

2.2 If $\alpha \in S_n$, prove that $\text{sgn}(\alpha^{-1}) = \text{sgn}(\alpha)$.

Proof:

If $\alpha = \beta_1 \beta_2 \cdots \beta_k$ (a complete factorization into disjoint cycles), then
 $\alpha^{-1} = \beta_k^{-1} \cdots \beta_2^{-1} \beta_1^{-1}$ (Proposition 2.4).
 By definition, $\text{sgn}(\alpha^{-1}) = (-1)^{n-k} = \text{sgn}(\alpha)$.

2.7 Given $X = \{1, 2, \dots, n\}$, let us call a permutation τ of X an **adjacency** if it is a transposition of the form $(i, i + 1)$ for $i < n$.

(i) Prove that every permutation in S_n , for $n \geq 2$, is a product of adjacencies.

Proof:

Every permutation $\alpha \in S_n$, $n \geq 2$, is a product of transpositions (Prop. 2.10), so we only need to show that any transposition can be written as a product of adjacencies.

Let $\alpha = \tau_1 \tau_2 \cdots \tau_l$. Let $\tau_i = (i j)$, $i < j$. (Note that $\tau_i = (j i)$ as well.)

Then $\tau_i = (i j) = (i + 1 \ i)(i + 2 \ i + 1) \cdots (j - 1 \ j - 2)(j - 1 \ j) \cdots (i + 1 \ i + 2)(i \ i + 1)$.

For example, $(1 \ 5) = (2 \ 1)(3 \ 2)(4 \ 3)(4 \ 5)(3 \ 4)(2 \ 3)(1 \ 2)$.

$\therefore \alpha$ is a product of adjacencies.

(ii) If $i < j$, prove that $(i j)$ is a product of an odd number of adjacencies. **Hint.** Use induction on $j - i$.

Proof:

If $j - i = 1$, then $(i j)$ is an adjacency. Assume $(i j)$ is a product of an odd number of adjacencies for some $j - i > 1$.

Then, by part (i),

$(i j) = (i + 1 \ i)(i + 2 \ i + 1) \cdots (j - 1 \ j - 2)(j - 1 \ j) \cdots (i + 1 \ i + 2)(i \ i + 1)$ is an odd number of adjacencies and

$(i \ j + 1) = (i + 1 \ i)(i + 2 \ i + 1) \cdots (j - 1 \ j - 2) \color{red}{(j \ j - 1)} \color{red}{(j \ j + 1)} (j - 1 \ j) \cdots (i + 1 \ i + 2)(i \ i + 1)$.

This is 2 more adjacencies than the odd number of adjacencies whose product is the transposition $(i j)$.

Since the sum of an odd number and 2 is odd, then the number of adjacencies whose product is the transposition $(i \ j + 1)$ is odd.

2.9 If α is an r -cycle and $1 < k < r$, is α^k an r -cycle?

No.

α is an r -cycle if and only if $\gcd(r, k) = 1$.

Proof:

Let i_1, i_2, \dots, i_r be distinct integers in $\{1, 2, \dots, n\}$.

\Rightarrow :

We will show this direction by contradiction.

Suppose $\gcd(r, k) = d > 1$.

Then $r = dm$ and $k = dn$ for some positive integers m and n . Note that $m > n$.

Thus $\alpha^k(i_1) = \alpha^{dn}(i_1) = i_{dn+1}$, $\alpha^{dn}(i_{dn+1}) = i_{2dn+1}$, \dots , $\alpha^{dn}(i_{(m-1)dn+1}) = i_{dmn+1} = i_1$.

$\therefore \alpha^k$ produces a cycle that does not include i_r , and, hence, cannot be an r -cycle.

\Leftarrow :

Now, suppose $\gcd(r, k) = 1$.

Then $\forall m, n \in \{1, 2, \dots, r\}$, such that $m \neq n$, $(mk + 1)(\text{mod } r) \neq (nk + 1)(\text{mod } r)$.

Otherwise, $mk + 1 - rp = nk + 1 - rq$ for some integers p, q .

Thus, $mk - nk = rp - rq = r(p - q)$, forcing $r \mid (m - n)k$.

