Абстрактные группы

30 ноября • 8 класс

Разбор

Определение. Пусть X — множество. ***Бинарной операцией*** на множестве X называется любое отображение $\bullet\colon X \times X \to X$. Хотя по смыслу $\bullet$ это просто функция двух аргументов и её следовало бы записывать $\bullet(g_1, g_2)$, для удобства пишут $g_1 \bullet g_2$, как с арифметическими операциями.

Пример 1. $+$ (сложение) и $\cdot$ (умножение) — бинарные операции на множестве целых чисел $\mathbb{Z}$.

Пример 2. Пусть M — любое множество. Тогда $\circ$ (композиция) — бинарная операция на множестве отображений из M в M.

Определение. Непустое множество G, снабжённое бинарной операцией $\bullet$, называется ***группой***, если выполнены **аксиомы** (G1), (G2) и (G3).

(G1) Операция $\bullet$ ***ассоциативна***:

$$(\forall g, h, k \in G): \quad (g \bullet h) \bullet k = g \bullet (h \bullet k).$$

(G2) Существует ***нейтральный*** элемент e_G для $\bullet$:

$$(\exists e_G \in G)(\forall g \in G): \quad e_G \bullet g = g = g \bullet e_G.$$

(G3) Каждый элемент в G имеет ***обратный*** относительно $\bullet$:

$$(\forall g \in G)(\exists g^{-1} \in G): \quad g^{-1} \bullet g = e_G = g \bullet g^{-1}.$$

Для краткости выкладок вы можете опускать значок операции, когда это не приводит к путанице, как с умножением: вместо $(g \bullet h) \bullet k$ писать $(gh)k$. Также можно писать просто e вместо e_G.

Пример 3. Пусть $G = \{e_G\}$ (множество из одного элемента), а $\bullet$ определена единственным возможным образом (каким?). Тогда для G тривиально выполнены все аксиомы, так что G — группа.

Задача 1. (a) Докажите, что $\mathbb{Z}$ с операцией $+$ является группой.
(b) Докажите, что $\mathbb{Z}$ с операцией $\cdot$ не является группой.

Решение: (a) Ассоциативность сложения целых чисел всем известна. Нейтральный элемент по сложению — 0. Обратный элемент по сложению к n — $-n$.
(b) Не существует такого целого числа 2^{-1}, что $2 \cdot 2^{-1} = 1$ (потому что левая часть равенства всегда делится на 2, а правая — нет), так что $(\mathbb{Z}, \cdot)$ — не группа. □

Задача 2. (a) Докажите, что в группе только один нейтральный элемент.
(b) Докажите, что у каждого элемента группы только один обратный элемент.

Решение: (a) Пусть e и e' — нейтральные элементы. Тогда

$$e = e \bullet e' = e',$$

где первое равенство следует из нейтральности e', а второе — из нейтральности e.
(b) Пусть h и k — обратные к g. Тогда

$$\begin{aligned} h = & \quad h \bullet e & \text{(определение нейтрального)} \\ = & \quad h \bullet (g \bullet k) & \text{(определение обратного)} \\ = & \quad (h \bullet g) \bullet k & \text{(ассоциативность)} \\ = & \quad e \bullet k & \text{(определение обратного)} \\ = & \quad k & \text{(определение нейтрального).} \end{aligned}$$

□

Задача 3. Докажите, что $D_n = \mathrm{Sym}(P_n)$ (группа симметрий правильного n-угольника) в самом деле является группой.

Решение: Знаем, что композиция отображений ассоциативна, а симметрии — частный случай отображениий, так что (G1) выполнена. Тождественное движение удовлетворяет аксиоме (G2). В листке про группы симметрий доказывали, что у движений есть обратные, так что (G3) выполнена. □

Определение. Пусть $(G, \bullet)$ — группа. Подмножество $H \subseteq G$ называется ***подгруппой***, если

$$e_G \in H,$$
$$(\forall h \in H): \quad h^{-1} \in H,$$
$$(\forall h_1, h_2 \in H): \quad h_1 \bullet h_2 \in H,$$

то есть «операция не выводит за пределы H».

Пример 4. В предыдущем листке доказывалось, что произведение чётных перестановок — чётная перестановка. Следовательно, подмножество всех чётных перестановок из S_n — подгруппа. Она обозначается A_n.

Задача 4. Найдите все подгруппы в D_3, выпишите количества элементов в них.

Решение: Обозначим один из поворотов через r, а одну из осевых симметрий через s. Тогда r^2 — второй поворот, а rs и r^2s — вторая и третья симметрии. Таким образом наша группа состоит из следующих элементов: $D_3 = \{e, r, r^2, s, rs, r^2s\}$.

Хотим перечислить всевозможные $H \subseteq D_3$. Переберём случаи.

- Допустим, $r \in H$. Тогда $r^2 \in H$.
  - Допустим, $s \in H$. Тогда $rs, r^2s \in H$, так что $H = D_3$.
  - Допустим, $s \notin H$. Тогда $rs, r^2s \notin H$, так что $H = \{e, r, r^2\}$.
- Допустим, $r \notin H$. Тогда $r^2 \notin H$.
  - Допустим, одна из осевых симметрий лежит в H. Тогда остальные две не лежат, иначе r и r^2 тоже попали бы в H. Следовательно H состоит только из этой осевой симметрии и e, то есть $H = \{e, s\}$, или $H = \{e, rs\}$, или $H = \{e, r^2s\}$.

– Допустим, ни одна из симметрий не лежит в H. Тогда $H = \{e\}$.

