7. Do Problem 6 for a shuffle requiring 20 repeats.
8. Express the permutations in Problem 3 as the product of transpositions.
9. Given the two transpositions $(1\ \ 2)$ and $(1\ \ 3)$, find a permutation σ such that $\sigma(1\ \ 2)\sigma^{-1} = (1\ \ 3)$.
10. Prove that there is no permutation σ such that $\sigma(1\ \ 2)\sigma^{-1} = (1\ \ 2\ \ 3)$.
11. Prove that there is a permutation σ such that $\sigma(1\ \ 2\ \ 3)\sigma^{-1} = (4\ \ 5\ \ 6)$.
12. Prove that there is no permutation σ such that $\sigma(1\ \ 2\ \ 3)\sigma^{-1} = (1\ \ 2\ \ 4)(5\ \ 6\ \ 7)$.

Middle-Level Problems

3. Prove that $(1\ \ 2)$ cannot be written as the product of disjoint 3-cycles.
4. Prove that for any permutation σ, $\sigma\tau\sigma^{-1}$ is a transposition if τ is a transposition.
5. Show that if τ is a k-cycle, then $\sigma\tau\sigma^{-1}$ is also a k-cycle, for any permutation σ.
6. Let Φ be an automorphism of S_3. Show that there is an element $\sigma \in S_3$ such that $\Phi(\tau) = \sigma^{-1}\tau\sigma$ for every $\tau \in S_3$.
7. Let $(1\ \ 2)$ and $(1\ \ 2\ \ 3\ \ \cdots\ \ n)$ be in S_n. Show that any subgroup of S_n that contains both of these must be all of S_n (so these two permutations generate S_n).
8. If τ_1 and τ_2 are two transpositions, show that $\tau_1\tau_2$ can be expressed as the product of 3-cycles (not necessarily disjoint).
9. Prove that if τ_1, τ_2, and τ_3 are transpositions, then $\tau_1\tau_2\tau_3 \neq e$, the identity element of S_n.
0. If τ_1, τ_2 are distinct transpositions, show that $\tau_1\tau_2$ is of order 2 or 3.
1. If σ, τ are two permutations that disturb no common element and $\sigma\tau = e$, prove that $\sigma = \tau = e$.
2. Find an algorithm for finding $\sigma\tau\sigma^{-1}$ for any permutations σ, τ of S_n.
3. Let σ, τ be two permutations such that they both have decompositions into disjoint cycles of cycles of lengths $m_1, m_2, \ldots, m_k$. (We say that they have similar decompositions into disjoint cycles.) Prove that for some permutation ρ, $\tau = \rho\sigma\rho^{-1}$.
4. Find the conjugacy class in S_n of $(1\ \ 2\ \ \cdots\ \ n)$. What is the order of the centralizer of $(1\ \ 2\ \ \cdots\ \ n)$ in S_n?
5. Do Problem 24 for $\sigma = (1\ \ 2)(3\ \ 4)$.

3. ODD AND EVEN PERMUTATIONS

We noticed in Section 2 that although every permutation is the product of transpositions, this decomposition is not unique. We did comment, however, that certain aspects of this kind of decomposition are unique. We go into this now.

Let's consider the special case of S_3, for here we can see everything explicitly. Let $f(x_1, x_2, x_3) = (x_1 - x_2)(x_1 - x_3)(x_2 - x_3)$ be an expression in the three variables x_1, x_2, x_3. We let S_3 act on $f(x) = f(x_1, x_2, x_3)$ as follows. If $\sigma \in S_3$, then

$$\sigma^*(f(x)) = (x_{\sigma(1)} - x_{\sigma(2)})(x_{\sigma(1)} - x_{\sigma(3)})(x_{\sigma(2)} - x_{\sigma(3)}).$$

We consider what σ^* does to $f(x)$ for a few of the σ's in S_3.

