Notes: F.P. Greenleaf 2000 - 2008

Algebra I: Section 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 interval $X = \{1, 2, \ldots, n\}$, 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*

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

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: the following symbols

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

all describe the same operation on X. 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 $(123) \neq (132)$.

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

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

$$\mathrm{supp}(\sigma) \cap \mathrm{supp}(\tau) = \{m_1, \ldots, m_k\} \cap \{n_1, \ldots, n_r\} = \emptyset \tag{2}$$

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*

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

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 $\text{supp}(\tau_i) = \mathcal{O}_i$. For the one-point orbits we simply take the 1-cycles $\tau_i = (x_i)$. There must, however, be some nontrivial orbits, for if every orbit were trivial we would have $\sigma = \text{id}_X$, which has been excluded.

For a nontrivial orbit $\mathcal{O} = H \cdot x$ we first observe that in the 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 $\sigma^\ell(x)$, $0 \leq \ell < k$. In fact, this can only happen by having $\{x, \sigma(x), \ldots, \sigma^{k-1}(x)\}$ distinct and $\sigma^k(x) = x$. [If $\ell > 0$ the definition of k is violated because $\sigma^k(x) = \sigma^\ell(x) \Rightarrow \sigma^{k-\ell}(x) = x$.] The list $\tau = (x, \sigma(x), \ldots, \sigma^{k-1}(x))$ enumerates the points in $\mathcal{O}$ in a particular order, and determines a cycle with $\text{supp}(\tau) = \mathcal{O}$. This 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 just a cyclically shifted version of $x, \sigma(x), \sigma^2(x), \ldots \sigma^{k-1}(x)$. 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 $X = \text{supp}(\tau_1) \cup \ldots \cup \text{supp}(\tau_r)$, and the τ_i commute because their supports are disjoint. Furthermore

(i) σ and τ_i have the same actions on the orbit $\mathcal{O}_i$

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

and from this it is apparent that $\sigma = \prod_{i=1}^r \tau_i$ throughout the space 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. □

One-point orbits must be taken into account in partitioning X, so the corresponding 1-cycles must be included in the factorization of σ if the support condition (3) is to hold. 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: For (c) no calculation is necessary, since the action $H \times \mathcal{O} \to \mathcal{O}$ on each orbit is transitive (see Section 4.2). □

5.1.4 Exercise. If σ and τ are nontrivial cycles 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?* □

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*

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

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 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, which makes it easy to enumerate all the types for a given n.

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.

5.1.6 Exercise. Here is a permutation in S_8, described by telling where each element in $X = [1, 8]$ ends up

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

Determine the decomposition into disjoint cycles and the cycle type of σ. □

5.1.7 Exercise. If $\sigma \in S_n$ has cycle indices $n_1 \le \ldots \le n_r$ prove that the order of σ as an element of S_n is the *least common multiple* $\mathrm{lcm}(n_1, \ldots, n_r)$ of those indices.
Hint: Try $r = 2$ to get started. □

5.1.8 Exercise. Table 1 above lists the cycle types in S_5. Verify the entries in the right-hand column by calculating the number of cycles of each type.
Hint: Recall our comments following 5.1.1 about the ambiguity inherent in our notation $\sigma = (i_1, \ldots, i_k)$ for cycles. □

5.2. Parity of a Permutation.

We now show that S_n is generated by its 2-cycles (i, j), so that 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 $e = (12)^2 = (12)^4$, etc. Nevertheless, there *is* something important that all such decompositions of σ have in common, as we shall see.

