MTHSC 412 Section 4.1 – Finite Permutation Groups

Kevin James

Note

Suppose that $A = \{a_1, a_2, \ldots, a_n\}$ is a finite set. Any permutation $f \in \mathcal{S}(A)$ can be identified with the permutation f' on $B = \{1, 2, \ldots, n\}$ defined by $f'(i) = j$ where $f(a_i) = a_j$. In fact, this identification gives an isomorphism of the groups $\mathcal{S}(A)$ and S_n.

Note

Suppose that $A = \{a_1, a_2, \ldots, a_n\}$ is a finite set. Any permutation $f \in \mathcal{S}(A)$ can be identified with the permutation f' on $B = \{1, 2, \ldots, n\}$ defined by $f'(i) = j$ where $f(a_i) = a_j$. In fact, this identification gives an isomorphism of the groups $\mathcal{S}(A)$ and S_n.

Definition

Given a permutation $\sigma \in S_n$ and $1 \leq a \leq n$, we call the set $\{\sigma^k(a) \quad | \quad k \geq 0\}$ an *orbit* of σ.

Note

Suppose that $A = \{a_1, a_2, \ldots, a_n\}$ is a finite set. Any permutation $f \in \mathcal{S}(A)$ can be identified with the permutation f' on $B = \{1, 2, \ldots, n\}$ defined by $f'(i) = j$ where $f(a_i) = a_j$. In fact, this identification gives an isomorphism of the groups $\mathcal{S}(A)$ and S_n.

Definition

Given a permutation $\sigma \in S_n$ and $1 \leq a \leq n$, we call the set $\{\sigma^k(a) \quad | \quad k \geq 0\}$ an *orbit* of σ.

Fact

Any permutation $\sigma \in S_n$ can be written as a disjoint product of cycles. The cycles in this decomposition correspond to the orbits of σ.

Miscellaneous Properties of Permutations

Fact

1. *If $f, g \in S_n$ are disjoint cycles, then $fg = gf$.*
2. *The inverse of $(a_1, a_2, \ldots, a_{n-1}, a_n)$ is* $(a_n, a_{n-1}, \ldots, a_2, a_1) = (a_1, a_n, a_{n-1}, \ldots, a_3, a_2)$.
3. *The order of an r-cycle $(a_1, \ldots, a_r)$ is r.*
4. $(a_1, \ldots, a_r)^{-1} = (a_1, \ldots, a_r)^{r-1}$.
5. *If $f = \sigma_1\sigma_2\ldots\sigma_k \in S_n$ where the σ_i are disjoint cycles of length r_i, then the order of f is the lowest common multiple of the r_i.*

Definition

A 2-cycle is called a *transposition*.

Definition

A 2-cycle is called a *transposition*.

Fact

Any permutation $\sigma \in S_n$ *can be written as a product of transpositons.*

Definition

A 2-cycle is called a *transposition*.

Fact

Any permutation $\sigma \in S_n$ can be written as a product of transpositons.

Proof.

Since any permutation can be written as a product of cycles, it suffices to show that any cycle can be written as a product of transpositions, and

Definition

A 2-cycle is called a *transposition*.

Fact

Any permutation $\sigma \in S_n$ can be written as a product of transpositons.

Proof.

Since any permutation can be written as a product of cycles, it suffices to show that any cycle can be written as a product of transpositions, and
$(a_1, a_2, \ldots, a_k) = (a_1, a_k)(a_1, a_{k-1}) \ldots (a_1, a_3)(a_1, a_2)$. $\square$

Example

Note that

$$(1,2)(2,3)(3,4) = (1,2)(5,6)(2,3)(3,4)(5,6)$$

So the number of transpositions in a decomposition of a permutation into transpositions is not unique.

Example

Note that

$$(1,2)(2,3)(3,4) = (1,2)(5,6)(2,3)(3,4)(5,6)$$

So the number of transpositions in a decomposition of a permutation into transpositions is not unique.

Theorem

Suppose that $f \in S_n$. If f can be decomposed into p transpositions and into q transpositions, then $p \equiv q \pmod 2$.

Example

Note that

$$(1,2)(2,3)(3,4) = (1,2)(5,6)(2,3)(3,4)(5,6)$$

So the number of transpositions in a decomposition of a permutation into transpositions is not unique.

Theorem

Suppose that $f \in S_n$. If f can be decomposed into p transpositions and into q transpositions, then $p \equiv q \pmod 2$.

We will develop the proof of this theorem over the next few slides...

Definition

Consider the polynomial in the variables $x_1, x_2, \ldots, x_n$ defined by $P = \prod_{1 \leq i < j \leq n} (x_i - x_j)$.

