

## §10. Группы

**10.1. Группы, подгруппы, циклы.** Множество  $G$  называется *группой*, если на нём задана операция композиции  $G \times G \rightarrow G, (g_1, g_2) \mapsto g_1 g_2$  со свойствами

$$\text{ассоциативность:} \quad \forall f, g, h \in G \quad (fg)h = f(gh) \quad (10-1)$$

$$\text{наличие единицы:} \quad \exists e \in G : \forall g \in G \quad eg = g \quad (10-2)$$

$$\text{наличие обратных:} \quad \forall g \in G \quad \exists g^{-1} \in G : g^{-1}g = e \quad (10-3)$$

Группа называется *коммутативной* или *абелевой*, если дополнительно имеет место

$$\text{коммутативность:} \quad \forall f, g \in G \quad fg = gf. \quad (10-4)$$

Левый обратный к  $g$  элемент  $g^{-1}$  из (10-3) является также и правым обратным, т. е.  $gg^{-1} = e$ , что устанавливается умножением правой и левой части в  $g^{-1}gg^{-1} = eg^{-1} = g^{-1}$  слева на левый обратный к  $g^{-1}$  элемент.

УПРАЖНЕНИЕ 10.1. Убедитесь, что обратный к  $g$  элемент  $g^{-1}$  однозначно определяется элементом  $g$  и что  $(g_1 \dots g_k)^{-1} = g_k^{-1} \dots g_1^{-1}$ .

Для единицы  $e$  из (10-2) при любом  $g \in G$  выполняются также и равенство  $ge = g$ , поскольку  $ge = g(g^{-1}g) = (gg^{-1})g = eg = g$ .

УПРАЖНЕНИЕ 10.2. Убедитесь, что единичный элемент  $e \in G$  единствен.

Если группа  $G$  конечна, число элементов в ней обозначается  $|G|$  и называется *порядком* группы  $G$ . Подмножество  $H \subset G$  называется *подгруппой*, если оно образует группу относительно имеющейся в  $G$  композиции. Для этого достаточно, чтобы вместе с каждым элементом  $h \in H$  в  $H$  лежал и обратный к нему элемент  $h^{-1}$ , а вместе с каждой парой элементов  $h_1, h_2 \in H$  — их произведение  $h_1 h_2$ . Единичный элемент  $e \in G$  автоматически окажется в  $H$ , т. к.  $e = hh^{-1}$  для произвольного  $h \in H$ .

УПРАЖНЕНИЕ 10.3. Проверьте, что пересечение любого множества подгрупп является подгруппой.

ПРИМЕР 10.1 (ГРУППЫ ПРЕОБРАЗОВАНИЙ)

Модельными примерами групп являются *группы преобразований*, обсуждавшиеся нами в н° 0.6. Все взаимно однозначные отображения произвольного множества  $X$  в себя очевидно образуют группу. Она обозначается  $\text{Aut } X$  и называется *группой автоморфизмов* множества  $X$ . Подгруппы  $G \subset \text{Aut } X$  называются *группами преобразований* множества  $X$ . Для  $g \in G$  и  $x \in X$  мы часто будем сокращать обозначение  $g(x)$  до  $gx$ . Группа всех автоморфизмов  $n$ -элементного множества  $X = \{1, \dots, n\}$  называется  *$n$ -той симметрической группой* и обозначается  $S_n$ . Порядок  $|S_n| = n!$ . Чётные перестановки образуют в  $S_n$  подгруппу, обозначаемую  $A_n$  и часто называемую *знакопеременной группой*. Порядок  $|A_n| = n!/2$ .

**10.1.1. Циклические группы и подгруппы.** Наименьшая по включению подгруппа в  $G$ , содержащая заданный элемент  $g \in G$ , состоит из всевозможных целых степеней  $g^m$  элемента  $g$ , где мы, как обычно, полагаем  $g^0 \stackrel{\text{def}}{=} e$  и  $g^{-n} \stackrel{\text{def}}{=} (g^{-1})^n$ . Она называется *циклической подгруппой*, порождённой  $g$ , и обозначается  $\langle g \rangle$ . Группа  $\langle g \rangle$  абелева и является образом сюръективного гомоморфизма абелевых групп  $\varphi_g : \mathbb{Z} \rightarrow \langle g \rangle, m \mapsto g^m$ , который переводит сложение в композицию. Если  $\ker \varphi_g \neq 0$ , то  $\ker \varphi_g = (n)$  и  $\langle g \rangle \simeq \mathbb{Z}/(n)$ , где  $n \in \mathbb{N}$  — наименьшая степень, для которой  $g^n = e$ . Она называется *порядком* элемента  $g$  и обозначается  $\text{ord}(g)$ . В этом случае

группа  $\langle g \rangle$  имеет порядок<sup>1</sup>  $n = \text{ord } g$  и состоит из элементов  $e = g^0, g = g^1, g^2, \dots, g^{n-1}$ . Если  $\ker \varphi_g = 0$ , то  $\varphi_g : \mathbb{Z} \xrightarrow{\simeq} \langle g \rangle$  является изоморфизмом и все степени  $g^m$  попарно различны. В этом случае говорят, что  $g$  имеет *бесконечный порядок* и пишут  $\text{ord } g = \infty$ .

Напомним<sup>2</sup>, что группа  $G$  называется *циклической*, если в ней есть такой элемент  $g \in G$ , что все элементы группы являются его целыми степенями, т. е.  $G = \langle g \rangle$ . Элемент  $g$  называется в этом случае *образующей* циклической группы  $G$ . Например, аддитивная группа целых чисел  $\mathbb{Z}$  циклическая, и её образующей является любая из элементов  $\pm 1$ . Согласно сл. 2.3 на стр. 52, всякая конечная подгруппа мультипликативной группы любого поля циклическая. Аддитивная группа вычетов  $\mathbb{Z}/(10)$  тоже циклическая, и её образующей является любая из четырёх классов<sup>3</sup>  $[\pm 1]_6, [\pm 3]_6$ .

УПРАЖНЕНИЕ 10.4. Укажите необходимые и достаточные условия для того, чтобы конечно порождённая абелева группа<sup>4</sup>  $G = \mathbb{Z}^r \oplus \mathbb{Z}/(p_1^{n_1}) \oplus \dots \oplus \mathbb{Z}/(p_\alpha^{n_\alpha})$  была циклической.

ЛЕММА 10.1

Элемент  $h = g^k$  тогда и только тогда является образующей циклической группы  $\langle g \rangle$  порядка  $n$ , когда  $\text{нод}(k, n) = 1$ .

Доказательство. Так как  $\langle h \rangle \subset \langle g \rangle$ , равенство  $\langle h \rangle = \langle g \rangle$  равносильно неравенству  $\text{ord } h \geq n$ . Если  $h^m = g^{mk} = e$ , то  $n \mid mk$ . При  $\text{нод}(n, k) = 1$  мы заключаем, что  $n \mid m$ , откуда  $m \geq n$  и, в частности,  $\text{ord } h \geq n$ . Если же  $n = n_1 d$  и  $k = k_1 d$ , где  $d > 1$ , то  $h^{n_1} = g^{k n_1} = g^{n k_1} = e$  и  $\text{ord } h \leq n_1 < n$ .  $\square$

**10.1.2. Разложение перестановок в композиции циклов.** Перестановка  $\tau \in S_n$  по кругу переводящая друг в друга какие-нибудь  $m$  различных элементов<sup>5</sup>

$$i_1 \mapsto i_2 \mapsto \dots \mapsto i_{m-1} \mapsto i_m \mapsto i_1 \quad (10-5)$$

и оставляющая на месте все остальные элементы, называется *циклом* длины  $m$ .

УПРАЖНЕНИЕ 10.5. Покажите, что  $k$ -тая степень цикла длины  $m$  является циклом тогда и только тогда, когда  $\text{нод}(k, m) = 1$ .

Цикл (10-5) часто бывает удобно обозначать  $\tau = |i_1, \dots, i_m\rangle$ , не смотря на то, что один и тот же цикл (10-5) допускает  $m$  различных таких записей, получающихся друг из друга циклическими перестановками элементов.

УПРАЖНЕНИЕ 10.6. Сколько имеется в  $S_n$  различных циклов длины  $k$ ?

ТЕОРЕМА 10.1

Каждая перестановка  $g \in S_n$  является композицией  $g = \tau_1 \dots \tau_k$  непересекающихся и, стало быть, попарно коммутирующих друг с другом циклов, причём такое разложение единственно с точностью до перестановки циклов.

<sup>1</sup>Таким образом, порядок элемента равен порядку порождённой им циклической подгруппы.

<sup>2</sup>См. п° 2.5.1 на стр. 51.

<sup>3</sup>Обратите внимание, что никакой из шести оставшихся классов образующей не являются.

<sup>4</sup>См. теор. 7.1 на стр. 119.

<sup>5</sup>Числа  $i_1, \dots, i_m$  могут быть любыми, не обязательно соседними или возрастающими.

Доказательство. Поскольку множество  $X = \{1, \dots, n\}$  конечно, в последовательности

$$x \xrightarrow{g} g(x) \xrightarrow{g} g^2(x) \xrightarrow{g} g^3(x) \xrightarrow{g} \dots, \quad (10-6)$$

возникающей при применении  $g$  к произвольной точке  $x \in X$ , случится повтор. Так как преобразование  $g : X \rightarrow X$  биективно, первым повторившимся элементом будет стартовый элемент  $x$ . Таким образом, каждая точка  $x \in X$  под действием  $g$  движется по циклу. В силу биективности  $g$  два таких цикла, проходящие через различные точки  $x$  и  $y$ , либо не пересекаются, либо совпадают. Таким образом, перестановка  $g$  является произведением непересекающихся циклов, очевидно, перестановочных друг с другом.  $\square$

УПРАЖНЕНИЕ 10.7. Покажите, что два цикла  $\tau_1, \tau_2 \in S_n$  перестановочны ровно в двух случаях: когда они не пересекаются или когда  $\tau_2 = \tau_1^s$  и оба цикла имеют одинаковую длину, взаимно простую с  $s$ .

ОПРЕДЕЛЕНИЕ 10.1 (цикловой тип перестановки)

Написанный в порядке нестрогого убывания набор длин непересекающихся циклов<sup>1</sup>, в которые раскладывается перестановка  $g \in S_n$ , называется *цикловым типом* перестановки  $g$  и обозначается  $\lambda(g)$ .

Цикловой тип перестановки  $g \in S_n$  удобно изображать  $n$ -клеточной диаграммой Юнга, а сами циклы записывать по строкам этой диаграммы. Например, перестановка

$$g = (6, 5, 4, 1, 8, 3, 9, 2, 7) = |1, 6, 3, 4\rangle |2, 5, 8\rangle |7, 9\rangle = \begin{array}{|c|c|c|c|} \hline 1 & 6 & 3 & 4 \\ \hline 2 & 5 & 8 & \\ \hline 7 & 9 & & \\ \hline \end{array}$$

имеет цикловой тип  $\begin{array}{|c|c|c|c|} \hline & & & \\ \hline \end{array}$ , т. е.  $\lambda(6, 5, 4, 1, 8, 3, 9, 2, 7) = (4, 3, 2)$ . Единственной перестановкой циклового типа  $\lambda = (1, \dots, 1)$  (один столбец высоты  $n$ ) является тождественная перестановка Id. Диаграмму  $\lambda = (n)$  (одна строка длины  $n$ ) имеют  $(n-1)!$  циклов максимальной длины  $n$ .

УПРАЖНЕНИЕ 10.8. Сколько перестановок в симметрической группе  $S_n$  имеют заданный цикловой тип, содержащий для каждого  $i = 1, \dots, n$  ровно  $m_i$  циклов длины  $i$ ?

ПРИМЕР 10.2 (вычисление порядка и знака перестановки)

Порядок перестановки  $g \in S_n$  равен наименьшему общему кратному длин непересекающихся циклов, из которых она состоит. Например, порядок перестановки

$$(3, 12, 7, 9, 10, 4, 11, 1, 6, 2, 8, 5) = |1, 3, 7, 11, 8\rangle |2, 12, 5, 10\rangle |4, 9, 6\rangle \in S_{12}$$

равен  $5 \cdot 4 \cdot 3 = 60$ . По правилу ниточек из прим. 8.1 на стр. 128 знак цикла длины  $\ell$  равен  $(-1)^{\ell-1}$ . Поэтому перестановка чётна тогда и только тогда, когда у неё чётное число циклов чётной длины.

УПРАЖНЕНИЕ 10.9. Найдите чётность  $g = (6, 5, 4, 1, 8, 3, 9, 2, 7) \in S_9$  и вычислите  $g^{15}$ .

<sup>1</sup>Включая циклы длины один, отвечающие элементам, которые перестановка оставляет на месте.

