Chapter 5

The Symmetric Group

The symmetric group $S(n)$ plays a fundamental role in mathematics. It arises in all sorts of different contexts, so its importance can hardly be overstated. There are thousands of pages of research papers in mathematics journals which involving this group in one way or another. We have already seen from Cayley's theorem that every finite group can be treated as a subgroup of $S(n)$ for some n. We will also see below its presence in the orthogonal group $O(n, \mathbb{R})$, namely as the set of all $n \times n$ permutation matrices. It turns out that due to the $LPDU$ decomposition which we saw in Chapter 2 that $S(n)$ also plays a role in describing the structure of the general linear group $GL(n, \mathbb{F})$, as well as certain other linear groups.

The purpose of this Chapter is to derive some of the elementary properties of $S(n)$. For example, we will see that there are several standard ways of representing its elements. We will also take a somewhat historical sidetrip by showing how $S(n)$ was involved in the critical work of Marian Rejewski which led to the first breaking of the Enigma cipher machine employed by the German military during the Second World War and made possible the now well known successes in deciphering the Enigma made at Bletchley Park. This was one of the turning points in the Second World War. Another reason Rejewski's work was historically significant is that was the first instance where modern algebra was actually used to solve a non-pure (i.e. applied) problem.

5.1 The Structure of $S(n)$

As always, $S(n)$ is the group of bijections or permutations of a set of n objects, say $X_n = \{1, 2, \ldots, n\}$. Its group operation is the composition of

bijections. We will frequently refer to the objects being permuted as letters. This will be convenient for when we take up cryptography.

Recall the notation

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}.$$

To simplify the notation, we will notation by also write

$$\sigma = [\sigma(1), \sigma(2), \ldots, \sigma(n)].$$

We will also frequently denote the identity element of $S(n)$ by (1). Notice that for each n, we can embed $S(n)$ as a subgroup of $S(n+1)$, namely as the set of all permutations $\sigma \in S(n+1)$ such that $\sigma(n+1) = n+1$.

The next topic we take up is how to decompose a permutation into manageable pieces. The first method we will see is to use transpositions.

5.1.1 Transpositions

We now introduce a set of building blocks for the symmetric group. These are called transpositions.

Definition 5.1. A permutation σ which interchanges two letters i and j and leaves all the other letters unchanged is called a *transposition*. The transposition σ which interchanges i and j will be denoted by (ij).

Clearly, transpositions are the simplest permutations since if $\sigma \in S(n)$ moves the letter i to j, then j also is permuted to something else. Notice that by our convention that $S(n) \subset S(n+1)$, the transposition $(ij) \in S(n)$ for all n such that $i, j \leq n$. Transpositions are easy to multiply. For example, $(23)(12)$ represents the permutation

$$1 \to 2 \to 3, \quad 2 \to 1 \to 1, \quad 3 \to 3 \to 2.$$

Hence, $(23)(12) = [3, 1, 2]$.

Obviously there are two ways to write a transposition: $(ij) = (ji)$. Also, $(ij)^{-1} = (ij)$: each transposition is its own inverse.

Here are some further examples.

Example 5.1. Consider $S(3)$. We saw above that $(23)(12) = [3, 1, 2]$. Taking the product in the other order gives a different result, namely $(12)(23) = [2, 3, 1]$. Hence $(23)(12) \neq (12)(23)$. To continue this example, note that

$$[2, 3, 1](12) = (12)(23)(12) = [3, 2, 1] = (13).$$

We can therefore infer that $[2,3,1] = (13)(12)$. Thus $[2,3,1]$ can be written as a product of transpositions.

Here's another example.

Example 5.2. If $\sigma \in S(3)$ is arbitrary, then

$$[\sigma(1), \sigma(2), \sigma(3)](23) = [\sigma(1), \sigma(3), \sigma(2)].$$

That is, if we multiply on the right by (ij), we interchange $\sigma(i)$ and $\sigma(j)$. (We will also use thisfact below.) On the other hand,

$$(12)[2,3,1] = [1,3,2] = (23).$$

Thus multiplying on the left by (ij) interchanges i and j in σ. Notice also that

$$(12)[2,3,1](12) = (23)(12) = [3,1,2].$$

The basic result is that every element of $S(n)$ can be decomposed into a product of transpositions. For example, from the last calculation, $[2,3,1] = (13)(12) = (12)(23)$. More generally, we have

Proposition 5.1. *If $n > 1$, every element of $S(n)$ can be represented in some (non-unique) way as a product of transpositions.*

Proof. Let $\sigma \in S(n)$ be represented as $\sigma = [\sigma(1), \sigma(2), \ldots, \sigma(n)]$. Suppose $\sigma(n) = k$. Then $(kn)\sigma(n) = n$, and we have

$$(kn)\sigma = [\sigma(1), \sigma(2), \ldots, \sigma(n), \ldots, \sigma(n-1), n],$$

where $\sigma(n)$ is the k-th component above. Now let us induct on n. The result is clear if $n = 2$, so let's suppose it's true for $n-1$ where $n \geq 3$. But then with σ as above, $\sigma' = [\sigma(1), \sigma(2), \ldots, \sigma(n-1)] \in S(n-1)$ can be represented as a product of transpositions lying in $S(n-1)$, say $\sigma' = t_1 \cdots t_m$. Hence, $\sigma = (kn)t_1 \cdots t_m$ is a representation of σ as a product of transpositions. This completes the proof. □

In practice, finding this product representation of an element of $S(n)$ is analogous to what you do when you invert a matrix using row operations. Here's an example.

Example 5.3. Consider $[2,4,1,3] \in S(4)$. We have

$$[2,4,1,3](13) = [1,4,2,3], \quad [1,4,2,3](23) = [1,2,4,3],$$

and

$$[1,2,4,3](34) = [1,2,3,4] = e.$$

Hence

$$[2,4,1,3](13)(23)(34) = [1,2,3,4] = e.$$

Therefore,

$$[2,4,1,3] = (34)(23)(13),$$

since $(ij)^{-1} = (ij)$.

5.1.2 Simple Transpositions and the Length Function

Certain transpositions can be further decomposed into transpositions. For example, $(13) = (12)(23)(12)$. The special transpositions used here, i.e. those of the form $(i\ i+1)$, are called *simple transpositions.* For another example, note that

$$(14) = (12)(23)(34)(23)(12).$$

Observe that $(14) = \pi(34)\pi^{-1}$, where $\pi = (12)(23)$. Hence, we can refine Proposition 5.1 as follows.

Proposition 5.2. *If $n > 1$, every element of $S(n)$ can be represented as a product of simple transpositions, although the representation still won't be unique.*

One of the ways that the simple transpositions are used is to measure the complexity of an element of $S(n)$. We associate a length to an element of $S(n)$ as follows.

