Теория алгебраических структур

Лекция 2

Теория групп

Эварист Галуа

25.10.1811–31.05.1832

Еще не зная об этом, мы используем алгебраические структуры с 1 класса: полугруппа $\Pi =< N, + >$, моноид $M =< N, \times >$. Важность понятия группы для математики в целом сопоставима только с важностью таких понятий как множество, отображение, функция, пространство…

Понятия группы, поля, нормальной подгруппы ввел Э. Галуа – один из самых удивительных математиков, оказавший громадное влияние на ее развитие. К сожалению, он был убит на дуэли в возрасте 20 лет. Уже в 16–18 лет он опубликовал работы о разрешимости уравнений в радикалах, но великие Коши, Фурье, Пуассон даже не смогли ничего понять. Множество его работ было утеряно (или так об этом сообщалось). Позже Коши часть понял и опубликовал под своим именем. Не надеясь на честность французских математиков, в письме другу Галуа просил сообщить свои новые результаты Гауссу и Якоби. Работы Галуа получили широкое признание только в 1870-х годах.

Теория групп широко используется не только практически во всех разделах математики, но и в других науках. Там, где есть симметрии, есть группа. В физике группы симметрий используются в кристаллографии; фермионы и бозоны определяются симметрией совместной волновой функции при перестановке частиц; симметрия относительно вращений в пространстве приводит к сохранению момента импульса. В химии группы самосовмещений геометрических фигур описывают строение молекул. Был случай, когда вещество в природе нашли через несколько лет после определения соответствующей ему группы. И даже в биологии используются группы при изучении симметрии цветка.

Полугруппа, моноид, группа. Определения и примеры

Определение 1. Говорят, что на множестве M задана бинарная операция $*$, если любой упорядоченной паре $< a, b >$ элементов из M ставится в соответствие элемент $a * b \in M$.

Примеры.

1. $a + b = c \in M$ – бинарная операция (M – числовое множество).
2. $[\bar{a}, \bar{b}] = \bar{c} \in M$ – бинарная операция (M– множество векторов).
3. $(\bar{a}, \bar{b}) = c \notin M$ – не является бинарной операцией: векторам ставится в соответствие число (M – множество векторов).

Бывают унарные операции – транспонирование матрицы; и операции для любого упорядоченного набора из n элементов.

Свойства операции:

1. $a * b = b * a$ – коммутативный закон операции.
2. $(a * b) * c = a * (b * c)$ – ассоциативный закон операции.

Утверждение 1. Если бинарная операция ассоциативна, то результат ее применения к последовательности элементов не зависит от расстановки скобок.

Символика: мультипликативная ($* \to \cdot\ (\times)$) и аддитивная ($* \to +$).

В мультипликативной символике: $(a^m)^n = a^{mn},\ a^{m+n} = a^m a^n$.

В аддитивной символике: $n(ma) = (nm)a,\ (m + n)a = ma + na.$

Если множество M конечное, то результат бинарной операции можно задать таблицей Кэли. Пусть $M = \{a_1, \dots, a_n\}$

$*$	a_1	a_2	…	a_n
a_1	$a_1 * a_1$	$a_1 * a_2$	…	$a_1 * a_n$
a_2	$a_2 * a_1$	$a_2 * a_2$	…	$a_2 * a_n$
…	…	…	…	…
a_n	$a_n * a_1$	$a_n * a_2$	…	$a_n * a_n$

Определение 2. Полугруппой называется множество M с заданной на нем бинарной ассоциативной операцией: $\Pi =< M, * >$.

Единичный элемент *e*: $\forall a \in M \quad a * e = e * a = a$.

Единственность единичного элемента докажем от противного.

Пусть $\exists e$ и $e' \Rightarrow e' = e \cdot e' = e$.

Определение 3. Моноид — это полугруппа с единицей $< M,*,e >$.

Проверяем: 1) ассоциативность операции; 2) наличие единичного элемента.

