

§12. Группы

12.1. 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

$$\text{ассоциативность:} \quad \forall f, g, h \in G \quad (fg)h = f(gh) \quad (12-1)$$

$$\text{наличие единицы:} \quad \exists e \in G : \forall g \in G \quad eg = g \quad (12-2)$$

$$\text{наличие обратных:} \quad \forall g \in G \quad \exists g^{-1} \in G : g^{-1}g = e \quad (12-3)$$

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

$$\text{коммутативность:} \quad \forall f, g \in G \quad fg = gf. \quad (12-4)$$

Левый обратный к g элемент g^{-1} , существование которого постулируется в (12-3), является также и правым обратным, т. е. удовлетворяет равенству $gg^{-1} = e$, которое получается умножением правой и левой частей в $g^{-1}gg^{-1} = eg^{-1} = g^{-1}$ слева на левый обратный к g^{-1} элемент.

Упражнение 12.1. Убедитесь, что обратный к g элемент g^{-1} однозначно определяется элементом g и что $(g_1 g_2 \dots g_k)^{-1} = g_k^{-1} \dots g_2^{-1} g_1^{-1}$.

Для единицы e из (12-2) при любом $g \in G$ выполняются также и равенство $ge = g$, поскольку $ge = g(g^{-1}g) = (gg^{-1})g = eg = g$.

Упражнение 12.2. 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 12.3. Проверьте, что пересечение любого множества подгрупп является подгруппой.

Пример 12.1 (группы преобразований)

Модельными примерами групп являются *группы преобразований*, обсуждавшиеся нами в п° 1.6. 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 автоморфизмов конечного множества $X = \{1, 2, \dots, n\}$ из n элементов называется *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 $|A_n| = n!/2$.

12.1.1. 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 $\langle g \rangle$. Будучи абелевой группой с одной образующей, $\langle g \rangle$ является образом сюръективного гомоморфизма $\varphi_g : \mathbb{Z} \twoheadrightarrow \langle g \rangle$,

$m \mapsto g^m$ переводящего 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 порядок¹ $n = \text{ord } g$ 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 $\text{ord } g = \infty$.

Напомним², что группа G называется *циклической*, если в ней существует элемент $g \in G$ такой, 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} является циклической, и в качестве образующего элемента можно взять любой из двух элементов ± 1 . В [предл. 3.12](#) на стр. 48 мы видели, что всякая конечная подгруппа в мультипликативной группе любого поля является циклической. Аддитивная группа вычетов $\mathbb{Z}/(10)$ также является циклической, и в качестве её образующего элемента можно взять любой из четырёх классов³ $[\pm 1]_6, [\pm 3]_6$.

Упражнение 12.4. Укажите необходимые и достаточные условия для того, чтобы конечно порождённая абелева группа⁴ $G = \mathbb{Z}^r \oplus \frac{\mathbb{Z}}{(p_1^{n_1})} \oplus \dots \oplus \frac{\mathbb{Z}}{(p_\alpha^{n_\alpha})}$ была циклической.

Лемма 12.1

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

Доказательство. Так как $\langle h \rangle \subset \langle g \rangle$, равенство $\langle h \rangle = \langle g \rangle$ равносильно неравенству $\text{ord } h \geq n$. Но $h^m = g^{mk} = e$ тогда и только тогда, когда mk делится на n . Если $\text{nod}(n, k) = 1$, то это возможно только при m делящемся на n , и в этом случае $\text{ord } h \geq n$. 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

12.1.2. Разложение перестановок в композиции циклов. Перестановка $\tau \in S_n$ по кругу переводящая друг в друга какие-нибудь m различных элементов⁵

$$i_1 \mapsto i_2 \mapsto \dots \mapsto i_{m-1} \mapsto i_m \mapsto i_1 \quad (12-5)$$

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

Упражнение 12.5. Покажите, что k -тая степень цикла длины m является циклом тогда и только тогда, когда $\text{nod}(k, m) = 1$.

Цикл (12-5) часто бывает удобно обозначать $\tau = |i_1, i_2, \dots, i_m\rangle$, не смотря на то, что один и тот же цикл (12-5) допускает m различных таких записей, получающихся друг из друга циклическими перестановками элементов.

Упражнение 12.6. Сколько имеется в S_n различных циклов длины k ?

¹таким образом, порядок элемента равен порядку порождённой им циклической подгруппы

²см. н° 3.5.1 на стр. 47

³обратите внимание, что остальные 6 классов не являются образующими

⁴см. теор. 10.5 на стр. 160

⁵числа i_1, i_2, \dots, i_m могут быть любыми, не обязательно соседними или возрастающими

Теорема 12.1

Каждая перестановка $g \in S_n$ является композицией непересекающихся циклов:

$$g = \tau_1 \tau_2 \cdots \tau_k. \quad (12-6)$$

Любые два цикла разложения (12-6) перестановочны: $\tau_i \tau_j = \tau_j \tau_i$, и оно единственно с точностью до перестановки циклов между собой.

Доказательство. Поскольку множество $X = \{1, 2, \dots, n\}$ конечно, в последовательности

$$x \xrightarrow{g} g(x) \xrightarrow{g} g^2(x) \xrightarrow{g} g^3(x) \xrightarrow{g} \cdots, \quad (12-7)$$

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

Определение 12.1 (цикловой тип перестановки)

Написанный в порядке нестрогого убывания набор длин непересекающихся циклов¹, 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 $\begin{array}{|c|c|c|c|} \hline & & & \\ \hline & & & \\ \hline & & & \\ \hline \end{array}$, т.е. $\lambda(6, 5, 4, 1, 8, 3, 9, 2, 7) = (4, 3, 2)$. Единственной перестановкой циклового типа $\lambda = (1, 1, \dots, 1)$ (один столбец высоты n) является тождественная перестановка Id . Диаграмму $\lambda = (n)$ (одна строка длины n) имеют $(n-1)!$ циклов максимальной длины n .

Упражнение 12.8. Сколько перестановок в симметрической группе S_n имеют заданный цикловой тип, содержащий для каждого $i = 1, 2, \dots, n$ m_i циклов длины i ?