Definition 5.2. The length $\ell(\sigma)$ of an element σ of $S(n)$ is defined to be the least number simple transpositions (counted with multiplicity) needed to express σ. A minimal length expression of an element σ is said to be *reduced.*

For example, the length of a simple transposition is 1, but $\ell(14) = 5$ since the expression $(14) = (12)(23)(34)(23)(12)$ is minimal. The length function has a number of interesting properties, some of which we will state in the next theorem. The proof of this result will be omitted.

Theorem 5.3. *The length function ℓ on $S(n)$ has the following properties:*

(i) If τ is a simple transposition, then for any $\sigma \in S(n)$, $\ell(\tau\sigma) = \ell(\sigma) \pm 1$ and $\ell(\sigma\tau) = \ell(\sigma) \pm 1$.

(ii) For any $\sigma \in S(n)$, $\ell(\sigma) = \ell(\sigma^{-1})$.

(*iii*) *There exists a unique element* $\sigma_0 \in S(n)$ *of maximal length. The length* $\ell(\sigma_0)$ *of* σ_0 *is* $n(n1-)/2$.

(*iv*) *For any* $\sigma \in S(n)$, $\ell(\sigma\sigma_0) = \ell(\sigma_0\sigma) = \ell(\sigma_0) - \ell(s)$.

The element σ_0 is called the *longest element* of $S(n)$.

Example 5.4. We can see how it works in the case of $S(3)$. The simple transpositions were denoted by σ_1 and σ_2, and the elements of $S(3)$ beyond the identity are $\sigma_1,\ \sigma_2,\ \sigma_1\sigma_2,\ \sigma_2\sigma_1$, and $\sigma_1\sigma_2\sigma_1 = \sigma_2\sigma_1\sigma_2$. Note that every expression here is reduced. Then we can see directly that multiplying any element by a simple transposition changes its length by ± 1.

5.1.3 Cycle Notation

In addition to representing permutations as products of transpositions, there is another standard technique for representing permutations. This is called the cycle notation.

Definition 5.3. A element σ of $S(n)$ is called a k-cycle if and only if $\sigma(i) = i$ for all but k integers i with $1 \leq i \leq n$, and if $\sigma(i) \neq i$, then $i, \sigma(i), \sigma^2(i), \ldots, \sigma^{k-1}(i)$ are the integers which σ permutes, i.e. does not fix. Such an element of $S(n)$ will be denoted by $(i\ \sigma(i)\ \sigma^2(i)\ \cdots\ \sigma^{k-1}(i))$.

We can illustrate cycle notation by taking an example from $S(4)$. The permutation $\sigma = [2, 3, 4, 1]$, namely

$$1 \to 2, \quad 2 \to 3, \quad 3 \to 4, \quad 4 \to 1$$

is the cycle denoted by

$$(1234)$$

since each each letter i is sent to the one to its right and the last letter is sent back to the first. This notation is slightly ambiguous, since each one of the cycles (1234), (2341), (3412) also represents σ. One gets around this by simply agreeing to identify two symbols if they represent the same permutation. Thus the symbols (1234), (2341) and (3412) are all equal since they stand for the same permutation. Notice that the entries occuring in a cycle don't need to be consecutive. For example, (135) is a 3-cycle in $S(5)$. Also note that a one cycle, e.g. (i), is the same as the identity permutation, which we have already agreed to denote by (1). Thus the only one cycle we will use is (1).

Transpositions are cycles of length two. For example, the transposition σ given by

$$1 \to 1, \quad 2 \to 3, \quad 3 \to 2, \quad 4 \to 4$$

is denoted by the cycle

$$(23).$$

Cycles are multiplied, like transpositions, by composing their permutations. For example, $(123)(13) = [1, 3, 2, 4] = (23)$. Two cycles that don't share a common letter are said to be *disjoint*, for example (13) and (24). Disjoint cycles commute. Indeed, since they act on different sets of letters, it doesn't matter in which order they are applied. Hence the product of two or more disjoint cycles can be written in any order, e.g. $(13)(24)(56) = (56)(24)(13)$ or $(123)(456) = (456)(123)$ in $S(6)$.

Non-disjoint cycles do not commute, however: $(ab)(bc) = (abc)$ while $(bc)(ab) = (acb)$. The important point is that all elements of $S(n)$ can be expressed as products of *disjoint cycles*, as we now prove.

Proposition 5.4. *Every element σ of $S(n)$ different fromn (1) can be written as a product of disjoint cycles of lengths greater than one. In any such representation of σ, the cycles themselves are unique, but the order in which they are written is irrelevant.*

Proof. Given σ, we can construct its cycle decomposition as follows. Consider the sequence $\sigma(1),\ \sigma^2(1),\ \ldots$. Eventually, this sequence has to repeat, and if the first repetition occurs after i applications of σ, we have $\sigma^i(1) = 1$ with i minimal. If $i = 1$, then (1) is a cycle. However, since a cycle of length one is the identity in $S(n)$, we can just omit it. If $i > 1$, then $(1\ \sigma(1)\ \sigma^2(1) \cdots\ \sigma^{i-1}(1))$ will be a cycle in σ. Now repeat this process with the smallest integer m not appearing among the powers $\sigma^j(1)$, ommiting one cycles. Continuing in this manner, we will eventually include every element i which σ does not fix in a cycle, so we obtain a cycle representation.

The proof of uniqueness will be by induction. Suppose we have a cycle representation of σ, say $\sigma = c_1 c_2 \cdots c_k$. If $k = 1$, the representation is clearly unique. Thus suppose $k > 1$, and assume uniqueness holds for all cycle decompositions involving less than k disjoint cycles. Let $\sigma = d_1 d_2 \cdots d_m$ be another disjoint cycle representation of σ. Since we can rearrange the product in any order, we may suppose that 1 occurs in both c_1 and d_1. It is thus clear that $c_1 = d_1$. Hence $c_2 \cdots c_k$ and $d_2 \cdots d_m$ are two disjoint cycle representations of $c_1^{-1}\sigma = d_1^{-1}\sigma$. By the induction hypothesis, $k = m$, and the cycles $c_2, \ldots, c_k$ and $d_2, \ldots, d_k$ coincide up to order. This proves the uniqueness assertion and thus finishes the proof. □

Example 5.5. Lets express the element $\sigma = [2, 3, 1, 5, 4] \in S(5)$ as a product of disjoint cycles. Now $\sigma(1) = 2, \sigma(2) = 3, \sigma(3) = 1$. Thus, (123) will be one of the cycles. The other will be (45), so $\sigma = (123)(45)$. Similarly,

$\tau = [5, 3, 2, 1, 4]$ will have (154) and (23) as its disjoint cycles. Thus $\tau = (154)(23)$

5.1.4 Conjugacy Classes

We will now prove another result about the disjoint cycle representation. Two elements σ and σ' of $S(n)$ will be said to have the same cycle structure if in their disjoint cycle representations $\sigma = c_1 c_2 \cdots c_k$ and $\sigma' = c'_1 c'_2 \cdots c'_m$ have the same number of cycles (i.e. $k = m$) and for each subscript i, the cycle length of c_i and the cycle length of c'_i coincide. We now introduce a new definition, which allows us to say when two permutations have the same cycle structure.

