cycles.

But the value of $\det \Phi(\sigma)$ is determined without reference to any factorization of σ into 2-cycles, so we get the same number $\mathrm{sgn}(\sigma) = (-1)^r$ no matter how σ is factored. Thus, the number of 2-cycles in any factorization of σ is either always even or always odd.

Finally, since $\det(AB) = \det(A) \cdot \det(B)$ for any pair of linear operators, we see that $\mathrm{sgn}(\sigma\tau) = \mathrm{sgn}(\sigma) \cdot \mathrm{sgn}(\tau)$. $\square$

For obvious reasons, we say a permutation is **even** if it can be written as a product of an even number of 2-cycles, so that $\mathrm{sgn}(\sigma) = +1$, and otherwise it is **odd**. Note that the identity e is even since $e = (12)(12)$ and all 2-cycles are odd. The idea set forth in (5) shows how to compute the parity of a cycle of any length.

5.2.4 Exercise. Verify that the map $\Phi : S_n \to \mathrm{GL}(n)$

$$\Phi(\sigma) = \text{ the linear operator } \tilde{\sigma} \text{ defined above}$$

is a homomorphism of groups, so that (i) $\Phi(e) = I$, and (ii) $\Phi(\sigma\tau) = \Phi(\sigma) \circ \Phi(\tau)$. Prove that Φ is a one-to-one mapping – i.e. that $\ker(\Phi)$ is trivial. □

5.2.5 Proposition. *In S_n all k-cycles have the same parity, namely*

$$\operatorname{sgn}(\sigma) = (-1)^{k-1} \quad \textit{for } k = 1, 2, \ldots \tag{8}$$

If σ is a product $\sigma = \sigma_1 \ldots \sigma_r$ of cycles of various lengths then $\operatorname{sgn}(\sigma) = \prod_{j=1}^{r} \operatorname{sgn}(\sigma_j)$, regardless of whether or not the cycles are disjoint.

PROOF: As in (5), we have $(1, 2, \ldots, k) = (1, k)(1, k-1) \ldots (1, 2)$. □

5.2.6 Definition. *The* **alternating group** A_n *is the set of all even permutations,*

$$A_n = \ker(\operatorname{sgn}) = \{\sigma \in S_n : \operatorname{sgn}(\sigma) = +1\} \tag{9}$$

Since the parity map sgn *is a homomorphism between groups, its kernel A_n is obviously a normal subgroup in S_n, with index $|S_n/A_n| = 2$. In fact,* sgn *assumes just two values and distinct A_n-cosets map to different values ± 1 under* sgn*; there actually are two distinct A_n-cosets because* $\operatorname{sgn}(e) = +1$ *and* $\operatorname{sgn}(1, 2) = -1$.

In Section 5.4 we will examine various subgroups of S_n for low values of n, but A_n is by far the most important. It plays a pivotal role in *Galois Theory*, where we will study algorithms for finding roots of polynomial equations $f(x) = 0$ in one variable. More precisely, we will demonstrate the impossibility of constructing a general algorithm for polynomials of degree $\deg f \geq 5$. These results ultimately rest on the algebraic properties of the alternating group, particularly

(10)

For $n \geq 5$, A_n is nonabelian and

(a) *A_n is a* **simple** *group – it contains no proper normal subgroups.*

(b) *A_n is the only normal subgroup in S_n, other than the trivial subgroups S_n and (e).*

Both statements fail for $n = 4$, but are true for A_3, which is abelian $\cong \mathbb{Z}_3$.

These facts are tricky to prove; we develop the details in Section 5.3.

5.2.7 Exercise. Referring to the list of cycle types in S_5 accompanying 5.1.5,

(a) Explain why $\operatorname{sgn}(\sigma)$ depends only on the cycle type of σ.

(b) Determine the parity for each cycle type in that table.

Start by recalling (8). □

***5.2.8 Exercise.** Prove that the cycles $\sigma = (1, 2)$ and $\tau = (1, 2, \ldots, n)$ generate S_n. *Hint:* It would suffice to show that every 2-cycle can be written as a word in the letters σ, τ and their inverses. Start by computing conjugates $\tau\sigma\tau^{-1}, \tau^2\sigma\tau^{-2}, \ldots$. □

5.2.9 Exercise. With Exercise 5.2.8 in mind, consider any arrangement $i_1, i_2, \ldots, i_n$ of the integers in $X = [1, n]$.

(a) Explain why the elements $\sigma = (i_1, i_2)$ and $\tau = (i_1, i_2, \ldots, i_n)$ together generate all of S_n.

From this you might wonder whether *any* 2-cycle and *any* n-cycle generate S_n. This conjecture fails to be true.

(b) Show that $\sigma = (1, 3)$ and $\tau = (1234)$ only generate a subgroup $H = \langle \sigma, \tau \rangle$ of order 8 in S_4

Hint: (a) is really an exercise in relabeling things; (b) shows that caution is sometimes needed in arguments based on "relabeling." □

5.2.10 Exercise. Express the following permutations in S_{10} as products of commuting disjoint cycles, and determine the parity of each operator.

