# О кубике Рубика

Семён Адлай

## 1 Неформальное введение

Кубом принято называть правильный гексаэдр – одно из пяти платоновых тел (тетраэдр, гексаэдр, октаэдр, додекаэдр, икосаэдр). Так как характеристика Эйлера для двумерной сферы – 2, то в каждом из пяти случаев выполняется тождество: число граней – число рёбер + число вершин = 2. В частности, для куба это тождество выглядит так: $6 - 12 + 8 = 2$. Кубик Рубика будем рассматривать, как состоящий из шести гранных, двенадцати рёберных и восьми вершинных кубиков, причём гранные кубики будем считать "фиксированными". Для этого выберем и "зафиксируем" один из шести гранных кубиков в качестве переднего. Далее выберем и "зафиксируем" один из четырёх ему соседних (то есть исключим из последующего выбора противоположный уже выбранному) гранных кубиков в качестве правого. 24 способа "фиксации" гранных кубиков соответствуют 24 элементам группы вращений куба. Каждому гранному кубику поставим в соответствие одну из шести цифр – $0, 1, 2, 3, 4, 5$. Рёберные и вершинные кубики сочтём расположенными в рёберных и вершинных ячейках, соответственно. Каждой из 12 рёберных ячеек поставим в соответствие упорядоченную пару цифр; а каждой из 8 вершинных ячеек - упорядоченную тройку. Верхний, правый и передний гранные кубики обозначим соответственно цифрами $0, 1$ и 2. Гранные кубики, противоположные друг другу, будут отличаться на 3 "по модулю 6". Рёберную ячейку обозначим парой в соответствии с двумя её соседними гранными кубиками, а вершинную – тройкой в соответствии с тремя её соседними гранными кубиками. Следующую упорядоченную последовательность 12 рёберных и 8 вершинных кубиков объявим "начальной позицией где "цвет" каждой "грани" совпадает с "цветом" соответствующего гранного кубика; или, точнее сказать, где каждый рёберный кубик совпадает как упорядоченная пара со своей рёберной ячейкой, и каждый вершинный кубик совпадает как упорядоченная тройка со своей вершинной ячейкой:

(01 12 20 23 34 42 45 50 04 53 31 15 012 234 450 531 240 105 321 543).

Заметим, что для задания начальной позиции гранные кубики можно не указывать, так как они нами уже "зафиксированы". Два способа упорядочить пару цифр соответствуют двум возможным "ориентациям" рёберного кубика в заданной ячейке. У вершинного кубика в определённой ячейке три возможные "ориентации" соответствуют трём циклическим перестановкам упорядоченной тройки. Отождествим начальную позицию с единичным элементом группы $S_{12} \times S_8 \times \mathbb{Z}_2^{12} \times \mathbb{Z}_3^8$. Группой Рубика $G$ будем называть подгруппу группы $S_{12} \times S_8 \times \mathbb{Z}_2^{12} \times \mathbb{Z}_3^8$, "порождённую" шестью "вращениями которые мы также обозначим цифрами $0, 1, 2, 3, 4, 5$. Из контекста станет ясно, указывает ли цифра на гранный кубик или на "вращение" соответствующего ему "слоя". Поспешим заявить, что, "зафиксировав" гранные кубики, мы шесть указанных цифр сможем освободить для однозначного указания именно вращений. Уточним, что по отношению к наружной нормали чётные цифры будут обозначать вращения по часовой стрелке, а нечётные – вращения против. Рассмотрим каноническую

проекцию

$$\pi := \pi_{12} \times \pi_8 : G \to S_{12} \times S_8$$
$$G \ni g \mapsto \pi(g) = (\pi_{12}(g), \pi_8(g)),$$

где $\pi_{12}$ проецирует элемент $g \in G$ на соответствующую ему перестановку рёберных кубиков, а $\pi_8$ проецирует тот же элемент $g$ на соответствующую ему перестановку вершинных кубиков. Так как любое из шести вращений соответствует 4-циклам в $S_{12}$ и $S_8$, то любой элемент $g \in G$, будучи порождённым этими вращениями, проецируется на элемент $\pi(g) = (\pi_{12}(g), \pi_8(g)) =: (\sigma, \tau)$, при том, что $\sigma$ и $\tau$ либо обе чётные, либо обе нечётные, как соответствующие элементу $g$ перестановки в $S_{12}$ и $S_8$. В последующих главах мы докажем, что это единственное ограничение на $\pi(g) = (\sigma, \tau)$ – образ произвольного элемента $g \in G$. Это единственное ограничение полностью характеризует $\pi(G)$ – образ гомоморфизма $\pi$, как подгруппу группы $S_{12} \times S_8$, индекс которой в $S_{12} \times S_8$ есть $[S_{12} \times S_8 : \pi(G)] = 2$. Тем самым мы сможем посчитать мощность группы $\pi(G)$:

$$|\pi(G)| = \frac{1}{2}|S_{12} \times S_8| = \frac{1}{2}(12!)(8!) = 2^{16}3^75^37^211 = 9656672256000;$$

а взяв произведение числа всевозможных "порождённых" шестью указанными "вращениями" сочетаний "ориентаций" рёберных ($2^{11}$) и числа всевозможных сочетаний "ориентаций" вершинных ($3^7$) кубиков, и посчитав мощность ядра $\pi$

$$|Ker(\pi)| = 2^{11}3^7 = 4478976,$$

мы сможем посчитать мощность и самой группы Рубика $G$:

$$|G| = |\pi(G)||Ker(\pi)| = (2^{16}3^75^37^211)(2^{11}3^7) = 2^{27}3^{14}5^37^211 = 43252003274489856000.$$

# 2 О симметрических группах

Пусть $n$ – натуральное число. Группу перестановок $n$ символов обозначим как $S_n$. Два элемента $\sigma, \tau \in S_n$ назовём сопряжёнными в $S_n$ (в дальнейшем будем опускать "в $S_n$"), если $\exists \rho \in S_n : \rho^{-1}\sigma\rho = \tau$.[1] Очевидно, что отношение сопряжённости является рефлексивным, и если $\sigma$ сопряжено с $\tau$, то $\tau$ сопряжено с $\sigma$. Другими словами, отношение сопряжённости является ещё и симметричным. Легко проверить, что это отношение также и транзитивно. Таким образом, $S_n$ можно разбить на классы сопряжённости. А так как любую перестановку из $S_n$ можно записать как композицию независимых циклов (хотя словосочетание независимые циклы мы не определяли, его смысл очевиден), то число классов сопряжённости $S_n$ есть число разбиений числа $n$ на суммы натуральных чисел. Это число мы обозначим как $P(n)$.

## 2.1 Подсчёт числа $P(n)$ – числа классов сопряжённости $S_n$

Определение 2.1 *Пусть $n \in \mathbb{N}$. Классом сопряжённости $S_n$ уровня $k$, $1 \leq k \leq n$, назовём любой класс сопряжённости $S_n$, представители которого состоят из циклов, длина которых не меньше $k$.*

[1] Мы полагаем, что перестановка слева применяется первой. Это противоречит принятому обозначению в общем случае, когда речь идёт о композиции функций. Однако в частном случае, когда речь идёт именно о композиции перестановок, порядок их применения слева направо встречается не так уж редко. Во всяком случае, предложенный в данной работе порядок применения перестановок слева направо нисколько не уступает в удобстве обратному порядку справо налево.

Число классов сопряжённости $S_n$ уровня $k$ – это число разбиений числа $n$ на суммы, состоящие из слагаемых, не меньших $k$. Это число мы будем обозначать как $P_k(n)$. Тогда $P_1(n) = P(n)$ и $P_n(n) = 1$. Тут же заметим, что $(\forall k > n)\ P_k(n) = 0$.