Пример 12.2 (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

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

¹включая циклы длины один, отвечающие элементам, которые перестановка оставляет на месте

равен $5 \cdot 4 \cdot 3 = 60$. По правилу ниточек из [прим. 9.2](#) на стр. 134 знак цикла длины ℓ равен $(-1)^{\ell-1}$. Поэтому перестановка чётна тогда и только тогда, когда у неё чётное число циклов чётной длины.

Упражнение 12.9. Найдите чётность $g = (6, 5, 4, 1, 8, 3, 9, 2, 7) \in S_9$ и вычислите g^{15} .

12.2. Группы фигур. Для любой фигуры Φ в евклидовом¹ пространстве \mathbb{R}^n биективные отображения $\Phi \rightarrow \Phi$ индуцированные ортогональными² линейными преобразованиями пространства \mathbb{R}^n , переводящими фигуру Φ в себя, образуют группу преобразований фигуры Φ . Эта группа называется *полной группой фигуры Φ* и обозначается O_Φ . Подгруппу $SO_\Phi \subset O_\Phi$, состоящую из биекций, индуцированных собственными³ ортогональными операторами $\mathbb{R}^n \rightarrow \mathbb{R}^n$, мы будем называть *собственной группой фигуры Φ* . Если фигура $\Phi \subset \mathbb{R}^n$ содержится в некоторой гиперплоскости $\Pi \subset \mathbb{R}^n$, то собственная группа фигуры Φ совпадает с полной: беря композицию любого несобственного движения из группы фигуры с отражением в плоскости Π , мы получаем собственное движение, которое действует на фигуру Φ точно также, как и исходное несобственное движение.

Упражнение 12.10. Изготовьте модели пяти *платоновых тел* — тетраэдра, октаэдра, куба, додекаэдра и икосаэдра (см. [рис. 12◊5](#) – [рис. 12◊8](#) на стр. 185).

Пример 12.3 (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. 12◊1](#). Группа D_2 такой луночки совпадает с группами описанного вокруг неё прямоугольника и вписанного в неё ромба⁴. Она состоит из тождественного отображения и трёх поворотов на 180° 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.

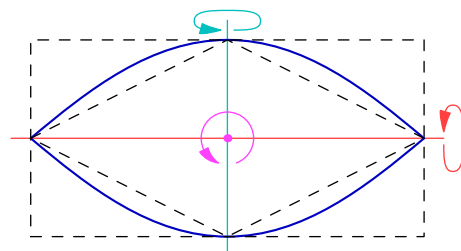


Рис. 12◊1. Двуугольник D_2 .

Упражнение 12.11. Убедитесь, что $D_2 \simeq \mathbb{Z}/(2) \oplus \mathbb{Z}/(2)$.

Следующая диэдральная группа — *группа треугольника D_3* — состоит из шести движений: тождественного, двух поворотов τ, τ^{-1} на $\pm 120^\circ$ вокруг центра треугольника и трёх

¹напомню, что *евклидовость* означает фиксацию в векторном пространстве \mathbb{R}^n симметричного билинейного положительного скалярного произведения $V \times V \rightarrow \mathbb{R}$, обозначаемого (v, w)

²линейный 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 $v = w$)

³т. е. ортогональными операторами определителя 1 или, что то же самое — сохраняющими ориентацию

⁴мы предполагаем, что луночка такова, что оба они не квадраты

осевых симметрий σ_{ij} относительно его медиан (см. рис. 12◊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 $\sigma_{23} = (1, 3, 2)$, $\sigma_{13} = (3, 2, 1)$, $\sigma_{12} = (2, 1, 3)$.

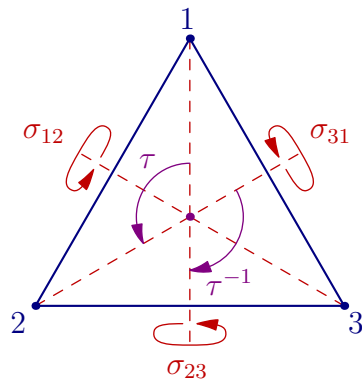


Рис. 12◊2. Группа треугольника.

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 углы¹ $2\pi k/n$ с $k = 0, 1, \dots, (n-1)$ и n осевых симметрий² 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. 12◊3).

Упражнение 12.12. Составьте таблицы умножения в группах D_3 , D_4 и D_5 , аналогичные таблице форм. (1-24) на стр. 14.

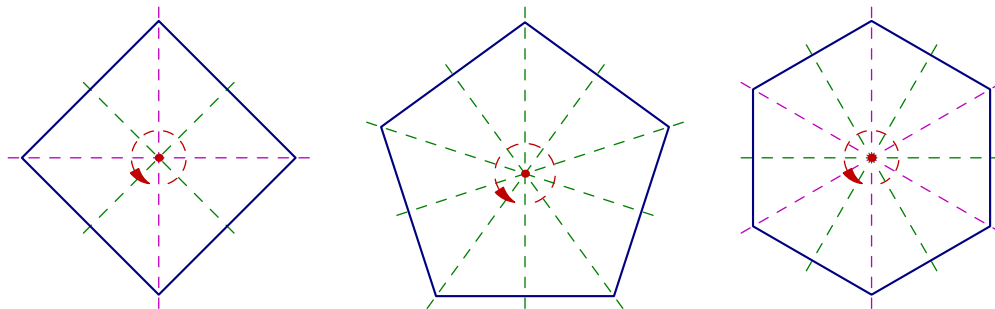


Рис. 12◊3. Оси диэдров D_4 , D_5 и D_6 .

Пример 12.4 (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.