Definition 5.4. Let G be an aribitrary group. Two elements a, b of G are said to be *G-conjugate* if there is an $x \in G$ such that $b = xax^{-1}$. The set of all elements of G conjugate to a is called the *G-conjugacy class* of a, or simply, the conjugacy class of a. We will denote this conjugacy class by G^a.

Proposition 5.5. *The conjugacy classes in a group G are the equivalence classes of an equivalence relation on G.*

Proof. The equivalence relation is simply that two elements are equivalent if and only if they lie in the same conjugacy class. □

Proposition 5.6. *Two elements of $S(n)$ have the same cycle structure if and only if*

Proof. If σ is a k-cycle, then so is $\tau\sigma\tau^{-1}$ for all $\tau \in S(n)$. It follows from this that two elements in the same conjugacy class have the same cycle structure. Conversely, if two permutations have the same cycle structure, then they are conjugate. This follows form the fact that any two k-cycles are conjugate, and the cycles are disjoint, so that the permutations involved in the conjugations can be chosen so that they commute. We will omit the details. □

For example, according to the theorem, (12)(34) and (13)(24) are similar since they both consist of two disjoint 2-cycles. Clearly (23)(12)(34)(23) = (13)(24).

5.2 The Alternating Group and the Signature

The signature of a permutation was already defined in Chapter **??** to be the mapping $sgn : S(n) \to \{\pm 1\}$ defined by the expression

$$\mathrm{sgn}(\sigma) = \prod_{i<j} \frac{\sigma(i) - \sigma(j)}{i - j}.$$

We can compute $sgn(\sigma)$ from the following Proposition.

Proposition 5.7. *For any $\sigma \in S(n)$, $sgn(\sigma) = (-1)^n(\sigma)$, where*

$$n(\sigma) = |\{(i,j) \mid 1 \le i < j \le n \ \text{ suchthat } \ \sigma(i) > \sigma(j)\}|.$$

Proof. It suffices to note that $i < j$ and $s(i) > \sigma(j)$ implies $(s(i) - \sigma(j))/(i - j) < 0$. Otherwise, $(s(i) - \sigma(j))/(i - j) > 0$. □

The fundamental result about the signature is

Theorem 5.8. *The map $sgn : S(n) \to C_2 = \{\pm 1\}$ is a homomorphism. Thus, if $\sigma, \tau \in S(n)$, then $sgn(\tau\sigma) = sgn(\tau)sgn(\sigma)$. If Moreover, if σ is a transposition, then $sgn(\sigma) = -1$. Consequently, $sgn(\sigma) = (-1)^m$, where m is the number of transpositions in any decomposition of σ into a product of transpositions. In particular, $sgn(\sigma) = (-1)^{\ell(\sigma)}$.*

Let us review the proof. In fact, now that we know the basics of group theory, we can simplify it a fair bit. Showing that sgn is a homomorphismis easy. If $\sigma, \tau \in S(n)$, we can write

$$\begin{aligned} \mathrm{sgn}(\sigma\tau) &= \prod_{i<j} \frac{\sigma\tau(i) - \sigma\tau(j)}{i - j} \\ &= \prod_{i<j} \frac{\sigma(\tau(i)) - \sigma(\tau(j))}{\tau(i) - \tau(j)} \prod_{i<j} \frac{\tau(i) - \tau(j)}{i - j} \\ &= \mathrm{sgn}(\sigma)\mathrm{sgn}(\tau), \end{aligned}$$

since τ is a bijection of $\{1, 2, \ldots, n\}$. The second step is to show that the sgn of a transposition is -1. Since $\tau(i\ j)\tau^{-1} = (\tau(i)\ \tau(j))$, we only need to show $sgn(1\ 2) = -1$. For if $\tau(1) = i$ and $\tau(2) = j$, then

$$sgn(i\ j) = sgn(\tau(1\ 2)\tau^{-1}) = sgn(\tau)sgn((1\ 2)sgn(\tau^{-1}) = sgn(1\ 2).$$

But $sgn(1\ 2) = (-1)^{n(1\ 2)}$, where $n(1\ 2)$ is the number of $i < j$ such that $(1\ 2)(i) > (1\ 2)(j)$. If $i = 1$, then only j which contributes to $n(1\ 2)$ is

$j = 2$. If $i \geq 2$, we only need to look at j's such that $j > i$, and for these, $(1\ 2)(i) < (1\ 2)(j)$. Thus, $n(1\ 2) = 1$, so $sgn(1\ 2) = -1$. Since, by the result of Exercise

It follows for example that the number of transpositions in any expression for σ is always either even or odd, depending on $\mathrm{sgn}(\sigma)$. If $\mathrm{sgn}(\sigma) = 1$, we say that σ is *even*. Likewise, we say σ *odd* if $\mathrm{sgn}(\sigma) = -1$.

Definition 5.5. The *alternating group* $A(n)$ is the normal subgroup of $S(n)$ defined as the kernel of the signature map. Thus $A(n)$ consists of all even permutations.

By the Isomorphism Theorem, $A(n)$ has index two, as the image of sgn is C_2. A famous result in classical algebra says that if $n > 4$, then $A(n)$ has no normal subgroups. We will prove this in a later chapter.

Definition 5.6. A group G with the property that its only normal subgroups are itself and the trivial subgroup $\{e\}$ is called *simple*.

For instance, a cyclic group of prime order is simple, and we just stated that $A(n)$ is simple if $n \geq 5$. In the last three or four decades, There was a major effort to classify the finite simple groups. Apparently, this program is now finished, although no one is completely certain since the papers whose union is supposed to comprise the classification take up some 10,000 pages in math journals. Hence there is still a need to simplify and unify all these results.

Exercises

Exercise 5.1. Find disjoint cycle representation of all the elements of $S(3)$.

Exercise 5.2. Find the expression for the k-cycle $(1\ 2\ \cdots\ k)$i n terms of the simple transpositions.

Exercise 5.3. Suppose that $\sigma \in S(n)$ is a k-cycle. Show that σ is even if and only if k is odd.

Exercise 5.4. Find an expression for the longest element of $S(4)$ and decompose it into disjoint cycles.

