АЛГЕБРА - 1: ГРУППЫ

Произведением $A \times B$ множеств A и B называется множество пар (a, b), где $a \in A$, $b \in B$. Отображение $f\colon A \to B$ множества A в множество B называется *инъективным*, или *инъекцией*, или *вложением*, если оно переводит разные элементы множества A в разные элементы множества B. Отображение f называется *сюръективным*, или *сюръекцией*, или *отображением "на"*, если в каждый элемент множества B переходит хотя бы один элемент множества A. Отображение f называется *биективным* (*биекцией*, *взаимнооднозначным отображением*), если оно инъективно и сюръективно. В этом (и только в этом!) случае определено обратное отображение $f^{-1}\colon B \to A$, такое что $f \circ f^{-1}$ является тождественным отображением множества B, а $f^{-1} \circ f$ является тождественным отображением множества A.

Если $f\colon A \to B$, $g\colon B \to C$ — два произвольных отображения, то их можно "перемножить", взяв их композицию $g \circ f$:

$$g \circ f(a) = g(f(a)), \quad a \in A.$$

Задача 1. Докажите, что для двух биективных отображений $f\colon A \to B$, $g\colon B \to C$ отображение $g \circ f$ также биективно, и $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

Пусть A — некоторое множество (конечное или бесконечное). Обозначим через $S(A)$ множество всех биективных оборажений из множества A на себя. Обозначим через 1 или e тождественное отображение множества A. Композиция отображений наделяет это множество операцией умножения.

Определение 1. Множество $S(A)$ вместе с операцией умножения (композицией) называется симметрической группой или группой подстановок.

Если множество A конечно и состоит из n элементов, то $S(A)$ обозначается S_n. Подстановки можно записывать в виде таблиц. Например, подстановка $\sigma\colon 1 \mapsto 3, 2 \mapsto 4, 3 \mapsto 1, 4 \mapsto 2$ чисел $1, 2, 3, 4$ записывается как

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}.$$

В верхней строке пишутся числа в порядке возрастания, а внижней — их образы.

Задача 2. Найдите произведение

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 2 & 1 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 4 & 1 & 2 \end{pmatrix}.$$

Задача 3. (1) Сколько элементов в группе S_n?
(2) Сколько из них оставляют 1 на месте? Сколько переводят 1 в n?
(3) Сколько из них удовлетворяют условию $\sigma(1) < \sigma(2)$?
(4) Сколько из них удовлетворяют условию $\sigma(1) < \sigma(2) < \cdots < \sigma(k)$, где $2 < k < n$?

Задача 4. Приведите пример двух подстановок $\sigma_1, \sigma_2 \in S_n$, таких что $\sigma_1 \circ \sigma_2 \neq \sigma_2 \circ \sigma_1$. Какое наименьшее возможное n можно взять для этого?

Циклической подстановкой множества элементов $a_1, \ldots, a_k \in A$ называется подстановка σ множества A, которая переводит a_1 в a_2, a_2 в a_3 и так далее по кругу, переводя a_k в a_1, и которая оставляет все остальные элементы множества A на месте. Число k называется длиной циклической подстановки, а сама подстановка обозначается $(a_1, a_2, \ldots, a_k)$. Циклическая подстановка длины 2 называется транспозицией. Она переставляет какие-то два элемента и соатвляет все остальные элементы на месте.

Задача 5. Найдите композицию двух транспозиций $(i, j) \circ (k, l)$. Рассмотрите все возможные варианты.

Задача 6. Пусть $\sigma \in S(A)$ — произвольная подстановка, а $\tau = (a_1, \ldots, a_k)$ — циклическая подстановка длины k. Чему равно $\sigma \circ \tau \circ \sigma^{-1}$?

Задача 7. (1) Докажите, что каждая подстановка σ из S_n представима как произведение транспозиций.
(2) Докажите, что количество подстановок в таком представлении всегда либо четно, либо нечетно. (Указание: рассмотрите, что прозойдет, если применить подстановку σ к переменным $x_1, \ldots, x_n$ в полиноме $P = \prod_{i<j}(x_i - x_j) = (x_1 - x_2)(x_1 - x_3)\ldots(x_{n-1} - x_n)$.)