¹при $k = 0$ получается тождественное преобразование

²или, что то же самое, поворотов на 180° в пространстве

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° вокруг прямых, проходящих через середины противоположных рёбер (см. рис. 12◊4). В несобственной группе, помимо перечисленных поворотов, имеется 6 отражений σ_{ij} в плоскостях, проходящих через середину ребра $[i, j]$ и противоположное ребро. При изоморфизме с S_4 отражение σ_{ij} переходит в транспозицию букв i и j , повороты на $\pm 120^\circ$, представляющие собой всевозможные композиции $\sigma_{ij}\sigma_{jk}$ с попарно различными i, j, k , переходят в циклические перестановки букв i, j, k , три вращения на $\pm 180^\circ$ относительно осей, соединяющих середины противоположных рёбер, — в одновременные транспозиции непересекающихся пар букв: $\sigma_{12}\sigma_{34} = (2, 1, 4, 3)$, $\sigma_{13}\sigma_{24} = (3, 4, 1, 2)$, $\sigma_{14}\sigma_{23} = (4, 3, 2, 1)$.

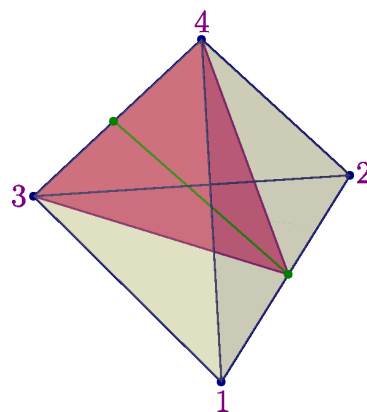


Рис. 12◊4. Плоскость симметрии σ_{12} и ось поворота $\sigma_{12}\sigma_{34}$ на 180° .

Упражнение 12.13. Убедитесь, что вместе с тождественным преобразованием эти три поворота образуют группу двуугольника D_2 .

Оставшиеся шесть несобственных преобразований тетраэдра отвечают шести циклическим перестановкам вершин $|1234\rangle$, $|1243\rangle$, $|1324\rangle$, $|1342\rangle$, $|1423\rangle$, $|1432\rangle$ 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 12.14. Выразите эти 6 движений через отражения σ_{ij} .

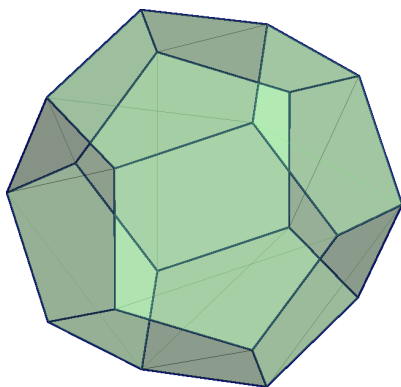


Рис. 12◊5. Додекаэдр.

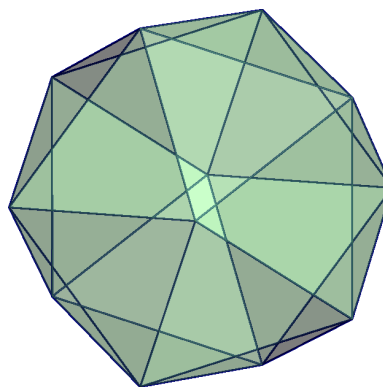


Рис. 12◊6. Икосаэдр.

Пример 12.5 (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. 12◊5 на стр. 184) 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° 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.

Упражнение 12.15. Покажите что полные группы куба, октаэдра и икосаэдра состоят, соответственно из 48, 48 и 120 движений, а собственные — из 24, 24 и 60 поворотов.

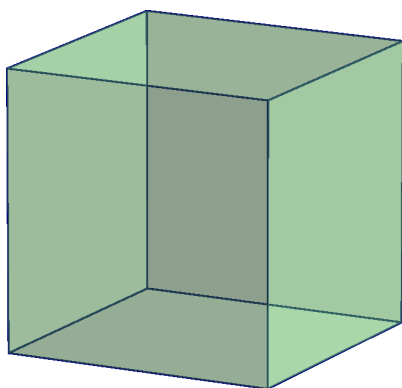


Рис. 12◊7. Куб.

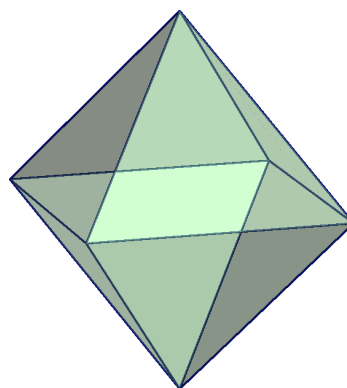


Рис. 12◊8. Октаэдр.

12.3. 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*, *мономорфизм* и *изоморфизм* применительно к отображению групп далее по умолчанию будут подразумевать, что это отображение является *гомоморфизмом* групп.

Упражнение 12.16. Убедитесь, что композиция гомоморфизмов тоже является гомоморфизмом.

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 $\varphi(g^{-1}) = \varphi(g)^{-1}$, поскольку $\varphi(g^{-1})\varphi(g) = \varphi(g^{-1}g) = \varphi(e_1) = e_2$. Поэтому образ

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

гомоморфизма групп является *подгруппой* группы G_2 . Полный прообраз единицы $e_2 \in G_2$

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

называется *ядром* гомоморфизма φ и является подгруппой в G_1 , поскольку из равенств $\varphi(g) = e_2$ и $\varphi(h) = e_2$ вытекает равенство $\varphi(gh) = \varphi(g)\varphi(h) = e_2e_2 = e_2$, а из равенства $\varphi(g) = e_2$ — равенство $\varphi(g^{-1}) = \varphi(g)^{-1} = e_2^{-1} = e_2$.

Предложение 12.1

Все непустые слои произвольного гомоморфизма групп $\varphi : G_1 \rightarrow G_2$ находятся во взаимно однозначном соответствии его ядром $\ker \varphi$, причём $\varphi^{-1}(\varphi(g)) = g(\ker \varphi) = (\ker \varphi)g$, где $g(\ker \varphi) \stackrel{\text{def}}{=} \{gh \mid h \in \ker \varphi\}$ и $(\ker \varphi)g \stackrel{\text{def}}{=} \{hg \mid h \in \ker \varphi\}$.