**10.2. Группы фигур.** Для любой фигуры  $\Phi$  в евклидовом<sup>1</sup> пространстве  $\mathbb{R}^n$  биективные отображения  $\Phi \rightarrow \Phi$  индуцированные ортогональными<sup>2</sup> линейными преобразованиями пространства  $\mathbb{R}^n$ , переводящими фигуру  $\Phi$  в себя, образуют группу преобразований фигуры  $\Phi$ . Эта группа называется *полной группой фигуры  $\Phi$*  и обозначается  $O_\Phi$ . Подгруппу  $SO_\Phi \subset O_\Phi$ , состоящую из биекций, индуцированных собственными<sup>3</sup> ортогональными операторами  $\mathbb{R}^n \rightarrow \mathbb{R}^n$ , мы будем называть *собственной группой фигуры  $\Phi$* . Если фигура  $\Phi \subset \mathbb{R}^n$  содержится в некоторой гиперплоскости  $\Pi \subset \mathbb{R}^n$ , то собственная группа фигуры  $\Phi$  совпадает с полной: беря композицию любого несобственного движения из группы фигуры с отражением в плоскости  $\Pi$ , мы получаем собственное движение, которое действует на фигуру  $\Phi$  точно также, как и исходное несобственное движение.

УПРАЖНЕНИЕ 10.10. Изготовьте модели пяти *платоновых тел* — тетраэдра, октаэдра, куба, додекаэдра и икосаэдра, см. рис. 10◊5 – рис. 10◊8 на стр. 172 – 173.

ПРИМЕР 10.3 (группы диэдров  $D_n$ )

Группа правильного плоского  $n$ -угольника, лежащего в пространстве  $\mathbb{R}^3$  так, что его центр находится в нуле, обозначается  $D_n$  и называется  *$n$ -той группой диэдра*. Простейший диэдр — *двуугольник* — возникает при  $n = 2$ . Его можно представлять себе как вытянутую симметричную луночку с двумя сторонами, изображённую на рис. 10◊1. Группа  $D_2$  такой луночки совпадает с группами описанного вокруг неё прямоугольника и вписанного в неё ромба<sup>4</sup>. Она состоит из тождественного отображения и трёх поворотов на  $180^\circ$  вокруг перпендикулярных друг другу осей, одна из которых проходит через вершины луночки, другая — через середины её сторон, а третья перпендикулярна плоскости луночки и проходит её центр.

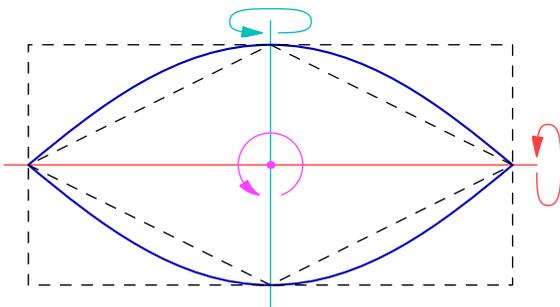


Рис. 10◊1. Двуугольник  $D_2$ .

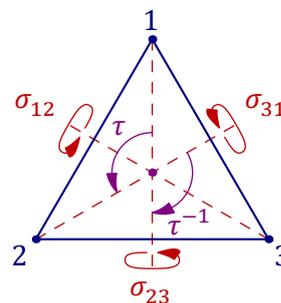


Рис. 10◊2. Группа треугольника.

УПРАЖНЕНИЕ 10.11. Убедитесь, что  $D_2 \simeq \mathbb{Z}/(2) \oplus \mathbb{Z}/(2)$ .

<sup>1</sup>Напомним, что *евклидовость* означает фиксацию в векторном пространстве  $\mathbb{R}^n$  симметричного билинейного положительного скалярного произведения  $V \times V \rightarrow \mathbb{R}$ , обозначаемого  $(v, w)$ , см. лекцию [http://http://gorod.bogomolov-lab.ru/ps/stud/geom\\_ru/2122/lec\\_03.pdf](http://http://gorod.bogomolov-lab.ru/ps/stud/geom_ru/2122/lec_03.pdf).

<sup>2</sup>Линейный оператор  $F : \mathbb{R}^n \rightarrow \mathbb{R}^n$  на евклидовом пространстве  $\mathbb{R}^n$  называется *ортогональным*, если он сохраняет скалярное произведение, т. е.  $\forall v, w \in \mathbb{R}^n (Fv, Fw) = (v, w)$  (достаточно, чтобы это равенство выполнялось при  $v = w$ ), см. лекцию [http://http://gorod.bogomolov-lab.ru/ps/stud/geom\\_ru/2122/lec\\_11.pdf](http://http://gorod.bogomolov-lab.ru/ps/stud/geom_ru/2122/lec_11.pdf).

<sup>3</sup>Т. е. сохраняющими ориентацию или, что то же самое, с определителем 1, см. раздел 10.2.1 на стр. 133 лекции [http://http://gorod.bogomolov-lab.ru/ps/stud/geom\\_ru/2122/lec\\_10.pdf](http://http://gorod.bogomolov-lab.ru/ps/stud/geom_ru/2122/lec_10.pdf).

<sup>4</sup>Мы предполагаем, что луночка такова, что оба они не квадраты.

Следующая диэдральная группа — группа треугольника  $D_3$  — состоит из шести движений: тождественного, двух поворотов  $\tau$ ,  $\tau^{-1}$  на  $\pm 120^\circ$  вокруг центра треугольника и трёх осевых симметрий  $\sigma_{ij}$  относительно его медиан (см. рис. 10◊2). Так как движение плоскости однозначно задаётся своим действием на вершины треугольника, группа треугольника  $D_3$  изоморфна группе перестановок  $S_3$  его вершин. При этом повороты на  $\pm 120^\circ$  отождествляются с циклическими перестановками  $(2, 3, 1)$ ,  $(3, 1, 2)$ , а осевые симметрии — с транспозициями  $\sigma_{23} = (1, 3, 2)$ ,  $\sigma_{13} = (3, 2, 1)$ ,  $\sigma_{12} = (2, 1, 3)$ . Поскольку движение плоскости, переводящее в себя правильный  $n$ -угольник, однозначно определяется своим действием на аффинный репер, образованный какой-нибудь вершиной и примыкающей к ней парой сторон, группа диэдра  $D_n$  при каждом  $n \geq 2$  состоит из  $2n$  движений: выбранную вершину можно перевести в любую из  $n$  вершин, после чего одним из двух возможных способов совместить рёбра. Эти  $2n$  движений суть  $n$  поворотов вокруг центра многоугольника на углы  $^1 2\pi k/n$  с  $k = 0, 1, \dots, (n-1)$  и  $n$  осевых симметрий<sup>2</sup> относительно прямых, проходящих при нечётном  $n$  через вершину и середину противоположной стороны, а при чётном  $n$  — через пары противоположных вершин и через середины противоположных сторон (см. рис. 10◊3).

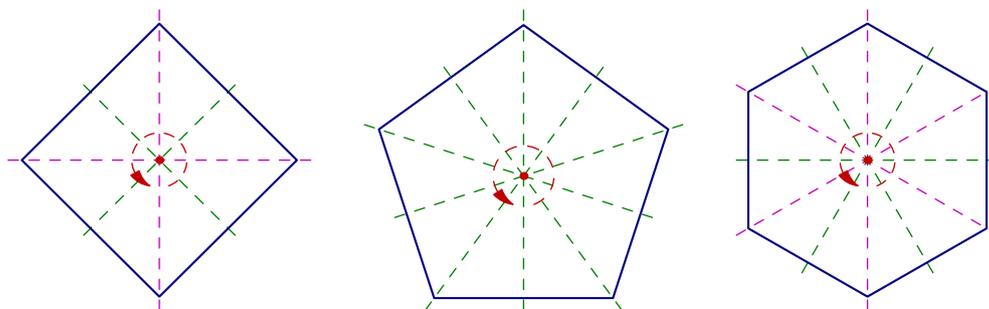


Рис. 10◊3. Оси диэдров  $D_4$ ,  $D_5$  и  $D_6$ .

УПРАЖНЕНИЕ 10.12. Составьте таблицы умножения в группах  $D_3$ ,  $D_4$  и  $D_5$ , аналогичные таблице из форм. (0-23) на стр. 13.

#### ПРИМЕР 10.4 (ГРУППА ТЕТРАЭДРА)

Поскольку каждое движение трёхмерного евклидова пространства  $\mathbb{R}^3$  однозначно задаётся своим действием на вершины правильного тетраэдра и это действие может быть произвольным, полная группа правильного тетраэдра с центром в нуле изоморфна группе  $S_4$  перестановок его вершин и состоит из 24 движений. Собственная группа состоит из  $12 = 4 \cdot 3$  движений: поворот тетраэдра однозначно задаётся своим действием на аффинный репер, образованный какой-нибудь вершиной и тремя выходящими из неё рёбрами, и может переводить эту вершину в любую из четырёх вершин, после чего остаются ровно три возможности для совмещения рёбер, сохраняющего ориентацию пространства. Полный список всех собственных движений тетраэдра таков: тождественное,  $4 \cdot 2 = 8$  поворотов на углы  $\pm 120^\circ$  вокруг прямых, проходящих через вершину и центр противоположной грани, а также 3 поворота на  $180^\circ$  вокруг прямых, проходящих через середины противоположных рёбер. В несобственной группе, помимо перечисленных поворотов, имеется 6 отражений  $\sigma_{ij}$  в плоскостях, проходящих через середину ребра  $[i, j]$  и противоположное ребро, см. рис. 10◊4.

<sup>1</sup>При  $k = 0$  получается тождественное преобразование.

<sup>2</sup>Или, что то же самое, поворотов на  $180^\circ$  в пространстве.

При изоморфизме с  $S_4$  отражение  $\sigma_{ij}$  переходит в транспозицию букв  $i$  и  $j$ , повороты на  $\pm 120^\circ$ , представляющие собой всевозможные композиции  $\sigma_{ij}\sigma_{jk}$  с попарно разными  $i, j, k$ , переходят в циклические перестановки букв  $i, j, k$ , три вращения на  $180^\circ$  относительно осей, соединяющих середины противоположных рёбер, — в одновременные транспозиции непересекающихся пар букв:  $\sigma_{12}\sigma_{34} = (2, 1, 4, 3)$ ,  $\sigma_{13}\sigma_{24} = (3, 4, 1, 2)$ ,  $\sigma_{14}\sigma_{23} = (4, 3, 2, 1)$ .

УПРАЖНЕНИЕ 10.13. Убедитесь, что вместе с тождественным преобразованием эти три поворота образуют группу двугольника  $D_2$ .

Оставшиеся шесть несобственных преобразований тетраэдра отвечают шести циклическим перестановкам вершин  $\{1234\}$ ,  $\{1243\}$ ,  $\{1324\}$ ,  $\{1342\}$ ,  $\{1423\}$ ,  $\{1432\}$  и реализуются поворотами на  $\pm 90^\circ$  относительно прямых, проходящих через середины противоположных рёбер с последующим отражением в плоскости, проходящей через центр тетраэдра и перпендикулярной оси поворота.

УПРАЖНЕНИЕ 10.14. Выразите эти 6 движений через отражения  $\sigma_{ij}$ .

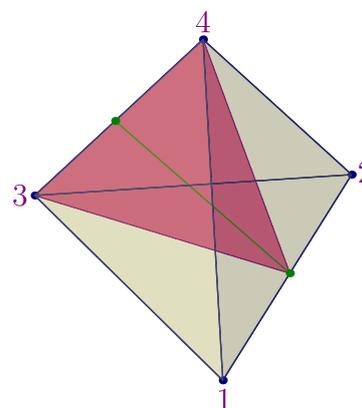


Рис. 10◊4. Зеркало отражения  $\sigma_{12}$  и ось поворота на  $180^\circ$ .

ПРИМЕР 10.5 (ГРУППА ДОДЕКАЭДРА)

Как и для тетраэдра, всякое вращение додекаэдра однозначно задаётся своим действием на аффинный репер, образованный вершиной и тремя выходящими из неё рёбрами, и может переводить эту вершину в любую из 20 вершин, а затем тремя способами совмещать рёбра с сохранением ориентации. Поэтому собственная группа додекаэдра (см. рис. 10◊5) состоит из  $20 \cdot 3 = 60$  движений:  $6 \cdot 4 = 24$  поворотов на углы  $2\pi k/5$ ,  $1 \leq k \leq 4$ , вокруг осей, проходящих через центры противоположных граней додекаэдра,  $10 \cdot 2 = 20$  поворотов на углы  $\pm 2\pi/3$  вокруг осей, проходящих через противоположные вершины, 15 поворотов на  $180^\circ$  вокруг осей, проходящих через середины противоположных рёбер, и тождественного преобразования. Полная группа додекаэдра состоит из  $20 \cdot 6 = 120$  движений и помимо перечисленных 60 поворотов содержит их композиции с центральной симметрией относительно центра додекаэдра.

