

# Черновик семинаров по алгебре.

Н. К. Животовский

nikita.zhivotovskiy@phystech.edu

5 марта 2015 г.

Материал находится в стадии разработки, может содержать ошибки и неточности. Автор будет благодарен за любые замечания и предложения, направленные по указанному адресу

## 1 Первый семинар

**Опр. 1.1.** Множество  $M$  с заданной на нем бинарной операцией  $*$  называется *группой*  $G = \langle M, * \rangle$ , если выполнены следующие аксиомы:

1. ассоциативность:  $\forall a, b, c: (a * b) * c = a * (b * c)$ .
2. существует единственный единичный элемент  $e$ , такой что  $e * x = x * e = x$ .
3. для любого элемента  $x$  существует ровно один обратный элемент  $y$ , то есть элемент, для которого  $x * y = y * x = e$ .

**Замечание 1.1.** Оба условия единственности являются избыточными.

Если для пары множество–бинарная операция выполнено только первое условие, то говорят о *полугруппе*, а в случае выполнения первых двух — о *мономе*.

Группа называется *абелевой* или *коммутативной*, если для всех элементов  $a, b$  имеет место  $a * b = b * a$ .

Примеры групп:

1.  $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$  с операцией сложения являются абелевыми группами.
2.  $\mathbb{Q} - \{0\}, \mathbb{R} - \{0\}, \mathbb{C} - \{0\}$  с операцией умножения, однако  $\mathbb{Z} - \{0\}$  не является группой по умножению.
3. Прямое произведение групп — тоже группа.
4. Линейное пространство — тоже группа по сложению.

**Упр. 1.1.** Пусть  $G$  — группа, докажите, что

1. Единичный элемент единственный.
2. Для каждого элемента группы существует единственный обратный элемент.
3. Для любых элементов  $a$  и  $b$  имеет место  $(a * b)^{-1} = (b^{-1} * a^{-1})$ .
4.  $(a^{-1})^{-1} = a$ .

5. Имеет место обобщенное ассоциативное правило.
6. Уравнения  $ax = b$  и  $ya = b$  имеют единственное решение.

Группа  $G$ , в которой множество  $M$  конечно, называется *конечной группой*, а количество элементов в нем — ее *порядком*.

*Порядок* элемента  $a$  группы  $G$  — это наименьшее натуральное число  $n$  такое, что  $x^n = e$ . Если такого  $n$  не существует, то говорят, что  $a$  имеет бесконечный порядок.

- Упр. 1.2.**
1. Элемент имеет порядок один тогда и только тогда, когда он единичный.
  2. В аддитивных группах  $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$  каждый не единичный элемент имеет бесконечный порядок.
  3. В мультипликативных группах  $\mathbb{Q} - \{0\}, \mathbb{R} - \{0\}$  элемент  $-1$  имеет порядок 2. Остальные элементы имеют бесконечный порядок.
  4.  $(a^{-1})^{-1} = a$ .
  5. Имеет место обобщенное ассоциативное правило.
  6. Уравнения  $ax = b$  и  $ya = b$  имеют единственное решение.

**Упр. 1.3.** Могут ли у конечной группы быть элементы бесконечного порядка?

Зафиксируем некоторое подмножество  $H$  элементов группы  $G$ . Если оно вместе с бинарной операцией группы  $G$  образует группу, то группа  $H$  называется *подгруппой группы  $G$* . Обозначение  $H < G$ .

**Теорема 1.1 (Критерий Подгруппы).**  $H \subseteq G$  является подгруппой группы  $G$  тогда и только тогда, когда

1.  $H \neq \emptyset$
2. для любых двух элементов  $a$  и  $b$  имеет место включение  $ab^{-1} \in H$ .

При этом, если  $H$  конечна, то достаточно проверить лишь замкнутость относительно умножения.

**Теорема 1.2 (Теорема Лагранжа).** Порядок подгруппы конечной группы делит ее порядок.

Сравнения по модулю. Запись  $a \equiv b \pmod{n}$  означает, что числа  $a$  и  $b$  дают один и тот же остаток при делении на число  $n$ . В таком случае говорят, что  $a$  и  $b$  сравнимы по модулю  $n$ . Эквивалентная формулировка  $a - b = kn$  для некоторого целого  $k$ .

Сравнение по модулю обладает свойствами:

1. *рефлексивности*  $a \equiv a \pmod{n}$ .
2. *симметричности*  $a \equiv b \pmod{n}$  влечет  $b \equiv a \pmod{n}$ .
3. *транзитивности*  $a \equiv b \pmod{n}$  и  $b \equiv c \pmod{n}$  влечет  $a \equiv c \pmod{n}$ .