Consider $\sigma = (1\ \ 2)$. Then $\sigma(1) = 2$, $\sigma(2) = 1$, and $\sigma(3) = 3$, so that

$$\begin{aligned}\sigma^*(f(x)) &= (x_{\sigma(1)} - x_{\sigma(2)})(x_{\sigma(1)} - x_{\sigma(3)})(x_{\sigma(2)} - x_{\sigma(3)})\\ &= (x_2 - x_1)(x_2 - x_3)(x_1 - x_3)\\ &= -(x_1 - x_2)(x_1 - x_3)(x_2 - x_3)\\ &= -f(x).\end{aligned}$$

So σ^* coming from $\sigma = (1\ \ 2)$ changes the sign of $f(x)$. Let's look at the action of another element, $\tau = (1\ \ 2\ \ 3)$, of S_3 on $f(x)$. Then

$$\begin{aligned}\tau^*(f(x)) &= (x_{\tau(1)} - x_{\tau(2)})(x_{\tau(1)} - x_{\tau(3)})(x_{\tau(2)} - x_{\tau(3)})\\ &= (x_2 - x_3)(x_2 - x_1)(x_3 - x_1)\\ &= (x_1 - x_2)(x_1 - x_3)(x_2 - x_3)\\ &= f(x),\end{aligned}$$

so τ^* coming from $\tau = (1\ \ 2\ \ 3)$ leaves $f(x)$ unchanged. What about the other permutations in S_3; how do they affect $f(x)$? Of course, the identity element e induces a map e^* on $f(x)$ which does not change $f(x)$ at all. What does τ^2, for τ above, do to $f(x)$? Since $\tau^* f(x) = f(x)$, we immediately see that

$$\begin{aligned}(\tau^2)^*(f(x)) &= (x_{\tau^2(1)} - x_{\tau^2(2)})(x_{\tau^2(1)} - x_{\tau^2(3)})(x_{\tau^2(2)} - x_{\tau^2(3)})\\ &= f(x). \quad \text{(Prove!)}\end{aligned}$$

Now consider $\sigma\tau = (1\ \ 2)(1\ \ 2\ \ 3) = (2\ \ 3)$; since τ leaves $f(x)$ alone and σ changes the sign of $f(x)$, $\sigma\tau$ must change the sign of $f(x)$. Similarly, $(1\ \ 3)$ changes the sign of $f(x)$. We have accounted for the action of every element of S_3 on $f(x)$.

Suppose that $\rho \in S_3$ is a product $\rho = \tau_1\tau_2\cdots\tau_k$ of transpositions $\tau_1, \ldots, \tau_k$; then ρ acting on $f(x)$ will change the sign of $f(x)$ k times, since each τ_i changes the sign of $f(x)$. So $\rho^*(f(x)) = (-1)^k f(x)$. If $\rho = \sigma_1\sigma_2\cdots\sigma_t$, where $\sigma_1, \ldots, \sigma_t$ are transpositions, by the same reasoning, $\rho^*(f(x)) = (-1)^t f(x)$. Therefore, $(-1)^k f(x) = (-1)^t f(x)$, whence $(-1)^t = (-1)^k$. This tells us that t and k have the *same parity*; that is, if t is odd, then k must be odd, and if t is even, then k must be even.

This suggests that although the decomposition of a given permutation σ as a product of transposition is not unique, *the parity of the number of transpositions in such a decomposition of σ might be unique.*

We strive for this goal now, suggesting to readers that they carry out the argument that we do for arbitrary n for the special case $n = 4$.

As we did above, define $f(x) = f(x_1, \ldots, x_n)$ to be

$$f(x) = (x_1 - x_2)\cdots(x_1 - x_n)(x_2 - x_3)\cdots(x_2 - x_n)\cdots(x_{n-1} - x_n)$$

$$= \prod_{i<j}(x_i - x_j),$$

where in this product i takes on all values from 1 to $n - 1$ inclusive, and j all those from 2 to n inclusive. If $\sigma \in S_n$, define σ^* on $f(x)$ by

$$\sigma^*(f(x)) = \prod_{i<j}(x_{\sigma(i)} - x_{\sigma(j)}).$$

If $\sigma, \tau \in S_n$, then

$$(\sigma\tau)^*(f(x)) = \prod_{i<j}(x_{(\sigma\tau)(i)} - x_{(\sigma\tau)(j)}) = \sigma^*\left(\prod_{i<j}(x_{\tau(i)} - x_{\tau(j)})\right)$$

$$= \sigma^*\left(\tau^*\left(\prod_{i<j}(x_i - x_j)\right)\right) = \sigma^*(\tau^*(f(x))) = (\sigma^*\tau^*)(f(x))$$

So $(\sigma\tau)^* = \sigma^*\tau^*$ when applied to $f(x)$.