(a) (1,2,3)(1,2) (b) (1,2,3,4,5)(1,2,3)(4,5) (c) (1,2)(1,3)(1,4)(2,5)

(d) (1,2)(1,2,3)(1,2) (e) (1,2,3)(4,5)(1,6,7,8,9)(1,5) □

5.2.11 Exercise. Does the set of odd permutations in S_n form a group? Explain. □

The Significance of the Simple Groups. A group G is **simple** if it has no proper *normal* subgroups, which means there are no homomorphisms that map G onto smaller, and perhaps more elementary groups. If a three-dimensional object is projected onto various planes, say by taking X-rays in different directions, the two-dimensional images are easier to read but important information may be lost in the projection process. Nevertheless, if we have access to two dimensional projections in many directions it is possible to mathematically reconstruct the original three-dimensional object. This is the whole idea of X-ray tomography, commonly known as a "CAT scan."

If a complicated group G has normal subgroups we may "project" it to various smaller quotient groups G/N. Since whole cosets in G collapse to single points in the quotient some information is lost, but sometimes the information that remains stands out in clear relief because the quotient process suppresses inessential information in the original group. And, by examining various quotients one can often deduce many properties of the more complex original object.

If G is simple its properties cannot be determined by projecting it onto smaller groups. The nature of the group must be analyzed whole, or not at all. The alternating groups A_n for $n \geq 5$ are groups of this sort. Other examples are the cyclic abelian groups $(\mathbb{Z}_p, +)$ for primes $p > 1$. As we will see later on, simple groups are the building blocks needed to construct arbitrary finite groups. As an example, in the next chapter we will explain how to construct "direct products" $G_1 \times G_2$ of arbitrary groups and will prove that: (i) Every nontrivial finite *abelian* group is a direct product of cyclic groups $\mathbb{Z}_n$, and (ii) Every cyclic group $\mathbb{Z}_n$ is a direct product of the simple groups $\mathbb{Z}_p$ where $p > 1$ are the prime divisors of n.

5.3. Conjugacy Classes in S_n.

The conjugacy class of an element $\sigma \in S_n$ is $C_\sigma = \{\tau\sigma\tau^{-1} : \tau \in S_n\}$. To describe the classes we must come to some better understanding of conjugation operations $\alpha_\tau(\sigma) = \tau\sigma\tau^{-1}$. We first show that conjugation has a very simple interpretation if σ is a k-cycle, and from this we will be able to determine the conjugate of any permutation using the decomposition theorem 5.1.2.

5.3.1 Theorem. *Let $\sigma = (m_1, \ldots, m_k)$ be any cycle. Conjugation by $\tau \in S_n$ yields another cycle of the same length*

$$\tau(m_1, \ldots, m_k)\tau^{-1} = (\tau(m_1), \ldots, \tau(m_k)) \tag{11}$$

In other words, the conjugate of σ is a new k-cycle whose entries are the τ-images of the entries in σ, in the same cyclic order.

Proof: The diagram [1] in Figure 5.2 shows the actions of the operators τ^{-1}, σ, τ, and $\tau\sigma\tau^{-1}$ on elements of $X = [1, n]$. The region $A = \{m_1, \ldots, m_k\}$ on the left is the support of σ and region B on the right is its τ-image $B = \tau(A) = \{\tau(m_1), \ldots, \tau(m_k)\}$. The cycle

[1] The sets A and B might overlap, but we depict them as disjoint for clarity.

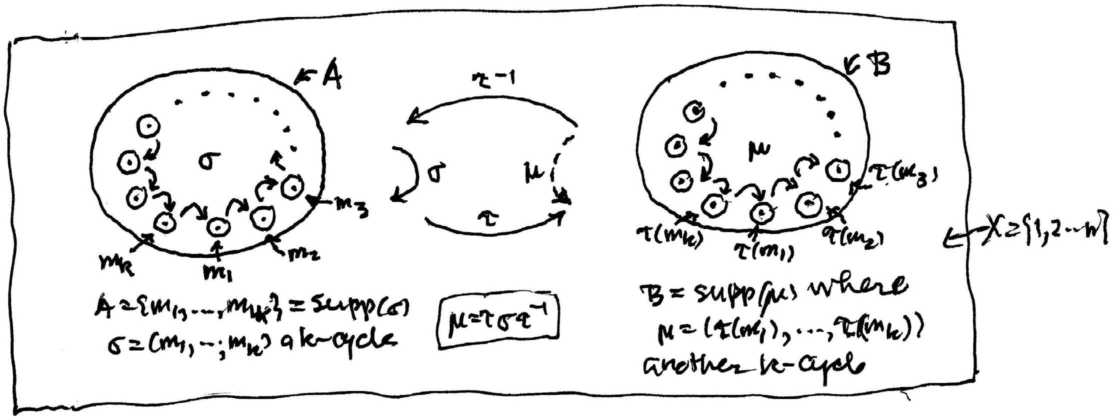

Figure 5.2. If $\sigma = (m_1, \ldots, m_k)$ has support $A = \{m_1, \ldots, m_k\}$, a permutation $\tau \in S_n$ maps A to $B = \tau(A) = \{\tau(m_1), \ldots, \tau(m_k)\}$ and also determines a new k-cycle $\mu = \big(\tau(m_1), \ldots, \tau(m_k)\big)$. We show that $\tau\sigma\tau^{-1} = \mu$.

