Лекция 11

Алгебраические системы

Определение 1. Пусть A – непустое множество.

Отображение $f: A^n \to A$ (или $\underbrace{A \times A \times \cdots \times A}_{n} \to A$)

называется *n-арной* (*n-местной*) *алгебраической операцией* на множестве A.

Определение 2. ***Алгебраической системой*** называется набор $\mathbf{S} = \langle A, f_1, f_2, \ldots \rangle$, где A –непустое множество, f_k - алгебраические операции, заданные на A.

- **Пример 1**. $\mathbf{S} = \langle \mathbb{Z}, +, \cdot, - \rangle$, где $\mathbb{Z}$ - целые числа
- **Пример 2.** $\mathbf{S} = \langle F, +, * \rangle$, где F - функции R→R
- **Пример 3**. $\mathbf{S} = \left\langle 2^A, \cup, \cap, \setminus, \neg \right\rangle$, где $2^A -$ множество всех подмножеств множества A.
- **Пример 4**. $\mathbf{S} = \left\langle \mathbb{Q} \setminus \{0\}, : \right\rangle$, где $\mathbb{Q} -$ рациональные.
- **Контр-примеры**. $\langle \mathbb{Z}, : \rangle$, $\langle \mathbb{N}, - \rangle$, $\langle \mathbb{Q}, : \rangle$

Определение 3. Пусть $\mathbf{S} = \langle A, f \rangle$ алгебраическая

система, $B \subset A$, причём $f(B) \subseteq B$,

т.е. B - замкнуто относительно операции $\boldsymbol{f}$ **.**

Тогда $\mathbf{S}_1 = \langle B, f \rangle$ - ***подсистема*** системы $\mathbf{S}$.

Пример 1. $\langle \mathbb{N}, +, \cdot \rangle$ подсистема системы $\langle \mathbb{Z}, +, \cdot \rangle$

Пример 2. $\left\langle \boldsymbol{F}^{\nearrow}, +, \cdot \right\rangle$ подсистема системы $\langle \boldsymbol{F}, +, \cdot \rangle$

$\boldsymbol{F}$ - множество всех функций $\mathbb{R} \to \mathbb{R}$

$\boldsymbol{F}^{\nearrow}$ - множество возрастающих функций.

Среди множества алгебраических систем выделим и рассмотрим те, что представляют реальный интерес, а свойства операций – наиболее существенны:

- Переместительный закон – ***коммутативность***,
- Сочетательный закон – ***ассоциативность***,
- Распределительный закон – ***дистрибутивность***.

$$\left(A+B\right)-A=B$$

Рассмотрим далее наиболее важные системы:

группы, **кольца** и **поля**.

Элементы теории групп

Теория групп — раздел общей алгебры, изучающий алгебраические структуры и их свойства.

Теория групп находится на одном из самых высоких уровней абстракции.

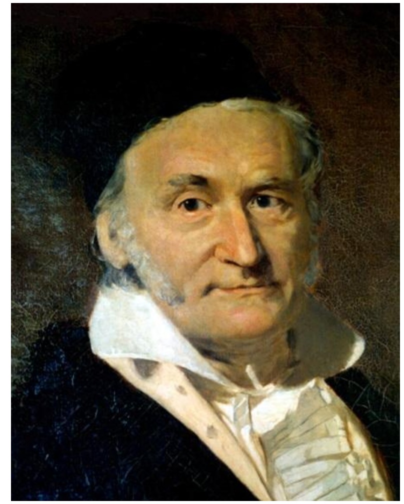
Группы возникают во всех областях математики, и методы теории групп оказывают сильное влияние на многие разделы математики.

В какой-то степени вся современная математика – это приложения теории групп.