Убедимся в верности следующей "реккурентной" формулы:

$$(\forall k:\ 1 \le k < n)\ \ P_k(n) = P_k(n-k) + P_{k+1}(n). \tag{1}$$

Действительно, число разбиений числа $n$ на суммы слагаемых, не меньших $k$ – $P_k(n)$, есть ничто иное как сумма числа разбиений числа $n$ на суммы слагаемых, не меньших $k$, и содержащие $k$ как слагаемое – $P_k(n-k)$, и числа разбиений числа $n$ на суммы слагаемых, строго превосходящих $k$ – $P_{k+1}(n)$.

Для непосредственного вычисления, скажем $P(8)$, кратно применим формулу (1):

$$P(8) = P_1(8) = P_1(7) + P_2(8) = P_1(7) + P_2(6) + P_3(8) =$$
$$= P_1(7) + P_2(6) + P_3(5) + P_4(8) = P_1(7) + P_2(6) + P_3(5) + P_4(4) + P_5(8).$$

Далее можно не продолжать, ибо известно, что $P_5(8) = 1$, так как число 8 разбивается на сумму слагаемых, строго превосходящих 4, лишь одним единственным образом.

Замечание 2.1 *Из формулы (1) немедленно следует равенство*

$$P_k(2k+l) = P_k(k+l) + P_{k+1}(2k+l),$$

*которое в случае, когда* $l = 0$ *или* $l = 1$, *упрощается в равенство*

$$P_k(2k+l) = P_k(k+l) + 1.$$

Таким образом, для вычислений будем пользоватся формулой:

$$P(n) = 1 + \sum_{1 \le k}^{2k \le n} P_k(n-k). \tag{2}$$

Замечание 2.2 *Если* $k \ge 2$, $l = 0$ *или* $l = 1$, *то* $P_k(k+l) = 1$ *и, следовательно, при* $n \ge 4$, *последнее слагаемое суммы в формуле (2) –* $P_k(k+l)$, $l = 0$ *или* $l = 1$, *всегда оказывается единицей, а равенство в замечании (2.1) упрощается далее:*

$$P_k(2k+l) = 1 + 1 = 2.$$

Примеры 2.1

$P(1) = 1$

$P(2) = 1 + P_1(1) = 1 + 1 = 2$

$P(3) = 1 + P_1(2) = 1 + 2 = 3$

$P(4) = 1 + P_1(3) + P_2(2) = 1 + 3 + 1 = 5$

$P(5) = 1 + P_1(4) + P_2(3) = 1 + 5 + 1 = 7$

$P(6) = 1 + P_1(5) + P_2(4) + P_3(3) = 1 + 7 + 2 + 1 = 11$

$P(7) = 1 + P_1(6) + P_2(5) + P_3(4) = 1 + 11 + 2 + 1 = 15.$

В последних двух примерах мы пользовались следствием формулы (1), указанном в замечаниях (2.1) и (2.2), для вычисления $P_2(4)$ и $P_2(5)$. Как было указано, оба значения равны 2.

Формулу (2) можно "немного обобщить":

$$(\forall m : 1 \leq m < n)\ \ P_m(n) = 1 + \sum_{m \leq k}^{2k \leq n} P_k(n-k). \tag{3}$$

Продолжим двумя сериями примеров вычислений, пользуясь формулой (3).

Примеры 2.2

$P_2(6) = 1 + P_2(4) + P_3(3) = 1 + 2 + 1 = 4$

$P_2(7) = 1 + P_2(5) + P_3(4) = 1 + 2 + 1 = 4$

$P_2(8) = 1 + P_2(6) + P_3(5) + P_4(4) = 1 + 4 + 1 + 1 = 7$

$P_2(9) = 1 + P_2(7) + P_3(6) + P_4(5) = 1 + 4 + 2 + 1 = 8$

$P_2(10) = 1 + P_2(8) + P_3(7) + P_4(6) + P_5(5) = 1 + 7 + 2 + 1 + 1 = 12.$

И опять в последних двух примерах мы не обошлись без замечания (2.2) для вычисления $P_3(6) = 2$ и $P_3(7) = 2$.

Примеры 2.3

$P_3(8) = 1 + P_3(5) + P_4(4) = 1 + 1 + 1 = 3$

$P_3(9) = 1 + P_3(6) + P_4(5) = 1 + 2 + 1 = 4.$

Полагаясь на сделанные вычисления, продолжим последней серией примеров, в итоге которой мы вычислим число классов сопряжённости не только для $S_8$, но и для $S_{12}$.

Примеры 2.4

$P(\mathbf{8}) = 1 + P_1(7) + P_2(6) + P_3(5) + P_4(4) = 1 + 15 + 4 + 1 + 1 = \mathbf{22}$

$P(9) = 1 + P_1(8) + P_2(7) + P_3(6) + P_4(5) = 1 + 22 + 4 + 2 + 1 = 30$

$P(10) = 1 + P_1(9) + P_2(8) + P_3(7) + P_4(6) + P_5(5) = 1 + 30 + 7 + 2 + 1 + 1 = 42$

$P(11) = 1 + P_1(10) + P_2(9) + P_3(8) + P_4(5) + P_5(6) = 1 + 42 + 8 + 3 + 1 + 1 = 56$

$P(\mathbf{12}) = 1 + P_1(11) + P_2(10) + P_3(9) + P_4(8) + P_5(7) + P_6(6) = 1 + 56 + 12 + 4 + 2 + 1 + 1 = \mathbf{77}.$

## 2.2 Порождающие подмножества $S_n$

Определение 2.2 *Пусть $n$ – натуральное. Будем говорить, что подмножество группы $S_n$ покрывает $n$, если оно не оставляет фиксированных символов. Другими словами, подмножество группы $S_n$ покрывает $n$, если для любого из $n$ символов, скажем для $s$, существует элемент $\sigma$ – элемент указанного подмножества – такой, что $\sigma(s) \neq s$.*

Теорема 2.1 *Пусть $n$ – натуральное, $n \geq 3$. Пусть подмножество $\{\sigma, \tau\} \subset S_n$ покрывает $n$, где $\sigma$ – $(n-1)$-цикл, а $\tau$ – транспозиция. Тогда подмножество $\{\sigma, \tau\}$ порождает $S_n$.*

Доказательство Без потери общности можем предположить, что $\sigma = (2 \dots n)$, $\tau = (1\ n-1)$. Сочтём известным тот факт, что $S_n$ порождается транспозициями, и тем самым будем считать нашу теорему доказанной, как только мы покажем, что $\sigma$ и $\tau$ порождают любую транспозицию. Мы сможем получить любую транспозицию вида $(1\ s)$, где $2 \leq s \leq n$, сопрягая $\tau$ с $\sigma$. А именно, $(1\ s) = (\sigma^s(1)\ \sigma^s(n-1)) = \sigma^{-s}\tau\sigma^s$. Но тогда, как и требовалось, $\sigma$ и $\tau$ порождают вообще любую транспозицию $(s\ t)$, где $1 \leq s < t \leq n$, ибо $(s\ t) = (1\ s)(1\ t)(1\ s)$. □

Следствие 2.1 *$S_8$ порождается подмножеством $\{\sigma, \tau\}$, покрывающим 8, где $\sigma$ – 7-цикл, а $\tau$ – транспозиция.*

Следствие 2.2 *$S_{12}$ порождается подмножеством $\{\sigma, \tau\}$, покрывающим 12, где $\sigma$ – 11-цикл, а $\tau$ – транспозиция.*

# 3 Группа Рубика $G$

Отныне будем сокращать словосочетания гранные кубики, рёберные кубики и вершинные кубики на грани, рёбра и вершины, соответственно.