Definition

Consider the polynomial in the variables $x_1, x_2, \ldots, x_n$ defined by $P = \prod_{1 \le i < j \le n}(x_i - x_j)$.

Definition

We define an action of S_n on any constant multiple cP of the polynomial P as follows.

$$\sigma(cP) = c\sigma(P) = c \prod_{1 \le i < j \le n} (x_{\sigma(i)} - x_{\sigma(j)}).$$

Example

Take $n = 3$.

Example

Take $n = 3$.
Then $P = (x_1 - x_2)(x_1 - x_3)(x_2 - x_3)$

Example

Take $n = 3$.
Then $P = (x_1 - x_2)(x_1 - x_3)(x_2 - x_3)$
Consider $\sigma = (1, 2)$ applied to P.

Example

Take $n = 3$.
Then $P = (x_1 - x_2)(x_1 - x_3)(x_2 - x_3)$
Consider $\sigma = (1, 2)$ applied to P.
$\sigma(P) = (x_2 - x_1)(x_2 - x_3)(x_1 - x_3) =$

Example

Take $n = 3$.
Then $P = (x_1 - x_2)(x_1 - x_3)(x_2 - x_3)$
Consider $\sigma = (1, 2)$ applied to P.
$\sigma(P) = (x_2 - x_1)(x_2 - x_3)(x_1 - x_3) = -P$.

Example

Take $n = 3$.
Then $P = (x_1 - x_2)(x_1 - x_3)(x_2 - x_3)$
Consider $\sigma = (1, 2)$ applied to P.
$\sigma(P) = (x_2 - x_1)(x_2 - x_3)(x_1 - x_3) = -P$.

Lemma

If $f \in S_n$, then $f(P) = (\pm 1)P$.

Example

Take $n = 3$.
Then $P = (x_1 - x_2)(x_1 - x_3)(x_2 - x_3)$
Consider $\sigma = (1, 2)$ applied to P.
$\sigma(P) = (x_2 - x_1)(x_2 - x_3)(x_1 - x_3) = \, - P$.

Lemma

If $f \in S_n$, then $f(P) = (\pm 1)P$.

Lemma

If $\tau = (r, s) \in S_n$ is any transposition, then $\tau(P) = -P$.

Example

Take $n = 3$.
Then $P = (x_1 - x_2)(x_1 - x_3)(x_2 - x_3)$
Consider $\sigma = (1, 2)$ applied to P.
$\sigma(P) = (x_2 - x_1)(x_2 - x_3)(x_1 - x_3) = \, - P$.

Lemma

If $f \in S_n$, then $f(P) = (\pm 1)P$.

Lemma

If $\tau = (r, s) \in S_n$ is any transposition, then $\tau(P) = -P$.

Lemma

Suppose that $f, g \in S_n$ then $f(g(P)) = (fg)(P)$.

Example

Take $n = 3$.
Then $P = (x_1 - x_2)(x_1 - x_3)(x_2 - x_3)$
Consider $\sigma = (1, 2)$ applied to P.
$\sigma(P) = (x_2 - x_1)(x_2 - x_3)(x_1 - x_3) = \ - P$.

Lemma

If $f \in S_n$, then $f(P) = (\pm 1)P$.

Lemma

If $\tau = (r, s) \in S_n$ is any transposition, then $\tau(P) = -P$.

Lemma

Suppose that $f, g \in S_n$ then $f(g(P)) = (fg)(P)$.

Now, we can prove the theorem...

Definition

A permutation that can be decomposed into an even number of transpositions is called an *even* permutation.

Definition

A permutation that can be decomposed into an even number of transpositions is called an *even* permutation.
A permutation that can be decomposed into an odd number of transpositions is called an *odd* permutation.

Definition

A permutation that can be decomposed into an even number of transpositions is called an *even* permutation.
A permutation that can be decomposed into an odd number of transpositions is called an *odd* permutation.

Fact

An r-cycle is even if and only if r is odd.

Definition

The alternating group A_n is the set of even permutations of S_n.

Definition

The alternating group A_n is the set of even permutations of S_n.

Theorem

$A_n \leq S_n$.

Definition

The alternating group A_n is the set of even permutations of S_n.

Theorem

$A_n \leq S_n$.

Example

$A_3 = \{e, (1,2,3), (1,3,2)\}$.

Definition

The alternating group A_n is the set of even permutations of S_n.

Theorem

$A_n \leq S_n$.