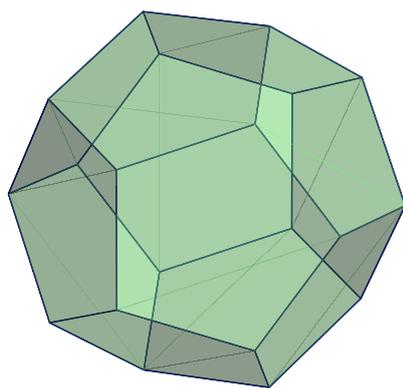


Рис. 10◊5. Додекаэдр.

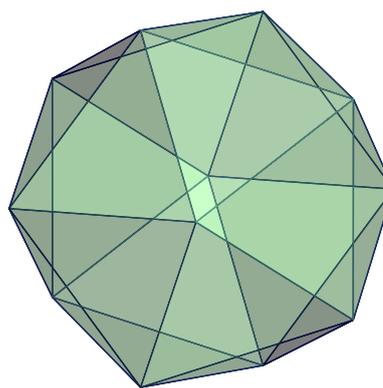


Рис. 10◊6. Икосаэдр.

УПРАЖНЕНИЕ 10.15. Покажите что полные группы куба, октаэдра и икосаэдра состоят, соответственно из 48, 48 и 120 движений, а собственные — из 24, 24 и 60 поворотов.

**10.3. Гомоморфизмы групп.** Отображение групп  $\varphi : G_1 \rightarrow G_2$  называется *гомоморфизмом*, если оно переводит композицию в композицию, т. е. для любых  $g, h \in G_1$  в группе  $G_2$  выполняется соотношение  $\varphi(gh) = \varphi(g)\varphi(h)$ . Термины *эпиморфизм*, *моморфизм* и *изоморфизм* применительно к отображению групп всегда подразумевают по умолчанию, что это отображение является *гомоморфизмом* групп.

УПРАЖНЕНИЕ 10.16. Убедитесь, что композиция гомоморфизмов тоже является гомоморфизмом.

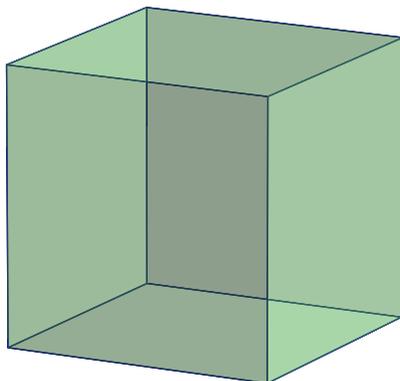


Рис. 10◊7. Куб.

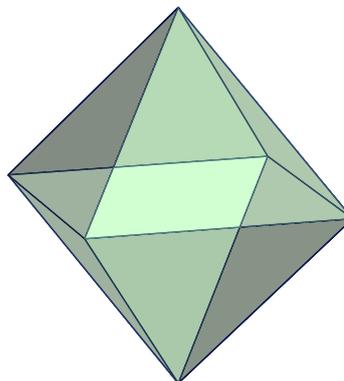


Рис. 10◊8. Октаэдр.

Каждый гомоморфизм групп  $\varphi : G_1 \rightarrow G_2$  переводит единицу  $e_1$  группы  $G_1$  в единицу  $e_2$  группы  $G_2$ : равенство  $\varphi(e_1) = e_2$  получается из равенств  $\varphi(e_1)\varphi(e_1) = \varphi(e_1e_1) = \varphi(e_1)$  умножением правой и левой части на  $\varphi(e_1)^{-1}$ . Кроме того, для любого  $g \in G$  выполняется равенство  $\varphi(g^{-1}) = \varphi(g)^{-1}$ , так как  $\varphi(g^{-1})\varphi(g) = \varphi(g^{-1}g) = \varphi(e_1) = e_2$ . Поэтому образ

$$\text{im } \varphi \stackrel{\text{def}}{=} \varphi(G_1) \subset G_2$$

гомоморфизма групп является *подгруппой* группы  $G_2$ . Полный прообраз единицы  $e_2 \in G_2$  называется *ядром* гомоморфизма  $\varphi$  и обозначается

$$\ker \varphi \stackrel{\text{def}}{=} \varphi^{-1}(e_2) = \{g \in G_1 \mid \varphi(g) = e_2\}.$$

Это подгруппа в  $G_1$ , поскольку равенства  $\varphi(g) = \varphi(h) = e_2$  влекут равенства

$$\varphi(gh) = \varphi(g)\varphi(h) = e_2e_2 = e_2 \quad \text{и} \quad \varphi(g^{-1}) = \varphi(g)^{-1} = e_2^{-1} = e_2.$$

**Предложение 10.1**

Для любого гомоморфизма групп  $\varphi : G_1 \rightarrow G_2$  и каждого  $g \in G_1$  выполняются равенства

$$\varphi^{-1}(\varphi(g)) = g(\ker \varphi) = (\ker \varphi)g, \quad \text{где} \\ g(\ker \varphi) \stackrel{\text{def}}{=} \{gh \mid h \in \ker \varphi\} \quad \text{и} \quad (\ker \varphi)g \stackrel{\text{def}}{=} \{hg \mid h \in \ker \varphi\}.$$

В частности, все непустые слои  $\varphi$  находится в биекции с  $\ker \varphi$ .

**Доказательство.** Если  $\varphi(t) = \varphi(g)$ , то  $\varphi(tg^{-1}) = \varphi(t)\varphi(g)^{-1} = e$  и  $\varphi(g^{-1}t) = \varphi(g)^{-1}\varphi(t) = e$ , т. е.  $tg^{-1} \in \ker \varphi$  и  $g^{-1}t \in \ker \varphi$ . Поэтому  $t \in (\ker \varphi)g$  и  $t \in g(\ker \varphi)$ . Наоборот, для всех  $h \in \ker \varphi$  выполняются равенства  $\varphi(hg) = \varphi(h)\varphi(g) = \varphi(g)$  и  $\varphi(gh) = \varphi(g)\varphi(h) = \varphi(g)$ . Тем

самым, полный прообраз  $\varphi^{-1}(\varphi(g))$  элемента  $\varphi(g)$  совпадает и с  $(\ker \varphi)g$ , и с  $g(\ker \varphi)$ , а  $(\ker \varphi)g$  и  $g(\ker \varphi)$  совпадают друг с другом. Взаимно обратные биекции

$$\begin{array}{ccccc} & t \mapsto tg^{-1} & & h \mapsto gh & \\ (\ker \varphi)g & \xrightarrow{\quad} & \ker \varphi & \xrightarrow{\quad} & g(\ker \varphi) \\ & hg \mapsto h & & g^{-1}t \mapsto t & \end{array}$$

между ядром и слоем  $\varphi^{-1}(\varphi(g)) = (\ker \varphi)g = g(\ker \varphi)$  задаются правым и левым умножениями элементов ядра на  $g$ , а элементов слоя — на  $g^{-1}$ .  $\square$

#### Следствие 10.1

Для того, чтобы гомоморфизм групп  $\varphi : G_1 \rightarrow G_2$  был инъективен, необходимо и достаточно, чтобы его ядро исчерпывалось единичным элементом.  $\square$

#### Следствие 10.2

Для любого гомоморфизма конечных групп  $\varphi : G_1 \rightarrow G_2$  выполнено равенство

$$|\operatorname{im}(\varphi)| = |G_1| / |\ker(\varphi)|. \quad (10-7)$$

В частности,  $|\ker \varphi|$  и  $|\operatorname{im} \varphi|$  делят  $|G_1|$ .  $\square$

#### Пример 10.6 (знакопеременные группы)

Согласно [сл. 8.2](#) на стр. 128 имеется мультипликативный гомоморфизм  $\operatorname{sgn} : S_n \rightarrow \{\pm 1\}$ , сопоставляющий перестановке её знак. Ядро этого гомоморфизма  $\ker \operatorname{sgn} = A_n$  представляет собою группу чётных перестановок, имеющую порядок  $|A_n| = n!/2$ .

#### Пример 10.7 (линейные группы)

Все линейные автоморфизмы любого векторного пространства  $V$  над произвольным полем  $\mathbb{k}$  образуют *полную линейную группу*  $\operatorname{GL}(V)$ . В силу мультипликативности определителя<sup>1</sup> отображение

$$\det : \operatorname{GL}(V) \rightarrow \mathbb{k}^\times, \quad F \mapsto \det F, \quad (10-8)$$

является гомоморфизмом полной линейной группы в мультипликативную группу  $\mathbb{k}^\times$  поля  $\mathbb{k}$ . Его ядро называется *специальной линейной группой* и обозначается

$$\operatorname{SL}(V) = \ker \det = \{F : V \simeq V \mid \det F = 1\}.$$

Если поле  $\mathbb{k} = \mathbb{F}_q$  состоит из  $q$  элементов и  $\dim V = n$ , полная линейная группа конечна и

$$|\operatorname{GL}_n(\mathbb{F}_q)| = (q^n - 1)(q^n - q)(q^n - q^2) \dots (q^n - q^{n-1}),$$

**УПРАЖНЕНИЕ 10.17.** Убедитесь в этом.

Так как гомоморфизм (10-8) сюръективен<sup>2</sup> порядок специальной линейной группы

$$|\operatorname{SL}_n(\mathbb{F}_q)| = |\operatorname{GL}_n(\mathbb{F}_q)| / |\mathbb{k}^\times| = \frac{(q^n - 1)(q^n - q) \dots (q^n - q^{n-1})}{q - 1}.$$

<sup>1</sup>См. [предл. 8.2](#) на стр. 133.

<sup>2</sup>Диагональный оператор  $F$  с собственными числами  $(\lambda, 1, \dots, 1)$  имеет  $\det F = \lambda$ .

Пример 10.8 (проективные группы)

Напомним<sup>1</sup>, что с каждым векторным пространством  $V$  ассоциировано *проективное пространство*  $\mathbb{P}(V)$ , точками которого являются одномерные векторные подпространства в  $V$  или, что то же самое, классы пропорциональности ненулевых векторов в  $V$ . Каждый линейный оператор  $F \in \text{GL}(V)$  корректно задаёт биекцию  $\bar{F} : \mathbb{P}(V) \rightarrow \mathbb{P}(V)$ , переводящую класс вектора  $v \neq 0$  в класс вектора  $F(v)$ . Таким образом возникает гомоморфизм  $F \mapsto \bar{F}$  группы  $\text{GL}(V)$  в группу биективных преобразований проективного пространства  $\mathbb{P}(V)$ . Образ этого гомоморфизма обозначается  $\text{PGL}(V)$  и называется *проективной линейной группой* пространства  $V$ . Из курса геометрии известно, что два оператора  $F, G \in \text{GL}(V)$  тогда и только тогда задают одинаковые преобразования  $\bar{F} = \bar{G}$  проективного пространства  $\mathbb{P}(V)$ , когда они пропорциональны, т. е.  $F = \lambda G$  для некоторого  $\lambda \in \mathbb{k}^\times$ . Поэтому ядром эпиморфизма групп

$$\pi : \text{GL}(V) \twoheadrightarrow \text{PGL}(V), \quad F \mapsto \bar{F} \quad (10-9)$$

является *подгруппа гомотетий*  $\Gamma \simeq \mathbb{k}^\times$ , состоящая из скалярных диагональных операторов. Таким образом, группа  $\text{PGL}(V)$  образована классами пропорциональности линейных операторов. Классы пропорциональности операторов с единичным определителем образуют в ней подгруппу, обозначаемую  $\text{PSL}(V) \subset \text{PGL}(V)$ . Ограничивая эпиморфизм (10-9) на  $\text{SL}(V) \subset \text{GL}(V)$  получаем эпиморфизм

$$\pi' : \text{SL}(V) \twoheadrightarrow \text{PSL}(V), \quad F \mapsto \bar{F} \quad (10-10)$$

ядром которого является конечная мультипликативная подгруппа  $\mu_n(\mathbb{k}) \subset \mathbb{k}^\times$  содержащихся в поле  $\mathbb{k}$  корней степени<sup>2</sup>  $n = \dim V = \dim \mathbb{P}(V) + 1$  из единицы.

Пример 10.9 (эпиморфизм  $S_4 \twoheadrightarrow S_3$ )

На проективной плоскости  $\mathbb{P}_2$  над любым полем  $\mathbb{k}$  с каждой четвёркой точек  $a, b, c, d$ , никакие три из которых не коллинеарны связана фигура, образованная тремя парами проходящих через эти точки прямых<sup>3</sup>

$$(ab) \text{ и } (cd), \quad (ac) \text{ и } (bd), \quad (ad) \text{ и } (bc) \quad (10-11)$$

и называемая *четырёхвершинником*, см. рис. 10◊9. Пары прямых (10-11) называются *противоположными сторонами* четырёхвершинника. С четырёхвершинником  $abcd$  ассоциирован треугольник  $xyz$  с вершинами в точках пересечения пар противоположных сторон

$$x = (ab) \cap (cd), \quad y = (ac) \cap (bd), \quad z = (ad) \cap (bc) \quad (10-12)$$

Каждая перестановка вершин  $a, b, c, d$  однозначно определяет линейное проективное преобразование<sup>4</sup> плоскости, что даёт вложение  $S_4 \hookrightarrow \text{PGL}_3(\mathbb{k})$ . Преобразования из  $S_4$  переводят ассоци-

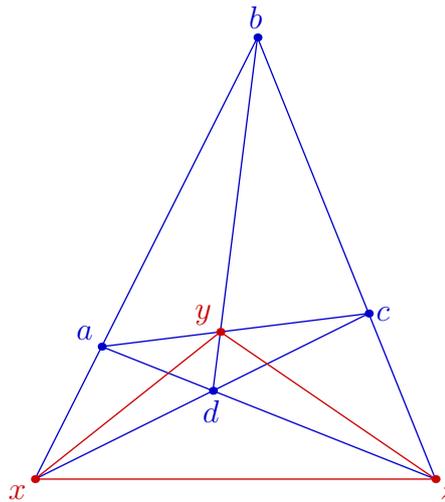


Рис. 10◊9. Четырёхвершинник и ассоциированный треугольник.

