§12. Группы

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

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

$$\text{наличие единицы:} \qquad \exists\, e \in G \;:\; \forall\, g \in G \quad eg = g \tag{12-2}$$

$$\text{наличие обратных:} \qquad \forall\, g \in G \quad \exists\, g^{-1} \in G \;:\; g^{-1}g = e \tag{12-3}$$

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

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

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 $\left(g_1 g_2 \cdots g_k\right)^{-1} = g_k^{-1} \cdots g_2^{-1} g_1^{-1}$.

Для единицы e из (12-2) при любом $g \in G$ выполнятся 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 n° 1.6. Все взаимно однозначные отображения произвольного множества X в себя очевидно образуют группу. Она обозначается $\operatorname{Aut} X$ и называется *группой автоморфизмов* множества X. Подгруппы $G \subset \operatorname{Aut} X$ 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 $g^0 \overset{\text{def}}{=} e$ и $g^{-n} \overset{\text{def}}{=} \left(g^{-1}\right)^n$. Она называется *циклической подгруппой*, порождённой g и обозначается $\langle g \rangle$. Будучи абелевой группой с одной образующей, $\langle g \rangle$ является образом сюрьективного 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 $\langle g \rangle \simeq \simeq \mathbb{Z}/(n)$, где $n \in \mathbb{N}$ — наименьшая степень, для которой $g^n = e$. Она называется *порядком* элемента g и обозначается $\operatorname{ord}(g)$. В этом случае группа $\langle g \rangle$ имеет порядок[1] $n = \operatorname{ord} g$ и состоит из элементов $e = g^0,\ g = g^1,\ g^2,\ \dots,\ g^{n-1}$. Если $\ker \varphi_g = 0$, то $\varphi_g : \mathbb{Z} \xrightarrow{\sim} \langle g \rangle$ является изоморфизмом и все степени g^m попарно различны. В этом случае говорят, что g имеет *бесконечный порядок* и пишут $\operatorname{ord} g = \infty$.

Напомним[2], 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 классов[3] $[\pm 1]_6$, $[\pm 3]_6$.

Упражнение 12.4. Укажите необходимые и достаточные условия для того, чтобы конечно порождённая абелева группа[4] $G = \mathbb{Z}^r \oplus \frac{\mathbb{Z}}{(p_1^{n_1})} \oplus \dots \oplus \frac{\mathbb{Z}}{(p_\alpha^{n_\alpha})}$ была циклической.

Лемма 12.1
Элемент $h = g^k$ тогда и только тогда является образующей циклической группы $\langle g \rangle$ порядка n, когда $\text{нод}(k, n) = 1$.

Доказательство. Так как $\langle h \rangle \subset \langle g \rangle$, равенство $\langle h \rangle = \langle g \rangle$ равносильно неравенству $\operatorname{ord} h \geqslant n$. Но $h^m = g^{mk} = e$ тогда и только тогда, когда mk делится на n. Если $\text{нод}(n, k) = 1$, то это возможно только при m делящемся на n, и в этом случае $\operatorname{ord} h \geqslant n$. Если же $n = n_1 d$ и $k = k_1 d$, где $d > 1$, то $h^{n_1} = g^{kn_1} = g^{nk_1} = e$ и $\operatorname{ord} h \leqslant n_1 < n$. □

12.1.2. Разложение перестановок в композиции циклов. Перестановка $\tau \in S_n$ по кругу переводящая друг в друга какие-нибудь m различных элементов[5]

$$i_1 \mapsto i_2 \mapsto \ \cdots \ \mapsto i_{m-1} \mapsto i_m \mapsto i_1 \tag{12-5}$$

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 $\text{нод}(k, m) = 1$.

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?

[1]таким образом, порядок элемента равен порядку порождённой им циклической подгруппы
[2]см. n° 3.5.1 на стр. 47
[3]обратите внимание, что остальные 6 классов не являются образующими
[4]см. теор. 10.5 на стр. 160
[5]числа $i_1, i_2, \dots, i_m$ могут быть любыми, не обязательно соседними или возрастающими

Теорема 12.1
Каждая перестановка $g \in S_n$ является композицией непересекающихся циклов:

$$g = \tau_1 \tau_2 \cdots \tau_k \,. \tag{12-6}$$

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

$$x \overset{g}{\longmapsto} g(x) \overset{g}{\longmapsto} g^2(x) \overset{g}{\longmapsto} g^3(x) \overset{g}{\longmapsto} \cdots , \tag{12-7}$$

возникающей при применении g к произвольной точке $x \in X$, случится повтор. Так как преобразование $g : X \xrightarrow{\sim} X$ 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. □

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 циклов[1], 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

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

имеет цикловой тип $\begin{array}{|c|c|c|c|}\hline \; & \; & \; & \; \\ \hline & & \\ \cline{1-3} & \\ \cline{1-2} \end{array}$, 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

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

[1]включая 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 евклидовом[1] пространстве $\mathbb{R}^n$ биективные отображения $\Phi \to \Phi$ индуцированные ортогональными[2] 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 $\mathrm{SO}_\Phi \subset \mathrm{O}_\Phi$, состоящую из биекций, индуцированных собственными[3] ортогональными операторами $\mathbb{R}^n \to \mathbb{R}^n$, 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 ромба[4]. 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.

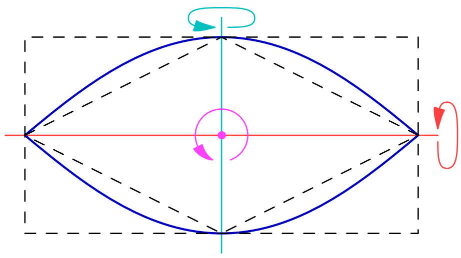


Рис. 12◇1. Двуугольник D_2.

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 $\pm 120°$ вокруг центра треугольника и трёх

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

[2] линейный оператор $F : \mathbb{R}^n \to \mathbb{R}^n$ 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 $v = w$)

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

[4] мы 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 $\pm 120°$ отождествляются с циклическими перестановками $(2, 3, 1)$, $(3, 1, 2)$, а осевые симметрии — с транспозициями $\sigma_{23} = (1, 3, 2)$, $\sigma_{13} = (3, 2, 1)$, $\sigma_{12} = (2, 1, 3)$.

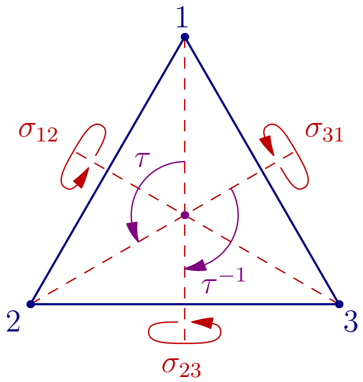


Рис. 12◇2. Группа треугольника.

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 $n \geqslant 2$ 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[2] 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.

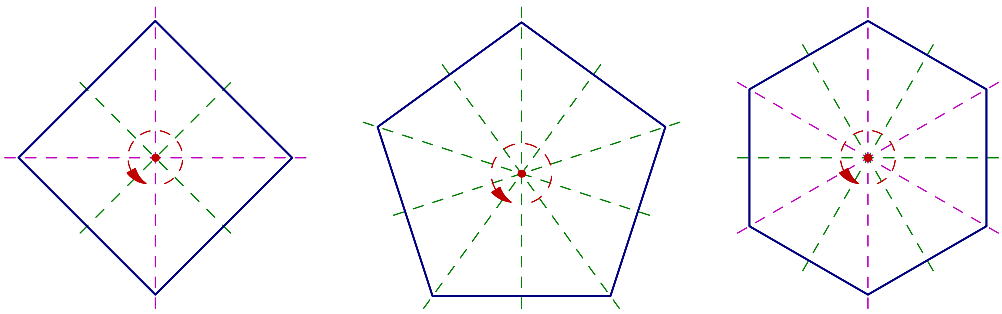


Рис. 12◇3. Оси диэдров D_4, D_5 и D_6.

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.

[1]при $k = 0$ получается тождественное преобразование

[2]или, 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: $\sigma_{12}\sigma_{34} = (2, 1, 4, 3)$, $\sigma_{13}\sigma_{24} = (3, 4, 1, 2)$, $\sigma_{14}\sigma_{23} = (4, 3, 2, 1)$.

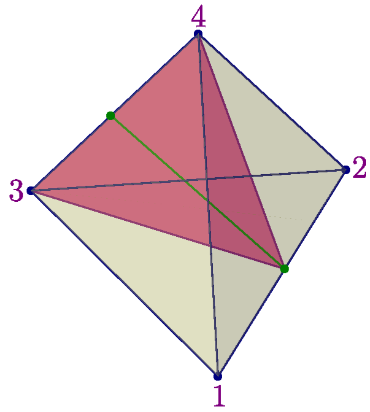


Рис. 12◇4. Плоскость симметрии σ_{12} и ось поворота $\sigma_{12}\sigma_{34}$ на 180°.

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}.

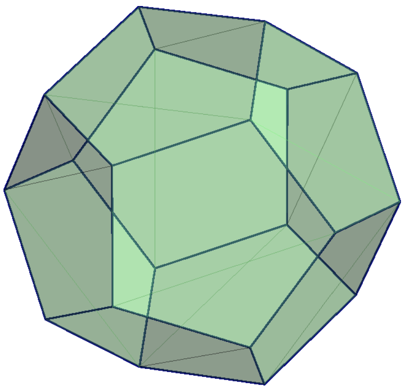


Рис. 12◇5. Додекаэдр.

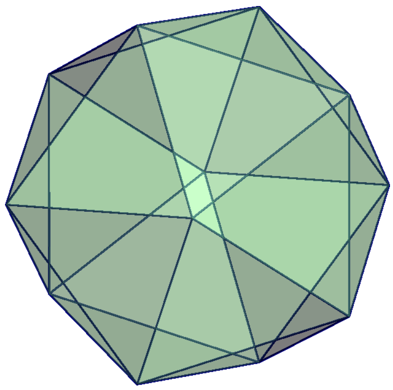


Рис. 12◇6. Икосаэдр.

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 $2\pi k/5$, $1 \leqslant k \leqslant 4$, 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.

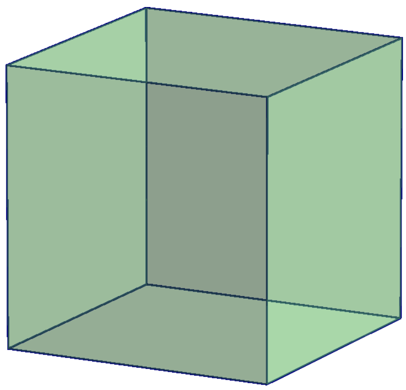


Рис. 12◇7. Куб.

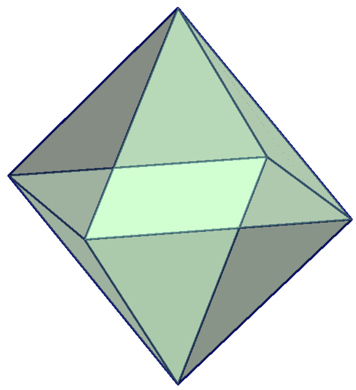


Рис. 12◇8. Октаэдр.

12.3. Гомоморфизмы групп. Отображение групп $\varphi : G_1 \to G_2$ 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 $\varphi : G_1 \to G_2$ 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

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

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

$$\ker\varphi \stackrel{\text{def}}{=} \varphi^{-1}\left(e_2\right) = \left\{ g \in G_1 \mid \varphi(g_1) = e_2 \right\} .$$

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 $\varphi : G_1 \to G_2$ находится во взаимно однозначном соответствии его ядром $\ker\varphi$, причём $\varphi^{-1}\big(\varphi(g)\big) = g(\ker\varphi) = (\ker\varphi)g$, где $g(\ker\varphi) \overset{\text{def}}{=} \{gh \mid h \in \ker\varphi\}$ и $(\ker\varphi)g \overset{\text{def}}{=} \{hg \mid h \in \ker\varphi\}$.

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 $\varphi^{-1}\big(\varphi(g)\big)$ 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

$$\begin{tikzcd} \ker\varphi \arrow[r, bend left, "h\mapsto gh"] & g(\ker\varphi) \arrow[l, bend left, "g^{-1}t \mapsfrom t"] \end{tikzcd}$$

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

Следствие 12.1
Для того, чтобы гомоморфизм групп $\varphi : G_1 \to G_2$ был инъективен, необходимо и достаточно, чтобы его ядро исчерпывалось единичным элементом. □

Следствие 12.2
Для любого гомоморфизма конечных групп $\varphi : G_1 \to G_2$ выполнено равенство

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

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

Пример 12.6 (знакопеременные группы)
В сл. 9.1 на стр. 134 мы построили гомоморфизм симметрической группы в мультипликативную группу знаков $\operatorname{sgn} : S_n \to \{\pm 1\}$, 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 $\Bbbk$ образуют *полную линейную группу* $\mathrm{GL}(V)$. В n° 9.3.1 на стр. 138 мы построили гомоморфизм полной линейной группы в мультипликативную группу $\Bbbk^*$ поля $\Bbbk$, сопоставляющий невырожденному линейному оператору $F : V \xrightarrow{\sim} V$ его определитель:

$$\det : \mathrm{GL}(V) \to \Bbbk^*\,, \quad F \mapsto \det F\,. \tag{12-9}$$

Ядро этого гомоморфизма называется *специальной линейной группой* и обозначается

$$\mathrm{SL}(V) = \ker\det = \{F : V \xrightarrow{\sim} V \ \ \det F = 1\}.$$

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

$$\left|\mathrm{GL}_n(\mathbb{F}_q)\right| = (q^n - 1)(q^n - q)(q^n - q^2)\ \cdots\ (q^n - q^{n-1})\,,$$

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

Упражнение 12.17. Убедитесь в этом.

Поскольку гомоморфизм (12-9) сюрьективен[1] порядок специальной линейной группы

$$\left|\mathrm{SL}_n(\mathbb{F}_q)\right| = \left|\mathrm{GL}_n(\mathbb{F}_q)\right| / |\Bbbk^*| (q^n - 1)(q^n - q)(q^n - q^2) \cdots (q^n - q^{n-1})/(q-1)$$

Пример 12.8 (проективные группы)

Напомним[2], 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 $F \in \mathrm{GL}(V)$ корректно задаёт биекцию $\overline{F} : \mathbb{P}(V) \to \mathbb{P}(V)$, переводящую класс вектора $v \neq 0$ в класс вектора $F(v)$. Таким образом возникает гомоморфизм $F \mapsto \overline{F}$ группы $\mathrm{GL}(V)$ в группу биективных преобразований проективного пространства $\mathbb{P}(V)$. Образ этого гомоморфизма обозначается $\mathrm{PGL}(V)$ и называется *проективной линейной группой* пространства V. Из курса геометрии известно, что два оператора $F, G \in \mathrm{GL}(V)$ тогда и только тогда задают одинаковые преобразования $\overline{F} = \overline{G}$ проективного пространства $\mathbb{P}(V)$, когда они пропорциональны, т. е. $F = \lambda G$ для некоторого $\lambda \in \Bbbk^*$. Поэтому ядром эпиморфизма групп

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

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

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

ядром которого является конечная мультипликативная подгруппа $\boldsymbol{\mu}_n(\Bbbk) \subset \Bbbk^*$ содержащихся в поле $\Bbbk$ корней n-той степени из единицы, где[3] $n = \dim V = \dim \mathbb{P}(V) + 1$.

Пример 12.9 (эпиморфизм $S_4 \twoheadrightarrow S_3$)

На проективной плоскости $\mathbb{P}_2$ над любым полем $\Bbbk$ с каждой четвёркой точек a, b, c, d, никакие 3 из которых не коллинеарны связана фигура, образованная тремя парами проходящих через эти точки прямых[4]

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

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

$$x = (ab) \cap (cd) \qquad y = (ac) \cap (bd) \qquad z = (ad) \cap (bc) \tag{12-13}$$

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

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

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

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

Каждая перестановка вершин a, b, c, d однозначно определяет линейное проективное преобразование[1] плоскости, что даёт вложение

$$S_4 \hookrightarrow \mathrm{PGL}_3(\Bbbk)\,.$$

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 сюрьективный гомоморфизм $S_4 \twoheadrightarrow S_3$. Его ядро имеет порядок $4!/3! = 4$ и состоит из тождественной перестановки и трёх пар независимых транспозиций

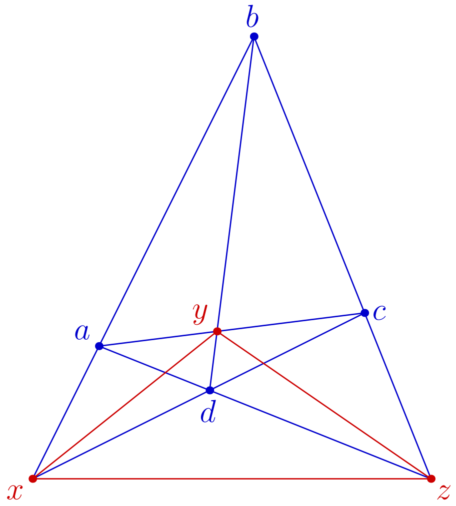


Рис. 12◇9. Четырёхвершинник и треугольник.

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

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 сюрьективный гомоморфизм

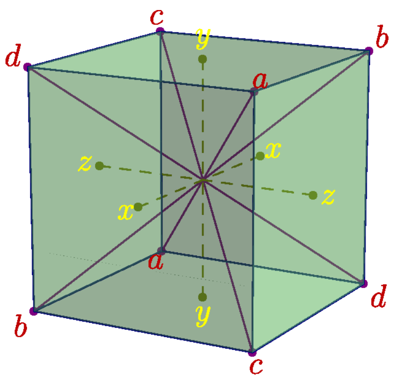


Рис. 12◇10. От куба к четырёхвершиннику.

$$\mathrm{SO}_{\text{куб}} \to S_4\,. \tag{12-14}$$

Так как обе группы имеют порядок 24, это изоморфизм. Он переводит 6 поворотов на ±90° вокруг прямых x, y, z в 6 циклов длины 4 циклового типа, 3 поворота на 180° вокруг тех же прямых — в 3 пары независимых транспозиций циклового типа, 8 поворотов на ±120° вокруг прямых a, b, c, d — в 8 циклов длины 3 циклового типа, а 6 поворотов на 180° вокруг осей, проходящих через середины противоположных рёбер — в 6 простых транспозиций циклового типа.

[1]напомню, что каждое линейное проективное преобразование $\overline{F} \in \mathrm{PGL}(V)$ 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 $\mathrm{SO}_{\text{куб}} \to S_3$, возникающий из действия группы куба на прямых x, y, z, согласован с изоморфизмом (12-14) и эпиморфизмом $S_4 \twoheadrightarrow S_3$ 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 $S_4 \twoheadrightarrow S_3$ 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 диагональ[1], 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:

$$\psi_{\text{дод}} : \mathrm{SO}_{\text{дод}} \to S_5 \tag{12-15}$$

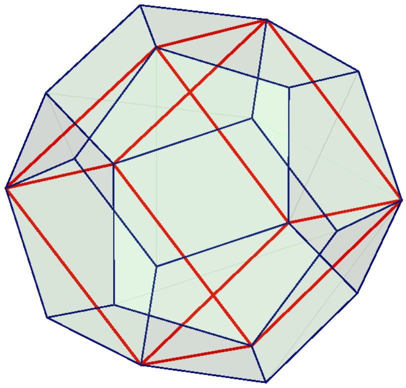


Рис. 12◇11. Один из пяти кубов на додекаэдре.

Глядя на модель додекаэдра, легко видеть, что образами $20 \cdot 3 = 60$ поворотов, из которых состоит группа $\mathrm{SO}_{\text{дод}}$ будут в точности 60 чётных перестановок: $6 \cdot 4 = 24$ поворота на углы $2\pi k/5$, $1 \leqslant k \leqslant 4$, 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 $\begin{smallmatrix}\square\square\square\\ \square\\ \square\end{smallmatrix}$; 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 $\begin{smallmatrix}\square\square\\ \square\square\\ \square\end{smallmatrix}$. 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.

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

---

[1]проще 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 $\mathrm{Aut}(X)$ группу всех взаимно однозначных отображений из X в себя. Гомоморфизм $\varphi : G \to \mathrm{Aut}(X)$ называется *действием* группы G на множестве X или *представлением* группы G автоморфизмами множества X. Отображение $\varphi(g) : X \to X$, отвечающее элементу $g \in G$ при действии φ часто бывает удобно обозначать через $\varphi_g : X \to X$. 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 *m-транзитивным*, если любые два упорядоченных набора из m 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 $\varphi : G \to \mathrm{Aut}\, X$ 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 $\varphi(G) \subset \mathrm{Aut}(X)$ множества X. Отметим, что любое свободное действие точно.

Пример 12.12 (регулярные действия)
Обозначим через X множество элементов группы G, а через $\mathrm{Aut}(X)$ — группу автоморфизмов этого *множества*[1]. Отображение $\lambda : G \to \mathrm{Aut}\, X$, переводящее элемент $g \in G$ в преобразование[2] $\lambda_g : x \mapsto gx$ левого умножения на g является гомоморфизмом групп, поскольку $\lambda_{gh}(x) = ghx = \lambda_g(hx) = \lambda_g\left(\lambda_h(x)\right) = \lambda_g \circ \lambda_h(x)$. 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* $\varrho_g : G \to \mathrm{Aut}(X)$ сопоставляет элементу $g \in G$ преобразование $x \mapsto xg^{-1}$ правого умножения на обратный[3] 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 $\mathbb{R}^* = \mathbb{R} \smallsetminus \{0\}$.

Пример 12.13 (присоединённое действие)
Отображение $\mathrm{Ad} : G \to \mathrm{Aut}(G)$, сопоставляющее элементу $g \in G$ автоморфизм *сопряже-*

---

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

[2] обратите 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

[3] 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)

ния этим элементом
$$\mathrm{Ad}_g : G \to G\,, \quad h \mapsto ghg^{-1}\,, \tag{12-16}$$
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 $g \mapsto \mathrm{Ad}_g$ является гомоморфизмом из G в $\mathrm{Aut}\, G$.

Образ присоединённого действия $\mathrm{Ad}(G) \subset \mathrm{Aut}\, G$ обозначается $\mathrm{Int}(G)$ и называется группой *внутренних автоморфизмов* группы G. Не лежащие в $\mathrm{Int}(G)$ 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 $\ker(\mathrm{Ad})$ 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
$$Z(G) = \ker(\mathrm{Ad}) = \{g \in G \mid \ \forall\, h{\in}G \ \ gh = hg\}\,.$$

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

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 n° 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 сюрьективное отображение[1] множеств $\mathrm{ev}_x : G \twoheadrightarrow Gx$, $g \mapsto gx$, 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
$$\mathrm{Stab}_G(x) = G_{xx} = \{g \in G \mid gx = x\} \tag{12-17}$$
или просто $\mathrm{Stab}(x)$, если понятно, о какой группе G идёт речь.

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

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

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

$$\mathrm{Stab}(x) \underset{h^{-1}fg \leftarrow\!\shortmid f}{\overset{s \mapsto hsg^{-1}}{\rightleftarrows}} G_{zy}\,, \tag{12-18}$$

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

Предложение 12.2 (формула для длины орбиты)
Длина орбиты произвольной точки x при действии на неё конечной группы преобразований G равна $|Gx| = |G| : |\mathrm{Stab}_G(x)|$. В частности, длины всех орбит и порядки стабилизаторов всех точек являются делителями порядка группы.

Доказательство. Группа G является дизъюнктным объединением множеств G_{yx} по всем $y \in Gx$ и согласно предыдущему все эти множества состоят из $|\mathrm{Stab}(x)|$ элементов. □

Предложение 12.3
Стабилизаторы всех точек, лежащих в одной орбите конечной группы, сопряжены:

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

В частности, все они имеют одинаковый порядок.

Доказательство. Это сразу следует из диаграммы (12-18). □

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 $w : \{1, 2, \dots, n\} \to A$. Сопоставим каждой перестановке $\sigma \in S_n$ преобразование $w \mapsto w\sigma^{-1}$, которое переставляет буквы в словах так, как предписывает[1] 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 $\mathrm{Stab}(w)$ 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 $|\mathrm{Stab}(w)| = m_1! \cdot m_2! \cdot \dots \cdot m_k!$. Тем самым, длина орбиты такого слова равна мультиномиальному коэффициенту

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

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

[1] т. е. переводит слово $w = a_{\nu_1} a_{\nu_2} \dots a_{\nu_n}$ в слово $a_{\nu_{\sigma^{-1}(1)}} a_{\nu_{\sigma^{-1}(2)}} \dots a_{\nu_{\sigma^{-1}(n)}}$, 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 $\mathrm{Ad}_g(\sigma) = g\sigma g^{-1}$, 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 $\tau = |i_1, i_2, \dots, i_k\rangle \in S_n$ перестановкой $g = (g_1, g_2, \dots, g_n)$ получится цикл

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

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

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

Количество перестановок циклового типа λ, т. е. длина соответствующей орбиты присоединённго 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 Полиа – Бернсайда)
Пусть конечная группа G действует на конечном множестве X. Для каждого $g \in G$ обозначим через $X^g = \{x \in X \mid gx = x\} = \{x \in X \mid g \in \mathrm{Stab}(x)\}$ множество неподвижных точек преобразования g. Тогда $|X/G| = |G|^{-1} \sum\limits_{g \in G} |X^g|$.

Доказательство. Обозначим через $F \subset G \times X$ множество всех таких пар (g, x), что $gx = x$. Иначе F можно описать как $F = \bigsqcup\limits_{x \in X} \mathrm{Stab}(x) = \bigsqcup\limits_{g \in G} X^g$. Первое из этих описаний получается из рассмотрения проекции $F \to X$, второе — из рассмотрения проекции $F \to G$. Согласно второму описанию, $|F| = \sum\limits_{g \in G} |X^g|$. 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. □

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 $\pm 60°$, двух поворотов $\tau^{\pm 2}$ на $\pm 120°$, центральной симметрии τ^3, трёх отражений σ_{14}, σ_{23}, σ_{36} относительно больших диагоналей и трёх отражений $\overline{\sigma}_{14}$, $\overline{\sigma}_{23}$, $\overline{\sigma}_{36}$ 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 $\left(n^6 + 3\,n^4 + 4\,n^3 + 2\,n^2 + 2\,n\right)/12$.

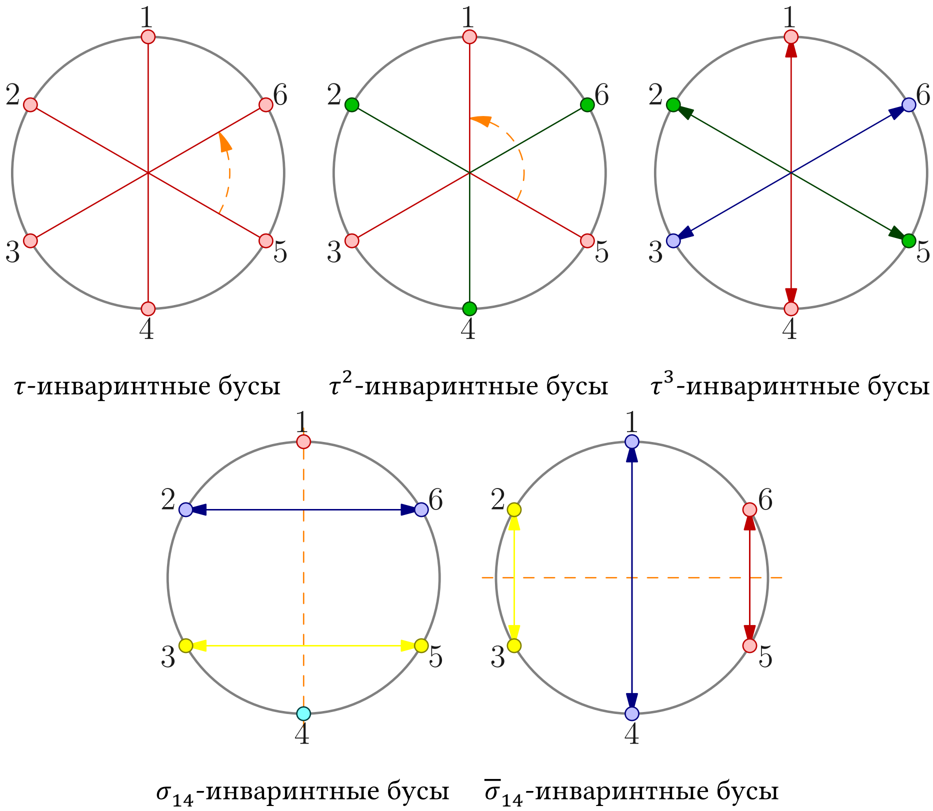


Рис. 12◇12. Симметричные ожерелья из шести бусин.

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

$$g_1 \underset{L}{\sim} g_2 \iff g_1 = hg_2 \text{ для некоторого } h \in H\,, \tag{12-19}$$

разбивающей группу G в дизъюнктное объединение орбит вида $Hg \overset{\text{def}}{=} \{hg \mid h \in H\}$, 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 $\varrho_h : g \mapsto gh^{-1}$ связано отношение эквивалентности

$$g_1 \underset{R}{\sim} g_2 \iff g_1 = g_2 h \text{ для некоторого } h \in H\,, \tag{12-20}$$

разбивающее группу G в дизъюнктное объединение орбит $gH \overset{\text{def}}{=} \{gh \mid h \in H\}$, 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 $[G : H] \overset{\text{def}}{=} |G/H|$. 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 $\langle g \rangle \subset G$. □

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

Пример 12.17 (ядра гомоморфизмов)
Ядро любого гомоморфизма групп $\varphi : G_1 \to G_2$ 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 ($V_4 \lhd S_4$)
Подгруппа Клейна $V_4 \subset S_4$ состоящая из перестановок циклового типа $\begin{array}{|c|c|}\hline \ & \ \\ \hline \ & \ \\ \hline\end{array}$ и тождественной перестановки нормальна.

