Лекция 13.

Гайфуллин Сергей Александрович

МГУ

29 октября, 2021

Определение.

Пусть G – непустое множество с одной бинарной операцией $(x, y) \mapsto x * y$. Тогда G называется <u>группой</u>, если выполнены следующие три аксиомы.

- для любых $x, y, z \in G$ выполнено $(x * y) * z = x * (y * z)$ (ассоциативность);
- существует $e \in G$ такой, что $\forall x \in G$ выполнено $e * x = x * e = x$. (нейтральный элемент);
- для каждого $g \in G$ существует $g^{-1} \in G$ такой, что $g * g^{-1} = g^{-1} * g = e$ (обратный элемент).

Если из контекста не понятно, какая операция имеется в виду, то используют обозначение $(G, *)$.

Определение.

Группа G называется <u>абелевой</u> (коммутативной) группой, если

- для любых $x, y \in G$ выполнено $x * y = y * x$ (коммутативность).

Примеры групп.

1. Числовые группы (все они абелевы)
   - по сложению $(\mathbb{Z},+)$, $(\mathbb{Q},+)$, $(\mathbb{R},+)$.
   - по умножению $\mathbb{Q}^\times=(\mathbb{Q}\setminus 0,\cdot)$, $\mathbb{R}^\times=(\mathbb{R}\setminus 0,\cdot)$, $(\{1,-1\},\cdot)$.
2. векторы по сложению (все они абелевы) $(\mathbb{R}^n,+)$, $(\mathrm{Mat}_{mn}(\mathbb{R}),+)$, $(\mathbb{Q}^n,+)$, $(\mathrm{Mat}_{mn}(\mathbb{Q}),+)$, $(\mathbb{Z}^n,+)$, $(\mathrm{Mat}_{mn}(\mathbb{Z}),+)$.
3. Симметрические группы $(S_n,\circ)$. (при $n\geq 3$ не абелевы)
4. Невырожденные матрицы по умножению (при $n\geq 2$ не абелевы) $\mathrm{GL}_n(\mathbb{R})=(\{A\in\mathrm{Mat}_{nn}(\mathbb{R})|\det A\neq 0\},\cdot)$, $\mathrm{GL}_n(\mathbb{Q})=(\{A\in\mathrm{Mat}_{nn}(\mathbb{Q})|\det A\neq 0\},\cdot)$.
5. Группы преобразований (почти всегда не абелевы)
   - $(S(X),\circ)$ – группа биекций $X\to X$ для некоторого фиксированного множества X.
   - группа движений плоскости $(\mathrm{Iso}(\mathbb{R}^2),\circ)$.

Множества с операциями, не являющиеся группами.

- $(\mathbb{N}, +)$ (нет нейтрального элемента)
- $(\mathbb{N} \cup \{0\}, +)$ (не к любому элементу есть обратный)
- $(\mathbb{Z}, \cdot)$ (не к любому элементу есть обратный)
- $(\mathrm{Mat}_{nn}(\mathbb{R}), \cdot)$ (не к любому элементу есть обратный)
- $(\mathbb{Z} \setminus \{3, -3\}, +)$ (не корректно определена операция)
- $(\mathbb{Z}, *)$, где $x * y = x + 2y$ (операция не ассоциативна)

Мультипликативная и аддитивная терминологии

Во многих примерах операция – это умножение. На самом деле это вопрос терминологии. Любую операцию в любой группе можно назвать умножением и писать $xy = x \cdot y$ вместо $x * y$. Нейтральный элемент группы будем также называть единицей группы (обозначается e). Такая терминология и обозначения называются мультипликативными.

В других примерах операция – это сложение. Однако обычно с операцией сложения получается абелева группа. Операцию в произвольной абелевой группе принято называть сложением. При этом нейтральный элемент называется нулем группы (обозначается 0), а обратный элемент к x – противоположным (обозначается $-x$). Такая терминология и обозначения называются аддитивными.

Заметим, что абелева группа является частным случаем произвольной группы. Поэтому к ней применимы обе терминологии. Это не должно вызывать путаницы, надо лишь научиться переводить выражения с одного языка на другой.

Простейшие следствия из аксиом

- Нейтральный элемент в группе единственный. Допустим противное: пусть e и e' – нейтральные элементы группы G. Тогда $e = ee' = e'$.
- Обратный элемент к данному элементу единственный. Допустим противное: пусть h и h' – обратные элементы к элементу g группы G. Тогда $h = h(gh') = (hg)h' = h'$.
- Если $xy = xz$, (или $yx = zx$), то $y = z$. Умножим обе части равенства на x^{-1} слева (справа).
- Если $gh = e$, то $g = h^{-1}$ и $h = g^{-1}$. Имеем $gh = e = gg^{-1}$, значит, $h = g^{-1}$. Второе аналогично.
- $(g^{-1})^{-1} = g$. В самом деле $gg^{-1} = e$, отсюда $(g^{-1})^{-1} = g$.
- Выполнена обобщенная ассоциативность. (Доказательство было ранее.)
- $(xy)^{-1} = y^{-1}x^{-1}$. Перемножим

$$xyy^{-1}x^{-1} = xex^{-1} = xx^{-1} = e.$$

Пусть $g \in G$, $k \in \mathbb{Z}$. Определим

$$g^k = \begin{cases} gg \dots g \quad (k \text{ раз}), \text{ если } k > 0; \\ e, \text{ если } k = 0; \\ g^{-1}g^{-1} \dots g^{-1} \quad (-k \text{ раз}), \text{ если } k < 0. \end{cases}$$

Тогда $g^a g^b = g^{a+b}$ и $(g^a)^b = g^{ab}$.
Упражнение: докажите это.