Создатели теории групп

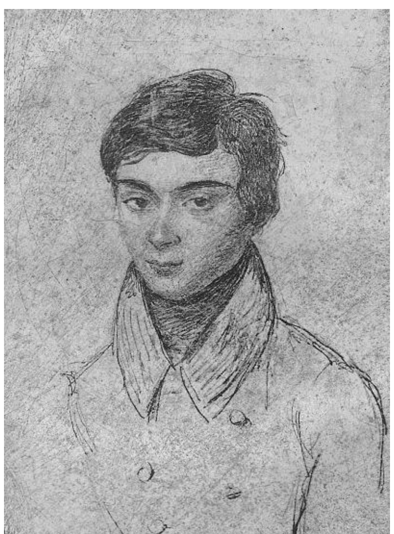
Леонард Эйлер

Ж.Л.Лагранж

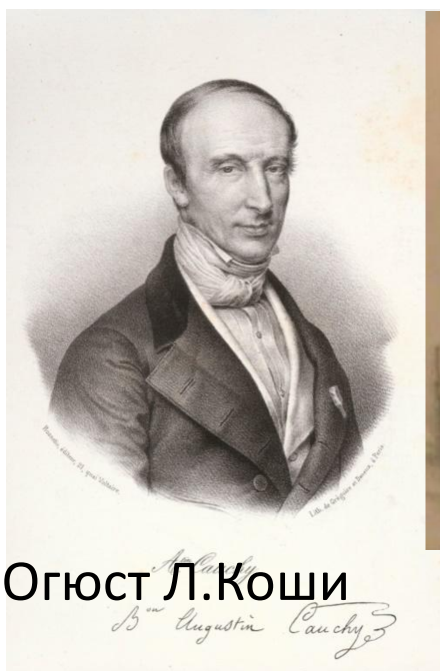


Карл Ф.Гаусс

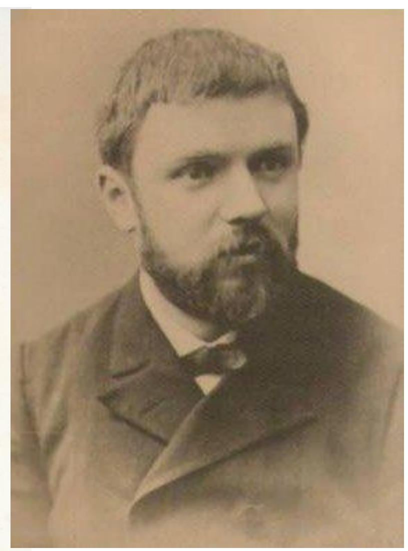
Нильс Г.Абель



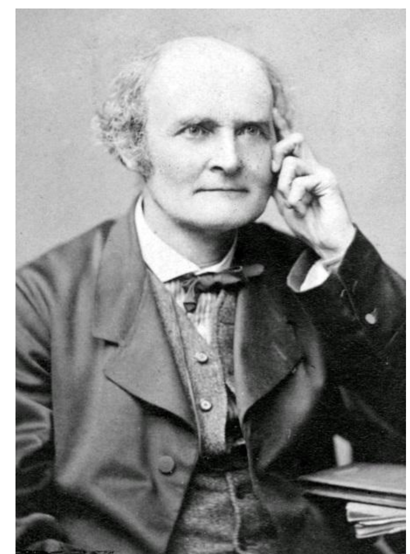
Эварист Галуа



Огюст Л.Коши



Анри Пуанкаре



Артур Кэли

Определение группы

Пусть имеется непустое множество G и определена бинарная операция $*$, замкнутая на этом множестве: $\forall a,b \in G \Rightarrow a*b = c \in G$

Множество G с операцией $*$ образует **группу**, если выполнены три условия (***аксиомы*** группы):

1) ассоциативность: $\forall a,b,c \in G \Rightarrow (a*b)*c = a*(b*c)$

2) существование **нейтрального** элемента e :

$$\exists e \in G \,|\, \forall a \in G \Rightarrow a*e = e*a = a$$

3) существование **обратного** элемента:

$$\forall a \in G \;\exists\, a^{-1} \in G \Rightarrow a*a^{-1} = a^{-1}*a = e$$

Терминология

Аддитивная группа (группа по сложению)	**Мультипликативная группа (группа по умножению)**
Операция $*$ - сложение	Операция $*$ - умножение
$a+b=c$	$a \cdot b=c$
Нейтральный элемент - <u>нуль</u>: $a+0=a$	Нейтральный элемент – <u>единица</u>: $a \cdot 1=a$
Обратный элемент – <u>противоположный</u>: $a+(-a)=0$	Обратный элемент – <u>обратный</u>: $a \cdot a^{-1}=1$
Обратное действие – **вычитание**	Обратное действие – **деление**

Еще несколько определений

- Если групповая операция коммутативна: $\boldsymbol{a} * \boldsymbol{b} = \boldsymbol{b} * \boldsymbol{a}$, то группа называется коммутативной или ***абелевой*** .
- ***Полугруппа*** – множество с замкнутой на нём ассоциативной бинарной операцией и нейтральным элементом. Обратная операция в полугруппе не всегда возможна.
- ***Подгруппа*** – подмножество группы, которое само является группой относительно той же операции.
- ***Циклическая*** группа – порожденная одним элементом.
- ***Изоморфизм*** групп – взаимно-однозначное соответствие (биекция) групп, сохраняющее операцию

$$\langle G,*\rangle \cong \langle H,\odot\rangle \quad \Leftrightarrow \quad f(u*v) = f(u)\odot f(v)$$

Примеры групп (1)

1. Множество целых чисел $\mathbf{Z}$ с операцией сложения «+»

2. Множество целых положительных чисел $\boldsymbol{Z}_+$ с операцией сложения по модулю $\boldsymbol{n}$.