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

$$\ker \varphi \begin{array}{c} \xrightarrow{h \mapsto gh} \\ \xleftarrow{g^{-1}t \leftarrow t} \end{array} g(\ker \varphi)$$

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

Следствие 12.1

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

Следствие 12.2

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

$$|\operatorname{im}(\varphi)| = |G_1| / |\ker(\varphi)|. \quad (12-8)$$

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

Пример 12.6 (знакопеременные группы)

В сл. 9.1 на стр. 134 мы построили гомоморфизм симметрической группы в мультипликативную группу знаков $\operatorname{sgn} : S_n \rightarrow \{\pm 1\}$, сопоставляющий перестановке её знак. Ядро знакового гомоморфизма обозначается $A_n = \ker \operatorname{sgn}$ и называется *знакопеременной группой* или группой чётных перестановок. Порядок $|A_n| = n!/2$.

Пример 12.7 (линейные группы)

Все линейные автоморфизмы произвольного векторного пространства V над произвольным полем \mathbb{k} образуют *полную линейную группу* $GL(V)$. В н° 9.3.1 на стр. 138 мы построили гомоморфизм полной линейной группы в мультипликативную группу \mathbb{k}^* поля \mathbb{k} , сопоставляющий невырожденному линейному оператору $F : V \simeq V$ его определитель:

$$\det : GL(V) \rightarrow \mathbb{k}^*, \quad F \mapsto \det F. \quad (12-9)$$

Ядро этого гомоморфизма называется *специальной линейной группой* и обозначается

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

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

$$|GL_n(\mathbb{F}_q)| = (q^n - 1)(q^n - q)(q^n - q^2) \cdots (q^n - q^{n-1}),$$

поскольку элементы $GL(V) \simeq GL_n(\mathbb{F}_q)$ взаимно однозначно соответствуют базисам пространства V .

Упражнение 12.17. Убедитесь в этом.

Поскольку гомоморфизм (12-9) сюръективен¹ порядок специальной линейной группы

$$|SL_n(\mathbb{F}_q)| = |GL_n(\mathbb{F}_q)| / |\mathbb{K}^*| (q^n - 1)(q^n - q)(q^n - q^2) \cdots (q^n - q^{n-1}) / (q - 1)$$

Пример 12.8 (проективные группы)

Напомним², что *проективное пространство* $\mathbb{P}(V)$, ассоциированное с векторным пространством V , это множество, точками которого являются одномерные векторные подпространства в V или, что то же самое, классы пропорциональности ненулевых векторов в V . Каждый линейный оператор $F \in GL(V)$ 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 $GL(V)$ в группу биективных преобразований проективного пространства $\mathbb{P}(V)$. Образ этого гомоморфизма обозначается $PGL(V)$ и называется *проективной линейной группой* пространства V . Из курса геометрии известно, что два оператора $F, G \in GL(V)$ 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 $\lambda \in \mathbb{K}^*$. Поэтому ядром эпиморфизма групп

$$\pi : GL(V) \twoheadrightarrow PGL(V), \quad F \mapsto \bar{F} \quad (12-10)$$

является *подгруппа гомотетий* $\Gamma \simeq \mathbb{K}^*$, состоящая из диагональных скалярных операторов $v \mapsto \lambda v$, $\lambda \in \mathbb{K}^*$. Таким образом, группа $PGL(V)$ образована классами пропорциональности линейных операторов. Классы пропорциональности операторов с единичным определителем образуют в ней подгруппу, обозначаемую $PSL(V) \subset PGL(V)$. Ограничение эпиморфизма (12-10) на подгруппу $SL(V) \subset GL(V)$ доставляет эпиморфизм

$$\pi' : SL(V) \twoheadrightarrow PSL(V), \quad F \mapsto \bar{F} \quad (12-11)$$

ядром которого является конечная мультипликативная подгруппа $\mu_n(\mathbb{K}) \subset \mathbb{K}^*$ содержащихся в поле \mathbb{K} корней n -той степени из единицы, где³ $n = \dim V = \dim \mathbb{P}(V) + 1$.

Пример 12.9 (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 3 из которых не коллинеарны связана фигура, образованная тремя парами проходящих через эти точки прямых⁴

$$(ab) \text{ и } (cd), \quad (ac) \text{ и } (bd), \quad (ad) \text{ и } (bc) \quad (12-12)$$

и называемая *четырёхвершинником* (см. рис. 12◊9). Пары прямых (12-12) называются *противоположными сторонами* четырёхвершинника. С четырёхвершинником $abcd$ ассоциирован треугольник xuz с вершинами в точках пересечения пар противоположных сторон

$$x = (ab) \cap (cd) \quad y = (ac) \cap (bd) \quad z = (ad) \cap (bc) \quad (12-13)$$

¹диагональный оператор F с собственными значениями $(\lambda, 1, 1, \dots, 1)$ имеет $\det F = \lambda$

²мы предполагаем, что читатель знаком с проективными пространствами и проективными преобразованиями по курсу геометрии

³напомню, что по определению, $\dim \mathbb{P}(V) \stackrel{\text{def}}{=} \dim V - 1$

⁴они отвечают трём возможным способам разбить точки a, b, c, d на две пары

Каждая перестановка вершин a, b, c, d однозначно определяет линейное проективное преобразование¹ плоскости, что даёт вложение

$$S_4 \hookrightarrow \text{PGL}_3(\mathbb{k}).$$

Преобразования из S_4 переводят ассоциированный треугольник xyz в себя, переставляя его вершины x, y, z согласно формулам (12-13). 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 $S_4 \twoheadrightarrow S_3$. Его ядро имеет порядок $4!/3! = 4$ и состоит из тождественной перестановки и трёх пар независимых транспозиций

$$(b, a, d, c), \quad (c, d, a, b), \quad (d, c, b, a).$$

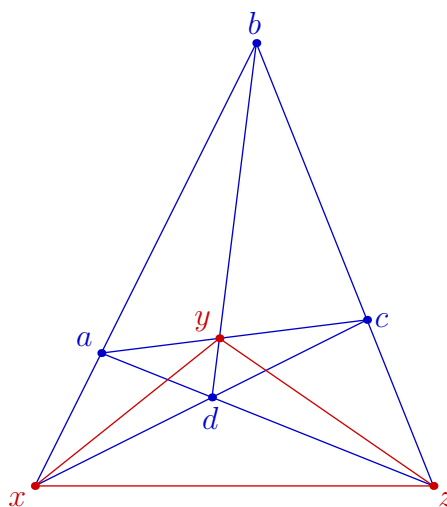


Рис. 12◊9. Четырёхвершинник и треугольник.