Определение.

Пусть G – группа с операцией $*$. Подмножество $H \subseteq G$ называется <u>подгруппой</u>, если H является группой относительно той же операции $*$.

Пример.

Множество $2\mathbb{Z}$ четных целых чисел образует подгруппу в группе $(\mathbb{Z}, +)$.

Лемма

Любая подгруппа содержит нейтральный элемент группы.

Доказательство. Пусть H – подгруппа G и e – нейтральный элемент G. Тогда в H есть нейтральный элемент e'. Получаем $ee' = e'e'$. Отсюда $e = e'$.

Лемма

Пусть H – подгруппа группы G. Рассмотрим $h \in H$ и пусть h^{-1} – обратный к h в G. Тогда $h^{-1} \in H$.

Доказательство. Так как H – группа, существует обратный элемент $h' \in H$. Тогда $hh' = hh^{-1} = e$. Отсюда $h' = h^{-1}$.

Теорема

Пусть H – подмножество группы G. Тогда H – подгруппа G тогда и только тогда, когда выполнены следующие условия:

1. $H \neq \varnothing$;
2. H замкнуто относительно операции, то есть если $h_1, h_2 \in H$, то $h_1 h_2 \in H$;
3. H замкнуто относительно взятия обратного, то есть если $h \in H$, то $h^{-1} \in H$.

Доказательство. Необходимость первых двух условий очевидна. Необходимость третьего условия следует из предыдущей леммы. Докажем достаточность. Пусть условия выполнены. Тогда из условий 1 и 2 H – непустое множество с бинарной операцией (той же, что и в G, а значит, ассоциативной). По условию 1 найдется $h \in H$. По условию 3, $h^{-1} \in H$. По условию 2 $hh^{-1} = e \in H$, то есть в H есть нейтральный элемент. По условию 3 каждый элемент имеет обратный.

Примеры.

- $(\mathbb{Z}, +) \subset (\mathbb{Q}, +) \subset (\mathbb{R}, +)$ – цепочка подгрупп;
- Множество A_n четных подстановок длины n образует подгруппу в S_n;
- Множество невырожденных верхнетреугольных матриц образует подгруппу в $\mathrm{GL}_n(\mathbb{R})$;
- Множество невырожденных диагональных матриц образует подгруппу в $\mathrm{GL}_n(\mathbb{R})$;
- Множество $\mathrm{SL}_n(\mathbb{R})$ матриц $n \times n$ с определителем 1 образует подгруппу в $\mathrm{GL}_n(\mathbb{R})$.
- Пересечение двух подгрупп группы G – подгруппа.

Определение.

Пусть R – непустое множество с двумя бинарными операциями $(x, y) \mapsto x + y$ и $(x, y) \mapsto xy$. Тогда R называется <u>кольцом</u>, если выполнены следующие аксиомы.

- для любых $x, y, z \in R$ выполнено $(x + y) + z = x + (y + z)$;
- существует $0 \in R$ такой, что $\forall x \in R$ выполнено $0 + x = x + 0 = x$;
- для каждого $r \in R$ существует $-r \in R$ такой, что $r + (-r) = (-r) + r = 0$;
- для любых $x, y \in R$ выполнено $x + y = y + x$;
- для любых $x, y, z \in R$ выполнено $(x + y)z = xz + yz$;
- для любых $x, y, z \in R$ выполнено $z(x + y) = zx + zy$.

Если из контекста не понятно, какие операции имеются в виду, то используют обозначение $(R, +, \cdot)$

- Говорят, что кольцо R <u>ассоциативно</u>, если для любых $x, y, z \in R$ выполнено $(xy)z = x(yz)$.
- Говорят, что кольцо R – это <u>кольцо с единицей</u>, если существует элемент $1 \neq 0$ такой, что $\forall r \in R$ выполено $1r = r1 = r$.
- Говорят, что ассоциативное кольцо с единицей R является <u>телом</u>, если $\forall r \neq 0$ существует r^{-1} такое, что $rr^{-1} = r^{-1}r = 1$.
- Говорят, что кольцо R <u>коммутативно</u>, если для любых $x, y \in R$ выполнено $xy = yx$.

Определение.

<u>Поле</u> – это коммутативное тело, то есть ассоциативное коммутативное кольцо с единицей, у которого каждый ненулевой элемент обратим.

Простейшие свойства.

- Ноль в кольце единственный.
- Противоположный элемент к каждому элементу единственный.
- Единица в кольце, если она есть, единственная.
- Обратный к данному элемент в кольце с единицей, если он есть, единственный.
- Для любого $x \in R$ выполнено $x0 = 0x = 0$. Докажем одно из равенств:
$$x0 = x(0+0) = x0 + x0.$$
Прибавим к каждой части $-(x0)$, получим $0 = x0$.
- Пусть R – ассоциативное кольцо с единицей. Множество обратимых элементов $R^{\times}$ с операцией умножения образует группу.

Примеры

- $(\mathbb{R}^3, [,])$ – не ассоциативное кольцо.
- $\mathrm{Mat}_{nn}(\mathbb{R}, +, \cdot)$, $\mathrm{Mat}_{nn}(\mathbb{Q}, +, \cdot)$ – не коммутативные ассоциативные кольца с единицей.
- $(\mathbb{Z}, +, \cdot)$ – коммутатвиное ассоциативное кольцо с единицей.
- $(2\mathbb{Z}, +, \cdot)$ – коммутатвиное ассоциативное кольцо.
- $(\mathbb{R}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$ – поля.