σ lists the elements of A in a particular cyclic order; we may transfer this order over to B to get a cycle $\mu = \big(\tau(m_1), \ldots, \tau(m_k)\big)$ with $\text{supp}(\mu) = B$. Cycles σ and τ act as cyclic 1-shifts on the elements in A and B, so that

$$\sigma(m_i) = m_{i+1} \qquad \text{and} \qquad \mu(\tau(m_i)) = \tau(m_{i+1})$$

and leave all other points fixed.

Now compare the actions of $\tau\sigma\tau^{-1}$ and μ on X:

Case 1: If $i \notin B$ then $\mu(i) = i$ by definition of μ while $\tau\sigma\tau^{-1}(i) = i$ because $i \notin B \Rightarrow \tau^{-1}(i) \notin A \Rightarrow \sigma(\tau^{-1}(i)) = \tau^{-1}(i)$ and

$$\tau\sigma\tau^{-1}(i) = \tau\tau^{-1}(i) = i \qquad \text{for all } i \notin B$$

The two operators have the same action on $X \sim B$.

Case 2: Every element in B is $\tau(m_i)$ for some $i \in [1, k]$ and by definition of μ we have $\mu(\tau(m_i)) = \tau(m_{i+1})$. On the other hand

$$\tau\sigma\tau^{-1}\big(\tau(m_i)\big) = \tau\big(\sigma(m_i)\big) = \tau\big(m_{i+1}\big)$$

so $\mu = \tau\sigma\tau^{-1}$ on B too. See Figure 5.2.

We conclude that $\tau\sigma\tau^{-1} = \mu$ as elements of S_n $\square$

A general permutation $\sigma \in S_n$ can be decomposed as a product of disjoint commuting cycles $\sigma = (m_1, \ldots, m_k) \cdot \ldots \cdot (n_1, \ldots, n_r)$. Since the conjugation operation is an automorphism we get

$$\begin{aligned} \tau\sigma\tau^{-1} &= \tau(m_1, \ldots, m_k)\tau^{-1} \cdot \ldots \cdot \tau(n_1, \ldots, n_r)\tau^{-1} \\ &= (\tau(m_1), \ldots, \tau(m_k)) \cdot \ldots \cdot (\tau(n_1), \ldots, \tau(n_r)) \end{aligned} \tag{12}$$

This exhibits the effect of conjugation on an arbitrary σ. It follows that the *lengths* of the disjoint cycles appearing in σ and $\tau\sigma\tau^{-1}$ are the same, even if the cycles themselves are different, and hence that

(13) All conjugates $\tau\sigma\tau^{-1}$ of a permutation σ have the same cycle type (4).

These remarks can be summarized as follows.

5.3.2 Corollary. *For $n \geq 2$, let $\sigma \in S_n$ and let $\tau\sigma\tau^{-1}$ be any conjugate. Then*

(i) *The support of the conjugate is the τ-image of* $\mathrm{supp}(\sigma)$*, so that*

$$\mathrm{supp}(\tau\sigma\tau^{-1}) = \tau\,(\mathrm{supp}(\sigma))$$

(ii) *If $\sigma = \sigma_1 \cdots \sigma_r$ is the disjoint cycle decomposition of σ then the decomposition of the conjugate is $\tau\sigma\tau^{-1} = \tau\sigma_1\tau^{-1} \cdot \ldots \cdot \tau\sigma_r\tau^{-1}$.*

(iii) *If $\sigma_i = (m_1, \ldots, m_k)$ then $\tau\sigma_i\tau^{-1} = (\tau(m_1), \ldots, \tau(m_k))$, as in* (11)*.*

(iv) *Conjugate elements in S_n have the same cycle types.*

5.3.3 Corollary. *Let $n \geq 2$. Two elements σ, σ' are conjugate in S_n if and only if they have the same cycle type.*

Proof: Implication ($\Rightarrow$) has just been proved. If the cycle type of σ is $1 \leq n_1 \leq n_2 \leq \ldots \leq n_r$ with $n_1 + \ldots + n_r = n$ let us label things in the disjoint cycle decompositions as

$$\begin{array}{rcl} \sigma = \sigma_1 \ldots \sigma_r & = & \big(s_1, \ldots, s_{n_1}\big) \cdot \big(s_{n_1+1}, \ldots, s_{n_2}\big) \cdot \ldots \\ \sigma' = \sigma'_1 \ldots \sigma'_r & = & \big(t_1, \ldots, t_{n_1}\big) \cdot \big(t_{n_1+1}, \ldots, t_{n_2}\big) \cdot \ldots \end{array}$$

Then let τ be the permutation such that $\tau(s_i) = t_i$ for $1 \leq i \leq n$. By 5.3.2 we see that $\tau\sigma_i\tau^{-1} = \sigma'_i$ for all i, hence $\tau\sigma\tau^{-1} = \sigma'$. $\square$

Other conjugators τ' can have the same effect, but that does not matter. The point is that there is at least one way to conjugate σ to get σ'.

