Георгий Потошин, 2024

Алгебра I, листочек 1

1. **Докажите, что всякая циклическая группа изоморфна $\mathbb{Z}/n\mathbb{Z}$ для некоторого $n \geq 0$.**

   Пусть $g \in G$ порождает G, положим $n = \text{ord}(g)$. Тогда построим гомоморфизм $\varphi : g^a \mapsto [a]_n$, $\varphi(g^a * g^b) = [a+b]_n = [a]_n + [b]_n$. Он инъективен $\varphi^{-1}(0) = \{g^a | [a]_n = [0]_n\} = 1$. То, что он сюръективен тоже очевидно, так как мы можем возводить g в любую степень. Изоморфизм построен.

2. **Какие подгруппы у циклической группы?**

   Мы будем рассматривать далее $G = \mathbb{Z}/n\mathbb{Z}$, $n \in \mathbb{N}_0$. Пусть $H \leq G$, введем на G стандартный линейный порядок. Тогда пусть $d = \min H \setminus \{0\}$. Очевидно, что $\langle d \rangle \leq H$. Пусть $a \in H \setminus \langle d \rangle$, тогда $a = kd + r$, $r < d$ и $r \in H$, противоречие, а значит $\langle d \rangle = H$. Тогда все подгруппы циклической группы циклические. Причем для $n \neq 0$, легко построить группу порядка $d|n$ - $\langle n/d \rangle$, а для $n = 0$, $\langle a \rangle = a\mathbb{Z}$.

3. (a) **Почти группа без ассоциативности:**

e	a	b	c
a	b	e	b
b	e	b	c
c	a	c	e

   В этой алгебре есть единица, есть единственный обратный, но операция не ассоциативна $(ab)c = ec = c$, но $a(bc) = ac = b$.

   (b) **Почти группа без 1 и обратных (полугруппа)** $(\mathbb{N}, +)$

   (c) **Почти группа без обратных (моноид)** $(\mathbb{N}_0, +)$

4. **Симметрические группы порядка $n \geq 3$ неабелевы.**

   Элементы симметрических групп здесь и далее я буду комбинировать слева направо, а действовать элементами справа. S_3 неабелева, так как $(2,3)(2,1) = (1,2,3)$, а $(2,1)(3,2) = (3,2,1)$, дальше легко проделать вложение, если оставить запись циклами $S_3 \hookrightarrow S_n$, $a \mapsto a$, так что S_n тоже неабелева.

5. **Докажите, что для ассоциативной операции все расстановки скобок в $g_1 \cdot \ldots \cdot g_n$ дают один и тот же результат.**

   Индукция по длине.

   База: $n = 1, 2, 3$ очевидно

   Шаг: Пусть $V = (g_1 \cdot \ldots) \cdot (g_k \cdot \ldots g_n)$ некая расстановка скобок. Всегда будет последнее умножение, оно перемножает два выражения меньшей длинны, для которых расстановка скобок не играет роли по предположению индукции, тогда ориентируем умножения в левой скобке влево, а в правой вправо и применим ассоциативность некоторое количество раз рекурсивно, переориентируя скобки в одну сторону:

   $$\begin{aligned} V &= (((g_1 g_2) \ldots g_k)(g_{k+1}(g_{k+2} \ldots g_n))) \\ &= ((((g_1 g_2) \ldots g_k) g_{k+1})(g_{k+2} \ldots g_n)) \\ &= \cdots \\ &= (((g_1 g_2) g_3) \ldots g_n) \end{aligned}$$

   В итоге любую ориентацию скобок можно свести к левой, а значит все они равны.

6. **Пусть G – группа, и пусть для любого ее элемента g выполнено $g^2 = e$. Докажите, что G абелева. Верно ли, что G абелева, если для любого элемента $g \in G$ выполнено $g^3 = e$?**

   Если G – группа инвлюций, то $(ab)(ba) = e = (ab)^2$, а значит $ab = ba$.