5.2.1 Lemma. *For $n \ge 2$, 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. □

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. □

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*

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

is uniquely determined. Furthermore, parity is multiplicative

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

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

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 $\operatorname{sgn}(\sigma)$. 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

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

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 $(\mathrm{GL}(n, \mathbb{R}), \circ)$ 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) $\det(\Phi(\sigma)) = \prod_{i=1}^{r} \det \Phi(\sigma_i) = (-1)^r = \operatorname{sgn}(\sigma)$ 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 into 2-cycles, so we get the same number $\operatorname{sgn}(\sigma) = (-1)^r$ 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 $\operatorname{sgn}(\sigma\tau) = \operatorname{sgn}(\sigma) \cdot \operatorname{sgn}(\tau)$. □

For obvious reasons, we say a permutation is **even** if it can be written as a product of an even

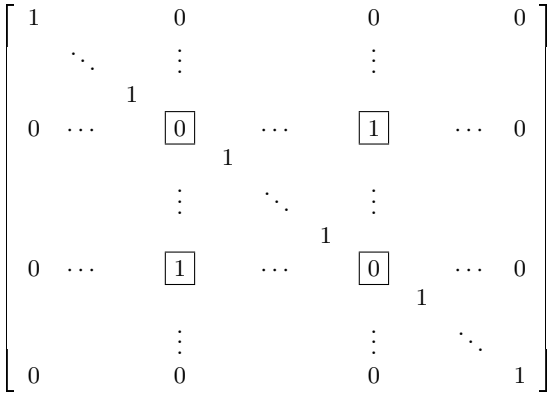

Figure 5.1. Permutation matrix associated with the 2-cycle $\sigma = (i, j)$ differs from the identity matrix only in rows/columns i and j.

number of 2-cycles, so that $\operatorname{sgn}(\sigma) = +1$, and otherwise it is **odd**. Note that the identity e is even, all 2-cycles are odd; the idea set forth in (5) immediately shows how to compute the parity of a cycle of any length.

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

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

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*

$$\operatorname{sgn}(\sigma) = (-1)^{k-1} \qquad \text{for } k = 1, 2, \dots \tag{8}$$

If σ is a product $\sigma = \sigma_1 \dots \sigma_r$ 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 $(1, 2, \dots, k) = (1, k)(1, k-1) \dots (1, 2)$. □

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

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

Since the parity map sgn *is a homomorphism between groups, its kernel A_n is obviously a normal subgroup in S_n. Furthermore, its index is $|S_n/A_n| = 2$. 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

For $n \geq 5$ we have

(10)

(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 $n = 3, 4$.

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 $\text{sgn}(\sigma)$ 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 12 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) $\sigma = (123)(45)(16789)(15)$ (b) $\tau = (12)(123)(12)$ □

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

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 conjugacy class 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*

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

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 in Figure 5.1 shows the actions of the operators τ^{-1}, σ, τ, and $\tau\sigma\tau^{-1}$ on elements of $X = [1, n]$. The shaded region in the second picture from the left is the support set $A = \text{supp}(\sigma) = \{m_1, \ldots, m_k\}$, and the other shaded regions are various images of A. Here $B = \tau(A) = \{n_1, \ldots, n_k\}$, where we write $n_i = \tau(m_i)$ for $1 \le i \le k$.

The support set A is invariant under σ (so that $\sigma(A) = A$) and σ *fixes* all points not in A (so $\sigma(j) = j$ for $j \notin A$). Obviously $\tau^{-1}(B) = \tau^{-1}\tau(A) = A$, as in the Figure 5.1. Furthermore,

$$\text{If } j \notin B, \text{ then } \tau^{-1}(j) \notin A, \text{ and then we have } \tau\sigma(\tau^{-1}(j)) = \tau\tau^{-1}(j) = j$$

Figure 5.2. The effect of conjugation $\sigma \mapsto \tau\sigma\tau^{-1}$ on a cycle $\sigma = (m_1, \ldots, m_k)$. Shaded regions are the sets $A = \text{supp}(\sigma) = \{m_1, \ldots, m_k\}$ and $B = \tau(A) = \{\tau(m_1), \ldots, \tau(m_k)\}$.