***5.3.4 Exercise.** For $n \geq 3$ prove that the center

$$Z(S_n) = \{\sigma \in S_n : \tau\sigma = \sigma\tau \text{ for all } \tau \in S_n\}$$

is trivial. Where did you use the hypothesis that $n \geq 3$ in your discussion?
Hint: If $\sigma \neq e$ there are indices $i \neq j$ such that $\sigma(i) = j$. If $\sigma \in Z(S_n)$ then $\sigma(i,j)\sigma^{-1} = \big(\sigma(i), \sigma(j)\big)$ would equal (i,j) for all $i \neq j$.
Note: $S_n \cong \mathbb{Z}_2$ (abelian) when $n = 2$. $\square$

5.3.5 Exercise. In S_5 the permutations

$$\sigma = (13)(245) \qquad \text{and} \qquad \sigma' = (423)(15)$$

have the same cycle type 23. Find an explicit permutation τ such that $\tau\sigma\tau^{-1} = \sigma'$.
Note: The answer is not unique. Conjugation by τ should map (13) to (15) and (245) to (423). $\square$

5.3.5A Exercise. Compute the product aba^{-1} where $a = (1,3,5)(1,2)$ and $b = (1,5,7,9)$ in S_{10}. $\square$

5.3.5B Exercise. In S_n with $n = 10$:

(a) Find a permutation a such that $axa^{-1} = y$ if $x = (1,2)(3,4)$ and $y = (5,6)(3,1)$

(b) Explain why there is no element a such that $a(1,2,3)a^{-1} = (1,3)(5,7,8)$.

(c) Explain why there is no element a such that $a(1,2)a^{-1} = (3,4)(1,5)$.

5.3.5C Exercise. Describe all conjugacy classes in S_6, providing an explicit class representative for each conjugacy class. Count the number of elements in each class and verify the class equation for this group. $\square$

5.3.5D Exercise. The *stabilizer* of a permutation σ is the subgroup

$$\mathrm{Stab}_{S_n}(\sigma) = \{x \in S_n : x\sigma x^{-1} = \sigma\}$$

List all elements in the stabilizers of the following permutations

(a) $\sigma = (123)$ in S_5 (b) $\sigma = (12)(345)$ in S_5

What are the cardinalities of these stabilizers? $\square$

5.3.5E Exercise. Prove that every element of S_n can be written as a product $\sigma = \tau_1 \cdot \ldots \cdot \tau_r$ of "flips," the two-cycles

$$(1,2) \quad (2,3) \quad \ldots \quad (n,1)$$

that interchange *adjacent* elements in the cyclically ordered set $[1,n]$.
Hint: It suffices to show any 2-cycle (i,j) is a product of "flips." (Why?) Consider the effect of conjugation operations on (i,j). $\square$

More about the Alternating Group $\mathbf{A_n}$. The next results are specifically concerned with A_n. The end result is to show that A_n is a **simple** group for $n \geq 5$ (but not $n = 2,3,4$), which means that A_n contains no proper normal subgroups. Simple groups cannot be reduced to nontrivial smaller groups by taking quotients, and are in a sense the fundamental "building blocks" for constructing all finite groups.

5.3.6 Lemma. *For $n \geq 3$ the alternating group A_n is generated by the set of all 3-cycles in S_n.*

Proof: Three-cycles are even permutations, so they all lie in A_n. By definition every element of A_n is a product of an *even* number of 2-cycles, so it suffices to show that every product $(i,j)(k,\ell)$ is a product of 3-cycles. If these 2-cycles are equal their product is e, which can also be written as $e = (123)(132)$; if they have just one entry in common, say $j = k$, then $(i,j)(j,\ell) = (i,j,\ell)$ is already a 3-cycle. If they have no entry in common they commute and then a direct calculation reveals that $(i,j)(k,\ell) = (i,j,k)(j,k,\ell)$, proving the lemma. $\square$

5.3.7 Lemma. *If $n \geq 5$ all 3-cycles are conjugate in A_n – i.e. if σ, σ' are 3-cycles, then there exists some $\tau \in A_n$ such that $\sigma' = \tau\sigma\tau^{-1}$.*

Proof: We know that two 3-cycles $\sigma = (i,j,k)$ and $\sigma' = (i',j',k')$ are *conjugate within* S_n because they have the same cycle type, so there is some $\tau \in S_n$ such that $\sigma' = \tau\sigma\tau^{-1}$. If τ is even we're done. Otherwise, since $n \geq 5$, we can find $r, s \in [1,n]$ not equal to any of the elements i,j,k. Then (r,s) commutes with σ, and we may replace τ by $\tau' = \tau \cdot (r,s)$ to get an even permutation that conjugates σ to σ'. $\square$

5.3.8 Theorem. *If $n \geq 5$ the alternating group A_n is simple.*

Proof: Let N be a nontrivial normal subgroup of A_n. We prove that N contains a 3-cycle. Since all 3-cycles are A_n-conjugate, all 3-cycles lie within N, and hence $N = A_n$ by 5.3.6.