Пример 12.10 (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. 12◊10). На проективной плоскости $\mathbb{P}_2 = \mathbb{P}(\mathbb{R}^3)$ эти 7 прямых становятся вершинами четырёхвершинника $abcd$ и ассоциированного с ним треугольника xyz (см. рис. 12◊9). Поворот на 180° вокруг оси, соединяющей середины противоположных рёбер куба, меняет местами примыкающие к этому ребру диагонали и переводит в себя каждую их двух оставшихся диагоналей. Тем самым, вращения куба осуществляют транспозиции любых двух соседних диагоналей, и мы имеем сюръективный гомоморфизм

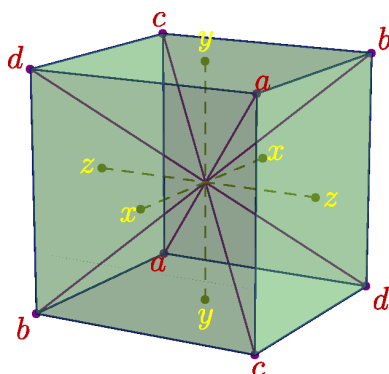


Рис. 12◊10. От куба к четырёхвершиннику.

$$\text{SO}_{\text{куб}} \twoheadrightarrow S_4. \tag{12-14}$$

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° 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° вокруг осей, проходящих через середины противоположных рёбер — в 6 простых транспозиций циклового типа $\square\square$.

¹напомню, 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

Гомоморфизм $SO_{\text{куб}} \rightarrow S_3$, возникающий из действия группы куба на прямых x, y, z , согласован с изоморфизмом (12-14) и эпиморфизмом $S_4 \rightarrow S_3$ из предыдущего прим. 12.9. 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 (12-14) переводит её в ядро эпиморфизма $S_4 \rightarrow S_3$ из предыдущего прим. 12.9.

Пример 12.11 (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 рисуется ровно одна диагональ¹, как на рис. 12◊11. Всего на поверхности додекаэдра имеется ровно 5 таких кубов — они биективно соответствуют пяти диагоналям какой-либо фиксированной грани. Собственная группа додекаэдра переставляет эти кубы друг с другом, что даёт гомоморфизм собственной группы додекаэдра в симметрическую группу S_5 :

$$\psi_{\text{дод}} : SO_{\text{дод}} \rightarrow S_5 \quad (12-15)$$

Глядя на модель додекаэдра, легко видеть, что образами $20 \cdot 3 = 60$ поворотов, из которых состоит группа $SO_{\text{дод}}$ будут в точности 60 чётных перестановок: $6 \cdot 4 = 24$ 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 $(\square\square\square)$; 15 поворотов на 180° вокруг осей, проходящих через середины противоположных рёбер додекаэдра, переходят во всевозможные пары независимых транспозиций, т. е. в 10 перестановок циклового типа $(\square\square)$. Оставшееся неучтённым тождественное преобразование додекаэдра задаёт тождественную перестановку кубов. Таким образом, гомоморфизм (12-15) является изоморфизмом собственной группы додекаэдра со знакопеременной подгруппой $A_5 \subset S_5$. В отличие от примера прим. 12.4 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.

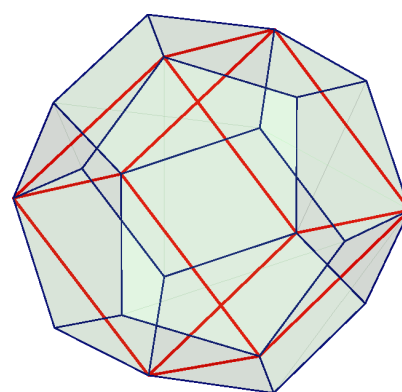


Рис. 12◊11. Один из пяти кубов на додекаэдре.

Упражнение 12.18. Покажите, что симметрическая группа S_5 не изоморфна полной группе додекаэдра.

¹проще всего это увидеть на модели додекаэдра, которую мы ещё раз настоятельно рекомендуем изготовить

12.4. 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 φ 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. $\forall g \in G \forall x \in X \quad gx = x \Rightarrow g = e$. Действие $\varphi : G \rightarrow \text{Aut} X$ называется *точным* (или *эффективным*), если каждый отличный от единицы элемент группы действует на X нетождественно, 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.

Пример 12.12 (регулярные действия)

Обозначим через X множество элементов группы G , а через $\text{Aut}(X)$ — группу автоморфизмов этого множества¹. Отображение $\lambda : G \rightarrow \text{Aut} X$, переводящее элемент $g \in G$ в преобразование² $\lambda_g : x \mapsto gx$ 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 обратный³ к g элемент.

Упражнение 12.19. Убедитесь, что ρ_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 12.13 (присоединённое действие)

Отображение $\text{Ad} : G \rightarrow \text{Aut}(G)$, сопоставляющее элементу $g \in G$ автоморфизм *сопряже-*

¹возможно, не перестановочных с имеющейся в G композицией, т. е. не обязательно являющихся автоморфизмами группы G

²обратите внимание, что это преобразование множества X не является гомоморфизмом группы G , поскольку равенство $g(h_1h_2) = (gh_1)(gh_2)$, вообще говоря, не выполняется

³появление 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)

ния этим элементом

$$\text{Ad}_g : G \rightarrow G, \quad h \mapsto ghg^{-1}, \quad (12-16)$$

называется *присоединённым действием* группы G на себе.

Упражнение 12.20. Убедитесь, что $\forall g \in G$ сопряжение (12-16) 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 (12-16) 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

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

Стабилизатор заданного элемента $g \in G$ в присоединённом действии состоит из всех элементов группы, коммутирующих с g . Он называется *централизатором* элемента g и обозначается $C_g = \text{Stab}_{\text{Int}(G)}(g) = \{h \in G \mid hg = gh\}$.