Пример 12.19 (внутренние автоморфизмы)
Подгруппа внутренних автоморфизмов $\mathrm{Int}(G) = \mathrm{Ad}(G)$ нормальна в группе $\mathrm{Aut}(G)$ всех автоморфизмов группы G, поскольку сопрягая внутренний автоморфизм $\mathrm{Ad}_g : h \mapsto ghg^{-1}$ произвольным автоморфизмом $\varphi : G \xrightarrow{\sim} G$, мы получаем внутренний автоморфизм $\varphi \circ \mathrm{Ad}_g \circ \varphi^{-1} = \mathrm{Ad}_{\varphi(g)}$.

Упражнение 12.26. Убедитесь в этом.

Пример 12.20 (параллельные переносы)
Подгруппа параллельных переносов нормальна в группе $\mathrm{Aff}(\mathbb{A}^n)$ всех биективных аффинных преобразований аффинного пространства $\mathbb{A}^n$, т. к. сопрягая параллельный перенос τ_v на вектор v любым аффинным преобразованием $\varphi : \mathbb{A}^n \to \mathbb{A}^n$, получаем перенос[1] $\tau_{D_\varphi(v)}$ 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

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

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 из[2] 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

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

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

$h_2 \in H$ 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. □

Определение 12.2
Множество смежных классов G/H нормальной подгруппы $H \lhd G$ с групповой структурой $g_1H \cdot g_2H \overset{\text{def}}{=} (g_1g_2)H$ называется *фактором* (или *фактор группой*) группы G по нормальной подгруппе H. Гомоморфизм групп $G \twoheadrightarrow G/H$, $g \mapsto gH$, называется *гомоморфизмом факторизации.*

Следствие 12.4
Каждый гомоморфизм групп $\varphi : G_1 \to G_2$ является композицией эпиморфизма факторизации $G_1 \twoheadrightarrow G_1/\ker\varphi$ 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, $\operatorname{im}\varphi \simeq G/\ker\varphi$.

Доказательство. Следствие утверждает, что слой $\varphi^{-1}\big(\varphi(g)\big)$ гомоморфизма φ над каждой точкой $\varphi(g) \in \operatorname{im}\varphi \subset G_2$ является левым сдвигом ядра $\ker\varphi$ на элемент g, что мы уже видели в предл. 12.1 на стр. 186. □

Предложение 12.5
Пусть $N, H \subset G$ — две подгруппы, причём $N \lhd G$ нормальна. Убедитесь, что множество $HN = \{hx \mid h \in H,\ x \in N\}$ является подгруппой в G, $H \cap N \lhd H$, $N \lhd HN$ и $HN/N \simeq H/(H \cap N)$.

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

$$\begin{gathered} h_1x_1h_2x_2 = \big(h_1h_2\big)\big(h_2^{-1}x_1h_2 \cdot x_2\big) \in HN\,, \\ (hx)^{-1}x^{-1}h^{-1} = h^{-1}(hxh^{-1}) \in HN\,, \end{gathered} \tag{12-22}$$

т. к. $h_2^{-1}x_1h_2 \in N$ и $hxh^{-1} \in N$. Нормальность $H \cap N \lhd H$ следует из нормальности $N \lhd G$. Сюрьективное отображение $\varphi : HN \to H/(H \cap N)$, 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 $H/(H \cap N) = \operatorname{im}\varphi \simeq$ $\simeq HN/\ker\varphi = HN/N$. □

Упражнение 12.29. Пусть $\varphi : G_1 \twoheadrightarrow G_2$ — сюрьективный гомоморфизм групп. Покажите, что полный прообраз $N_1 = \varphi^{-1}(N_2)$ любой нормальной подгруппы $N_2 \lhd G_2$ 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 $\varphi : G \to G'$ с ядром $H = \ker\varphi$. Если группа G' представлена как группа преобразований[1] какого-либо множества X, то возникает такое действие $G \to \operatorname{Aut} X$ 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.

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

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 $\mathrm{Tors}(G) = 0$ (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 $k = dr$, $m = \mathrm{ord}(\tau) = ds$, где $\text{нод}(r, s) = 1$. Если $d > 1$, то τ^d является произведением d независимых циклов длины s, и $\tau^k = \left(\tau^d\right)^r$ будет произведением s-тых степеней этих циклов. Остаётся показать, что когда $\mathrm{ord}(\tau) = m$ взаимно прост с k, то τ^k тоже цикл длины m. Если для какого-то элемента a цикла τ выполняется равенство $\left(\tau^k\right)^r(a) = a$, то kr делится на m, что при $\text{нод}(k, m) = 1$ возможно только когда r делится на m. Поэтому $r \geqslant m$, 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: $n!/\prod\limits_{i=1}^{n} i^{m_i} m_i!$ (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 сюрьективное отображение множества заполнений на множество всех перестановок циклового типа λ; прообраз каждой перестановки состоит из $\prod\limits_{i=1}^{n} i^{m_i} m_i!$ 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 додекадра с вершинами в центрах граней октаэдра и икосаэдра соответственно.

Упр. 12.17. Зафиксируем в V какой-либо базис и сопоставим оператору $F \in \mathrm{GL}(V)$ 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 — $|V| - |\Bbbk \cdot f_1| = q^n - q$ возможностей, для выбора третьего — $|V| - |\Bbbk \cdot f_1 \oplus \Bbbk \cdot f_2| = q^n - q^2$ возможностейи 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 $|\,\mathrm{SO}_{\text{ико}}\,| = 20 \cdot 3 = 60$ и$|\,\mathrm{O}_{\text{ико}}\,| = 20 \cdot 6 = 120$.

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 $Hg_1 = H(g_2 g_1^{-1}) g_2 = Hg_2$.

Упр. 12.25. Включение $gHg^{-1} \subset H$ влечёт включение $H \subset g^{-1}Hg$. Если это так для всех $g \in G$, то заменяя g на g^{-1} мы получаем обратное к исходному включение $gHg^{-1} \supset H$.

Упр. 12.26. $\varphi \circ \mathrm{Ad}_g \circ \varphi^{-1} : h \mapsto \varphi\big(g\, \varphi^{-1}(h)\, g^{-1}\big) = \varphi(g)\, h\, \varphi(g)^{-1}$.

Упр. 12.27. Для любой точки $x \in \mathbb{R}^n$ положим $p = \varphi^{-1}(x)$. Так как $\varphi : \mathbb{R}^n \to \mathbb{R}^n$ 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 $\varphi(gxg^{-1}) = \varphi(g)\varphi(x)\varphi(g)^{-1} \in N_2$ в силу нормальности $N_2 \lhd G_2$. Поэтому $N_1 = \varphi^{-1}(N_2) \lhd G_1$. Композиция сюрьективных гомоморфизмов $G_1 \twoheadrightarrow G_2 \twoheadrightarrow G_2/N_2$ является сюрьективным гомоморфизмом с ядром N_1.

§13. Немного о строении групп

13.1. Свободные группы и соотношения. С произвольным множеством M связана группа F_M, которая называется *свободной группой*, порождённой множеством M. Она состоит из классов эквивалентных слов, написанных буквами x и x^{-1}, $x \in M$, по наименьшему отношению эквивалентности, отождествляющему между собою слова, которые отличаются друг от друга вставкой или удалением[1] двубуквенного фрагмента xx^{-1} или $x^{-1}x$. Композиция определяется как приписывание одного слова к другому. Единицей служит пустое слово. Обратным к классу слова $w = x_1x_2\ \dots\ x_m$ является класс слова $w^{-1} = x_m^{-1} \dots x_2^{-1}x_1^{-1}$, где каждое x_i — имеет вид x или x^{-1} с $x \in M$ и $\left(x^{-1}\right)^{-1} \stackrel{\text{def}}{=} x$.

Упражнение 13.1. Убедитесь, что композиция корректно определена на классах эквивалентности слов и что в каждом классе содержится ровно одно *несократимое*[2] слово, которое одновременно является и самым коротким словом в своём классе.

Элементы множества M называются *образующими* свободной группы F_M. Свободная группа с k образующими обозначается F_k. Группа $F_1 \simeq \mathbb{Z}$ — это циклическая группа бесконечного порядка. Группа F_2 классов слов 4-буквенного алфавита x, y, x^{-1}, y^{-1} уже довольно трудно обозрима.

Упражнение 13.2. Постройте инъективный гомоморфизм групп $F_{\mathbb{N}} \hookrightarrow F_2$.

Предложение 13.1 (универсальное свойство свободных групп)
Отображение $i_M : M \to F_M$, переводящее элемент $x \in M$ в класс однобуквенного слова $x \in F_M$, обладает следующим свойством: для любой группы G и любого отображения множеств $\varphi_M : M \to G$ существует единственный гомоморфизм групп $\varphi : F_M \to G$, такой что $\varphi_M = \varphi \circ i_M$. Для любого обладающего этим свойством отображения $i'_M : M \to F'$ множества M в группу F' имеется единственный изоморфизм групп $i' : F_M \xrightarrow{\sim} F'$, такой что $i'_M = i' \circ i_M$.

Доказательство. Гомоморфизм φ единствен, поскольку обязан переводить слово

$$w = x_1^{\varepsilon_1}x_2^{\varepsilon_2}\ \cdots\ x_m^{\varepsilon_m} \in F_M \qquad (x_\nu \in M\,, \quad \varepsilon_\nu = \pm 1)$$

в произведение $\varphi_M(x_1)^{\varepsilon_1}\varphi_M(x_2)^{\varepsilon_2}\ \cdots\ \varphi_M(x_m)^{\varepsilon_m} \in G$. С другой стороны, это правило корректно задаёт гомоморфизм групп, что доказывает первое утверждение. Если отображение $i' : M \to F'$ множества M в группу F' обладает универсальным свойством из предл. 13.1, то существуют единственные гомоморфизмы $i' : F_M \to F'$ и $i : F' \to F_M$, встраивающиеся в коммутативные диаграммы

$$\begin{tikzcd}
F_M \arrow[rr, equal, "\mathrm{Id}_{F_M}"] & & F_M \arrow[dd, dashed, "i'"] \\
& M \arrow[ul, "i_M"'] \arrow[ur, "i_M"] \arrow[dl, "i'_M"] \arrow[dr, "i'_M"'] & \\
F' \arrow[uu, dashed, "i"] \arrow[rr, equal, "\mathrm{Id}_{F'}"'] & & F'
\end{tikzcd}
\qquad
\begin{tikzcd}
F_M \arrow[dd, equal, "\mathrm{Id}_{F_M}"'] \arrow[dr, dashed, "i"'] & & & & F' \arrow[dd, equal, "\mathrm{Id}_{F'}"] \arrow[dl, dashed, "i'"] \\
& F' \arrow[dl, dashed, "i'"'] & M \arrow[l, "i'_M"'] \arrow[r, "i_M"] \arrow[ull, "i_M"'] \arrow[dll, "i_M"] \arrow[urr, "i'_M"] \arrow[drr, "i'_M"'] & F_M \arrow[dr, dashed, "i"] & \\
F_M & & & & F'
\end{tikzcd}$$

[1] в начале, в конце, или же между произвольными двумя последовательными буквами слова
[2] т. е. не содержащее двубуквенных фрагментов xx^{-1} и $x^{-1}x$

Разложения вида $i_M = \varphi \circ i_M$, $i'_M = \psi \circ i'_M$ в силу их единственности возможны только с $\varphi = \mathrm{Id}_{F_M}$, $\psi = \mathrm{Id}_{F'}$. Поэтому $i' \circ i = \mathrm{Id}_{F'}$, $i \circ i' = \mathrm{Id}_{F_M}$. □

13.1.1. Задание групп образующими и соотношениями. Если гомоморфизм групп

$$\varphi : F_M \twoheadrightarrow G\,, \tag{13-1}$$

заданный отображением $\varphi_M : M \to G$, $m \mapsto g_m$, множества M в группу G, оказывается *сюрьективным*, то говорят, что группа G *порождается* элементами $g_m = \varphi_M(m)$, $m \in M$, а сами эти элементы называются *образующими* группы G. В этом случае G исчерпывается всевозможными произведениями $g_1^{\varepsilon_1} g_2^{\varepsilon_2} \cdots g_k^{\varepsilon_k}$, $\varepsilon = \pm 1$, образующих и обратных к ним элементов. Группа G называется *конечно порождённой*, если она допускает конечное множество образующих. Ядро $\ker\varphi \lhd F_M$ эпиморфизма (13-1) называется *группой соотношений* между образующими g_m. Набор слов $R \subset \ker\varphi$ называется набором *определяющих соотношений*, если $\ker\varphi$ — это наименьшая нормальная подгруппа в F_M, содержащая R. Это означает, что любое соотношение можно получить из слов множества R конечным числом умножений, обращений и сопряжений произвольными элементами из свободной группы F_M. Группа, допускающая конечное число образующих с конечным набором определяющих соотношений называется *конечно определённой*.

Всякую группу можно задать образующими и соотношениями, например, взяв в качестве M множество всех элементов группы. Удачный выбор образующих с простыми определяющими соотношениями часто позволяет прояснить строение группы, явно строить её гомоморфизмы в другие группы и т. п. Однако в общем случае выяснить, изоморфны ли две группы, заданные своими образующими и определяющими соотношениями, и даже определить, отлична ли группа, заданная образующими и соотношениями, от тривиальной группы $\{e\}$, бывает непросто. Более того, даже в классе конечно определённых групп обе эти задачи являются *алгоритмически неразрешимыми*[1].

Предложение 13.2
Пусть группа G_1 задана множеством образующих M и набором определяющих соотношений R, а G_2 — произвольная группа. Отображение $\varphi : M \to G_2$ тогда и только тогда корректно задаёт гомоморфизм групп $G_1 \to G_2$ правилом

$$x_1^{\varepsilon_1} x_2^{\varepsilon_2} \cdots x_m^{\varepsilon_m} \mapsto \varphi(x_1)^{\varepsilon_1} \varphi(x_2)^{\varepsilon_2} \cdots \varphi(x_m)^{\varepsilon_m}\,,$$

когда для каждого слова $w = x_1^{\varepsilon_1} x_2^{\varepsilon_2} \cdots x_m^{\varepsilon_m} \in R$ в группе G_2 выполняется соотношение

$$\varphi(x_1)^{\varepsilon_1} \varphi(x_2)^{\varepsilon_2} \cdots \varphi(x_m)^{\varepsilon_m} = 1\,.$$

Доказательство. Отображения множеств $\varphi_M : M \to G_2$ биективно соответствуют гомоморфизмам групп $\varphi : F_M \to G_2$. Такой гомоморфизм φ факторизуется до гомоморфизма из группы $G_1 = F_M / N_R$, где $N_R \lhd F_M$ — наименьшая нормальная подгруппа, содержащая R, тогда и только тогда, когда $N_R \subset \ker\psi$. Так как $\ker\psi \lhd F_M$, для этого необходимио и достаточно включения $R \subset \ker\psi$. □

[1] в формальном смысле, принятом в математической логике

Пример 13.1 (образующие и соотношения группы диэдра)
Покажем, что группа диэдра D_n задаётся двумя образующими x_1, x_2 и соотношениями

$$x_1^2 = x_2^2 = (x_1x_2)^n = e\,. \tag{13-2}$$

Оси симметрии правильного n-угольника разбивают его на $2n$ конгруэнтных прямоугольных треугольников (см. рис. 13◇1). Выберем один из них и обозначим через e. Поскольку любое движение плоскости однозначно задаётся своим действием на треугольник e, $2n$ движений $g \in D_n$ взаимно однозначно соответствуют треугольникам $g(e)$, в которые они переводят треугольник e. Пометим треугольник $g(e)$ преобразованием g. Обозначим через ℓ_1 и ℓ_2 стороны треугольника e, а через σ_1 и σ_2 — отражения плоскости относительно этих сторон. Тогда треугольники, получающиеся из e последовательными «перекатываниями» через стороны в направлении против ЧС пометятся элементами σ_2 , $\sigma_2\sigma_1$, $\sigma_2\sigma_1\sigma_2$, $\sigma_2\sigma_1\sigma_2\sigma_1$, … , а треугольники, получающиеся «перекатываниями» по ЧС — элементами σ_1 , $\sigma_1\sigma_2$, $\sigma_1\sigma_2\sigma_1$, $\sigma_1\sigma_2\sigma_1\sigma_2$, …

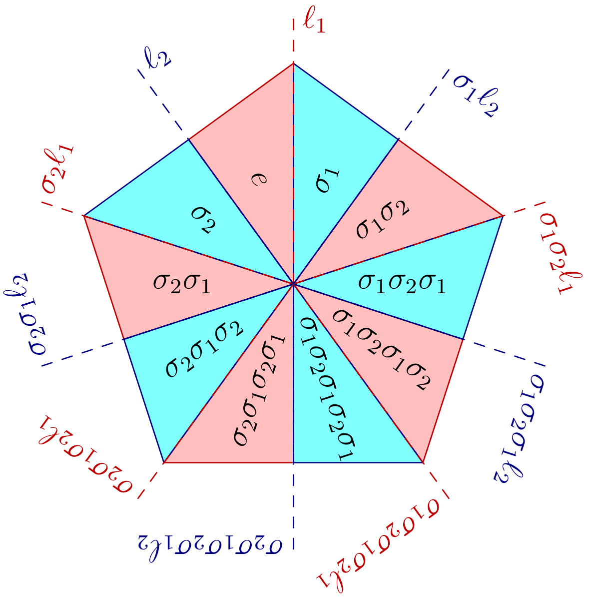


Рис. 13◇1. Группа диэдра порождается отражениями.

Упражнение 13.3. Пусть F — произвольное движение плоскости, а σ_ℓ — отражение относительно прямой ℓ. Убедитесь, что $F \circ \sigma_\ell \circ F^{-1} = \sigma_{F(\ell)}$ или, что то же самое, $\sigma_{F(\ell)} \circ F = F \circ \sigma_\ell$.

Так как композиция $\sigma_1 \circ \sigma_2$ является поворотом в направлении от ℓ_2 к ℓ_1 на удвоенный угол между ℓ_2 и ℓ_1 , равный $2\pi/n$, в группе D_n выполняются соотношения

$$\sigma_1^2 = \sigma_2^2 = (\sigma_1\sigma_2)^n = e\,. \tag{13-3}$$

По предл. 13.2 правило $x_1 \mapsto \sigma_1$, $x_2 \mapsto \sigma_2$ корректно задаёт сюрьективный гомоморфизм $\varphi : F_2/H \twoheadrightarrow D_n$ из фактора свободной группы F_2 с образующими x_1, x_2 по наименьшей нормальной подгруппе $H \lhd F_2$, содержащей слова x_1^2, x_2^2 и $(x_1x_2)^n$. Каждое слово в алфавите $\{x_1, x_2\}$ по модулю соотношений (13-2) записывается словом $x_1x_2x_1\dots$ или $x_2x_1x_2\dots$ длины $< 2n$. Два таких слова переводятся гомоморфизмом φ в один и тот же элемент $g \in D_n$, если и только если сумма их длин равна[1] $2n$:

$$\varphi(\underbrace{x_1x_2x_1\dots}_{k}) = \underbrace{\sigma_1\sigma_2\sigma_1\dots}_{k} = g = \underbrace{\sigma_2\sigma_1\sigma_2\dots}_{2n-k} = \varphi(\underbrace{x_2x_1x_2\dots}_{2n-k})\,. \tag{13-4}$$

Упражнение 13.4. Убедитесь, что $\underbrace{x_1x_2x_1\dots}_{k} = \underbrace{x_2x_1x_2\dots}_{2n-k} \iff (x_1x_2)^n = e\,.$

Таким образом, гомоморфизм $\varphi : F_2/H \xrightarrow{\sim} D_n$ биективен.

[1]этому отвечают два способа «перекатить» треугольник e в треугольник g — двигаясь против ЧС и по ЧС, как на рис. 13◇1)

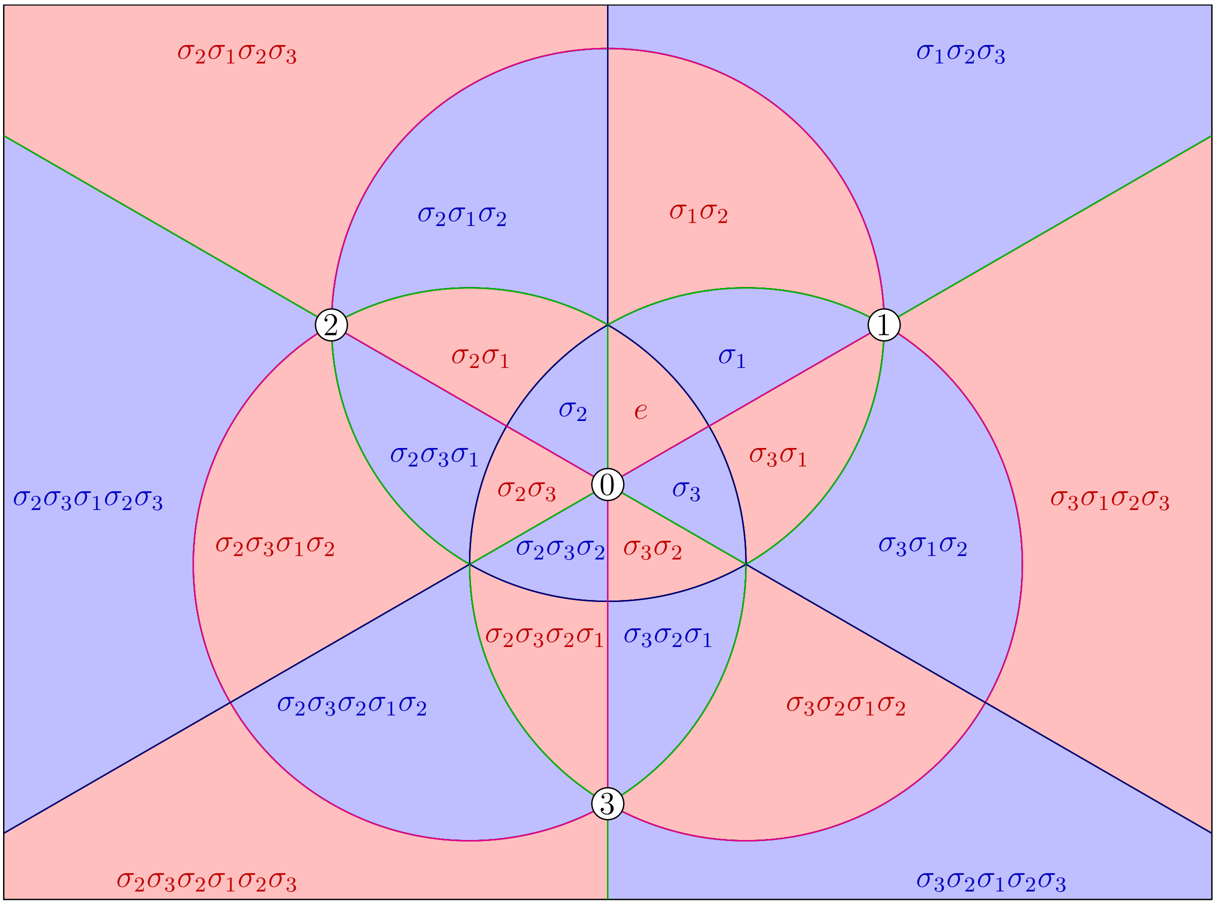


Рис. 13⋄2. Триангуляция сферы плоскостями симметрии тетраэдра в стереографической проекции из диаметрально противоположной к вершине «0» точки на плоскость, параллельную грани «123».

Пример 13.2 (образующие и соотношения несобственных групп платоновых тел) Рассмотрим платоново тело M с треугольными гранями — тетраэдр, октаэдр или икосаэдр. Плоскости симметрии многогранника M барицентрически разбивают каждую из граней на 6 треугольников, которые сходятся по $2m_1$ штук в вершинах M, по $2m_2$ штук в серединах рёбер M и по $2m_3$ штук в центрах граней M. Значения m_1, m_2, m_3 и общее число треугольников N для различных M таковы[1]:

M	m_1	m_2	m_3	N
тетраэдр	2	3	3	24
октаэдр	2	3	4	48
икосаэдр	2	3	5	120

Пересечения плоскостей симметрии с описанной около M сферой задают её триангуляцию N конгруэнтными сферическими треугольниками с углами[2] π / m_1, π / m_2, π / m_3

[1] n-угольный диэдр из предыдущего прим. 13.1 тоже вписывается в эту схему с $m_1 = 2$, $m_2 = 2$, $m_3 = n$ и $N = 4n$, если считать, что две его грани различны — скажем, покрашены в разные цвета, так что отражение в плоскости n-угольника является *нетривиальным* преобразованием

[2] они равны углам, под которыми пересекаются соответствующие плоскости симметрии

(см. рис. 13◇2 на стр. 201). Поскольку любое линейное преобразование $\mathbb{R}^3$ однозначно задаётся своим действием на базисные векторы с концами в вершинах какого-нибудь сферического треугольника, который мы пометим буквой e, преобразования несобственной группы O_M тела M взаимно однозначно соответствуют N треугольникам триангуляции[1]. Мы пометим каждый треугольник тем преобразованием $g \in \mathrm{O}_M$, которое переводит в него треугольник e. Назовём плоскости, высекающие стороны треугольника e, буквами π_1, π_2, π_3 так, чтобы угол между плоскостями π_i и π_j равнялся π/m_k, и обозначим отражение в плоскости π_i через σ_i. Согласно предыдущему прим. 13.1 эти отражения удовлетворяют шести соотношениям:

$$\sigma_i^2 = e \qquad \text{и} \qquad (\sigma_i\sigma_j)^{m_k} = e\,, \tag{13-5}$$

в которых $i = 1, 2, 3$, а (i, j, k) пробегает циклические перестановки номеров $(1, 2, 3)$.

Упражнение 13.5. Убедитесь в этом.

Так как из треугольника e можно попасть в любой треугольник g последовательными отражениями относительно сторон, правило $x_i \mapsto \sigma_i$ задаёт сюрьективный гомоморфизм из свободной группы F_3 на алфавите $\{x_1, x_2, x_3\}$ в группу O_M. В силу соотношений (13-5) он корректно факторизуется до эпиморфизма $\varphi : F_3/H \twoheadrightarrow \mathrm{O}_M$, где $H \triangleleft F_3$ — наименьшая нормальная подгруппа, содержащая 6 слов

$$x_i^2 \qquad \text{и} \qquad (x_i x_j)^{m_k}\,. \tag{13-6}$$

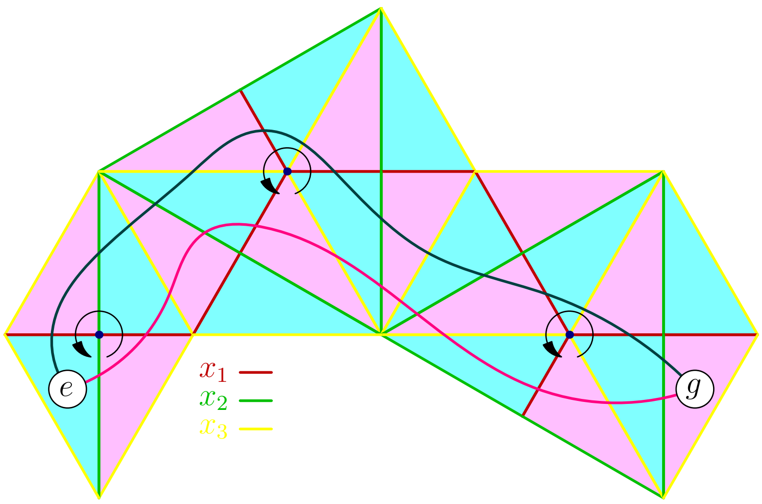


Рис. 13◇3. $\mathbf{x_1x_2}x_3x_2\mathbf{x_3x_1x_3x_1}x_2x_3x_2\mathbf{x_1x_3x_1}x_2 = g = \mathbf{x_2x_1}x_3x_2\mathbf{x_1x_3}x_2x_3x_2\mathbf{x_3x_1x_3}x_2$

Чтобы показать, что φ — изоморфизм, достаточно проверить, что любые два слова w_1, w_2 в алфавите $\{x_1, x_2, x_3\}$, переходящие в один и тот же элемент $g \in \mathrm{O}_M$, эквивалентны по модулю слов (13-6). Каждое слово $\sigma_{i_1}\sigma_{i_2}\cdots\sigma_{i_m} = g$ задаёт последовательность треугольников $e = g_0, g_1, g_2, \dots, g_m = g$, в которой треугольник $g_{k+1} = g_k\sigma_{k+1}$ получается из треугольника g_k отражением относительно их общей стороны, высекаемой на сфере плоскостью $g_k(\pi_{i_{k+1}})$ — образом плоскости $\pi_{i_{k+1}}$ при преобразовании g_k.

Упражнение 13.6. Удостоверьтесь, что

$$\sigma_{g_k(\pi_{i_{k+1}})} \circ \sigma_{g_{k-1}(\pi_{i_k})} \circ \cdots \circ \sigma_{g_1(\pi_{i_2})} \circ \sigma_{\pi_{i_1}} = \sigma_{i_1}\sigma_{i_2}\cdots\sigma_{i_k}\sigma_{i_{k+1}}\,.$$

[1]что ещё раз позволяет вычислить порядок этой группы

Эта последовательность отражений однозначно считывается по любой гладкой кривой, соединяющей e с g внутри образованной треугольниками ленты и трансверсально пересекающей внутренние рёбра этой ленты, как на рис. 13◇3). Две такие кривые, производящие слова w_1 и w_2, можно продеформировать одну в другую по поверхности сферы. При прохождении через вершину триангуляции, в которой сходятся $2n$ треугольников, в задаваемом кривой слове некоторый фрагмент вида $x_1x_2x_1\dots$ длины k заменятся равным ему в F_3/H фрагментом вида $x_2x_1x_2\dots$ «дополнительной» длины $2n-k$ — как это происходило в форм. (13-4) и упр. 13.4 на стр. 200. Например, слова, отвечающие верхней и нижней траекториям на рис. 13◇3 выше

$$\boldsymbol{x_1x_2}x_3x_2\boldsymbol{x_3x_1x_3x_1}x_2x_3x_2\boldsymbol{x_1x_3x_1}x_2 \mapsto g$$
$$\boldsymbol{x_2x_1}x_3x_2\boldsymbol{x_1x_3}x_2x_3x_2\boldsymbol{x_3x_1x_3}x_2 \mapsto g\,,$$

преобразуются одно в другое применением циклических соотношений

$$x_1x_2 = x_2x_1\,,\quad x_3x_1x_3x_1 = x_1x_3 \quad \text{и} \quad x_3x_1x_3 = x_1x_3x_1$$

в трёх отмеченных на (13-4) вершинах. Таким образом, любые два слова, ведущие из e в g лежат в одном классе группы F_3/H.