Exercise 5.5. Let $(i_1\ i_2\ \cdots\ i_k)$ denote a k-cycle in $S(n)$. Show that for any σ in $S(n)$, we have that

$$\sigma(i_1\ i_2\ \cdots\ i_k)\sigma^{-1} = (\sigma(i_1)\ \sigma(i_2)\ \cdots\ \sigma(i_k)).$$

Exercise 5.6. Use the result of Exercise 5.5 to show that any k-cycle $(i_1\ i_2\ \cdots\ i_k) \in S(n)$ is conjugate to $(1\ 2\ \ldots\ k)$. Conclude that any two k-cycles are conjugate.

Exercise 5.7. Write down all the elements of $S(3)$ and $A(4)$ in disjoint cycle notation.

Exercise 5.8. Prove Proposition 5.5.

Exercise 5.9. Write the element $(ab)(bc)(cd)(de)(af)$ of $S(6)$ as a product of disjoint cycles.

Exercise 5.10. Find the disjoint cycle decomposition for the permutation

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
F	B	V	R	S	U	E	N	Z	J	A	C	M	D	L	P	Q	S	K	O	H	T	X	I	Y	G

Exercise 5.11. Assume $\tau \in S(n)$.

(a) Show that if τ is a transposition, then for any $\sigma \in S(n)$, $\sigma\tau\sigma^{-1}$ is also a transposition.

(b) Show that if $\tau^k = (1)$ for some $k > 0$, then the same is true for $\sigma\tau\sigma^{-1}$ for all $\sigma \in S(n)$.

(c) Show that for any τ, there exists a $\sigma \in S(n)$ such that $\sigma\tau\sigma^{-1} = \tau^{-1}$.

Exercise 5.12. Compute the disjoint cycle decompositions of $(abcd)^i$ for $i = 2, 3, 4$. In general, how do the disjoint cycle decompositions of a permutation π and its square π^2 differ?

Exercise 5.13. Give a recipe for the order of an element of $S(n)$, and use it to find the largest order of an element in $S(n)$.

Exercise 5.14. What is the largest order of an element in $A(n)$.

5.3 $S(n)$ and the $n \times n$ Permutation Matrices

Recall that the set $P(n)$ of $n \times n$ permutation matrices consists of all matrices P which can be obtained by a rearrangement of the rows of I_n. The permutation matrices were introduced in the context of row operations, since for any $n \times n$ permutation matrix P and any $A \in \mathbb{F}^{n \times n}$, PA is A up to the same rearrangement of A's rows as in P.

We have already seen that $P(n)$ is a matrix group. In fact, each element of $P(n)$ has orthonormal columns, so $P(n) \subset O(n, \mathbb{R})$. But it can easily be shown that $P(n)$ is closed under multiplication, so $P(n)$ is a finite subset of a group which is closed under multiplication hence is a subgroup.

Since the symmetric group is also involved in rearrangments, it's not unexpected that $S(n)$ and $P(n)$ should have similar properties. In fact, we will now show $S(n) \cong P(n)$ by exhibiting an explicit isomorphism. This is a very useful result, since, as we will also show below, the group $P(n)$ has an important geometric interpretation. Thus This demonstrates is one way of relating combinatorics and geometry.

Proposition 5.9. *For each $\sigma \in S(n)$, let*

$$P_\sigma := (\mathbf{e}_{\sigma(1)}\ \mathbf{e}_{\sigma(2)}\ \dots\ \mathbf{e}_{\sigma(n)}).$$

Then the mapping $\varphi : S(n) \to P(n)$ defined by $\varphi(\sigma) = P_\sigma$ is an isomorphism onto $P(n)$.

Proof. A convenient way to describe the permutation matrices is to note that every column and row has exactly one nonzero entry and that entry is 1. Thus any permutation matrix P has the form P_σ, so φ is surjective. To show φ is a homomorphism it suffices to consider the case where σ is a transposition, say $\sigma = (ij)$. Then $P_\sigma = P_{(ij)}$ is simply I_n with rows i and j interchanged, which is the same thing as I_n with columns i and j interchanged. Therefore, since right multiplication by $P_{(ij)}$ interchanges the ith and jth columns and leaves all the other columns alone, $P_\tau P_\sigma$ is P_μ, where $\mu \in S(n)$ is the element such that $\mu(m) = \tau(m)$ if $m \neq i, j$, $\mu(i) = \tau(j)$ and $\mu(j) = \tau(i)$. But μ is exactly $\tau(ij)$, hence

$$P_\tau P_\sigma = P_\mu = P_{\tau(ij)} = P_{\tau\sigma}.$$

Since every element of $S(n)$ is a product of transpositions, we immediately conclude that $\varphi(\sigma\tau) = \varphi(\sigma)\varphi(\tau)$ for all $\sigma, \tau \in S(n)$. Since φ sends $S(n)$

onto $P(n)$, it is also one to one as both $S(n)$ and $P(n)$ have order $n!$ Hence φ is an isomorphism. □

Corollary 5.10. *For every $\sigma \in S(n)$, we have $\det(P_\sigma) = sgn(\sigma)$. Hence, $P(n) \cap SO(n)$ is isomorphic to the alternating group $A(n)$.*

Proof. By the classical formula for det,

$$\det(P) = \sum_{\pi \in S(n)} \text{sgn}(\pi)\ p_{\pi(1)1}\ p_{\pi(2)2}\ \cdots\ p_{\pi(n)n}.$$

Clearly, if $P = P_\sigma$, then the only non-zero term is $sgn(\sigma)$. For another proof, note that the sign of det changes sign when two rows of P are interchanged, so it follows that $\det(P_\sigma) = (-1)^{\ell(\sigma)} \det(I_n)$. But $sgn(\sigma) = (-1)^{\ell(\sigma)}$ and $\det(I_n) = 1$. □

5.3.1 The Connection With Reflections and Rotations

We will now make a remark on the isomorphism $S(n) \cong P(n)$ which reveals a fundamental connection between the symmetric group and the geometry of $\mathbb{R}^n$. As we have seen, $S(n)$ is generated by transpositions (ij), so let us consider what sort of orthogonal linear transformations the corresponding permutation matrices $P_{(ij)}$ define. Clearly $P_{(ij)}$ interchanges $\mathbf{e}_i$ and $\mathbf{e}_j$ and leaves every other $\mathbf{e}_k$ fixed. I claim that $P_{(ij)}$ is the reflection through the $(n-1)$-dimensional subspace H in $\mathbb{R}^n$ with equation $x_i - x_j = 0$, i.e. the hyperplane orthogonal to $\mathbf{e}_i - \mathbf{e}_j$. To see this, note that H is spanned by the $\mathbf{e}_k$, where $k \neq i, j$, and $\mathbf{e}_i + \mathbf{e}_j$. As $P_{(ij)}$ fixes each of these vectors, it leaves the hyperplane H pointwise fixed. It also sends the vector $\mathbf{e}_i - \mathbf{e}_j$ orthogonal to H to its negative $\mathbf{e}_j - \mathbf{e}_i$, so $P_{(ij)}$ is indeed the reflection of R^n through H. We will call $P_{(ij)}$ the *reflection matrix* corresponding to H. We conclude