Подстановка $\sigma \in S_n$ называется (не)четной, если количество транспозиций в ее представлении (не)четно.

Задача 8. Найдите четность цикла длины k.

На множестве $S(A)$ заданы следующие структуры: умножение, взятие обратной подстановки, тождественная подстановка. Эту ситуацию удобно аксиоматизировать.

Определение 2. Пусть G — множество, где задана операция "умножения" $g, h \mapsto g \cdot h$, "взятие обратного" $g \mapsto g^{-1}$ и задан "единичный элемент" e, причем все это удовлетворяет следующим аксиомам:

(1) Ассоциативность: $(g_1 \cdot g_2) \cdot g_3 = g_1 \cdot (g_2 \cdot g_3)$ для всех $g_1, g_2, g_3 \in G$;
(2) Единица: $e \cdot g = g \cdot e = g$ для всех $g \in G$;
(3) Обратный элемент: $g \cdot g^{-1} = g^{-1} \cdot g = e$ для всех $g \in G$.

Тогда G называется *группой*.

Подмножество $H \subset G$, замкнутое относительно этих операций, называется *подгруппой* группы G. В частности, подгруппа всегда содержит единицу группы.

Задача 9. Дана группа G. Докажите, что:

(1) если $gh = h$ или $hg = h$, то $g = e$;
(2) если $gh = e$ или $hg = e$, то $h = g^{-1}$.

Таким образом, операция умножения однозначно задает единицу и операцию взятия обратного элемента (если они существуют).

Задача 10. Являются ли группами следующие множества с указанными операциями:

(1) натуральные числа с операцией сложения;
(2) целые числа с операцией сложения;
(3) целые числа с операцией умножения;
(4) рациональные числа с операцией умножения;
(5) вещественные числа с операцией сложения;
(6) вещественные числа с операцией умножения;
(7) движения плоскости с операцией композиции;
(8) числа открытого интервала $(-1, 1)$ с операцией $u \cdot v = (u + v)/(1 + uv)$ (проверьте также, что операция корректно определена);
(9) фигуры (множества точек) на плоскости с операцией объединения;
(10) фигуры (множества точек) на плоскости с операцией симметрической разности: $A * B$ состоит из точек, которые принадлежат ровно одной из фигур A или B;
(11) отображения из фиксированного множества A в фиксированную группу G, с операцией $(f \cdot g)(a) = f(a) \cdot g(a)$.

Произведение групп G_1 и G_2 состоит из всех пар (g_1, g_2), $g_1 \in G_1, g_2 \in G_2$ с групповой операцией $(g_1, g_2) \cdot (g_1', g_2') = (g_1 \cdot g_1', g_2 \cdot g_2')$. Оно обозначается $G_1 \times G_2$.

Отображение $f\colon G \to G'$ называется гомоморфизмом, если оно сохраняет умножение: $f(g_1 g_2) = f(g_1) f(g_2)$.

Задача 11. Проверьте, что любой гомоморфизм групп переводит единицу группы G в единицу группы G' и сохраняет операцию взятия обратного элемента: $f(g^{-1}) = f(g)^{-1}$ для любого $g \in G$.

Гомоморфизм называется изоморфизмом, если он биективен. Группы, между которыми существует изоморфизм, называются *изоморфными*.