<sup>1</sup>Мы предполагаем, что читатель знаком с проективными пространствами и проективными преобразованиями по курсу геометрии, см. лекции [http://gorod.bogomolov-lab.ru/ps/stud/geom\\_ru/2122/lec\\_16.pdf](http://gorod.bogomolov-lab.ru/ps/stud/geom_ru/2122/lec_16.pdf) и [http://gorod.bogomolov-lab.ru/ps/stud/geom\\_ru/2122/lec\\_17.pdf](http://gorod.bogomolov-lab.ru/ps/stud/geom_ru/2122/lec_17.pdf).

<sup>2</sup>Напомним, что по определению  $\dim \mathbb{P}(V) \stackrel{\text{def}}{=} \dim V - 1$ .

<sup>3</sup>Они отвечают трём возможным способам разбить точки  $a, b, c, d$  на две пары.

<sup>4</sup>Напомним, что каждое линейное проективное преобразование  $\bar{F} \in \text{PGL}(V)$  однозначно определяется своим действием на любые  $\dim V + 1$  точек пространства  $\mathbb{P}(V)$ , никакие  $\dim V$  из которых не лежат в одной гиперплоскости.

ированный треугольник  $xuz$  в себя, переставляя его вершины  $x, y, z$  согласно формулам (10-12). Например, 3-цикл  $(b, c, a, d) \in S_4$  задаёт циклическую перестановку  $(y, z, x)$ , а транспозиции  $(b, a, c, d)$ ,  $(a, c, b, d)$  и  $(c, b, a, d)$  дают транспозиции  $(x, z, y)$ ,  $(y, x, z)$  и  $(z, y, x)$  соответственно. Таким образом, мы получаем сюръективный гомоморфизм  $S_4 \rightarrow S_3$ . Его ядро имеет порядок  $4!/3! = 4$  и состоит из тождественной перестановки и трёх пар независимых транспозиций  $(b, a, d, c)$ ,  $(c, d, a, b)$ ,  $(d, c, b, a)$ .

ПРИМЕР 10.10 ( $S_4$  И СОБСТВЕННАЯ ГРУППА КУБА)

Линейные преобразования евклидова пространства  $\mathbb{R}_3$ , составляющие собственную группу куба с центром в нуле, действуют на четырёх прямых  $a, b, c, d$ , соединяющих противоположные вершины куба, а также на трёх прямых  $x, y, z$ , соединяющих центры его противоположных граней, см. рис. 10◊10. На проективной плоскости  $\mathbb{P}_2 = \mathbb{P}(\mathbb{R}^3)$  эти 7 прямых становятся вершинами четырёхвершинника  $abcd$  и ассоциированного с ним треугольника  $xuz$ , как на рис. 10◊9. Поворот на  $180^\circ$  вокруг оси, соединяющей середины противоположных рёбер куба, меняет местами примыкающие к этому ребру диагонали и переводит в себя каждую из двух оставшихся диагоналей. Тем самым, вращения куба осуществляют транспозиции любых двух соседних диагоналей, и мы имеем сюръективный гомоморфизм  $SO_{\text{куб}} \rightarrow S_4$ . Так как обе группы имеют порядок 24, это изоморфизм. Он переводит 6 поворотов на  $\pm 90^\circ$  вокруг прямых  $x, y, z$  в 6 циклов длины 4 циклового типа  $\square\square\square\square$ , 3 поворота на  $180^\circ$  вокруг тех же прямых — в 3 пары независимых транспозиций циклового типа  $\square\square$ , 8 поворотов на  $\pm 120^\circ$  вокруг прямых  $a, b, c, d$  — в 8 циклов длины 3 циклового типа  $\square\square\square$ , а 6 поворотов на  $180^\circ$  вокруг осей, проходящих через середины противоположных рёбер — в 6 простых транспозиций циклового типа  $\square\square$ . Гомоморфизм  $SO_{\text{куб}} \rightarrow S_3$ , возникающий из действия группы куба на прямых  $x, y, z$ , согласован с изоморфизмом  $SO_{\text{куб}} \simeq S_4$  и эпиморфизмом  $S_4 \rightarrow S_3$  из предыдущего прим. 10.9. Его ядро состоит из собственных ортогональных преобразований евклидова пространства  $\mathbb{R}^3$ , переводящих в себя каждую из декартовых координатных осей  $x, y, z$  в  $\mathbb{R}^3$ , и совпадает, таким образом, с группой двуугольника  $D_2$  с осями  $x, y, z$ . В таком контексте эту группу иногда называют *четвертной группой Клейна* и обозначают  $V_4$ . Изоморфизм  $SO_{\text{куб}} \simeq S_4$  переводит её в ядро эпиморфизма  $S_4 \rightarrow S_3$  из прим. 10.9.

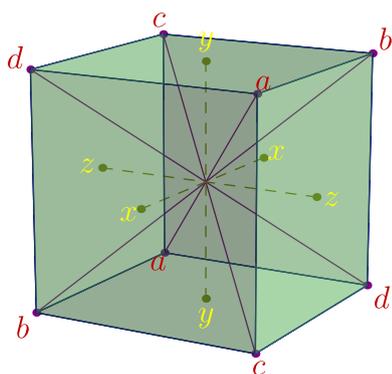


Рис. 10◊10. От куба к четырёхвершиннику.

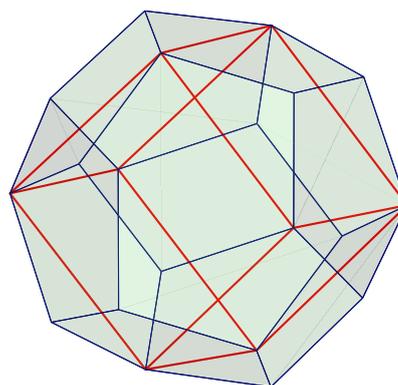


Рис. 10◊11. Один из пяти кубов на додекаэдре.

ПРИМЕР 10.11 (СОБСТВЕННАЯ ГРУППА ДОДЕКАЭДРА И  $A_5$ )

Любая диагональ любой грани додекаэдра единственным образом достраивается до лежащего на поверхности додекаэдра куба, образованного диагоналями граней так, что в каждой грани

рисуеться ровно одна диагональ<sup>1</sup>, как на рис. 10♦11. Всего таких кубов на поверхности додекаэдра имеется ровно пять, и они биективно соответствуют пяти диагоналям какой-нибудь фиксированной грани. Собственная группа додекаэдра переставляет эти кубы друг с другом, что даёт гомоморфизм собственной группы додекаэдра в симметрическую группу  $S_5$

$$\psi_{\text{дод}} : SO_{\text{дод}} \rightarrow S_5. \quad (10-13)$$

Глядя на модель додекаэдра, легко видеть, что образами  $20 \cdot 3 = 60$  поворотов, из которых состоит группа  $SO_{\text{дод}}$  являются 60 чётных перестановок: тождественное преобразование додекаэдра задаёт тождественную перестановку кубов;  $6 \cdot 4 = 24$  поворота на углы  $2\pi k/5$ ,  $1 \leq k \leq 4$ , вокруг осей, проходящих через центры противоположных граней, переходят во всевозможные циклы длины 5, т. е. в 24 перестановки циклового типа  $\square\square\square\square\square$ ;  $10 \cdot 2 = 20$  поворотов на углы  $\pm 2\pi/3$  вокруг осей, проходящих через противоположные вершины додекаэдра, переходят во всевозможные циклы длины 3, т. е. в 20 перестановок циклового типа  $\begin{smallmatrix} \square & \square & \square \\ & \square & \end{smallmatrix}$ ; 15 поворотов на  $180^\circ$  вокруг осей, проходящих через середины противоположных рёбер додекаэдра, переходят во всевозможные пары независимых транспозиций, т. е. в 10 перестановок циклового типа  $\begin{smallmatrix} \square & \square \\ \square & \square \end{smallmatrix}$ . Таким образом, гомоморфизм (10-13) является изоморфизмом собственной группы додекаэдра со знакопеременной подгруппой  $A_5 \subset S_5$ . В отличие от прим. 10.4 переход от собственной группы додекаэдра к полной не добавляет новых перестановок кубов, поскольку каждое несобственное движение является композицией собственного движения и центральной симметрии, которая переводит каждый из кубов в себя.

Упражнение 10.18. Покажите, что симметрическая группа  $S_5$  не изоморфна полной группе додекаэдра.

**10.4. Действие группы на множестве.** Пусть  $G$  — группа, а  $X$  — множество. Обозначим через  $\text{Aut}(X)$  группу всех взаимно однозначных отображений из  $X$  в себя. Гомоморфизм

$$\varphi : G \rightarrow \text{Aut}(X)$$

называется *действием* группы  $G$  на множестве  $X$  или *представлением* группы  $G$  автоморфизмами множества  $X$ . Отображение  $\varphi(g) : X \rightarrow X$ , отвечающее элементу  $g \in G$  при действии  $\varphi$  часто бывает удобно обозначать через  $\varphi_g : X \rightarrow X$ . Тот факт, что сопоставление  $g \mapsto \varphi_g$  является гомоморфизмом групп, означает, что  $\varphi_{gh} = \varphi_g \circ \varphi_h$  для всех  $g, h \in G$ . Если понятно, о каком действии идёт речь, мы часто будем сокращать  $\varphi_g(x)$  до  $gx$ . При наличии действия группы  $G$  на множестве  $X$  мы пишем  $G : X$ . Действие называется *транзитивным*, если любую точку множества  $X$  можно перевести в любую другую точку каким-нибудь преобразованием из группы  $G$ , т. е.  $\forall x, y \in X \exists g \in G : gx = y$ . Более общим образом, действие называется *t-транзитивным*, если любые два упорядоченных набора из  $t$  различных точек множества  $X$  можно перевести друг в друга подходящими преобразованиями из  $G$ . Действие называется *свободным*, если каждый отличный от единицы элемент группы действует на  $X$  без неподвижных точек, т. е.  $\forall g \in G \forall x \in X gx = x \Rightarrow g = e$ . Действие  $\varphi : G \rightarrow \text{Aut } X$  называется *точным* (или

<sup>1</sup>Проще всего это увидеть на модели додекаэдра, которую я ещё раз настоятельно рекомендую изготовить — см. упр. 10.10 на стр. 170.

эффективным), если каждый отличный от единицы элемент группы действует на  $X$  не тождественно, т. е. когда  $\ker \varphi = e$ . Точное представление отождествляет  $G$  с группой преобразований  $\varphi(G) \subset \text{Aut}(X)$  множества  $X$ . Отметим, что любое свободное действие точно.

Если группа  $G$  действует на множестве  $X$ , то она действует и на подмножествах множества  $X$ : элемент  $g \in G$  переводит подмножество  $M \subset X$  в подмножество  $gM = \{gt \mid t \in M\}$ . При этом отображение  $g : M \rightarrow gM, x \mapsto gx$  биективно, и обратным к нему является отображение  $g^{-1} : gM \rightarrow M, y \mapsto g^{-1}y$ , ибо  $g^{-1}gx = ex = x$ . Говорят, что элемент  $g \in G$  *нормализует*<sup>1</sup> подмножество  $M \subset X$ , если  $gM = M$ , т. е.  $gx \in M$  для каждого  $x \in M$ . Каждый такой элемент задаёт биекцию  $g|_M : M \rightarrow M$ . Если эта биекция тождественна, т. е.  $gx = x$  для всех  $x \in M$ , то говорят, что элемент  $g$  *централизует* подмножество  $M$ . Множество всех элементов  $g \in G$ , нормализующих (соотв. централизующих) данное подмножество  $M \subset X$  обозначается  $N(M)$  (соотв.  $Z(M)$ ) и называется *нормализатором* (соотв. *централизатором*) подмножества  $M \subset X$  при заданном действии группы  $G$  на  $X$ .

УПРАЖНЕНИЕ 10.19. Убедитесь, что  $N(M)$  и  $Z(M)$  являются подгруппами в  $G$ .