Определение 3.1 *Если упорядоченная пара $i_0 i_1$ – ребро, то упорядоченную пару или транспозицию $(i_0\ i_1)$ будем называть неориентированным ребром.*

*Если упорядоченная тройка $i_0 i_1 i_2$ – вершина, то 3-цикл $(i_0\ i_1\ i_2)$ будем называть неориентированной вершиной.*

Но и прилагательные неориентированное и неориентированная мы будем опускать, если они подразумеваются контекстом. Как раз в следующей главе – главе (3.1) – рёбра и вершины предполагаются неориентированными. В главе (3.2) такого о рёбрах и вершинах подразумевать не станем. Если понадобится подчеркнуть, что ребро не неориентированное или что вершина не неориентированная, то мы прибегнем к прилагательным ориентированное и ориентированная, соответственно. Если мы упорядоченной парой (тройкой) $i$ обозначили ребро (вершину), то будем прибегать к тому же обозначению $i$ для обозначения неориентированного ребра (неориентированной вершины), то есть будем опускать скобки $(\cdot)$, указывающие на преобразование пары или тройки $i$ в соответствующий цикл $(i)$.

Определение 3.2 *Элемент $g \in G$ группы Рубика назовём рёберным, если он не "затрагивает" вершины. Аналогично, элемент $g \in G$ группы Рубика назовём вершинным, если он не "затрагивает" рёбра.*

## 3.1 Подгруппа $\pi(G)$ – образ гомоморфизма $\pi$

Лемма 3.1.1 *Группа Рубика содержит рёберный 11-цикл.*

Замечание 3.1.1 *Прилагательное рёберный можно было бы опустить, так как любой элемент группы Рубика порядка 11 является рёберным* 11*-циклом.*

Предъявим элемент, существование которого утверждается леммой (3.1), и обозначим его как $h_{11}$. А именно,

$$h_{11} := (0123)^3$$

является рёберным 11-циклом. Элемент $h_{11}$ переводит "начальную позицию"

(01 12 20 23 34 42 45 50 04 53 31 15 012 234 450 531 240 105 321 543).

в позицию

(35 31 12 51 20 10 45 24 32 04 50 43 012 234 450 531 240 105 321 543).

Другими словами, элемент $h_{11}$ выражается следующей циклической перестановкой 11 рёбер:

(01 24 50 31 12 20 34 51 23 40 35).

Заметим, что $h_{11}$ оставляет ребро 45 фиксированным.

Лемма 3.1.2 *Группа Рубика содержит вершинный* 7*-цикл.*

Замечание 3.1.2 *Хотя любой элемент группы Рубика порядка 7 является циклом, прилагательное вершинный в последней лемме ни в коем случае не является лишним.*

Предъявим элемент, существование которого утверждается леммой (3.2), и обозначим его как $h_7$. А именно,

$$h_7 := (0122)^9$$

является вершинным 7-циклом. Элемент $h_7$ переводит "начальную позицию"

(01 12 20 23 34 42 45 50 04 53 31 15 012 234 450 531 240 105 321 543).

в позицию

(01 12 20 23 34 42 45 50 04 53 31 15 450 024 051 012 531 132 342 543).

Более кратко, элемент $h_7$ выражается следующей циклической перестановкой 7 вершин:

(012 531 240 342 321 051 450).

Заметим, что $h_7$ оставляет вершину 543 фиксированной.

Лемма 3.1.3 *Группа Рубика содержит элемент* $h_2$ 2*-го порядка, транспонирующий два ребра и транспонирующий две вершины.*

Замечание 3.1.3 *Элемент, указанный в лемме (3.3), можно подобрать так, чтобы не только ребро* 45 *оказалось одним из двух переставляемых, но и чтобы вершина* 543 *тоже оказалась одной из двух переставляемых. Именно такой элемент мы и подберём. Это позволит нам пользоваться следствиями (2.1) и (2.2) ) теоремы (2.1) с целью доказательства следующей теоремы – теоремы (3.1).*

Предъявим элемент $h_2$:

$$h_2 := 24442224443443334244422244 \ 30553330004443053330004443055533300044402221120004402221120000.$$

Элемент $h_2$ выражается следующей рёберно-вершинной парой транспозиций:

$$(45\ 43)(543\ 045).$$

Элемент $h_2$ был подобран в согласии с замечанием (3.3).

Замечание 3.1.4 *Для вышеуказанной рёберно-вершинной пары транспозиций мы могли бы "укоротить" элемент $h_2$, взяв*

$$h_2 = 24442224443443334244422244430553330004444305333000444430555333000.^{2}$$

*Тем не менее, присоединив к "укороченному" $h_2$ "суффикс"*

$$g_3 := (440222112000)^2,$$

*именно "удлинённый" $h_2$ становится элементом 2-го порядка в самой группе $G$. "Укороченный" $h_2$ является элементом 6-го порядка в группе $G$. Разумеется, и "удлинённый" и "укороченный" $h_2$ отображается в элемент 2-го порядка в $\pi(G)$. Более того, их образы совпадают в $\pi(G)$. Меняя "ориентацию" вершины 450 на 045 и "ориентацию" вершины 234 на 342 элементом-суффиксом $g_3$, мы тем самым сохранили "ориентацию" всех рёбер и вершин, оставшихся "на своих местах" после приложения "удлинённого" $h_2$. Если бы мы всё же указали на "укороченный элемент" в качестве выбранного, то пришлось бы нам указать и на соответствующую ему, уже менее симпатичную, рёберно-вершинную пару транспозиций:*

$$(45\ 43)(543\ 504\ 354\ 450\ 435\ 045)(234\ 342\ 423).$$

Замечание 3.1.5 *Следует отметить, что циклическая перестановка упорядоченной тройки символов 2 3 4 указанным в замечании (3.4) элементом-суффиксом $g_3$ является обратной его циклической перестановке упорядоченной тройки символов 4 5 0.*

Подробный разговор об ориентации нуждается хотя бы в строгом её определении, что будет сделано в главе (3.2). В той же главе – главе (3.2), мы вернёмся к обсуждению элемента $g_3$. А сейчас подытожим полученные нами результаты в следующей теореме – теореме (3.1).

Для доказательства теоремы (3.1) будет удобным дать ещё два определения.

Определение 3.1.1 *Пусть $h \in G$. Будем говорить, что $h$ – чётно (нечётно), если оба образа преобразования $h$ – $\pi_{12}(h)$ и $\pi_8(h)$ являются чётными (нечётными), как перестановки в $S_{12}$ и $S_8$, соответственно.*

[2] Для минимизации вероятности возникновения ошибки в столь длинной последовательности цифр была написана программа, с помощью которой выполнялась автоматическая проверка этой и всех других, ей предшествующих и последующих, указанных в работе, последовательностей вращений.

Определение 3.1.2 *Рассмотрим $S_{12}$ и $S_8$ как группы перестановок рёбер и вершин, соответственно. Будем называть транспозицию в $S_{12}$ особой, или особого вида, если ребро 45, а точнее ребро в ячейке 45, оказалось одним из двух переставляемых. Транспозицию в $S_8$ назовём особой, или особого вида, если вершина 543, а точнее вершина в ячейке 543, оказалась одной из двух переставляемых. Особые транспозиции в $S_{12}$ и $S_8$ будем обозначать как $\tau_{12}$ и $\tau_8$, соответственно. Будем говорить, что транспозиция вида $\tau_n$, если она особая как транспозиция в $S_n$.*

Замечание 3.1.6 *$\pi_{12}(h_2)$ является одной из 11 нетривиальных транспозицией вида $\tau_{12}$, а $\pi_8(h_2)$ – одной из 7 нетривиальных транспозицией вида $\tau_8$. Конечно же, тривиальные перестановки $e_{12}$ и $e_8$ являются транспозициями вида $\tau_{12}$ и $\tau_8$, соответственно.*

Замечание 3.1.7 *Пусть $h \in G$, $h$ – чётно (нечётно). Тогда $\pi_{12}(h)$, будучи чётной (нечётной) перестановкой, выражается как композиция чётного (нечётного) числа транспозиций, каждая из которых, в свою очередь, может быть представлена как композиция трёх транспозиций особого вида*

$$\tau_{12} = (\pi_{12}(h_{11}))^{-p}\pi_{12}(h_2)(\pi_{12}(h_{11}))^p = \pi_{12}(h_{11}^{-p}h_2h_{11}^p),\ 0 \le p \le 10.^3$$

