

АЛГЕБРА

для потока «Прикладная математика и информатика»

*Четвёртый модуль 2020 – 2021 уч.
года*

ЛЕКЦИЯ

2

Г.М. Полотовский
(polotovsky@gmail.com)

14 апреля 2021

г.

Из истории появления понятия «группа»



**Жозеф Луи
Лагранж**
1736 – 1813

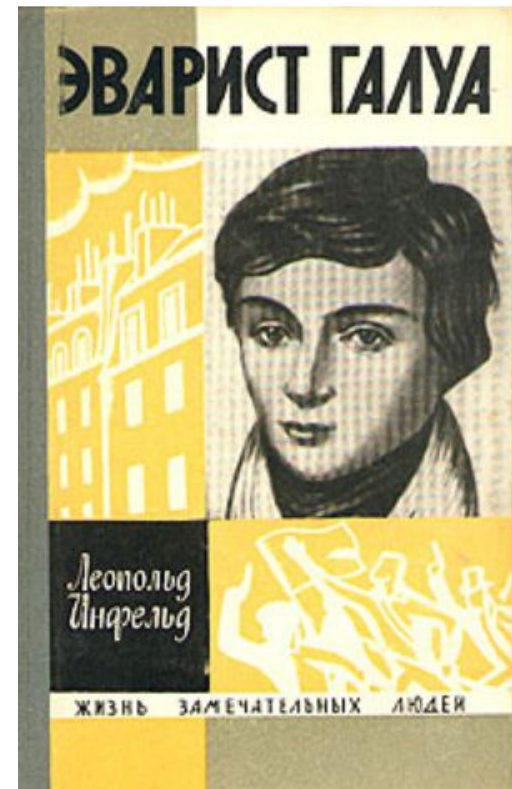
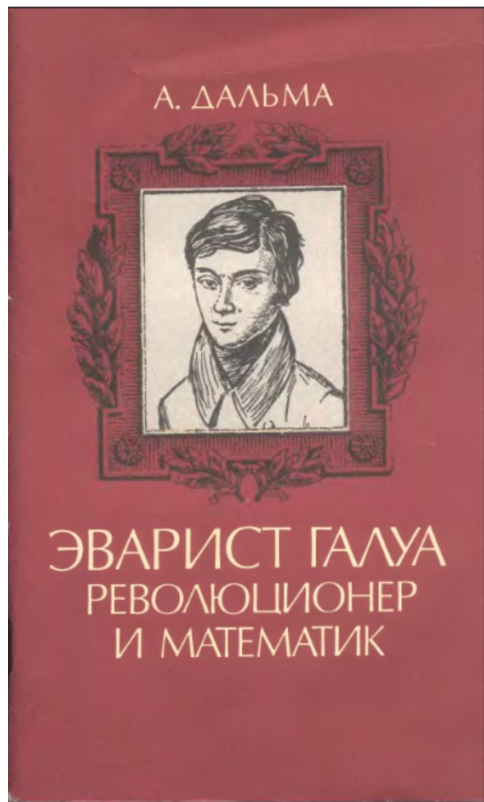
1771 г. – изучал группы
 S_n



Эварист Галуа в 15-летнем возрасте.
Карандашный портрет с натуры.

1811 – 1832

≈ 1831 – термин
«группа»



<https://www.rulit.me/author/dalma-a/evarist-galua-revolucioner-i-matematik-get-475922.html>

<http://pyrkov-professor.ru/default.aspx?tabid=190&ArticleId=764>

Группа
носки

о	О	Д	В	В _Д
О	О	Д	В	В _Д
Д	Д	О	В _Д	В
В	В	В _Д	О	Д
В _Д	В _Д	В	Д	О

$\cong$

Группа
симметрий



*	О	R _X	R _Y	R _O
О	О	R _X	R _Y	R _O
R _X	R _X	О	R _O	R _Y
R _Y	R _Y	R _O	О	R _X
R _O	R _O	R _Y	R _X	О

Группа
солдата

☆	С	П	Л	К
С	С	П	Л	К
П	П	К	С	Л
Л	Л	С	К	П
К	К	Л	П	С

$\cong$

Четверная группа Клейна
(1884)

Здесь “+” – сложение по модулю 4.