   Если у нетривиальных элементов группы порядок равен трём, то она вообще говоря не абелева, так как есть группа вращений правильной треугольной пирамиды. Она по очевидным соображениям не абелева, но все её нетривиальные вращения имеют порядок 3.

7. **Опишите все автоморфизмы и все подгруппы в следующих группах: $\mathbb{Z}, \mathbb{Z}/n\mathbb{Z}, S_3, S_4$.**

- $\mathrm{Aut}(\mathbb{Z})$. Пусть n порождает $\mathbb{Z}$, тогда очевидно, $\langle n \rangle = n\mathbb{Z}$. А значит, $n = \pm 1$. Заметим, что порождающий должен переходить в порождающий, иначе гомоморфизм не сюръективен. А значит есть всего два автоморфизма. $1 \mapsto 1$ и $1 \mapsto -1$.
- $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$. Пусть g порождает $\mathbb{Z}/n\mathbb{Z}$ это эквивалентно тому, что $lg = kn + 1$, некоторая степень g равна 1. Это эквивалентно тому, что $g \wedge n = 1$. Тогда $(\varphi_m(1) = m) \wedge n = 1$ будут всеми автоморфизмами группы. Причем они комбинируются по следующему закону $(\varphi_n \circ \varphi_m : 1 \mapsto m \mapsto nm) = \varphi_{nm}$. А значит группа автоморфизмов изоморфна мультипликативной группе соответствующего кольца.
- $\mathrm{Aut}(S_3)$. Перечислим нетривиальные элементы группы: $i_1 = (3,2)$, $i_2 = (1,3)$, $i_3 = (1,2)$ – инволюции, $t_1 = (1,2,3)$, $t_2 = (3,2,1)$ - 3-циклы. Очевидно, что при автоморфизме инволюции переходят в инволюции, а трициклы в трициклы. По этому свойству можно провести классификацию.

	e	i_1	i_2	i_3	t_1	t_2
e	e	i_1	i_2	i_3	t_1	t_2
i_1	i_1	e	t_2	t_1	i_3	i_2
i_2	i_2	t_1	e	t_2	i_1	i_3
i_3	i_3	t_2	t_1	e	i_2	i_1
t_1	t_1	i_2	i_3	i_1	t_2	e
t_2	t_2	i_3	i_1	i_2	e	t_1

Перечислим нетривиальные автоморфизмы для которых t_1 и t_2 неподвижные точки:

$$t_1 \mapsto t_1, \quad t_2 \mapsto t_2, \quad i_1 \mapsto i_2$$
$$i_2 = i_1 t_2 \mapsto i_2 t_2 = i_3, \quad i_3 \mapsto i_1$$

Это отображение совпадет с сопряжением по t_2, так как:

$$\begin{aligned} S_{t_2} : \quad & t_1 \mapsto t_2 t_1 t_2^{-1} = t_2^{-1} = t_1 \\ & t_2 \mapsto t_2 \\ & i_1 \mapsto t_2 i_1 t_2^{-1} = i_3 t_1 = i_2 \\ & i_2 \mapsto t_2 i_2 t_1 = i_1 t_1 = i_3 \\ & t_3 \mapsto i_1 \end{aligned}$$

$$t_1 \mapsto t_1, \quad t_2 \mapsto t_2$$
$$i_1 \mapsto i_3, \quad i_2 \mapsto i_1, \quad i_3 \mapsto i_2$$

Это отображение совпадет с сопряжением по t_1, так как:

$$\begin{aligned} S_{t_1} : \quad & t_1 \mapsto t_1 \\ & t_2 \mapsto t_2 \\ & i_1 \mapsto t_1 i_1 t_2 = i_2 t_2 = i_3 \\ & i_2 \mapsto t_1 i_2 t_2 = i_3 t_2 = i_1 \\ & t_3 \mapsto i_2 \end{aligned}$$

Теперь меняем t_1 и t_2 местами.

$$t_1 \mapsto t_2, \quad t_2 \mapsto t_1, \quad i_1 \mapsto i_1$$
$$i_2 = i_1 t_2 \mapsto i_1 t_1 = i_3, \quad i_3 \mapsto i_2$$