Таким образом, все возможные подгруппы: $\{e\}$, $\{e, s\}$, $\{e, rs\}$, $\{e, r^2 s\}$, $\{e, r, r^2\}$ и D_3. $\square$

Задача 5. Пусть $g_1, g_2, g_3, g_4 \in G$, где $(G, \bullet)$ — какая-то группа. Придайте однозначный смысл выражению $g_1 \bullet g_2 \bullet g_3 \bullet g_4$.

Решение: Значение этого выражения можно определить любым из пяти способов: $((g_1 \bullet g_2) \bullet g_3) \bullet g_4$, $(g_1 \bullet (g_2 \bullet g_3)) \bullet g_4$, $(g_1 \bullet g_2) \bullet (g_3 \bullet g_4)$, $g_1 \bullet ((g_2 \bullet g_3) \bullet g_4)$ или $g_1 \bullet (g_2 \bullet (g_3 \bullet g_4))$. Из-за ассоциативности, ответ получится одним и тем же.

$$
\begin{aligned}
(g_1 \bullet (g_2 \bullet g_3)) \bullet g_4 &= ((g_1 \bullet g_2) \bullet g_3) \bullet g_4 && \text{(ассоциативность} \\
&= (g_1 \bullet g_2) \bullet (g_3 \bullet g_4) && \text{(ассоциативность} \\
&= g_1 \bullet (g_2 \bullet (g_3 \bullet g_4)) && \text{(ассоциативность)} \\
&= g_1 \bullet ((g_2 \bullet g_3) \bullet g_4) && \text{(ассоциативность)}
\end{aligned}
$$

$\square$

Определение. Для элемента g группы $(G, \bullet)$ и натурального числа n запись g^n обозначает $\underbrace{g \bullet g \bullet \cdots \bullet g}_{n \text{ раз}}$, а запись g^{-n} обозначает $\underbrace{g^{-1} \bullet g^{-1} \bullet \cdots \bullet g^{-1}}_{n \text{ раз}}$.

Теорема 1. *В группах можно сокращать множители справа, то есть для любых трёх элементов g, h, k группы $(G, \bullet)$ имеем*

$$g \bullet k = h \bullet k \;\Rightarrow\; g = h.$$

Доказательство. Так как G — группа, у элемента k существует обратный k^{-1}. Тогда имеем

$$
\begin{aligned}
g \bullet k &= h \bullet k && \Rightarrow \\
(g \bullet k) \bullet k^{-1} &= (h \bullet k) \bullet k^{-1} && \Rightarrow \text{(пользуемся ассоциативностью)} \\
g \bullet (k \bullet k^{-1}) &= h \bullet (k \bullet k^{-1}) && \Rightarrow \text{(определение обратного)} \\
g \bullet e_G &= h \bullet e_G && \Rightarrow \text{(определение нейтрального)} \\
g &= h.
\end{aligned}
$$

$\square$

Теорема 2. *В группах можно сокращать множители слева, то есть для любых трёх элементов g, h, k группы $(G, \bullet)$ имеем*

$$k \bullet g = k \bullet h \;\Rightarrow\; g = h.$$

Это первый (но далеко не последний) пример пользы от изучения групп в целом, вместо изучения конкретных интересующих нас групп. Раньше мы отдельно доказывали, что можно сокращать множители в группе симметрий фигуры и в группе перестановок. Теперь мы доказали это разом для всех групп. Так что, когда в будущем нам потребуется изучить какую-нибудь новую группу (например, группу всех вращений куба или группу всех преобразований кубика Рубика), мы сразу будем знать про неё кучу полезных фактов.

Задачи для самостоятельного решения

Задача 1. Придумайте ещё 2 бинарных операции на множестве $\mathbb{Z}$.
Задача 2. Сколько всего бинарных операций на множестве из n элементов?
Задача 3. Докажите, что S_n (группа перестановок n элементов) в самом деле является группой.
Задача 4. Докажите, что для любых двух элементов g, h любой группы $(G, \bullet)$ выполнено

$$(g \bullet h)^{-1} = h^{-1} \bullet g^{-1}.$$

Определение. Группа $(G, \bullet)$ называется ***коммутативной***, если выполнена аксиома (G4).

(G4) Операция $\bullet$ ***коммутативна***:

$$(\forall g, h \in G): \quad g \bullet h = h \bullet g.$$

Задача 5. (a) Докажите, что группа A_3 коммутативна.
(b) Докажите, что группа A_4 не коммутативна.
Задача 6 (3 балла). Пусть группа $(G, \bullet)$ такова, что для всех $g \in G$ выполнено $g^2 = e_G$. Покажите, что G коммутативна.
Задача 7. (a) Найдите все подгруппы в S_3, количества элементов в них. (b) Найдите все подгруппы в A_4, количества элементов в них.
Задача 8. Докажите теорему 2.

В предыдущих листках мы уже выписывали таблицы умножения для некоторых групп. Можно сделать это для любой группы.

$\bullet$	e	$\cdots$	h	$\cdots$
e	e	$\cdots$	h	$\cdots$
$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$
g	g	$\cdots$	$g \bullet h$	$\cdots$
$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$

Задача 9. Покажите, что в каждая строка и каждый столбец содержат все элементы группы ровно по одному разу. *(прямо как судоку!)*
Задача 10. (a) Покажите, что есть лишь одна возможная таблица умножения для группы из 2 элементов. (b, 2 балла) Покажите, что есть лишь одна возможная таблица умножения для группы из 3 элементов. (c, 4 балла) Найдите все возможные таблицы умножения для группы из 4 элементов.