Элемент $a \in M$ называется **обратимым**, если $\exists a^{-1} \in M$: $a * a^{-1} = a^{-1} * a = e$

(a – обратимый элемент, a^{-1} – **обратный элемент** к a).

Единственность обратного элемента докажем от противного

Пусть для $a \in M$

$$\exists a^{-1} \text{ и } \tilde{a}^{-1} \Rightarrow \tilde{a}^{-1} = e * \tilde{a}^{-1} = (a^{-1} * a) * \tilde{a}^{-1} = a^{-1} * (a * \tilde{a}^{-1}) = a^{-1} * e = a^{-1}.$$

Определение 4. Группа — это моноид, в котором каждый элемент обратим.

$$\mathrm{G} =< M,*,e >.$$

Если операция коммутативна, то соответственно полугруппа, моноид, группа называются **коммутативными или абелевыми**.

Полугруппа, моноид, группа называются **конечными порядка *p***, если они состоят из p элементов. Полугруппа, моноид, группа **бесконечного порядка**, если состоят из бесконечного числа элементов.

При проверке, какой структурой является множество с заданной бинарной операцией $< M,* >$ с начала необходимо убедиться, что задана бинарная операция (**замкнутость операции**). Затем ассоциативность операции, существование единичного элемента (принадлежность рассматриваемому множеству), существование обратных элементов.

Полугруппа	Моноид	Группа
1. Ассоциативность операции $*$		
	2. Существование единичного элемента: $\exists e \in M$	
		3. Существование обратного элемента: $\forall a \in M\ \exists a^{-1} \in M$

Определение 6. Подполугруппа – замкнутое относительно заданной бинарной операции подмножество Π'полугруппы Π: $\Pi' \subseteq \Pi$

$$\forall a, b \in \Pi' \Rightarrow a * b \in \Pi'.$$

Аналогично подмоноид и подгруппа

Определение 7. Подмоноид M' – замкнутое относительно заданной бинарной операции подмножество M' с единицей ($e \in M'$).

Определение 8. Подгруппа – замкнутое относительно заданной бинарной операции подмножество G', причем $e \in \mathrm{G}'$ и $\forall a \in \mathrm{G}' \Rightarrow a^{-1} \in \mathrm{G}'$.

При проверке того, что структура является подполугруппой, подмоноидом или подгруппой необходимо дополнительно проверить **замкнутость** бинарной операции, т.е. результат операции принадлежит множеству (в данном случае подмножеству).

Примеры 1 – 12.

1. $G =< \mathbb{Z}, +, 0 >$ – группа, $e = 0, \forall a \to a^{-1} = -a$. Подгруппа: <четные, +, 0> и числа кратные произвольному $k: < \{kz\}, +, 0 >$
2. Группы также: $< \mathbb{Q}, +, 0 >, < \mathbb{R}, +, 0 >, < \mathbb{C}, +, 0 >$ – комплексные числа.
3. $< \mathbb{Z}, \times, 1 >$ – моноид. Отсутствует обратный элемент, например к 2 – $\frac{1}{2}$. Подмоноид – натуральные числа. Кратные – не содержат 1.
4. Группы: $< \mathbb{Q}\backslash\{0\}, \times, 1 >, < \mathbb{R}\backslash\{0\}, \times, 1 >$.

   Матрицы
5. Матрицы $< \mathbb{R}^{m \times n}, +, 0 >, e = 0$ – нулевая матрица, $M^{-1} = -M$ – группа.
6. Квадратные матрицы $< M, \times, E >$ – некоммутативный моноид: для вырожденных матриц $(detA = 0) \Rightarrow \nexists A^{-1}$ обратной матрицы.

7. Квадратные матрицы $< M,\times, E >$ – некоммутативная группа, если $detA \neq 0 \Rightarrow \exists a^{-1}$. Замкнутость: $det(A \cdot B) = detA \cdot detB \neq 0$.