Let $\sigma \neq e$ be an element in N whose set of fixed points $\mathrm{Fix}(\sigma) = \{k \in X : \sigma(k) = k\}$ is as large as possible, where $X = [1,n]$. We prove that σ must be a 3-cycle. If we decompose $X = \mathcal{O}_1 \cup \ldots \cup \mathcal{O}_r$ into disjoint orbits under $H = \langle\sigma\rangle$, then at least one orbit must be nontrivial, for otherwise $\sigma = e$.

Case 1: All orbits (except the fixed points) have 2 elements. Then σ is a product of commuting disjoint 2-cycles; the number of factors is even, so there must be at least two distinct 2-point orbits $\{i,j\}$ and $\{k,\ell\}$. On their union $S = \{i,j,k,\ell\}$ the action of σ is the same as that of the product $(i,j)(k,\ell)$. Notice that $\mathrm{Fix}(\sigma) \cap \{i,j,k,\ell\} = \emptyset$.

Since $n \geq 5$ we can pick an integer $r \neq i, j, k, \ell$. Form the 3-cycle $\tau = (k, \ell, r)$ and consider the commutator $\sigma' = [\tau, \sigma] = \tau\sigma\tau^{-1}\sigma^{-1}$. Since N is normal in A_n we get $\sigma \in N \Rightarrow \tau\sigma\tau^{-1} \in N \Rightarrow \sigma' \in N$. By its definition, σ' must leave fixed the integers i and j, and it obviously leaves fixed the points in $\mathrm{Fix}(\sigma) \sim \{r\}$. Thus $|\mathrm{Fix}(\sigma')| \geq 1 + |\mathrm{Fix}(\sigma)|$, contradicting the maximality property of σ. The only remaining possibility is:

Case 2: There is some orbit with $|\mathcal{O}| \geq 3$. Suppose $i, j, k \in \mathcal{O}$ with $\sigma : i \to j \to k \to \ldots \to i$. If $\mathcal{O}$ consists only of these three points in X, then σ is already the 3-cycle (i, j, k), and we're done. If $\mathcal{O}$ includes just one more point r, then σ would be the odd 4-cycle (i, j, k, r), which is impossible. Thus $\mathcal{O}$ includes at least two more points r, s and $\sigma : i \to j \to k \to r \to s \to \ldots \to i$. Let $\tau = (k, r, s)$, and form the commutator σ' as before. Then $\sigma' \in N$ and $\sigma'(j) = j$. Since $\mathrm{Fix}(\sigma') \supseteq \mathrm{Fix}(\sigma)$ and $j \notin \mathrm{Fix}(\sigma)$, the element σ' has more fixed points than σ, which is impossible. Thus the only viable possibility in Case 2 is: σ was a 3-cycle to begin with. □

5.3.9 Exercise. If $n \geq 5$ prove that $(e) \subseteq A_n \subseteq S_n$ are the only normal subgroups in S_n. □

For future reference we note that the A_n-conjugacy classes in A_n can be described using what we know about S_n-classes in S_n together with the following observation.

5.3.10 Proposition. *Let $G = S_n$ and $A = A_n$ for $n \geq 3$. For $s \in A$ we have $G \cdot s = A \cdot s$ (orbits under conjugation) $\Leftrightarrow$ the stabilizer $\mathrm{Stab}_{S_n}(s) = \{\sigma \in S_n : \sigma s \sigma^{-1} = s\}$ is not contained in A. If $\mathrm{Stab}_{S_n}(s) \subseteq A$ the G-orbit $G \cdot s$ is the union of two A-orbits of equal cardinality.*

Proof: If $s' = gsg^{-1}$ we get $\mathrm{Stab}_{S_n}(s') = g\,\mathrm{Stab}_{S_n}(s)g^{-1}$, thus $\mathrm{Stab}_{S_n}(s) \subseteq A_n \Leftrightarrow \mathrm{Stab}_{S_n}(s') \subseteq A_n$ for any s' in the S_n-conjugacy class $G \cdot s$. If $\mathrm{Stab}_{S_n}(s) \subseteq A_n$ then $\mathrm{Stab}_{A_n}(s) = \mathrm{Stab}_{S_n}(s) \cap A_n = \mathrm{Stab}_{S_n}(s)$ and $|G \cdot s| = |G/\mathrm{Stab}_{S_n}(s)| = 2|A_n/\mathrm{Stab}_{S_n}(s)|$, so $G \cdot s =$ two A_n-orbits of equal size. If $\mathrm{Stab}_{S_n}(s) \not\subseteq A_n$, let $g_0 \in \mathrm{Stab}_{S_n}(s) \sim A_n$. For $g \in G \sim A_n$ we have $g \cdot s = gg_0^{-1} \cdot (g_0 \cdot s) = gg_0^{-1} \cdot s$. But $gg_0^{-1} \in A_n$ because the product of two odd permutations is even, so $G \cdot s = A \cdot s$. □

As an example: the S_5-orbits in A_5 are described by their cycle types, as above. Computing stabilizers, we can determine which of these S_5 orbits split into two A_5-conjugacy classes, with the following result.