Proposition 5.11. *The group of $n \times n$ permutation matrices $P(n)$ is generated by the $n \times n$ reflection matrices $P_{(ij)}$. In fact, it is generated by the reflection matrices $P_{(i\ i+1)}$ corresponding to the simple reflections.*

Proof. This follows from the above discussion and the fact that $S(n)$ is generated by the simple transpositions. □

Example 5.6. The permutation matrix

$$P = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

sends $\mathbf{e}_1$ to $\mathbf{e}_2$, $\mathbf{e}_2$ to $\mathbf{e}_1$ and $\mathbf{e}_3$ to $\mathbf{e}_3$. Thus P leaves the plane H spanned by $\mathbf{e}_1 + \mathbf{e}_2$ and $\mathbf{e}_3$ pointwise fixed and sends $\mathbf{e}_1 - \mathbf{e}_2$ to $\mathbf{e}_2 - \mathbf{e}_1$.

A finite subgroup of $O(n, \mathbb{R})$ which is generated by reflections is called a *reflection group*. The mathematics of reflection groups is extremely elegant. For a detailed but elementary treatment of reflection groups, see Refelction Groups and Coxeter Groups by James Humphreys. Reflection groups are also used in crystallography and some other areas of chemistry and physics.

Exercise 5.15. List all elements of $P(3)$ and decompose each into a product of $P_{(ij)}$'s, where (ij) is a simple transposition.

Exercises

Exercise 5.16. List all elements of $P(3)$ and decompose each into a product of $P_{(ij)}$'s, where (ij) is a simple transposition.

5.4 $S(n)$ Pairings

We're now going to give a beautiful result on $S(n)$ which even played an important role in crytography in during the Second World War and the period immediately preceding it. This result describes the structure of the product of two $S(n)$ pairings.

Definition 5.7. A *pairing* is an element of $S(n)$ which is equal to its own inverse.

Transpositions are pairings. For example, $(ab)(ab) = (1)$. (Notice that we are using the convention that (1) denotes the identity element of $S(n)$.) Elements that can be written as products of disjoint transpositions are pairings. For example, $(ab)(ce)(df)$ is a pairing in $S(6)$. Indeed,

$$((ab)(ce)(df))^2 = (ab)^2(ce)^2(df)^2 = (1).$$

Conversely, if $\pi \in S(n)$ is a pairing, then π can be written as a product of disjoint transpositions. Let's consider an example with $n = 4$. If $\pi(a) = c$ for example, then $\pi(c) = a$ since $\pi = \pi^{-1}$ and $\pi^{-1}(c) = a$. Thus (ac) is one of the disjoint cycles of π. The only possibilities for $\pi(b)$ are b or d. In the first case, $\pi = (ac)$, and, in the other, $\pi = (ac)(bd)$.

Proposition 5.12. *The pairings in $S(n)$ are exactly those elements of $S(n)$ which can be written as a product of disjoint transpositions.*

Proof. The reasoning we have just given obviously extends for all n. □

If π is self inverse, then the substitution cipher constructed from π is also deciphered by π. This is primarily why pairings are interesting. It turns out that products of pairings have a beautiful property.

Example 5.7. Let $\sigma = (ab)(cd)$ and $\tau = (ad)(bc)$. Both σ and τ pairings in $S(4)$. Let's compute $\tau\sigma$ and $\sigma\tau$.

$$\tau\sigma = (ad)(bc)(ab)(cd),$$

which is the permutation

$$a \to c, \quad b \to d, \quad c \to a, \quad d \to b.$$

Hence $\tau\sigma = (ac)(bd)$. Similarly, $\sigma\tau = (ac)(bd)$ too. In this example, the product of the two the pairings is a pairing. This isn't the case in general however. What turns out important is the structure of the cycles in the product.

The beautiful key fact about pairings was discovered by a Polish cryptographer named Marian Rejewski in the 1930's, while he was trying to unravel the mystery of the German cipher machine known as the Enigma. This theorem has been called "the theorem that won WWII" because Rejewski used it to find a crack the Enigma cipher.

Theorem 5.13. *Let σ and τ be pairings in the same $S(n)$ which fix exactly the same letters (and hence move exactly the same letters). Then the number of disjoint cycles in $\sigma\tau$ of every length is even (but possibly 0). Thus, if $\sigma\tau$ has a cycle of length $k > 0$, then it has an even number of them. Conversely, an element of $S(n)$ which has the property that in its disjoint cycle representation, there are an even number disjoint cycles of each possible length is a product of two pairings (though possibly in many ways).*

Note that the condition that σ and τ fix exactly the same letters eliminates possible problems such as what happens when $\sigma = (12)$ and $\tau = (23)$. The product $\tau\sigma = (132)$, which clearly doesn't satisfy the conclusion of the Theorem.

In Example 5.7, $\sigma\tau$ has 4 cycles of length two. Let's see why Rejewski's Theorem holds. Consider two pairings

$$\sigma = (a\ e)(b\ f)(c\ g)(h\ d) \quad \text{and} \quad \tau = (b\ e)(f\ c)(h\ g)(a\ d)$$

both of which move a, b, c, d, e, f, g and no other letters. The way to understand why there are an even number of cycles of each length in $\sigma\tau$ is to consider the following arrangement:

$$\begin{array}{ccccccccc} a & & h & & c & & b & & a \\ & d & & g & & f & & e & \end{array} .$$

Note that one sees how τ acts by reading diagonally down from left to right, while σ is obtained by reading diagonally up from left to right. Thus the disjoint cycle decomposition of $\sigma\tau$ is immediately revealed. Read the top row from left to right to get one cycle, and read the bottom row from right to left to get the other. Hence the cycles of each length occur in pairs. Clearly, this consideration can be used on the product of any two pairings that move the same letters.

5.5 Cryptology and the Symmetric Group

Cryptology is the science of designing and breaking ciphers. A cipher is a system for disguising a message so that only the sender and the person the message is intended for can read it. Thus a cipher needs to be distinguished from a code, although coding theory is certainly a part of cryptology. Cryptology has two area, cryptography and cryptanalysis. A cryptographer designs ciphers and a cryptanalyst tries to break them.

5.5.1 Substitution Ciphers and $S(n)$

The symmetric group, which we know plays a major role in combinatorics, also has many applications in cryptology. Let's begin with a simple example of this. A substitution cipher is a permutation of the alphabet, that is an element of the group $S(26)$. The following substitution cipher can be deciphered by analyzing the frequencies of the letters the message contains.