*Аналогично, $\pi_8(h)$ выражается как композиция чётного числа транспозиций особого вида*

$$\tau_8 = (\pi_8(h_7))^{-q}\pi_8(h_2)(\pi_8(h_7))^q = \pi_8(h_7^{-q}h_2h_7^q),\ 0 \le q \le 6.$$

*Теперь запишем, для указанных $\tau_{12}$ и $\tau_8$, пользуясь независимостью $h_{11}$ и $h_7$,*

$$(\tau_{12}, \tau_8) = (\pi_{12}(h_{11}^{-p}h_2h_{11}^p), \pi_8(h_7^{-q}h_2h_7^q)) =$$
$$= (\pi_{12}(h_{11}^{-p}h_7^{-q}h_2h_7^qh_{11}^p), \pi_8(h_{11}^{-p}h_7^{-q}h_2h_7^qh_{11}^p)) = \pi(h_{11}^{-p}h_7^{-q}h_2h_7^qh_{11}^p) =: \tau$$

*и увидим, что $\pi(h)$ можно выразить как комозицию чётного (нечётного) числа элементов $S_{12} \times S_8$ вида $\tau$.*

Замечание 3.1.8 *На самом деле, как мы установили уже в "неформальном введении $h$ – чётно (нечётно) тогда и только тогда, когда либо $\pi_{12}(h) \in S_{12}$, либо $\pi_8(h) \in S_8$ чётна (нечётна), как перестановка в $S_{12}$ или $S_8$, соответственно.*

Замечание 3.1.9 *$h$ – чётно (нечётно) тогда и только тогда, когда оно состоит из чётного (нечётного) числа вращений $0, 1, 2, 3, 4, 5$.*

Зададим гомоморфизм

$$\phi : \mathbb{Z}_2 \to S_{12} \times S_8$$
$$1 \mapsto (\pi_{12}(h_2), \pi_8(h_2)) = \pi(h_2),$$

и действие $\mathbb{Z}_2$ на $A_{12} \times A_8$ сопряжением с $\phi(z)$ :

$$(\forall z \in \mathbb{Z}_2, \forall \sigma \in A_{12} \times A_8)\ \ z \cdot \sigma := \phi(z)\sigma\phi(z).^4$$

[3] О том, что любую транспозицию можно выразить как композицию трёх транспозиций особого вида, было сказано в доказательстве теоремы (2.1).

[4] Это тоже действие, что и действие $z \cdot \sigma := \phi(z)\sigma\phi(z)^{-1}$, так как характиристика $\mathbb{Z}_2 = 2$, а $\phi$ – гомоморфизм.

Определим группу $H := (A_{12} \times A_8) \rtimes \mathbb{Z}_2$ с операцией, соответствующей указанному нами действию $\mathbb{Z}_2$ на $A_{12} \times A_8$ :

$$(\forall z', z'' \in \mathbb{Z}_2, \forall \sigma', \sigma'' \in A_{12} \times A_8)\ \ (\sigma', z')(\sigma'', z'') = (\sigma, z),$$

где $\sigma = \sigma'(z' \cdot \sigma'') = \sigma'\phi(z')\sigma''\phi(z') \in A_{12} \times A_8$, а $z = z'z'' \in \mathbb{Z}_2$.

Теорема 3.1 *Группа Рубика $G$ содержит подгруппу $H$, изоморфную группе $(A_{12}\times A_8)\rtimes\mathbb{Z}_2$ с операцией, указанной в её определении, предшествующем теореме.*[5]

Доказательство Сразу же отметим, что $(A_{12} \times A_8) \trianglelefteq (A_{12} \times A_8) \rtimes \mathbb{Z}_2$ хотя бы потому, что $[(A_{12} \times A_8) \rtimes \mathbb{Z}_2 : A_{12} \times A_8] = 2$.

Пусть $h_{11}$, $h_7$ и $h_2$ – элементы группы $G$, указанные леммами (3.1), (3.2) и (3.3), соответственно. Заметим, что пара $\pi_{12}(h_{11})$ – образ элемента $h_{11}$ и $\pi_{12}(h_2)$ – образ элемента $h_2$, в $\pi_{12}(G) \leq S_{12}$, порождает $S_{12}$, будучи парой, удовлетворяющей условиям следствия (2.2) теоремы (2.1). Другими словами, подмножество $\{\pi_{12}(h_{11}), \pi_{12}(h_2)\}$ покрывает 12, притом, что $\pi_{12}(h_{11})$ является 11-циклом, а $\pi_{12}(h_2)$ – транспозицией в $S_{12}$. Таким образом, отображение $\pi_{12}$ является сюръективным: $\pi_{12}(G) = S_{12}$. Аналогично, пара $\pi_8(h_7)$ – образ элемента $h_7$ и $\pi_8(h_2)$ – образ элемента $h_2$, в $\pi_8(G) \leq S_8$, порождает $S_8$, будучи парой, удовлетворяющей условиям следствия (2.1) теоремы (2.1). Тем самым и отображение $\pi_8$ является сюръективным: $\pi_8(G) = S_8$.

Продемонстрировать сюръективность $\pi_{12}$ и $\pi_8$ можно и по-другому. Из замечания (3.6) следует, что $\pi_{12}(G)$ содержит все транспозиции вида $\tau_{12}$ и, следовательно, вообще все транспозиции в $S_{12}$ вместе со всеми её перестановками. Из замечания (3.6) также следует, что $\pi_8(G)$ содержит все транспозиции вида $\tau_8$ и, стало быть, вообще все перестановки $S_8$.

Покажем, что если $(\sigma_{12}, \sigma_8)$ – произвольный элемент группы $A_{12} \times A_8$, то

$$\exists h \in G,\ h \text{ – чётно и } \pi(h) = (\sigma_{12}, \sigma_8).$$

Для того, чтобы это показать, запишем $\sigma_{12}$, как композицию чётного числа транспозиций вида $\tau_{12}$, из замечания (3.6), а $\sigma_8$, как композицию чётного числа транспозиций вида $\tau_8$, из того же замечния (3.6):

$$\sigma_{12} = \rho_1\rho_2 \dots \rho_s,$$
$$s \text{ – чётное, и каждая транспозиция } \rho_i \text{ – транспозиция вида } \tau_{12} :$$
$$\rho_i = \pi_{12}(h_{11}^{-p_i} h_2 h_{11}^{p_i}),\ 0 \leq p_i \leq 10,\ 1 \leq i \leq s;$$

$$\sigma_8 = \omega_1\omega_2 \dots \omega_t,$$
$$t \text{ – чётное, и каждая транспозиция } \omega_j \text{ – транспозиция вида } \tau_8 :$$
$$\omega_j = \pi_8(h_7^{-q_j} h_2 h_7^{q_j}),\ 0 \leq q_j \leq 6,\ 1 \leq j \leq t.$$

Искомый элемент $h$ удовлетворяет:

$$\pi(h) = (\pi_{12}(h), \pi_8(h)) = (\sigma_{12}, \sigma_8).$$

[5]Мы уже успели отождествить две изоморфные друг другу группы, хотя следует заметить, что, строго говоря, группа $H$, указанная в теореме, лишь изоморфна группе $H$, указанной в её определении.