Данное отношение разбивает все  $\mathbb{Z}$  на классы.

**Упр. 1.4.** Найдите два последних знака числа  $2^{1000}$ .

Важнейшие для нас понятия для целых чисел — деление с остатком и определение наибольшего общего делителя.

*Алгоритм Евклида.* Пусть нужно найти НОД( $a, b$ ). Поделим  $a$  на  $b$  получим в остатке число  $r_1$ . Теперь поделим  $b$  на  $r_1$  получим число  $r_2$ . И так далее, последний ненулевой остаток будет наибольшим общим делителем. Следствием данного алгоритма является лемма Безу.

## 2 Второй семинар

Множество классов, на которые  $\mathbb{Z}$  разбивается с помощью отношения сравнения по модулю  $n$  называется называются классами вычетов. Обозначение  $\mathbb{Z}/n\mathbb{Z}$ . Легко определить сложение и умножение на классах. Обозначение класса и его про

**Упр. 2.1.** Доказать, что классы вычетов по сложению образуют абелеву группу.

**Упр. 2.2.** Доказать, что множество обратимых элементов  $\mathbb{Z}/n\mathbb{Z}$  (обозначение  $(\mathbb{Z}/n\mathbb{Z})^\times$ ) образует группу по умножению и состоит из тех классов, представители которых состоят из элементов взаимно простых с  $n$ .

Функция  $\varphi : \mathbb{N} \rightarrow \mathbb{Z}_+$  ставящее в соответствие каждому  $n$  число натуральных чисел, меньших  $n$  и взаимно простых с ним, называется функцией Эйлера.

**Утв. 2.1.** Порядок группы  $(\mathbb{Z}/n\mathbb{Z})^\times$  равен  $\varphi(n)$ .

**Теорема 2.2 (теорема Эйлера).** Для взаимно простых  $a$  и  $n$ .

$$a^{\varphi(n)} \equiv 1 \pmod{n}$$

**Доказательство.**

Рассмотрим группу  $(\mathbb{Z}/n\mathbb{Z})^\times$ , ее порядок равен  $\varphi(n)$ , а порядок любого элемента в конечной группе делит порядок группы. Следовательно, любой элемент  $(\mathbb{Z}/n\mathbb{Z})^\times$  в степени  $\varphi(n)$  является единичным. Осталось вспомнить структуру  $(\mathbb{Z}/n\mathbb{Z})^\times$ . ■

Очевидным следствием является Малая теорема Ферма

**Теорема 2.3 (малая теорема Ферма).** Для  $a \neq 0$ , для простых  $p$

$$a^p \equiv a \pmod{p}$$

**Утв. 2.4.** Пусть  $p$  — простое число. Порядок группы  $(\mathbb{Z}/p\mathbb{Z})^\times$  равен  $p-1$  и состоит из всех классов  $\mathbb{Z}/p\mathbb{Z}$ , кроме класса нуля.

**Упр. 2.3.** Решить уравнение  $21x \equiv 13 \pmod{34}$ .

Достаточно показать, что класс 21 обратим в группе  $\mathbb{Z}_{34}^\times$ . Это действительно так, потому что числа 34 и 21 взаимно просты. Осталось найти, обратный к 21 элемент. Из теоремы Эйлера таким элементом будет класс  $21^{\varphi(34)-1}$ . Осталось найти  $21^{15} \pmod{34}$ . Оказывается, что  $21^2 \equiv -1 \pmod{34}$ . В результате решение  $x \equiv 13^2 \pmod{34}$ , то есть,  $x \equiv 33 \pmod{34}$

Группа называется циклической, если все ее элементы являются степенями какого-то одного элемента. Циклические группы из  $n$  элементов обозначаются  $C_n$ .

Легко понять, что циклическая группа, у которой никакие степени не совпадают естественным образом отождествляется с аддитивной группой  $\mathbb{Z}$ . Также легко показать, что если порождающий элемент  $a$  имеет порядок  $n$ , то есть минимальное натуральное число, при возведении в которое  $a$  получается единичный элемент, то все элементы группы представляются перечисляются  $e, a, a^2, \dots, a^{n-1}$ .