ПРИМЕР 10.12 (РЕГУЛЯРНЫЕ ДЕЙСТВИЯ)

Обозначим через  $X$  множество элементов группы  $G$ , а через  $\text{Aut}(X)$  — группу автоморфизмов этого множества<sup>2</sup>. Отображение  $\lambda : G \rightarrow \text{Aut}(X)$ , переводящее элемент  $g \in G$  в преобразование<sup>3</sup>  $\lambda_g : x \mapsto gx$  левого умножения на  $g$  является гомоморфизмом групп, поскольку

$$\lambda_{gh}(x) = ghx = \lambda_g(hx) = \lambda_g(\lambda_h(x)) = \lambda_g \circ \lambda_h(x).$$

Оно называется *левым регулярным действием* группы  $G$  на себе. Так как равенство  $gh = h$  в группе  $G$  влечёт равенство  $g = e$ , левое регулярное действие свободно и, в частности, точно. Симметричным образом, *правое регулярное действие*  $\rho_g : G \rightarrow \text{Aut}(X)$  сопоставляет элементу  $g \in G$  преобразование  $x \mapsto xg^{-1}$  правого умножения на обратный<sup>4</sup> к  $g$  элемент.

УПРАЖНЕНИЕ 10.20. Убедитесь, что  $\rho_g$  является свободным действием.

Тем самым, любая абстрактная группа  $G$  может быть реализована как группа преобразований некоторого множества. Например, левые регулярные представления числовых групп реализуют аддитивную группу  $\mathbb{R}$  группой сдвигов  $\lambda_v : x \mapsto x + v$  числовой прямой, а мультипликативную группу  $\mathbb{R}^*$  — группой гомотетий  $\lambda_c : x \mapsto cx$  проколотой прямой  $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$ .

ПРИМЕР 10.13 (ПРИСОЕДИНЁННОЕ ДЕЙСТВИЕ)

Отображение  $\text{Ad} : G \rightarrow \text{Aut}(G)$ , сопоставляющее элементу  $g \in G$  автоморфизм сопряжения этим элементом

$$\text{Ad}_g : G \rightarrow G, \quad h \mapsto ghg^{-1}, \quad (10-14)$$

называется *присоединённым действием* группы  $G$  на себе.

<sup>1</sup>В этом случае также говорят, что подмножество  $M \subset X$  является  $g$ -инвариантным.

<sup>2</sup>Возможно, не перестановочных с имеющейся в  $G$  композицией, т. е. не обязательно являющихся автоморфизмами группы  $G$ .

<sup>3</sup>Обратите внимание, что это преобразование множества  $X$  не является гомоморфизмом группы  $G$ , поскольку равенство  $g(h_1 h_2) = (gh_1)(gh_2)$ , вообще говоря, не выполняется.

<sup>4</sup>Появление  $g^{-1}$  не случайно: проверьте, что сопоставление элементу  $g \in G$  отображения правого умножения на  $g$  является не гомоморфизмом, а антигомоморфизмом (т. е. оборачивает порядок сомножителей в произведениях).

УПРАЖНЕНИЕ 10.21. Убедитесь, что  $\forall g \in G$  сопряжение (10-14) является гомоморфизмом из  $G$  в  $G$  и что отображение  $g \mapsto \text{Ad}_g$  является гомоморфизмом из  $G$  в  $\text{Aut } G$ .

Образ присоединённого действия  $\text{Ad}(G) \subset \text{Aut } G$  обозначается  $\text{Int}(G)$  и называется группой внутренних автоморфизмов группы  $G$ . Не лежащие в  $\text{Int}(G)$  автоморфизмы группы  $G$  называются внешними. В отличие от левого и правого регулярных действий присоединённое действие, вообще говоря, не свободно и не точно. Например, если группа  $G$  абелева, все внутренние автоморфизмы (10-14) тождественные, и ядро присоединённого действия в этом случае совпадает со всей группой. В общем случае  $\ker(\text{Ad})$  образовано такими  $g \in G$ , что  $ghg^{-1} = h$  для всех  $h \in G$ . Последнее равенство равносильно равенству  $gh = hg$  и означает, что  $g$  коммутирует со всеми элементами группы. Подгруппа элементов, перестановочных со всеми элементами группы  $G$  называется центром группы  $G$  и обозначается

$$Z(G) = \ker(\text{Ad}) = \{g \in G \mid \forall h \in G \ gh = hg\}.$$

Стабилизатор заданного элемента  $g \in G$  в присоединённом действии состоит из всех элементов группы, коммутирующих с  $g$ . Он называется централизатором элемента  $g$  и обозначается

$$Z(g) = \{h \in G \mid hg = gh\}.$$

**10.4.1. Орбиты.** Со всякой группой преобразований  $G$  множества  $X$  связано бинарное отношение  $y \sim x$  на  $X$ , означающее, что  $y = gx$  для некоторого  $g \in G$ . Это отношение рефлексивно, ибо  $x = ex$ , симметрично, поскольку  $y = gx \iff x = g^{-1}y$ , и транзитивно, т. к. из равенств  $y = gx$  и  $z = hy$  вытекает равенство  $z = (hg)x$ . Таким образом, это отношение является эквивалентностью. Класс эквивалентности точки  $x \in X$  состоит из всех точек, которые можно получить из  $x$ , применяя всевозможные преобразования из группы  $G$ . Он обозначается  $Gx = \{gx \mid g \in G\}$  и называется  $G$ -орбитой точки  $x$ . Согласно н° 0.4 на стр. 10 множество  $X$  распадается в дизъюнктное объединение орбит. Множество всех орбит называется фактором множества  $X$  по действию группы  $G$  и обозначается  $X/G$ . С каждой орбитой  $Gx$  связано сюръективное отображение<sup>1</sup> множество  $\text{ev}_x : G \rightarrow Gx$ ,  $g \mapsto gx$ , слой которого над точкой  $y \in Gx$  состоит из всех преобразований группы  $G$ , переводящих  $x$  в  $y$ . Он называется транспортёром  $x$  в  $y$  и обозначается  $G_{yx} = \{g \in G \mid gx = y\}$ . Слой над самой точкой  $x$  состоит из всех преобразований, оставляющих  $x$  на месте. Он называется стабилизатором точки  $x$  в группе  $G$  и обозначается  $\text{Stab}_G(x) = G_{xx} = \{g \in G \mid gx = x\}$  или просто  $\text{Stab}(x)$ , если понятно, о какой группе  $G$  идёт речь.

УПРАЖНЕНИЕ 10.22. Убедитесь, что  $\text{Stab}_G(x)$  является подгруппой в группе  $G$ .

Если  $y = gx$  и  $z = hx$ , то для любого  $s \in \text{Stab}(x)$  преобразование  $hsg^{-1} \in G_{zy}$ . Наоборот, если  $fy = z$ , то  $h^{-1}fg \in \text{Stab}(x)$ . Таким образом, мы имеем обратные друг другу отображения множеств:

$$\text{Stab}(x) \begin{array}{c} \xrightarrow{hsg^{-1}} \\ \xleftarrow{h^{-1}fg} \end{array} G_{zy}, \quad (10-15)$$

и стало быть, для любых трёх точек  $x, y, z$  из одной  $G$ -орбиты имеется биекция между  $G_{zy}$  и  $\text{Stab}(x)$ .

<sup>1</sup>При желании его можно воспринимать как «некоммутативное» отображения вычисления.

Предложение 10.2 (формула для длины орбиты)

Длина орбиты произвольной точки  $x$  при действии на неё конечной группы преобразований  $G$  равна  $|Gx| = |G| : |\text{Stab}_G(x)|$ . В частности, длины всех орбит и порядки стабилизаторов всех точек являются делителями порядка группы.

Доказательство. Группа  $G$  является дизъюнктивным объединением транспортёров  $G_{yx}$  по всем точкам  $y \in Gx$ , и каждый транспортёр состоит из  $|\text{Stab}(x)|$  элементов.  $\square$

Предложение 10.3

Стабилизаторы всех точек, лежащих в одной орбите конечной группы, сопряжены:

$$y = gx \Rightarrow \text{Stab}(y) = g \text{Stab}(x) g^{-1} = \{ghg^{-1} \mid h \in \text{Stab}(x)\}.$$

В частности, все они имеют одинаковый порядок.

Доказательство. Это сразу следует из диаграммы (10-15).  $\square$

Пример 10.14 (действие перестановок букв на словах)

Зафиксируем какой-нибудь  $k$ -буквенный алфавит  $A = \{a_1, \dots, a_k\}$  и рассмотрим множество  $X$  всех  $n$ -буквенных слов  $w$ , которые можно написать с его помощью. Иначе  $X$  можно воспринимать как множество всех отображений  $w : \{1, \dots, n\} \rightarrow A$ . Сопоставим каждой перестановке  $\sigma \in S_n$  преобразование  $w \mapsto w\sigma^{-1}$ , которое переставляет буквы в словах так, как предписывает  $\sigma$ . Таким образом, мы получили действие симметрической группы  $S_n$  на множестве слов. Орбита слова  $w \in X$  под действием этой группы состоит из всех слов, где каждая буква алфавита встречается столько же раз, сколько в слове  $w$ . Стабилизатор  $\text{Stab}(w)$  слова  $w$ , в котором буква  $a_i$  встречается  $m_i$  раз (для каждого  $i = 1, \dots, k$ ), состоит из перестановок между собою одинаковых букв и имеет порядок  $|\text{Stab}(w)| = m_1! \dots m_k!$ . Тем самым, длина орбиты такого слова равна мультиномиальному коэффициенту

$$|S_n w| = \frac{|S_n|}{|\text{Stab}(w)|} = \frac{n!}{m_1! \dots m_k!} = \binom{n}{m_1 \dots m_k}.$$

Этот пример показывает, что разные орбиты могут иметь разную длину, и порядки стабилизаторов точек из разных орбит могут быть разными.

Упражнение 10.23. Для каждого из пяти платоновых тел рассмотрите действие группы этого тела на его гранях и по формуле для длины орбиты найдите порядок собственной и несобственной группы каждого из платоновых тел.

Пример 10.15 (классы сопряжённости в симметрической группе)

Перестановка  $\text{Ad}_g(\sigma) = g\sigma g^{-1}$ , сопряжённая перестановке  $\sigma = (\sigma_1, \dots, \sigma_n) \in S_n$ , для каждого  $i = 1, 2, \dots, n$  переводит элемент  $g(i)$  в элемент  $g(\sigma_i)$ . Поэтому при сопряжении цикла  $\tau = (i_1, \dots, i_k) \in S_n$  перестановкой  $g = (g_1, \dots, g_n)$  получится цикл  $g\tau g^{-1} = (g_{i_1}, \dots, g_{i_k})$ . Если перестановка  $\sigma \in S_n$  имеет цикловой тип  $\lambda$  и является произведением независимых циклов, записанных по строкам диаграммы  $\lambda$ , то действие на такую перестановку внутреннего автоморфизма  $\text{Ad}_g$  заключается в применении отображения  $g$  к заполнению диаграммы  $\lambda$ , т. е. в замене каждого числа  $i$  числом  $g_i$ .

<sup>1</sup>Т. е. переводит слово  $w = a_{v_1} \dots a_{v_n}$  в слово  $a_{v_{\sigma^{-1}(1)}} a_{v_{\sigma^{-1}(2)}} \dots a_{v_{\sigma^{-1}(n)}}$ , на  $i$ -том месте которого стоит та буква, номер которой в исходном слове  $w$  переводится перестановкой  $\sigma$  в номер  $i$ .

Таким образом, орбиты присоединённого действия симметрической группы  $S_n$  на себе взаимно однозначно соответствуют  $n$ -клеточным диаграммам Юнга, и орбита, отвечающая диаграмме  $\lambda$ , состоит из всех перестановок циклового типа  $\lambda$ . Если диаграмма  $\lambda$  имеет  $m_i$  строк длины  $i$  для каждого  $i = 1, \dots, n$ , то централизатор любой перестановки  $\sigma$  циклового типа  $\lambda$  состоит из таких перестановок элементов заполнения диаграммы  $\lambda$  независимыми циклами перестановки  $\sigma$ , которые не меняют  $\sigma$ , т. е. циклически переставляют элементы вдоль строк или произвольным образом переставляют строки одинаковой длины между собой как единое целое. Тем самым, порядок стабилизатора перестановки циклового типа  $\lambda$  зависит только от  $\lambda$  и равен  $z_\lambda = 1^{m_1} \cdot m_1! \cdot 2^{m_2} \cdot m_2! \cdot \dots \cdot n^{m_n} \cdot m_n! = \prod_{i=1}^n m_i! i^{m_i}$ . Количество перестановок циклового типа  $\lambda$ , т. е. длина соответствующей орбиты присоединённого действия, равна  $n!/z_\lambda$ .