Упражнение 13.7. Выберем в треугольнике e точку a, а в треугольнике g — точку b так, чтобы они не были диаметрально противоположными и соединяющая их *геодезическая*[1] не проходила через вершины триангуляции. Покажите, что:

а) длина представляющего g слова, считанного с этой геодезической, не зависит от удовлетворяющего предыдущим условиям выбора точек a и b

б) все считываемые с таких геодезических слова имеют наименьшую возможную длину, среди всех слов, представляющих g

в) любое представляющее g слово минимальной длины считывается с некоторой геодезической.

Пример 13.3 (образующие и соотношения симметрической группы)

Симметрическая группа S_{n+1} изоморфна несобственной группе O_Δ правильного n-мерного симплекса[2] $\Delta = [0, 1, \dots, n] \subset \mathbb{R}^n$, поскольку каждая перестановка вершин однозначно определяет ортогональное преобразование пространства $\mathbb{R}^n$, осуществляющее такую перестановку. Все грани симплекса Δ тоже являются правильными симплексами и взаимно однозначно соответствуют собственным подмножествам в $\{1, 2, \dots, n\}$. Симплекс Δ симметричен относительно $n(n+1)/2$ гиперплоскостей π_{ij}, проходящих через середину ребра $[i,j]$ и противоположную ему грань коразмерности 2 с вершинами $\{0, 1, \dots, n\} \smallsetminus \{i,j\}$. Отражение $\sigma_{ij} \in \mathrm{O}_\Delta$ в этой плоскости отвечает в S_{n+1} транспозиции элементов i и j.

Упражнение 13.8. Убедитесь, что любые две плоскости π_{ij} и π_{km} с $\{i,j\} \cap \{k,m\} = \varnothing$ ортогональны, а плоскости π_{ij} и π_{jk} с различными i, j, k пересекаются под углом 60°.

---

[1] или прямая в *сферической* геометрии, т. е. кратчайшая из двух дуг большого круга, высекаемого на сфере плоскостью, проходящей через точки a, b и центр сферы

[2] здесь и далее мы обозначаем вершины симплекса числами от 0 до n, как на рис. 13◇2 на стр. 201, и считаем, что симметрическая группа S_{n+1} переставляет символы $0, 1, \dots, n$

Плоскости π_{ij} осуществляют *барицентрическое разбиение* симплекса Δ на $n!$ меньших симплексов с вершинами в центрах граней симплекса Δ. Обозначим через $\langle i_0 i_1 \,\dots\, i_m\rangle$ центр m-мерной грани с вершинами в $i_0, i_1, \dots, i_m$ и сопоставим каждой перестановке

$$g = (g_0, g_1, \dots, g_n) \in S_{n+1}$$

симплекс барицентрического разбиения с вершинами в точках[1]

$$\big[\langle g_0\rangle, \langle g_0, g_1\rangle, \langle g_0, g_1, g_2\rangle, \dots, \langle g_0 g_1 \dots g_{n-1}\rangle, \langle g_0 g_1 \dots g_n\rangle\big]\,. \tag{13-7}$$

Это соответствие устанавливает такую биекцию между симплексами барицентрического разбиения и элементами группы $S_{n+1} \simeq \mathrm{O}_\Delta$, что симплекс (13-7) является образом «начального» симплекса

$$\big[\langle 0\rangle, \langle 01\rangle, \langle 012\rangle, \dots, \langle 0, 1, \dots, n-1\rangle, \langle 0, 1, \dots, n\rangle\big]\,. \tag{13-8}$$

под действием ортогонального преобразования, задаваемого перестановкой g. Как и в предыдущем примере, надпишем на каждом симплексе отвечающее ему преобразование g и спроектируем гиперповерхность симплекса Δ из его центра на описанную вокруг Δ сферу S^{n-1}, т. е. рассмотрим триангуляцию этой сферы её пересечениями гиперплоскостями π_{ij}. Эта триангуляция состоит из $n!$ конгруэнтных $(n-1)$-мерных симплексов, надписанных элементами группы S_{n+1}. При $n = 3$, т. е. для группы S_4, мы получим тетраэдрическую триангуляцию сферы S^2 треугольниками с углами $\pi/3$, $\pi/3$ и $\pi/2$, изображённую на рис. 13◇2 на стр. 201. Начальному симплексу (13-8), помеченному тождественным преобразованием e, отвечает симплекс триангуляции, высекаемый из сферы n гиперплоскостями $\pi_i = \pi_{i-1,i}$ с $1 \leqslant i \leqslant n$. Обозначим через $\sigma_i = \sigma_{i-1,i}$ отражения в этих гиперплоскостях. В симметрической группе S_{n+1} эти отражения суть транспозиции $|i-1, i\rangle$ пар соседних элементов. В силу упр. 13.8 они удовлетворяют соотношениям[2]

$$\sigma_i^2 = e\,, \quad \sigma_i\sigma_{i+1}\sigma_i = \sigma_{i+1}\sigma_i\sigma_{i+1} \quad \text{и} \quad \sigma_i\sigma_j = \sigma_j\sigma_i \quad \text{при} \quad |i-j| \geqslant 2\,. \tag{13-9}$$

Упражнение 13.9. Убедитесь непосредственно, что соотношения (13-9) выполняются для *транспозиций* σ_i в группе S_{n+1}.

В силу этих соотношений, гомоморфизм свободой группы на алфавите $\{x_1, x_2, \dots, x_n\}$, переводящий x_i в σ_i, факторизуется до гомоморфизма $\varphi : F_n/H \to S_{n+1}$, где $H \lhd F_n$ — наименьшая нормальная подгруппа, содержащая слова

$$x_i^2\,, \qquad (x_i x_{i+1})^3 \quad \text{и} \quad (x_i x_j)^2 \text{ с } |i-j| \geqslant 2\,. \tag{13-10}$$

Чтобы убедиться в его сюрьективности, выберем в симплексах e и g точки a и b так, чтобы они не были диаметрально противоположны и соединяющая их геодезическая[3] не

[1]т. е. с первой вершиной в вершине g_0 самого симплекса Δ, следующей вершиной — в середине выходящего из g_0 ребра $[g_0, g_1]$, следующей — в центре примыкающей к этому ребру треугольной грани $[g_0, g_1, g_2]$ и т. д. последняя вершина является центром всего симплекса Δ

[2]соотношение $\sigma_i\sigma_{i+1}\sigma_i = \sigma_{i+1}\sigma_i\sigma_{i+1}$ является более употребительной в данном контексте записью циклического соотношения $(\sigma_i\sigma_{i+1})^3 = e$ на поворот $\sigma_i\sigma_{i+1}$ на 120° вокруг $(n-2)$-мерного подпространства $\pi_i \cap \pi_{i+1}$

[3]кратчайшая из двух дуг ab большой окружности, высекаемой из сферы двумерной плоскостью, проходящей через точки a, b и центр сферы

пересекала граней коразмерности 2. Пройдя из a в b по этой геодезической, мы получим представление элемента g словом $x_1 x_2 \, \dots \, x_m$, где i_ν — это номер такой из плоскостей π_ν, что переход из ν-того встретившегося нам по дороге симплекса[1] g_ν к следующему $(\nu+1)$-му симплексу происходит сквозь гиперплоскость $g_\nu(\pi_\nu)$. Инъективность гомоморфизма φ устанавливается дословно так же, как в прим. 13.2. Каждому слову $w \in F_n$, переходящему в элемент $g \in \mathrm{O}_\Delta$, отвечает ведущая из e в g «трубка», образованная симплексами триангуляции. Слово w состоит из номеров гиперграней, разделяющих соседние симплексы этой трубки, и может быть считано при движении из e в g по любой идущей внутри трубки кривой, трансверсально пересекающей эти грани. Любые две такие кривые можно продеформировать по сфере друг в друга. Когда в процессе этой деформации кривая пересекает грань $g(\pi_i \cap \pi_j)$ коразмерности 2, происходит замена некоторого фрагмента слова либо при помощи циклического соотношения $(x_i x_j)^2 = e$, отвечающего перпендикулярным плоскостям с $|i-j| \geqslant 2$, либо при помощи циклического соотношения $(x_i x_{i+1})^3$, отвечающего плоскостям, пересекающимся под углом 60°. В ортогональной проекции вдоль $(n-2)$-мерного подпространства $g(\pi_i \cap \pi_j)$ на ортогональную ему двумерную плоскость мы увидим картину вроде показанной на рис. 13◇3 на стр. 202. Таким образом, симметрическая группа S_{n+1} задаётся n транспозициями x_i пар соседних элементов с определяющими соотношениями (13-10).

Разумеется, эту геометрическую картину можно выхолостить до сугубо комбинаторного рассуждения, что мы сделаем в n° 13.1.2 ниже.

Упражнение 13.10. Покажите, что знакопеременная группа A_{n+1} порождается а) парами транспозиций б) 3-циклами $|k-2, k-1, k\rangle$, где $2 \leqslant k \leqslant n$.

13.1.2. Порядок Брюа на S_{n+1}. Будем называть число инверсных пар в перестановке[2] $g = (g_0, g_1, \dots, g_n) \in S_{n+1}$ *длиной* перестановки g и обозначать его $\ell(g)$.

Упражнение 13.11. Убедитесь, что длина перестановок из S_{n+1} лежит в пределах от 0 до $n(n+1)/2$, причём имеется ровно по одной перестановке минимальной и максимальной длины. Что это за перестановки?

Правое умножение перестановки g на транспозицию $\sigma_i = |i-1, i\rangle$ приводит к перестановке $g\sigma_i$, отличающейся от g транспозицией $(i-1)$-того и i-го символов g_{i-1} и g_i :

$$\big(g_1, \dots, g_{i-2}, \boldsymbol{g_{i-1}}, \boldsymbol{g_i}, g_{i+1}, \dots, g_n\big) \circ \sigma_i = \big(g_1, \dots, g_{i-2}, \boldsymbol{g_i}, \boldsymbol{g_{i-1}}, g_{i+1}, \dots, g_n\big) \,,$$

причём $\ell(g\sigma_i) = \ell(g)+1$, если $g_{i-1} < g_i$, и $\ell(g\sigma_i) = \ell(g)-1$, если $g_{i-1} > g_i$. Поэтому любая перестановка g длины $\ell(g) = m$ может быть записана словом дины m

$$g = \sigma_{i_1}\sigma_{i_2} \cdots \sigma_{i_m} \,, \quad \ell(g) = m \,, \tag{13-11}$$

в котором каждое умножение справа на очередное σ_{i_ν} переставляет между собой соседние возрастающие элементы $h_{i_\nu - 1} < h_{i_\nu}$ перестановки $(h_0, h_1, \dots, h_n) = \sigma_{i_1}\sigma_{i_2} \, \cdots \, \sigma_{i_\nu - 1}$. Частичный порядок на S_{n+1}, в котором $g < h$, если h получается из g увеличивающими длину транспозициями соседних элементов, называется *порядком Брюа*. Слово $w = x_{i_1} x_{i_2} \, \cdots \, x_{i_m}$

[1]как и в прим. 13.2 мы последовательно нумеруем встречающиеся симплексы так, что $e = g_0$, а $g = g_{m+1}$

[2]напомню, пара (i,j), где $1 \leqslant i < j \leqslant n$ называется *инверсной парой* перестановки $g \in S_n$, если $g_i = g(i) > g(j) = g_j$, см. n° 9.2 на стр. 133

в свободной группе F_n с образующими $x_1, x_2, \dots, x_n$ называется *минимальным словом* перестановки $g \in S_{n+1}$, если $m = \ell(g)$ и $g = \sigma_{i_1}\sigma_{i_2} \cdots \sigma_{i_m}$. Начальные фрагменты минимального слова задают строго возрастающую в смысле порядка Брюа последовательность элементов $h_\nu = \sigma_{i_1}\sigma_{i_2} \cdots \sigma_{i_\nu} \in S_{n+1}$. Перестановка g может иметь много разных минимальных слов, однако не может быть записана никаким более коротким словом.

Упражнение 13.12. Проверьте, что в терминах прим. 13.3 проход из симплекса e в симплекс g по любой геодезической, не пересекающей граней коразмерности 2, задаёт минимальное слово элемента g и что каждое минимальное слово элемента g считывается с некоторой такой геодезической.

Предложение 13.3
При гомоморфизме $\varphi : F_n \to S_{n+1}$, $x_i \mapsto \sigma_i$, каждое слово $w \in F_n$ эквивалентно минимальному слову перестановки $\varphi(w) \in S_{n+1}$ по модулю соотношений

$$x_i^2 = e\,, \quad x_i x_{i+1} x_i = x_{i+1} x_i x_{i+1} \quad \text{и} \quad x_i x_j = x_j x_i \text{ при } |i-j| \geqslant 2\,,$$

а все минимальные слова перестановки $\varphi(w)$ эквивалентны между собой.

Доказательство. Индукция по количеству букв в слове $w \in F_{n-1}$. Для $w = \varnothing$ утверждение очевидно. Пусть для всех слов из $\leqslant m$ букв предложение доказано. Достаточно для каждого m-буквенного слова w и каждой буквы x_ν проверить предложение для слова wx_ν. Если слово w не является минимальным словом элемента $g = \varphi(w)$, то по индукции оно эквивалентно более короткому минимальному слову. Тогда и wx_ν эквивалентно более короткому слову, и предложение справедливо по индукции. Поэтому мы будем далее считать, что слово w является минимальным словом элемента $g = \varphi(w) = (g_0, g_1, \dots, g_n)$. Возможны два случая: либо $g_{\nu-1} > g_\nu$, либо $g_{\nu-1} < g_\nu$. В первом случае у перестановки g есть минимальное слово вида ux_ν, по предположению индукции эквивалентное слову w. Тогда $wx_\nu \sim ux_\nu x_\nu \sim u$ и элемент $\varphi(wx_\nu) = \varphi(u)$ является образом более короткого, чем w слова u, эквивалентного слову wx_ν. По индукции, слово u эквивалентно минимальному слову элемента $\varphi(wx_\nu)$ и все такие слова эквивалентны друг другу. Поэтому то же верно и для эквивалентного u слова wx_ν.

Остаётся рассмотреть случай $g_{\nu-1} < g_\nu$. Здесь $\ell(g\sigma_\nu) = \ell(g) + 1$ и слово wx_ν является минимальным словом для элемента $\varphi(wx_\nu)$. Мы должны показать, что любое другое минимальное слово w' этого элемента эквивалентно wx_ν. Для самой правой буквы слова w' есть 3 возможности: либо она равна x_ν, либо она равна $x_{\nu\pm1}$ либо она равна x_μ с $|\mu-\nu| \geqslant 2$. В пером случае $w' = ux_\nu$, где u, как и w, является минимальным словом элемента g. По индукции $u \sim w$, а значит, и $w' = ux_k \sim wx_k$.

Пусть теперь $w' = ux_{\nu+1}$ — ситуация, когда $w' = ux_{\nu-1}$, полностью симметрична. Поскольку оба слова wx_ν и $ux_{\nu+1}$ минимальны для перестановки $h = \varphi(wx_\nu) = \varphi(ux_{\nu+1})$, в перестановке h на местах с номерами $\nu-1$, ν, $\nu+1$ стоят числа $g_\nu > g_{\nu-1} > g_{\nu+1}$, а в перестановке $g = (g_0, g_1, \dots, g_n) = \varphi(w)$ на этих же местах — числа $g_{\nu-1} < g_\nu > g_{\nu+1}$ с $g_{\nu-1} > g_{\nu+1}$. Поэтому у перестановки h имеется минимальное слово вида $sx_{\nu+1}x_\nu x_{\nu+1}$, а у перестановки g — минимальное слово вида $tx_\nu x_{\nu+1}$. Перестановка $h' = \varphi(s) = \varphi(t)$ отличается от h тем, что числа на местах с номерами $\nu-1$, ν, $\nu+1$ в ней возрастают и равны $g_{\nu+1} < g_{\nu-1} < g_\nu$. Поскольку $\ell(h') = \ell(h) - 3 = \ell(g) - 2$, оба слова t и s минимальны для h' и по индукции эквивалентны. Кроме того, по индукции w эквивалентно $tx_\nu x_{\nu+1}$.

Поэтому $wx_\nu \sim tx_\nu x_{\nu+1}x_\nu \sim sx_\nu x_{\nu+1}x_\nu \sim sx_{\nu+1}x_\nu x_{\nu+1}$. Но $sx_{\nu+1}x_\nu \sim u$, поскольку оба слова минимальны для одной и той же перестановки[1] длины $m = \ell(h) - 1$. Таким образом, $wx_\nu \sim ux_{\nu+1}$.

Наконец, пусть $h = \varphi(wx_\nu) = \varphi(ux_\mu)$, где $|\mu - \nu| \geqslant 2$. Тогда в h есть два непересекающихся фрагмента $g_{\nu-1} > g_\nu$ и $g_{\mu-1} > g_\mu$. Поэтому у h есть минимальные слова вида $tx_\mu x_\nu$ и вида $sx_\nu x_\mu$, где t и s являются минимальными словами для перестановки $\varphi(t) = \varphi(s)$, отличающейся от h тем, что расматриваемые 2 фрагмента в ней имеют вид $g_\nu < g_{\nu-1}$ и $g_\mu < g_{\mu-1}$. Так как длина этой перестановки равна $\ell(h) - 2 = m - 1$, по индукции $t \sim s$. Поскольку tx_μ — минимальное слово для g, по индукции $w \sim tx_\mu$. Аналогично, т. к. sx_ν и u — минимальные слова для перестановки $\varphi(sx_\nu) = \varphi(u)$, отличающейся от h' транспозицией первого из двух фрагментов и потому имеющей длину $\ell(h) - 1 = m$, по индукции $sx_\nu \sim u$. Таким образом, $wx_\nu \sim tx_\mu x_\nu \sim sx_\mu x_\nu \sim sx_\nu x_\mu \sim ux_\mu$, что и требовалось. □

13.2. Простые группы и композиционные факторы. Группа G называется *простой*, если она не содержит нормальных подгрупп, отличных от $\{e\}$ и G. Например, любая группа простого порядка проста, поскольку по теореме Лагранжа вообще не содержит никаких подгрупп кроме $\{e\}$ и G. Согласно сл. 12.1 на стр. 186 простота группы G равносильна тому, что всякий гомоморфизм $G \to G'$ либо является вложением, либо отображает всю группу G в единицу.

Определение 13.1 (композиционный ряд)
Конечная строго убывающая последовательность подгрупп

$$G = G_0 \supsetneq G_1 \supsetneq G_2 \supsetneq \cdots \supsetneq G_{n-1} \supsetneq G_n = \{e\} \tag{13-12}$$

называется *композиционным рядом* или *рядом Жордана – Гёльдера* группы G, если при каждом i подгруппа G_{i+1} нормальна в G_i и фактор G_i/G_{i+1} прост. В этой ситуации неупорядоченный набор простых групп G_i/G_{i+1} (в котором возможны повторения) называется набором *композиционных факторов* (или *факторов Жордана – Гёльдера*) группы G. Число n называется *длиной* композиционного ряда (13-12).

Пример 13.4 (композиционные факторы S_4)
Выше мы видели, что симметрическая группа S_4 имеет композиционный ряд

$$S_4 \rhd A_4 \rhd V_4 \rhd \mathbb{Z}/(2) \rhd \{e\},$$

в котором $A_4 \lhd S_4$ — подгруппа чётных перестановок, $V_4 \lhd A_4$ — подгруппа Клейна, состоящая из тождественной перестановки и трёх перестановок циклового типа , а

$$\mathbb{Z}/(2) \lhd V_4 \simeq \mathbb{Z}/(2) \oplus \mathbb{Z}/(2)$$

любая из трёх циклических подгрупп второго порядка, порождённых неединичными элементами. Таким образом, симметрическая группа S_4 имеет композиционные факторы $\mathbb{Z}/(2) = S_4/A_4$, $\mathbb{Z}/(3) = A_4/V_4$, $\mathbb{Z}/(2) = V_4/\big(\mathbb{Z}/(2)\big)$ и $\mathbb{Z}/(2) = \mathbb{Z}/(2)/\{e\}$.

Упражнение 13.13. Убедитесь, что $A_4/V_4 \simeq \mathbb{Z}/(3)$.

[1] она отличается от g, h и h' тем, что числа в позициях с номерами $\nu - 1$, ν, $\nu + 1$ в ней упорядочены как $g_\nu > g_{\nu+1} < g_{\nu-1}$, где $g_\nu > g_{\nu-1}$

Теорема 13.1 (теорема Жордана – Гёльдера)
Если группа G имеет конечный композиционный ряд, то неупорядоченный набор его композиционных факторов не зависит от выбора композиционного ряда. В частности, все композиционные ряды имеют одинаковую длину.

Доказательство. Пусть у группы G есть два композиционных ряда

$$G = P_0 \supsetneq P_1 \supsetneq P_2 \supsetneq \cdots \supsetneq P_{n-1} \supsetneq P_n = \{e\} \tag{13-13}$$

$$G = Q_0 \supsetneq Q_1 \supsetneq Q_2 \supsetneq \cdots \supsetneq Q_{m-1} \supsetneq Q_m = \{e\}\,. \tag{13-14}$$

Мы собираемся вставить между последовательными членами этих рядов дополнительные цепочки нестрого убывающих подгрупп так, чтобы получившиеся удлинённые последовательности состояли из одинакового числа элементов, а между их последовательными факторами возникла бы такая естественная биекция, при которой соответствующие друг другу факторы будут изоморфны. Применяя предл. 12.5 на стр. 197 к нормальной подгруппе $P_{i+1} \lhd P_i$ и подгруппам $Q_\nu \cap P_i \subset P_i$, мы для каждого i получаем цепочку

$$P_i \supseteq (Q_1 \cap P_i)P_{i+1} \supseteq (Q_2 \cap P_i)P_{i+1} \supseteq \cdots \supseteq (Q_{m-1} \cap P_i)P_{i+1} \supseteq P_{i+1}\,, \tag{13-15}$$

которая начинается с P_i, кончается в P_{i+1} и имеет $(Q_{k+1} \cap P_i)P_{i+1} \lhd (Q_k \cap P_i)P_{i+1}$ с

$$\frac{(Q_k \cap P_i)P_{i+1}}{(Q_{k+1} \cap P_i)P_{i+1}} \simeq \frac{(Q_k \cap P_i)}{(Q_{k+1} \cap P_i)(Q_k \cap P_{i+1})}\,. \tag{13-16}$$

Упражнение 13.14. Убедитесь в этом, т. е. для любой четвёрки подгрупп A, B, C, D, таких что $A \lhd B$ и $C \lhd D$, постройте изоморфизм $(B \cap D)C/(A \cap D)C \simeq (B \cap D)/(A \cap D)(B \cap C)$.

Группа P_{i+1} является нормальной подгруппой во всех группах цепочки (13-15). Факторизуя по ней, получаем цепочку

$$\frac{P_i}{P_{i+1}} \supseteq \frac{(Q_1 \cap P_i)P_{i+1}}{P_{i+1}} \supseteq \frac{(Q_2 \cap P_i)P_{i+1}}{P_{i+1}} \supseteq \cdots \supseteq \frac{(Q_{m-1} \cap P_i)P_{i+1}}{P_{i+1}} \supseteq \{e\}\,, \tag{13-17}$$

в которой каждая подгруппа нормальна в предыдущей, а последовательные факторы

$$\frac{(Q_k \cap P_i)P_{i+1}/P_{i+1}}{(Q_{k+1} \cap P_i)P_{i+1}/P_{i+1}} \simeq \frac{(Q_k \cap P_i)P_{i+1}}{(Q_{k+1} \cap P_i)P_{i+1}} \simeq \frac{(Q_k \cap P_i)}{(Q_{k+1} \cap P_i)(Q_k \cap P_{i+1})}$$

совпадают с (13-16). Так как группа P_i/P_{i+1} проста, мы заключаем, что в цепочке (13-17) имеется ровно одно нестрогое включение, а все остальные включения — равенства. Тем самым, ровно один из факторов (13-16) отличен от единицы и изоморфен P_i/P_{i+1}.

Те же самые рассуждения с заменой P на Q позволяют вставить между последовательными группами $Q_k \rhd Q_{k+1}$ композиционного ряда (13-14) убывающую цепочку подгрупп

$$Q_k \supseteq (P_1 \cap Q_k)Q_{k+1} \supseteq (P_2 \cap Q_k)Q_{k+1} \supseteq \cdots \supseteq (P_{n-1} \cap Q_k)Q_{k+1} \supseteq Q_{k+1}\,, \tag{13-18}$$

каждая из которых нормальна в предыдущей, а последовательные факторы имеют вид

$$\frac{(P_i \cap Q_k)Q_{k+1}}{(P_{i+1} \cap Q_k)Q_{k+1}} \simeq \frac{(Q_k \cap P_i)}{(Q_{k+1} \cap P_i)(Q_k \cap P_{i+1})} \tag{13-19}$$

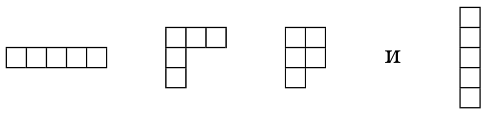
и изоморфны соответствующим факторам (13-16). Таким образом, вставляя между последовательными элементами композиционного ряда (13-13) цепочки (13-15), а между последовательными элементами ряда (13-14) — цепочки (13-18), мы получим цепочки одинаковой длины, в которых не все включения строгие, однако факторы которых находятся в естественной биекции, такой что соответственные факторы (13-19) и (13-16) изоморфны. Остаётся заметить, что группа Q_{k+1} является нормальной подгруппой во всех группах цепочки (13-18), и то же рассуждение, как с подгруппой P_{i+1} для цепочки (13-15), показывает, что при фиксированном k среди факторов (13-19) имеется ровно один отличный от единицы, и он изоморфен Q_k/Q_{k+1}. □

Замечание 13.1. Непростая группа может иметь несколько разных композиционных рядов с одинаковым набором факторов, а группы с одинаковыми наборами факторов Жордана-Гёльдера не обязательно изоморфны.

13.2.1. Конечные простые группы. Одним из крупных достижений математики XX века было создание полного списка всех конечных простых групп. Этот список состоит из нескольких бесконечных серий и 26 так называемых *спорадических групп*, не входящих в серии. Бесконечные серии делятся на три семейства: циклические группы $\mathbb{Z}/(p)$ простого порядка, знакопеременные группы A_n с[1] $n \geqslant 5$ и простые линейные алгебраические группы над конечными полями[2], такие как $\mathrm{PSL}_n(\mathbb{F}_q)$, $\mathrm{PSO}_n(\mathbb{F}_q)$, $\mathrm{PSp}_n(\mathbb{F}_q)$ и т. п. Эта классификация является итогом сотен работ десятков авторов по множеству напрямую несвязанных друг с другом направлений. Последние пробелы в ней, как принято считать, были устранены лишь в 2008 году. Какая-либо универсальная концепция, позволяющая единообразно классифицировать все конечные простые группы до сих пор не известна. Далее мы обсудим простоту знакопеременных групп.

Лемма 13.1
Знакопеременная группа A_5 проста.

Доказательство. В симметрической группе две перестановки сопряжены тогда и только тогда, когда у них одинаковый цикловой тип. Цикловые типы чётных перестановок из S_5 изображаются диаграммами



(13-20)

(5-циклы, 3-циклы, пары независимых транспозиций и тождественное преобразование). Эти классы сопряжённости в S_5 имеют мощность

$$5!/5 = 24 \qquad 5!/(3 \cdot 2) = 20 \qquad 5!/(2^2 \cdot 2) = 15 \qquad \text{и} \qquad 1\,.$$

Если перестановка относится к одному из последних трёх типов (13-20), то её централизатор содержит транспозицию пары неподвижных элементов или пары элементов, составляющих цикл длины 2. Поэтому две такие перестановки, сопряжённые в S_5, сопряжены

[1] группа $A_3 \simeq \mathbb{Z}/(3)$ тоже проста

[2] описание и классификация таких групп даются в курсах линейных алгебраических и арифметических групп; представление о них можно получить по книге *Дж. Хамфри.* Линейные алгебраические группы. М., «Наука», 1980

и в A_5. Стало быть, перестановки каждого из трёх последних типов (13-20) образуют один класс сопряжённости также и в A_5. Циклы длины 5 разбиваются в A_5 на два класса сопряжённости: 12 циклов, сопряжённых $|1,2,3,4,5\rangle$, и 12 циклов, сопряжённых $|2,1,3,4,5\rangle$. Поскольку любая нормальная подгруппа $H \lhd A_5$ вместе с каждой перестановкой содержит и все ей сопряжённые, $|H| = 12\varepsilon_1 + 12\varepsilon_2 + 20\varepsilon_3 + 15\varepsilon_4 + 1$, где каждый из коэффициентов ε_k равен либо 1, либо 0. С другой стороны, $|H|$ является делителем $|A_5| = 60 = 3 \cdot 4 \cdot 5$.

Упражнение 13.15. Убедитесь, что такое возможно ровно в двух случаях: когда все $\varepsilon_k = 1$ или когда все $\varepsilon_k = 0$.

Таким образом, нормальные подгруппы в A_5 исчерпываются единичной подгруппой и всей группой A_5. □

Теорема 13.2
Все знакопеременные группы A_n с $n > 5$ тоже просты.

Доказательство. Индукция по n. Стабилизатор $\mathrm{Stab}_{A_n}(k)$ любого элемента $k \in \{1, 2, \dots, n\}$ изоморфен A_{n-1}. Если $N \lhd A_n$, то пересечение $N \cap \mathrm{Stab}_{A_n}(k) \lhd \mathrm{Stab}_{A_n}(k)$ по индукции либо совпадает со $\mathrm{Stab}_{A_n}(k)$ либо равно $\{e\}$. Поскольку стабилизаторы всех элементов сопряжены, подгруппа N либо содержит стабилизаторы всех элементов $1, 2, \dots, n$, либо тривиально пересекается с каждым из них. В первом случае N содержит все пары транспозиций и, стало быть, совпадает с A_n по упр. 13.10. Во втором случае если в N есть хоть одна перестановка, переводящая некое i в $j \neq i$, то в силу тривиальности $\mathrm{Stab}_N(j)$ эта перестановка является *единственной* в N перестановкой, переводящей i в j. Но при $n \geqslant 6$ у любой перестановки $g \in A_n$, переводящей i в j и не имеющей неподвижных точек, есть сопряжённые ей в A_n и отличные от неё перестановки, также переводящие i в j.