**Теорема 2.5.** *Всякая подгруппа циклической группы циклическая.*

**Упр. 2.4.** Выяснить какие подгруппы есть у  $\mathbb{Z}$ .

**Утв. 2.6.** Пусть  $G$  порождена элементом  $a$ . Тогда,

- если  $G$  – бесконечная, то она может быть порождена только  $a$  или  $a^{-1}$
- если  $G$  конечная и имеет порядок  $n$ , то она порождена всеми элементами  $a^k$  такими, что  $a^k$  взаимно просто с  $n$  и только ими.

**Доказательство.**

Доказательство первого факта очевидно. Доказательство второго факта заключается в наблюдении того, что степени порождающих элементов сами по себе образуют циклическую группу. Причем ее порядок равен порядку данного элемента. Таким образом, для порождения необходимо и достаточно, чтобы порядок элемента  $a^k$  равнялся  $n$ . Для этого докажем, что  $a^k$  в конечной циклической группе имеет порядок  $n/(n, k)$ . Пусть  $(n, k) = d$ , тогда  $n = db, k = dc$  и  $(b, c) = 1$ . Докажем, что  $(a^k)^b = e$ . Действительно,

$$(a^k)^b = a^{kb} = a^{dcb} = e.$$

Таким образом, порядок элемента  $a^k$  делит  $b$ . Пусть он равен  $s$ , тогда  $b = st$  и  $a^{ks} = e$ . Таким образом  $n|ks$  или  $db|dcs$ , а из взаимной простоты получаем, что  $b|s$ . Таким образом, порядок действительно равен  $n/(n, k)$ . ■

Элемент  $a \in (\mathbb{Z}/p\mathbb{Z})^\times$  называется квадратичным вычетом, если существует класс, такой, что  $b^2 = a$ .

**Утв. 2.7.** Всего существует  $\frac{p-1}{2}$  квадратичных вычетов по модулю  $p$ .

**Доказательство.**

Запишем все элементы в виде  $\{-\frac{p-1}{2}, -\frac{p+1}{2}, \dots, \frac{p-1}{2}, \frac{p+1}{2}\}$ . Очевидно, что квадраты противоположенных по знакам классов совпадают. Одновременно, для разных по модулю выражений результаты не совпадают. ■

**Упр. 2.5.** Вспомнить, что такое группа подстановок (перестановок), разложение в циклы, четность и нечетность подстановок и их свойства.

**Упр. 2.6.** Доказать, что в  $S_8$  нет элементов порядка 56.

### 3 Третий семинар

**Упр. 3.1.** Контрольная на 30 минут.

**Опр. 3.1.** Гомоморфизм — это отображение  $\varphi$  групп  $\langle G, * \rangle \rightarrow \langle H, \times \rangle$ , которое сохраняет групповую операцию:

$$\varphi(x * y) = \varphi(x) \times \varphi(y), \forall x, y \in G.$$

**Опр. 3.2.** Взаимоднозначный гомоморфизм — изоморфизм.

**Упр. 3.2.** Изоморфны ли

- $(\mathbb{R}, +)$  и  $(\mathbb{R}_+, \times)$  (Да, с помощью отображения  $x \rightarrow \exp(x)$ .)
- $(\mathbb{R}, +)$  и  $(\mathbb{Q}, +)$  (Нет, так как целые и действительные числа не равномощны.)
- $S_3$  и  $\mathbb{Z}/6\mathbb{Z}$  (Нет, так как одна абелева, а другая нет.)
- $(\mathbb{Z}, +)$  и  $(\mathbb{Q}, +)$  (от противного: пусть  $\varphi(1) = a$ , тогда  $\varphi(1/2) = b$ , но  $b + b = a$ , значит  $a = 2b$ . Продолжаем так же для  $1/4$  пока не придем к нечетному образу.)

**Упр. 3.3.** Для каких групп отображение в себя, заданное  $x \rightarrow x^{-1}$ , является гомоморфизмом. (Очевидно, что для Абелевых и только для них)

Гомоморфизмы произвольных абелевых групп  $G, H$  сами образуют абелеву группу гомоморфизмов, которую мы будем обозначать  $\text{НОМ}(G, H)$ . Единичным элементом является гомоморфизм, переводящий все элементы в единичный, а сложение гомоморфизмов определено  $\varphi_1 + \varphi_2 : x \rightarrow \varphi_1(x) + \varphi_2(x)$ .

**Упр. 3.4.** Бесконечная циклическая группа изоморфна  $(\mathbb{Z}, +)$ , а конечная изоморфна  $\mathbb{Z}/n\mathbb{Z}$ , где  $n$  — порядок порождающего элемента.