Cycle Type	**Representative**	**# Elements**	**Stabilizer**	$\mathrm{Stab}_{S_n}(s) \subseteq A_5$?
11111	e	1	G	no
113	(123)	20	contains (45) and (123)	no
122	(12)(34)	15	contains (12) and (34)	no
5	(12345)	24	$\langle(12345)\rangle \cong \mathbb{Z}_5$	yes

The last S_5-class splits into two A_5-classes, each of order 12.

We only need to know whether $\mathrm{Stab}_{S_5}(s) \subseteq A_5$ to determine the sizes of all A_5-classes. Table entries under the heading "Stabilizer" were determined as follows. For the 22-cycle $\sigma = (12)(34)$ we have

$$\tau\sigma\tau^{-1} = \big(\tau(1), \tau(2)\big)\big(\tau(3), \tau(4)\big) = \left\{ \begin{array}{l} (21)(34) \text{ if } \tau = (12) \\ (12)(43) \text{ if } \tau = (34) \end{array} \right\} = \sigma$$

so the stabilizer contains (12) and (34) and cannot lie within A_5. There are other elements in this stabilizer. For instance conjugation by the 22-cycle $\tau = (13)(24)$ switches $(12) \leftrightarrow (34)$ but has no effect on their product $\sigma = (12)(34)$. In fact, the full stabilizer of σ is the 4-element subgroup containing all 22-cycles

$$\mathrm{Stab}_{S_5}(\sigma) = \{e\,,\ (12)(34)\,,\ (13)(24)\,,\ (14)(23)\,\}$$

As another example, τ stabilizes $\sigma' = (12345) \Leftrightarrow \big(\tau(1), \tau(2), \ldots, \tau(5)\big) = (12345)$, which happens $\Leftrightarrow \tau$ is a "j-shift on the cyclic-ordered list (12345): $\tau(i) \equiv i + j \pmod 5$ for all i. Since σ' is the 1-shift that means $\tau = (\sigma')^j \in \langle \sigma' \rangle$ so $\mathrm{Stab}_{S_5}(12345) = \langle\, (12345) \,\rangle \subseteq A_5$ as claimed.

5.4. The Structure of S_3 and S_4.

We now examine the pattern of subgroups in S_3 and S_4 (as well as A_3, A_4), giving a complete analysis for S_3. This information is often needed to analyze the structure of more complicated groups. There is nothing much to say about the abelian group $S_2 \cong \mathbb{Z}_2$; for $n \geq 5$ the situation is more complicated, and the pattern of subgroups changes dramatically.

5.4.1 Example (Subgroups in $\mathbf{S}_3$). The order of S_3 is $3! = 6$, so by Lagrange a subgroup $H \subseteq S_3$ can only have order $|H| = 1, 2, 3, 6$. The extreme values correspond to the trivial subgroups $H = (e)$ and $H = S_3$.

Case 1: $|H| = 3$. The alternating group $A_3 = \ker(\mathrm{sgn}) = \{e\} \cup \{\text{two 3-cycles}\}$ is a *normal* subgroup of order $6/2 = 3$ since $|S_n/A_n| = 2$ for any n. Obviously $A_3 \cong \mathbb{Z}_3$ since there is only one group of order 3. There are no other subgroups of order three in S_3, for if $|H| = 3$ then $H \cap A_3$ is a subgroup in both A_3 and H, and by Lagrange can only have order 3 (in which case $H = A_3$) or 1 (and then $A_3 \cap H = (e)$). The latter possibility cannot arise. If it did, then by the counting principle 3.4.7 the product set would have cardinality $|HA_3| = |H| \cdot |A_3| \,/\, |H \cap A_3| = 9$, which exceeds $|S_3| = 6$. Only one case remains.

Case 2: $|H| = 2$. The cycle types in S_3 are

Cycle Type	**Example**	**#(Elements in $\mathbf{S}_3$)**
111	e	1
12	any 2-cycle	3
3	any 3-cycle	2

All elements of S_3 are accounted for since $1 + 3 + 2 = 6$. If $|H| = 2$ it cannot contain a

$$\begin{array}{ccccccc} & & & S_3 & & & \\ & & \nearrow & \uparrow & \nwarrow & & \\ H_1 = \langle(12)\rangle & & H_2 = \langle(13)\rangle & & H_3 = \langle(23)\rangle & & A_3 \\ & & \nwarrow & \uparrow & \nearrow & & \\ & & & (e) & & & \end{array}$$

Figure 5.3. The pattern of subgroups in the permutation group S_3. The only normal subgroup is A_3.

