Лекция 3

Лемма 1. *Пусть g – элемент группы G такой, что* $\mathrm{ord}g = n$, *а m – целое число. Тогда*

$$\mathrm{ord}g^m = \frac{n}{НОД(m,n)} = \frac{НОК(m,n)}{m}.$$

Доказательство. Докажем это утверждение только для положительных m, так как $\mathrm{ord}(g^{-m}) = \mathrm{ord}((g^m)^{-1}) = \mathrm{ord}(g^m)$, а также $\mathrm{ord}(g^0) = e$.

Рассмотрим группу $\langle g\rangle$. По предыдущей лемме она изоморфна $\mathbb{Z}_n$. Более того при построенном изоморфизме этих групп элемент g соответствует $1 \in \mathbb{Z}_n$, и элемент g^m соответствует $m \in \mathbb{Z}_n$. Таким образом, нам нужно доказать, что порядок $m \in \mathbb{Z}_n$ равен $\frac{n}{\mathrm{НОД}(m,n)} = \frac{\mathrm{НОК}(m,n)}{m}$. Порядок – это такая минимальная натуральная степень k, в которой элемент равен e. В аддитивных обозначениях получаем $\mathrm{ord}(m) = k$, если k – это минимальное натуральное число такое, что $mk = 0$ в $\mathbb{Z}_n$. Для целых чисел условие перепишется как mk делится на n. Получается, что mk – общее кратное m и n. Таким образом, $k \geq \frac{\mathrm{НОК}(m,n)}{m}$.С другой стороны $k = \frac{\mathrm{НОК}(m,n)}{m}$ подходит, так как $mk = \frac{\mathrm{НОК}(m,n)}{m}m = \mathrm{НОК}(m,n)$ делится на n. □

Теорема 1. *1) Подгруппа циклической группы циклическая;*
2) Все подгруппы $\mathbb{Z}$ имеют вид $\langle k\rangle = k\mathbb{Z} \cong \mathbb{Z}$;
3) Все подгруппы $\mathbb{Z}_n$ имеют вид $\langle d\rangle = d\mathbb{Z}_n \cong \mathbb{Z}_{\frac{n}{d}}$ для некоторого d – делителя n;
4) Пусть $m \in \mathbb{Z}_n$. Тогда $\langle m\rangle = \langle НОД(m,n)\rangle$.

Доказательство. 1) Следует из пунктов 2) и 3).

2) Пусть H – подгруппа в $\mathbb{Z}$. Если $H = \{0\}$, то $H = \langle 0\rangle$, что укладывается в утверждение задачи. Пусть $H \neq \{0\}$. Если $h \in H$ – отрицательное число, то положительное число $-h$ также лежит в H. Значит, в H есть натуральные числа. Выберем k – минимальное натуральное число из H. Пусть $h \in H$. Тогда $h = kq + r$, где $0 \leq r < k$. При этом $kq \in H$, $h \in H$, следовательно, $r \in H$. Если $r \neq 0$, получаем противоречие с выбором k. Значит, $r = 0$ и h делится на k. Отсюда $H = \langle k\rangle$.

3) Пусть H – подгруппа в $\mathbb{Z}_n$. Если $H = \{0\}$, то $H = \langle n\rangle$, что укладывается в утверждение задачи. Пусть $H \neq \{0\}$. Рассмотрим минимальное натуральное число d такое, что его класс лежит в H. Ясно, что $d < n$. Пусть $h \in H$. Тогда $h = dq + r$, где $0 \leq r < d$. При этом $dq \in H$, $h \in H$, следовательно, $r \in H$. Если $r \neq 0$, получаем противоречие с выбором d. Значит, $r = 0$ и h делится на d. Отсюда $H = \langle d\rangle$. Докажем, что d – делитель n. Если это не так, то $n = kd + s$, $0 < s < d$. Но тогда в $\mathbb{Z}_n$ выполнено $s = kd \in H$, противоречие с выбором d. Итак, d – делитель n. Осталось сказать, что порядок d в группе $\mathbb{Z}_n$ равен $\frac{n}{d}$. Значит, $H = \langle d\rangle \cong \mathbb{Z}_{\frac{n}{d}}$.

4) $\langle m\rangle$ – циклическая группа. По лемме 1, $\mathrm{ord}(m) = \frac{n}{\mathrm{НОД}(m,n)}$. Значит $|\langle m\rangle| = \frac{n}{\mathrm{НОД}(m,n)}$. Следовательно, по пункту 3), $\langle m\rangle = \langle \mathrm{НОД}(m,n)\rangle$. □

Особый интерес представляют гомоморфизмы и изоморфизмы из группы в себя.