**Опр. 3.3.** Автоморфизм — изоморфизм, отображающий группу на себя.

**Упр. 3.5.** Доказать, что в любой группе элементы  $x$  и  $y^{-1}xy$  имеют один и тот же порядок.

Решение состоит в понимании того, что  $x \rightarrow y^{-1}xy$  является автоморфизмом (так называемый *внутренний автоморфизм*). И автоморфизм сохраняет порядки элементов.

**Упр. 3.6.** Изоморфны ли  $C_8 \times C_2$  и  $C_4 \times C_4$ .

Не изоморфны так как в первой группе есть элемент порядка 8, а во второй такого нет.

**Упр. 3.7.** Опишите все гомоморфизмы групп  $\mathbb{Z}/8\mathbb{Z}$  в  $\mathbb{Z}/6\mathbb{Z}$ .

$\mathbb{Z}/8\mathbb{Z}$  циклическая группа. Гомоморфный образ циклической группы — циклическая группа. Ясно, что гомоморфизм в этом случае определяется образом единицы, то есть элементом  $\varphi(1)$ . Также ясно, что порядок  $\varphi(1)$  делит порядок  $1 \in \mathbb{Z}/8\mathbb{Z}$  и одновременно он должен делить 6 так как является элементом  $\mathbb{Z}/6\mathbb{Z}$ . Таким образом, порядок  $\varphi(1)$  может быть равен 1 или 2. Таким образом всего два гомоморфизма  $\varphi(1) = 0$  и  $\varphi(1) = 3$ .

**Упр. 3.8.** Может ли гомоморфизм  $C_{36}$  в  $C_{20}$  обладать тем свойством, что образ порождающего элемента первой группы переходит в квадрат порождающего элемента второй группы?

Переходим к рассмотрению  $\mathbb{Z}/36\mathbb{Z}$  и  $\mathbb{Z}/20\mathbb{Z}$  и получаем противоречие с порядком образа, так как 36 не делится на 5.

**Упр. 3.9.** Доказать, что группа автоморфизмов циклической группы абелева. Найти порядок группы автоморфизмов циклической группы порядка 12. Является ли эта группа циклической?

Абелевость следует из общего утверждения, заключающегося в том, что множество гомоморфизмов абелевой группы образуют группу по сложению. Далее понимаем, что при автоморфизме порождающий элемент должен переходить в порождающий.

**Упр. 3.10.** Сколько подгрупп, изоморфных  $C_4$ , содержится в  $C_{12} \times C_{18}$ ?

**Утв. 3.1 (теорема Кэли).** Всякая группа порядка  $n$  изоморфна некоторой подгруппе симметрической группы  $S_n$ .

Рассмотрим для каждого элемента  $a$  операцию  $L_a : x \rightarrow ax$ . Легко доказать, что она переставляет элементы группы. Таким образом, каждому элементу сопоставляется некоторая перестановка. Теперь нужно построить изоморфизм между группой и различными  $L_a$ , введя на них групповую операцию очевидным образом.

## 4 Четвертый семинар

Пусть  $G$  некоторая группа, а  $H$  – ее подгруппа. Для элемента  $x \in G$  введем множество  $xH = \{xh | h \in H\}$ . Оно называется *левым смежным классом*. Аналогично правым смежным классом назовем  $Hg$ .

**Утв. 4.1 (теорема о смежных классах).** Смежные классы  $xH$  и  $yH$  либо не пересекаются, либо совпадают.

Количество смежных классов группы  $G$  по подгруппе  $H$  называется *индексом подгруппы* и обозначается  $(G : H)$ .

**Утв. 4.2 (повторение теоремы Лагранжа).** Пусть  $H$  – подгруппа группы  $G$ . Тогда

$$|G| = (G : H) \times |H|$$

**Упр. 4.1.** Вспомните определение нормальной подгруппы.

Обозначим  $G/H$  – совокупность смежных классов  $G$  по  $H$ . В некотором смысле обозначение соответствует тому, что мы разбили группу на смежные классы. Оказывается, что если группа  $H$  нормальная, то  $G/H$  является группой с операцией  $(xH) \times (yH) = (xyH)$ .

**Упр. 4.2.** Докажите, что  $\mathbb{Z}/n\mathbb{Z}$  изоморфна фактор группе  $\mathbb{Z}$  по подгруппе  $n\mathbb{Z}$ .

**Упр. 4.3.** Докажите, что  $(G \times H)/(G \times \{e\})$  изоморфна  $H$ .

Рассмотрим гомоморфизм  $\varphi(g, h) = (e, h)$ . Рассмотрим

Центром группы  $G$  называется множество ее элементов  $Z(G)$ , которые коммутируют со всеми ее элементами.