3-cycle, since they have order 3. Hence $H = \langle \sigma \rangle \cong \mathbb{Z}_2$ for some 2-cycle σ. There are only three 2-cycles (1,2), (1,3), (2,3). Each generates a different subgroup H and $H \cap A_3 = (e)$ in every case. The pattern of subgroups is shown in Figure 5.3, where arrows $A \to B$ indicate inclusions $A \subseteq B$. None of the H_i are normal in S_3.

A_3 is the only proper *normal* subgroup. Taking the quotient we get the sequence of homomorphisms

$$e \longrightarrow A_3 \cong \mathbb{Z}_3 \longrightarrow S_3 \xrightarrow{\ \pi\ } S_3/A_3 \cong \mathbb{Z}_2 \longrightarrow e$$

in which $A_3 \cong \mathbb{Z}_3$ and $S_3/A_3 \cong \mathbb{Z}_2$. As we will explain in Section 6.4, this means S_3 is a *solvable* group, a fact that assumes great importance in Galois theory. In Section 6.2 we will conduct a complete analysis of *all* possible groups of order 6, up to isomorphism, and there we will discover a natural geometric interpretation of S_3 as the symmetry group of the equilateral triangle. The subgroups $H_1, \ldots, H_3, A_3$ also have natural interpretations in this geometric setting. They correspond to the three reflections across lines extending from a vertex to the midpoint of the opposite edge. $\square$

This discussion made effective use of the pattern of conjugacy classes in S_3, which by Corollary 5.3.3 correspond precisely to the various cycle types. We will exploit this again in the analysis of *normal* subgroups in S_4. The following observation is particularly useful in searching for normal subgroups in any finite group.

5.4.2 Lemma. *Let $C_0 = (e), C_1, \ldots, C_r$ be the distinct conjugacy classes in a group G, and let H be any subgroup. Then H is normal in G if and only if it is a union $H = C_{i_1} \cup \ldots \cup C_{i_s}$ of whole conjugacy classes from G.*

PROOF: If $x \in H$ and $H \lhd G$, then by definition of "normality" the entire conjugacy class $C_x = \{gxg^{-1} : g \in G\}$ must be contained in H. Therefore $H \lhd G \Rightarrow H$ is a union of whole conjugacy classes from G. Conversely if H is a subgroup and is a union of whole conjugacy classes, each class is invariant under conjugation $\alpha_g(y) = gyg^{-1}$, and hence $gHg^{-1} \subseteq H$ for all $g \in G$. $\square$

5.4.3 Exercise. In S_3 verify that the subgroup $H = \langle(12)\rangle$, consisting of the elements e and (12), is *not* a normal subgroup. Is the same true in S_n for $n > 3$? $\square$

Once we have determined the conjugacy classes in a group G we can determine normal subgroups in G by seeking ways to combine classes so that their union is a subgroup. Obviously we must include the trivial class $C_0 = (e)$; other classes must be added in pairs, owing to the following symmetry among conjugacy classes in any group.

***5.4.4 Exercise.** Let G be a group and $C_x = \{gxg^{-1} : g \in G\}$ any conjugacy class. Prove that

(a) *The inversion map $J(y) = y^{-1}$ permutes the conjugacy classes in G.* That is, the J-image $J(C_x) = \{y^{-1} : y \in C_x\}$ of any conjugacy class is again a single conjugacy class.

(b) Verify that $J(C_x) = C_{x^{-1}}$ for any $x \in G$. $\square$

Some classes can be their own inverses; a trivial example is the class $C_0 = (e)$, but there are other possibilities such as the class consisting of all 2-cycles.

If we are lucky, there will not be many conjugacy classes to consider. We are aided by the following observation.

The following purely numerical constraints

(14)
(i) $|H| = |C_{i_1}| + \ldots + |C_{i_s}|$
(ii) $|H|$ *must divide* $|G|$

restrict the combinations of classes whose union can be a subgroup H.

5.4.5 Exercise. Use Lemma 5.4.2 to obtain an alternative proof that A_3 is the only proper normal subgroup in S_3. $\square$

5.4.6 Example (Normal Subgroups in $\mathbf{S}_4$). Since $|S_4| = 4! = 24$, subgroups can only have orders $|H| = 1, 2, 3, 4, 6, 8, 12, 24$. The alternating group $A_4 = \ker(\mathrm{sgn})$ has index $|S_4/A_4| = 2$ because the left multiplication operator $\lambda(\sigma) = (12)\cdot\sigma$ on S_n sends odd permutations to even, and vice-versa. Thus A_4 is a normal subgroup of order 12. It is less obvious that A_4 is the *only* normal subgroup of order 12, but in fact we will soon show that it is.

The possible cycle types in S_4 are easy to enumerate.