Возмём $h = h_{12}h_8$, где

$$h_{12} = h_{11}^{-p_1} h_2 h_{11}^{p_1} h_{11}^{-p_2} h_2 h_{11}^{p_2} \dots h_{11}^{-p_s} h_2 h_{11}^{p_s},$$

$$h_8 = h_7^{-q_1} h_2 h_7^{q_1} h_7^{-q_2} h_2 h_7^{q_2} \dots h_7^{-q_t} h_2 h_7^{q_t},$$

и проверим, что

$$\pi(h) = \pi(h_{12}h_8) = (\pi_{12}(h_{12}h_8), \pi_8(h_{12}h_8)) =$$
$$= (\pi_{12}(h_{12})\pi_{12}(h_8), \pi_8(h_{12})\pi_8(h_8)) = (\pi_{12}(h_{12}), \pi_8(h_8)) = (\sigma_{12}, \sigma_8).$$

В предпоследнем равенстве мы пользовались тем, что $\pi_{12}(h_8) = e_{12}$ – единичный элемент $S_{12}$, и, что $\pi_8(h_{12}) = e_8$ – единичный элемент $S_8$. Равенство $(\pi_{12}(h_{12}), \pi_8(h_8)) = (\sigma_{12}, \sigma_8)$ обеспечено самой конструкцией элементов $h_{12}$ и $h_8$.

Если $\sigma_{12}$ и $\sigma_8$ – нечётные в $S_{12}$ и $S_8$, соответственно, то $(\sigma_{12}\pi_{12}(h_{12}), \sigma_8\pi_8(h_8)) \in A_{12} \times A_8$, и мы можем найти $h$ – такой, что

$$\pi(h) = (\sigma_{12}\pi_{12}(h_{12}), \sigma_8\pi_8(h_8)).$$

Тогда $hh_2$ является тем элементом $G$, отображением которого является $(\sigma_{12}, \sigma_8)$:

$$\pi(hh_2) = \pi(h)\pi(h_2) = (\sigma_{12}\pi_{12}(h_{12}), \sigma_8\pi_8(h_8))(\pi_{12}(h_{12}), \pi_8(h_8)) = (\sigma_{12}, \sigma_8).$$

Остаётся проверить, что отображение:

$$\psi : G \to H = (A_{12} \times A_8) \rtimes \mathbb{Z}_2$$

$$h \mapsto \begin{cases} (\pi(h), 0) & \textit{при } h \textit{ – чётно}, \\ (\pi(hh_2), 1) & \textit{при } h \textit{ – нечётно}, \end{cases}$$

с операцией в группе $H$, указанной в определении, предшествующем теореме, является гомоморфизмом. Ключевым в проверке того, что $\psi$ – гомоморфизм, является то, что таковым является $\pi$. Осуществим, однако, детальную проверку. Пусть $h', h'' \in G$. Отметим, что $\phi(0) = (e_{12}, e_8) =: e$ – единичный элемент $A_{12} \times A_8$ и рассмотрим четыре возможных случая.

- Оба $h'$ и $h''$ чётны:

$$\psi(h')\psi(h'') = (\pi(h'), 0)(\pi(h''), 0) =$$
$$= (\pi(h')\phi(0)\pi(h'')\phi(0), 0) = (\pi(h')\pi(h''), 0) = (\pi(h'h''), 0) = \psi(h'h'').$$

- $h'$ – чётно, $h''$ – нечётно:

$$\psi(h')\psi(h'') = (\pi(h'), 0)(\pi(h''h_2), 1) =$$
$$= (\pi(h')\phi(0)\pi(h''h_2)\phi(0), 1) = (\pi(h')\pi(h''h_2), 1) = (\pi(h'h''h_2), 1) = \psi(h'h'').$$

- $h'$ – нечётно, $h''$ – чётно:

$$\psi(h')\psi(h'') = (\pi(h'h_2), 1)(\pi(h''), 0) = (\pi(h'h_2)\phi(1)\pi(h'')\phi(1), 1) =$$
$$= (\pi(h'h_2)\pi(h_2)\pi(h'')\pi(h_2), 1) = (\pi(h'h_2h_2h''h_2), 1) = (\pi(h'h''h_2), 1) = \psi(h'h'').$$

- Оба $h'$ и $h''$ нечётны:

$$\psi(h')\psi(h'') = (\pi(h'h_2), 1)(\pi(h''h_2), 1) = (\pi(h'h_2)\phi(1)\pi(h''h_2)\phi(1), 0) =$$
$$= (\pi(h'h_2)\pi(h_2)\pi(h''h_2)\pi(h_2), 0) = (\pi(h'h_2h_2h''h_2), 0) = (\pi(h'h''h_2), 0) = \psi(h'h'').$$

Так как в сюръективности $\phi$ сомневаться не приходится, подгруппу $H \leq G$ можем смело считать порожденной элементами $h_{11}$, $h_7$ и $h_2$, и считать теорему (3.1) доказанной. $\square$

Замечание 3.1.10 *О единственности $h$ с заданным отображением $\pi(h) = (\sigma_{12}, \sigma_8)$, существование которого, было доказано в предыдущей теореме – теореме (3.1), не может быть и речи. Каждый такой $h$ оказывается среди* 4478976, *обладающих его образом $\pi(h)$, о чём будет рассказано в следующей главе – главе (3.2).*

## 3.2 Нормальная подгруппа Ker($\pi$) – ядро гомоморфизма $\pi$

Понятие ячейки, уже введённое в "неформальном введении является ключевым в этой главе. Подчеркнём, что 12 рёберных ячеек и 8 вершинных оказываются фиксированными, поскольку таковыми являются все 6 граней. Каждую из 12 рёберных ячеек мы обозначили конкретной упорядоченной парой, а каждую из 8 вершинных конкретной упорядоченной тройкой. Каждой рёберной ячейке, как конкретной упорядоченной паре, соответствуют два ребра, как две возможные перестановки этой пары. Каждой вершинной ячейке, как конкретной упорядоченной тройке, соответствуют три вершины, как три возможные циклические перестановки этой тройки. Таким образом, число всевозможных рёбер совпадает с числом всевозможных вершин – $12 \cdot 2 = 8 \cdot 3 = 24$.

Мы будем опускать прилагательное рёберная или вершинная, указывая ячейку, если оно подразумевается контекстом.

Определение 3.2.1 *Если $ij$ – рёберная ячейка, $i'j'$ – ребро, а $g \in G$ – преобразование, переводящее начальную позицию*

$$(\ldots\ i\,j\ \ldots)$$

*в позицию*

$$(\ldots\ i'\,j'\ \ldots),$$

*то мы будем говорить, что ребро $i'j'$ заняло ячейку $ij$ под действием преобразования $g$.*

*Аналогично, если $ijk$ – вершинная ячейка, $i'j'k'$ – вершина, а преобразование $g$ переводит начальную позицию*

$$(\ldots\ i\,j\,k\ \ldots)$$

*в позицию*

$$(\ldots\ i'\,j'\,k'\ \ldots),$$

*то мы будем говорить, что вершина $i'j'k'$ заняла ячейку $ijk$ под действием преобразования $g$.*

### 3.2.1 Рёберная подгруппа ядра гомоморфизма $\pi$

Многие рассуждения этого параграфа – параграфа (3.2.1) – можно считать предварительными. Они получат дальнейшее развитие в следующем параграфе – параграфе (3.2.2).

Отождествим $S_2$ – группу перестановок упорядоченной пары символов 0 и 1 с двухэлементной группой вычетов $\mathbb{Z}_2$.

Определение 3.2.1.1 *Пусть $j := j_0 j_1$ – ячейка и пусть перестановка $\sigma \in S_2$ такая, что ребро $j^\sigma := j_{\sigma(0)} j_{\sigma(1)}$ заняло ячейку $i := i_0 i_1$ под действием преобразования $g \in G$. Другими словами, пусть $g \in G$ переводит начальную позицию*

$$( \dots \quad i_0 \;\; i_1 \quad \dots )$$

*в позицию*

$$( \dots \; j_{\sigma(0)} j_{\sigma(1)} \; \dots ).$$

*Если $\sigma$ – нетривиальна, то будем говорить, что неориентированному ребру $j = j_0 j_1$ задана ориентация $1 \in \mathbb{Z}_2$, в ячейке $i = i_0 i_1$, под действием преобразования $g \in G$; и ориентация $0 \in \mathbb{Z}_2$, если иначе.*

Четыре рёберные ячейки, соответствующие некой заданной грани $i$, $0 \le i \le 5$, обозначим как $i$-ячейки.