Упражнение 13.16. Убедитесь в этом.

Поскольку N нормальна, все эти перестановки тоже лежат в N. Противоречие. □

13.3. Полупрямые произведения. Для пары подгрупп N, H группы G положим

$$NH = \{xh \mid x \in N\,,\ h \in H\}\,.$$

Отображение множеств $N \times H \to NH$, $(x,h) \mapsto xh$, биективно тогда и только тогда, когда $N \cap H = \{e\}$. В самом деле, при $x_1h_1 = x_2h_2$ элемент $x_2^{-1}x_1 = h_2h_1^{-1} \in N \cap H$, и если это пересечение исчерпывается единичным элементом, то $x_2 = x_1$ и $h_2 = h_1$, а если в пересечении есть элемент $z \neq e$, то две различных пары (e,e), $(z, z^{-1}) \in N \times H$ перейдут в один и тот же элемент $e \in NH$.

Будем называть подгруппы $N, H \subset G$ *дополнительными*, если $N \cap H = \{e\}$ и $NH = G$. В этом случае группа G как множество находится в биекции с прямым произведением $N \times H$. Если подгруппа $N \lhd G$ при этом нормальна, то композиция элементов $g_1 = x_1h_1$ и $g_2 = x_2h_2$ может быть выражена в терминах пар (x_1,h_1), $(x_2,h_2) \in N \times H$. А именно, т. к.

$$g_1g_2 = x_1h_1x_2h_2 = x_1(h_1x_2h_1^{-1}) \cdot h_1h_2$$

и $h_1x_2h_1^{-1} \in N$, мы можем *описать* группу G как множество $N \times H$ с операцией композиции, заданной правилом

$$(x_1,h_1) \cdot (x_2,h_2) = (x_1\,\mathrm{Ad}_{h_1}(x_2), h_1h_2)\,, \tag{13-21}$$

где через $\mathrm{Ad}_h : N \xrightarrow{\sim} N$, $x \mapsto hxh^{-1}$, обозначено присоединённое действие элемента h на нормальной подгруппе N. В этой ситуации говорят, что группа G является *полупрямым произведением* нормальной подгруппы $N \lhd G$ и дополнительной к ней подгруппы $H \subset G$ и пишут $G = N \rtimes H$. Если сопряжение элементами из подгруппы H действует на подгруппе N тривиально, что равносильно перестановочности $xh = xh$ любых двух элементов $x \in N$ и $h \in H$, то полупрямое произведение называется *прямым*. В этом случае

$$(x_1, h_1) \cdot (x_2, h_2) = (x_1 x_2, h_1 h_2)$$

для любых пар (x_1, h_1), $(x_2, h_2) \in N \times H$.

Пример 13.5 ($D_n = \mathbb{Z}/(n) \rtimes \mathbb{Z}/(2)$)
Группа диэдра D_n содержит нормальную подгруппу поворотов, изоморфную аддитивной группе $\mathbb{Z}/(n)$. Подгруппа второго порядка, порождённая любым отражением, дополнительна к группе поворотов и изоморфна аддитивной группе $\mathbb{Z}/(2)$. Присоединённое действие отражения на группе поворотов меняет знак у угла поворота. При отождествлении группы поворотов с $\mathbb{Z}/(n)$ это действие превращается в умножение на -1. Таким образом, $D_n = \mathbb{Z}/(n) \rtimes \mathbb{Z}/(2)$ и в терминах пар $(x, y) \in \mathbb{Z}/(n) \times \mathbb{Z}/(2)$ композиция на группе диэдра задаётся правилом

$$\left(x_1, y_1\right) \cdot \left(x_2, y_2\right) = \left(x_1 + (-1)^{y_1} x_2, y_1 + y_2\right), \quad x_1, x_2 \in \mathbb{Z}/(n), \quad y_1, y_2 \in \mathbb{Z}/(2).$$

13.3.1. Полупрямое произведение групп. Предыдущую конструкцию можно применить к двум абстрактным группам N и H как только задано действие группы H на группе N, т. е. имеется гомоморфизм

$$\psi : H \to \operatorname{Aut} N, \quad h \mapsto \psi_h : N \xrightarrow{\sim} N, \tag{13-22}$$

группы H в группу автоморфизмов группы N. По аналогии с формулой (13-21) зададим на декартовом произведении $N \times H$ операцию композиции правилом

$$(x_1, h_1) \cdot (x_2, h_2) = (x_1 \psi_{h_1}(x_2), h_1 h_2). \tag{13-23}$$

Упражнение 13.17. Проверьте, что формула (13-23) задаёт на $N \times H$ структуру группы с единицей (e, e) и обращением $(x, h)^{-1} = \left(\psi_h^{-1}(x^{-1}), h^{-1}\right)$, где $\psi_h^{-1} = \psi_{h^{-1}}$ — автоморфизм, обратный к $\psi_h : N \xrightarrow{\sim} N$.

Полученная таким образом группа называется *полупрямым произведением* групп N и H по действию $\psi : N \to \operatorname{Aut} H$ и обозначается $N \rtimes_\psi H$. Подчеркнём, что результат зависит от выбора действия ψ. Если действие тривиально, т. е. $\psi_h = \mathrm{Id}_N$ для всех $h \in H$, мы получаем прямое произведение $N \times H$ с покомпонентными операциями.

Упражнение 13.18. Убедитесь, что элементы вида (x, e) с $x \in N$ образуют в группе $G = N \rtimes_\psi H$ нормальную подгруппу N', изоморфную N, и фактор $G/N' \simeq H$, а элементы вида (e, h) с $h \in H$ образуют подгруппу H', дополнительную к N', и G является полупрямым произведением подгрупп N' и H'.

13.4. $\boldsymbol{p}$-группы и теоремы Силова. Группа порядка p^n, где $p \in \mathbb{N}$ — простое, называется *p-группой*. Поскольку все подгруппы p-группы также являются p-группами, длина любой орбиты p-группы при любом её действии на любом множестве либо делится на p, либо равна единице. Мы получаем простое, но полезное

Предложение 13.4
Пусть p-группа G действует на конечном множестве X, число элементов в котором не делится на p. Тогда G имеет на X неподвижную точку. □

Предложение 13.5
Любая p-группа имеет нетривиальный центр.

Доказательство. Рассмотрим присоединённое действие группы на себе. Центр группы представляет собой множество неподвижных точек этого действия. Поскольку и число элементов в группе, и длины всех орбит, содержащих более одной точки, делятся на p, кроме одноточечной орбиты e должны быть и другие одноточечные орбиты. □

Упражнение 13.19. Покажите, что любая группа G порядка p^2 (где p простое) абелева.

13.4.1. Силовские подгруппы. Пусть G — произвольная конечная группа. Запишем её порядок в виде $|G| = p^n m$, где p — простое, $n \geqslant 1$, и m взаимно просто с p. Всякая подгруппа $S \subset G$ порядка $|S| = p^n$ называется *силовской p-подгруппой* в G. Количество силовских p-подгрупп в G обозначается через $N_p(G)$.

Теорема 13.3 (теорема Силова)
Для любого простого p, делящего $|G|$, силовские p-подгруппы в G существуют. Все они сопряжены друг другу, и любая p-подгруппа в G содержится в некоторой силовской p-подгруппе.

Доказательство. Пусть $|G| = p^n m$, где m взаимно просто с p. Обозначим через $\mathcal{E}$ множество p^n-элементных подмножеств в G и рассмотрим действие G на $\mathcal{E}$, индуцированное левым регулярным действием G на себе. Стабилизатор точки $F \in \mathcal{E}$ состоит из всех элементов $g \in G$, левое умножение на которые переводит множество $F \subset G$ в себя:

$$\mathrm{Stab}(F) = \{g \in G \mid gF \subset F\}.$$

Так как $g_1 x \neq g_2 x$ при $g_1 \neq g_2$ в группе G, группа $\mathrm{Stab}(F)$ свободно действует на множестве F и все орбиты этого действия состоят из $|\mathrm{Stab}(F)|$ точек. Поэтому $|F| = p^n$ делится на $|\mathrm{Stab}(F)|$ и имеется следующая альтернатива: либо длина G-орбиты элемента $F \in \mathcal{E}$ делится на p, либо G-орбита элемента $F \in \mathcal{E}$ состоит из m элементов и $|\mathrm{Stab}(F)| = p^n$, т. е. подгруппа $\mathrm{Stab}(F) \subset G$ силовская. Во втором случае согласно предл. 13.4 каждая p-подгруппа $H \subset G$ (в частности, каждая силовская подгруппа), имеет на G-орбите элемента F неподвижную точку gF, а значит, содержится в силовской подгруппе $\mathrm{Stab}(gF) = g\,\mathrm{Stab}(F)\,g^{-1}$, сопряжённой к $\mathrm{Stab}(F)$ (и совпадает с ней, если H силовская). Таким образом, для доказательства теоремы остаётся убедиться, что в множестве $\mathcal{E}$ есть G-орбита, длина которой не делится на p. Это вытекает из следующей ниже леммы. □

Лемма 13.2
$|\mathcal{E}| = \binom{p^n m}{p^n} \equiv m \pmod{p}$ не делится на p.

Доказательство. Класс вычетов $\binom{p^n m}{p^n} \pmod p$ равен коэффициенту при x^{p^n}, возникающему при раскрытии бинома $(1+x)^{p^n m}$ над полем $\mathbb{F}_p = \mathbb{Z}/(p)$. Так как возведение в p-тую степень над $\mathbb{F}_p$ является аддитивным гомоморфизмом, $(1+x)^{p^n} = 1 + x^{p^n}$, откуда $(1+x)^{p^n m} = \left(1 + x^{p^n}\right)^m = 1 + mx^{p^n} +$ старшие степени. □

Следствие 13.1 (дополнение к теореме Силова)
В условиях теоремы Силова число N_p силовских p-подгрупп в G делит m и сравнимо с единицей по модулю p.

Доказательство. Обозначим множество силовских p-подгрупп в G через $\mathcal{S}$ и рассмотрим действие G на $\mathcal{S}$, индуцированное присоединённым действием G на себе. По теореме Силова это действие транзитивно, откуда $|\mathcal{S}| = |G|/|\mathrm{Stab}(P)|$, где $P \in \mathcal{S}$ — произвольно взятая силовская p-подгруппа. Поскольку $P \subset \mathrm{Stab}(P)$, порядок $|\mathrm{Stab}(P)|$ делится на $|P| = p^n$, а значит $|\mathcal{S}|$ делит $|G|/p^n = m$, что доказывает первое утверждение.

Для доказательства второго утверждения достаточно проверить, что P, действуя сопряжениями на $\mathcal{S}$, имеет там ровно одну неподвижную точку, а именно, саму себя. Тогда порядки всех остальных P-орбит будут делиться на p, и мы получим $|\mathcal{S}| \equiv 1 \pmod p$.

Пусть силовская подгруппа $H \in \mathcal{S}$ неподвижна при сопряжении подгруппой P. Это означает, что $P \subset \mathrm{Stab}(H) = \{g \in G \mid gHg^{-1} \subset H\}$. Поскольку $H \subset \mathrm{Stab}(H) \subset G$, порядок $|\mathrm{Stab}(H)| = p^n m'$, где $m' | m$ и взаимно просто с p. Таким образом, и P, и H являются силовскими p-подгруппами в $\mathrm{Stab}(H)$, причём H нормальна в $\mathrm{Stab}(H)$. Так как все силовские подгруппы сопряжены, мы заключаем, что $H = P$, что и требовалось. □

Пример 13.6 (группы порядка pq с простыми $p > q$ и нод$(p-1, q) = 1$)
Пусть $|G| = pq$, где $p > q$ простые. Тогда в G есть ровно одна силовская p-подгруппа $H_p \simeq \mathbb{Z}/(p)$, автоматически нормальная. Рассмотрим любую силовскую q-подгруппу $H_q \simeq \mathbb{Z}/(q)$. Поскольку H_p и H_q просты, $H_p \cap H_q = e$ и $G = H_p H_q$. Согласно n° 13.3 $G = H_p \underset{\psi}{\rtimes} H_q$ для некоторого гомоморфизма $\psi : H_q \to \mathrm{Aut}\, H_p$.

Упражнение 13.20. Убедитесь, что $\mathrm{Aut}(H_p)$ — циклическая группа порядка $p - 1$.

Аддитивный гомоморфизм $\psi : \mathbb{Z}/(q) \to \mathbb{Z}/(p-1)$ однозначно задаётся своим значением на образующей $[1]_q$ $\mathbb{Z}$-модуля $\mathbb{Z}/(q)$. Поскольку $0 = \psi(0) = \psi(q \cdot [1]_q) = q \cdot \psi([1]_q)$, элемент $\psi([1]_q) \in \mathbb{Z}/(p-1)$ должен аннулироваться оператором умножения на $q : x \mapsto qx$. Но при нод$(p-1, q) = 1$ в $\mathbb{Z}$-модуле $\mathbb{Z}/(p-1)$ этот оператор обратим, откуда $\psi = 0$, т. е. в мультипликативной записи гомоморфизм $\psi : H_q \to \mathrm{Aut}\, H_p$ переводит H_q в тождественное преобразование. Поэтому $G = H_p \times H_q \simeq \mathbb{Z}/(p) \oplus \mathbb{Z}/(q)$ при простых $p > q$ с нод$(p-1, q) = 1$.

Пример 13.7 (группы порядка $2p$)
Пусть $|G| = 2p$, где $p > 2$ простое. Рассуждая как в предыдущем примере, заключаем, что $G = \mathbb{Z}/(p) \underset{\psi}{\rtimes} \mathbb{Z}/(2)$ для некоторого действия $\psi : \mathbb{Z}/(2) \to \mathrm{Aut}\big(\mathbb{Z}/(p)\big) \simeq \mathbb{F}_p^*$, которое однозначно задаётся элементом $\psi([1]) \in \mathbb{F}_p^*$ с $\psi([1])^2 = 1$. Таких элементов имеется ровно два: $\psi([1]) = 1$ и $\psi([1]) = -1$. В первом случае действие ψ тривиально и $G \simeq \mathbb{Z}/(p) \oplus \mathbb{Z}/(q)$. Во втором случае $[0] \in \mathbb{Z}/(2)$ действует на $\mathbb{Z}/(p)$ тривиально, а $[1] \in \mathbb{Z}/(2)$ действует на $\mathbb{Z}/(p)$ сменой знака, т. е. $G \simeq D_p$ это группа правильного p-угольника.

Упр. 13.1. Первое очевидно, второе вытекает из того, что при вставке фрагмента $x^{\varepsilon}x^{-\varepsilon}$ в произвольное слово w получится такое слово, в котором сокращение любого фрагмента вида $y^{\varepsilon}y^{-\varepsilon}$ приведёт либо обратно[1] к слову w, либо к слову, получающемуся из w сначала сокращением *того же самого фрагмента* $y^{\varepsilon}y^{-\varepsilon}$, а уже затем вставкой $x^{\varepsilon}x^{-\varepsilon}$ в *то же самое место*, что и в w.

Упр. 13.2. Отобразите $n \in \mathbb{N}$ в $x^n y x^n \in F_2$ и воспользуйтесь предл. 13.1 на стр. 198.

Упр. 13.4. Так как $x_1^2 = x^2 = e$, $\underbrace{x_1 x_2 x_1 \dots}_{n} = \underbrace{x_2 x_1 x_2 \dots}_{n}$ и $(x_2 x_1)^n = e$.

Упр. 13.5. Композиция $\sigma_i \circ \sigma_j$ отражений в плоскостях π_i и π_j является поворотом на удвоенный угол $2\pi/m_k$ между этими плоскостями вокруг прямой $\pi_i \cap \pi_j$ в направлении от π_j к π_i.

Упр. 13.6. Это следует из упр. 13.3 на стр. 200.

Упр. 13.7. Первое вытекает из того, что геодезическая прямая, проходящая через вершину триангуляции, разбивает $2m_i$ рёбер, сходящихся в этой вершине, в точности пополам — тем самым, при прохождении геодезической через вершину в отвечающем ей слове один фрагмент длины n заменяется другим фрагментом длины n. Утверждения (б) и (в) доказываются индукцией по длине минимального слова, ведущего в g. Пусть они верны для элемента g. Достаточно убедиться, что они верны для всех элементов $g\sigma_i$. Проведём из e в g геодезическую так, чтобы она сама или её продолжение пересекало сторону $g(\pi_i)$ треугольника g и обозначим через $u = g$ считанное с этой геодезической минимальное слово для g. Если геодезическая входит в треугольник g через сторону $g(\pi_i)$, то $u = w\sigma_i$, а значит $g\sigma_i = w$ имеет более короткое минимальное слово и утверждения верны для него по индукции. Если продолжение геодезической выходит из g через $g(\pi_i)$, то оно попадает в $g\sigma_i$, и значит $g\sigma_i = u\sigma_i$. Либо это минимальное слово для $g\sigma_i$, и тогда утверждения (а) и (б) верны, либо $g\sigma_i$ можно записать более коротким словом, и тогда утверждения (а) и (б) верны для $g\sigma_i$ по индукции.

Упр. 13.8. Обозначим через v_i вектор, идущий из центра симплекса Δ в вершину i. Вектор $n_{ij} = v_i - v_j$ ортогонален гиперплоскости π_{ij}, поскольку для любого $k \neq i, j$ скалярное произведение $\big(n_{ij}, v_k - (v_i + v_j)/2\big) = (v_i, v_k) - (v_j, v_k) + (v_i, v_i)/2 - (v_j, v_j)/2 = 0$, т. к. все произведения (v_i, v_j) с $i \neq j$ и все скалярные квадраты (v_i, v_i) одинаковы. Аналогичная выкладка показывает, что при $\{i, j\} \cap \{k, m\} = \varnothing$ векторы n_{ij} и n_{km} ортогональны. Векторы $v_i - v_k$ и $v_k - v_j$ образуют в натянутой на них двумерной плоскости стороны правильного треугольника с вершинами в концах векторов v_i, v_j и v_k, и угол между ними равен 60°.

Упр. 13.12. Воспользуйтесь индукцией по длине минимального слова и тем же рассуждением, что в упр. 13.8.

Упр. 13.13. При эпиморфизме S_4 на группу треугольника из прим. 12.9 подгруппа чётных перестановок $A_4 \subset S_4$ переходит в группу вращений треугольника.

[1] обратите внимание, что такое происходит *не только* при сокращении того же самого фрагмента $x^{\varepsilon}x^{-\varepsilon}$, который был перед этим вставлен, но и при сокращении одной из букв $x^{\pm\varepsilon}$ с её соседкой

Упр. 13.14. По предл. 12.5 $(A \cap D)C \lhd D$, поскольку $C \lhd D$. Изоморфизм $HN/N \simeq H/H \cap N$ из предл. 12.5 в случае $G = D$, $H = B \cap D$ и $N = (A \cap D)C$ имеет требуемый вид

$$(B \cap D)C/(A \cap D)C \simeq (B \cap D)/(A \cap D)(B \cap C).$$

В самом деле, $A \subset B \Rightarrow HN = (B \cap D)(A \cap D)C = (B \cap D)C$. Равенство

$$H \cap N = (B \cap D) \cap (A \cap D) = (A \cap D)(B \cap C)$$

вытекает из того, что любой элемент $d = ac \in (B \cap D) \cap (A \cap D)$ с $d \in B \cap D$, $a \in A \cap D$, и $c \in C$ имеет $c = a^{-1}d \in C \cap B$.

Упр. 13.15. Правая часть формулы $|H| = 12\varepsilon_1 + 12\varepsilon_2 + 20\varepsilon_3 + 15\varepsilon_4 + 1$, приведённая по модулю 3, по модулю 4 и по модулю 5, равна, соответственно, $1 - \varepsilon_3$, $1 - \varepsilon_4$ и $1 + 2(\varepsilon_1 + \varepsilon_2)$. Она может делиться на 3 или на 4 только если $\varepsilon_3 = 1$ или $\varepsilon_4 = 1$. В обоих случаях $|H| \geqslant 16$, так что $|H|$ не может быть ни 3, ни 4, ни $3 \cdot 4$, ни $3 \cdot 5$. Если $|H|$ делится на 5, то $\varepsilon_1 = \varepsilon_2 = 1$ и $|H| \geqslant 25$, так что $|H|$ не может быть ни 5, ни $4 \cdot 5$. Остаются ровно две возможности: $|H| = 1$ и $|H| = 3 \cdot 4 \cdot 5$.

Упр. 13.16. Рассмотрим любое $k \notin i, j, g^{-1}(i)$. Тогда $g(k) = m \notin \{i, j, k\}$. При $n \geqslant 6$ найдётся чётная перестановка h, оставляющая на месте i, j, k и переводящая m в $\ell \neq m$. Тогда hgh^{-1} переводит i в j, а k — в $\ell \neq m$.

Упр. 13.17. Проверка ассоциативности:

$$\big((x_1, h_1) \cdot (x_2, h_2)\big) \cdot (x_3, h_3) = \big(x_1\psi_{h_1}(x_2),\ h_1h_2\big) \cdot (x_3, h_3) = \big(x_1\psi_{h_1}(x_2)\psi_{h_1h_2}(x_3),\ h_1h_2h_3\big)$$
$$(x_1, h_1) \cdot \big((x_2, h_2) \cdot (x_3, h_3)\big) = (x_1, h_1) \cdot \big(x_2\psi_{h_2}(x_3),\ h_2h_3\big) = \Big(x_1\psi_{h_1}\big(x_2\psi_{h_2}(x_3)\big),\ h_1h_2h_3\Big).$$

Но $\psi_{h_1}\big(x_2\psi_{h_2}(x_3)\big) = \psi_{h_1}(x_2)\psi_{h_1} \circ \psi_{h_2}(x_3) = \psi_{h_1}(x_2)\psi_{h_1h_2}(x_3)$. Существование единицы: $(x, h) \cdot (e, e) = (x, \psi_h(e), he) = (x, h)$, поскольку $\psi_h(e) = e$ в силу того, что ψ_h гомоморфизм. Существование обратного: $\big(\psi_h^{-1}(x^{-1}),\ h^{-1}\big) \cdot (x, h) = \big(\psi_h^{-1}(x^{-1})\psi_h^{-1}(x^{-1}),\ h^{-1}h\big) = (e, e)$.

Упр. 13.18. Так как $\psi : H \to \operatorname{Aut} N$ — гомоморфизм, $\psi_e = \mathrm{Id}_N$ и

$$(x_1, e) \cdot (x_2, e) = (x_1\psi_e(x_2), e) = (x_1x_2, e),$$

т. е. элементы (x, e) образуют подгруппу, изоморфную N. Она нормальна, поскольку

$$(y, h) \cdot (x, e) \cdot \big(\psi_h^{-1}(y^{-1}), h^{-1}\big) = (y\psi_h(x), h) \cdot \big(\psi_h^{-1}(y^{-1}), h^{-1}\big) = \big(y\psi_h(x)y^{-1}, e\big).$$

Элементы (e, h) очевидно образуют дополнительную подгруппу, изоморфную H, и

$$\mathrm{Ad}_{(e,h)}(x, e) = (\psi_h(x), e).$$

Упр. 13.19. Пусть центр $Z(G) = C$. Если $|C| = p$, то $C \simeq \mathbb{Z}/(p) \simeq G/C$. Пусть $a \in C$ — образующая центра, $b \in G$ — такой элемент, что смежный класс bC является образующей в G/C. Тогда любой элемент группы имеет вид $b^k a^m$. Так как a централен, любые два таких элемента коммутируют.

Упр. 13.20. Аддитивные автоморфизмы группы $\mathbb{Z}/(p)$ суть линейные автоморфизмы одномерного векторного пространства над полем $\mathbb{F}_p$. Они образуют группу $\mathrm{GL}_1(\mathbb{F}_p) \simeq \mathbb{F}_p^*$ ненулевых элементов поля $\mathbb{F}_p$ по умножению. Как и всякая конечная мультипликативная подгруппа поля, она циклическая.

§14. Пространство с билинейной формой

14.1. Билинейные формы. Пусть V — векторное пространство над полем $\Bbbk$. Отображение $\beta : V \times V \to \Bbbk$, $(u,w) \mapsto \beta(u,w)$, линейное по каждому из двух аргументов при фиксированном другом, называется *билинейной формой* на пространстве V. Билинейность означает, что при всех $\lambda \in \Bbbk$ и $u, w \in V$ выполняются равенства

$$\beta(u, \lambda w) = \lambda\beta(u,w) = \beta(\lambda u, w)$$
$$\beta(u_1 + u_2, w_1 + w_2) = \beta(u_1, w_1) + \beta(u_1, w_2) + \beta(u_2, w_1) + \beta(u_2, w_2).$$

Если на пространствах V_1 и V_2 заданы билинейные формы β_1 и β_2, то линейное отображение $f : V_1 \to V_2$ называется *изометрическим* (или *гомоморфизмом билинейных форм*), если $\forall\, v, w \in V_1\ \beta_1(v,w) = \beta_2\big(f(v), f(w)\big)$. Билинейные формы β_1 и β_2 называются *изоморфными*, если между пространствами V_1 и V_2 имеется изометрический изоморфизм.

14.1.1. Матрицы Грама. Билинейные формы на V образуют векторное подпространство в пространстве всех функций $V \times V \to \Bbbk$. Если зафиксировать в пространстве V базис $e = (e_1, e_2, \dots, e_n)$, то каждая билинейная форма β будет однозначно задаваться своими значениями $\beta_{ij} = \beta(e_i, e_j)$ на всевозможных парах базисных векторов. Таблица этих значений называется *матрицей Грама* формы β. Мы будем обозначать матрицы Грама одноимёнными формам большими буквами:

$$B_e = \left(\beta_{ij}\right), \quad \text{где} \quad \beta_{ij} = \beta(e_i, e_j).$$

Значение формы β на любой паре векторов $u = ex = \sum x_i e_i$ и $w = ey = \sum y_j e_j$ равно:

$$\beta(u,w) = \beta\Big(\sum_i x_i e_i\,, \sum_j y_j e_j\Big) = \sum_{ij} \beta_{ij} x_i y_j = x^t B y\,, \tag{14-1}$$

где через x^t и y обозначены, соответственно, строка и столбец координат векторов u и w в базисе $e = (e_1, e_2, \dots, e_n)$. Поскольку нулевую матрицу Грама имеет лишь тождественно нулевая билинейная форма, и любая матрица $B = \left(\beta_{ij}\right)$ размера $n \times n$ задаёт по формуле (14-1) билинейную форму β на пространстве с базисом $e = (e_1, e_2, \dots, e_n)$, отображение $\beta \mapsto B_e$, сопоставляющее билинейной форме β её матрицу Грама в фиксированном базисе e, задаёт изоморфизм пространства билинейных форм с пространством квадратных матриц размера $n \times n$. В частности, размерность пространства билинейных форм на n-мерном векторном пространстве равна n^2.

Более общим образом, произвольным двум наборам векторов пространства V

$$u = (u_1, u_2, \dots, u_k) \quad \text{и} \quad w = (w_1, w_2, \dots, w_m)$$

можно сопоставить их *взаимную матрицу Грама* $B_{uw} = \big(\beta(u_i, w_j)\big)$. Если для двух векторов $a, b \in V$ положить

$$a \cdot b \overset{\text{def}}{=} \beta(a,b) \in \Bbbk\,, \tag{14-2}$$

а для двух матриц A, B, элементами которых являются векторы пространства V, обозначить через $A \cdot B$ матрицу с элементами из $\Bbbk$, вычисленную по правилам умножения матриц с использованием для перемножения векторов операции (14-2), то взаимную матрицу Грама двух наборов векторов $u = (u_1, u_2, \dots, u_k)$ и $w = (w_1, w_2, \dots, w_m)$ можно описать формулой $B_{uv} = u^t \cdot w$, где u^t — столбец из векторов $u_1, u_2, \dots, u_k$. Отметим, что

$$B_{wu} = B_{uw}^t\,.$$

Если наборы векторов u и w линейно выражаются через наборы векторов e и f по формулам $u = eC_{eu}$ и $w = fC_{fw}$, то матрица Грама B_{uw} выражается через матрицу Грама B_{ef} и матрицы перехода C_{eu} и C_{fw} по формуле

$$B_{uw} = u^t \cdot w = \left(eC_{eu}\right)^t \cdot \left(fC_{fw}\right) = C_{eu}^t e^t \cdot fC_{fw} = C_{eu}^t B_{ef} C_{fw} . \tag{14-3}$$

В частности, если два базиса e и f пространства V связаны переходом $f = eC_{ef}$, то

$$B_f = C_{ef}^t B_e C_{ef} = \left(C_{fe}^{-1}\right)^t B_e C_{fe}^{-1} . \tag{14-4}$$

Отметим, что *определитель Грама* при замене базиса умножается на ненулевой квадрат:

$$\det B_f = \det B_e \cdot \det^2 C_{ef} = \det B_e \,/\det^2 C_{fe} . \tag{14-5}$$

14.1.2. Корреляции. Задание билинейной формы $\beta : V \times V \to \Bbbk$ равносильно заданию линейного оператора

$$\beta : V \to V^* , \quad v \mapsto \beta(*, v) , \tag{14-6}$$

переводящего вектор $v \in V$ в линейную форму $w \mapsto \beta(w, v)$. Этот оператор называется *правой корреляцией* билинейной формы β. Мы умышленно обозначили его той же буквой, что и форму.

Упражнение 14.1. Убедитесь, что матрица оператора $\beta : V \to V^*$ написанная в произвольном базисе e пространства V и двойственном базисе e^* пространства[1] V^*, равна матрице Грама B_e формы β в базисе e.