**10.4.2. Перечисление орбит.** Подсчёт числа элементов в факторе  $X/G$  конечного множества  $X$  по действию конечной группы  $G$  наталкивается на очевидную трудность: поскольку длины у орбит могут быть разные, число орбит «разного типа» придётся подсчитывать по отдельности, заодно уточняя по ходу дела, что именно имеется в виду под «типом орбиты». Разом преодолеть обе эти трудности позволяет

**ТЕОРЕМА 10.2 (ФОРМУЛА ПОЛИА – БЕРНСАЙДА)**

Пусть конечная группа  $G$  действует на конечном множестве  $X$ . Для каждого  $g \in G$  обозначим через  $X^g = \{x \in X \mid gx = x\} = \{x \in X \mid g \in \text{Stab}(x)\}$  множество неподвижных точек преобразования  $g$ . Тогда  $|X/G| = |G|^{-1} \sum_{g \in G} |X^g|$ .

**Доказательство.** Обозначим через  $F \subset G \times X$  множество всех таких пар  $(g, x)$ , что  $gx = x$ . Иначе  $F$  можно описать как  $F = \bigsqcup_{x \in X} \text{Stab}(x) = \bigsqcup_{g \in G} X^g$ . Первое из этих описаний получается из рассмотрения проекции  $F \rightarrow X$ , второе — из рассмотрения проекции  $F \rightarrow G$ . Согласно второму описанию,  $|F| = \sum_{g \in G} |X^g|$ . С другой стороны, из первого описания мы заключаем, что  $|F| = |G| \cdot |X/G|$ . В самом деле, стабилизаторы всех точек, принадлежащих одной орбите, имеют одинаковый порядок, и сумма этих порядков по всем точкам орбиты равна произведению порядка стабилизатора на длину орбиты, т. е.  $|G|$ . Складывая по всем  $|X/G|$  орбитам, получаем требуемое.  $\square$

**ПРИМЕР 10.16 (ОЖЕРЕЛЬЯ)**

Пусть имеется неограниченный запас одинаковых по форме бусин  $n$  различных цветов. Сколько различных ожерелий можно сделать из 6 бусин? Ответом на этот вопрос является количество орбит группы диэдра  $D_6$  на множестве всех раскрасок вершин правильного шестиугольника в  $n$  цветов. Группа  $D_6$  состоит из 12 элементов: тождественного преобразования  $e$ , двух поворотов  $\tau^{\pm 1}$  на  $\pm 60^\circ$ , двух поворотов  $\tau^{\pm 2}$  на  $\pm 120^\circ$ , центральной симметрии  $\tau^3$ , трёх отражений  $\sigma_{14}, \sigma_{23}, \sigma_{36}$  относительно больших диагоналей и трёх отражений  $\bar{\sigma}_{14}, \bar{\sigma}_{23}, \bar{\sigma}_{36}$  относительно срединных перпендикуляров к сторонам. Единица оставляет на месте все  $n^6$  раскрасок. Раскраски, симметричные относительно остальных преобразований, показаны на рис. 10.12 на стр. 182. Беря на этих рисунках все допустимые сочетания цветов, получаем, соответственно,  $n, n^2, n^3, n^4$  и  $n^3$  раскрасок. По теор. 10.2 число 6-бусинных ожерелий равно  $(n^6 + 3n^4 + 4n^3 + 2n^2 + 2n)/12$ .

**УПРАЖНЕНИЕ 10.24.** Подсчитайте количество ожерелий из 7, 8, 9, и 10 бусин.

**10.5. Смежные классы и факторизация.** Каждая подгруппа  $H \subset G$  задаёт на группе  $G$  два отношения эквивалентности, происходящие из левого и правого регулярного действия подгруппы  $H$  на группе  $G$ . Левое действие  $\lambda_h : g \mapsto hg$  приводит к эквивалентности

$$g_1 \underset{L}{\sim} g_2 \iff g_1 = hg_2 \text{ для некоторого } h \in H, \tag{10-16}$$

разбивающей группу  $G$  в дизъюнктное объединение орбит вида  $Hg \stackrel{\text{def}}{=} \{hg \mid h \in H\}$ , называемых *правыми смежными классами* (или *правыми сдвигами*) подгруппы  $H$  в группе  $G$ . Множество правых смежных классов обозначается  $H \backslash G$ .

УПРАЖНЕНИЕ 10.25. Покажите, что равенство  $Hg_1 = Hg_2$  равносильно любому из эквивалентных друг другу включений  $g_2g_1^{-1} \in H, g_1g_2^{-1} \in H$ .

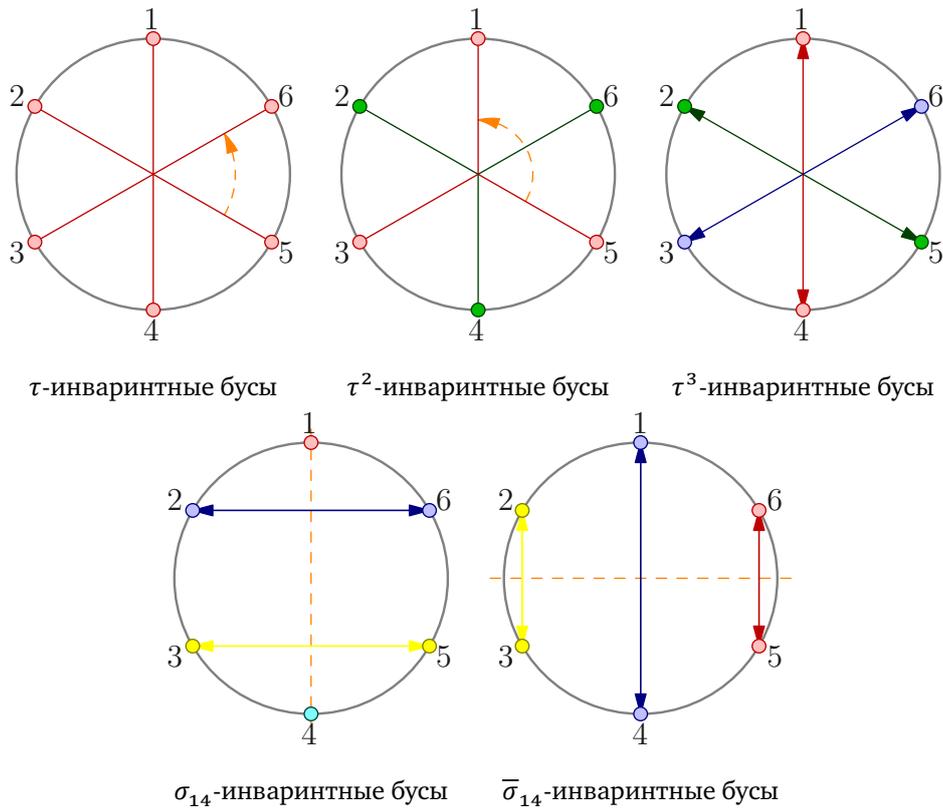


Рис. 10♦12. Симметричные ожерелья из шести бусин.

С правым действием  $\varrho_h : g \mapsto gh^{-1}$  связано отношение эквивалентности

$$g_1 \underset{R}{\sim} g_2 \iff g_1 = g_2h \text{ для некоторого } h \in H, \tag{10-17}$$

разбивающее группу  $G$  в дизъюнктное объединение орбит  $gH \stackrel{\text{def}}{=} \{gh \mid h \in H\}$ , которые называются *левыми смежными классами* (или *левыми сдвигами*) подгруппы  $H$  в группе  $G$ . Множество левых смежных классов обозначается  $G/H$ .

Поскольку и левое и правое действия подгруппы  $H$  на группе  $G$  свободны, все орбиты каждого из них состоят из  $|H|$  элементов. Тем самым, число орбит в обоих действиях одинаково и равно  $|G| / |H|$ . Это число называется *индексом* подгруппы  $H$  в группе  $G$  и обозначается  $[G : H] \stackrel{\text{def}}{=} |G/H|$ . Нами установлена

ТЕОРЕМА 10.3 (ТЕОРЕМА ЛАГРАНЖА ОБ ИНДЕКСЕ ПОДГРУППЫ)

Порядок и индекс любой подгруппы  $H$  в произвольной конечной группе  $G$  нацело делят порядок группы  $G$  и  $[G : H] = |G| : |H|$ .

СЛЕДСТВИЕ 10.3

Порядок любого элемента конечной группы нацело делит порядок группы.

Доказательство. Порядок элемента  $g \in G$  равен порядку порождённой им циклической подгруппы  $\langle g \rangle \subset G$ .  $\square$

**10.5.1. Нормальные погруппы.** Подгруппа  $H \subset G$  называется *нормальной* (или *инвариантной*), если для любого  $g \in G$  выполняется равенство  $gHg^{-1} = H$  или, что то же самое,  $gH = Hg$ . Иначе можно сказать, что подгруппа  $H \subset G$  нормальна тогда и только тогда, когда левая и правая эквивалентности (10-16) и (10-17) совпадают друг с другом и, в частности,  $H \setminus G = G/H$ . Если подгруппа  $H \subset G$  нормальна, мы пишем  $H \triangleleft G$ .

ПРИМЕР 10.17 (ядра гомоморфизмов)

Ядро любого гомоморфизма групп  $\varphi : G_1 \rightarrow G_2$  является нормальной подгруппой в  $G_1$ , поскольку при  $\varphi(h) = e$  для любого  $g \in G$  имеем равенство

$$\varphi(ghg^{-1}) = \varphi(g)\varphi(h)\varphi(g)^{-1} = \varphi(g)\varphi(g)^{-1} = e,$$

означающее, что  $g(\ker \varphi)g^{-1} \subset \ker \varphi$ . Это согласуется с равенством правых и левых смежных классов  $g(\ker \varphi) = (\ker \varphi)g$ , установленным нами в предл. 10.1.

ПРИМЕР 10.18 ( $V_4 \triangleleft S_4$ )

Подгруппа Клейна  $V_4 \subset S_4$  состоящая из перестановок циклового типа  $\begin{pmatrix} & & & \\ & & & \\ & & & \\ & & & \end{pmatrix}$  и тождественной перестановки нормальна.

ПРИМЕР 10.19 (внутренние автоморфизмы)

Подгруппа внутренних автоморфизмов  $\text{Int}(G) = \text{Ad}(G)$  нормальна в группе  $\text{Aut}(G)$  всех автоморфизмов группы  $G$ , поскольку сопрягая внутренний автоморфизм  $\text{Ad}_g : h \mapsto ghg^{-1}$  произвольным автоморфизмом  $\varphi : G \rightarrow G$ , мы получаем внутренний автоморфизм  $\varphi \circ \text{Ad}_g \circ \varphi^{-1} = \text{Ad}_{\varphi(g)}$ .

УПРАЖНЕНИЕ 10.26. Убедитесь в этом.

ПРИМЕР 10.20 (ПАРАЛЛЕЛЬНЫЕ ПЕРЕНОСЫ)

Подгруппа параллельных переносов нормальна в группе  $\text{Aff}(\mathbb{A}^n)$  всех биективных аффинных преобразований аффинного пространства  $\mathbb{A}^n$ , т. к. сопрягая параллельный перенос  $\tau_v$  на вектор  $v$  любым аффинным преобразованием  $\varphi : \mathbb{A}^n \rightarrow \mathbb{A}^n$ , получаем перенос<sup>1</sup>  $\tau_{D_\varphi(v)}$  на вектор  $D_\varphi(v)$ .

УПРАЖНЕНИЕ 10.27. Убедитесь в этом.

<sup>1</sup>Напомню, что преобразование  $\varphi : \mathbb{A}(V) \rightarrow \mathbb{A}(V)$  аффинного пространства  $\mathbb{A}(V)$ , ассоциированного с векторным пространством  $V$ , называется *аффинным*, если отображение  $D_\varphi : \overline{pq} \mapsto \overline{\varphi(p)\varphi(q)}$  является корректно определённым линейным преобразованием векторного пространства  $V$  (оно называется *дифференциалом* отображения  $\varphi$ ).

ПРИМЕР 10.21 (НОРМАЛИЗАТОР И ЦЕНТРАЛИЗАТОР, СР. С УПР. 10.19 НА СТР. 178)

Пусть группа  $G$  действует на множестве  $X$  и  $M \subset X$  — произвольное подмножество. Напомню<sup>1</sup>, что подгруппы  $N(M) \stackrel{\text{def}}{=} \{g \in G \mid \forall x \in M \ gx \in M\}$  и  $Z(M) \stackrel{\text{def}}{=} \{g \in G \mid \forall x \in M \ gx = x\}$  называются соответственно *нормализатором* и *централизатором* подмножества  $M$ . Поскольку для любых  $g \in N(M)$ ,  $h \in Z(M)$  и  $x \in M$  выполняется равенство  $ghg^{-1}x = gg^{-1}x = x$ , ибо  $h(g^{-1}x) = g^{-1}x$ , так как  $g^{-1}x \in M$ , централизатор является нормальной подгруппой в нормализаторе.