Определение 1. Гомоморфизм $\varphi\colon G \to G$ называется *эндоморфизмом*. Изомомрфизм $\varphi\colon G \to G$ называется *автоморфизмом*.

Легко видеть, что композиция двух эндоморфизмов – это эндоморфизм, а композиция двух автоморфизмов – автоморфизм. Множество эндоморфизмов группы G с операцией композиции образует моноид $\mathrm{End}(G)$ с нейтральным элементом id. Множество автоморфизмов группы G с операцией композиции образует группу $\mathrm{Aut}(G)$.

Пусть g – элемент группы G. Рассмотрим отображение $\varphi_g\colon G \to G$, определенное по правилу $\varphi_g(h) = ghg^{-1}$.

Лемма 2. *Отображение φ_g является автоморфизмом группы G.*

Доказательство. Проверим, что φ_g – гомоморфизм:

$$\varphi_g(hf) = ghfg^{-1} = ghg^{-1}gfg^{-1} = \varphi_g(h)\varphi_g(f).$$

То, что φ_g – биекция следует из того, что существует обратное отображение. А именно, обратное к φ_g отображение – это $\varphi_{g^{-1}}$. □

Автоморфизм называются *внутренним*, если он имеет вид φ_g для некоторого $g \in G$.

Предложение 1. *Множество внутренних автоморфизмов с операцией композиции образует подгруппу* $\mathrm{Inn}(G)$ *в* $\mathrm{Aut}(G)$.

Доказательство. Докажем равенство $\varphi_g \circ \varphi_h = \varphi_{gh}$. Для этого применим этот гомоморфизм к элементу $s \in G$:

$$\varphi_g \circ \varphi_h(s) = \varphi_g(\varphi_h(s)) = \varphi_g(hsh^{-1}) = ghsh^{-1}g^{-1} = (gh)s(gh)^{-1} = \varphi_{gh}(s).$$

Из доказанного равенства следует замкнутость $\mathrm{Inn}(G)$ относительно композиции. Кроме того $\mathrm{id} = \varphi_e \in \mathrm{Inn}(G)$. Осталось проверить, что $\mathrm{Inn}(G)$ замкнуто относительно взятия обратного. Для этого заметим, что $\varphi_g \circ \varphi_{g^{-1}} = \varphi_e = \mathrm{id}$. □

Теорема 2. *1)* $\mathrm{Aut}(\mathbb{Z}) \cong \mathbb{Z}_2$,
2) $\mathrm{Aut}(\mathbb{Z}_n) \cong \mathbb{Z}_n^\times$.

Замечание 1. Напомним, что $\mathbb{Z}_n^\times$ – это группа обратимых по умножению элементов кольца вычетов $\mathbb{Z}_n$. Группа $\mathbb{Z}_n^\times$ состоит из вычетов взаимно простых с n. В частности, $|\mathbb{Z}_n^\times| = \varphi(n)$, где $\varphi(\cdot)$ – функция Эйлера.

Доказательство теоремы **??**. 1) Пусть ψ – автоморфизм $\mathbb{Z}$. Тогда $\psi(0) = 0$. Пусть $\psi(1) = k$. Тогда

$$\psi(2) = \psi(1+1) = \psi(1) + \psi(1) = 2k,$$
$$\psi(3) = \psi(1+1+1) = \psi(1) + \psi(1) + \psi(1) = 3k,$$

и т.д. Аналогично $\psi(-1) = -k$, $\psi(-2) = \psi((-1)+(-1)) = -2k$. Получаем

$$\psi(m) = mk.$$

Однако при $k \neq \pm 1$ гомоморфизм ψ не будет сюръективен. При $k = 1$ и $k = -1$ получаем тождественное отображение и отображение $\{x \mapsto -x\}$. Легко видеть, что эти два автоморфизма с операцией композиции образуют группу, изоморфную $\mathbb{Z}_2$.

2) Аналогично случаю 1 любой гомоморфизм $\psi\colon \mathbb{Z}_n \to \mathbb{Z}_n$ имеет вид

$$\psi_k\colon m \mapsto km.$$

Если k не обратим, то в образе ψ_k не лежит 1, а значит, ψ_k не сюръективно. Если же k обратим, то для любого вычета l имеем $\psi_k(k^{-1}l) = l$. Следовательно, ψ_k сюръективно, а значит, так как множество $\mathbb{Z}_n$ конечно, гомоморфизм ψ_k – биекция.