Замечание 3.2.1 *К ячейке $i_0 i_1$ сходятся грани $i_0$ и $i_1$, и тем самым ячейка $i_0 i_1$ является $i_k$-ячейкой для $k = 0$ и $k = 1$.*

Определение 3.2.1.2 *Пусть ребро $j_0 j_1$ занимает ячейку $i_0 i_1$, являющуюся $i_k$-ячейкой, $0 \le k \le 1$. Тогда будем говорить, что символ $j_k$ ребра $j_0 j_1$, в ячейке $i_0 i_1$, граничит с $i_k$.*

Следующая формула, формула (4), полагается на два определения – определение (3.2.1.1) и определение (3.2.1.2).

Пусть неориентированному ребру $j = j_0 j_1$ задана ориентация $z \in \mathbb{Z}_2$ в $i_k$-ячейке $i_0 i_1$, $k = 0$ или $k = 1$. Пусть $l = 0$ или $l = 1$ такое, что символ $j_l$ ребра $j_0 j_1$ граничит с $i_k$. Сочтём $k$ и $l$ элементами $\mathbb{Z}_2$. Тогда ориентация вершины $j_0 j_1$ в ячейке $i_0 i_1$ совпадает с разницей $k - l$ в $\mathbb{Z}_2$, то есть

$$\mathbb{Z}_2 \ni z = k - l, \tag{4}$$

что позволяет нам вычислить ориентацию ребра в ячейке двумя способами, соответствующими двум граням, сходящимся к ней.

Утверждение 3.1 *Сумма ориентаций четырёх рёбер, расположенных в четырёх $i$-ячейках, инвариантна при вращении $i$, $0 \le i \le 5$.*

Действительно, если для каждого $m$, $0 \le m \le 3$, $l_m$ такой, что символ $j^m_{l_m}$ неориентированного ребра $j^m_0 j^m_1$, в $i$-ячейке $i^m_0 i^m_1$, граничит с $i$, а $k_m$ такой, что $i^m_{k_m} = i$, то сумму ориентаций, о которой идёт речь, с помощью формулы (4) можно вычислить так:

$$\sum_m k_m - l_m = \sum_m k_m - \sum_m l_m,$$

где первая сумма $\sum_m k_m$ – константа, зависящая только от грани $i$, и каждое слагаемое второй – $l_m$ – зависит лишь от ориентации, заданной соответствующему ребру – $j_0^m j_1^m$, до вращения $i$, и не изменяется при её изменении после вращения $i$. Итак, ни та, ни другая сумма не зависит от вращения $i$.

И всё же, если утверждение (3.1) не покажется убедительным, то мы рекомендуем "перейти" к следующему параграфу – параграфу (3.2.2), в котором доказывается "усиленная" версия утверждения (3.1) – утверждение (3.2).

Замечание 3.2.2 *Сумма ориентаций всех рёбер в начальной позиции равна* $0 \in \mathbb{Z}_2$, *так как ориентация любого ребра в своей "исходной" ячейке равна* $0 \in \mathbb{Z}_2$.

Из утверждения (3.1), учитывая замечание (3.2.2), вытекает следующее следствие – следствие (3.1).

Следствие 3.1 *Сумма ориентаций всех рёбер "всегда" равна* $0 \in \mathbb{Z}_2$.

### 3.2.2 Вершинная подгруппа ядра гомоморфизма $\pi$

Рассмотрим $A_3$ как группу чётных перестановок упорядоченной тройки символов 0, 1 и 2, порождённой циклом $(0\,1\,2\,)$, и отождествим её с трёхэлементной группой вычетов $\mathbb{Z}_3$.

Определение 3.2.2.1 *Пусть* $i := i_0 i_1 i_2$ *и* $j := j_0 j_1 j_2$ *– ячейки, и пусть перестановка* $\sigma \in A_3$ *такая, что вершина* $j^\sigma := j_{\sigma(0)} j_{\sigma(1)} j_{\sigma(2)}$ *заняла ячейку* $i := i_0 i_1 i_2$ *под действием преобразования* $g \in G$. *Другими словами, пусть* $g \in G$ *переводит начальную позицию*

$$(\ \ldots \quad i_0\ i_1\ i_2 \quad \ldots\ )$$

*в позицию*

$$(\ \ldots\ j_{\sigma(0)} j_{\sigma(1)} j_{\sigma(2)}\ \ldots\ ).$$

*Если* $z \in \mathbb{Z}_3$ *такое, что* $\sigma = (0\,1\,2\,)^z$, *то будем говорить, что неориентированная вершина* $j$ *приобрела ориентацию* $z$ *под действием преобразования* $g \in G$, *или что неориентированной вершине* $j$ *задана ориентация* $z$ *в ячейке* $i$.

*Если подразумевать преобразование* $g$, *ячейку* $i$ *и то, что вершина* $j$ *неориентирована, то сокращённо будем говорить, что вершине* $j$ *задана ориентация* $z$.

*Саму перестановку* $\sigma$ *будем обозначать как* $\sigma(g)$, *или как* $\sigma(g, j)$.

Замечание 3.2.3 *Хотя в определении (3.2.2.1)* $j$ *и* $j^\sigma$ *– две различные вершины, если* $\sigma$ *нетривиальна,* $j$ *и* $j^\sigma$ *совпадают, независимо от* $\sigma$, *как две неориентированные вершины, с одной и той же неориентированной вершиной.*

Замечание 3.2.4 *В определении (3.2.2.1) требование от* $j$ *быть ячейкой является формальным. Если конкретная, уже отнюдь не формальная, ячейка* $i$ *подразумевается, то ячейку* $j$ *может занять вообще любая упорядочная тройка, а* $\sigma$ *даже "не узнает". В частности, ячейку* $j = j_0 j_1 j_2$ *может занять любая вершина* $j' = j'_0 j'_1 j'_2$. *Такую "независимость"* $\sigma$ *от* $j$, *обеспеченную оставленной "в покое" ячейкой* $i$, *выразим так:*

$$\sigma(g, j) = \sigma(g, j').$$

*Тем самым, мы подчеркнём, что в определении (3.2.2.1) упорядочная тройка $j$ является "фиктивной переменной фукции $\sigma$".*

Четыре ячейки, соответствующие некой заданной грани $i$, $0 \leq i \leq 5$, обозначим как $i$-ячейки.

Замечание 3.2.5 *К ячейке $i_0i_1i_2$ сходятся 3 грани – $i_0$, $i_1$ и $i_2$, и тем самым ячейка $i_0i_1i_2$ является $i_k$-ячейкой для $k = 0$, 1 и 2.*

Определение 3.2.2.2 *Пусть $k = 0$, 1 или 2, и пусть вершина $j_0j_1j_2$ занимает $i_k$-ячейку $i_0i_1i_2$. Тогда будем говорить, что символ $j_k$ вершины $j_0j_1j_2$, в ячейке $i_0i_1i_2$, граничит с $i_k$.*

Пользуясь двумя определениями – определением (3.2.2.1) и определением (3.2.2.2), выведем формулу (5) для вычисления ориентации, приобретённой вершиной.

Пусть заданы $k$ и $l$, $0 \leq k, l \leq 2$. Пусть неориентированной вершине $j = j_0j_1j_2$ задана ориентация $z \in \mathbb{Z}_3$, в $i_k$-ячейке $i = i_0i_1i_2$, и пусть символ $j_l$ вершины $j$ граничит с $i_k$. Сочтём $k$ и $l$ элементами $\mathbb{Z}_3$. Тогда $z$ – ориентация вершины $j$, заданная в ячейке $i$, вычисляется как разница $k - l$ в $\mathbb{Z}_3$, то есть

$$\mathbb{Z}_3 \ni z = k - l. \tag{5}$$

Действительно, если $z$ – ориентация вершины $j$, заданная в ячейке $i$, то, по определению (3.2.2.1), вершина $j^\sigma$ занимает ячейку $i$, где $\sigma = (0\,1\,2\,)^z$. Тогда, по определению (3.2.2.2), $\sigma(l) = k$, а следовательно, $z = \sigma(l) - l = k - l$, что и утверждается формулой (5).