**10.5.2. Фактор группы.** Попытка определить умножение на множестве левых смежных классов  $G/H$  неабелевой группы  $G$  формулой

$$(g_1H) \cdot (g_2H) \stackrel{\text{def}}{=} (g_1g_2)H, \quad (10-18)$$

вообще говоря, некорректна: различные записи  $g_1H = f_1H$  и  $g_2H = f_2H$  одних и тех же классов могут приводить к *различным* классам  $(g_1g_2)H \neq (f_1f_2)H$ .

УПРАЖНЕНИЕ 10.28. Убедитесь, что для группы  $G = S_3$  и подгруппы второго порядка  $H \subset G$ , порождённой транспозицией  $\sigma_{12}$ , формула (10-18) некорректна.

ПРЕДЛОЖЕНИЕ 10.4

Для того, чтобы правило  $g_1H \cdot g_2H = (g_1g_2)H$  корректно определяло на  $G/H$  структуру группы, необходимо и достаточно, чтобы подгруппа  $H$  была нормальна в  $G$ .

Доказательство. Если формула (10-18) корректна, то она задаёт на множестве смежных левых классов  $G/H$  групповую структуру: ассоциативность композиции наследуется из<sup>2</sup>  $G$ , единицей служит класс  $eH = H$ , обратным к классу  $gH$  — класс  $g^{-1}H$ . Факторизация  $G \rightarrow G/H$ ,  $g \mapsto gH$ , является гомоморфизмом групп с ядром  $H$ . Поэтому подгруппа  $H$  нормальна в силу [прим. 10.17](#). Наоборот, если  $H$  нормальна и  $f_1H = g_1H$ ,  $f_2H = g_2H$ , то  $f_1f_2H = f_1g_2H = f_1Hg_2 = g_1Hg_2 = g_1g_2H$  в силу равенства  $g_2H = Hg_2$ .  $\square$

ОПРЕДЕЛЕНИЕ 10.2

Множество смежных классов  $G/H$  нормальной подгруппы  $H \triangleleft G$  с операцией

$$g_1H \cdot g_2H \stackrel{\text{def}}{=} (g_1g_2)H$$

называется *фактором* (или *факторгруппой*) группы  $G$  по нормальной подгруппе  $H$ . Гомоморфизм групп  $G \rightarrow G/H$ ,  $g \mapsto gH$ , называется *гомоморфизмом факторизации*.

СЛЕДСТВИЕ 10.4

Каждый гомоморфизм групп  $\varphi : G_1 \rightarrow G_2$  является композицией эпиморфизма факторизации  $G_1 \rightarrow G_1/\ker \varphi$  и мономорфизма  $G_1/\ker \varphi \hookrightarrow G_2$ , переводящего смежный класс  $g \ker \varphi \in G_1/\ker \varphi$  в элемент  $\varphi(g) \in G_2$ . В частности,  $\text{im } \varphi \simeq G/\ker \varphi$ .

Доказательство. Следствие утверждает, что слой  $\varphi^{-1}(\varphi(g))$  гомоморфизма  $\varphi$  над каждой точкой  $\varphi(g) \in \text{im } \varphi \subset G_2$  является левым сдвигом ядра  $\ker \varphi$  на элемент  $g$ , что мы уже видели в [предл. 10.1](#) на стр. 173.  $\square$

<sup>1</sup>См. п° 10.4 на стр. 177.

<sup>2</sup> $(g_1H \cdot g_2H) \cdot g_3H = (g_1g_2)H \cdot g_3H = ((g_1g_2)g_3)H = (g_1(g_2g_3))H = g_1H \cdot (g_2g_3)H = g_1H \cdot (g_2H \cdot g_3H)$ .

Предложение 10.5

Если подгруппа  $H \subset G$  нормализует<sup>1</sup> подгруппу  $N \subset G$ , то множества  $HN = \{hn \mid h \in H, n \in N\}$  и  $NH = \{nh \mid n \in N, h \in H\}$  совпадают друг с другом и являются подгруппой в  $G$ , причём  $N \triangleleft HN$ ,  $H \cap N \triangleleft H$  и  $HN/N \simeq H/(H \cap N)$ .

Доказательство.  $NH = HN$  ибо  $nh = h(h^{-1}nh) \in HN$  и  $hn = (hnh^{-1})h \in NH$  для всех  $n \in N$ ,  $h \in H$ . Это подгруппа, так как  $(nh)^{-1} = h^{-1}n^{-1} \in HN = NH$  и

$$(n_1 h_1)(n_2 h_2) = n_1(h_1 n_2)h_2 = n_1(n_3 h_3)h_2 = (n_1 n_3)(h_3 h_2) \in NH$$

(существование таких  $n_3 \in N$  и  $h_3 \in H$ , что  $h_1 n_2 = n_3 h_3$ , вытекает из равенства  $HN = NH$ ). Подгруппы  $H \cap N \triangleleft H$  и  $N \triangleleft HN$  нормальны, так как по условию  $hNh^{-1} \subset N$  для всех  $h \in H$ . Отображение  $H/(H \cap N) \rightarrow HN/N$ ,  $h(H \cap N) \mapsto hN$ , очевидно корректно определено, биективно и является гомоморфизмом групп.  $\square$

Упражнение 10.29. Пусть  $\varphi : G_1 \rightarrow G_2$  — сюръективный гомоморфизм групп. Покажите, что полный прообраз  $N_1 = \varphi^{-1}(N_2)$  любой нормальной подгруппы  $N_2 \triangleleft G_2$  является нормальной подгруппой в  $G_1$  и  $G_1/N_1 \simeq G_2/N_2$ .

**10.6. Коммутант.** В группе  $G$  произведение  $(g, h) \stackrel{\text{def}}{=} ghg^{-1}h^{-1}$  называется *коммутатором*<sup>2</sup> элементов  $g, h$ . Название связано с тем, что  $(g, h)hg = gh$ . В частности,  $gh = hg$  если и только если  $(g, h) = e$ . Очевидно, что  $(g, h)^{-1} = (h, g)$  и  $\text{Ad}_f(g, h) = (\text{Ad}_f g, \text{Ad}_f h)$ , где

$$\text{Ad}_f : G \rightarrow G, \quad x \mapsto fxf^{-1},$$

автоморфизм сопряжения. Поэтому всевозможные конечные произведения коммутаторов элементов группы  $G$  образуют нормальную подгруппу, которая обозначается  $G' \triangleleft G$  и называется *коммутантом* группы  $G$ . Так как  $(g, h) = \text{Ad}_g(h)h^{-1}$ , коммутаторы элементов  $g \in G$  с элементами  $h$  из любой нормальной подгруппы  $N \triangleleft G$  лежат в  $N$ , т. е.  $(G, N) = (N, G) \subset N$ . В частности,  $(G, G') \subset G'$ . Всякий гомоморфизм  $\varphi : G \rightarrow H$  ограничивается в гомоморфизм  $\varphi|_{G'} : G' \rightarrow H'$ , и если  $\varphi$  сюръективен, то сюръективен и  $\varphi|_{G'}$ .

Предложение 10.6 (универсальное свойство фактора по коммутанту)

Всякий гомоморфизм  $\varphi : G \rightarrow A$  в абелеву группу  $A$  единственным образом пропускается через гомоморфизм факторизации  $\pi : G \twoheadrightarrow G/G'$ , т. е. существует единственный такой гомоморфизм  $\varphi' : G/G' \rightarrow A$ , что  $\varphi = \varphi'\pi$ .

Доказательство. Гомоморфизм  $\varphi'$  обязан действовать по правилу  $gG' \mapsto \varphi(g)$ . Оно корректно, так как  $G' \subset \ker \varphi$ , поскольку в  $A$  все коммутаторы тривиальны.  $\square$

Следствие 10.5

Фактор группа  $G/N$  абелева если и только если  $N \supseteq G'$ .

Доказательство. Применяем предл. 10.6 к эпиморфизму  $G \twoheadrightarrow G/N$ .  $\square$

<sup>1</sup>Т. е.  $hNh^{-1} = N$  для всех  $h \in H$ .

<sup>2</sup>Или *групповым коммутатором*, который не следует путать с коммутатором  $[f, g] = fg - gf$  элементов ассоциативной алгебры.

ПРИМЕР 10.22 (КОММУТАНТЫ СИММЕТРИЧЕСКИХ И ЗНАКОПЕРЕМЕННЫХ ГРУПП)

Поскольку каждый коммутатор в  $S_n$  является чётной перестановкой,  $S'_n \triangleleft A_n$ . Так как  $|A_3| = 3$  и группа  $S_3$  не абелева,  $S'_3 = A_3$ . Тем самым, при любом  $n$  коммутант  $S'_n$  содержит все 3-циклы.

УПРАЖНЕНИЕ 10.30. Убедитесь, что группа  $A_n$  порождается 3-циклами.

Мы заключаем, что  $S'_n = A_n$ . Поскольку  $|A_4/V_4| = 3$ , группа  $A_4/V_4 \simeq \mathbb{Z}/(3)$  абелева, откуда  $A'_4 \subseteq V_4$  по сл. 10.5. Так как группа  $A_4$  не абелева,  $A'_4$  содержит пару независимых транспозиций, а значит, и все сопряжённые ей пары, т. е.  $A'_4 = V_4$ . Отсюда вытекает, что при любом  $n$  коммутатор  $A'_n$  содержит все пары независимых транспозиций.

УПРАЖНЕНИЕ 10.31. Убедитесь, что при  $n \geq 5$  группа  $A_n$  порождается парами независимых транспозиций.

Мы заключаем, что  $A'_n = A_n$  при  $n \geq 5$ .

ПРИМЕР 10.23 (КОММУТАНТЫ ЛИНЕЙНЫХ ГРУПП)

Пусть  $\mathbb{k}$  — произвольное поле. Так как  $\det(f, g) = 1$  для всех  $f, g \in \text{GL}_n(\mathbb{k})$ , мы заключаем, что  $\text{GL}'_n(\mathbb{k}) \leq \text{SL}_n(\mathbb{k})$ . Покажем, что  $\text{SL}'_n(\mathbb{k}) = \text{SL}_n(\mathbb{k})$  за исключением  $\text{SL}_2(\mathbb{F}_2)$  и  $\text{SL}_2(\mathbb{F}_3)$ .

УПРАЖНЕНИЕ 10.32. Убедитесь, что  $\text{SL}_2(\mathbb{F}_2) = \text{GL}_2(\mathbb{F}_2) \simeq S_3$  и  $\text{SL}_2(\mathbb{F}_3)/\{\pm E\} \simeq A_4$ .

Легко видеть, что любую матрицу из  $\text{SL}_n(\mathbb{k})$  можно превратить в единичную элементарными преобразованиями, заключающимися в прибавлении к одной из строк другой строки, умноженной на произвольное число, т. е. в умножении матрицы слева на матрицу вида<sup>1</sup>

$$T_{ij}(\alpha) \stackrel{\text{def}}{=} E + \alpha E_{ij}, \quad \text{где } i \neq j. \quad (10-19)$$

УПРАЖНЕНИЕ 10.33. Убедитесь в этом и покажите, что  $(T_{ij}(\alpha), T_{jk}(\beta)) = T_{ik}(\alpha\beta)$  для любых трёх различных индексов  $i, j, k$ .

Из упражнения вытекает, что при  $n \geq 3$  коммутант  $\text{SL}'_n(\mathbb{k})$  содержит все трансвекции, и тем самым  $\text{GL}'_n(\mathbb{k}) = \text{SL}'_n(\mathbb{k}) = \text{SL}_n(\mathbb{k})$  при  $n \geq 3$ .

УПРАЖНЕНИЕ 10.34. Покажите, что при  $n = 2$  и  $\{i, j\} = \{1, 2\}$  коммутатор трансвекции  $T_{ij}(\alpha)$  с диагональной матрицей  $\beta E_{ii} + \beta^{-1} E_{jj} \in \text{SL}_2(\mathbb{k})$  равен  $T_{ij}(\alpha(1 - \beta^2))$ .

Мы заключаем, что при  $\mathbb{k} \neq \mathbb{F}_2, \mathbb{F}_3$  коммутант  $\text{SL}'_2(\mathbb{k})$  тоже содержит все трансвекции. Таким образом,  $\text{GL}'_n(\mathbb{k}) = \text{SL}'_n(\mathbb{k}) = \text{SL}_n(\mathbb{k})$  за исключением групп  $\text{GL}_2$  и  $\text{SL}_2$  над полями  $\mathbb{F}_2$  и  $\mathbb{F}_3$ .

УПРАЖНЕНИЕ 10.35. Вычислите коммутанты  $\text{GL}'_2(\mathbb{F}_2) = \text{SL}'_2(\mathbb{F}_2)$ ,  $\text{GL}'_2(\mathbb{F}_3)$  и  $\text{SL}'_2(\mathbb{F}_3)$ .

<sup>1</sup>Такие матрицы называются *трансвекциями*.

## Ответы и указания к некоторым упражнениям

Упр. 10.1. Если  $fg = e$  и  $gh = e$ , то  $f = fe = f(gh) = (fg)h = eh = h$ .