12.4.1. 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 *орбитой* x под действием G . Согласно н° 1.4 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 отображение¹ множеств $\text{ev}_x : G \rightarrow Gx$, $g \mapsto gx$, слой которого над точкой $y \in Gx$ состоит из всех преобразований из группы G , переводящих x в y . Он называется *транспортёром* из 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

$$\text{Stab}_G(x) = G_{xx} = \{g \in G \mid gx = x\} \quad (12-17)$$

или просто $\text{Stab}(x)$, если понятно, о какой группе G идёт речь.

Упражнение 12.21. Убедитесь, что $\text{Stab}_G(x)$ является подгруппой в группе G .

¹при желании его можно воспринимать как «некоммутативное» отображения вычисления

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:

$$\text{Stab}(x) \begin{array}{c} \xrightarrow{s \mapsto hsg^{-1}} \\ \xleftarrow{h^{-1}fg \mapsto f} \end{array} G_{zy}, \quad (12-18)$$

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

Предложение 12.2 (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 множеств G_{yx} по всем $y \in Gx$ и согласно предыдущему все эти множества состоят из $|\text{Stab}(x)|$ элементов. \square

Предложение 12.3

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 (12-18). \square

Пример 12.14 (действие перестановок букв на словах)

Зафиксируем какой-нибудь k -буквенный алфавит $A = \{a_1, a_2, \dots, a_k\}$ и рассмотрим множество X всех n -буквенных слов w , которые можно написать с его помощью. Иначе X можно воспринимать как множество всех отображений $w : \{1, 2, \dots, n\} \rightarrow A$. Сопоставим каждой перестановке $\sigma \in S_n$ преобразование $w \mapsto w\sigma^{-1}$, которое переставляет буквы в словах так, как предписывает¹ σ . 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 $|\text{Stab}(w)| = m_1! \cdot m_2! \cdot \dots \cdot m_k!$. Тем самым, длина орбиты такого слова равна мультиномиальному коэффициенту

$$|S_n w| = \frac{|S_n|}{|\text{Stab}(w)|} = \frac{n!}{m_1! \cdot m_2! \cdot \dots \cdot m_k!} = \binom{n}{m_1 \dots m_k}.$$

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

¹т. е. переводит слово $w = a_{v_1} a_{v_2} \dots a_{v_n}$ 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 σ в номер i

Упражнение 12.22. 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 12.15 (классы сопряжённости в симметрической группе)

Перестановка $\text{Ad}_g(\sigma) = g\sigma g^{-1}$, сопряжённая перестановке $\sigma = (\sigma_1, \sigma_2, \dots, \sigma_n) \in S_n$, для каждого $i = 1, 2, \dots, n$ переводит элемент $g(i)$ в элемент $g(\sigma_i)$. Поэтому при сопряжении цикла $\tau = (i_1, i_2, \dots, i_k) \in S_n$ перестановкой $g = (g_1, g_2, \dots, g_n)$ получится цикл

$$g\tau g^{-1} = (g_{i_1}, g_{i_2}, \dots, g_{i_k}).$$

Если перестановка $\sigma \in S_n$ имеет цикловой тип λ и является произведением независимых циклов, записанных по строкам диаграммы λ , то действие на такую перестановку внутреннего автоморфизма Ad_g заключается в применении отображения g к заполнению диаграммы λ , т. е. в замене каждого числа i числом g_i .

Таким образом, орбиты присоединённого действия симметрической группы S_n на себе взаимно однозначно соответствуют n -клеточным диаграммам Юнга, и орбита, отвечающая диаграмме λ , состоит из всех перестановок циклового типа λ . Если диаграмма λ имеет m_i строк длины i для каждого $i = 1, 2, \dots, n$, то централизатор любой перестановки σ циклового типа λ состоит из таких перестановок элементов заполнения диаграммы λ независимыми циклами перестановки σ , которые не меняют σ , 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 λ зависит только от λ и равен

$$z_\lambda = 1^{m_1} \cdot m_1! \cdot 2^{m_2} \cdot m_2! \cdot \dots \cdot n^{m_n} \cdot m_n! = \prod_{\alpha=1}^n m_\alpha! \alpha^{m_\alpha}.$$

Количество перестановок циклового типа λ , т. е. длина соответствующей орбиты присоединённого действия, равна $n!/z_\lambda$.

12.4.2. 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 12.2 (формула Поля – 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 12.16 (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 τ^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. 12◊12. Беря на этих рисунках все допустимые сочетания цветов, получаем, соответственно, n, n^2, n^3, n^4 и n^3 раскрасок. По теор. 12.2 искомое число 6-бусинных ожерелий равно $(n^6 + 3n^4 + 4n^3 + 2n^2 + 2n)/12$.