Замечание 3.2.6 *Формула (5) позволяет нам вычислить ориентацию вершины в ячейке тремя способами, соответствующими трём граням, сходящимся к ячейке.*

Замечание 3.2.7 *Пусть $k = 0$, 1 или 2, и пусть вершина $i := i_0i_1i_2$ занимает $i_k$-ячейку $i = i_0i_1i_2$. По определению (3.2.2.2), символ $i_k$ вершины $i$ граничит с $i_k$. Если $\sigma = \sigma(i_k, i)$, то вершина $i^\sigma = i_{\sigma(0)}i_{\sigma(1)}i_{\sigma(2)} =: i'_0i'_1i'_2$ займёт $i_k$-ячейку, скажем, ячейку $i''_0i''_1i''_2$, под действием вращения $i_k$. Так как под действием вращения $i_k$ тот же символ $i_k = i'_{\sigma^{-1}(k)}$ вершины $i^\sigma = i'_0i'_1i'_2$, в ячейке $i''_0i''_1i''_2$, граничит с $i_k$, то $i''_{\sigma^{-1}(k)} = i_k$.*

Несколько "обобщим" "частное" замечание (3.2.7) замечанием (3.2.8).

Замечание 3.2.8 *Пусть $k = 0$, 1 или 2, и пусть вершина $j := j_0j_1j_2$ занимает $i_k$-ячейку $i := i_0i_1i_2$. По определению (3.2.2.2), символ $j_k$ вершины $j = j_0j_1j_2$ граничит с $i_k$. Запишем, пользуясь замечанием (3.2.4), $\sigma = \sigma(i_k, i) = \sigma(i_k, j)$. Тогда вершина $j^\sigma = j_{\sigma(0)}j_{\sigma(1)}j_{\sigma(2)} =: j'_0j'_1j'_2$ займёт $i_k$-ячейку, скажем, ячейку $i'_0i'_1i'_2$, под действием вращения $i_k$, где $i'_{\sigma^{-1}(k)} = i_k$, по замечанию (3.2.7). Так как $j_k = j'_{\sigma^{-1}(k)}$, то тот же символ – символ $j_k$ вершины $j^\sigma = j'_0j'_1j'_2$, теперь уже в ячейке $i'_0i'_1i'_2$ граничит с $i_k$.*

Менее формально, но более лаконично, замечание (3.2.8), запишем так:

"символ вершины, граничащий с $i$, не изменяется при вращении $i$".

Пользуясь формулой (5) и полагаясь на последнее замечание – замечание (3.2.8), докажем следующее утверждение – утверждение (3.2).

Утверждение 3.2 *Пусть задано $i$, $0 \leq i \leq 5$. Сумма ориентаций четырёх вершин, расположенных в четырёх $i$-ячейках, инвариантна при вращении $i$.*

Доказательство Пронумеруем четыре $i$-ячейки "последовательными" элементами из $\mathbb{Z}_4$ по направлению вращения $i$. Пусть до вращения $i$, для каждого $m \in \mathbb{Z}_4$, вершина $j^m := j_0^m j_1^m j_2^m$ занимает $i$-ячейку $i^m := i_0^m i_1^m i_2^m$. Зададим для каждого $m$ $k_m$ такой, что $i_{k_m}^m = i$. Без потери общности предположим далее, что ориентация каждой из четырёх неориентированных вершин $j^m$, заданная в соответствующей ячейке $i^m$, равна нулю в $\mathbb{Z}_3$. Тогда, если для каждого $m$ $l_m$ такой, что символ $j_{l_m}^m$ вершины $j^m$, в $i$-ячейке $i^m$, граничит с $i$, то $l_m = k_m$. Более того, по замечанию (3.2.8), $l_m$ зависит только от самой неориентированной вершины $j^m$ и не зависит от вращения $i$. Ориентацию $z_m$ вершины $j^m$, заданную после вращения $i$, в ячейке $i^{m+1}$, можно вычислить по формуле (5):

$$\mathbb{Z}_3 \ni z_m = k_{m+1} - l_m = k_{m+1} - k_m.$$

Следовательно,

$$\mathbb{Z}_3 \ni \sum_m z_m = \sum_m k_m - k_{m+1} = 0,$$

что и требовалось доказать. □

Замечание 3.2.9 *Мы не только доказали утверждение (3.2), но и выяснили, каковой окажется приобретённая ориентация каждой из четырёх вершин после вращения $i$.*

Замечание 3.2.10 *Сумма ориентаций всех вершин в начальной позиции равна $0 \in \mathbb{Z}_3$, так как ориентация любой вершины в своей "исходной" ячейке равна $0 \in \mathbb{Z}_3$.*

Из утверждения (3.2), учитывая замечание (3.2.10), вытекает следствие (3.2).

Следствие 3.2 *Сумма ориентаций, приобретённых под действием любого элемента $g \in G$, всех вершин равна $0 \in \mathbb{Z}_3$.*

### 3.2.3 Структура ядра гомоморфизма $\mathbf{Ker}(\pi)$

Основная работа для докательства следующей теоремы – теоремы (3.2) – была уже проделана в предыдущей главе – главе (3.2). Осталась лишь "техническая" её часть. По ходу доказательства мы будем подразумевать следствия (3.1) и (3.2) утверждений (3.1) и (3.2), соответственно.

Теорема 3.2 *Группа Рубика содержит нормальную подгруппу $N$, изоморфную группе $\mathbb{Z}_2^{11} \times \mathbb{Z}_3^7$.*

Доказательство Определим $N := \mathrm{Ker}(\pi)$, обеспечив тем самым "нормальность" подгруппы $N$ в группе $G$. Подгруппа $N$ "порождается" двумя элементами, которые мы назовём $g_2$ и $g_3$, порядка 2 и 3, соответственно.[6]

$$g_2 := 041115544545554551000444.$$

[6]Точнее сказать, подгруппа $N \trianglelefteq G$, будучи нормальной, "порождается" элементами $g_2$ и $g_3$, при их сопряжении элементами подгруппы $H \leq G$. Разумеется, сама группа $\mathbb{Z}_2^{11} \times \mathbb{Z}_3^7$ никак не сможет породить себя никакими двумя собственными генераторами, и мы, боже упаси, такого предлагать не станем. Здесь уместно отметить,что и $g_3^2$ может быть получен соответствующим ему сопряжением $g_3$.

Рёберный элемент $g_2$ задаёт ориентацию $1 \in \mathbb{Z}_2$ паре неориентированных рёбер 45 и 40 в "своих" ячейках 45 и 40, соответственно.

Так как подгруппа $H \leq G$ содержит все транспозиции рёбер вида $\tau_{12}$, то орбита элемента $g_2$ под действием $H$ сопряжениями содержит все 11 элементов, задающих ориентацию $1 \in \mathbb{Z}_2$ любой паре рёбер, одно из которых ребро 45, в "своих" ячейках, одна из которых ячейка 45. Эти 11 элементов уже непосредственно, то есть без всякой на то помощи от $H$, порождают всевозможные ориентации рёбер. Точнее сказать, мы можем придать любым "угодным" нам 11 рёбрам любую "угодную" нам ориентацию. Лишь оставленное нами 12-ое ребро будет иметь уже вынужденную, определённую нашим выбором ориентации, ориентацию.