Table 5.1

Cycle Type	Example	#(Elements in $\mathbf{S}_4$)
1111	e	1
112	any 2-cycle	$6 = \frac{4\cdot 3}{2}$
13	any 3-cycle	$8 = \frac{4\cdot 3\cdot 2}{3}$
22	any 22-cycle	$3 = \frac{1}{2}\cdot\frac{4\cdot 3}{2}\cdot\frac{2\cdot 1}{2}$
4	any 4-cycle	$6 = \frac{4\cdot 3\cdot 2\cdot 1}{4}$

In arriving at the counts for each type you must recall the ambiguities in cycle notation noted in 5.1.1. The count of 22-cycles involves the extra redundancy $(12)(34) = (34)(12)$, in addition to the fact that $(12) = (21)$ and $(34) = (43)$; hence the extra factor $\frac{1}{2}$ out front.

All classes are accounted for since there are $1 + 6 + 3 + 8 + 6 = 24$ elements in all. As in 5.3.3, all elements of the same cycle type constitute a single conjugacy class in S_4. The only combinations of classes whose union has cardinality 12 are: (i) 6 + 6 and (ii) 1 + 3 + 8 ; the first cannot produce a subgroup since the class $C_0 = (e)$ is not included, and the second produces A_3. Hence A_3 is the *only* normal subgroup of order 12. By examining our counts of cycle types we see immediately that there cannot be normal subgroups of order $8, 6, 3,$ or 2. Excluding the trivial normal subgroups $H = (e)$ and $H = S_4$, there is one remaining possibility.

Case 2: $|H| = 4$. The only combination of classes whose sizes add up to 4 is 1 + 3, corresponding to

$$H = \{e\} \cup \{\text{ all 22-cycles}\} = \{e\} \cup \{(12)(34), (13)(24), (14)(23)\}$$

It is easily checked that the 2,2-cycles $a = (12)(34), b = (13)(24), c = (14)(23)$ satisfy the relations $a^2 = b^2 = c^2 = e$ and $ab = c = ba, bc = a = cb, ca = b = ac$. This abelian group $H = V_4$ is sometimes known as the *Klein Viergroup*. Up to isomorphism it is one of two possible groups of order 4, the other being the cyclic group $\mathbb{Z}_4$. (We will verify this in Section 6.2.)

The normal subgroups in S_4 are related by a chain of inclusions

$$(e) \subseteq V_4 \subseteq A_4 \subseteq S_4$$

Each is normal in G, and hence in the next larger group in the chain. The quotient groups are $V_4 = V_4/(e)$, $A_4/V_4 \cong \mathbb{Z}_3$, and $S_4/A_4 \cong \mathbb{Z}_2$. The last two isomorphisms follow from the fact that, up to isomorphism, the only groups of order 2 or 3 are $(\mathbb{Z}_2, +)$ and $(\mathbb{Z}_3, +)$; simple counting shows that $|A_4/V_4| = 12/4 = 3$ and $|S_4/A_4| = 24/12 = 2$. As we will explain in Section 6.4, the fact that the successive quotients are all abelian means that S_4 is a *solvable* group, and this turns out to be the reason that there exist algorithms for finding the (complex) roots of any polynomial of degree $\deg(f) \leq 4$. The above diagram also shows that A_4 is not a *simple* group, because the proper subgroup V_4 is normal in S_4, and hence in A_4. $\square$

There is a simple model for Klein's group V_4. If we equip the Cartesian product set $\mathbb{Z}_2 \times \mathbb{Z}_2$ with the following binary operation

$$(a, b) * (a', b') = (a + a', b + b') \qquad \text{(add components separately, as with vectors)}$$

it is easy to verify that $G = (\mathbb{Z}_2 \times \mathbb{Z}_2, *)$ is a group. It has four elements $e = (0,0), a = (1,0), b = (0,1), c = (1,1)$. The group is abelian with $|G| = 4$ but the nonzero elements all have order $o(x) = 2$ so G cannot be isomorphic to the cyclic group $(\mathbb{Z}_4, +)$. Nontrivial elements satisfy the relations

$$a * b = c \qquad b * c = a \qquad c * a = b$$

which suffice to construct the multiplication table in Table 5.2.

$*$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Table 5.2 Multiplication table for $(\mathbb{Z}_2 \times \mathbb{Z}_2, *)$. The group is abelian because table entries are symmetric across the diagonal. Obviously $a^2 = b^2 = c^2 = e$ and $a * b = c, b * c = a, c * a = b$.

5.4.7 Exercise. Verify the counts shown in the right hand column of Table 5.1. Verify that there are no normal subgroups in S_4 of order $|N| = 8, 6, 3$, or 2. $\square$

5.4.8 Exercise. Identify all A_4-conjugacy classes in A_4 using the results posted in Proposition 5.3.10 and the cycle types listed in Table 5.1. $\square$

5.4.9 Exercise. Determine all subgroups $H \subseteq A_4$ that are *normal subgroups of* A_4.
Hint: We have already discussed the nature of S_n- and A_n-conjugacy classes in A_n. $\square$