Since $r \nmid k$, then $r \mid (m - n)$. But $1 \leq m \leq r$, $1 \leq n \leq r$, and $m \neq n$,

so $-r < 1 - n \leq m - n \leq r - n < r$. This gives us that $|m - n| < r$, hence $r \nmid (m - n)$.

$\therefore \{(jk + 1)(\text{mod } r) \mid j \in \{1, 2, \dots, r\}\} = \{1, 2, \dots, r\}$.

So then $\forall j \in \{0, 1, 2, \dots, r\}$, $\alpha^k(i_{jk+1}) = i_{(j+1)k+1}$.

Thus $\{\alpha^k(i_{jk+1}) \mid j \in \{0, 1, 2, \dots, r\}\} = \{i_1, i_2, \dots, i_r\}$.

$\therefore \alpha^k$ is an r -cycle.

2.11 (i) Prove, for all i , that $\alpha \in S_n$ moves i if and only if α^{-1} moves i .

Proof:

\Rightarrow : Assume α moves i . Suppose $\alpha = \beta_1 \beta_2 \cdots (i c_1 c_2 \dots c_k) \cdots \beta_t$ is the complete factorization of α into disjoint cycles.

Then $\alpha^{-1} = \beta_t^{-1} \cdots (c_k \dots c_1 i) \cdots \beta_2^{-1} \beta_1^{-1}$ by Proposition 2.4.

By definition of $(c_k \dots c_1 i)$, α^{-1} moves i .

\Leftarrow : Proof is similar to \Rightarrow as we can simply interchange α and α^{-1} in the proof above to conclude that if α^{-1} moves i then α moves i .

\therefore For all i , $\alpha \in S_n$ moves i if and only if α^{-1} moves i .

(ii) Prove that if $\alpha, \beta \in S_n$ are disjoint and if $\alpha\beta = (1)$, then $\alpha = (1)$ and $\beta = (1)$.

Proof:

Let $\alpha, \beta \in S_n$ be disjoint permutations such that $\alpha\beta = (1)$,

We will show by contradiction that $\alpha = (1)$ and $\beta = (1)$.

Suppose that $\alpha \neq (1)$.

Then $\exists i$ such that $\alpha(i) = j \neq i$. Since α, β are disjoint, then

$\alpha\beta(i) = \alpha(i) = j$.

$\therefore \alpha\beta \neq (1)$, a contradiction.

$\therefore \alpha = (1)$.

So now we have $\beta = (1)\beta = \alpha\beta = (1)$.

$\therefore \alpha = (1)$ and $\beta = (1)$.

2.15 If $n \geq 3$, show that if $\alpha \in S_n$ commutes with every $\beta \in S_n$, then $\alpha = (1)$.

Proof:

Assume $\exists \alpha$ such that $\alpha\beta = \beta\alpha$ for every $\beta \in S_n$.

We shall show $\alpha = (1)$ by assuming $\alpha \neq (1)$ and arriving at a contradiction.

Suppose $\alpha \neq (1)$, then $\exists i, j \in \{1, 2, \dots, n\}$ such that $\alpha(i) = j$ and $i \neq j$.

Let $\beta \in S_n$ such that $\beta(i) = i$, $\beta(j) = k$, and $\beta(k) = j$ where $i \neq k \neq j$. Since $n \geq 3$, then we know such a β exists.

So $\alpha\beta(i) = \alpha(i) = j \neq k = \beta(j) = \beta\alpha(i)$, and we have our contradiction.

$\therefore \alpha = (1)$.

Thm 2.12

For all $\alpha, \beta \in S_n$, $\text{sgn}(\alpha\beta) = \text{sgn}(\alpha)\text{sgn}(\beta)$.

Proof:

Let $a, b \in \{1, 2, \dots, n\}$ such that $a \neq b$. Let $\tau = (a b)$.

We will show

$$* \text{sgn}(\tau\alpha) = -\text{sgn}(\alpha) \text{ for any } \alpha \in S_n.$$

Case 1:

Suppose $\alpha = (a c_1 c_2 \dots c_k)(b d_1 d_2 \dots d_L)\gamma_1 \gamma_2 \dots \gamma_t$, a complete factorization into disjoint cycles where $K, L \geq 0$, $\alpha \in S_n$.