8. **Множество всех биекций множества X в себя**: $f(x): X \to X$. Операция – композиция: $\circ \Rightarrow < M,\circ, e_x >$ – некоммутативная группа. Существует обратная функция и тоже биекция.

$$\big(f(x) \circ g(x)\big) \circ h(x) = f(x) \circ \big(g(x) \circ h(x)\big)$$

$$f(x) \circ g(x) \neq g(x) \circ f(x)$$

9. **Свободная группа.** Элементы – слова из символов алфавита и обратных символов.

$$w_1 = a_1..a_\text{k}, \qquad w_2 = b_1 \dots b_m,$$

Операция $*$ – приписывание одного слова к другому (ассоциативная, но не коммутативная):

$$w_1 * w_2 = a_1 \dots a_k b_1 \dots b_m$$

$e = \Lambda$ – пустое слово.

$\forall a_i, b_i \qquad \exists a_i^{-1}, b_i^{-1}$. Тогда

$w_1^{-1} = (a_1 \dots a_k)^{-1} = a_k^{-1} \dots a_1^{-1} \Rightarrow w_1 * w_1^{-1} = w_1^{-1} * w_1 = \Lambda$. Покажем это.

$w_1 * w_1^{-1} = a_1 \dots (a_k * a_k^{-1}) \dots a_1^{-1} = a_1 \dots \Lambda \dots a_1^{-1} = \dots = a_1 * a_1^{-1} = \Lambda,$

для $w_1^{-1} * w_1$ аналогично.

10. Понятие **конечной группы** содержательно как само по себе, так и в связи с их ролью в алгебраической теории чисел, комбинаторике, теории кодирования, теории решеток, классификации многообразий, и т.д.

Порядок конечной группы равен числу элементов группы.

Конечную полугруппу, моноид, группу можно задать таблицей Кэли:

Пусть $M = \{a_1, a_2\}$ – два элемента:

$*$	a_1	a_2
a_1	a_1/a_2	a_1/a_2
a_2	a_1/a_2	a_1/a_2

Всего полугрупп из двух элементов 16.

Пусть единичный элемент принадлежит множеству M.

Положим $a_2 = e$. Тогда $a_2 \cdot a_2 \neq e$, т. к. $a_2 \neq e$ Аналогично $a_1 = e$

$*$	e	a_2
e	e	a_2
a_2	a_2	e/a_2

$*$	e	a_1
e	e	a_1
a_1	a_1	e/a_1

Всего моноидов из двух элементов 4.

Всего групп из двух элементов 2: $a_1 = e$ или $a_2 = e$.

$*$	$a_1 = e$	a_2
e	e	a_2
a_2	a_2	e

$*$	a_1	$a_2 = e$
a_1	e	a_1
e	a_1	e

Пример группы из четырех элементов. $M = \{a_1, a_2, a_3, a_4\}$. Не учитывая, какой элемент единичный, позже покажем, что таких групп две. В таблице пример одной из них.

$a_1 = e$.

$*$	e	a_2	a_3	a_4
e	e	a_2	a_3	a_4
a_2	a_2	a_3	a_4	e
a_3	a_3	a_4	e	a_2
a_4	a_4	e	a_2	a_3

$$e * a_i = a_i * e = a_i \qquad (a_1 = e)$$

$$a_2^{-1} = a_4 \qquad a_3 * a_3 = e \Rightarrow a_3^{-1} = a_3 \qquad a_4^{-1} = a_2$$

Легко показать, что в конечной группе в любой строке или столбце таблицы Кэли все элементы различны (самостоятельно, от противного).

11. Группа классов вычетов по модулю n: $x = y (\mathrm{mod}\, n)$. В каждом классе целые числа с одинаковым остатком от деления на n.

Для $n = 4 \Rightarrow$ 4 класса

$$C_0 = \{0; \pm 4; \pm 8; \dots\}$$

$$C_1 = \{1; 5; -3; 9; -7; \dots\}$$

$$C_2 = \{2; 6; -2; 10; -6; \dots\}$$

$$C_3 = \{3; 7; -1; 11; -5; \dots\}$$

Введем операцию сложение: $C_l + C_k = C_r, \quad r = (l + k)(\mathrm{mod}\, n)$

Построим таблицу Кэли для операции сложения. Получим группу.