Thus, the conjugate $\tau\sigma\tau^{-1}$ acts trivially on all points that lie outside of B. On the other hand, if we consider a point $\tau(m_i)$ lying in B, then by the definition of "cycle" $\sigma = (m_1, \ldots, m_k)$ we get

$$\tau\sigma\tau^{-1}(\tau(m_i)) = \tau\sigma(m_i) = \begin{cases} \tau(m_{i+1}) & \text{if } 1 \leq i < k \\ \tau(m_1) & \text{if } i = k \end{cases}$$

Thus $\tau\sigma\tau^{-1}$ cyclically shifts entries one space to the right in the ordered list of integers $\tau(m_1), \ldots, \tau(m_k)$, leaving all other points in X fixed. It follows that $\tau(m_1, \ldots, m_k)\tau^{-1} = (\tau(m_1), \ldots, \tau(m_k))$. □

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

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

Thus we have determined 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 the support of σ, so that*

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

(*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 already been proved. For ($\Leftarrow$), suppose σ and σ' have the same cycle types $n_1 \leq \ldots \leq n_r$. The indices n_i are precisely the lengths of the cycles in the

disjoint cycle decompositions, so the decompositions of σ and σ' involve the same number r of disjoint cycles. Writing $C_i = \mathrm{supp}(\sigma_i),\ C_i' = \mathrm{supp}(\sigma_i')$ for the supports of the factors, we have $n_i = |C_i| = |C_i'|$ for each i. But the supports partition $X = [1, n]$

$$X = \bigcup_{i=1}^{r} C_i = \bigcup_{i=1}^{r} C_i' \qquad \text{with } C_i \cap C_j = \emptyset \text{ and } C_i' \cap C_j' = \emptyset \text{ for } i \neq j$$

It is then obvious that there exists a bijection $\psi : X \to X$ that

(i) maps C_i to C_i' for each i, and

(ii) preserves the cyclic order of the points in the cycles $\sigma_i = (m_1, \ldots, m_k)$ and $\sigma_i' = (m_1', \ldots, m_k')$, so that $\psi(m_j) = m_j'$ for $1 \leq j \leq k$, $1 \leq i \leq r$.

This map will not be uniquely determined, except for the one-point cycles, but that does not matter. The point is that ψ is a permutation in S_n, and has the properties

$$\psi\sigma_i\psi^{-1} = (\psi(m_1), \ldots, \psi(m_k)) = (m_1', \ldots, m_k') = \sigma_i' \qquad \text{for all } i$$

Hence $\psi\sigma\psi^{-1} = \sigma'$, as required. □

5.3.4 Exercise. For $n \geq 2$ prove that the center $Z(S_n) = \{\sigma \in S_n : \tau\sigma = \sigma\tau \text{ for all } \tau \in S_n\}$ is trivial.
Hint: The center is the union of all the one-point conjugacy classes. Which cycle types correspond to such classes? □

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). □

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, by (3), and then a direct calculation reveals that $(i, j)(k, \ell) = (i, j, k)(j, k, \ell)$, proving the lemma. □

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'. □

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 $\sigma' = \tau\sigma\tau^{-1}\sigma^{-1}$. 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 Lemma. *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 G_s is not contained in A, and if $G_s \subseteq A$ the G-orbit $G \cdot s$ is the union of two A-orbits of equal cardinality.*

PROOF: Since A is normal, $G_s \subseteq A \Leftrightarrow G_{s'} \subseteq A$ for any $s' \in G \cdot s$. [In fact, if $s' = gsg^{-1}$ then $G_{s'} = gG_sg^{-1} \subseteq A$.] If $s \in A$ and $G_s \subseteq A$ then $A_s = G_s \cap A = G_s$ and $|G \cdot s| = |G/G_s| = 2|A/G_s|$, so $G \cdot s$ splits into two A-orbits of equal size. If $G_s \not\subseteq A$, let $g_0 \in G_s \sim A$. For $g \in G \sim A$ we have $g \cdot s = gg_0^{-1} \cdot (g_0 \cdot s) = gg_0^{-1} \cdot s$. Here $gg_0^{-1} \in A$ because the product of two odd permutations is even, so $G \cdot s = A \cdot s$. □

As an example: taking $n = 5$, 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 G_s**	$G_s \subseteq A_5$?
1	e	1	G	no
22	(12)(34)	15	$\langle(12), (34)\rangle \cong \mathbb{Z}_2 \times \mathbb{Z}_2$	no
3	(123)	20	$\langle(45), (123)\rangle \cong \mathbb{Z}_2 \times \mathbb{Z}_3$	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. In general stabilizers of suitably chosen class representatives in A_n are fairly easy to compute, and in any case we only need to know whether $G_s \subseteq A_n$ to determine the pattern of A_n-classes.