Это отображение совпадет с сопряжением по i_1, так как:

$$\begin{aligned} S_{t_2}: \quad & t_1 \mapsto i_1 t_1 i_1 = i_3 i_1 = t_2 \\ & t_2 \mapsto t_1 \\ & i_1 \mapsto i_1 i_1 i_1 = i_1 \\ & i_2 \mapsto i_1 i_2 t_1 = t_2 i_1 = i_3 \\ & t_3 \mapsto i_2 \end{aligned}$$

$$\begin{aligned} & t_1 \mapsto t_2, \quad t_2 \mapsto t_1, \quad i_1 \mapsto i_2 \\ & i_2 \mapsto i_1, \quad i_3 \mapsto i_3 \end{aligned}$$

Это отображение совпадет с сопряжением по i_3, так как:

$$\begin{aligned} S_{t_2}: \quad & t_1 \mapsto i_3 t_1 i_3 = i_2 i_3 = t_2 \\ & t_2 \mapsto t_1 \\ & i_1 \mapsto i_3 i_1 i_3 = t_2 i_1 = i_2 \\ & i_2 \mapsto i_1 \\ & t_3 \mapsto i_3 \end{aligned}$$

$$\begin{aligned} & t_1 \mapsto t_2, \quad t_2 \mapsto t_1, \quad i_1 \mapsto i_3 \\ & i_2 \mapsto i_2, \quad i_3 \mapsto i_1 \end{aligned}$$

Это отображение совпадет с сопряжением по i_2, так как:

$$\begin{aligned} S_{t_2}: \quad & t_1 \mapsto i_2 t_1 i_2 = i_1 i_2 = t_2 \\ & t_2 \mapsto t_1 \\ & i_1 \mapsto i_2 i_1 i_2 = t_1 i_2 = i_3 \\ & i_2 \mapsto i_2 \\ & t_3 \mapsto i_1 \end{aligned}$$

Так как каждое отображение совпало с сопряжением, то они автоморфизмы. Больше автоморфизмов по построению нет. $S_{\cdot}: \ \mathrm{Aut}(S_3) \leftrightarrow S_3$

- $\mathrm{Aut}(S_4)$. Покажем, что группа S_4 совершенна, то есть, что все её автоморфизмы на самом деле сопряжение. В S_4 6 транспозиций и ещё 3 инволюции, которые $(2,2)$-циклы. Очевидно, что инволюции должны отправляться в инволюции. Если транспозицию применить к (3)-циклу, то может произойти 2 вещи $(abc)(ab) = (cb)$ или $(abc)(cd) = (abdc)$, мы получим или элемент порядка 2 или порядка 3. Если $(2,2)$-цикл применить к (3)-циклу, то $(abc)(ab)(cd) = (bdc)$ мы получим элемент порядка 3. Так что транспозиции не могут быть отправлены в $(2,2)$-циклы, а только в транспозиции, за неимением других инволюций.

  Теперь проверим, что если транспозиции отправляются в транспозиции, то это сопряжение. Пусть автоморфизм отправляет $(ab) \mapsto (a'b')$. Тогда если $(cb) \mapsto (c'b'')$, $c \neq a$ то раз (ab) и (cb) не коммутируют, то не коммутируют и $(a'b')$ и $(c'b'')$, а значит с точностью до перестановок c' и b'' либо $b'' = a'$, либо $b'' = b'$, зафиксируем второе. Пусть теперь $a \neq d \neq c$, тогда $(db) \mapsto (d'b''')$, так как прообраз не коммутировал с (ab) и (cb), то и образ тоже не будет. Тогда $(d'b''')$ совпадет с $(a'b')$ и $(c'b')$ ровно по 1 букве. А значит будет либо $b' \in \{d', b'''\}$ и мы положим $b''' = b'$, либо $\{c', a'\} = \{d', b'''\}$, но в этом случае $(c'a')(a'b')(c'b') = (a'b')$, а комбинация их прообразов $(db)(ab)(cb) = (dacb)$, так что второй случай не возможен. Из этого мы заключаем, что во всех остальных транспозициях с b все их образы содержат b'. Такое соответствие задаст перестановку, так как оно инъективно, потому как для случая ≥ 4 для b и d можно найти коммутирующие транспозиции (ab) и (cd), их образы не будут пересекаться по действию, а значит $b' \neq d'$ Назовём эту перестановку g. Тогда построим автоморфизм S по ней.