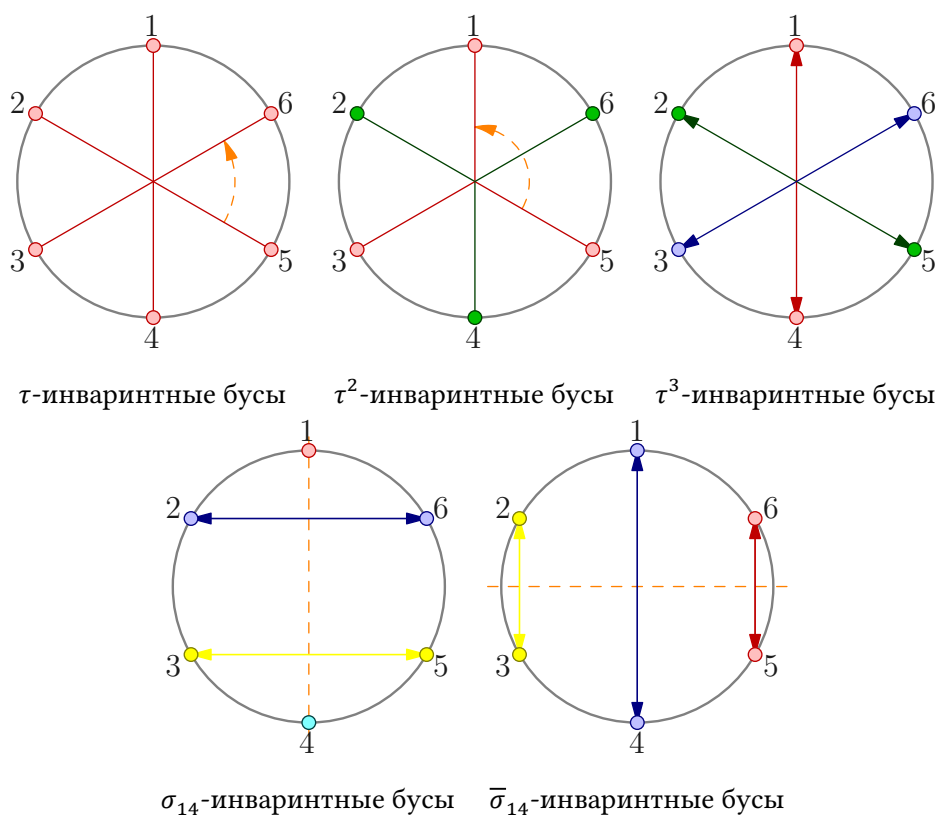


Рис. 12◊12. Симметричные ожерелья из шести бусин.

Упражнение 12.23. Подсчитайте количество ожерелий из 7, 8, 9, и 10 бусин.

12.5. 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

$$g_1 \sim_L g_2 \iff g_1 = hg_2 \text{ для некоторого } h \in H, \quad (12-19)$$

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 12.24. Покажите, что равенство $Hg_1 = Hg_2$ равносильно любому из эквивалентных друг другу включений $g_1^{-1}g_2 \in H$, $g_2^{-1}g_1 \in H$.

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

$$g_1 \sim_R g_2 \iff g_1 = g_2h \text{ для некоторого } h \in H, \quad (12-20)$$

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 12.3 (теорема Лагранжа об индексе подгруппы)

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

Следствие 12.3

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

12.5.1. Нормальные подгруппы. 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 (13-1) и (13-2) совпадают друг с другом и, в частности, $H \backslash G = G/H$. Если подгруппа $H \subset G$ нормальна, мы пишем $H \triangleleft G$.

Пример 12.17 (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 $g(\ker \varphi)g^{-1} \subset \ker \varphi$.

Упражнение 12.25. Покажите, что если для любого $g \in G$ есть включение $gHg^{-1} \subset H$, то все эти включения — равенства.

Отметим, что совпадение правых и левых смежных классов ядра $g(\ker \varphi) = (\ker \varphi)g$ уже было установлено нами ранее в [предл. 12.1](#).

Пример 12.18 ($V_4 \triangleleft S_4$)

Подгруппа Клейна $V_4 \subset S_4$ состоящая из перестановок циклового типа $\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$ и тождественной перестановки нормальна.

Пример 12.19 (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 $\varphi : G \xrightarrow{\simeq} G$, мы получаем внутренний автоморфизм $\varphi \circ \text{Ad}_g \circ \varphi^{-1} = \text{Ad}_{\varphi(g)}$.

Упражнение 12.26. Убедитесь в этом.

Пример 12.20 (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 τ_v на вектор v любым аффинным преобразованием $\varphi : \mathbb{A}^n \rightarrow \mathbb{A}^n$, получаем перенос¹ $\tau_{D_\varphi(v)}$ на вектор $D_\varphi(v)$.

Упражнение 12.27. Убедитесь в этом.

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

$$(g_1H) \cdot (g_2H) \stackrel{\text{def}}{=} (g_1g_2)H, \quad (12-21)$$

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 12.28. Убедитесь, что для группы $G = S_3$ и подгруппы второго порядка $H \subset G$, порождённой транспозицией σ_{12} , формула (13-3) некорректна.

Предложение 12.4

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 (13-3) корректна, то она задаёт на множестве смежных левых классов G/H групповую структуру: ассоциативность композиции наследуется из² G , единицей служит класс $eH = H$, обратным к классу gH — класс $g^{-1}H$. Факторизация $G \twoheadrightarrow G/H$, $g \mapsto gH$, является гомоморфизмом групп с ядром H . Поэтому подгруппа H нормальна в силу прим. 13.1. Наоборот, пусть H нормальна и пусть $f_1H = g_1H$ и $f_2H = g_2H$. Мы должны убедиться, что $(f_1f_2)H = (g_1g_2)H$. Так как левый смежный класс $f_2H = g_2H$ совпадает с правым классом Hg_2 , каждый элемент вида f_1f_2h можно переписать как $f_1h_1g_2$ с подходящими $h_1 \in H$. Аналогично, $f_1h_1 = h_2g_1$ для подходящего

¹напомним, что преобразование $\varphi : \mathbb{A}(V) \rightarrow \mathbb{A}(V)$ аффинного пространства $\mathbb{A}(V)$, ассоциированного с векторным пространством V , называется *аффинным*, если отображение $D_\varphi : \vec{p}\vec{q} \mapsto \varphi(\vec{p})\varphi(\vec{q})$ является корректно определённым линейным преобразованием векторного пространства V (оно называется *дифференциалом* отображения φ)

² $(g_1H \cdot g_2H) \cdot g_3H = (g_1g_2)H \cdot g_3H = ((g_1g_2)g_3)H = (g_1(g_2g_3))H = g_1H \cdot (g_2g_3)H = g_1H \cdot (g_2H \cdot g_3H)$

$h_2 \in H$ в виду равенств $f_1H = g_1H = Hg_1$. Наконец из равенства $H(g_1g_2) = (g_1g_2)H$ мы заключаем, что $f_1f_2h = h_2g_1g_2 = g_1g_2h_3$ для некоторого $h_3 \in H$, откуда $(f_1f_2)H \subset (g_1g_2)H$. Противоположное включение доказывается аналогично. \square

Определение 12.2

Множество смежных классов G/H нормальной подгруппы $H \triangleleft G$ с групповой структурой $g_1H \cdot g_2H \stackrel{\text{def}}{=} (g_1g_2)H$ называется *фактором* (или *фактор группой*) группы G по нормальной подгруппе H . Гомоморфизм групп $G \rightarrow G/H$, $g \mapsto gH$, называется *гомоморфизмом факторизации*.