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\cong$

+	0	2	3	1
0	0	2	3	1
2	2	0	1	3
3	3	1	2	0
1	1	3	0	3

$\cong$

+	0	3	1	2
0	0	3	1	2
3	3	2	0	1
1	1	0	2	3
2	2	1	3	0

$\mathbb{Z}_4$

$\mathbb{Z}_4$

$\mathbb{Z}_4$

Определение 4. (Изоморфизм групп). Группы $(G, *)$ и $(H, \circ)$ называются *изоморфными*, если

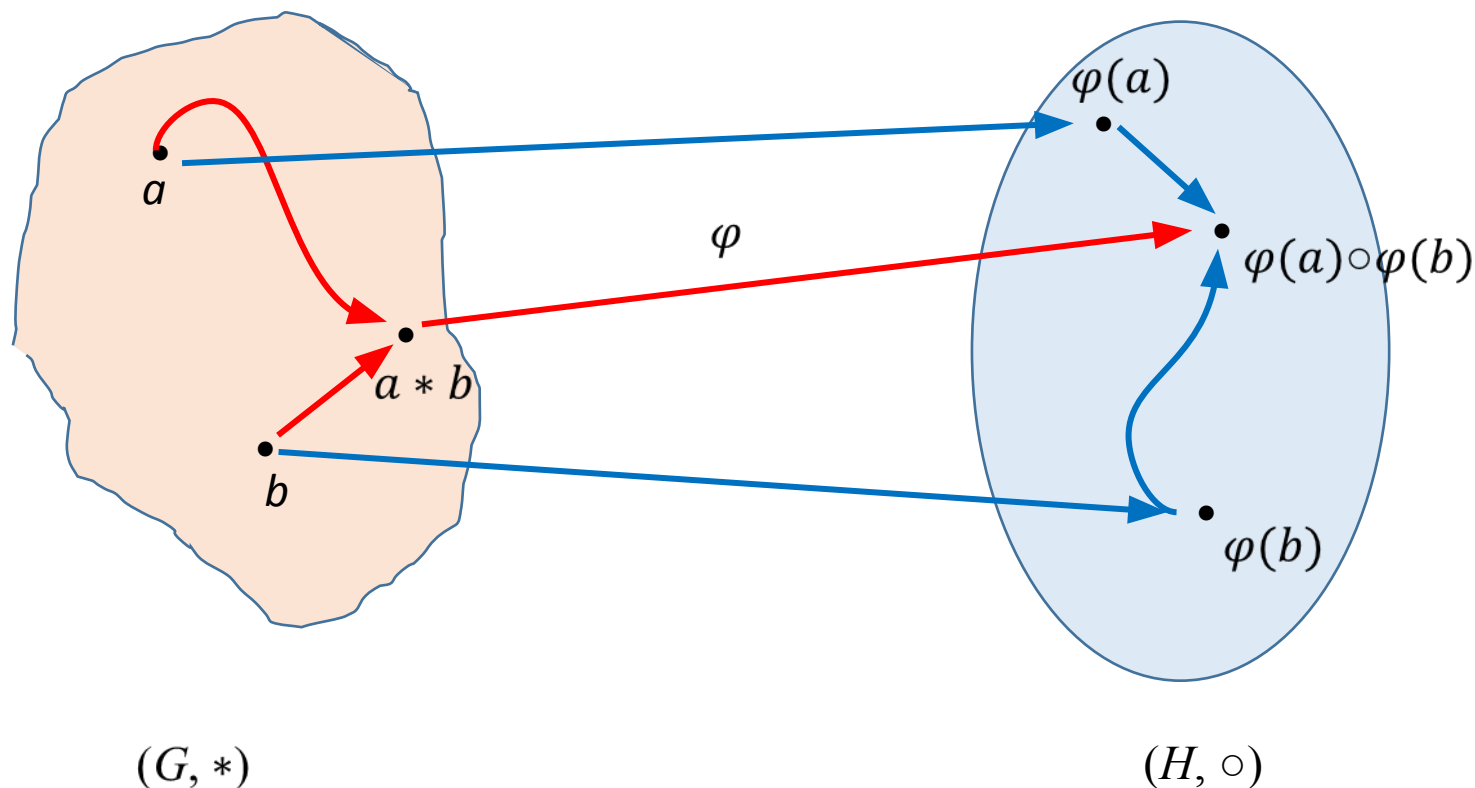
1) существует взаимно однозначное отображение

$$\varphi: G \rightarrow H;$$

2) отображение φ сохраняет операцию, т. е.

$$\varphi(a * b) = \varphi(a) \circ \varphi(b) \quad \forall a, b \in G.$$

При этом само отображение φ называется *изоморфизмом групп* $(G, *)$ и $(H, \circ)$.