$$\begin{array}{ccc} S_n & \xrightarrow{\cdot h} & S_n \\ {\scriptstyle \cdot g}\downarrow & & \downarrow{\scriptstyle \cdot g} \\ S_n & \xrightarrow{\cdot (h)S} & S_n \end{array}$$

То есть, если нужно понять куда перейдет a под действием $(h)S$, $(h)S = (..ab..)$ и $h = (..a'b'..)$, где $a'g = a$ и $b'g = b$, то $a(h)S = a(..ab..) = b = b'g = a'hg = ag^{-1}hg$, а это сопряжение по g^{-1}. Тогда все автоморфизмы - сопряжения. Покажем, что сопряжение по разным элементам различны. Две перестановки различаются минимум по 2м индексам $ig \neq ih$ и $jg \neg jh$. Тогда очевидно, что транспозиция этих 2х индексов (ij) при каждом сопряжении о g или h переходит в разные элементы. Описано.

8. **Приведите пример группы G, обладающей автоморфизмом, не являющимся внутренним.**

   Пусть $G = \mathbb{Z}/3\mathbb{Z}$ - коммутативна, тогда все сопряжения очевидно слипаются. При этом есть нетривиальный автоморфизм:

   $$0 \mapsto 0$$
   $$1 \mapsto 2$$
   $$2 \mapsto 1$$

9. **Пусть n и m – целые положительные взаимно простые числа. Постройте изоморфизм групп $\mathbb{Z}/nm\mathbb{Z} \cong Z/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$.**

   Построим

   $$\varphi : Z/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \longrightarrow \mathbb{Z}/nm\mathbb{Z}$$
   $$([k]_n, [l]_m) \mapsto [km + ln]_{mn}$$

   Это морфизм, так как $\varphi([a+b],[c+d]) = [(a+b)m + (c+d)n] = [am + cn + bm + dn] = \varphi([a],[c]) + \varphi([b],[d])$. Он сюрьективен, так как выражение $km + ln$ принимает все возможные значения в $\mathbb{Z}$, и так как это отображение между множествами одного конечного порядка, то он и биективен. Изморфизм построен.

10. **Классифицируйте с точностью до изоморфизма все группы G такие, что G содержит не более 6 элементов.**

    - $|G| = 1$, очевидно единственная группа 1.
    - $|G| = p$, порядок прост, единственная группа $\mathbb{Z}/p\mathbb{Z}$.
    - $|G| = 4$
      (a) a, b, c - инволюции и пусть $ab = c$.

e	a	b	c
a	e	c	b
b	c	e	a
c	b	a	e

      Видно, что эта группа изоморфна V_4.
      (b) Есть элемент порядка 4, тогда это $\mathbb{Z}/4\mathbb{Z}$.
    - $|G| = 6$
      (a) Если мы нашли элемент порядка 6, то это $\mathbb{Z}/6\mathbb{Z}$.
      (b) Если в группе все элементы инволюции. Тогда инволюция своим действием на нетривиальные элементы группы свяжет их в пары, то есть $ba = c, ca = b, da = f, fa = d$.

      $$ba = c \Rightarrow a = bc \qquad \Rightarrow ac = b$$
      $$ca = b \Rightarrow a = cb \qquad \Rightarrow ab = c$$
      $$da = f \Rightarrow a = fd \qquad \Rightarrow ad = f$$
      $$fa = d \Rightarrow a = df \qquad \Rightarrow af = d$$

e	a	b	c	d	f
a	e	c	b	f	d
b	c	e	a	$\cdot$	$\cdot$
c	b	a	e	$\cdot$	$\cdot$
d	f	$\cdot$	$\cdot$	e	a
f	d	$\cdot$	$\cdot$	a	e

Но дальше заполнить таблицу нам не удастся, так как db, если смотреть на столбец может быть равен или d или f, а если смотреть на строчку, то либо b, либо c.