What does a transposition τ do to $f(x)$? We claim that $\tau^*(f(x)) = -f(x)$. To prove this, assuming that $\tau = (i\ \ j)$ where $i < j$, we count up the number of $(x_u - x_v)$, with $u < v$, which get transformed into an $(x_a - x_b)$ with $a > b$. This happens for $(x_u - x_j)$ if $i < u < j$, for $(x_i - x_v)$ if $i < v < j$, and finally, for $(x_i - x_j)$. Each of these leads to a change of sign on $f(x)$ and since there are $2(j - i - 1) + 1$ such, that is, an odd number of them, we get an odd number of changes of sign on $f(x)$ when acted on by τ^*. Thus $\tau^*(f(x)) = -f(x)$. Therefore, our claim that $\tau^*(f(x)) = -f(x)$ for every transposition τ is substantiated.

If σ is any permutation in S_n and $\sigma = \tau_1\tau_2\cdots\tau_k$, where $\tau_1, \tau_2, \ldots$ are transpositions, then $\sigma^* = (\tau_1\tau_2\cdots\tau_k)^* = \tau_1^*\tau_2^*\cdots\tau_k^*$ as acting on and since each $\tau_i^*(f(x)) = -f(x)$, we see that $\sigma^*(f(x)) = (-1)^k f(x)$. larly, if $\sigma = \zeta_1\zeta_2\cdots\zeta_t$, where $\zeta_1, \zeta_2, \ldots, \zeta_t$ are transpositions, $\sigma^*(f(x)) = (-1)^t f(x)$. Comparing these two evaluations of $\sigma^*(f(x)$ conclude that $(-1)^k = (-1)^t$. So these two decompositions of σ as the uct of transpositions are of the same parity. *Thus any permutation is the product of an odd number of transpositions or the product of an number of transpositions, and no product of an even number of transpos can equal a product of an odd number of transpositions.*

This suggests the following

Definition. The permutation $\sigma \in S_n$ is an *odd permutation* if σ product of an odd number of transpositions, and is an *even permutatio* is the product of an even number of transpositions.

What we have proved above is

Theorem 3.3.1. A permutation in S_n is either an odd or an even mutation, *but cannot be both.*

With Theorem 3.3.1 behind us we can deduce a number of its c quences.

Let A_n be the set of all even permutations; if $\sigma, \tau \in A_n$, then we ir diately have that $\sigma\tau \in A_n$. Since A_n is thus a finite closed subset of th nite) group S_n, A_n is a subgroup of S_n, by Lemma 2.3.2. A_n is called the *nating group of degree n.*

We can show that A_n is a subgroup of S_n in another way. We alr saw that A_n is closed under the product of S_n, so to know that A_n is a group of S_n we merely need show that $\sigma \in S_n$ implies that $\sigma^{-1} \in S_n$. Fo permutation σ we claim that σ and σ^{-1} are of the same parity. Why? W $\sigma = \tau_1\tau_2\cdots\tau_k$, where the τ_i are transpositions, then

$$\sigma^{-1} = (\tau_1\tau_2\cdots\tau_k)^{-1} = \tau_k^{-1}\tau_{k-1}^{-1}\cdots\tau_2^{-1}\tau_1^{-1} = \tau_k\tau_{k-1}\cdots\tau_2\tau_1,$$

since $\tau_i^{-1} = \tau_i$. Therefore, we see that the parity of σ and σ^{-1} is (-1) they are of equal parity. This certainly shows that $\sigma \in A_n$ forces $\sigma^{-1} \in$ whence A_n is a subgroup of S_n.

But it shows a little more, namely that A_n is a *normal subgroup* o For suppose that $\sigma \in A_n$ and $\rho \in S_n$. What is the parity of $\rho^{-1}\sigma\rho$? By above, ρ and ρ^{-1} are of the same parity and σ is an even permutation so $\rho^{-1}\sigma\rho$ is an even permutation, hence is in A_n. Thus A_n is a normal subgroup of S_n.