Теорема 2.1. Пусть $(G, *) \cong (H, \circ)$ и $\varphi: G \rightarrow H$ изоморфизм. Тогда

1) $\varphi(e_G) = e_H$;

2) $\varphi(a^{-1}) = (\varphi(a))^{-1} \quad \forall a \in G.$

Доказательство.

1) $\varphi(a) = \varphi(a * e_G) = \varphi(a) \circ \varphi(e_G) \quad \forall a \in G \implies \varphi(e_G) = e_H$

2) $\varphi(e_G) = \varphi(a * a^{-1}) = \varphi(a) \circ \varphi(a^{-1}) \implies \varphi(a) \circ \varphi(a^{-1}) = e_H.$
 $\varphi(e_G) = e_H$

Замечание о классификации конечных групп

порядок	число групп ^[4]	коммутативных	некоммутативных
0	0	0	0
1	1	1	0
2	1	1	0
3	1	1	0
4	2	2	0
5	1	1	0
6	2	1	1
7	1	1	0
8	5	3	2
9	2	2	0
10	2	1	1
11	1	1	0
12	5	2	3
13	1	1	0
14	2	1	1
15	1	1	0

16	14	5	9
17	1	1	0
18	5	2	3
19	1	1	0
20	5	2	3
21	2	1	1
22	2	1	1
23	1	1	0
24	15	3	12
25	2	2	0
26	2	1	1
27	5	3	2
28	4	2	2
29	1	1	0
30	4	1	3

Замечание о классификации конечных групп

Теорема классификации утверждает, что список конечных *простых* групп состоит из 18 счётных бесконечных семейств, плюс 26 исключительных = *спорадических* групп.



Большой монстр =
группа Фишера – Гриса
(1981)

порядок

$$2^{41} \cdot 3^{40} \cdot 5^9 \cdot 7^6 \cdot 11^2 \cdot 13^3 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71 = 808\,017\,424\,794\,512\,875\,886\,459\,904\,961\,710\,757\,005\,754\,368\,000\,000\,000.$$



Бэби-монстр (начало 1970-х) имеет

$$2^{41} \cdot 3^{13} \cdot 5^6 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 31 \cdot 47 = 4154781481226426191177580544000000$$

Определение 5. Пусть $(G, *)$ – группа и $H \subset G$. H называется *подгруппой* группы G , если H является группой относительно той же операции $*$.

Замечание: пусть G группа, e – её нейтральный элемент. Тогда $\{e\}$ и G являются подгруппами группы G .

Из определения 5 непосредственно следует, что $e_G \in H$ и e_G является нейтральным элементом в H (поскольку нейтральный в группе единственный) и что H замкнуто относительно операции $*$ и взятия обратного элемента.

Однако проверку перечисленных условий можно заменить проверкой одного условия:

Теорема 2.2 (критерий подгруппы).

H подгруппа группы $G \iff \forall a, b \in H \quad ab^{-1} \in H$.

Замечание: в аддитивной записи последнее условие имеет вид $a - b \in H$.

Доказательство.

→ Очевидно, поскольку по условию H – группа.

← Положим $b = a$. Тогда $ab^{-1} = aa^{-1} = e_G \in H$.

Пусть $d \in H$. Положим в условии $a = e, b = d$, тогда $ab^{-1} = ed^{-1} = d^{-1} \in H$.

Пусть $c, d \in H$. Тогда $d^{-1} \in H$. Положим в условии $a = c, b = d^{-1}$, тогда $ab^{-1} = c(d^{-1})^{-1} = cd \in H$.

(Докажите самостоятельно, что $(d^{-1})^{-1} = d$.)

Примеры.

1) Множество всех четных чисел является подгруппой в $(\mathbb{Z}, +)$.

2) Множество $SL_n(\mathbb{R})$ является подгруппой в $GL_n(\mathbb{R})$.