Если обозначить через $\langle \, * \, , \, * \, \rangle : V^* \times V \to \Bbbk$ спаривание векторов с ковекторами[2], то билинейная форма восстанавливается по своей правой корреляции как

$$\beta(u, w) = \langle \, \beta w \, , \, u \, \rangle \; .$$

Если на пространствах V_1 и V_2 заданы билинейные формы с корреляциями β_1 и β_2, то линейное отображение $f : V_1 \to V_2$ является изометрическим, если и только если

$$\beta_1 = f^* \beta_2 f \, , \tag{14-7}$$

т. е. когда коммутативна диаграмма

$$\begin{tikzcd} V_1^* & V_2^* \arrow[l, "f^*"'] \\ V_1 \arrow[u, "\beta_1"] \arrow[r, "f"] & V_2 \arrow[u, "\beta_2"'] \end{tikzcd} ,$$

в которой $f^* : V_2^* \to V_1^*$ это двойственное к f линейное отображение[3], что ещё раз объясняет матричные соотношения (14-3) и (14-4).

Упражнение 14.2. Убедитесь, что равенство (14-7) означает, что

$$\forall \, v, w \in V_1 \quad \beta_1(v, w) = \beta_2\big(f(v), f(w)\big) .$$

[1] j-тый столбец этой матрицы образован координатами вектора $\beta(e_j)$ в базисе e^*

[2] см. прим. 7.5 на стр. 107

[3] напомню (см. n° 7.3 на стр. 109), что линейное отображение $f^* : W^* \to U^*$, двойственное к $f : U \to W$, определяется тем, что $\forall \, \xi \in W^* \; \forall \, u \in U \; \langle \, f^*\xi \, , \, u \, \rangle = \langle \, \xi \, , \, fu \, \rangle$

Двойственный к правой корреляции $\beta : V \to V^*$ оператор $\beta^* : V^{**} = V \to V$ связан с оператором β соотношением $\langle \beta^* u , w \rangle = \langle \beta w , u \rangle$, и задаёт билинейную форму

$$\beta^*(u,w) = \langle \beta^* w , u \rangle = \langle \beta u , w \rangle = \beta(w,u),$$

получающуюся из формы β перестановкой аргументов. В терминах формы β оператор

$$\beta^* : V \to V^*, \quad v \mapsto \beta(v,*) \tag{14-8}$$

переводит вектор $v \in V$ в линейную форму $w \mapsto \beta(v,w)$. Поэтому он называется *левой корреляцией* билинейной формы[1] β.

Упражнение 14.3. Убедитесь в том, что матрица левой корреляции в двойственных базисах e и e^* пространств V и V^* это транспонированная матрица Грама B_e^t формы β в базисе e.

Если корреляции β и β^* пропорциональны друг другу: $\beta^* = c\beta$, то $\beta(u,w) = c\beta(w,u) = c^2\beta(u,w)$, откуда при $\beta(u,w) \neq 0$ получаем $c = \pm 1$. Таким корреляциям отвечают *симметричные* формы $\beta(u,w) = \beta(w,u)$ с $\beta^* = \beta$ и кососимметричные формы $\beta(u,w) = -\beta(w,u)$ с $\beta^* = -\beta$. Специальным свойствам (косо) симметричных форм будет посвящён раздел n° 14.4 ниже, отдельно симметричным формам — весь следующий §15.

14.1.3. Характеристический многочлен несимметричной формы. Будем называть формы $\beta(u,w) \neq \pm\beta(w,u)$ *несимметричными*. Каждая несимметричная билинейная форма β задаёт двумерное пространство корреляций, порождённое β и β^* и называемое *пучком корреляций* формы β . Мы обозначим его

$$\mathcal{C}_\beta = \{\lambda \cdot \beta^* + \varrho \cdot \beta : V \to V^* \mid \lambda, \varrho \in \Bbbk\} \subset \mathrm{Hom}(V, V^*). \tag{14-9}$$

Можно воспринимать $\mathcal{C}_\beta$ как *пучок билинейных форм* $\lambda\beta(u,w) + \mu\beta(w,u)$. На пучке $\mathcal{C}_\beta$ имеется каноническая инволюция, действующая на операторы сопряжением, а на формы — перестановкой аргументов, и переставляющая друг с другом координаты (λ, ϱ). Определитель

$$\chi_\beta(\lambda, r) = \det\left(\lambda B_e^t + \varrho B_e\right) \tag{14-10}$$

называется *характеристическим многочленом* формы β. Это однородный многочлен степени $\dim V$ (возможно нулевой) от переменных (λ, ϱ). Он *зависит* от выбора базиса e в котором пишется матрица Грама B_e. При выборе другого базиса $\varepsilon = eC_{e\varepsilon}$ получится многочлен, отличающийся от (14-10) постоянным множителем:

$$\det\left(\lambda B_\varepsilon^t + \varrho B_\varepsilon\right) = \det\left(\lambda C_{e\varepsilon}^t B_e^t C_{e\varepsilon} + \varrho C_{e\varepsilon}^t B_e C_{e\varepsilon}\right) = \det\left(\lambda B_e + \varrho B_e\right) \cdot \det^2 C_{e\varepsilon}$$

Будем называть несимметричную форму *регулярной*, если её характеристический многочлен (14-10) ненулевой. В этом случае его корни $\mu = \varrho : \lambda$ на проективной прямой[2] $\mathbb{P}_1 = \mathbb{P}(\mathcal{C}_\beta)$ называются *характеристическими числами* формы β. Они не зависят от выбора базиса в V. То же вычисление показывает, что изоморфные формы имеют одинаковые

[1]но является при этом *правой* корреляцией для формы β^*

[2]включая значения $0 = 0 : 1$ и $0^{-1} = \infty = 1 : 0$, возникающие при $\det(B_e) = 0$, т. е. когда форма β вырождена, но регулярна

наборы характеристических чисел. Так как определитель не меняется при транспонировании матрицы, характеристический многочлен симметричен по λ, ϱ:

$$\chi_\beta(\lambda, \varrho) = \det\left(\lambda B_e^t + \varrho B_e\right) = \det\left(\lambda B_e^t + \varrho B_e\right)^t = \det\left(\lambda B_e + \varrho B_e^t\right) = \chi_\beta(\varrho, \lambda).$$

Поэтому вместе с каждым характеристическим числом $\mu \neq \pm 1$ обратное число μ^{-1} также является характеристическим и имеет ту же кратность, что μ. Характеристическим значениям $\lambda : \varrho$ отвечают вырожденные корреляции (14-9). Для регулярной формы β они образуют конечный набор из $\leqslant \dim V$ одномерных подпространств в $\mathcal{C}_\beta$. Все остальные корреляции в $\mathcal{C}_\beta$ невырождены.

Упражнение 14.4. Покажите, что в пучке корреляций (14-9) есть ровно одна симметричная и ровно одна кососимметричная форма. Могут ли обе они быть вырождены, если несимметричная форма β невырождена?

14.1.4. Невырожденность билинейной формы β можно характеризовать многими способами.

Предложение 14.1 (критерии невырожденности)
Следующие условия на билинейную форму $\beta : V \times V \to \Bbbk$ с матрицей Грама B_e в некотором базисе $e = (e_1, e_2, \dots, e_n)$ пространства V эквивалентны:

1) $\det B_e \neq 0$
2) для любого ненулевого $u \in V$ $\exists\, w \in V : \beta(u, w) \neq 0$
3) левая корреляция $\beta^* : V \xrightarrow{\sim} V^*$ является изоморфизмом
4) любой ковектор $\xi : V \to \Bbbk$ представим в виде $\xi(v) = \beta(u_\xi, v)$ с $u_\xi \in V$
5) для любого ненулевого $w \in V$ $\exists\, u \in V : \beta(u, w) \neq 0$
6) правая корреляция $\beta : V \xrightarrow{\sim} V^*$ является изоморфизмом
7) любой ковектор $\xi : V \to \Bbbk$ представим в виде $\xi(v) = \beta(v, w_\xi)$ с $w_\xi \in V$.

В частности, если условие (1) выполнено для какого-то базиса e, то оно выполнено и для любого другого базиса, а векторы u_ξ и w_ξ в (4) и (7) однозначно определяются ковектором ξ (если существуют).

Доказательство. Поскольку $\dim V = \dim V^*$, условия (2) и (4), означающие, соответственно, что $\ker \beta^* = 0$ и что $\operatorname{im} \beta^* = V^*$, равносильны условию (3). По той же причине эквивалентны друг другу и условия (5), (6), (7). Поскольку матрицы операторов β^* и β в двойственных друг другу базисах e и e^* суть B_e^t и B_e, их невырожденность равносильна тому, что $\det B_e^t = \det B_e \neq 0$. □

Определение 14.1
Билинейные формы β, удовлетворяющие условиям предл. 14.1 называются *невырожденными* или *неособыми*. Все остальные билинейные формы называются *вырожденными* или *особыми*.

14.1.5. Ядра. Если форма β вырождена, то *обе* её корреляции имеют ненулевые ядра

$$\ker\beta = \{u \in V \mid \forall\, v \in V\ \beta(v,u) = 0\} \quad \text{и} \quad \ker\beta^* = \{u \in V \mid \forall\, v \in V\ \beta(u,v) = 0\}\,,$$

называемые, соответственно, *правым* и *левым* ядром билинейной формы β. Вообще говоря, это *разные* подпространства в V, однако размерность у них одинакова, поскольку операторы β^* и β сопряжены друг другу и, стало быть, имеют одинаковый ранг[1].

14.2. Конструкции с невырожденными формами. Если билинейная форма β невырождена, то для любого базиса $e = (e_1, e_2, \dots, e_n)$ пространства V прообразы векторов двойственного базиса $e^* = (e_1^*, e_2^*, \dots, e_n^*)$ пространства V^* относительно левой и правой корреляций образуют в V два базиса ${}^\vee e = ({}^\vee e_1, {}^\vee e_2, \dots, {}^\vee e_n)$ и $e^\vee = (e_1^\vee, e_2^\vee, \dots, e_n^\vee)$, называемые *левым* и *правым* двойственными относительно формы β к исходному базису e, поскольку

$$\beta\left({}^\vee e_i, e_j\right) = \beta\left(e_i, e_j^\vee\right) = \begin{cases} 1 & \text{при } i = j \\ 0 & \text{при } i \neq j\,. \end{cases} \tag{14-11}$$

Они выражаются через базис e по формулам ${}^\vee e = e\,{B_e^{-1}}^t$ и $e^\vee = e\,B_e^{-1}$. Знание двойственного базиса позволяет раскладывать произвольный вектор $v \in V$ по базису e как

$$v = \sum_\nu \beta\left({}^\vee e_\nu, v\right) \cdot e_\nu = \sum_\nu \beta\left(v, e_\nu^\vee\right) \cdot e_\nu\,, \tag{14-12}$$

в чём легко убедиться применив к обеим частям функционалы $\beta\left({}^\vee e_\nu, *\right)$ и $\beta\left(*, e_\nu^\vee\right)$ соответственно.

14.2.1. Группа изометрий $\mathrm{O}_\beta(V)$ невырожденной билинейной формы β на пространстве V определяется как множество всех операторов $g : V \to V$, сохраняющих форму β в том смысле, что

$$\forall\, u, w \in V \quad \beta(gu, gw) = \beta(u, w)\,.$$

В терминах корреляций это означает равенство $g^*\beta g = \beta$, из которого вытекает, что $\det g \neq 0$. Поэтому каждая изометрия обратима, и обратный к изометрии g оператор $g^{-1} = \beta^{-1}g^*\beta$ также является изометрией.

Упражнение 14.5. Убедитесь в этом.

Так как композиции изометрий очевидно тоже являются изометриями, изометрии действительно образуют группу. В упр. 14.8 ниже изометрии формы β будут охарактеризованы как операторы, сопряжённые относительно формы β к своим обратным.

14.2.2. Биекция между формами и операторами. Если на пространстве V задана билинейная форма $\beta : V \times V \to \Bbbk$, то каждому линейному оператору $f : V \to V$ можно сопоставить корреляцию $\beta f : V \to V^*$ или билинейную форму $\beta f(u,w) = \beta(u, fw)$. Отображение

$$\operatorname{End} V \to \operatorname{Hom}(V, V^*)\,, \quad f \mapsto \beta f\,, \tag{14-13}$$

линейно и является изоморфизмом, если форма β невырождена, т. к. в этом случае каждая корреляция $\psi : V \to V^*$ имеет вид $\psi = \beta f$ для единственного оператора $f = \beta^{-1}\psi$. При изоморфизме (14-13) невырожденным операторам соответствуют невырожденные формы и наоборот.

[1]по-другому можно было бы сказать, что матрицы B_e^t и B_e этих операторов транспонированы друг другу, а значит, имеют равный ранг

14.2.3. Канонический оператор. Оператор $\varkappa = \beta^{-1}\beta^* : V \to V$, отвечающий при изоморфизме (14-13) левой корреляции β^*, т. е. такой что

$$\forall\, u, w \in V \quad \beta(w,u) = \beta(u, \varkappa w)\,, \tag{14-14}$$

называется *каноническим оператором* формы β. Если форма β невырождена, он существует и единствен. Мы будем писать $\varkappa_\beta$, когда надо уточнять, о какой форме β идёт речь. Матрица K оператора $\varkappa$ в любом базисе пространства V выражается через матрицу Грама B формы β в этом базисе по формуле $K = B^{-1}B^t$.

Упражнение 14.6. Убедитесь, что при замене матрицы Грама по правилу $B \mapsto C^tBC$ с $C \in \mathrm{GL}_n(\Bbbk)$ матрица $K = B^{-1}B^t$ меняется как $K \mapsto C^{-1}KC$.

Так как $\forall\, u, w \in V\ \beta(u,w) = \beta(w, \varkappa u) = \beta(\varkappa u, \varkappa w)$, канонический оператор является изометрическим. Характеристический многочлен канонического оператора

$$\chi_\varkappa(t) = \det(tE - B^{-1}B^t) = \det{}^{-1}(B)\cdot\det(tB - B^t) = \det{}^{-1}(B)\cdot\chi_\beta(-1,t)$$

пропорционален ограничению характеристического многочлена $\chi_\beta(\lambda,\varrho) = \det(\lambda\beta^* + \varrho\beta)$ формы β на прямую $\lambda = -1$. Поэтому собственные числа канонического оператора суть характеристические числа формы β, взятые с противоположным знаком. В n° 14.2.6 ниже мы докажем такой факт:

Теорема 14.1
Над алгебраическим полем $\Bbbk$ характеристики нуль две невырожденые билинейных формы на конечномерном векторном пространстве изометрически изоморфны тогда и только тогда, когда их канонические операторы подобны. □

Доказательство теор. 14.1 использует *сопряжение* операторов невырожденной билинейной формой, часто встречающееся и во многих других задачах линейной алгебры.

14.2.4. Сопряжение операторов. На пространстве V с невырожденной билинейной формой β каждому линейному оператору $f : V \to V$ можно сопоставить *правый сопряжённый оператор* $f^\vee = \beta^{-1}f^*\beta : V \to V$, получающийся сопряжением двойственного к f оператора $f^* : V^* \to V^*$ изоморфизмом $\beta : V \xrightarrow{\sim} V^*$, т. е. включающийся в коммутативную диаграмму

$$\begin{tikzcd} V^* \arrow[r, "f^*"'] & V^* \\ V \arrow[u, "\beta"] \arrow[r, "f^\vee"] & V \arrow[u, "\beta"'] \end{tikzcd}\ . \tag{14-15}$$

На языке билинейных форм правый сопряжённый оператор однозначно определяется соотношением

$$\forall u, w \in V \quad \beta(fu, w) = \beta(u, f^\vee w)\,. \tag{14-16}$$

Симметричным образом *левый сопряжённый* к f оператор ${}^\vee f = (b^*)^{-1} f^*\beta^* : V \to V$ задаётся соотношением

$$\forall u, w \in V \quad \beta({}^\vee f u, w) = \beta(u, fw) \tag{14-17}$$

и получается сопряжением двойственного к f оператора f^* левой корреляцией β^* формы β, т. е. включается в коммутативную диаграмму

$$\begin{tikzcd} V^* \arrow[r, "f^*"] & V^* \\ V \arrow[u, "\beta^*"] \arrow[r, "{}^\vee f"] & V \arrow[u, "\beta^*"'] \end{tikzcd} \tag{14-18}$$

Матрицы ${}^\vee F_e$ и $F_e^\vee$ операторов ${}^\vee f$ и $f^\vee$ в произвольном базисе пространства V выражаются через матрицу F оператора f и матрицу Грама B формы φ по формулам

$${}^\vee F = \left(B^t\right)^{-1} F^t B^t \quad \text{и} \quad F^\vee = B^{-1} F B\,. \tag{14-19}$$

Упражнение 14.7. Покажите, что ${}^\vee\left(f^\vee\right) = f = \left({}^\vee f\right)^\vee$.

Равенства $\beta(fgu, w) = \beta(gu, f^\vee w) = \beta(u, g^\vee f^\vee w)$ и $\beta(u, fgw) = \beta({}^\vee fu, gw) = \beta({}^\vee g {}^\vee fu, w)$ показывают, что левое и правое сопряжения являются по отношению к композиции операторов *антигомоморфизмами*, т. е. $(fg)^\vee = g^\vee f^\vee$ и ${}^\vee(fg) = {}^\vee g {}^\vee f$.

Упражнение 14.8. Покажите, что оператор $g : V \to V$ является изометрией невырожденной билинейной формы β, если и только если он обратим и ${}^\vee g = g^\vee = g^{-1}$.

Предложение 14.2
На векторном пространстве V с невырожденной билинейной формой β следующие условия на линейный оператор $f : V \to V$ эквивалентны друг другу:

$$1)\ f^{\vee\vee} = f \qquad 2)\ {}^{\vee\vee} f = f \qquad 3)\ {}^\vee f = f^\vee \qquad 4)\ \varkappa f = f \varkappa\,.$$

Доказательство. Беря в (3) правые сопряжённые, мы по упр. 14.7 получаем (1), а беря в (1) левые сопряжённые, получаем (3). Поэтому (1) ⇔ (3) и, аналогично, (2) ⇔ (3). Далее, (3) ⇔ $(b^*)^{-1} f^* \beta^* = \beta^{-1} f^* \beta \Leftrightarrow \beta\,(b^*)^{-1} f^* = f^* \beta\,(b^*)^{-1} \Leftrightarrow f \beta^{-1} \beta^* = \beta^{-1} \beta^* f \Leftrightarrow (4)$. □

14.2.5. Рефлексивные операторы. Мы будем называть операторы $f : V \to V$, удовлетворяющие условиям предл. 14.2, *рефлексивными* относительно формы β. Рефлексивные операторы образуют в $\mathrm{End}(V)$ подалгебру — централизатор канонического оператора $\varkappa_\beta$. Рефлексивный оператор f называется *самосопряжённым*, если $f^\vee = f$, и *антисамосопряжённым* — если $f^\vee = -f$. Всякий рефлексивный оператор является суммой самосопряжённого и антисамосопряжённого операторов: $f = (f + f^\vee)/2 + (f - f^\vee)/2$.

Предложение 14.3
Невырожденные формы α и β на пространстве V тогда и только тогда имеют равные канонические операторы $\varkappa_\alpha = \varkappa_\beta$, когда $\alpha = \beta f$ для некоторого самосопряжённого относительно обеих форм невырожденного линейного оператора[1] $f : V \to V$.

Доказательство. Если канонические операторы совпадают $\beta^{-1}\beta^* = \alpha^{-1}\alpha^*$, то совпадают и двойственные к ним: $\beta\left(\beta^*\right)^{-1} = \alpha\,(\alpha^*)^{-1}$. Тогда оператор $f = \beta^{-1}\alpha = \left(\beta^*\right)^{-1}\alpha^*$ перестановочен с $\varkappa_\alpha = \varkappa_\beta$, ибо $f\varkappa_\alpha = \beta^{-1}\alpha^* = \varkappa_\beta f$, и удовлетворяет равенству $\alpha = \beta f$. Наоборот, если $\alpha = \beta f$ и f самосопряжён относительно β, т. е. $f = f^\vee = \beta^{-1} f^* \beta$, то $\varkappa_\alpha = \alpha^{-1}\alpha^* = f^{-1}\beta^{-1} f^* \beta^* = f^{-1} f^\vee \beta^{-1}\beta^* = \beta^{-1}\beta^* = \varkappa_\beta$. □

[1] т. е. $\forall\, u, w \in V\ \alpha(u, w) = \beta(u, fw)$, см. n° 14.2.2 на стр. 218

14.2.6. Доказательство теор. 14.1. Если $\alpha = g^*\beta g$ для некоторого линейного изоморфизма $g : V \xrightarrow{\sim} V$, то $\varkappa_\alpha = \alpha^{-1}\alpha^* = g^{-1}\beta^{-1}\beta^* g = g^{-1}\varkappa_\beta g$. Наоборот, пусть α и β имеют подобные канонические операторы $\varkappa_\alpha = g^{-1}\varkappa_\beta g$. Заменяя β изоморфной корреляцией $g^*\beta g$, мы можем и будем считать, что $\varkappa_b = \varkappa_\alpha$. Тогда по предл. 14.3 $\alpha(u,w) = \beta(u, fw)$ для некоторого невырожденного линейного оператора $f : V \xrightarrow{\sim} V$, самосопряжённого относительно формы β. Согласно лем. 14.1, которую мы докажем ниже, можно подобрать такой многочлен $p(x) \in \Bbbk[x]$, что оператор $h = p(f)$ имеет $h^2 = f$. Оператор h тоже самосопряжён относительно β, поскольку $h^\vee = p(f)^\vee = p(f^\vee) = p(f) = h$, и переводит форму b в форму α, так как $\alpha(u,w) = \beta(u, fw) = \beta(u, h^2 w) = \beta(hu, hw)$. Это доказывает теор. 14.1.

Лемма 14.1
Над алгебраическим полем $\Bbbk$ характеристики нуль для любого оператора f с нулевым ядром, действующего на конечномерном векторном пространстве, существует такой многочлен $p(x) \in \Bbbk[x]$, что $p(f)^2 = f$.

Доказательство. Можно считать, что f является оператором умножения на t в прямой сумме фактор колец вида $\Bbbk[t]/(t-\lambda)^m$ с $\lambda \neq 0$. Обозначим через m_λ максимальный из показателей элементарных делителей оператора f вида $(t-\lambda)^m$ с данным $\lambda \in \operatorname{Spec}(f)$. Полагая $s = t - \lambda$ и беря первые m_λ членов формального биномиального разложения[1]

$$\sqrt{t} = \sqrt{\lambda + s} = \lambda^{1/2} \cdot \sqrt{1 + \lambda^{-1/2} s} = \lambda^{1/2} + \frac{1}{2}\, s - \frac{\lambda^{-1/2}}{8}\, s^2 + \frac{\lambda^{-1}}{16}\, s^3 - \cdots ,$$

где $\lambda^{1/2} \in \Bbbk$ — один из двух корней уравнения $x^2 = \lambda$, получаем в правой части такой многочлен $p_\lambda(t)$, что $p_\lambda^2(t) \equiv t \,(\operatorname{mod}(t-\lambda)^{m_\lambda})$. По китайской теореме об остатках из многочленов $p_\lambda(t)$ можно изготовить один многочлен $p(t)$, такой что сравнения

$$p^2 \equiv t \,(\operatorname{mod}(t-\lambda)^{m_\lambda})$$

будут выполнены одновременно для всех $\lambda \in \operatorname{Spec}(f)$. Тем самым, $p^2(f) = f$. □

Замечание 14.1. Над алгебраически незамкнутыми полями теор. 14.1 неверна. Так, над полем $\mathbb{Q}$ имеется огромное число неизоморфных невырожденных форм с тождественным каноническим оператором[2], и полное их перечисление выглядит необозримой задачей. В следующем параграфе мы опишем классы изоморфных симметричных билинейных форм над полем $\mathbb{R}$ и над простыми конечными полями $\mathbb{F}_p$, а также дадим более геометрическое доказательство тому, что над алгебраически замкнутым полем в каждой размерности имеется единственная с точностью до изоморфизма невырожденная симметричная билинейная форма. С кососимметричными формами, для которых $\varkappa = -\mathrm{Id}_V$, дела обстоят намного проще, и в n° 14.5 ниже мы покажем, что над любым полем $\Bbbk$ характеристики $\operatorname{char}\Bbbk \neq 2$ в каждой чётной размерности имеется единственная с точностью до изоморфизма невырожденная кососимметричная форма, а в нечётных размерностях невырожденных кососимметричных форм не существует.

[1] см. формулу (4-23) на стр. 59
[2] т. е. невырожденных *симметричных* билинейных форм

14.3. Ортогоналы и ортогональные проекции. Для подпространства U в векторном пространстве V с билинейной формой $\beta : V \times V \to \Bbbk$ обозначим через

$$ {}^{\perp}U = \{ v \in V \mid \forall u \in U \ \beta(v,u) = 0 \}, \tag{14-20} $$
$$ U^{\perp} = \{ v \in V \mid \forall u \in U \ \beta(u,v) = 0 \} \tag{14-21} $$

левый и *правый ортогоналы* к U. Вообще говоря, это *разные* подпространства в V.

Предложение 14.4
Если билинейная форма β на конечномерном пространстве V невырождена, то для всех подпространств $U \subset V$ выполняются равенства

$$ \dim {}^{\perp}U = \dim V - \dim U = \dim U^{\perp} \quad \text{и} \quad \left({}^{\perp}U\right)^{\perp} = U = {}^{\perp}\left(U^{\perp}\right). $$

Доказательство. Первые два равенства вытекают из того, что левый и правый ортогоналы (14-20) и (14-21) являются прообразами подпространства $\operatorname{Ann} U \subset V^*$ при изоморфизмах $\beta^* : V \xrightarrow{\sim} V^*$ и $\beta : V \xrightarrow{\sim} V^*$, задаваемых левой и правой корреляциями (??) формы β, и того, что $\dim \operatorname{Ann} U = \dim V - \dim U$ по предл. 7.2 на стр. 107. Вторые два равенства верны, поскольку U содержится в подпространствах $({}^{\perp}U)^{\perp}$ и ${}^{\perp}(U^{\perp})$, а их размерность по предыдущему равна $\dim U$. □

Предложение 14.5
Если ограничение формы β на конечномерное подпространство $U \subset V$ невырождено, то $V = U^{\perp} \oplus U$ и для каждого вектора $v \in V$ его проекция ${}_Uv$ на U вдоль $U^{\perp}$ однозначно определяется тем, что $\forall u \in U \quad \beta(u,v) = \beta(u, v_U)$. Она вычисляется в терминах любой пары двойственных относительно формы β базисов пространства U по формуле

$$ v_U = \sum_i \beta\left({}^{\vee}u_i, v\right) \cdot u_i . $$

Симметричным образом, имеется прямое разложение $V = U \oplus {}^{\perp}U$ в котором проекция ${}_Uv$ вектора $v \in V$ на U вдоль ${}^{\perp}U$ однозначно определяются тем, что

$$ \forall u \in U \quad \beta(v,u) = \beta({}_Uv, u), $$

и вычисляется в терминах любой пары двойственных относительно формы β базисов пространства U по формуле ${}_Uv = \sum \beta\left(v, u_i^{\vee}\right) \cdot u_i$.

Доказательство. Коль скоро ограничение формы β на U невырождено, для любого $v \in V$ линейная форма $\beta(v) : u \mapsto \beta(u,v)$ на подпространстве U имеет вид скалярного умножения справа на некоторый вектор $v_U \in U$, который однозначно определяется по v. Тем самым, $\forall u \in U$ выполняется равенство $\beta(u,v) = \beta(u, v_U)$, равносильное равенству $\beta(u, v - v_U) = 0$, и любой вектор $v \in V$ имеет единственное разложение

$$ v = (v - v_U) + v_U , \quad \text{где} \quad v_U \in U \quad \text{и} \quad v - v_U \in U^{\perp}. $$

Стало быть, $V = U^{\perp} \oplus U$. Поскольку $\beta({}^{\vee}u_i, v) = \beta({}^{\vee}u_i, v_U)$, разложение (14-12) имеет для вектора v_U вид $v_U = \sum \beta\left({}^{\vee}u_i, v_U\right) \cdot u_i = \sum \beta\left({}^{\vee}u_i, v\right) \cdot u_i$. Доказательства для левого ортогонала полностью симметричны. □

Упражнение 14.9. В условиях предл. 14.5 убедитесь, что отображения $V \twoheadrightarrow U$, заданные правилами $v \mapsto {}_U v$ и $v \mapsto v_U$, а также отображения $V \twoheadrightarrow {}^\perp U$ и $V \twoheadrightarrow U^\perp$, заданные правилами $v \mapsto v - {}_U v$ и $v \mapsto v - v_U$, линейны и сюрьективны (здесь и далее ${}_U v$ и v_U означают проекции вектора v на U вдоль ${}^\perp U$ и $U^\perp$ соответственно).

Следствие 14.1
Если и сама билинейная форма β на конечномерном пространстве V и её ограничение на подпространство $U \subset V$ оба невырождены, то и ограничения формы β на левый и на правый ортогоналы ${}^\perp U$ и $U^\perp$ к подпространству U также невырождены, а проекции

$$v_{{}^\perp U} \overset{\text{def}}{=} v - v_U \quad \text{и} \quad {}_{U^\perp}v \overset{\text{def}}{=} v - {}_U v$$

произвольного вектора $v \in V$ на ${}^\perp U$ и на $U^\perp$ вдоль U в прямых разложениях

$$U \oplus {}^\perp U = V = U^\perp \oplus U$$

однозначно определяются свойствами

$$\forall w \in {}^\perp U \; \beta(w, v) = \beta(w, v_{{}^\perp U}) \quad \text{и} \quad \forall w \in U^\perp \; \beta(v, w) = \beta({}_{U^\perp}v, w).$$

Доказательство. Для любого вектора $w \in U^\perp$ найдётся вектор $v \in V$ с $\beta(v, w) \neq 0$. Раскладывая его как $v = {}_U v + {}_{U^\perp}v$, где ${}_U v \in U$, ${}_{U^\perp}v = v - {}_U v \in U^\perp$, и пользуясь равенством $\beta({}_U v, w) = 0$, заключаем, что $\beta({}_{U^\perp}v, w) = \beta(v, w) \neq 0$. Стало быть, ограничение формы β на $U^\perp$ невырождено. То же вычисление показывает, что $\beta(v, w) = \beta({}_{U^\perp}v, w)$ для всех $w \in U^\perp$, откуда по предл. 14.5, применённой к подпространству $U^\perp$ в качестве U, мы заключаем, что ${}_{U^\perp}v$ является проекцией v на $U^\perp$ вдоль ${}^\perp\!\left(U^\perp\right) = U$ в прямом разложении $V = {}^\perp\!\left(U^\perp\right) \oplus U^\perp = U \oplus U^\perp$. Утверждения про левый ортогонал проверяются симметричным образом. □

Следствие 14.2
В условиях предыдущего сл. 14.1 ограничение на подпространство ${}^\perp U \subset V$ проекции пространства V на $U^\perp$ вдоль U и ограничение на подпространство $U^\perp \subset V$ проекции пространства V на ${}^\perp U$ вдоль U являются взаимно обратными изометрическими изоморфизмами между левым и правым ортогоналами к U. Эти изоморфизмы переводят друг в друга проекции $v_{{}^\perp U}$ и ${}_{U^\perp}v$ любого вектора $v \in V$ на ${}^\perp U$ и на $U^\perp$ вдоль U.