Упр. 10.2. Для двух единичных элементов  $e'$  и  $e''$  выполнены равенства  $e' = e'e'' = e''$ .

Упр. 10.4. Ответ: либо  $r = 1$  и  $\text{Tors}(G) = 0$  (т. е.  $G \simeq \mathbb{Z}$ ), либо  $r = 0$  (т. е.  $G$  конечна) и каждое простое число  $p \in \mathbb{N}$  присутствует в каноническом разложении

$$G = \frac{\mathbb{Z}}{(p_1^{n_1})} \oplus \dots \oplus \frac{\mathbb{Z}}{(p_\alpha^{n_\alpha})}$$

не более одного раза. Доказательство аналогично доказательству [предл. 9.2](#) на стр. 155.

Упр. 10.5. Пусть  $k = dr$ ,  $m = \text{ord}(\tau) = ds$ , где  $\text{нод}(r, s) = 1$ . Если  $d > 1$ , то  $\tau^d$  является произведением  $d$  независимых циклов длины  $s$ , и  $\tau^k = (\tau^d)^r$  будет произведением  $s$ -тых степеней этих циклов. Остаётся показать, что когда  $\text{ord}(\tau) = m$  взаимно прост с  $k$ , то  $\tau^k$  тоже цикл длины  $m$ . Если для какого-то элемента  $a$  цикла  $\tau$  выполняется равенство  $(\tau^k)^r(a) = a$ , то  $kr$  делится на  $m$ , что при  $\text{нод}(k, m) = 1$  возможно только когда  $r$  делится на  $m$ . Поэтому  $r \geq m$ , т. е. длина содержащего  $a$  цикла перестановки  $\tau^k$  не меньше  $m$ .

Упр. 10.6. Ответ:  $n(n-1) \dots (n-k+1)/k$  (в числителе дроби  $k$  сомножителей).

Упр. 10.7. Непересекающиеся циклы очевидно коммутируют. Если коммутирующие циклы  $\tau_1$  и  $\tau_2$  пересекаются по элементу  $a$ , то  $\tau_1(a)$  является элементом цикла  $\tau_2$ , поскольку в противном случае  $\tau_2\tau_1(a) = \tau_1(a)$ , а  $\tau_1\tau_2(a) \neq \tau_1(a)$ , так как  $\tau_2(a) \neq a$ . По той же причине  $\tau_2(a)$  является элементом цикла  $\tau_1$ , и значит, оба цикла состоят из одних и тех же элементов. Пусть  $\tau_1(a) = \tau_2^s(a)$ . Любой элемент  $b$ , на который оба цикла реально действуют имеет вид  $b = \tau_2^r(a)$ , и цикл  $\tau_1$  действует на него как  $\tau_2^s$ :

$$\tau_1(b) = \tau_1\tau_2^r(a) = \tau_2^r\tau_1(a) = \tau_2^r\tau_2^s(a) = \tau_2^s\tau_2^r(a) = \tau_2^s(b).$$

Второе утверждение следует из [упр. 10.5](#).

Упр. 10.8. Ответ:  $n! / \prod_{i=1}^n i^{m_i} m_i!$  (ср. с форм. (0-11) на стр. 9). Решение: сопоставим каждому заполнению диаграммы циклов  $\lambda$  неповторяющимися числами от 1 до  $n$  произведение независимых циклов, циклически переставляющих элементы каждой строки слева направо; получаем сюръективное отображение множества заполнений на множество всех перестановок циклового типа  $\lambda$ ; прообраз каждой перестановки состоит из  $\prod_{i=1}^n i^{m_i} m_i!$  заполнений, получающихся друг из друга независимыми циклическими перестановками элементов в каждой строке и произвольными перестановками строк одинаковой длины между собою как единого целого.

Упр. 10.9.  $|1, 6, 3, 4\rangle^{15} \cdot |2, 5, 8\rangle^{15} \cdot |7, 9\rangle^{15} = |1, 6, 3, 4\rangle^{-1} \cdot |7, 9\rangle = (4, 2, 6, 3, 5, 1, 9, 8, 7)$

Упр. 10.14. Ответ:  $|1, 2, 3, 4\rangle = \sigma_{12}\sigma_{23}\sigma_{34}$ ,  $|1, 2, 4, 3\rangle = \sigma_{12}\sigma_{24}\sigma_{34}$ ,  $|1, 3, 2, 4\rangle = \sigma_{13}\sigma_{23}\sigma_{24}$ ,  $|1, 3, 4, 2\rangle = \sigma_{13}\sigma_{34}\sigma_{24}$ ,  $|1, 4, 2, 3\rangle = \sigma_{24}\sigma_{23}\sigma_{13}$ ,  $|1, 4, 3, 2\rangle = \sigma_{34}\sigma_{23}\sigma_{12}$ .

Упр. 10.15. Подсчёт для группы куба дословно тот же, что и для группы додекаэдра. Группы октаэдра и икосаэдра изоморфны группам куба и додекаэдра с вершинами в центрах граней октаэдра и икосаэдра соответственно.

Упр. 10.17. Зафиксируем в  $V$  какой-либо базис и сопоставим оператору  $F \in \text{GL}(V)$  базис, состоящий из векторов  $f_i = F(e_i)$ . Для выбора первого базисного вектора  $f_1$  имеется  $|V| - 1 = q^n - 1$  возможностей, для выбора второго —  $|V| - |\mathbb{k} \cdot f_1| = q^n - q$  возможностей, для выбора третьего —  $|V| - |\mathbb{k} \cdot f_1 \oplus \mathbb{k} \cdot f_2| = q^n - q^2$  возможностей и т. д.

Упр. 10.18. Подсказка: центральная симметрия коммутирует со всеми элементами полной группы додекаэдра; покажите, что единственная перестановка в  $S_5$ , коммутирующая со всеми перестановками из  $S_5$  — это тождественное преобразование.

Упр. 10.23. Проиллюстрируем рассуждение на примере икосаэдра. И собственная и полная группы транзитивно действуют на 20 его треугольных гранях. Стабилизатор грани в собственной и полной группах представляет собой собственную и полную группу треугольника на плоскости, состоящую, соответственно из 3 и из 6 преобразований. По формуле для длины орбиты получаем  $|\text{SO}_{\text{ико}}| = 20 \cdot 3 = 60$  и  $|\text{O}_{\text{ико}}| = 20 \cdot 6 = 120$ .

Упр. 10.25. Равенство  $h_1 g_1 = h_2 g_2$  влечёт равенства  $g_2 g_1^{-1} = h_2^{-1} h_1 \in H$  и  $g_1 g_2^{-1} = h_1^{-1} h_2 \in H$ . С другой стороны, если один из обратных друг другу элементов  $g_2 g_1^{-1}$  и  $g_1 g_2^{-1}$  лежит в  $H$ , то в  $H$  лежит и второй, и  $H g_1 = H(g_2 g_1^{-1}) g_2 = H g_2$ .

Упр. 10.26.  $\varphi \circ \text{Ad}_g \circ \varphi^{-1} : h \mapsto \varphi(g \varphi^{-1}(h) g^{-1}) = \varphi(g) h \varphi(g)^{-1}$ .

Упр. 10.27. Для любой точки  $x \in \mathbb{R}^n$  положим  $p = \varphi^{-1}(x)$ . Так как  $\varphi : \mathbb{R}^n \rightarrow \mathbb{R}^n$  аффинно,  $\varphi(p + v) = x + D_\varphi(v)$ . Поэтому  $\varphi \circ \tau_v \circ \varphi^{-1} : x \mapsto \varphi(p + v) = x + D_\varphi(v)$ .

Упр. 10.29. Если  $\varphi(x) \in N_2$ , то  $\varphi(g x g^{-1}) = \varphi(g) \varphi(x) \varphi(g)^{-1} \in N_2$  в силу нормальности  $N_2 \triangleleft G_2$ . Поэтому  $N_1 = \varphi^{-1}(N_2) \triangleleft G_1$ . Композиция сюръективных гомоморфизмов  $G_1 \twoheadrightarrow G_2 \twoheadrightarrow G_2/N_2$  является сюръективным гомоморфизмом с ядром  $N_1$ .

Упр. 10.30. Поскольку  $S_n$  порождается транспозициями, подгруппа  $A_n$  порождается парами транспозиций. Но  $|ij\rangle|jk\rangle = |ijk\rangle$  и  $|ij\rangle|k\ell\rangle = |ijk\rangle|jk\ell\rangle$  при различных  $i, j, k, \ell$ .

Упр. 10.31. Воспользуйтесь равенством  $|ij\rangle|jk\rangle = |ij\rangle|\ell m\rangle|jk\rangle|\ell m\rangle$  для различных  $i, j, k, \ell, m$ .

Упр. 10.32. Первый изоморфизм задаётся действием группы  $\text{SL}_2(\mathbb{F}_2) \simeq \text{GL}_2(\mathbb{F}_2)$  на трёх ненулевых векторах координатной плоскости  $\mathbb{F}_2^2$ , второй — действием группы  $\text{PSL}_2(\mathbb{F}_3) \stackrel{\text{def}}{=} \text{SL}_2(\mathbb{F}_3)/\{\pm E\}$  на четырёх одномерных векторных подпространствах в  $\mathbb{F}_3^2$  или, что то же самое, действием дробно линейных преобразований  $t \mapsto (at + b)/(ct + d)$ , где  $a, b, c, d \in \mathbb{F}_3$  и  $ad \neq bc$ , на четырёх точках проективной прямой  $\mathbb{P}_1(\mathbb{F}_3) = \{-1, 0, 1, \infty\}$ .

Упр. 10.33. Модифицируйте метод Гаусса: используя только операцию прибавления к одной из строк матрицы некоторой кратности другой строки, сначала добейтесь того, чтобы в первом столбце было хотя бы два ненулевых элемента, причём один из них стоял в первой строке, затем добейтесь того, чтобы в левом верхнем углу матрицы оказалась единица, и наконец занулите первый столбец ниже первой строки, после чего повторите процедуру со вторым столбцом и второй строкой, и т. д. Для вычисления коммутатора воспользуйтесь равенствами

$$T_{ij}^{-1}(\alpha) = (E + \alpha E_{ij})^{-1} = E - \alpha E_{ij} = T_{ij}(-\alpha)$$

$$T_{ij}(\alpha) T_{jk}(\beta) = E + E_{ij}(\alpha) + E_{jk}(\beta) + E_{ik}(\alpha\beta)$$

Упр. 10.34. Прямое вычисление:

$$(E + \alpha E_{ij})(\beta E_{ii} + \beta^{-1} E_{jj})(E - \alpha E_{ij})(\beta^{-1} E_{ii} + \beta E_{jj}) = (E + \alpha E_{ij})(E - \alpha \beta^2 E_{ij}) = E + \alpha(1 - \beta^2) E_{ij}.$$

Упр. 10.35. Так как  $\text{SL}_2(\mathbb{F}_2) = \text{GL}_2(\mathbb{F}_2) = S_3$ , коммутанты  $\text{GL}'_2(\mathbb{F}_2) = \text{SL}'_2 = \{E, T, T^2\} \simeq A_3$ , где

$$T = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \quad \text{и} \quad T^2 = T^{-1} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$$

циклически переставляют ненулевые векторы  $(1, 0)$ ,  $(0, 1)$ ,  $(1, 1)$  пространства  $\mathbb{F}_2^2$ . Поскольку  $(T_{ij}(\alpha), E_{ii} - E_{jj}) = T_{ij}(-\alpha)$ , коммутант  $GL_2'(\mathbb{F}_3)$  содержит все трансвекции и равен  $SL_2(\mathbb{F}_3)$ . Для вычисления  $SL_2'(\mathbb{F}_3)$  воспользуйтесь факторизацией  $SL_2(\mathbb{F}_3) \twoheadrightarrow PSL_2(\mathbb{F}_3) \simeq A_4$  по нормальной подгруппе  $\{\pm E\} \triangleleft SL_2(\mathbb{F}_3)$ . Она сюръективно отображает коммутант  $SL_2'(\mathbb{F}_3)$  на группу Клейна  $A_4' = V_4$ , состоящую независимых транспозиций двух пар точек проективной прямой

$$\mathbb{P}_1(\mathbb{F}_3) = \{(1 : 0), (0 : 1), (1 : 1), (1 : -1)\},$$

которые задаются следующими матрицами из  $SL_2(\mathbb{F}_3)$  с точностью до знака

$$I = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad J = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \quad K = \begin{pmatrix} -1 & 1 \\ 1 & 1 \end{pmatrix}.$$

Убедитесь, что  $I^2 = J^2 = K^2 = -E$  и  $IJ = -JI = K$ ,  $JK = -KJ = I$ ,  $KI = -IK = J$ . Таким образом, коммутант  $SL_2(\mathbb{F}_3)'$  имеет порядок 8 и изоморфен группе *кватернионных единиц*  $Q_8 \stackrel{\text{def}}{=} \{\pm E, \pm I, \pm J, \pm K\}$ .