F KVZSDVS XNZVN
NSKZOFOSK OL ULWESO
ZOK ULHDRSWK ZK CLKO
FCUWSR DLWON XNZOSNSFR

Exercise 5.17. Solve the cipher.

Without giving the solution, we can make a few general comments. Let σ be the permutation which produces the cipher. To decipher the message, we have to find σ^{-1}. The frequencies in the cipher text should roughly correspond to the frequencies of letters in ordinary English. For example, there are 8 S's, it's a good guess is that S is E or I. There are six Z's, so Z is another candidate for E or I. But there are no commonly used two letter words that begin with E, and several that begin with I, so Z very likely is I. Since I has now been used and the only two one letter words are A and I, we may infer that F is A. This is a start, but there is still some work to do.

If the cipher text were altered, your job as a cryptanalyst would be to determine how. For example, F LXCWIBZ FWJGZ is an encipherment of the first line of the cipher text.[1] The new cipher text is no longer obtained by a simple substitution.

A more sophisticated cipher would be one which enciphers the first letter by a permutation σ_1, the second by another permutation σ_2, the third

[1]The second letter is shifted one to the right, the third two etc.

by σ_3 and so on. If the sequence of permutations was sufficiently random and didn't repeat often, the cipher would be virtually unbreakable. This variation of the substitution cipher has been incoporated into a number of commercial cipher machines. We will take up the most famous of these machines, which is known as the Enigma. This was the cipher machine which was used by the German military in World War II. In the original Enigmas, the sequence of permutations repeated every $(26)^3 = 17576$ letters, and later models were even more sophisticated. We will describe how the Enigma operated and how the initial breakthrough was made by some Polish math students in the early 1930's.

5.6 Breaking the Enigma

The Enigma machine is a cipher machine that was used by the German military from about 1929 until the end of the Second World War in 1945. It was adapted from a commercial cipher machine manufactured and marketed in Germany starting in 1920. The purpose of a cipher machine is, of course, to encipher a plain text message to produce a cipher text, which only someone with the same machine will be able to decipher without actually breaking the cipher. The Enigma was one of the most sophisticated cipher machine ever built. For each message, there were approximately 7.02×10^{60} possible decipherings. Because of this, it's not surprising that the Germans considered it unbreakable.

We will now describe how the Enigma worked and how three inexperienced Polish cryptanalysts had by 1932 made the initial breakthrough which eventually lead to a complete understanding of the Enigma cipher. In order to keep the presentation as simple as possible, we will ignore some of the features of the design and concentrate on the key components, which were the rotors and how they were set. A complete account can be found in "Enigma" by W. Kozacuk, which contains appendices written by Rejewski himself. Another account is given in "Intercept" by Jozef Garlinski. Both books are fascinating reading.

One of the most significant points is that the solution of the Enigma cipher was the first occasion abstract algebra was applied to the field of cryptology. Nowadays, cryptology is recognized as a sub-field of mathematics, and nations employ thousands of mathematicians as cryptographers and cryptanalysts. But before 1932, no one had ever used anything more sophisticated than elementary statistics in analyzing a cipher.

Before 1929, Polish Military Intelligence, concerned about the potential

threat posed by German rearmanent, had been deciphering a substantial amount of Germany's military transmissions. In 1929, an entirely new system of encipherment started to be used. Messages appeared to consist of random letter groups. There were no discernable patterns. It was guessed that Germany had begun to use a cipher machine to conceal its military secrets, and some sort of machine like the Enigma, which after all, was available on the open market, would have been a likely candidate. Not wanting to show their cards, the Germans had left the commercial version of Enigma on the market, and the Poles were able to obtain one. They readily surmised that the German military was using a modified version of their machine, and they set about to see what they could learn. Poland was intercepting from 60 to 80 of these enciphered messages a day and had begun to suspect that the first six letters in each message contained the instructions telling an Enigma operator how to set up his machine for the deciphering process. In fact, as we will see below, it was logical to guess that they were a double encryption of the rotor settings the operator should use.

At first the Poles made little headway, but their efforts were bolstered Poland's close ally, France, which had obtained some information from a disgruntled German communications clerk. Out of this came a confirmation that the Germans were indeed using modified Enigmas. In addition the Poles received some vital data which proved to be crucial.

Now in 1929, the cryptographer's basic tools were probability, statistics, intuition, luck and the willingness to sacrifice one's sanity by pouring over messages trying to discern the key patterns. Although the first two of these tools were of no help in attacking the Enigma cipher, Poland, in 1929, had many of the world's best mathematicians, and, to take advantage of this, the head of the Polish Cryptographical Bureau (secretly) recruited some of them to teach a course in cryptography at the University of Poznan. It turned out that three of the students excelled in the course, and they were recruited to work on the Enigma for the Polish Cryptographical Bureau.

The first clue came from a pattern common to all the first six letter groups. Suppose that the following first six letter groups came from fifteen messages all intercepted on the same day. See if you can spot the clue.

fowvat	*wrtyuo*	*qvtnmo*	*kophau*	*evprmu*
qmlnxz	*wvqymk*	*dgybhj*	*orcdla*	*mijwce*
abocrh	*coeiaw*	*ntplbu*	*zugmcf*	*lhmqzp*

In order to grasp the significance of what you may have discovered, we need to say something about how an Enigma machine worked. An Enigma

has typewriter keyboard except there are only keys for the standard alphabet, hence only 26 keys. A lampboard with 26 lights also labelled a through z is mounted behind the keyboard, and each key is wired to a light. Whenever a key is pressed, one of the lamps is illuminated. But if a letter, say a, is pressed over and over, a different lamp lights each time. For example, pressing $aaaaa$ might produce $bsfgt$. Actually, the pattern would eventually repeat but not until a was pressed $(26)^3$ times. Another feature was that if a key were pressed, its own lamp could never light. This is because pressing the letter a for example disconnected the a lamp. Another feature was that if pressing a produced b, then pressing b would have produced a.

Operating an Enigma required two people, one to type in the plain text and the other to read the cipher text as the lights on the lampboard illuminated one after another. An enciphered message was then sent by telegram.

Inside an Enigma were three internal rotors side by side and rotating on a horizontal axle. Each of the rotors had 26 terminals equally spaced around its right hand circumference and 26 around its left hand circumference. The terminals around each circumference represented the alphabet in the usual $abc\ldots$ order. The key was that each terminal on the right circumference of a rotor was wired internally to a terminal on the left. Thus when a current passes through a rotor from a right hand terminal to one on the left, the corresponding letter on the right is permuted, so each rotor acted as an element of $S(26)$. On the left of the third rotor was a reflector having 26 terminals around its circumference, each in contact with the 26 terminals on the left side of the third rotor. The reflector acted by an element of $S(26)$, except that the permutation given by the reflector was, by construction, a pairing (why?). Moreover the reflector had to move every letter, since if an unpaired letter were pressed, no lamp would be illuminated.