Доказательство. Линейный оператор $U^\perp \to {}^\perp U$, заданный правилом $w \mapsto w_{{}^\perp U} = w - w_U$, изометричен, т. к. для любых двух векторов $w', w'' \in U^\perp$

$$\beta(w' - w'_U, w'' - w''_U) = \beta(w', w'') - \beta(w', w''_U) + \beta(w'_U, w''_U) = \beta(w', w'')$$

в силу равенств $\beta(w'_U, w'') = 0$ и $\beta(w', w''_U) = \beta(w'_U, w''_U)$, первое из которых выполняется, поскольку $w'_U \in U$, а $w'' \in U^\perp$, а второе — поскольку $\beta(w', u) = \beta(w'_U, u)$ для всех u из U, включая $u = w''_U$. Изометричность оператора ${}^\perp U \xrightarrow{\sim} U^\perp$ устанавливается аналогично. Поскольку обе проекции $v \mapsto {}_U v$ и $v \mapsto v_U$ тождественно действуют на U, для любого вектора $v \in V$ выполняются равенства

$$\begin{aligned}
\left({}_{U^\perp}v\right)_{{}^\perp U} &= \left(v - {}_U v\right) - \left(v - {}_U v\right)_U = v - {}_U v - v_U + {}_U v = v - v_U = v_{{}^\perp U}, \\
{}_{U^\perp}\!\left(v_{{}^\perp U}\right) &= \left(v - v_U\right) - {}_U\!\left(v - v_U\right) = v - v_U - {}_U v + v_U = v - {}_U v = {}_{U^\perp}v,
\end{aligned}$$

из которых вытекают все остальные утверждения доказываемого следствия. □

14.4. (Косо)симметричные формы. Билинейная форма β на пространстве V называется *симметричной*, если $\forall\, v, w \in V\ \beta(v,w) = \beta(w,v)$, т. е. $\varkappa_\beta = \mathrm{Id}_V$ и $\beta^* = \beta$. Форма β называется *кососимметричной*, если $\forall\, v, w \in V\ \beta(v,w) = -\beta(w,v)$, т. е. $\varkappa_\beta = -\mathrm{Id}_V$ и $\beta^* = -\beta$.

Упражнение 14.10. Покажите, что если $\forall\, v \in V\ \beta(v,v) = 0$, то форма β кососимметрична, а при $\mathrm{char}(\Bbbk) \neq 2$ верно и обратное.

На языке матриц (косо) симметричность формы означает (косо) симметричность её матрицы Грама в каком-нибудь (а значит, и в любом) базисе. Произвольная билинейная форма β однозначно представляется в виде суммы симметричной и кососимметричной:

$$\beta(v,w) = \beta_+(v,w) + \beta_-(v,w), \quad \text{где}$$
$$\beta_+(v,w) = (\beta(v,w) + \beta(w,v))/2, \quad \beta_-(v,w) = (\beta(v,w) - \beta(w,v))/2,$$

т. е. пространство билинейных форм на V является прямой суммой подпространств симметричных и кососимметричных форм или, эквивалентно,

$$\mathrm{Hom}(V, V^*) = \mathrm{Hom}_+(V, V^*) \oplus \mathrm{Hom}_-(V, V^*)$$

является прямой суммой собственных подпространств, отвечающих собственным числам $+1$ и -1 инволютивного оператора дуализации $* : \beta \to \beta^*$.

Упражнение 14.11. Вычислите $\dim \mathrm{Hom}_\pm(V, V^*)$ при $\dim V = n$.

14.4.1. Ядро (косо) симметричной формы. Левое и правое ядра (косо) симметричной формы β совпадают друг с другом. Это подпространство называется просто *ядром* формы β и обозначается $\ker\beta = {}^\perp V = V^\perp = \{w \in V \mid \forall\, v \in V\ \beta(w,v) = \pm\beta(v,w) = 0\}$.

Предложение 14.6
Ограничение (косо) симметричной формы β на любое дополнительное к её ядру подпространство $U \subset V$ невырождено.

Доказательство. Пусть $U \subset V$ таково, что $V = \ker\beta \oplus U$. Если $w \in U$ удовлетворяет для всех $u \in U$ соотношению $\beta(w,u) = 0$, то записывая произвольный вектор $v \in V$ в виде $v = e + u$ с $e \in \ker\beta$, $u \in U$ мы получим $\beta(w,v) = \beta(w,e) + \beta(w,u) = 0$, откуда $w \in U \cap \ker\beta^* = U \cap \ker\beta = 0$. □

Предостережение 14.1. Для несимметричной билинейной формы предл. 14.6, вообще говоря, неверно. А именно, рассуждение из доказательства предл. 14.6 показывает, что вектор w, лежащий в дополнительном к $\ker\beta = V^\perp$ подпространстве U ортогонален этому подпространству *слева*, если и только если он ортогонален слева всему V, т. е. лежит в ${}^\perp V = \ker\beta^*$. Иными словами, $V = U \oplus V^\perp \Rightarrow {}^\perp U \cap U = {}^\perp V \cap U$.

Упражнение 14.12. Приведите пример билинейной формы $\beta : V \to V^*$ и такого подпространства $U \subset V$, что $V = U \oplus \ker\beta$ и $U \cap \ker\beta^* \neq 0$.

14.4.2. Сопряжение операторов. Поскольку канонический оператор $\varkappa = \pm\mathrm{Id}_V$ невырожденной (косо) симметричной формы лежит в центре алгебры $\mathrm{End}\, V$, все операторы $f : V \to V$ рефлексивны. В частности, левый и правый сопряжённые к любому оператору f совпадают друг с другом: $f^\vee = \beta^{-1} f^* \beta = (\beta^*)^{-1} f^* \beta^* = {}^\vee f$ и определяются эквивалентными друг другу соотношениями $\beta(fu, w) = \beta(u, f^\vee w)$ и $\beta(f^\vee u, w) = \beta(u, fw)$, а дважды сопряжённый оператор совпадает с исходным: $f^{\vee\vee} = f$. Самосопряжённые и антисамосопряжённые операторы определяются, соответственно, равенствами

$$\beta(fu, w) = \beta(u, fw) \quad \text{и} \quad \beta(fu, w) = -\beta(u, fw) \qquad (\forall\, u, w \in V)$$

и являются собственными векторами с собственными значениями ± 1 инволюции

$$\vee : \mathrm{End}(V) \to \mathrm{End}(V)\,, \quad f \mapsto f^\vee$$

сопряжения относительно формы β. Согласно прим. 11.1 на стр. 169 пространство $\mathrm{End}(V)$ является прямой суммой собственных ± 1-подпространств этой инволюции, т. е. каждый оператор $f : V \to V$ однозначно представляется в виде суммы самосопряжённого и антисамосопряжённого: $f = (f + f^\vee)/2 + (f - f^\vee)/2$.

14.4.3. Ортогоналы и проекции. Если форма β на V (косо) симметрична, то левый ортогонал к любому подпространству $U \subset V$ совпадает с правым:

$${}^\perp U = U^\perp = \{ w \in V \mid \beta(w, u) = \pm\beta(u, w) = 0 \ \ \forall u \in U \}\,.$$

Если ограничение (косо) симметричной формы β на подпространство $U \subset V$ невырождено, то по сл. 14.1 $V = U \oplus U^\perp$. Подпространство $U^\perp$ называется в этом случае *ортогональным дополнением* к подпространству U. Проекция $v_U = {}_U v$ вектора $v \in V$ на U вдоль $U^\perp$ называется *ортогональной проекцией* на U и однозначно определяется тем, что

$$\forall\, u \in U \ \beta(u, v) = \beta(u, v_U)\,.$$

Если форма β невырождена на всём V, то согласно предл. 14.5 $\dim U^\perp = \dim V - \dim U$ и $U^{\perp\perp} = U$ для всех подпространств $U \subset V$. Если при этом ограничение формы β на подпространство $U \subset V$ также невырождено, то по сл. 14.1 невырождено и ограничение формы на $U^\perp$. Отметим, однако, что ограничение невырожденной (косо) симметричной формы на подпространство вполне может оказаться вырожденным и даже тождественно нулевым.

14.4.4. Изотропные подпространства. Подпространства $U \subset V$, на которые форма β ограничивается в тождественно нулевую форму, называются *изотропными подпространствами* формы β. Например, любое одномерное подпространство изотропно для любой кососимметричной формы (если $\mathrm{char}\, \Bbbk \neq 2$).

Предложение 14.7
Размерность изотропного подпространства невырожденной билинейной формы на пространстве V не может превосходить $\dim V/2$.

Доказательство. Изотропность подпространства $U \subset V$ означает, что корреляция $V \xrightarrow{\sim} V^*$ отображает U внутрь $\mathrm{Ann}\, U \subset V^*$. Поскольку корреляция невырожденной формы инъективна, $\dim U \leqslant \dim \mathrm{Ann}\, U = \dim V - \dim U$, откуда $2 \dim U \leqslant \dim V$. □

Всюду далее мы предполагаем, что $\mathrm{char}(\Bbbk) \neq 2$.

14.5. Симплектические пространства. Прямая сумма $W = U^* \oplus U$, наделённая кососимметричной билинейной формой

$$\omega\big((\xi_1, u_1), (\xi_2, u_2) \big) = \langle\, \xi_1 \,,\, u_2 \,\rangle - \langle\, \xi_2 \,,\, u_1 \,\rangle \;, \tag{14-22}$$

называется *симплектическим пространством* и обозначается Ω_{2n}, где $n = \dim U$. В базисе, составленном из векторов $e_1^*, e_2^*, \dots , e_n^*, e_1, e_2, \dots , e_n$ каких-нибудь двойственных друг другу базисов в U^* и в U, матрица Грама формы ω имеет вид

$$J = \begin{pmatrix} 0 & E \\ -E & 0 \end{pmatrix} . \tag{14-23}$$

Матрица J называется *симплектической единицей* и удовлетворяет соотношениям $J^2 = -E$, $\det J = 1$. В частности, форма ω невырождена. Базис, в котором матрица Грама невырожденной кососимметричной формы имеет вид (14-23), называется *симплектическим базисом* этой формы.

Упражнение 14.13. Убедитесь, что прямая ортогональная сумма $\Omega_{2m} \oplus \Omega_{2k}$ изометрически изоморфна $\Omega_{2(m+k)}$.

Теорема 14.2
Над произвольным полем $\Bbbk$ любое пространство V с невырожденной кососимметричной формой ω изометрически изоморфно симплектическому пространству. В частности, размерность $\dim V$ чётна.

Доказательство. В качестве первого базисного вектора возьмём произвольный ненулевой вектор $e_1 \in V$. Поскольку ω невырождена, существует $w \in V$, такой что $\omega(e_1, w) = a \neq 0$. Положим $e_2 = w/a$. Матрица Грама ограничения ω на двумерное подпространство $U \subset V$, порождённое векторами e_1, e_2, равна

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} .$$

Тем самым, $\omega|_U$ невырождена, $V = U \oplus U^\perp$, ограничение $\omega|_{U^\perp}$ также невырождено, и мы можем воспользоваться индукцией по размерности. □

Упражнение 14.14. Убедитесь непосредственно, что определитель кососимметричной квадратной матрицы нечётного размера равен нулю.

14.5.1. Симплектическая группа $\mathrm{Sp}_{\boldsymbol{\omega}}(\boldsymbol{W})$. Изометрические линейные преобразования $F : W \to W$ невырожденной кососимметричной формы ω на $2n$-мерном пространстве W называются *симплектическими* и образуют группу $\mathrm{Sp}_\omega(W)$, называемую *симплектической группой* формы ω. Сопоставление оператору его матрицы в симплектическом базисе изоморфно отображает группу $\mathrm{Sp}_\omega(W)$ на *группу симплектических матриц*

$$\mathrm{Sp}_{2n}(\Bbbk) = \{ F \in \mathrm{Mat}_{2n}(\Bbbk) \mid F^t \cdot J \cdot F = J \} .$$

Если в соответствии с разложением $W = U^* \oplus U$, заданным выбором симплектического базиса, записать матрицу оператора F в блочном виде

$$F = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$$

с $A : U^* \to U^*$, $B : U \to U^*$, $C : U^* \to U$, $D : U \to U$, то условие $F^t \cdot J \cdot F = J$ запишется как

$$\begin{pmatrix} A^t & C^t \\ B^t & D^t \end{pmatrix} \begin{pmatrix} 0 & E \\ -E & 0 \end{pmatrix} \begin{pmatrix} A & B \\ C & D \end{pmatrix} = \begin{pmatrix} 0 & E \\ -E & 0 \end{pmatrix}$$

Упражнение 14.15. Проверьте, что это равенство равносильно соотношениям:

$$C^t A = A^t C\,, \quad D^t B = B^t D\,, \quad E + C^t B = A^t D\,.$$

Из этих равенств видно, что полная линейная группа $\mathrm{GL}(U)$ гомоморфно вкладывается в симплектическую группу $\mathrm{Sp}_\omega(U^* \oplus U)$ по правилу

$$\mathrm{GL}(U) \ni G \mapsto \begin{pmatrix} \left(G^t\right)^{-1} & 0 \\ 0 & G \end{pmatrix} \in \mathrm{Sp}_\omega(U^* \oplus U)\,.$$

14.5.2. Лагранжевы и симплектические подпространства. Изотропные подпространства максимальной размерности n в $2n$-мерном симплектическом пространстве V с формой ω называются *лагранжевыми*.

Упражнение 14.16. Покажите, что каждое изотропное подпространство симплектической формы содержится в некотором лагранжевом, а каждое лагранжево подпространство совпадает со своим ортогоналом.

Предложение 14.8
Каждое изотропное подпространство U невырожденной кососимметричной формы ω содержится в некотором симплектическом подпространстве W размерности $\dim W = 2\dim U$, и любой базис в U дополняется до симплектического базиса в W.

Доказательство. Выберем в U базис $u_1, u_2, \dots, u_m$, дополним его до базиса в V и рассмотрим двойственный к нему относительно ω базис. Первые m векторов $u_1^\vee, u_2^\vee, \dots, u_m^\vee$ двойственного базиса удовлетворяют равенствам

$$\omega\left(u_i, u_j^\vee\right) = \begin{cases} 1 & \text{при } i = j \\ 0 & \text{при } i \neq j\,, \end{cases} \tag{14-24}$$

которые не нарушаются при добавлении к любому из векторов $u_j^\vee$ любой линейной комбинации векторов u_i. Заменяя каждый вектор $u_j^\vee$ вектором

$$w_j = u_j^\vee - \sum_{\nu<j} \omega\left(u_j^\vee, u_\nu^\vee\right) \cdot u_\nu\,, \tag{14-25}$$

получаем набор векторов $w_1, w_2, \dots, w_m$, также удовлетворяющий равенствам (14-24), но порождающий изотропное подпространство, поскольку для всех i, j

$$\omega(w_i, w_j) = \omega(u_i^\vee, u_j^\vee) - \omega(u_j^\vee, u_i^\vee) \cdot \omega(u_i^\vee, u_i) = 0\,.$$

Таким образом, векторы u_i и w_j с $1 \leqslant i, j \leqslant m$ составляют симплектический базис своей линейной оболочки. □

Следствие 14.3 (из доказательства предл. 14.8)
Для каждого лагранжева подпространства $L \subset V$ имеется дополнительное лагранжево подпространство $L' \subset V$, такое что $V = L \oplus L'$. Каждый базис e подпространства L однозначно достраивается некоторым базисом e' подпространства L' до симплектического базиса пространства V. При фиксированном L' все дополнительные к L лагранжевы подпространства L'' биективно соответствуют антисамосопряжённым[1] относительно формы ω линейным операторам $f : L \to L'$.

Доказательство. Беря в предыдущем доказательстве $U = L$ и $u = e$ получаем разложение $W = V = L \oplus L'$, в котором лагранжево подпространство L' натянуто на векторы w_j из формулы (14-25). Корреляция $\omega : v \mapsto \omega(*, v)$ задаёт изоморфизм подпространства L' с пространством L^* и базис w в L', дополняющий базис e пространства L до симплектического базиса в V, однозначно описывается как прообраз двойственного к e базиса e^* в L^* при этом изоморфизме. Всякое дополнительное к L подпространство $L'' \subset L \oplus L'$ биективно проектируется на L вдоль L' , т. е. для любого $u \in L$ существует единственный вектор $f(u) \in L'$, такой что $u + f(u) \in L''$. Правило $u \mapsto f(u)$ задаёт линейное отображение $f : L \to L'$, графиком которого является L''. Изотропность подпространства L'' равносильна антисамомопряжённости оператора f, поскольку $\omega\,(u_1 + f(u_1), u_2 + f(u_2)) = \omega\,(u_1, f(u_2)) + \omega\,\big(f(u_1), u_2\big)$ в силу лагранжевости подпространств $L \ni u_1, u_2$ и $L' \ni f(u_1), f(u_2)$. □

Упражнение 14.17. Покажите, что симплектическая группа $\mathrm{Sp}_\omega(V)$ транзитивно действует на множестве всех симплектических подпространств $W \subset V$ каждой фиксированной размерности $\dim W = 2d$ и на множестве всех изотропных подпространств $U \subset V$ каждой фиксированной размерности[2] $\dim U = d$.

14.5.3. Пфаффиан. Рассмотрим имеющие $i < j$ элементы a_{ij} кососимметричной матрицы $A = (a_{ij})$ размера $(2n)\times(2n)$ как независимые переменные и обозначим через $\mathbb{Z}[a_{ij}]$ кольцо многочленов от этих переменных с целыми коэффициентами. В этом разделе мы покажем, что существует единственный многочлен $\mathrm{Pf}(A) \in \mathbb{Z}[a_{ij}]$, такой что

$$\mathrm{Pf}(A)^2 = \det(A) \quad \text{и} \quad \mathrm{Pf}(J') = 1\,,$$

где J' — блочно диагональная матрица, составленная из 2×2-блоков $\boxed{\begin{matrix} 0 & 1 \\ -1 & 0 \end{matrix}}$. Этот многочлен называется *пфаффианом* кососимметричной матрицы A и явно выражается через матричные элементы по формуле

$$\mathrm{Pf}(A) = \sum_{\substack{\{i_1,j_1\}\sqcup\dots\sqcup\{i_n,j_n\}= \\ =\{1,2,\dots,2n\}}} \mathrm{sgn}\big(i_1 j_1 i_2 j_2 \dots i_n j_n\big) \cdot a_{i_1 j_1} a_{i_2 j_2} \,\cdots\, a_{i_n j_n}\,, \tag{14-26}$$

где суммирование происходит по всем разбиениям множества $\{1, 2, \dots, 2n\}$ в объединение n непересекающихся пар $\{i_\nu, j_\nu\}$, порядок которых не существенен, а sgn означает знак соответствующей перестановки[3].

Упражнение 14.18. Проверьте, что $\mathrm{Pf}(A)^2 = \det(A)$, для кососимметричных матриц A размеров 2×2 и 4×4.

[1] т. е. таким операторам f, что $\forall\, u, w\ \omega(fu, w) + \omega(u, fw) = 0$

[2] в обоих случаях $1 \leqslant d \leqslant \dim V/2$

[3] убедитесь, что правая часть не меняется ни при перестановках пар друг с другом, ни при перестановке элементов в каждой паре

Чтобы установить существование пфаффиана, проинтерпретируем A как матрицу Грама невырожденной кососимметричной формы на координатном векторном пространстве K^{2n} над полем $K = \mathbb{Q}(a_{ij})$ рациональных функций от переменных a_{ij} с коэффициентами в $\mathbb{Q}$. По теор. 14.2 эта форма обладает симплектическим базисом. Перегруппировывая его векторы по парам $e_1^*, e_1, e_2^*, e_2, \dots, e_n^*, e_n$, получаем базис с матрицей Грама J'. Тем самым, $A = C \cdot J' \cdot C^t$ для некоторой матрицы $C \in \mathrm{GL}_{2n}(K)$. Поскольку $\det J' = 1$,

$$\det(A) = \det(C)^2 .$$

Дабы удостовериться, что $\det C = \mathrm{Pf}(A) \in \mathbb{Z}[a_{ij}]$, введём для кососимметричной матрицы $B = \big(b_{ij}\big)$, элементы которой также рассматриваются как независимые переменные, вспомогательный однородный грассманов многочлен второй степени

$$\beta_B(\xi) = (\xi B) \wedge \xi^t = \sum_{ij} b_{ij} \xi_i \wedge \xi_j$$

от n переменных $\xi = (\xi_1, \xi_2, \dots, \xi_n)$ с коэффициентами в кольце $\mathbb{Z}[b_{ij}]$. Так как чётные мономы $\xi_i \wedge \xi_j$ перестановочны, $\beta_B^n = \beta_B \wedge \beta_B \wedge \dots \wedge \beta_B = n! \cdot \mathrm{Pf}(B) \cdot \xi_1 \wedge \xi_2 \wedge \dots \wedge \xi_{2n}$, где

$$\mathrm{Pf}(B) = \sum_{\substack{\{i_1, j_1\} \sqcup \dots \sqcup \{i_n, j_n\} = \\ = \{1, 2, \dots, 2n\}}} \mathrm{sgn}\big(i_1 j_1 i_2 j_2 \dots i_n j_n\big) \cdot b_{i_1 j_1} b_{i_2 j_2} \cdots b_{i_n j_n} \in \mathbb{Z}[b_{ij}]$$

тот же, что и формуле (14-26). При линейной замене координат ξ по формуле $\xi = \eta\, C$, где $C \in \mathrm{GL}_{2n}(K)$ — интересующая нас матрица, грассманов многочлен $\beta_B(\xi)$ переписывается с коэффициентами в кольце $K[b_{ij}]$ как

$$\beta_B(\xi) = (\xi\, B) \wedge \xi^t = (\eta\, CB) \wedge (\eta\, C)^t = (\eta\, CBC^t) \wedge \eta^t = \beta_{CBC^t}(\eta)$$

а его n-тая внешняя степень — как $\beta_{CBC^t}(\eta)^n = n! \cdot \mathrm{Pf}(CBC^t) \cdot \eta_1 \wedge \eta_2 \wedge \dots \wedge \eta_{2n}$. Поскольку $\xi_1 \wedge \xi_2 \wedge \dots \wedge \xi_{2n} = \det C \cdot \eta_1 \wedge \eta_2 \wedge \dots \wedge \eta_{2n}$, многочлены $\mathrm{Pf}(B) \in \mathbb{Z}[b_{ij}]$ и $\mathrm{Pf}(CBC^t) \in K[b_{ij}]$ связаны в кольце $K[b_{ij}] \supset \mathbb{Z}[b_{ij}]$ соотношением $\mathrm{Pf}(CBC^t) = \mathrm{Pf}(B) \cdot \det C$. Полагая в нём $B = J'$, получаем равенство $\mathrm{Pf}(A) = \det C$ в поле $K = \mathbb{Q}(a_{ij})$. Поэтому $\det(C) \in \mathbb{Z}[a_{ij}]$ и $\det(A) = \det^2(C) = \mathrm{Pf}^2(A)$, что доказывает существование пфаффина и формулу (14-26). Единственность пфаффиана вытекает из того, что многочлен

$$x^2 - \det A = \big(x - \mathrm{Pf}(A)\big)\big(x + \mathrm{Pf}(A)\big) \in \mathbb{Z}[a_{ij}][x]$$

имеет в целостном кольце $\mathbb{Z}[a_{ij}]$ ровно два корня $x = \pm \mathrm{Pf}(A)$, а требование $\mathrm{Pf}(J') = 1$ однозначно фиксирует знак.

Упр. 14.2. Равенство форм $\beta_1(u,w) = \beta_2(fu,fw)$ на языке корреляций означает

$$\langle\, \beta_1 w\,,\, u\,\rangle = \langle\, \beta_2 f w\,,\, fu\,\rangle = \langle\, f^*\beta_2 f w\,,\, u\,\rangle\ .$$

Упр. 14.4. Всякая корреляция *единственным* образом раскладывается в сумму симметричной и кососимметричной: $\beta = (\beta+\beta^*)/2 + (\beta-\beta^*)/2$. Оба слагаемых лежат в пучке $\mathcal{C}_\beta$. Ответ на второй вопрос — да, например

$$B = \begin{pmatrix} 1 & 0 & 0\\ 0 & 0 & 1\\ 0 & -1 & 0\end{pmatrix}$$

Упр. 14.7. ${}^\vee\!\left(f^\vee\right) = \left(\beta^*\right)^{-1}\left((\beta)^{-1}f^*\beta\right)^*\beta^* = f^{**} = f\ .$

Упр. 14.8. Условие $\forall\, u,w \in V\ \beta(u,w) = \beta(gu,gw)$ равносильно равенству $g^*\beta g = \beta$, которое влечёт $\det g \neq 0$ и эквивалентно равенству $\beta^{-1}g^*\beta = g^{-1}$. Переходя к двойственным операторам, получаем равенство $\gamma^*\beta^*g = \beta^*$, равносильное равенству $\left(\beta^*\right)^{-1}g^*\beta^* = g^{-1}$.

Упр. 14.10. Первое следует из равенства $\beta(v+w,v+w) = \beta(v,v)+\beta(w,w)+\beta(v,w)+\beta(w,v)$, второе — из равенства $\beta(v,v) = -\beta(v,v)$.

Упр. 14.11. Это размерности пространств симметричных и кососимметричных матриц размера $n\times n$, равные $n(n\pm 1)/2$.

Упр. 14.14. $\det\omega = \det(-\omega^t) = (-1)^{\dim V}\det\omega^t = (-1)^{\dim V}\det\omega$.

§15. Пространства со скалярным произведением

Всюду в этом параграфе мы по умолчанию предполагаем, что характеристика основного поля $\Bbbk$ отлична от 2.

15.1. Алгебра SV^*: неформальное описание. Зафиксируем в векторном пространстве V над полем $\Bbbk$ некоторый базис $e_1, e_2, \dots, e_n$ и будем обозначать через

$$x = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} \quad \text{и} \quad x^t = (x_1, x_2, \dots, x_n)$$

столбцы и строки координат векторов $v \in V$ в этом базисе. Каждый многочлен от координат $f \in \Bbbk[x_1, x_2, \dots, x_n]$ задаёт на пространстве V функцию, значение которой на векторе $a = \sum \alpha_i e_i$ равно результату подстановки $x_i = \alpha_i$, $1 \leqslant i \leqslant n$, в многочлен f:

$$f : V \to \Bbbk, \quad a = \sum \alpha_i e_i \mapsto f(a) = f(\alpha_1, \alpha_2, \dots, \alpha_n). \tag{15-1}$$

Упражнение 15.1. Покажите, что сопоставление многочлену f функции $a \mapsto f(a)$ является гомоморфизмом алгебры многочленов $\Bbbk[x_1, x_2, \dots, x_n]$ в алгебру функций $V \to \Bbbk$, что его образ не зависит от выбора базиса и что этот гомоморфизм инъективен[1] тогда и только тогда, когда поле $\Bbbk$ бесконечно.

У этой конструкции есть очевидное неудобство: она зависит от выбора координат в V. Избавиться от этого неудобства можно записывая многочлены в виде линейных комбинаций произведений ковекторов $\xi \in V^*$ и не выражая последние через какой-либо конкретный базис. Так, пространство всех однородных многочленов степени d вместе с нулевым многочленом может быть описано как линейная оболочка всевозможных произведений $\xi_1 \xi_2 \dots \xi_d$ наборов произвольных ковекторов $\xi_\nu \in V^*$. Раскладывая эти ковекторы по базису $x_1, x_2, \dots, x_n \in V^*$ в виде $\xi_i = \sum a_{ij} x_j$, мы можем записать каждое такое произведение в виде многочлена от x_i. Однако разные линейные комбинации произведений ковекторов могут при этом записываться одинаковыми многочленами: например, в силу дистрибутивности произведения многочленов мы заведомо имеем для любых $\xi, \eta, \varphi, \psi \in V^*$ и $a, b, c, d \in \Bbbk$ равенства вида $(a\,\xi + b\,\eta)(\varphi + d\,\psi) = ab\,\xi\varphi + ad\,\xi\psi + bc\,\eta\varphi + bd\,\eta\psi$.

Таким образом, мы имеем две возможности для записи однородных многочленов степени d на пространстве V — однозначную, но привязанную к выбору конкретного базиса $x_1, x_2, \dots, x_n \in V^*$ запись в виде линейной комбинации мономов $x_1^{m_1} x_2^{m_2} \cdots x_n^{m_n}$ с $\sum m_i = d$, и неоднозначную запись в виде линейной комбинации произведений произвольных ковекторов $\xi_1 \xi_2 \dots \xi_d$, которая не зависит от выбора базиса. В терминах второй записи интерпретация многочленов как функций на V тоже не зависит от выбора базиса: каждому произведению $\xi_1 \xi_2 \dots \xi_d$ сопоставляется функция

$$\xi_1 \xi_2 \dots \xi_d : v \mapsto \prod_{\alpha=1}^{d} \langle\, \xi_\alpha\, ,\, v \,\rangle \tag{15-2}$$

[1] т. е. разным многочленам отвечают разные функции на V

и это сопоставление по линейности продолжается на линейные комбинации произведений ковекторов. Отметим, что корректность этого правила, т. е. независимость значения $f(v)$ от способа представления f в виде линейной комбинации произведений ковекторов, вытекает из того, что оно является лишь иной записью заведомо корректного правила (15-1). С другой стороны, сопоставление многочлену функции по формуле (15-2) делает второе утверждение из упр. 15.1 и многие другие подобные утверждения самоочевидными, а также упрощает некоторые формулы.