Следствие 12.4

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 φ 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. 12.1](#) на стр. 186. \square

Предложение 12.5

Пусть $N, H \subset G$ — две подгруппы, причём $N \triangleleft G$ нормальна. Убедитесь, что множество $NN = \{hx \mid h \in N, x \in N\}$ является подгруппой в G , $H \cap N \triangleleft H$, $N \triangleleft HN$ и $NN/N \simeq H/(H \cap N)$.

Доказательство. $NN \subset G$ — подгруппа, поскольку при $h_1, h_2, h \in N$ и $x_1, x_2, x \in N$

$$\begin{aligned} h_1x_1h_2x_2 &= (h_1h_2)(h_2^{-1}x_1h_2 \cdot x_2) \in NN, \\ (hx)^{-1}x^{-1}h^{-1} &= h^{-1}(h_xh^{-1}) \in NN, \end{aligned} \tag{12-22}$$

т. к. $h_2^{-1}x_1h_2 \in N$ и $h_xh^{-1} \in N$. Нормальность $H \cap N \triangleleft H$ следует из нормальности $N \triangleleft G$. Сюръективное отображение $\varphi : NN \rightarrow H/(H \cap N)$, переводящее произведение hx в класс $h \cdot (H \cap N)$, корректно определено, поскольку $h_1x_1 = h_2x_2 \Rightarrow h_1^{-1}h_2 = x_1x_2^{-1} \in H \cap N$, откуда $h_1 \cdot (H \cap N) = h_1 \cdot (h_1^{-1}h_2) \cdot (H \cap N) = h_2 \cdot (H \cap N)$. Вычисление (13-4) показывает, что φ — гомоморфизм групп. Так как $\ker \varphi = eN = N$, по [сл. 13.2](#) имеем $H/(H \cap N) = \text{im } \varphi \simeq \simeq NN/\ker \varphi = NN/N$. \square

Упражнение 12.29. 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 $G_1/N_1 \simeq G_2/N_2$.

12.5.3. Геометрический смысл нормальности. Согласно [предл. 13.1](#) и [прим. 13.1](#) нормальность подгруппы $H \subset G$ равносильна наличию гомоморфизма $\varphi : G \rightarrow G'$ с ядром $H = \ker \varphi$. Если группа G' представлена как группа преобразований¹ какого-либо множества X , то возникает такое действие $G \rightarrow \text{Aut } X$ исходной группы G на X , что H состоит из всех преобразований группы G , оставляющих на месте каждую точку X . Таким образом, нормальность подгруппы H означает наличие действия группы G на некоем множестве X с ядром H . Например, четвертная подгруппа Клейна $V_4 \subset S_4$ является ядром действия собственной группы куба на парах противоположных граней.

¹как мы видели в [прим. 12.12](#), такое представление всегда возможно

Ответы и указания к некоторым упражнениям

Упр. 12.1. Если $fg = e$ и $gh = e$, то $f = fe = f(gh) = (fg)h = eh = h$.

Упр. 12.2. Для двух единичных элементов e' и e'' выполнены равенства $e' = e'e'' = e''$.

Упр. 12.4. 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

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

не более одного раза. Доказательство аналогично доказательству [предл. 11.3](#) на стр. 166.

Упр. 12.5. Пусть $k = dr$, $m = \text{ord}(\tau) = ds$, где $\text{nod}(r, s) = 1$. Если $d > 1$, то τ^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 τ^k тоже цикл длины m . Если для какого-то элемента a цикла τ выполняется равенство $(\tau^k)^r(a) = a$, то kr делится на m , что при $\text{nod}(k, m) = 1$ возможно только когда r делится на m . Поэтому $r \geq m$, т. е. длина содержащего a цикла перестановки τ^k не меньше m .

Упр. 12.6. Ответ: $n(n-1) \cdots (n-k+1)/k$ (в числителе дроби k сомножителей).

Упр. 12.7. Непересекающиеся циклы очевидно коммутируют. Если коммутирующие циклы τ_1 и τ_2 пересекаются по элементу a , то $\tau_1(a)$ является элементом цикла τ_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 τ_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 τ_1 действует на него как τ_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. 12.5](#).

Упр. 12.8. Ответ: $n! / \prod_{i=1}^n i^{m_i} m_i!$ (ср. с формулой (1-12) на стр. 10). Решение: сопоставим каждому заполнению диаграммы циклов λ 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 λ ; 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. 12.9. $|1, 6, 3, 4\rangle^{15} \cdot |2, 5, 8\rangle^{15} \cdot |7, 9\rangle^{15} = |1, 6, 3, 4\rangle^{-1} \cdot |7, 9\rangle = (4, 2, 6, 3, 5, 1, 9, 8, 7)$

Упр. 12.14. 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. 12.15. 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. 12.17. Зафиксируем в V какой-либо базис и сопоставим оператору $F \in GL(V)$ 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. 12.18. 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. 12.22. 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 $|SO_{\text{ико}}| = 20 \cdot 3 = 60$ и $|O_{\text{ико}}| = 20 \cdot 6 = 120$.
- Упр. 12.24. 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 $g_1^{-1} g_2$ и $g_2^{-1} g_1$ 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. 12.25. Включение $g H g^{-1} \subset H$ влечёт включение $H \subset g^{-1} H g$. Если это так для всех $g \in G$, то заменяя g на g^{-1} мы получаем обратное к исходному включение $g H g^{-1} \supset H$.
- Упр. 12.26. $\varphi \circ \text{Ad}_g \circ \varphi^{-1} : h \mapsto \varphi(g \varphi^{-1}(h) g^{-1}) = \varphi(g) h \varphi(g)^{-1}$.
- Упр. 12.27. 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. 12.29. 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 .