**Упр. 4.4.** Докажите, что центр – нормальная подгруппа.

Доказывается очевидным образом с помощью критерия подгруппы и того, что группы сопряженные с центром совпадают с ним.

**Упр. 4.5.** Пусть  $G$  некоторая группа. И пусть фактор группа  $G/Z(G)$  — циклическая. Тогда  $G$  является Абелевой группой.

Так как  $G/Z(G)$  циклическая, то ее элементы порождаются  $wZ(G)$  для некоторого  $w \in G$ . Пусть  $a, b \in G$ . Так как группа циклическая, то  $aZ(G) = w^n Z(G)$  и  $bZ(G) = w^m Z(G)$  для некоторых  $m, n$ . Отсюда следует, что  $a = w^n z_1$  и  $b = w^m z_2$  для некоторых  $z_1, z_2 \in Z(G)$ . Теперь убеждаемся, что  $ab = ba$ .

**Упр. 4.6.** Группа  $G$  порядка  $pq$  для простых  $p$  и  $q$  либо Абелева, либо имеет тривиальный центр.

Если центр нетривиальная собственная подгруппа, то она по теореме Лагранжа может иметь порядок  $p$  или  $q$ . Пусть для определенности он равен  $p$ , тогда  $(G : Z(G)) = q$ . Тогда как и любая группа простого порядка  $G/Z(G)$  циклическая, а значит согласно предыдущему пункту  $G$  — Абелева. Получаем противоречие.

Напомним, что элемент  $b$  сопряжен с  $a$  посредством  $g$  с элементом  $a$ , если  $b = gag^{-1}$ . Отношение сопряженности разбивает группу на непересекающиеся классы. Очевидно, что элементы центра группы и только они образуют одноэлементные классы сопряженности. Если  $n_1, \dots, n_r$  размеры нетривиальных классов сопряженности, то  $|G| = |Z(G)| + n_1 + n_2 + \dots + n_r$ .

**Упр. 4.7.** Нормализатор  $N(a)$  — множество всех элементов группы  $G$ , коммутирующих с  $a$ . Доказать, что размер класса сопряженности элемента  $a$  равен  $(G : N(a))$ .

Рассмотрим фактор множество  $G/N(a)$  и рассмотрим отображение  $\varphi : G/N(a) \rightarrow G$ , который отображает смежный класс  $gN(a)$  в  $gag^{-1}$ . Очевидно, что оно инъективный. Действительно,  $gN(a) = g_1N(a)$  тогда и только тогда, когда  $gg_1^{-1} \in N(a)$ , то есть коммутирует с  $a$ , а значит при этом  $gag^{-1} = g_1ag_1^{-1}$ . Если  $gN(a) \neq g_1N(a)$ , то и  $gag^{-1} \neq g_1ag_1^{-1}$ . Осталось понять, что образом этого отображения будут все сопряженные с  $a$  элементы и воспользоваться тем, что индекс делит порядок группы.

**Упр. 4.8.** Группа называется  $p$ -группой, если ее порядок является степенью простого числа. Доказать, что центр  $p$  группы нетривиален.

Для группы порядка  $p$  утверждение тривиально. Также утверждение тривиально для любой Абелевой группы. Теперь достаточно показать, что  $G/Z(G)$  состоит из нетривиальных классов. Пусть  $g_1, \dots, g_n$  различные элементы  $G$ , таких что классы сопряженных  $G$  содержат ровно по одному такому элементу. Пусть с каждым элементом  $g_i$  сопряжены  $n_i$ . Тогда  $|G| = |Z(G)| + n_1 + n_2 + \dots + n_r$ . Так как  $n_i$  делит порядок группы и отлично от единицы, то каждое  $n_i$  делится на  $p$ . Из последнего уравнения получается, что  $|Z(G)| \neq 1$ .

**Упр. 4.9.** Доказать, что группа порядка  $p^2$  — Абелева, где  $p$  простое число.

Только что мы показали, что центр  $p$ -группы нетривиален, а значит она Абелева, как группа порядка  $pq$ .

**Упр. 4.10.** Доказать, что нормальная подгруппа индекса  $k$  содержит все элементы, порядки которых взаимно просты с  $k$ .

Действием группы  $G$  на множестве  $X$  называется гомоморфизм  $\varphi : G \rightarrow S(X)$ , где  $S(X)$  — группа биекций  $X$ . Формальное обозначение  $g(x)$ ,  $x \in X$ .