Группы; группы подстановок

Листок 2

Теорема Лагранжа; группы подстановок.

Задача 1 (теорема Лагранжа). Если G — конечная группа, H — ее подгруппа, то количество правых (левых) смежных классов G по H равно $G : H$ (это количество называется *индексом* подгруппы H в группе G).

Определение 1. *Порядком* элемента g группы G называется минимальное натуральное число $n > 0$ такое, что $g^n = e$. Если такого числа не существуют, то говорят, что порядок элемента g бесконечен.

Задача 2. В конечной группе порядок любого элемента делит порядок группы.

Задача 3 (малая теорема Ферма). Для любого простого числа p и любого натурального a

$$a^p \equiv a \mod p.$$

Задача 4. Найдите все неизоморфные группы порядка p (p — простое число).

Задача 5. Если в группе G для любого $g \in G$ выполняется $g^2 = e$, то G — абелева группа.

Задача 6. Найдите все неизоморфные группы порядка 6.

Задача 7. Приведите пример бесконечной неабелевой группы.

Задача 8. Существует ли бесконечная группа, все элементы которой имеют конечный порядок?

Задача 9. Найдите все конечные группы, в которых существует наибольшая собственная подгруппа.

Задача 10. Для каких подстановок из $\mathbf{S}_n$ все остальные подстановки с ними коммутируют?

Задача 11. Найдите произведение подстановок:

а) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 4 & 7 & 1 & 5 & 2 & 6 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 1 & 4 & 3 & 7 & 6 & 5 \end{pmatrix}$;

б) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 4 & 5 & 6 & 2 & 1 & 8 & 7 & 9 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 9 & 8 & 7 & 1 & 2 & 3 & 6 & 5 & 4 \end{pmatrix}$;

в) $\begin{pmatrix} 1 & 2 & 3 & \ldots & n-2 & n-1 & n \\ 2 & 3 & 4 & \ldots & n-1 & n & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 & \ldots & n-2 & n-1 & n \\ n & 1 & 2 & \ldots & n-3 & n-2 & n-1 \end{pmatrix}$.

Задача 12. Найдите порядок подстановки в группе $\mathbf{S}_n$:

а) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 4 & 7 & 1 & 5 & 2 & 6 \end{pmatrix}$;

б) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 4 & 5 & 6 & 2 & 1 & 8 & 7 & 9 \end{pmatrix}$;

в) $\begin{pmatrix} 1 & 2 & 3 & \ldots & n-2 & n-1 & n \\ 2 & 3 & 4 & \ldots & n-1 & n & 1 \end{pmatrix}$.

Определение 2. *Инверсией* для подстановки

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & \dots & n-1 & n \\ i_1 & i_2 & i_3 & \dots & i_{n-1} & i_n \end{pmatrix}$$

называется пара $k, l \in \{1, \dots, n\}$, для которой $k < l$ и $i_k > i_l$.

Задача 13. Найдите все инверсии в подстановке

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 4 & 5 & 6 & 2 & 1 & 8 & 7 & 9 \end{pmatrix}.$$

Определение 3. *Четностью* подстановки $\sigma \in \mathbf{S}_n$ называется четность числа инверсий в ней.

Задача 14. Определите четность следующих подстановок:

а) $\begin{pmatrix} 1 & 2 & 3 & \dots & n-2 & n-1 & n \\ 2 & 3 & 4 & \dots & n-1 & n & 1 \end{pmatrix}$;

б) $\begin{pmatrix} 1 & 2 & 3 & \dots & n-2 & n-1 & n \\ n & n-1 & n-2 & \dots & 3 & 2 & 1 \end{pmatrix}$;

в) $\begin{pmatrix} 1 & 2 & 3 & \dots & n-2 & n-1 & n \\ n & 2 & 3 & \dots & n-2 & n-1 & 1 \end{pmatrix}$.

Определение 4. Подстановка, которая меняет только два элемента, а все остальные оставляет на месте, называется *транспозицией*. Если транспозиция меняет местами элементы i и j, то она обозначается просто через (i, j).

Задача 15. Умножение подстановки (справа или слева) на произвольную транспозицию меняет ее четность на противоположную.

Задача 16. Каких подстановок в группе $\mathbf{S}_n$ больше — четных или нечетных?

Задача 17. Докажите, что каждая подстановка может быть разложена в произведение транспозиций.

Задача 18. Докажите, что каждая подстановка может быть разложена в произведение подстановок только следующего вида:

а) транспозиций $(1,2)$, $(2,3)$, …, $(i, i+1)$, …, $(n-1, n)$;

б) транспозиций $(1,2)$, $(1,3)$, …, $(1, i)$, …, $(1, n)$;

в) всего лишь двух подстановок — транспозиции $(1,2)$ и подстановки

$$\begin{pmatrix} 1 & 2 & 3 & \dots & n-2 & n-1 & n \\ 2 & 3 & 4 & \dots & n-1 & n & 1 \end{pmatrix}.$$

Задача 19. Докажите, что при умножении подстановок их четности складываются по модулю два.

Определение 5. *Циклом* $(i_1\, i_2 \dots i_{k-1}\, i_k)$ называется подстановка, в которой i_1 отображается в i_2, i_2 — в i_3, …, i_{k-1} — в i_k, i_k — в i_1, а остальные элементы отображаются сами в себя.

Два цикла $(i_1,\, i_2 \dots i_{p-1}\, i_p)$ и $(j_1\, j_2 \dots j_{q-1}\, j_q)$ называются *независимыми*, если множества $\{i_1, \dots, i_p\}$ и $\{j_1, \dots, j_q\}$ не пересекаются.

Задача 20. Любая подстановка единственным образом раскладывается в произведение независимых циклов.

Задача 21. Докажите, что каждая четная подстановка может быть разложена в произведение подстановок только следующего вида:

а) циклов длины три;

б) циклов $(1\,2\,3)$, $(1\,2\,4)$, …, $(1\,2\,n)$.

Задача 22. Найдите четность подстановки, разложенной в произведение циклов длин $l_1, \ldots, l_q$.

Задача 23. Найдите порядок подстановки, разложенной в произведение циклов длин $l_1, \ldots, l_q$.

Задача 24. Найдите произведение двух подстановок, разложенных в произведение независимых циклов:

а) $(1\,2\,3\,4)(5\,6\,7)(8\,9) \cdot (1\,2)(3\,4\,5)(6\,7\,8\,9)$;

б) $(1\,2)(3\,4)(5\,6)(7\,8) \cdot (1\,8)(2\,7)(3\,6)(4\,5)$.

Задача 25. Докажите, что два цикла $\{i_1, \ldots, i_p\}$ и $\{j_1, \ldots, j_q\}$ коммутируют тогда и только тогда, когда либо данные циклы являются независимыми, либо один из них есть степень другого.

Задача 26. Каких подстановок больше в группе $\mathbf{S}_n$ — четного или нечетного порядка?

Задача 27. Какие подстановки могут быть представлены в виде произведения двух циклов?

Задача 28. Пусть в разложении $\sigma \in \mathbf{S}_n$ на непересекающиеся циклы число циклов длины i равно m_i. При каких значениях $m_2, \ldots, m_n$ найдется такая подстановка τ, что $\tau^2 = \sigma$?