3) Множество A_n четных подстановок является подгруппой в S_n .

Из критерия подгруппы легко следует утверждение, которое Вам предлагается для **самостоятельного доказательства**:

Если $\{H_i\}_{i \in I}$ некоторое семейство подгрупп группы G , то $H = \bigcap_{i \in I} H_i$ также

является подгруппой в G , т.е. пересечение любого количества подгрупп будет подгруппой.

Определение 6. Пусть $g \in G$, $n \in \mathbb{Z}$. Введем понятие n -ой степени элемента G :

Если $n > 0$, то $g^n = \underbrace{gg \cdots g}_{n \text{ раз}}$. Если $n = 0$, то $g^n = e$. Если $n < 0$, то $g^n = \underbrace{g^{-1}g^{-1} \cdots g^{-1}}_{-n \text{ раз}}$.

Замечание: в аддитивной записи определение 6 превращается в определение кратного:

Если $n > 0$, то $ng = \underbrace{g + g + \cdots + g}_{n \text{ раз}}$. Если $n = 0$, то $ng = 0$.

Если $n < 0$, то $ng = \underbrace{(-g) + (-g) + \cdots + (-g)}_{-n \text{ раз}}$.

Теорема 2.3. Пусть G – группа. Тогда $\forall m, n \in \mathbb{Z}, g \in G$ имеет место $g^m g^n = g^{m+n}$; $(g^m)^n = g^{mn}$, в частности, $(g^m)^{-1} = (g^{-1})^m = g^{-m}$.

Доказательство легко вытекает из определения степени и из обобщённой ассоциативности.

Теорема 2.4. Если G – коммутативная группа, то $(ab)^n = a^n b^n$.

Теорема 2.5. Пусть G – группа, $g \in G$. Множество $\langle g \rangle = \{g^n \mid n \in \mathbb{Z}\}$ всех степеней элемента g является подгруппой в G .

Это утверждение непосредственно следует из определения 6 и теоремы 2.3.

Определение 7. Подгруппа $\langle g \rangle$ называется *циклической подгруппой*, порождённой элементом g , а элемент g – *порождающим элементом* подгруппы $\langle g \rangle$.

Замечания: в аддитивной записи $\langle g \rangle = \{ng \mid n \in \mathbb{Z}\}$; образующий элемент циклической подгруппы, вообще говоря, может быть выбран не единственным способом.

Примеры.

1. $G = \mathbf{C} \setminus \{0\}$ относительно операции умножения комплексных чисел.

$i^0 = 1, i^1 = i, i^2 = -1, i^3 = -i, i^4 = 1; \langle i \rangle = \{1, i, -1, -i\}$ – подгруппа порядка 4.

$$2. \quad GL_2(R) = \left\{ \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \middle| a_{ij} \in R, \begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} \neq 0 \right\}.$$

Пусть $A = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$, тогда $\langle A \rangle = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \right\}$, поскольку

$$A^2 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = E.$$

Таким образом, циклическая группа, порождённая матрицей A , имеет порядок 2.

$$\text{Если } A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \text{ то } A^2 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix};$$

$$A^3 = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 3 \\ 0 & 1 \end{pmatrix}; \dots; A^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}.$$

Таким образом, теперь подгруппа, порождённая матрицей A , имеет бесконечный порядок.

Пусть G – произвольная группа, $g \in G$. Рассмотрим циклическую подгруппу, порожденную элементом g . Возможны следующие два случая:

- 1). Все степени элемента g различны между собой. Тогда группа $\langle g \rangle$ бесконечна и не существует такого целого ненулевого числа n , что $g^n = e$.
- 2). Существуют различные $s < t$, такие что $g^s = g^t$. Умножим это равенство на g^{-s} , получим $g^{t-s} = e$. Следовательно, существует такое целое положительное число n , что $g^n = e$. Среди таких чисел n можно выбрать наименьшее.

Определение *Порядком элемента* g называется наименьшее целое положительное число n , такое что $g^n = e$. Обозначение: $\text{ord } g = n$. Если такого числа не существует, то говорят, что g имеет бесконечный порядок.

Примеры.

1) $G = \mathbb{Z}$, $\text{ord } 0 = 1$, порядки остальных элементов G бесконечны, так как если кратное $nm = 0$ при $n \neq 0$, то $m = 0$.