Элемент $g_3$ уже был нами указан. Это тот самый элемент-суффикс, "удлиняющий" $h_2$. Однако, мы для разнообразия укажем другой.

$$g_3 := (231133322244)^2.^7$$

Вершинный элемент $g_3$ задаёт ориентацию $1 \in \mathbb{Z}_3$ неориентированной вершине 543 в ячейке 543 и "противоположную" ориентацию $-1 \in \mathbb{Z}_3$ неориентированной вершине 240 в ячейке 240.

Так как подгруппа $H \leq G$ содержит все транспозиции вершин вида $\tau_8$, то орбита элемента $g_3$ под действием $H$ сопряжениями содержит все 7 элементов, ориентирующих вершинные пары содержащие вершину 543, в "своих" ячейках, и задающих вершине 543 ориентацию $1 \in \mathbb{Z}_3$ в ячейке 543. Эти 7 элементов, уже непосредственно, порождают всевозможные ориентации вершин. Точнее сказать, мы можем придать любым "угодным" нам 7 вершинам любую "угодную" нам ориентацию. Лишь оставленная нами 8-ая вершина будет иметь уже вынужденную, определённую нашим выбором ориентации, ориентацию.

Так как две подгруппы, порожденные орбитой рёберного $g_2$ и орбитой вершинного $g_3$, соответственно, перескаются тривиально, а орбиты $g_2$ и $g_3$, в своей совокупности, содержат все порождающие подгруппы $N$, мы можем считать теорему (3.2) доказанной. $\square$

## 3.3 Структура группы Рубика $G$

Теорема 3.3 *Группа Рубика $G$ изоморфна группе* $(\mathbb{Z}_2^{11} \times \mathbb{Z}_3^7) \rtimes ((A_{12} \times A_8) \rtimes \mathbb{Z}_2)$.

Доказательство Вся работа, необходимая для доказательства этой итоговой теоремы, уже была проделана нами. Мы выделили две группы – $H = (A_{12} \times A_8) \rtimes \mathbb{Z}_2$ и $N = \mathbb{Z}_2^{11} \times \mathbb{Z}_3^7$; и доказали, что $N \trianglelefteq G$ (теорема (3.2)) и что $H \leq G$ (теорема (3.1)). Нам также известно, что пересечение $N \cap H$ есть тривиальная подгруппа $G$ – подгруппа $G$, состоящая из одного единственного единичного элемента, и что $N \rtimes H$ порождает группу $G$. Мы вправе писать

$$G = (\mathbb{Z}_2^{11} \times \mathbb{Z}_3^7) \rtimes ((A_{12} \times A_8) \rtimes \mathbb{Z}_2),$$

и считать теорему (3.3) доказанной. $\square$

[7] По-видимому, это единственное преобразование, получившее имя Рубика – имя самого изобретателя кубика Рубика.

# 4 Заключение

## 4.1 Три элемента, порождающих группу Рубика

Из предыдущего раздела "Группа Рубика $G$" мы приходим к выводу, что группа Рубика порождается элементами – $h_2$, $h_7$, $h_{11}$, $g_2$ и $g_3$. Зная структуру группы Рубика, мы далее выводим следующие тождества:

$$(h_7 g_2)^2 = h_7^2, \ \ (h_7 g_2)^7 = g_2,$$
$$(h_{11} g_3)^3 = h_{11}^3, \ \ (h_{11} g_3)^{11} = g_3^2.$$

А следовательно, группа Рубика порождается тремя элементами – $h_2$, $h_7 g_2$ и $h_{11} g_3$.

## 4.2 Элемент группы Рубика максимального порядка

Максимальным порядком элемента группы Рубика $G$ является $1260 = 6 \cdot 210 = 2^2 \cdot 3^2 \cdot 5 \cdot 7$. Обозначим такой элемент как $g_{1260}$. Проекцией элемента $g_{1260}$ является элемент $\pi(g_{1260})$ группы $\pi(G)$ порядка $210 = 2 \cdot 3 \cdot 5 \cdot 7$, причём $\pi(g_{1260})$ "обязан" содержать рёберную транспозицию и вершинный 3-цикл. Таким образом, $\pi(g_{1260})$ является произведением независимых двух рёберных транспозиций, рёберного цикла длиной 7 и двух вершинных циклов длиной 3 и 5. Приведём пример элемента $g_{1260}$, найденного с помощью ЭВМ Д. Батлером:

$$g_{1260} = 1110035553.$$

Указанный элемент $g_{1260}$ переводит начальную позицию

(01 12 20 23 34 42 45 50 04 53 31 15 012 234 450 531 240 105 321 543)

в позицию

(04 13 50 53 51 42 02 01 21 23 45 34 045 321 024 213 012 354 234 315),

что соответствует следующему произведению циклов:

(105 354 531 213 342 510 435 153 321 234 051 543 315 132 423)(012 240 504 201 024 450 120 402 045)
(01 50 20 54 13 12 40 10 05 02 45 31 21 04)(15 43 51 34)(23 53).

В журнале Наука и Жизнь, № 10, 1985 года, И.З. Атнабаев сообщил, что нашёл вручную, без ЭВМ, другой элемент. Назовём его $g_{210}$.

$$g_{210} = 111042.$$

К сожалению, его пример оказался ошибочным. Элемент $g_{210}$ не является элементом порядка 1260, а элементом порядка 210. Верь или проверь.

## Обозначения

| | |
|---|---|
| $:=$ | определение (если $A$ определяет $B$, то будем писать $B := A$ или $A =: B$ – двоеточие со стороны определяемого); |
| $A \times B$ | прямое, то есть декартово, произведение A и B; |
| $A \cap B$ | пересечение A и B, то есть совокупность элементов, содержащихся и в A, и в B; |
| $\sigma \in A$ | $\sigma$ – элемент, содержащийся в $A$; |
| $\lvert A \rvert$ | мощность множества $A$, то есть число его элементов (во всех рассматриваемых нами случаях это число конечное); |
| $\mathbb{N}$ | множество натуральных чисел; |
| $\mathbb{Z}_n$ | группа вычетов по модулю $n$, $n$ – натуральное; |
| $S_n$ | группа перестановок $n$ символов, $n$ – натуральное; |
| $A_n$ | подгруппа чётных перестановок группы $S_n$; |
| $(i_1 i_2 \dots i_k)$ | $k$-цикл, то есть циклическая перестановка символов: $i_j \mapsto i_{j+1}$, $1 \leq j \leq k-1$, и $i_k \mapsto i_1$; |
| $e_n$ | единичный элемент группы $S_n$, то есть её тривиальная перестановка, фиксирующая все $n$ символов; |
| $\tau_n$ | особая транспозиция – транспозиция вида $(i\,\cdot) \in S_n$, $1 \leq i \leq n$, $i$ – фиксирован, то есть транспозиция, переставляющая заданный символ $i$ с другим символом (перестановка $(i\,i)$ не запрещается, то есть тривиальная перестановка $e_n$ является перестановкой вида $\tau_n$, каковым бы ни был задан символ $i$); |
| $P(n)$ | число разбиений числа $n$ на суммы натуральных чисел – оно же число классов сопряжённости группы $S_n$; |
| $P_k(n)$ | число разбиений числа $n$ на суммы натуральных чисел, не меньших $k$, $k$ – натуральное; |
| $[G : H]$ | индекс подгруппы $H$ в группе $G$ ($H$, разумеется, не обязана быть нормальной подгруппой группы $G$); |
| $\mathrm{Ker}(\pi)$ | ядро отображения $\pi$, то есть прообраз единичного элемента отображения $\pi$; |
| $H \leq G$ | $H$ – подгруппа (не обязательно собственная) группы $G$; |
| $N \trianglelefteq G$ | $N$ – нормальная подгруппа группы $G$; |
| $G/N$ | факторгруппа группы $G$, факторизованной по её нормальной подгруппе $N$; |
| $N \rtimes H$ | полупрямое произведение групп N и H, при том, что $N \trianglelefteq N \rtimes H$; |
| $\square$ | доказательство завершено. |