(c) Тогда в группе можно найти элемент порядка 3 b. Порядок группы четен, тогда в группе найдётся инволюция, так как в противном случая $G = \{e, a, a^{-1}, \dots, b, b^{-1}\}$ и её порядок нечетен. Пусть a - инволюция. Тогда в группе есть как минимум a, b, b^2, ab, ab^2. $H =< b >$ нормальна, так как у неё всего 2 класса смежности, а значит $H = gH \sqcup H = Hg \sqcup H$, то есть $gH = Hg$ для любого g, а значит $gHg^{-1} = Hgg^{-1} = H$. Тогда возможно 2 случая:

- $aba = b$. Тогда $ab^2 = aabaaba = b^2a$, $ab = aaba = ba$ и $ab^2a = aabaabaa = b^2$.

e	a	b	b^2	ab	ab^2
a	e	ab	ab^2	b	b^2
b	ab	b^2	e	ab^2	a
b^2	ab^2	e	b	a	ab
ab	b	ab^2	a	b^2	e
ab^2	b^2	a	ab	e	b

Если приглядеться, то мы получили $\mathbb{Z}/n\mathbb{Z}$, так как например у ab порядок 6.

- $aba = b^2$. Тогда $ab^2a = aabaa = b$, $ba = abbaa = ab^2$ и $bab = ab^2b = a$, $b^2a = abaa = ab$.

e	a	b	b^2	ab	ab^2
a	e	ab	ab^2	b	b^2
b	ab^2	b^2	e	a	b^2
b^2	ab	e	b	ab^2	ab
ab	b^2	ab^2	a	e	b
ab^2	b	a	ab	b^2	e

У нас три инволюции a, ab, ab^2. И два элемента порядка 3, что очень похоже на S_3. Сопоставив

$$a \mapsto (12) \quad ab \mapsto (23) \quad ab^2 \mapsto (13)$$
$$b = a(ab) \mapsto (12)(23) = (321) \quad b^2 = a(ab^2) \mapsto (12)(13) = (123)$$

мы получим изоморфизм. Так как $aba = (23)(12) = (123) = b^2$.

11. **Назовем множество элементов $H = \{g1, g2, ...\}$ группы G порождающими, если каждый элемент из G можно записать в виде произведения элементов из H и обратных к ним. Будем говорить, что G конечно порождена, если множество H можно выбрать конечным. Является ли группа $(\mathbb{Q}, +)$ конечно порожденной?**

Пусть $H = \{\frac{p_1}{q_1}, \dots, \frac{p_n}{q_n}\}$, что $p_i \wedge q_i = 1$. Возьмём $q = q_1 \dots q_n + 1$. Если $< H >= \mathbb{Q}$, то

$$\frac{1}{q} = n_1\frac{p_1}{q_1} + \dots + n_n\frac{p_n}{q_n}$$
$$1 = q(n_1\frac{p_1}{q_1} + \dots + n_n\frac{p_n}{q_n})$$
$$q_1 \cdot \dots \cdot q_n = q(\sum_i n_i p_i \prod_{j \neq i} q_i)$$

но это противоречит с фактом, что $q \wedge q_1 \dots q_n = 1$. Так что $< H >\neq \mathbb{Q}$ и группа $\mathbb{Q}$ не конечно порожденная.

12. **Элемент симметрической группы S_n, то есть группы биекций n-элементного множества X, называется транспозицией, если он меняет местами два элемента X, а остальные элементы X оставляет на месте. Покажите, что транспозиции порождают S_n.**

Пусть $g \in S_n$, тогда g при действии на $\{1, \dots, n\}$ разобьёт его на циклы. Циклы не будут пересекаться, так как иначе было бы $ag = bg$ и действие g не было бы инъективным. Тогда g

разбивается на произведение циклов. Эти циклы очевидно коммутируют, так как действуют дизъюнктивно. Каждый цикл раскладывается в произведение транспозиций. $(a_1 a_2 \dots a_k) = (a_k a_{k-1}) \dots (a_2 a_1)$.