Briefly then, the terminals on adjacent rotors were in contact (left side of the right rotor to right side of the middle rotor etc.) and in contact with the reflector. So when the operator pressed a key, say a, a current passed through the three internal rotors from right to left, through the reflector then back through the rotors in the opposite order causing a lamp different from a, perhaps w, to light up.

For example, suppose the permutations for the three rotors from right to left are labeled σ_R, σ_M, σ_L and ρ is the pairing of the reflector. Suppose the a key is struck. Then this action is represented by

$$\sigma_R^{-1}\sigma_M^{-1}\sigma_L^{-1}\rho\sigma_L\sigma_M\sigma_R(a) = w$$

Now ρ is a pairing and

$$\sigma_R^{-1}\sigma_M^{-1}\sigma_L^{-1}\rho\sigma_L\sigma_M\sigma_R = (\sigma_L\sigma_M\sigma_R)^{-1}\rho\sigma_L\sigma_M\sigma_R.$$

Thus the enciphering of $a \to w$ is produced by a pairing, since any element conjugate to a pairing is a pairing. This shows why pressing w instead of a would give a. It is because, by definition, a pairing is its own inverse. This key feature of the Enigma made enciphering and deciphering the same operation.

What complicated the encipherment is the fact that each rotor could be independently rotated through all 26 positions, so every rotor could in fact produce 26 distinct elements of $S(26)$. Every time a key on the keyboard was pressed, the first rotor moved forward one terminal. This shift corresponds to the cyclic permutation $\pi = (abc\ldots xyz)$. Hence the second letter would be enciphered by a new pairing, namely

$$\pi^{-1}\sigma_R^{-1}\pi\sigma_M^{-1}\sigma_L^{-1}\rho\sigma_L\sigma_M\pi^{-1}\sigma_R\pi.$$

Notice that we have used $\pi^{-1}\sigma_R\pi$ here since the middle and left rotors would have been kept stationary. Without the factor π^{-1}, all three rotors would advance 1/26 revolution together. As soon as the first 26 letters had been enciphered and the right hand rotor had made a complete revolution, the middle rotor advanced 1/26th of a revolution. The 27th letter was thus enciphered by

$$\sigma_R^{-1}\pi^{-1}\sigma_M^{-1}\pi\sigma_L^{-1}\rho\sigma_L\pi^{-1}\sigma_M\pi\sigma_R$$

since $\pi^{26} = (1)$. As soon as $26^2 = 626$ letters were enciphered, the left hand rotor moved forward 1/26th of a revolution and so on. The rotors thus kept cycling through different pairings until $26^3 = 17576$ keys were pressed, after which the cycle repeated.

As we noted above, for two Enigmas with the same initial rotor settings, enciphering and deciphering were the same operation. The operator who received a message had only to type in the ciphertext and the assistant read off the plaintext as the lamps lit up. To ensure that the starting positions were always the same, a *daily key* schedule was issued. On a given day, all machines would be set at the daily key. If on September 5, 1930, the daily key was xsf, then on that day all Enigmas would begin sending and deciphering with the right rotor set at f, the middle at s and the left at x. To increase security, each operator also selected another three letter key, a so called *telegram key*, e.g. arf. Then, before enciphering took place, the operator, with the Enigma set to the daily key xsf, enciphered the telegram

key arf. As an error detecting device, the operator actually typed $arfarf$, producing the six letter string (such as $wyuigh$) which opened the message. This six letter string was then sent (by morse code) as the first six letters of the enciphered message. After sending this doubly enciphered telegram key, the operator set his rotors to arf and proceeded to encipher the plaintext. The operator on the receiving end, with his Enigma set to the daily key xsf, typed in $wyuigh$. The deciphered string $arfarf$ told him to reset his rotors to arf before typing in the ciphertext. Of course, if something like $antark$ was received, this signalled a transmission error and the message couldn't be deciphered until the doubly enciphered telegram key was resent.

The double encipherment of the telegram key was considered necessary. Radio transmissions were often hard to pick up, and moreover, there was always the possibility of human error under the difficulties experienced under battle conditions. This, however, turned out to be the weak link. The reason was a particular feature of the method for enciphering the telegram key. Look at the first six letter groups from the fifteen messages all intercepted on the same day again.

$fowvat$	$wrtyuo$	$qvtmno$	$kophau$	$evprmu$
$qmlnxz$	$wvqymk$	$dgybhj$	$orcdla$	$mijwce$
$abocrh$	$coeiaw$	$ntplbu$	$zugmcf$	$lhmqzp$

The interesting feature of all the above six letter groups is that whenever two messages have the same first letter, they have the same fourth letter and conversely. This also holds for the second and fifth letters and the third and sixth letters. A trained cryptographer would have noticed this feature right away, but an untrained eye (such as the author's) might not see it for quite awhile. This pattern clearly supported the double encryption hypothesis. But what could be sometimes deduced from it was the telegram key itself.

The significance was realized by one of the three cryptographers, Marian Rejewski, who was mentioned in the previous section. His idea was to string together all the first and fourth letters of first six letters for all the intercepted messages from a particular day. Doing this for the above fifteen intercepts gives

$$aci \ldots zmwy \ldots qnlq \ldots odb \ldots fv \ldots er \ldots kh \ldots$$

Working from the 60-80 daily intercepts, Rejewski was sometimes able to string together the whole alphabet each time getting an element of $\pi \in S(26)$. This permutation π could then be factored into disjoint cycles. For example, in the above example, (qnl) is a cycle. What Rejewski noticed was

that the permutations he obtained had the property we considered in the last section. The cycles of length k occured in pairs. That is, the number of cycles of each length in π was a multiple of two. Rejewski (realizing the result stated in Theorem 5.6) could then seek to decompose this element of $S(26)$ into two pairings.

He did the same for the second and fifth and the third and sixth letters. If successful in all three cases, he would ultimately obtain six pairings, all of which contained some information, however little, about the wiring of the rotors. But as we will see below, this job could be extremely difficult.

Why does π have to be the product of two pairings? Recall that on a given day, all Enigmas were set to the same daily key, say xsf. If an operator chose arf as the telegram key, then after setting his Enigma to xsf, he typed $arfarf$. This would produce a six letter group such as $wyuigh$. Then $\pi(w) = i$. Now let σ_1 be first pairing, so that $\sigma_1(a) = w$. The second pairing gives $\sigma_2(a) = i$. Then clearly,

$$\sigma_2\sigma_1(w) = \sigma_2\sigma_1^2(a) = \sigma_2(a) = i.$$

Thus $\pi = \sigma_2\sigma_1$, which explains why there were an even number of disjoint cycles of each length in π, and also gives an explicit factorization of π into pairings.