3. Множество рациональных положительных чисел $\boldsymbol{Q}_+$ с операцией умножения.

4. Множество векторов в пространстве с операцией сложения векторов

5. Множество непрерывных монотонно возрастающих функций, заданных на отрезке $[0;1]$ с операцией композиции: $f(x) \circ g(x) = f\big(g(x)\big)$.

Примеры групп (2)

6. Множество подстановок (биекций) некоторого множества X . Групповая операция - композиция (последовательное выполнение).
7. Множество самосовмещений равностороннего треугольника. Операция - композиция.
8. Множество невырожденных квадратных матриц порядка n с операцией умножения матриц.
9. Множество слов в некотором алфавите с операцией приписывания одного слова в конец другому (конкатенация).
10. Множество целых степеней некоторого числа a относительно умножения.

Пример выполнения РГЗ

Выяснить, образует ли группу множество векторов пространства относительно операции векторного произведения векторов.

Решение.

Замкнутость операции очевидна: $\forall \overline{a}, \overline{b}\ \exists \overline{c} = \overline{a} \times \overline{b}$.

Аксиома 1 (ассоциативность) не выполняется. Например,

$\overline{i} \times \left(\overline{j} \times \overline{j} \right) = \overline{i} \times \overline{0} = \overline{0}$, но $\left(\overline{i} \times \overline{j} \right) \times \overline{j} = \overline{k} \times \overline{j} = -\overline{i}$.

Не выполняются также аксиомы 2 и 3, т.е. нет нейтрального элемента («вектора-единицы») и нет «обратного вектора».

Следовательно, множество векторов пространства с векторным произведением в качестве операции <u>**не** образует группу</u>.

Общие свойства групп

- Нейтральный элемент в группе – единственный.
- Для каждого элемента группы существует только один обратный элемент.
- Уравнения $\boldsymbol{a * x = b}$ и $\boldsymbol{x * a = b}$ всегда разрешимы в группе. Это утверждение равносильно аксиомам группы 2 и 3.
- $(a * b)^{-1} = b^{-1} * a^{-1}$

Конечные группы

- ***Порядок*** группы $\mathbf{G}$ – число элементов, $|G|$
- Групповая операция («умножение») может быть задана ***таблицей Кэли***.

  Например, для группы $G_4 = \{1, -1, i, -i\}$ с обычным умножением:

	1	-1	***i***	***-i***
1	1	-1	***i***	***-i***
-1	-1	1	***-i***	***i***
i	***i***	***-i***	-1	1
-i	***-i***	***i***	1	-1

Таблица Кэли всегда образует латинский квадрат.

Порождающий элемент ***i.***

Подгруппы: $\{1\}, \{1, -1\}$

Порядок элемента $\boldsymbol{g}$ конечной группы – минимальное натуральное число $\boldsymbol{m}$ такое, что $g^m = 1$.

Конечные группы

Теорема Лагранжа.

Порядок любой подгруппы конечной группы является делителем порядка группы.

Теорема Коши.

Любая группа, порядок которой делится на простое число ***p***, имеет элемент порядка ***p***.

Теорема Кэли.

Любая группа простого порядка (***p-группа***) – абелева и циклическая.

Теорема Фробениуса.

Все группы одного и того же простого порядка изоморфны друг другу.

- ***Симметрическая группа*** – группа всех ***автоморфизмов*** (биекций на себя) некоторого множества ***X***.

Если |X| = *n*, то она обозначается S_n и называется ***группой подстановок*** *n* элементов с операцией композиции. Порядок группы равен *n*!

Пример. Снежинка описывается группой симметрии D_6 . Она имеет 12 элементов: 6 поворотов и 6 видов осевой симметрии.

Каждая конечная группа G изоморфна некоторой подгруппе S(G).

Теорема о классификации простых конечных групп – наиболее значительный прорыв в математике XX века. Теорема (с доказательством) насчитывает более 10 тысяч печатных страниц и еще не закончена.

Методы и результаты теории групп с успехом используются во всех разделах математики, и кроме того, в физике, квантовой теории, единой теории поля, космологии, кристаллографии, химии, биологии, социологии, лингвистике, криптографии, стеганографии, архитектуре, теории музыки, и других.