+	C_0	C_1	C_2	C_3
C_0	C_0	C_1	C_2	C_3
C_1	C_1	C_2	C_3	C_0
C_2	C_2	C_3	C_0	C_1
C_3	C_3	C_0	C_1	C_2

$$\exists e = C_0 \quad C_1^{-1} = C_3 \qquad C_3^{-1} = C_1 \qquad C_2^{-1} = C_2$$

Построим таблицу Кэли для операции умножения. $C_e * C_k = C_r, \; r = (e * k)\mathrm{mod}n$

*	C_0	C_1	C_2	C_3
C_0	C_0	C_0	C_0	C_0
C_1	C_0	C_1	C_2	C_3
C_2	C_0	C_2	C_0	C_2
C_3	C_0	C_3	C_2	C_1

Получим моноид: $e = C_1 \qquad C_1^{-1} = C_1 \qquad \nexists\, C_2^{-1} \qquad C_3^{-1} = C_3$

12. Группа самосовмещений правильного n-угольника.

Группа состоит из поворотов и симметрий: $G =< M, \circ, \varphi_0 >$, где $M -$ множество вершин $n -$ угольника, $\circ -$ операция композиция, $\varphi_0 = e$ (поворот на 0°) – единичный элемент.

1. Повороты на $0, \frac{2\pi}{n}, \dots, \frac{2\pi(n-1)}{n}$. Для определенности, против часовой стрелки.

2. Симметрии (будем обозначать $-\psi$)

12.1. **Для треугольника** ($n = 3$) получим три поворота и три симметрии:

$$G_{\triangle} = \{\varphi_0, \varphi_1(\tfrac{2\pi}{3}), \varphi_2(\tfrac{4\pi}{3}), \psi_1, \psi_2, \psi_3\}$$

Симметрии относительно осей l_1, l_2, l_3.

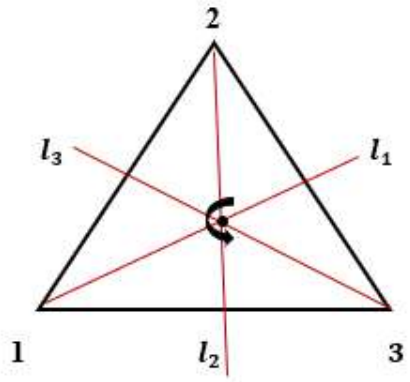


Таблица Кэли для группы $G_{\triangle}$.

$\circ$	φ_0	φ_1	φ_2	ψ_1	ψ_2	ψ_3
φ_0	φ_0	φ_1	φ_2	ψ_1	ψ_2	ψ_3
φ_1	φ_1	φ_2	φ_0	ψ_2	ψ_3	ψ_1
φ_2	φ_2	φ_0	φ_1	ψ_3	ψ_1	ψ_2
ψ_1	ψ_1	ψ_3	ψ_2	φ_0	φ_2	φ_1
ψ_2	ψ_2	ψ_1	ψ_3	φ_1	φ_0	φ_2
ψ_3	ψ_3	ψ_2	ψ_1	φ_2	φ_1	φ_0

$$e = \varphi_0, \quad \varphi_0^{-1} = \varphi_0, \quad \varphi_1^{-1} = \varphi_2, \quad \varphi_2^{-1} = \varphi_1, \quad \psi_i^{-1} = \psi_i, i = 1, \dots, 3$$

Пример нахождения элементов: $\varphi_1 \circ \psi_2 = \psi_3$ (сначала применяем симметрию ψ_2, затем поворот против часовой стрелки на угол $\frac{2\pi}{3}$):