13. **Верно ли, что всякая подгруппа H в прямом произведении групп $G_1 \times G_2$ имеет вид $H_1 \times H_2$, где H_i это подгруппа в G_i для $i = 1, 2$?**

$V_4 = \mathbb{Z}_2 \times \mathbb{Z}_2$. Подгруппы множителей $0, \mathbb{Z}_2 \leq \mathbb{Z}_2$. При этом $< (1,1) >$ имеет порядок 2 и не равна $0 \times \mathbb{Z}_2$ или $\mathbb{Z}_2 \times 0$.

14. **("Обращение теоремы Лагранжа") Пусть n делится на m. Может ли в группе порядка n не быть подгруппы порядка m?**

$|A_4| = 12$. А этой группе нет элементов порядка 6, так что $\mathbb{Z}_6$ не $\hookrightarrow A_4$. Другая группа порядка 6 - S_3. В ней 3 инволюции и они не коммутируют. В группе A_4 тоже три инволюции, но они коммутируют:

$$(12)(34)(13)(24) = (14)(23)$$
$$(13)(24)(12)(34) = (14)(23)$$

. Так что в A_4 нет подгрупп порядка 6.

15. **Модулярной группой назовем множество матриц**

$$\mathrm{SL}_2(\mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in \mathbb{Z},\ ad - cd = 1 \right\}$$

с операцией умножения. Проверьте аксиомы группы. Докажите, что модулярная группа порождается матрицами

$$R = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}, \quad S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

- Умножение любых матриц, подходящего размера ассоциативно, так как

$$AB = \left[\sum_k a_k^i b_j^k \right]_j^i,$$
$$A(BC) = \left[\sum_k a_k^i \, [BC]_j^k \right]_j^i$$
$$= \left[\sum_k a_k^i \sum_l b_l^k c_j^l \right]_j^i$$
$$= \left[\sum_k \sum_l a_k^i b_l^k c_j^l \right]_j^i$$
$$= \left[\sum_l \sum_k a_k^i b_l^k c_j^l \right]_j^i$$
$$= \left[\sum_l \left[\sum_k a_k^i b_l^k \right] c_j^l \right]_j^i$$
$$= (AB)\, C$$

- Единицей очевидно будет $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.
- Обратной к модулярной матрице $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ как нетрудно заметить будет $\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$.

Поэтому $\mathrm{SL}_2(\mathbb{Z})$ – группа.

Пусть $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$. Тогда эту матрицу можно свести к единичной, умножая её на R и S справа, действуя по следующему рекурсивному алгоритму:

Если a и b одного знака, то домножим матрицу на R

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} b & b-a \\ d & d-c \end{pmatrix}$$

Заметим, что таким образом модуль чисел в первой строчке будет на следующем шаге меньше.

Если a и b разных знаков, то мы домножим матрицу на S

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} b & -a \\ d & -c \end{pmatrix}$$

И теперь в первой строке числа одного знака.

Продолжая эту процедуру, мы получим матрицу вида $\begin{pmatrix} a & 0 \\ c & d \end{pmatrix}$, она модулярна, а значит $ad = 1$, так как числа целые, то $a = \pm 1 = d$. Дальше, мы повторим ту же процедуру для нижней строки, так как в верхней были ± 1 и 0, то они там так и останутся. Тогда в конце алгоритма у нас будет матрица вида $\begin{pmatrix} 0 & \pm 1 \\ \mp 1 & 0 \end{pmatrix}$, но это явно либо S, либо S^{-1}. Домножив на подходящую, мы получим единичную. Тогда если перемножить обратные ко всём, на что мы умножали в обратном порядке, то мы получим разложение изначальной матрицы.