Example

$A_3 = \{e, (1,2,3), (1,3,2)\}$.

$$A_4 = \left\{ \begin{array}{l} e,\ \ (1,2,3),\ \ (1,2,4),\ \ (1,3,2),\ \ (1,3,4),\ \ (1,4,2),\ \ (1,4,3), \\ (2,3,4),\ (2,4,3),\ (1,2)(3,4),\ (1,3)(2,4),\ (1,4)(2,3) \end{array} \right\}.$$

Definition

Suppose that $a, b \in G$. The conjugate of a by b is bab^{-1}.

Definition

Suppose that $a, b \in G$. The conjugate of a by b is bab^{-1}.
We say that $c \in G$ is a conjugate of a if and only if there is $b \in G$ such that $c = bab^{-1}$.

Definition

Suppose that $a, b \in G$. The conjugate of a by b is bab^{-1}.
We say that $c \in G$ is a conjugate of a if and only if there is $b \in G$ such that $c = bab^{-1}$.

Note (Conjugates of Permutations)

Suppose that $f, g \in S_n$. If $1 \leq i, j \leq n$ and $f(i) = j$,

Definition

Suppose that $a, b \in G$. The conjugate of a by b is bab^{-1}.
We say that $c \in G$ is a conjugate of a if and only if there is $b \in G$ such that $c = bab^{-1}$.

Note (Conjugates of Permutations)

Suppose that $f, g \in S_n$. If $1 \leq i, j \leq n$ and $f(i) = j$, then $gfg^{-1}(g(i)) =$

Definition

Suppose that $a, b \in G$. The conjugate of a by b is bab^{-1}.
We say that $c \in G$ is a conjugate of a if and only if there is $b \in G$ such that $c = bab^{-1}$.

Note (Conjugates of Permutations)

Suppose that $f, g \in S_n$. If $1 \leq i, j \leq n$ and $f(i) = j$, then $gfg^{-1}(g(i)) = g(f(i)) =$

Definition

Suppose that $a, b \in G$. The conjugate of a by b is bab^{-1}.
We say that $c \in G$ is a conjugate of a if and only if there is $b \in G$ such that $c = bab^{-1}$.

Note (Conjugates of Permutations)

Suppose that $f, g \in S_n$. If $1 \leq i, j \leq n$ and $f(i) = j$, then $gfg^{-1}(g(i)) = g(f(i)) = g(j)$,

Definition

Suppose that $a, b \in G$. The conjugate of a by b is bab^{-1}.
We say that $c \in G$ is a conjugate of a if and only if there is $b \in G$ such that $c = bab^{-1}$.

Note (Conjugates of Permutations)

Suppose that $f, g \in S_n$. If $1 \leq i, j \leq n$ and $f(i) = j$,
then $gfg^{-1}(g(i)) = g(f(i)) = g(j)$,
that is gfg^{-1} sends $g(i)$ to $g(j)$.

Definition

Suppose that $a, b \in G$. The conjugate of a by b is bab^{-1}.
We say that $c \in G$ is a conjugate of a if and only if there is $b \in G$ such that $c = bab^{-1}$.

Note (Conjugates of Permutations)

Suppose that $f, g \in S_n$. If $1 \leq i, j \leq n$ and $f(i) = j$,
then $gfg^{-1}(g(i)) = g(f(i)) = g(j)$,
that is gfg^{-1} sends $g(i)$ to $g(j)$.
Thus, if
$f = (a_{1,1}, a_{1,2}, \ldots, a_{1,r_1})(a_{2,1}, \ldots, a_{2,r_2}) \ldots (a_{k,1}, \ldots, a_{k,r_k})$
is a decomposition of f into distinct cycles,

Definition

Suppose that $a, b \in G$. The conjugate of a by b is bab^{-1}.
We say that $c \in G$ is a conjugate of a if and only if there is $b \in G$ such that $c = bab^{-1}$.

Note (Conjugates of Permutations)

Suppose that $f, g \in S_n$. If $1 \leq i, j \leq n$ and $f(i) = j$,
then $gfg^{-1}(g(i)) = g(f(i)) = g(j)$,
that is gfg^{-1} sends $g(i)$ to $g(j)$.
Thus, if
$f = (a_{1,1}, a_{1,2}, \ldots, a_{1,r_1})(a_{2,1}, \ldots, a_{2,r_2}) \ldots (a_{k,1}, \ldots, a_{k,r_k})$
is a decomposition of f into distinct cycles,
then $gfg^{-1} =$
$(g(a_{1,1}), \ldots, g(a_{1,r_1}))(g(a_{2,1}), \ldots, g(a_{2,r_2})) \ldots (g(a_{k,1}), \ldots, g(a_{k,r_k}))$