Of course, if we know either σ_1 or σ_2, then we know that the first letter of the telegram key is $\sigma_1(w) = \sigma_2(i) = a$. If the other pairings are also known, it follows that the complete telegram key for this transmission is known. Knowing the telegram keys for an enciphered message would be extremely useful if the daily key were also known. This is where the contribution of the French spy came in. It turned out that French intelligence had turned an apparently disgruntled German code clerk who sold them the daily keys covering a period of two months. These were turned over to the Poles which turned out to be a tremendous windfall. The only problem, which will be illustrated below, is that although the factorization into pairings exists, it isn't necessarily unique.

However, with this as a starting point, using several other very clever and imaginative devices, the three crytographers were able to decipher their first Enigma message by the end of 1932, and, by 1934, they had completely solved the puzzle of the wiring of the rotors and were able to build an exact replica of the Enigma (an Enigma double). This story should serve as as an inspiration to every budding young mathematician!!

Let's now take a simple example of how the pairings are found.

Example 5.8. Suppose the alphabet has been shortened to $abcdef$ and

consider $(ahc)(dgb)$. We want to write this as $\sigma\tau$, where σ and τ are pairings. We can clearly see that $e \to e$ and $f \to f$. Imitating the procedure illustrated after Rejewski's Theorem, consider the three possibilities taking the cyclic permutations of b, d, g into account:

$$\begin{array}{cccccccc} a & & h & & c & & a \\ & b & & g & & d & \end{array}$$

$$\begin{array}{cccccccc} a & & h & & c & & a \\ & g & & d & & b & \end{array}$$

and

$$\begin{array}{cccccccc} a & & h & & c & & a \\ & d & & b & & g & \end{array}$$

Thus there are three possible solutions:

$$\sigma = (ab)(hg)(cd)(ef), \quad \tau = (ad)(cg)(bh)(ef),$$
$$\sigma = (ag)(dh)(bc)(ef), \quad \tau = (ab)(cd)(gh)(ef),$$
$$\sigma = (ad)(bh)(cg)(ef), \quad \tau = (ag)(cd)(dh)(ef).$$

Notice that we included (ef) in each pairing in order to involve all the letters, but it disappears in the product since $(ef)^2 =$. It's not hard to see that these are the only solutions.

Example 5.9. Consider the permutation

$$\pi = (depzvlyq)(aronjfmx)(bgktu)(wscih).$$

Thus we consider pairs of arrays such as

$$\begin{array}{ccccccccccccccccc} d & & e & & p & & z & & v & & l & & y & & q & & d \\ & x & & m & & f & & j & & n & & o & & r & & a & \end{array}$$

and

$$\begin{array}{ccccccccccc} & & b & & g & & k & & t & & u & & b & & \\ & h & & i & & c & & s & & w & & & & \end{array}$$

One possible solution is therefore

$$\sigma = (dx)(em)(fp)(jz)(nv)(lo)(ry)(aq)(bh)(gi)(kc)(st)(uw),$$

and

$$\tau = (ad)(qr)(oy)(ln)(jv)(fz)(mp)(ex)(bw)(us)(tc)(ki)(gh).$$

Since we obtain all solutions by cyclicly permuting the second rows of the two arrays, there are 128 solutions in all.

To continue our discussion, if the hypothesis that the first 6 letters are the key repeated is correct, then we must have $\sigma(d) = \tau(e)$. But this is the case, since $\sigma(d) = x$ and $\tau(e) = x$. This suggests the possibility that the first letter in the key is x. Now it is a fact of human nature, extensively exploited by the Poles, that the German operators would tend to choose familiar keys; so we would be led to suspect that the key is xyz. This would lead us to seek solutions σ, τ for (2) so that $\sigma(h) = \tau(c) = y$ and solutions σ, τ for (3) so that $\sigma(z) = \tau(n) = z$. But this last fact kills our hypothesis, since, in (3), $\sigma(z) \neq z$. Thus, we have to discard xyz as a possible key and test some other possibility, say xxx.

As mentioned above, by 1934, the three cryptographers had succeeded in reconstructing the rotors and all other aspects of the machine and the Polish government had secretly manufactured their own duplicates. This was all quite amazing since Poland was economically depressed, and the financial outlay for this project was a serious strain on the national treasury. Yet because of the ingenuity of the cryptographers, the Poles were light years ahead of the British and French, who despite their great economic advantage, had been completely shut out in their own attempts to unravel the Enigma's mystery (which illustrates once more that money is not always the answer).

Rejewski had even constructed a primitive computer, which he called a Bomb, to test for the daily keys. Fortunately, a couple of months before the Germans' surprise invasion of Poland in September, 1939, two of the duplicate Enigmas were handed over to the French, who gave one to the British. With this windfall, the British cryptographers at Bletchley Park were immediately able to encipher a certain amount of the intercepted radio traffic, somewhere on the order of 150 intercepts per day. But after the war started, the Germans upgraded their security far more often, so the cryptographers would frequently be stymied until they figured out what modifications the Germans had made. In 1943, the British, under the leadership of Turing, built the first true electronic computer to test for the daily keys. They also called it the Bomb, apparently in deference to the Rejewski's original. However, the British do not seem to have been willing to admit that they had not made the original Enigma breakthrough. With the Bomb, the Bletchley Park cryptanalysts were eventually able to read virtually all of the top secret communications of the German High Command, apparently often before the generals for whom the communiques were intended.

An amusing sidelight is that when the British and French needed to communicate about matters concerning Enigma, they used their own Enigma doubles to ensure complete security. Apparently, the Germans never guessed that this radio traffic came from duplicates of their own Enigmas. If they

had, it would have tipped them off that the Enigma was no longer secure, which would have been a disaster.

Summary The purpose of this chapter was to give an introduction to the theory of the symmetric group. In particular, we say that it is generated by transpositions and that two elements of $S(n)$ are conjugate if and only if they have the same cycle structure. We also proved that $S(n)$ is isomorphic to the group of $n \times n$ permutation matrices. The signature of a permutation, which was introduced in Chapter **??** is a homomorphism of $S(n)$ to $C_2 = \{\pm 1\}$ whose kernel $A(n)$ is the set of all even permutations, which is known as the alternating group. The alternating group is the first example of a non-cyclic group which is simple. That is, the only normal subgroups of $A(n)$ are itself and the trivial subgroup.

We next presented a not well know but nevertheless beautiful result of Rejewski on pairings. It turns out that this result played a crucial role in breaking the Enigma cipher used by Germany in WW2. In the last section of this chapter, we gave a description of the Enigma and how pairings were crucial in its decryption.