Итак, $\mathrm{Aut}(\mathbb{Z}_n)$ состоит из ψ_k для $k \in \mathbb{Z}_n^\times$. Докажем, что отображение

$$\zeta\colon \mathrm{Aut}(\mathbb{Z}_n) \to \mathbb{Z}_n^\times, \qquad \zeta(\psi_k) = k$$

является изоморфизмом. Это очевидно биекция, осталось проверить, что ζ – гомоморфизм. Это следует из равенства $\psi_k \circ \psi_m = \psi_{km}$, которое легко проверить. □

Определение 2. Пусть H – подгруппа группы G. Рассмотрим элемент $g \in G$. *Левым смежным классом элемента g по подгруппе H* называется множество

$$gH = \{gh \mid h \in H\}.$$

Правым смежным классом элемента g по подгруппе H называется множество

$$Hg = \{hg \mid h \in H\}.$$

Лемма 3. *1) $g \in fH$ тогда и только тогда, когда $f^{-1}g \in H$,*

1') $g \in Hf$ тогда и только тогда, когда $gf^{-1} \in H$,

2) Левые (правые) смежные классы – это классы эквивалентности. (Более точно, отношение $g \sim f$, если $g \in fH$ является отношением эквивалентности.)

3) Следующие мощности одинаковы $|gH| = |Hg| = |H|$.

Доказательство. 1) $g \in fH \iff g = fh \iff f^{-1}g = h$.

1') $g \in Hf \iff g = hf \iff gf^{-1} = h$.

2) Докажем только для левых смежных классов. Для правых аналогично.

Рефлексивность: $g \in gH$ так как $e \in H$,

Симметричность:

$$g \in fH \iff f^{-1}g \in H \iff (f^{-1}g)^{-1} = g^{-1}f \in H \iff f \in gH.$$

Транзитивность:

$$g \in fH, f \in sH \Longrightarrow f^{-1}g \in H, s^{-1}f \in H \Longrightarrow s^{-1}ff^{-1}g = s^{-1}g \in H.$$

3) Следует из того, что $gh_1 = gh_2$ тогда и только тогда, когда $h_1 = h_2$. □

Замечание 2. Из пункта 2 следует, что левые (правые) смежные классы либо не пересекаются, либо совпадают.

Определение 3. Индекс подгруппы H группы G – это мощность множества левых смежных классов. Обозначается индекс $[G : H]$

Задача 1. Докажите, что $gH \leftrightarrow Hg^{-1}$ – биекция между левыми и правыми смежными классами, и следовательно мощность правых смежных классов также равна индексу подгруппы. (То, что количество левых и правых смежных классов одинаково для конечной группы будет следовать из теоремы Лагранжа, но это верно и для бесконечных групп.)

Теорема 3. *(Лагранж) Пусть G – конечная группа и H – подгруппа G. Тогда*

$$|G| = |H| \cdot [G : H].$$

Доказательство. Поскольку каждый элемент группы G лежит в некотором левом смежном классе и левые смежные классы либо совпадают, либо не пересекаются, вся группа G разбивается на непересекающиеся левые смежные классы. Так как мощность каждого смежного класса равна $|H|$, мощность всей группы равна $|H|$ умножить на количество смежных классов. □

Следствие 1. *(Следствия из теоремы Лагранжа)*

1) Порядок конечной группы делится на порядок ее подгруппы.

2) Порядок конечной группы делится на порядок ее элемента.

3) Для любого элемента g конечной группы G выполнено $g^{|G|} = e$.

4) Группа простого порядка циклическая.

5) (Теорема Эйлера) Пусть m и n – взаимно простые натуральные числа. Тогда $n^{\varphi(m)}$ имеет остаток 1 при делении на m.

Доказательство. 1) Очевидно следует из теоремы Лагранжа.

2) Пусть g – элемент конечной группы G. Рассмотрим циклическую подгруппу $H = \langle g \rangle$. Поскольку $\mathrm{ord}(g) = |H|$, порядок G делится на $\mathrm{ord}(g)$.

3) Пусть $|G| = \mathrm{ord}(g) \cdot k$. Тогда $g^{|G|} = (g^{\mathrm{ord}(g)})^k = e^k = e$.

4) Пусть $|G| = p$ – простое число. Рассмотрим $g \neq e \in G$. Поскольку порядок g делит p и не равен 1, получаем $\mathrm{ord}(g) = p$. А значит, $G = \langle g \rangle$.

5) Применим пункт 3 к группе $\mathbb{Z}_m^\times$ и ее элементу n. Получаем

$$n^{|\mathbb{Z}_m^\times|} = n^{\varphi(m)} = 1.$$

□