Чтобы подчеркнуть независимость алгебры многочленов на V от выбора координат, мы всюду далее будем обозначать пространство однородных многочленов степени d на пространстве V через S^dV^*, а всю алгебру многочленов на V — через

$$SV^* = \bigoplus_{d\geqslant 0} S^dV^*\,, \quad \text{где} \quad S^0V^* \stackrel{\text{def}}{=} \Bbbk \quad \text{и} \quad S^1V^* \stackrel{\text{def}}{=} V^*\,,$$

и называть эту алгебру *симметрической алгеброй*[1] пространства V^*. Фиксация в V^* базиса $x = (x_1, x_2, \dots, x_n)$ задаёт изоморфизм $\varphi_x : SV^* \xrightarrow{\sim} \Bbbk[x_1, x_2, \dots, x_n]$. При выборе другого базиса $y = x \cdot C$ композиция изоморфизмов

$$\varphi_x \circ \varphi_y^{-1} : \Bbbk[y_1, y_2, \dots, y_n] \xrightarrow{\sim} SV^* \xrightarrow{\sim} \Bbbk[x_1, x_2, \dots, x_n]$$

переводит многочлен $f(y) \in \Bbbk[y_1, y_2, \dots, y_n]$ в многочлен $f(xC) \in \Bbbk[x_1, x_2, \dots, x_n]$, т. е. представляет собою линейную замену координат в многочленах.

Ещё раз подчеркнём, что алгебра многочленов SV^* всегда бесконечна и бесконечномерна, даже если векторное пространство V является конечным множеством (когда основное поле $\Bbbk$ конечно). Но над бесконечным полем по упр. 15.1 различным элементам алгебры SV^* отвечают различные функции на V.

Упражнение 15.2. Покажите, что над полем характеристики нуль пространство S^dV^* линейно порождается чистыми d-тыми степенями ξ^d всевозможных линейных форм $\xi \in V^*$, и явно выразите многочлен $x_1^2x_2 + x_2^2x_3$ в виде линейной комбинации кубов линейных форм от x_1, x_2, x_3.

15.2. Симметричные билинейные и квадратичные формы. Однородные многочлены $q \in S^2V^*$ называются *квадратичными формами* на пространстве V. Если $\operatorname{char}(\Bbbk) \neq 2$, то в координатах квадратичную форму q удобно записывать в виде

$$q(x) = \sum_{i,j} x_i q_{ij} x_j = x^t \cdot Q \cdot x\,, \tag{15-3}$$

где суммирование происходит по всем парам индексов $1 \leqslant i, j \leqslant n$ и коэффициенты q_{ij} организованы в симметричную матрицу $Q = \left(q_{ij}\right)$ размера $n \times n$ так, что при $i \neq j$ величина $q_{ji} = q_{ij}$ равна *половине*[2] фактического коэффициента при x_ix_j, получающегося после приведения подобных слагаемых. Из такой записи видно, что квадратичная форма $q : V \to \Bbbk$, задаваемая многочленом (15-3), имеет вид $q(v) = \tilde{q}(v, v)$, где $\tilde{q} : V \times V \to \Bbbk$,

[1]формальное определение симметрической алгебры, не апеллирующее к координатам и пригодное для бесконечномерных пространств, мы дадим позже, когда будем заниматься тензорными произведениями

[2]над полем характеристики 2 многочлен x_1x_2 в таком виде не записывается

$\tilde{q}(x,y) = x^t \cdot Q \cdot y$, — *симметричная билинейная* форма с матрицей Грама Q. Эта форма называется *поляризацией* многочлена q. Если $\operatorname{char} \Bbbk \neq 2$, поляризация $\tilde{q}$ однозначно определяется квадратичным многочленом q по формулам

$$\tilde{q}(v,w) = \big(q(v+w) - q(v) - q(w)\big)/2 = \big(q(v+w) - q(v-w)\big)/4\,. \tag{15-4}$$

Упражнение 15.3. Проверьте это и покажите, что $\tilde{q}(x,y) = \frac{1}{2}\sum\limits_i y_i \frac{\partial q(x)}{\partial x_i}$.

Мы будем называть матрицу Q из представления (15-3) *матрицей Грама* квадратичного многочлена q. Поскольку ранг матрицы не меняется при её умножении на обратимую матрицу, а при замене базиса матрица Грама меняется по правилу $Q \mapsto C^tQC$ с обратимой матрицей C, ранг матрицы Грама не зависит от выбора базиса. Он называется *рангом квадратичной формы* q.

Теорема 15.1 (теорема Лагранжа)
Над любым полем $\Bbbk$ с $\operatorname{char} \Bbbk \neq 2$ для любой симметричной билинейной формы $\tilde{q}$ на пространстве V в V существует базис с диагональной матрица Грама.

Доказательство. Если $\dim V = 1$ или $\tilde{q}$ тождественно равна 0, то матрица Грама уже диагональна. Если $\tilde{q} \not\equiv 0$, то отвечающий форме $\tilde{q}$ квадратичный многочлен $q(v) = \tilde{q}(v,v)$ согласно (15-4) тоже не является тождественным нулём, и найдётся вектор $e \in V$, такой что $\tilde{q}(e,e) \neq 0$. Возьмем его в качестве первого вектора искомого базиса. Поскольку ограничение формы $\tilde{q}$ на одномерное пространство $\Bbbk \cdot e$ невырождено, V по предл. 14.5 распадается в прямую ортогональную сумму $(\Bbbk \cdot e) \oplus e^{\perp}$, где $e^{\perp} = \{\, v \in V \mid \tilde{q}(e,v) = 0 \,\}$. По индукции, в $e^{\perp}$ существует базис с диагональной матрицей Грама. Добавляя к нему e, получаем нужный базис в V. □

Следствие 15.1
Всякая квадратичная форма над любым полем $\Bbbk$ с $\operatorname{char} \Bbbk \neq 2$ линейной обратимой заменой переменных приводится к виду $\sum a_i x_i^2$.

Следствие 15.2
Над алгебраически замкнутым полем $\Bbbk$ характеристики $\operatorname{char}(\Bbbk) \neq 2$ две квадратичные формы тогда и только тогда переводятся одна в другую линейной обратимой заменой координат, когда их матрицы Грама имеют одинаковый ранг.

Доказательство. Над алгебраически замкнутым полем ненулевые диагональные элементы матрицы Грама преобразуются в единицы заменой базисных векторов по формуле $e_i \mapsto e_i/\sqrt{q(e_i)}$. Количества единиц и нулей на главной диагонали такой матрицы равны рангу формы и размерности её ядра и не зависят от выбора базиса. Поэтому любые две формы одинакового ранга обратимой линейной заменой координат приводятся к одинаковому виду $\sum x_i^2$. □

15.2.1. Определитель Грама. Над алгебраически незамкнутым полем отнормировать ортогональный базис до ортонормального, вообще говоря, невозможно. Простейшим инвариантом, доставляющим препятствие к этому, является определитель $\det Q_e$ матрицы Грама Q формы q в произвольном базисе e. При переходе к другому базису определитель Грама умножается на квадрат определителя матрицы перехода. Поэтому с точностью до умножения на ненулевой квадрат из поля $\Bbbk$ определитель Грама не зависит от выбора базиса. В частности, форма, определитель Грама которой не является квадратом, не имеет ортонормального базиса. Мы будем обозначать класс определителя Грама по модулю умножения на ненулевые квадраты через $\det q \in \Bbbk/\Bbbk^{*2}$ и писать $a \sim b$, если $a = \lambda^2 b$ для ненулевого $\lambda \in \Bbbk$. Квадратичная форма q называется *вырожденной*, если $\det q = 0$. Формы с $\det q \neq 0$ называются *невырожденными*.

Пример 15.1 (квадратичные формы от двух переменных)
По теореме Лагранжа ненулевая квадратичная форма от двух переменных

$$q(x) = a\,x_1^2 + 2\,b\,x_1 x_2 + c\,x_2^2 = (x_1, x_2)\begin{pmatrix} a & b \\ b & c \end{pmatrix}\begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$$

подходящей линейной заменой координат приводятся либо к виду αt^2 с $\alpha \neq 0$, либо к виду $\alpha t_1^2 + \beta\,t_2^2$, где $\alpha \neq 0$ и $\beta \neq 0$. В первом случае $ac - b^2 \sim \det q \sim \alpha \cdot 0 = 0$, форма q вырождена и пропорциональна полному квадрату линейной формы $t = t(x_1, x_2)$. Такая форма зануляется вдоль одномерного подпространства $\mathrm{Ann}(t) \subset V$ и отлична от нуля на всех остальных векторах. Во втором случае $ac - b^2 \sim \det q \sim \alpha\beta \neq 0$ и форма q невырождена. Если существует ненулевой вектор $v = (\vartheta_1, \vartheta_2)$, такой что $q(v) = \alpha\vartheta_1^2 + \beta\vartheta_2^2 = 0$, то $-\det q \sim -\alpha\beta \sim -\beta/\alpha = (\vartheta_1/\vartheta_2)^2$ является полным квадратом[1], и тогда

$$\alpha t_1^2 + \beta\,t_2^2 = \alpha\left(t_1 + \frac{\vartheta_1}{\vartheta_2}t_2\right)\left(t_1 - \frac{\vartheta_1}{\vartheta_2}t_2\right)$$

является произведением двух непропорциональных линейных форм. Такая форма тождественно зануляются на двух одномерных подпространствах и отлична от нуля на всех прочих векторах. Она называется *гиперболической*. Если же $-\det q$ не квадрат, то $q(v) \neq 0$ при $v \neq 0$. Такая форма называется *анизотропной*.

15.2.2. Изотропные и анизотропные подпространства. Подпространство $U \subset V$ называется *анизотропным* для квадратичной формы q, если $q(v) = \tilde{q}(v, v) \neq 0$ для любого ненулевого $v \in V$. Например, вещественное евклидово пространство является анизотропным по отношению к евклидовому скалярному произведению. В прим. 15.1 мы видели, что двумерное подпространство U анизотропно, если и только если $-\det\left(q|_U\right)$ не квадрат в $\Bbbk$. Над алгебраически замкнутым полем $\Bbbk$ анизотропных форм от $\geqslant 2$ переменных не бывает.

Подпространство $U \subset V$ называется *изотропным* для квадратичной формы q, если ограничение $q|_U \equiv 0$ или, что то же самое, $\tilde{q}(u_1, u_2) = 0\ \forall\ u_1, u_2 \in U$. Ненулевые векторы v, порождающие одномерные изотропные подпространства, называются *изотропными векторами*. Для таких векторов $q(v) = \tilde{q}(v, v) = 0$.

Согласно прим. 15.1, ненулевая квадратичная форма от двух переменных вырождена тогда и только тогда, когда у неё имеется ровно одно одномерное изотропное подпространство, а невырожденная квадратичная форма от двух переменных либо анизотропна, либо имеет ровно два различных одномерных изотропных подпространства.

Предложение 15.1
Размерность изотропного подпространства U в пространстве V с невырожденной симметричной билинейной формой β не превышает $\dim V/2$.

[1] отметим, что $\vartheta_2 \neq 0$ в силу равенства $\alpha\vartheta_1^2 + \beta\vartheta_2^2 = 0$

Доказательство. Поскольку форма β невырождена, оператор корреляции

$$\beta : V \to V^*, \quad v \mapsto \beta(\,*\,, v),$$

является изоморфизмом. Изотропность $U \subset V$ означает, что $\beta(U) \subset \operatorname{Ann}(U)$. Поэтому $\dim U = \dim \beta(U) \leqslant \dim \operatorname{Ann} U = \dim V - \dim U$, откуда $2\dim U \leqslant \dim V$. □

15.2.3. **$2n$-мерное гиперболическое пространство H_{2n}** определяется как прямая сумма $V^* \oplus V$, где $\dim V = n$, наделённая симметричной билинейной формой

$$h\left(\xi_1 + v_1, \xi_2 + v_2\right) \stackrel{\text{def}}{=} \left\langle\, \xi_1\,,\, v_2 \,\right\rangle + \left\langle\, \xi_2\,,\, v_1 \,\right\rangle,$$

которая ограничивается в тождественно нулевые формы на подпространства V и V^*, а на любой паре паре вектор-ковектор равна свёртке $h(\xi, v) = h(v, \xi) = \langle\, \xi\,,\, v\,\rangle$. Базис H_{2n}, составленный из векторов $e_1, e_2, \dots, e_n, e_1^*, e_2^*, \dots, e_n^*$ каких-нибудь двойственных базисов V и V^*, называется *гиперболическим базисом*. Матрица Грама такого базиса имеет вид

$$\begin{pmatrix} 0 & E \\ E & 0 \end{pmatrix},$$

где 0 и E — нулевая и единичная $n \times n$-матрицы. Тем самым, форма h невырождена и обладает изотропными подпространствами половинной размерности, так что оценка из предл. 15.1 является точной. Прямая ортогональная сумма $H_{2m} \oplus H_{2k}$ изометрически изоморфна $H_{2(m+k)}$. Векторы $p_i = e_i + e_i^*$ и $q_i = e_i - e_i^*$ образуют ортогональный базис формы h со скалярными квадратами $h(p_i, p_i) = 2$, $h(q_i, q_i) = -2$.

Лемма 15.1
Всякое m-мерное изотропное подпространство U в пространстве V с невырожденной симметричной формой β содержится в некотором $2m$-мерном гиперболическом подпространстве $W \subset V$, и любой базис в U дополняется до гиперболического базиса в W.

Доказательство. Выберем в U базис $u_1, u_2, \dots, u_m$, дополним его до базиса в V и рассмотрим двойственный базис относительно невырожденной формы β. Первые m векторов $u_1^\times, u_2^\times, \dots, u_m^\times$ этого двойственного базиса таковы, что

$$\beta\left(u_i, u_j^\times\right) = \begin{cases} 1 & \text{при } i = j \\ 0 & \text{при } i \neq j, \end{cases} \tag{15-5}$$

причём добавление к любому из векторов $u_j^\times$ любой линейной комбинации векторов u_i не нарушает этого свойства. Заменяя каждый $u_j^\times$ на

$$w_j = u_j^\times - \frac{1}{2}\sum_\nu \beta\left(u_j^\times, u_\nu^\times\right) u_\nu,$$

получим набор векторов $w_1, w_2, \dots, w_m$, также удовлетворяющий (15-5) и порождающий изотропное подпространство, поскольку $\beta(w_i, w_j) = \beta(u_i^\times, u_j^\times) - \frac{1}{2}\,\beta(u_i^\times, u_j^\times) - \frac{1}{2}\,\beta(u_j^\times, u_i^\times) = 0$ для всех $1 \leqslant i, j \leqslant n$. □

Теорема 15.2
Любое пространство V с невырожденной симметричной билинейной формой раскладывается в прямую ортогональную сумму гиперболического и анизотропного подпространства.

Доказательство. Индукция по $\dim V$. Если $\dim V = 1$ или в V нет изотропных векторов, то само V является анизотропным пространством. Если в V есть ненулевой изотропный вектор e, то по лем. 15.1 он содержится в некоторой гиперболической плоскости H_2. Поскольку ограничение формы на эту плоскость невырождено, пространство V раскладывается в ортогональную прямую сумму $V = H_2 \oplus H_2^{\perp}$. По индукции, $H_2^{\perp} = H_{2k} \oplus U$, где U анизотропно и ортогонально H_{2k}. Тогда $V = H_{2k+2} \oplus U$. □

Следствие 15.3
Любая квадратичная форма q от n переменных линейной обратимой координат приводится к виду $x_1x_{i+1} + x_2x_{i+2} + \cdots + x_ix_{2i} + \alpha(x_{2i+1}, x_{2i+1} \ldots, x_r)$, где $r = \operatorname{rk}(q)$ и $\alpha(x) \neq 0$ при $x \neq 0$. □

15.3. Изометрии невырожденной симметричной формы. Напомним[1], что линейный оператор $f : V \to V$ называется *изометрией* невырожденной формы β, если

$$\forall\, u, w \in V \quad \beta(fu, fw) = \beta(u, w)$$

или, что то же самое, если $f^*\beta f = \beta$, где $\beta : V \to V^*$, $v \mapsto \beta(\,*\,, v)$ — корреляция формы β. Если форма $\beta = \tilde{q}$ является поляризацией квадратичной формы q, то в силу форм. (15-4) на стр. 232 для изометричности оператора f достаточно, чтобы он сохранял квадратичную форму q, т. е. чтобы $q(fv) = q(v)$ для всех $v \in V$. Поэтому группу изометрий O_β симметричной билинейной формы $\beta = \tilde{q}$ также называют *ортогональной группой* квадратичной формы q и обозначают O_q.

Пример 15.2 (изометрии гиперболической плоскости)
Оператор $f : H_2 \to H_2$ имеющий в гиперболическом базисе e, e^* матрицу

$$F = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

является изометрическим оператором гиперболической формы, когда

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

что равносильно уравнениям $ac = bd = 0$ и $ad+bc = 1$, имеющим два семейства решений:

$$F_\lambda = \begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix} \quad \text{и} \quad \widetilde{F}_\lambda = \begin{pmatrix} 0 & \lambda \\ \lambda^{-1} & 0 \end{pmatrix}, \quad \text{где } \lambda \in \Bbbk^* \text{ любое.} \tag{15-6}$$

Если основное поле $\Bbbk = \mathbb{R}$, то оператор F_λ с $\lambda > 0$ называется *гиперболическим поворотом*, поскольку траектория каждого ненулевого вектора $v = (x, y)$ при действии на него операторов F_λ с $\lambda \in (0, \infty)$ представляет собой гиперболу $xy = \text{const}$. Если положить $\lambda = e^t$

[1] см. n° 14.2.1 на стр. 218

и перейти к ортогональному базису $p = (e + e^*)/\sqrt{2}$, $q = (e - e^*)/\sqrt{2}$, оператор F_λ запишется в нём матрицей

$$\begin{pmatrix} 1/\sqrt{2} & 1/\sqrt{2} \\ 1/\sqrt{2} & -1/\sqrt{2} \end{pmatrix} \cdot \begin{pmatrix} e^t & 0 \\ 0 & e^{-t} \end{pmatrix} \cdot \begin{pmatrix} 1/\sqrt{2} & 1/\sqrt{2} \\ 1/\sqrt{2} & -1/\sqrt{2} \end{pmatrix} = \begin{pmatrix} \operatorname{ch} t & \operatorname{sh} t \\ \operatorname{sh} t & \operatorname{ch} t \end{pmatrix}$$

аналогичной матрице поворота евклидовой плоскости. При $\lambda < 0$ оператор F_λ является композицией гиперболического поворота с центральной симметрией относительно нуля. В обоих случаях операторы F_λ собственные и лежат в $\mathrm{SL}(\mathbb{R}^2)$, т. е. сохраняют площадь. Операторы $\widetilde{F}_\lambda$ несобственные и являются композициями гиперболических поворотов с отражением относительно оси гиперболы. Они сохраняют абсолютную величину площади, но меняют ориентацию.

15.3.1. Отражения. С каждым анизотропным вектором $e \in V$ связано прямое ортогональное разложение $V = \Bbbk \cdot e \oplus e^\perp$, где $e^\perp = \{v \in V \mid \beta(e, v) = 0\}$. Линейный оператор

$$\sigma_e : V \to V, \quad v \mapsto \sigma_e(v) \overset{\text{def}}{=} v - 2\,\frac{\beta(e, v)}{\beta(e, e)} \cdot e \tag{15-7}$$

тождественно действует на $e^\perp$ и переводит e в $-e$. Поэтому $\sigma_e \in \mathrm{O}_\beta$ и $\sigma_e^2 = 1$. Оператор (15-7) называется *отражением в гиперплоскости* $e^\perp$ (см. рис. 15◇1).

Упражнение 15.4. Убедитесь, что для любой изометрии $f : V \to V$ и любого анизотропного $e \in V$ выполняется равенство $f \circ \sigma_e \circ f^{-1} = \sigma_{f(e)}$.

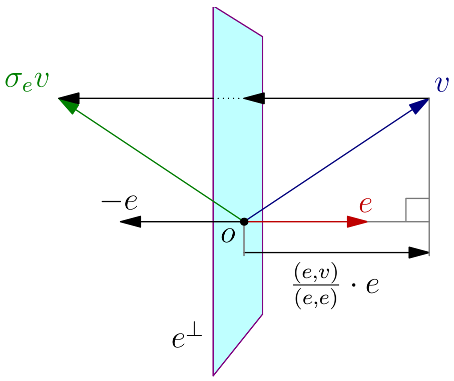


Рис. 15◇1. Отражение σ_e.

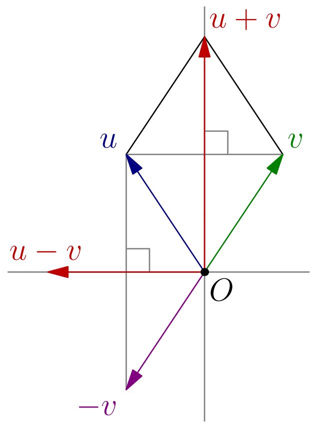


Рис. 15◇2. Отражения в ромбе.

Лемма 15.2
В пространстве с невырожденной симметричной билинейной формой β для любых двух различных анизотропных векторов u, v с равными скалярными квадратами $\beta(u, u) = \beta(v, v) \neq 0$ существует отражение, переводящее u либо в v либо в $-v$.

Доказательство. Если u и v коллинеарны, то искомым отражением является $\sigma_v = \sigma_u$. Если u и v неколлинеарны, то хотя бы одна из двух диагоналей натянутого на них ромба (см. рис. 15◇2) анизотропна. В самом деле, эти диагонали ортогональны между собою: $\beta(u+v, u-v) = \beta(u, u) - \beta(v, v) = 0$, и если бы они обе имели нулевые скалярные квадраты, то ограничение формы на их линейную оболочку, совпадающую с линейной оболочкой векторов u и v, было бы нулевым, что не так. Отражение σ_{u-v} переводит u в v, а отражение σ_{u+v} переводит u в $-v$. □

Упражнение 15.5. Проверьте последние два утверждения прямым вычислением и покажите, что если пространство V анизотропно, то всегда существует отражение, переводящее u в точности в v.

Теорема 15.3
Всякая изометрия n-мерного пространства с невырожденной симметричной формой является композицией не более $2n$ отражений.

Доказательство. Индукция по n. Ортогональная группа одномерного пространства состоит из тождественного оператора E и отражения $-E$. Рассмотрим изометрию $f : V \xrightarrow{\sim} V$ n-мерного пространства. Выберем в V какой-нибудь анизотропный вектор v и обозначим через σ отражение, переводящее $f(v)$ либо в v, либо в $-v$. Композиция σf переводит v в $\pm v$, а значит, переводит в себя $(n-1)$-мерную гиперплоскость $v^{\perp}$. По индукции, действие σf на $v^{\perp}$ является композицией не более $2(n-1)$ отражений. Продолжим гиперплоскости в $v^{\perp}$, относительно которых происходили эти отражения, до гиперплоскостей в V, добавив к ним вектор v. Тогда композиция $2n-2$ отражений в этих расширенных гиперплоскостях совпадает σf на $v^{\perp}$, и σf либо равен этой композиции, либо получается из неё применением ещё одного отражения в гиперплоскости $v^{\perp}$, переводящего v в $-v$. В любом случае, σf является композицией не более $2n-1$ отражений. Следовательно, $f = \sigma\sigma f$ это композиция не более $2n$ отражений. □

Упражнение 15.6. Докажите, что любая изометрия n-мерного анизотропного пространства является композицией $\leqslant n$ отражений.

Теорема 15.4 (лемма Витта)
Пусть на пространствах U, V, W заданы какие-то невырожденные симметричные билинейные формы. Если существует изометрический изоморфизм прямой ортогональной суммы $U \oplus V$ с прямой ортогональной суммой $U \oplus W$, то существует изометрический изоморфизм V с W.

Доказательство. Индукция по $\dim U$. Если $U = 0$, доказывать нечего. Если $\dim U = 1$, то $U = \Bbbk \cdot u$, где u анизотропен. Пусть имеется изометрический изоморфизм ортогональных прямых сумм $f : \Bbbk \cdot u \oplus V \xrightarrow{\sim} \Bbbk \cdot u \oplus W$. Рассмотрим отражение σ второго пространства, переводящее $f(u)$ в $\pm u$. Изометрический изоморфизм σf переводит $\Bbbk \cdot u$ в $\Bbbk \cdot u$, а значит, изоморфно отображает ортогональное дополнение к u в первом пространстве на ортогональное дополнение к u во втором, т. е. даёт искомый изометрический изоморфизм $\sigma f : V \xrightarrow{\sim} W$. Если $\dim U > 1$, то выберем в U какой-нибудь анизотропный вектор u и рассмотрим ортогональное разложение $U = \Bbbk \cdot u \oplus u^{\perp}$. Применяя предположение индукции к $U = \Bbbk \cdot u$ получим изометрический изоморфизм $u^{\perp} \oplus V$ с $u^{\perp} \oplus W$. Второй раз применяя индуктивное предположение с $U = u^{\perp}$, получаем искомую изометрию V с W. □

Следствие 15.4

Построенное в теореме (теор. 15.2) разложение пространства V с невырожденной симметричной билинейной формой в прямую ортогональную сумму гиперболического и анизотропного подпространств единственно в том смысле, что для любых двух таких разложений $V = H_{2k} \oplus U = H_{2m} \oplus W$ анизотропные подпространства U и W изометрически изоморфны, а гиперболические пространства имеют равные размерности $2k = 2m$.

Доказательство. Пусть $m \geqslant k$, так что $H_{2m} = H_{2k} \oplus H_{2(m-k)}$. Тождественное отображение $\mathrm{Id}_V : H_{2k} \oplus U \xrightarrow{\sim} H_{2k} \oplus H_{2(m-k)} \oplus W$ является изометрическим изоморфизмом. По лемме Витта существует изометрический изоморфизм $U \xrightarrow{\sim} H_{2(m-k)} \oplus W$. Поскольку в U нет изотропных векторов, гиперболическое подпространство $H_{2(m-k)}$ нулевое. Таким образом, $k = m$ и U изометрически изоморфно W. □

Следствие 15.5

Пусть подпространства U, W в в пространстве V с невырожденной симметричной билинейной формой таковы, что ограничения формы на U и на W невырождены и существует изометрический изоморфизм $\varphi : U \xrightarrow{\sim} W$. Тогда φ продолжается (многими способами) до изометрического автоморфизма всего пространства V, совпадающего с φ на подпространстве U.

Доказательство. Достаточно показать, что в условиях теоремы ортогоналы $U^\perp$ и $W^\perp$ изометрически изоморфны: тогда для любого изометрического изоморфизма $\psi : U^\perp \xrightarrow{\sim} W^\perp$, отображение $U \oplus U^\perp = V \to V = W \oplus W^\perp$, $(u, u') \mapsto \big(\varphi(h'), \psi(u')\big)$ даст требуемое продолжение. По условию, отображения $\eta : U \oplus U^\perp \to V$, $(u, u') \mapsto u + u'$ и $\zeta : U \oplus W^\perp \to V$, $(u, w') \mapsto \varphi(u) + w'$, являются изометрическими изоморфизмами. Поэтому композиция $\zeta^{-1}\eta : U \oplus U^\perp \xrightarrow{\sim} U \oplus W^\perp$ тоже является изометрическим изоморфизмом. По лемме Витта $U^\perp$ и $W^\perp$ изометрически изоморфны. □

Следствие 15.6

Ортогональная группа любой невырожденной симметричной билинейной формы транзитивно действует на гиперболических и на изотропных подпространствах данной размерности.

Доказательство. Утверждение про гиперболические подпространства вытекает из предыдущего следствия. Утверждение про изотропные подпространства сводится к утверждению про гиперболические подпространства при помощи лем. 15.1. □

Пример 15.3 (квадратичные формы над $\mathbb{F}_p$ при $p > 2$)

Зафиксируем какой-нибудь не квадрат $\varepsilon \in \mathbb{F}_p$. В n° 3.5.2 мы видели, что ненулевые квадраты образуют в мультипликативной группе поля $\mathbb{F}_p = \mathbb{Z}/(p)$ подгруппу индекса 2. Поэтому любой ненулевой элемент $\mathbb{F}_p$ умножением на подходящий ненулевой квадрат может быть сделан равным либо 1, либо ε. Из теор. 15.1 вытекает тогда, что всякая квадратичная форма над $\mathbb{F}_p$ обратимой линейной заменой переменных приводится к виду

$$q(x) = \sum x_i^2 + \varepsilon \sum x_j^2 \tag{15-8}$$

(наборы переменных в первой и второй сумме не пересекаются). Заметим, что уравнение

$$a x_1^2 + b x_2^2 = c \tag{15-9}$$

разрешимо в $\mathbb{F}_p$ при любых ненулевых a, b и любом c, поскольку когда x_1 и x_2 независимо друг от друга пробегают поле $\mathbb{F}_p$, функции ax_1^2 и $c - bx_2^2$ принимают по $(p+1)/2$ различных значений, так что эти множества значений имеют хотя бы один общий элемент $ax_1^2 = c - bx_2^2$. Разрешимость уравнения (15-9) означает, что каждая невырожденная квадратичная форма q на двумерном пространстве принимает все значения из поля $\Bbbk$. В частности, существует вектор e с $q(e) = 1$, а значит, координаты, в которых форма q имеет вид $x_1^2 + x_2^2$ или $x_1^2 + \varepsilon x_2^2$. Это позволяет сделать вторую сумму в (15-8) состоящей из не более, чем одного слагаемого, т. е. каждая квадратичная форма q ранга r над полем $\mathbb{F}_p$ в подходящих координатах записывается как $x_1^2 + \dots + x_{r-1}^2 + x_r^2$, если $\det q$ квадрат, или как $x_1^2 + \dots + x_{r-1}^2 + \varepsilon x_r^2$, если $\det q$ не квадрат.