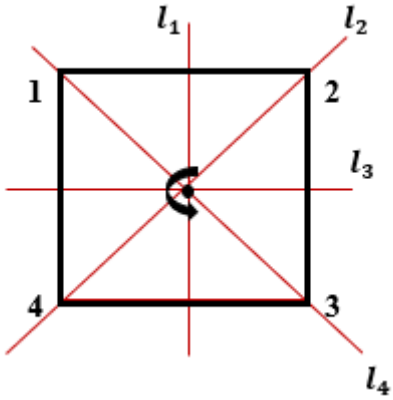
Группа некоммутативная: $\psi_2 \circ \varphi_1 = \psi_1$.

Подгруппы:

1. $H_1 = \{\varphi_0\}$
2. $H_2 = \{\varphi_0, \varphi_1, \varphi_2\} =< \varphi_1 >=< \varphi_2 > -$ группа вращений
3. $H_3 = \{\varphi_0, \psi_1\} =< \psi_1 >$
4. $H_4 = \{\varphi_0, \psi_2\} =< \psi_2 >$
5. $H_5 = \{\varphi_0, \psi_3\} =< \psi_3 >$
6. $H_6 = G_{\triangle}$

12.2. Группа самосовмещений квадрата

$G_{\square} = \{\varphi_0, \varphi_1(\frac{\pi}{2}), \varphi_2(\pi), \varphi_3(\frac{3\pi}{2}), \psi_1, \psi_2, \psi_3, \psi_4\}$



ψ_i соответствует оси l_i

Таблица Кэли

∘	φ_0	φ_1	φ_2	φ_3	ψ_1	ψ_2	ψ_3	ψ_4
φ_0	φ_0	φ_1	φ_2	φ_3	ψ_1	ψ_2	ψ_3	ψ_4
φ_1	φ_1	φ_2	φ_3	φ_0	ψ_4	ψ_1	ψ_2	ψ_3
φ_2	φ_2	φ_3	φ_0	φ_1	ψ_3	ψ_4	ψ_1	ψ_2
φ_3	φ_3	φ_0	φ_1	φ_2	ψ_2	ψ_3	ψ_4	ψ_1
ψ_1	ψ_1	ψ_2	ψ_3	ψ_4	φ_0	φ_1	φ_2	φ_3
ψ_2	ψ_2	ψ_3	ψ_4	ψ_1	φ_3	φ_0	φ_1	φ_2
ψ_3	ψ_3	ψ_4	ψ_1	ψ_2	φ_2	φ_3	φ_0	φ_1
ψ_4	ψ_4	ψ_1	ψ_2	φ_3	φ_1	φ_2	φ_3	φ_0

$e = \varphi_0,\ \varphi_0^{-1} = \varphi_0,\ \varphi_1^{-1} = \varphi_3,\ \varphi_2^{-1} = \varphi_2,\ \varphi_3^{-1} = \varphi_1,\ \psi_i^{-1} = \ \psi_i, i = 1, \dots, 4.$

Некоммутативная группа (убедиться самостоятельно).

Выделена группа вращений квадрата.

Подгруппы:

1. $H_1 = \{\varphi_0\}$
2. $H_2 = \{\varphi_0, \varphi_1, \varphi_2, \varphi_3\} =< \varphi_1 >=< \varphi_3 >$ – группа вращений квадрата.
3. $H_3 = \{\varphi_0, \varphi_2\} =< \varphi_2 >$
4. $H_4 = \{\varphi_0, \psi_1\} =< \psi_1 >$
5. $H_5 = \{\varphi_0, \psi_2\} =< \psi_2 >$
6. $H_6 = \{\varphi_0, \psi_3\} =< \psi_3 >$
7. $H_7 = \{\varphi_0, \varphi_2, \psi_1, \psi_3\}$
8. $H_8 = \{\varphi_0, \varphi_2, \psi_2, \psi_4\}$
9. $H_7 = G_{\square}$

Убедитесь, что при попытке построения любой другой подгруппы нарушится замкнутость операции.