Since $(a b)(a c_1 c_2 \dots c_k)(b d_1 d_2 \dots d_L) = (a c_1 c_2 \dots c_k b d_1 d_2 \dots d_L)$, then

$$\text{sgn}(\tau\alpha) = \text{sgn}((a c_1 c_2 \dots c_k b d_1 d_2 \dots d_L)\gamma_1 \gamma_2 \dots \gamma_t) = (-1)^{n-(t+1)} = -(-1)^{n-(t+2)} = -\text{sgn}((a c_1 c_2 \dots c_k)(b d_1 d_2 \dots d_L)\gamma_1 \gamma_2 \dots \gamma_t) = -\text{sgn}(\alpha).$$

Case 2:

Suppose $\alpha = (a c_1 c_2 \dots c_k b d_1 d_2 \dots d_L)\gamma_1 \gamma_2 \dots \gamma_t$, a complete factorization into disjoint cycles where $K, L \geq 0$, $\alpha \in S_n$.

Since $(a b)(a c_1 c_2 \dots c_k)(b d_1 d_2 \dots d_L) = (a c_1 c_2 \dots c_k b d_1 d_2 \dots d_L)$, then

$(a b)(a b)(a c_1 c_2 \dots c_k)(b d_1 d_2 \dots d_L) = (a b)(a c_1 c_2 \dots c_k b d_1 d_2 \dots d_L)$, hence

$(a c_1 c_2 \dots c_k)(b d_1 d_2 \dots d_L) = (a b)(a c_1 c_2 \dots c_k b d_1 d_2 \dots d_L)$.

$$\therefore \text{sgn}(\tau\alpha) = \text{sgn}((a c_1 c_2 \dots c_k)(b d_1 d_2 \dots d_L)\gamma_1 \gamma_2 \dots \gamma_t) = (-1)^{n-(t+2)} = -(-1)^{n-(t+1)} = -\text{sgn}((a c_1 c_2 \dots c_k b d_1 d_2 \dots d_L)\gamma_1 \gamma_2 \dots \gamma_t) = -\text{sgn}(\alpha).$$

Now suppose $\alpha = \tau_1 \tau_2 \dots \tau_m$ where each τ_i is a transposition (apply Prop. 2.10) and $\beta = \gamma_1 \gamma_2 \dots \gamma_t$ a complete factorization into disjoint cycles.

We will show $\text{sgn}(\alpha\beta) = \text{sgn}(\alpha)\text{sgn}(\beta)$ by induction on m .

Let $m = 1$. Then $\alpha = \tau_1 (c_1) (c_2) \dots (c_{n-2})$,

hence $\text{sgn}(\alpha) = (-1)^{n-(n-1)} = -1$.

By definition, $\text{sgn}(\beta) = (-1)^{n-t}$.

And by *, $\text{sgn}(\alpha\beta) = -\text{sgn}(\beta) = -(-1)^{n-t}$.

$\therefore \text{sgn}(\alpha\beta) = \text{sgn}(\alpha)\text{sgn}(\beta)$.

Let $m > 1$ and assume $\text{sgn}(\gamma\beta) = \text{sgn}(\gamma)\text{sgn}(\beta)$ for any γ that is a product of m transpositions.

Define $\alpha = \tau_{m+1} \tau_1 \tau_2 \dots \tau_m$, where τ_{m+1} is a transposition in S_n .

Let $\gamma = \tau_1 \tau_2 \dots \tau_m$.

By *, $\text{sgn}(\alpha) = \text{sgn}(\tau_{m+1}\gamma) = -\text{sgn}(\gamma)$.

So then, by our induction hypothesis,

$$\text{sgn}(\alpha\beta) = \text{sgn}(\tau_{m+1}\gamma\beta) = -\text{sgn}(\gamma\beta) = -\text{sgn}(\gamma)\text{sgn}(\beta) = \text{sgn}(\alpha)\text{sgn}(\beta).$$

$\therefore \text{sgn}(\alpha\beta) = \text{sgn}(\alpha)\text{sgn}(\beta)$ for all $\alpha, \beta \in S_n$.