We summarize what we have done in

Theorem 3.3.2. A_n, the alternating group of degree n, is a normal subgroup of S_n.

We look at this in yet another way. From the very definitions involved we have the following simple rules for the product of permutations:

1. The product of two even permutations is even.
2. The product of two odd permutations is even.
3. The product of an even permutation by an odd one (or of an odd one by an even one) is odd.

If σ is an even permutation, let $\theta(\sigma) = 1$, and if σ is an odd permutation, let $\theta(\sigma) = -1$. The foregoing rules about products translate into $\theta(\sigma\tau) = \theta(\sigma)\theta(\tau)$, so θ is a *homomorphism* of S_n onto the group $E = \{1, -1\}$ of order 2 under multiplication. What is the kernel, N, of θ? By the very definition of A_n we see that $N = A_n$. So by the First Homomorphism Theorem, $E \simeq S_n/A_n$. Thus $2 = |E| = |S_n/A_n| = |S_n|/|A_n|$, if $n > 1$. This gives us that $|A_n| = \frac{1}{2}|S_n| = \frac{1}{2}n!$.

Therefore,

Theorem 3.3.3. For $n > 1$, A_n is a normal subgroup of S_n of order $\frac{1}{2}n!$.

Corollary. For $n > 1$, S_n contains $\frac{1}{2}n!$ even permutations and $\frac{1}{2}n!$ odd permutations.

A final few words about the proof of Theorem 3.3.1 before we close this section. Many different proofs of Theorem 3.3.1 are known. Quite frankly, we do not particularly like any of them. Some involve what might be called a "collection process," where one tries to show that e cannot be written as the product of an odd number of transpositions by assuming that it is such a shortest product, and by the appropriate finagling with this product, shortening it to get a contradiction. Other proofs use other devices. The proof we gave exploits the gimmick of the function $f(x)$, which, in some sense, is extraneous to the whole affair. However, the proof given is probably the most transparent of them all, which is why we used it.

Finally, the group A_n, for $n \geq 5$, is an extremely interesting group. We

shall show in Chapter 6 that the only normal subgroups of A_n, for n (e) and A_n itself. A group with this property is called a *simple* grou[
be confused with an *easy* group). The abelian finite simple groups ar the groups of prime order. The A_n for $n \geq 5$ provide us with an infi ily of *nonabelian* finite simple groups. There are other infinite familie simple groups. In the last 20 years or so the heroic efforts of algebra determined all finite simple groups. The determination of these simpl runs about 10,000 printed pages. Interestingly enough, any nonabeli simple group must have *even* order.

PROBLEMS

Easier Problems

1. Find the parity of each permutation.
   (a) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 4 & 5 & 1 & 3 & 7 & 8 & 9 & 6 \end{pmatrix}$.
   (b) $(1\ 2\ 3\ 4\ 5\ 6)(7\ 8\ 9)$.
   (c) $(1\ 2\ 3\ 4\ 5\ 6)(1\ 2\ 3\ 4\ 5\ 7)$.
   (d) $(1\ 2)(1\ 2\ 3)(4\ 5)(5\ 6\ 8)(1\ 7\ 9)$.
2. If σ is a k-cycle, show that σ is an odd permutation if k is even, a even permutation if k is odd.
3. Prove that σ and $\tau^{-1}\sigma\tau$, for any $\sigma, \tau \in S_n$, are of the same parity.
4. If $m < n$, we can consider $S_m \subset S_n$ by viewing $\sigma \in S_n$ as ac $1, 2, \ldots, m, \ldots, n$ as it did on $1, 2, \ldots, m$ and σ leaves $j > n$ Prove that the parity of a permutation in S_m, when viewed this wa element of S_n, does not change.
5. Suppose you are told that the permutation
$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 1 & 2 & & & 7 & 8 & 9 & 6 \end{pmatrix}$$
   in S_9, where the images of 5 and 4 have been lost, is an even pe tion. What must the images of 5 and 4 be?

Middle-Level Problems

6. If $n \geq 3$, show that every element in A_n is a product of 3-cycles.
7. Show that every element in A_n is a product of n-cycles.
8. Find a normal subgroup in A_4 of order 4.