Теорема Кэли. *Любая группа G изоморфна некоторой подгруппе симметрической группы $S(A)$.*

Доказательство. Возьмем в качестве A саму группу G и зададим для каждого элемента $g \in G$ подстановку $\sigma_g \in S(G)$ как умножение слева на g:

$$\sigma_g\colon G \to G, h \mapsto gh.$$

Тогда отображение $f\colon G \to S(G)$, $g \mapsto \sigma_g$ задает изоморфизм группы G с подгруппой в $S(G)$, состоящей из всех подстановок вида σ_g. Действительно, $\sigma_{g_1 g_2} = \sigma_{g_1} \circ \sigma_{g_2}$ (то есть отображение $g \mapsto \sigma_g$ является гомоморфизмом групп), и из равенства $\sigma_{g_1} = \sigma_{g_2}$ следует, что $g_1 = g_2$ (то есть соотвествие $g \leftrightarrow \sigma_g$ взаимно-однозначно). $\square$

Теорема Лагранжа ([1], Глава 4, §5)**.** *Пусть G — группа, состоящая из конечного числа элементов, и H — ее произвольная подгруппа. Тогда число элементов подгруппы H делит число элементов группы G.*

Число элементов группы G обозначается $|G|$. Используя это обозначение, мы можем записать теорему Лагранжа короче: если $|G| < \infty$, то $|H|$ делит $|G|$.

Пусть g — произвольный элемент группы G. Если существует такое $n \in \mathbb{N}$, что $g^n = e$, то говорят, что g имеет конечный порядок. Наименьшее такое n называется порядком элемента g.

Задача 12. Пусть g — элемент порядка n. Докажите, что все элементы $g^0 = e, g^1 = g, \ldots, g^{n-1}$ различны и образуют подгруппу, изоморфную группе $\mathbb{Z}_n$ всех остатков по модулю n с операцией сложения.

В частности, по теореме Лагранжа следует, что в конечной группе порядок любого элемента является делителем $|G|$. Используя этот факт, мы можем легко доказать теорему Эйлера:

Тоерема Эйлера. *Пусть $a, n \in \mathbb{N}$ — два взаино-простых числа. Тогда $a^{\phi(n)} \equiv 1 \mod n$ (тут $\phi(n)$ — это функция Эйлера, равная числу всех остатков по модулю n, взаимно простых с n).*

Доказательство. Рассмотрим множество $\mathbb{Z}_n^*$ всех остатков по модулю n, взаимно простых с n. Тогда оно ообразует группу (проверьте!) относительно операции умножения остатков. При этом по определению $|Z_n^*| = \phi(n)$. Пусть m — порядок элемента a (точнее, его остатка по модулю n) в этой группе. Тогда m является делителем $\phi(n)$, и

$$a^{\phi(n)} = (a^d)^{\phi(n)/d} = 1^{\phi(n)/d} = 1$$

в группе $\mathbb{Z}_n^*$. Но это в точности означает, что $a^{\phi(n)} \equiv 1 \mod n$. □

Группа G называется *коммутативной* или *абелевой*, если в дополнение к ассоциативности ее умножение коммутативно: $g_1 g_2 = g_2 g_1$ для любых элементов $g_1, g_2 \in G$. Абелевы группы устроены проще, чем некоммутативные. В частности, известно описание всех конечных абелевых групп.

Теорема ([1], Глава 9, §1)**.** *Пусть G — конечная абелева группа. Тогда она изоморфна прямому произведению групп:*

$$\mathbb{Z}_{l_1} \times \mathbb{Z}_{l_2} \times \cdots \times \mathbb{Z}_{l_r}$$

где l_1 делит l_2, l_2 делит l_3, ..., l_{r-1} делит l_r. Причем набор чисел $(l_1, \ldots, l_r)$ определен однозначно.

Некоторые из этих групп в свою очередь могут быть разложены в прямое произведение меньших групп:

Задача 13. (Китайская теорема об остатках) Докажите, что если k, l – взаимно простые натуральные числа, то $\mathbb{Z}_{kl}$ изоморфна $\mathbb{Z}_k \times \mathbb{Z}_l$, а группа $\mathbb{Z}_{kl}^*$ изоморфна $\mathbb{Z}_k^* \times \mathbb{Z}_l^*$.

Задача 14. Опишите с точностью до изоморфизма все группы из $n \leq 6$ элементов.

Список литературы

[1] Э.Б. Винберг, Курс алгебры, М.: Изд-во “Факториал Пресс”, 2001.