5.4. The Structure of S_3 and S_4.

Here we 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 in analyzing 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 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 $A_3 = \ker(\text{sgn})$ is a *normal* subgroup of order $6/2 = 3$ since A_n has index $|S_n/A_n| = 2$ 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 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 3-cycle,

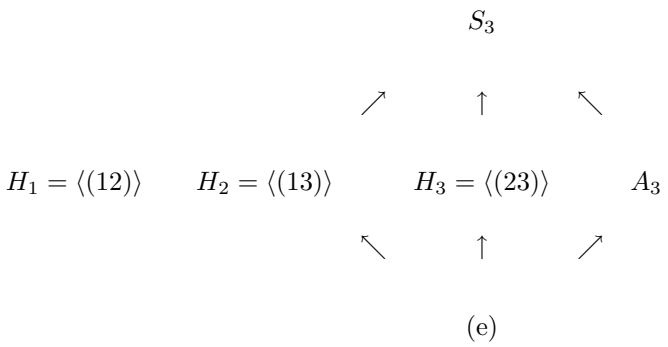

Figure 5.3. The pattern of subgroups in the permutation group S_3. The only normal subgroup is A_3.

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 such that $H \cap A_3 = (e)$. The pattern of subgroups is shown in Figure 5.3, where arrows $A \to B$ indicate inclusions $A \subseteq B$.

There is just one proper *normal* subgroup, namely A_3. Taking the quotient we get the sequence of homomorphisms

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

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 will assume great importance later on in our study of 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. □

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.

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 $g \in G$. □

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 $n > 3$?
Hint: $\tau H \tau^{-1} \neq H \Leftrightarrow \tau(12)\tau^{-1} \neq (12)$. (Why?) □

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 $x \in G$.

Some classes can be their own inverses (a trivial example being the class $C_0 = (e)$). □

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

$$\begin{aligned} &(i)\ |H| = |C_{i_1}| + \ldots + |C_{i_s}| \\ &(ii)\ |H| \text{ must divide } |G| \end{aligned} \tag{14}$$

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

5.4.5 Exercise. Use Lemma 5.4.2 to prove that A_3 is the only proper normal subgroup in S_3. □

5.4.6 Example (Normal Subgroups in S_4). Since $|S_4| = 4! = 24$, subgroups can only have orders $|H| = 1, 2, 3, 4, 6, 8, 12, 24$. The alternating group $A_4 = \ker(\text{sgn})$ has index $|S_4/A_4| = 2$, so A_4 is a normal subgroup of order 12. It is not so obvious that A_4 is the *only* such subgroup, but in fact it is.

The possible cycle types in S_4 are easy to enumerate.

Cycle Type	**Example**	**#(Elements in S_4)**
1111	e	1
112	any 2-cycle	$6 = \frac{4\cdot 3}{2}$
22	any 2,2-cycle	$3 = \frac{1}{2}\cdot\frac{4\cdot 3}{2}\cdot\frac{2\cdot 1}{2}$
13	any 3-cycle	$8 = \frac{4\cdot 3\cdot 2}{3}$
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 2,2-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.

5.4.7 Exercise. Verify the counts shown in the right hand column of this table. Where does the extra "$\frac{1}{2}$" come from in the count of 22-cycles? □

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

$$H = \{e\} \cup \{\text{ all 2,2-cycles }\} = \{e, (12)(34), (13)(24), (14)(23)\}$$

It is easily checked that the cycles $a = (12)(34), b = (13)(24), c = (14)(23)$ satisfy the relations $a^2 = b^2 = c^2 = e$ and $ab = c = ba$. 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 exists an algorithm 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. □

5.4.8 Exercise. Determine all normal subgroups in the alternating group A_4.
Hint: We have already discussed the nature of conjugacy classes in A_n. □