Из разрешимости уравнения (15-9) также вытекает, что невырожденная квадратичная форма $ax_1^2 + bx_2^2 + cx_3^2 + \ \cdots$ от не менее трёх переменных всегда имеет ненулевой изотропный вектор — например, вектор $(\alpha_1, \alpha_2, 1, 0, \dots)$ с $a\alpha_1^2 + b\alpha_2^2 = -c$. Поэтому анизотропные формы над полем $\mathbb{F}_p$ бывают только в размерностях 1 и 2 и с точностью до изоморфизма исчерпываются невырожденными одномерными формами x^2 и εx^2 и двумерными формами $x_1^2 + x_2^2$, когда $p \equiv -1 \pmod 4$ и $x_1^2 + \varepsilon x_2^2$, когда $p \equiv 1 \pmod 4$.

Упражнение 15.7. Покажите, что форма $x_1^2 + x_2^2$ гиперболична при $p \equiv 1 \pmod 4$ и анизотропна при $p \equiv -1 \pmod 4$, а форма $x_1^2 + \varepsilon x_2^2$, наоборот, анизотропна при $p \equiv 1 \pmod 4$ и гиперболична при $p \equiv -1 \pmod 4$.

Таким образом, квадратичная форма над полем $\mathbb{F}_p$ либо гиперболична, либо является прямой ортогональной суммой гиперболической формы и одной из четырёх перечисленных выше анизотропных форм.

Пример 15.4 (вещественные квадратичные формы)

В силу теор. 15.1, всякая вещественная квадратичная форма q от n вещественных переменных линейной заменой координат преобразуется к виду

$$q(x) = x_1^2 + x_2^2 + \dots + x_p^2 - x_{p+1}^2 - x_{p+2}^2 - \dots - x_{p+m}^2 \,. \tag{15-10}$$

Для этого достаточно построить в $\mathbb{R}^n$ какой-нибудь базис $e_1, e_2, \dots, e_n$ с диагональной матрицей Грама, а затем поделить каждый e_i с $q(e_i) \neq 0$ на $\sqrt{|q(e_i)|}$.

Числа p и m называются *положительным* и *отрицательным индексами инерции* квадратичной формы q, а их разность $p - m$ — просто *индексом* формы q. Пару чисел (p, m) также называют *сигнатурой* формы β. Сумма $p + m = \operatorname{rk} q$ не зависит от выбора базиса, в котором q имеет вид (15-10). Покажем, что каждый из индексов p, m также не зависит от этого выбора. Заменяя V на фактор $V / \ker q$, мы можем считать, что форма q невырождена. Тогда она раскладывается в ортогональную прямую сумму гиперболической и анизотропной формы. Двумерная вещественная форма сигнатуры $(1,1)$ гиперболична, поскольку $x_1^2 - x_2^2 = (x_1 + x_2)(x_1 - x_2) = 2y_1y_2$, где $y_{1,2} = (x_1 \pm x_2)/\sqrt{2}$. Поэтому над полем $\mathbb{R}$ в каждой размерности с точностью до изоморфизма имеются ровно две неизоморфные анизотропные формы: *положительно определённая* (или *евклидова*), для которой $\beta(v, v) > 0 \ \forall \ v \neq 0$, и *отрицательно определённая*, для которой $\beta(v, v) < 0 \ \forall \ v \neq 0$. Их матрицы Грама в подходящих базисах равны E и $-E$. Таким образом, форма (15-10) является ортогональной прямой суммой гиперболической формы h размерности $2\min(p, m)$ и анизотропной формы α размерности $|p - m|$, которая положительно определена, если

$p > m$ и отрицательно определена, если $p < m$. Из единственности разложения в ортогональную прямую сумму гиперболической и анизотропной формы вытекает, что числа $p - m$ и $\min(p, m)$ не зависят от способа разложения, а числа p и m однозначно по ним восстанавливаются. Мы доказали

Следствие 15.7
Две квадратичных формы с вещественными коэффициентами тогда и только тогда переводятся друг в друга обратимой линейной заменой переменных, когда они имеют одинаковый ранг и индекс. □

Упражнение 15.8. Докажите, что положительный индекс инерции формы q равен наибольшей из размерностей подпространств, на которые q ограничивается в положительно определённую форму, а отрицательный — наибольшей из размерностей подпространств, на которые q ограничивается в отрицательно определённую форму.

Пример 15.5 (отыскание сигнатуры вещественной формы)
Рассмотрим матрицу Грама формы q в произвольном базисе и обозначим через $\varDelta_i$ её *главный угловой минор*, стоящей в первых i строках и первых i столбцах. Этот минор является определителем Грама ограничения формы q на линейную оболочку V_i первых i базисных векторов $e_1, e_2, \dots, e_i$. Он зануляется, если $q|_{V_i}$ вырождена, и имеет знак $(-1)^{m_i}$, если $q|_{V_i}$ невырождена и имеет отрицательный индекс инерции m_i. Таким образом, читая слева направо последовательность $\varDelta_1, \varDelta_2, \dots, \varDelta_{\dim V}$ можно проследить за последовательным изменением сигнатуры формы $q|_{V_i}$ при переходе от V_i к V_{i+1} или за появлением у формы q изотропных векторов, что позволяет найти сигнатуру всякий раз, когда в этой последовательности нет двух подряд стоящих нулей.

Пусть, например, $\varDelta_1 < 0$, $\varDelta_2 = 0$, $\varDelta_3 < 0$, $\varDelta_4 > 0$. Так как ограничение $q|_{V_2}$ вырождено, в V_2 имеется изотропный вектор. Поэтому невырожденная форма $q|_{V_3}$ является суммой гиперболической плоскости сигнатуры $(1, 1)$ и одномерного анизотропного пространства, т. е. имеет сигнатуру $(2, 1)$ или $(1, 2)$. Поскольку $\varDelta_3 < 0$, сигнатура $(p, m)_{V_3} = (2, 1)$. Из $\varDelta_4 > 0$ вытекает, что на всём пространстве сигнатура $(p, m)_V = (2, 2)$.

Когда ни один из главных угловых миноров не обращается в нуль, ограничение формы на каждое из пространств V_i невырождено, и знак у $\varDelta_{i+1}$ отличается от знака $\varDelta_i$ тогда и только тогда, когда $m_{i+1} = m_i + 1$. Поэтому полный отрицательный индекс инерции m формы q равен числу перемен знака в последовательности $1, \varDelta_1, \varDelta_2, \dots, \varDelta_{\dim V}$. Это наблюдение называется *критерием Сильвестра*.

15.4. Проективные квадрики. Множество одномерных изотропных подпространств квадратичной формы $q \in S^2V^*$, понимаемое как множество точек проективного пространства[1] $\mathbb{P}(V)$, ассоциированного с векторным пространством V, обозначается

$$V(q) = \{v \in \mathbb{P}(V) \mid q(v) = 0\},$$

[1] мы полагаем, что читатель знаком с проективными пространствами по курсу геометрии; если это не так, см. мою лекцию по геометрии http://gorod.bogomolov-lab.ru/ps/stud/geom_ru/lec_09.pdf или §18 из книги http://vyshka.math.ru/pspdf/textbooks/gorodentsev/algebra-1.pdf

и называется *проективной квадрикой*. Поскольку пропорциональные квадратичные форму задают одну и ту же квадрику, квадрики как геометрические фигуры являются точками проективного пространства $\mathbb{P}(S^2V^*)$, которое мы будем называть *пространством квадрик* в $\mathbb{P}(V)$.

Согласно сл. 15.3 уравнение квадрики $V(q) \subset \mathbb{P}_n = \mathbb{P}(V)$ в подходящих однородных координатах имеет вид

$$x_0x_1 + x_2x_3 + \dots + x_{2m}x_{2m+1} + \alpha(x_{2m+2}, \dots, x_r) = 0\,, \tag{15-11}$$

где форма $\alpha(x)$ анизотропна[1]. Число входящих в уравнение переменных равно рангу $\operatorname{rk} q$ квадратичной формы q, а линейная оболочка остальных $n-r$ базисных векторов, координаты вдоль которых не задействованы в (15-11), составляет ядро формы q. Число $2(m+1)$ в уравнении (15-11) равно размерности гиперболического ортогонального слагаемого формы q и по сл. 15.4 не зависит от выбора координат, где форма q имеет вид (15-11). Две квадрики называются *изоморфными* (или *проективно эквивалентными*), если одна переводится в другую линейным проективным автоморфизмом[2].

Мы обозначаем через $\tilde{q} : V \times V \to \Bbbk$ поляризацию квадратичной формы q, а через $\hat{q} : V \to V^*$ оператор корреляции[3] билинейной симметричной формы $\tilde{q}$. Проективизация ядра корреляции

$$\operatorname{Sing} Q \stackrel{\text{def}}{=} \mathbb{P}(\ker \hat{q}) = \mathbb{P}\{w \in V \mid \forall\, u \in V\ \tilde{(}u, w) = 0\} \tag{15-12}$$

называется *множеством особых точек* (или *вершинным пространством*) квадрики $V(q)$. Квадрика называется *гладкой* или *невырожденной*, если вершинное пространство пусто, и *особой* или *вырожденной* — в противном случае. Так как вершинное пространство особой квадрики, очевидно, лежит на ней, вырожденная квадрика никогда не пуста.

Пример 15.6 (квадрики на прямой)
На проективной прямой $\mathbb{P}_1$ над произвольным полем $\Bbbk$ характеристики $\operatorname{char}(\Bbbk) \neq 2$ имеется единственная с точностью до изоморфизма вырожденная квадрика, которая в подходящих координатах задаётся уравнением $x_0^2 = 0$ и по этой причине называется *двойной точкой*. Неособая квадрика $V(q)$, у которой $-\det q$ является квадратом, задаётся в подходящих координатах уравнением $x_0x_1 = 0$ и представляет собой пару различных точек. Неособая квадрика $V(q)$, у которой $-\det q$ не квадрат, пуста. Таким образом, пересечение произвольной квадрики $Q \subset \mathbb{P}_n$ с произвольной прямой ℓ либо совпадает с ℓ, либо является двойной точкой, либо парой различных точек, либо пусто, причём над алгебраически замкнутым полем последнее невозможно.

Упражнение 15.9. Покажите, что $p \in \operatorname{Sing} Q$ тогда и только тогда, когда каждая проходящая через p прямая либо лежит на Q либо пересекает Q по двойной точке p.

[1] $\alpha(x) \neq 0$ при $x \neq 0$

[2] т. е. биективным отображением $\mathbb{P}(V) \xrightarrow{\sim} \mathbb{P}(V)$, индуцированным невырожденным линейным оператором $V \xrightarrow{\sim} V$

[3] напомню, он переводит вектор $v \in V$ в линейную форму $u \mapsto \tilde{q}(u, v)$ на V

Теорема 15.5
Пересечение $Q' = L \cap Q$ произвольной квадрики $Q \subset \mathbb{P}(V)$ с любым дополнительным[1] к $\operatorname{Sing} Q$ проективным подпространством $L \subset \mathbb{P}(V)$ представляет собой гладкую квадрику в L, и квадрика Q является *линейным соединением*[2] этой неособой квадрики Q' и вершинного пространства $\operatorname{Sing} Q$.

Доказательство. Первое утверждение следует из предл. 14.6. Второе — из упр. 15.9: любая не лежащая в $\operatorname{Sing} Q$, но пересекающая $\operatorname{Sing} Q$ прямая имеет вид (ab) с $a \in \operatorname{Sing} Q$ и $b \in L$ и либо целиком лежит на квадрике Q и в этом случае $b \in L \cap Q = Q'$, либо пересекает Q по двойной точке a и в этом случае $b \notin Q'$. □

15.4.1. Гладкие квадрики. Линейные проективные автоморфизмы $\overline{F} : \mathbb{P}(V) \simeq \mathbb{P}(V)$, индуцированные изометриями $F \in \mathrm{O}_q$ невырожденной квадратичной формы q, переводят квадрику $V(q)$ в себя и называются *автоморфизмами* этой квадрики. Согласно сл. 15.6 группа проективных автоморфизмов квадрики $V(q)$ транзитивно действует на точках квадрики, а также на лежащих на квадрике проективных подпространствах любой фиксированной размерности. Поэтому максимальная размерность проходящего через данную точку квадрики подпространства, лежащего на квадрике, одинакова для всех точек. Она называется *планарностью* квадрики. Неособые квадрики разной планарности, очевидно, проективно не эквивалентны. Планарность гладкой квадрики, заданной уравнением (15-11) с $r = n$ и анизотропной формой α, равна m. Таким образом, квадрики с разными размерностями гиперболических компонент проективно не эквивалентны. Если вся форма $q(x_0, x_1, \dots, x_n) = \alpha(x_0, x_1, \dots, x_n)$ анизотропна, то квадрика $V(q)$ пуста, и мы полагаем её планарность равной -1.

Пример 15.7 (гладкие квадрики над алгебраически замкнутым полем)
Поскольку над алгебраически замкнутым полем $\Bbbk$ имеется ровно одна анизотропная форма x^2, n-мерная гладкая квадрика $Q_n \subset \mathbb{P}_{n+1}$ над алгебраически замкнутым полем единственна и в подходящих координатах она задаётся при чётном $n = 2m$ уравнением

$$x_0x_1 + x_2x_3 + \cdots + x_{2m}x_{2m+1} = 0\,, \tag{15-13}$$

при нечётном $n = 2m + 1$ уравнением

$$x_0x_1 + x_2x_3 + \cdots + x_{2m}x_{2m+1} = x_{2m+2}^2\,. \tag{15-14}$$

Через каждую точку обеих квадрик (15-13) и (15-14) проходит m-мерное проективное подпространство, лежащее на квадрике, и подпространств большей размерности на этих квадриках нет.

Пример 15.8 (гладкие вещественные квадрики)
Поскольку над полем $\Bbbk = \mathbb{R}$ в каждой размерности k имеется единственная с точностью до знака анизотропная форма $\alpha_k(x_1, x_2, \dots, x_k) = \sum\limits_{i=1}^{k} x_i^2$, гладкая n-мерная вещественная квадрика в $\mathbb{P}_{n+1} = \mathbb{P}\left(\mathbb{R}^{n+2}\right)$ в подходящих координатах имеет вид

$$x_0x_1 + x_2x_3 + \cdots + x_{2m}x_{2m+1} = x_{2m+2}^2 + x_{2m+3}^2 + \cdots + x_{n+1}^2\,, \tag{15-15}$$

[1] напомню, что проективные подпространства $K = \mathbb{P}(U)$ и $L = \mathbb{P}(W)$ в $\mathbb{P}_n = \mathbb{P}(V)$ называются *дополнительными*, если $K \cap L = \varnothing$ и $\dim K + \dim L = n - 1$ или, что то же самое, если $V = U \oplus W$

[2] т. е. объединением всех прямых (ab) с $a \in Q'$ и $b \in \operatorname{Sing} Q$

где $-1 \leqslant m \leqslant n/2$. Мы будем называть такую квадрику *m-планарной* и обозначать $Q_{n,m}$. Иначе m-планарную квадрику $Q_{n,m}$ можно охарактеризовать как квадрику сигнатуры $(n+2-m, m)$ или как как квадрику индекса $n+2-2m$. В координатах Лагранжа уравнение квадрики $Q_{n,m}$ имеет вид

$$t_0^2 + t_1^2 + \cdots + t_m^2 = t_{m+1}^2 + t_{m+2}^2 + \cdots + t_{n+1}^2 \,. \tag{15-16}$$

Переход от гиперболических координат x_ν к лагранжевым координатам t_ν задаётся формулами $x_{2i} = t_{m+i} + t_i$, $x_{2i+1} = t_{m+i} - t_i$ при $0 \leqslant i \leqslant m$ и $x_j = t_j$ при $2m+2 \leqslant j \leqslant n+2$.

Квадрики разной планарности проективно неэквивалентны, так как через каждую точку m-планарной квадрики проходит m-мерное проективное подпространство, лежащее на квадрике, и подпространств большей размерности на $Q_{n,m}$ нет. В частности, (-1)-планарная квадрика $t_0^2+t_1^2+\cdots+t_n^2 = 0$ пуста. Непустая не содержащая прямых квадрика планарности нуль $t_0^2 = t_1^2 + t_2^2 + \cdots + t_n^2$ называется *эллиптической*. Квадрики большей планарности называются *гиперболическими*.

15.4.2. Касательные пространства. Прямая ℓ, проходящая через точку $p \in Q$, называется *касательной* к квадрике Q в точке p, если она лежит на Q или пересекает Q по двойной точке p. Объединение всех прямых, касательных к квадрике Q в точке $p \in Q$, называется *касательным пространством* к Q в p и обозначается T_pQ.

Предложение 15.2
Прямая (ab) касается квадрики $V(q)$ в точке $a \in Q$ тогда и только тогда, когда $\tilde{q}(a,b) = 0$.

Доказательство. Ограничение формы q на линейную оболочку векторов $a, b \in V$ имеет в базисе a, b матрицу Грама

$$G = \begin{pmatrix} 0 & \tilde{q}(a,b) \\ \tilde{q}(b,a) & \tilde{q}(b,b) \end{pmatrix} .$$

Оно тождественно нулевое или особое тогда и только тогда, когда $\det G = 0$, что равносильно равенству $\tilde{q}(a,b) = \tilde{q}(b,a) = 0$. □

Следствие 15.8
Видимый из точки $b \notin V(q)$ контур[1] квадрики $V(q)$ высекается из неё гиперплоскостью $\operatorname{Ann} \hat{q}(b) = \{x \mid \tilde{q}(b,x) = 0\}$. Если точка $p \in V(q)$ неособа, то $T_pV(q) = \{x \in \mathbb{P}_n \mid \tilde{q}(p,x) = 0\}$ является гиперплоскостью в $\mathbb{P}_n$, а если точка $p \in \operatorname{Sing} V(q)$, то $T_pV(q) = \mathbb{P}_n$ совпадает со всем пространством.

Доказательство. Если $b \notin V(q)$, то $\tilde{(}b,b) = q(b) \neq 0$ и линейное уравнение $\tilde{q}(b,x) = 0$ нетривиально. Если $p \in V(q)$, то уравнение $\tilde{q}(p,x) = 0$ имеет вид $0 = 0$ и выполняется для всех точек $x \in \mathbb{P}_n$, если и только если точка $p \in \operatorname{Sing} V(q)$. □

Замечание 15.1. Линейное уравнение $\tilde{q}(p,x) = 0$, задающее касательное пространство $T_pV(q) \subset \mathbb{P}_n$ в точке $p \in V(q)$, может быть записано как

$$\sum_{i=0}^{n} \frac{\partial q}{\partial x_i}(p) \cdot x_i = 0 \,.$$

[1]т. е. ГМТ касания с $V(q)$ всевозможных касательных, опущенных на $V(q)$ из b

В частности, точка p особа, если и только если все частные производные $\frac{\partial q}{\partial x_i}(p) = 0$.

Упражнение 15.10. Покажите, что $\operatorname{Sing} Q = \bigcap\limits_{p\in Q} T_pQ$.

Пример 15.9 (коника Веронезе)
Над алгебраически замкнутым полем $\Bbbk$ квадрики на проективной прямой $\mathbb{P}_1$ суть то же самое, что неупорядоченные пары точек на $\mathbb{P}_1$. Поэтому неупорядоченные пары точек $\{a,b\}$ на $\mathbb{P}_1 = \mathbb{P}(U)$, $\dim U = 2$, биективно параметризуются точками проективной плоскости $\mathbb{P}_2 = \mathbb{P}(S^2U^*)$ по правилу

$$\{a,b\} \leftrightarrow q_{a,b}(t) = \det(t,a)\cdot\det(t,b)\,. \tag{15-17}$$

При этом парам совпадающих точек $\{a,a\}$ отвечают вырожденные квадрики $\det^2(t,a)$, являющиеся квадратами линейных форм. Если зафиксировать в U и U^* двойственные базисы (e_0,e_1) и (t_0,t_1), а в качестве базиса в S^2U^* взять $(t_0^2, 2t_0t_1, t_1^2)$, так что квадратичная форма $q(t) = x_0t_0^2 + 2x_1\,t_0t_1 + x_2t_1^2$ с матрицей Грама $\begin{pmatrix} x_0 & x_1\\ x_1 & x_2\end{pmatrix}$ будет иметь в нём однородные координаты $(x_0 : x_1 : x_2)$, то паре точек $a = (\alpha_0 : \alpha_1)$ и $b = (\beta_0, \beta_1)$ на $\mathbb{P}_1 = \mathbb{P}(U)$ соответствие (15-17) сопоставит точку $x \in \mathbb{P}_2 = \mathbb{P}(S^2U^*)$ с координатами

$$x_0 = \alpha_1\beta_1\,,\quad x_1 = -(\alpha_0\beta_1 + \alpha_1\beta_0)/2\,,\quad x_2 = \alpha_0\beta_0\,, \tag{15-18}$$

а пары совпадающих точек $\{a,a\}$ составят гладкую *конику Веронезе* C с уравнением

$$\det\begin{pmatrix} x_0 & x_1\\ x_1 & x_2\end{pmatrix} = x_0x_2 - x_1^2 = 0\,. \tag{15-19}$$

Вложение Веронезе $\mathbb{P}_1 = \mathbb{P}(U) \hookrightarrow \mathbb{P}_2 = \mathbb{P}(S^2U^*)$, сопоставляющее точке $a = (\alpha_0 : \alpha_1)$ на $\mathbb{P}_1$ двойную точку $\{a,a\}$ на $\mathbb{P}_2$, биективно отображает прямую на конику (15-19) по правилу

$$(\alpha_0 : \alpha_1) \mapsto (x_0 : x_1 : x_2) = (\alpha_1^2 : -\alpha_0\alpha_1 : \alpha_0^2)\,. \tag{15-20}$$

Поскольку при фиксированном $a \in U$ и переменном $b \in U$ квадратичные формы вида $\det(t,a)\det(t,b)$ образуют двумерное векторное подпространство в S^2U^*, пары точек вида $\{a,b\}$ с фиксированным a и переменным b составляют прямую на $\mathbb{P}_2$, касающуюся коники Веронезе C в точке $\{a,a\}$.

Упражнение 15.11. Покажите, что каждая линейная инволюция[1] на $\mathbb{P}_1$ имеет над алгебраически замкнутым полем ровно две различных неподвижных точки.

Из наличия у гладкой коники C на $\mathbb{P}_2$ квадратичной параметризации (15-20) вытекает, что гладкая коника C пересекается с кривой $D \subset \mathbb{P}_2$, заданной однородным уравнением $f(x) = 0$ степени d, не более, чем по $2d$ точкам, или целиком содержится в этой кривой в качестве компоненты. В самом деле, подставляя $(x_0 : x_1 : x_2) = (\alpha_1^2 : -\alpha_0\alpha_1 : \alpha_0^2)$ в $f(x) = 0$ получаем уравнение $f\big(x(\alpha)\big) = 0$, корнями которого являются значения параметра α в точках пересечения $C \cap D$ и которое либо выполнено тождественно по α, либо является однородным многочленом степени $2d$ и имеет не более $2d$ корней на $\mathbb{P}_1$. В частности, через 5 точек на $\mathbb{P}_2$ проходит не более одной гладкой коники.

[1] т. е. нетождественное отображение $\sigma : \mathbb{P}(U) \to \mathbb{P}(U)$, индуцированное каким-либо невырожденным линейным оператором $\widetilde{\sigma} : U \to U$ и удовлетворяющее соотношению $\sigma^2 = \mathrm{Id}_{\mathbb{P}(U)}$

Упражнение 15.12. Покажите, что над любым полем через любые 5 точек на $\mathbb{P}_2$ можно провести конику, причём если никакие 4 из 5 точек не коллинеарны, то такая коника единственна, а если никакие 3 не коллинеарны, то и гладка.

Пример 15.10 (квадрика Сегре)
Рассмотрим два 2-мерных векторных пространства U_- и U_+ и положим $W = \mathrm{Hom}(U_-, U_+)$. Операторы $U_- \to U_+$ ранга 1 образуют в $\mathbb{P}_3 = \mathbb{P}(W)$ *квадрику Сегре*

$$Q_s = \{F : U_- \to U_+ \mid \det F = 0\} = \left\{ \begin{pmatrix} x_0 & x_1 \\ x_2 & x_3 \end{pmatrix} \,\middle|\, x_0x_3 - x_1x_2 = 0 \right\}. \tag{15-21}$$

Если оператор $F : U_- \to U_+$ имеет ранг 1, то подпространство $\operatorname{im} F \subset U_+$ одномерно и порождается некоторыми вектором $v \in U_+$, который определяется по F однозначно с точностью до пропорциональности. Действие оператора F на произвольный вектор $u \in U_-$ происходит по правилу $F(u) = \xi(u) \cdot v$, где $\xi \in U_-^*$ однозначно определяется выбором v и порождает одномерное подпространство $\mathrm{Ann}\ker F \subset U_-^*$. Наоборот, для любых ненулевых $v \in U_+$ и $\xi \in U_-^*$ оператор

$$\xi \otimes v \;:\; U_- \to U_+ , \quad u \mapsto \xi(u)\, v , \tag{15-22}$$

имеет ранг 1. Таким образом, *вложение Сегре*

$$s : \mathbb{P}(U_-^*) \times \mathbb{P}(U_+) \hookrightarrow \mathbb{P}\,\mathrm{Hom}(U_-, U_+) , \quad (\xi, v) \mapsto \xi \otimes v , \tag{15-23}$$

устанавливает биекцию между $\mathbb{P}_1 \times \mathbb{P}_1 = \mathbb{P}(U_-^*) \times \mathbb{P}(U_+)$ и квадрикой Сегре (15-21). Поскольку 2×2-матрицы ранга 1 имеют пропорциональные строки и столбцы и матрицы с фиксированными отношениями

$$\begin{gathered} ([\text{строка } 1] : [\text{строка } 2]) = (t_0 : t_1) \\ ([\text{столбец } 1] : [\text{столбец } 2]) = (\xi_0 : \xi_1) \end{gathered} \tag{15-24}$$

составляют двумерные векторные подпространства в W, проективизации этих двумерных подпространств образуют на квадрике Сегре два семейства прямых, таких что каждая точка квадрики является точкой пересечения пары прямых из разных семейств. Эти прямые являются образами координатных прямых $\mathbb{P}_1 \times v$ и $\xi \times \mathbb{P}_1$ на $\mathbb{P}_1 \times \mathbb{P}_1$ при вложении (15-23), т. к. оператор $\xi \otimes v$, отвечающий форме $\xi = (\xi_0 : \xi_1) \in U_-^*$ и вектору $v = (t_0 : t_1) \in U_+$, имеет матрицу

$$\xi \otimes v = \begin{pmatrix} t_0 \\ t_1 \end{pmatrix} \cdot \begin{pmatrix} \xi_0 & \xi_1 \end{pmatrix} = \begin{pmatrix} \xi_0 t_0 & \xi_1 t_0 \\ \xi_0 t_1 & \xi_1 t_1 \end{pmatrix} \tag{15-25}$$

строки и столбцы которой относятся как в (15-24). В силу биективности отображения Сегре, все соотношения инцидентности между координатными прямыми на $\mathbb{P}_1 \times \mathbb{P}_1$ сохранятся и между их образами на квадрике. Поэтому прямые в каждом из двух семейств (15-24) попарно скрещиваются, любые две прямые из разных семейств пересекаются, каждая точка квадрики Сегре является точкой пересечения двух прямых из различных семейств, и никаких других прямых на квадрике Сегре нет в силу того, что лежащая на Q_s прямая, проходящая через заданную точку $p \in Q_s$, содержится в конике $Q_s \cap T_p Q_s$, которая полностью исчерпывается парой пересекающихся в точке p образов координатных прямых с $\mathbb{P}_1 \times \mathbb{P}_1$.

Упражнение 15.13. Покажите, что любые 9 точек, а также любые 3 прямые в $\mathbb{P}_3$ лежат на некоторой квадрике, причём квадрика, проходящая через три попарно непересекающиеся прямые, автоматически является гиперболической квадрикой Сегре.

Предложение 15.3
Сечение $\Pi \cap Q$ неособой квадрики Q гиперплоскостью Π либо является неособой квадрикой в Π, либо имеет единственную особую точку p, и в этом случае плоскость $\Pi = T_pQ$, а квадрика $\Pi \cap Q$ является конусом с вершиной в p над неособой квадрикой $Q' = \Pi' \cap Q$, которая высекается из Q любой не проходящей через p гиперплоскостью $\Pi' \subset T_pQ$ и имеет на единицу меньшую планарность, чем Q.

Доказательство. Пусть $Q = V(q) \subset \mathbb{P}(V)$ и $\Pi = \mathbb{P}(W)$. Тогда

$$\dim\ker\left(\hat{q}|_W\right) = \dim\left(W \cap \hat{q}^{-1}(\operatorname{Ann} W)\right) \leqslant \\ \leqslant \dim \hat{q}^{-1}(\operatorname{Ann} W) = \dim \operatorname{Ann} W = \dim V - \dim W = 1\,.$$

Если $\dim\ker\left(\hat{q}|_W\right) = 1$ и это ядро порождается вектором p, то $p \in Q \cap \Pi$ и $\operatorname{Ann}(\hat{q}(p)) = W$, откуда $T_pQ = \Pi$. Наоборот, если $\Pi = T_pQ = \mathbb{P}(\operatorname{Ann}\hat{q}(p))$, то вектор $p \in \operatorname{Ann}\hat{q}(p)$ лежит в ядре ограничения $\hat{q}$ на $\operatorname{Ann}\hat{q}$ и порождает его, т. к. оно одномерно. Ограничение q на любую не проходящую через p гиперплоскость $\Pi' = \mathbb{P}(U) \subset T_pQ$ при этом невырождено, и пространство V является ортогональной прямой суммой $V = U \oplus U^{\perp}$, где $\dim U^{\perp} = 2$ и ограничение $q|_{U^{\perp}}$ тоже невырождено. Поскольку $p \in U^{\perp}$ является изотропным вектором для $q|_{U^{\perp}}$, подпространство $U^{\perp} \subset V$ — гиперболическая плоскость. Поэтому размерность гиперболической составляющей формы $q|_U$, задающей квадрику $Q' = \Pi' \cap Q$, на 2 меньше, чем у q. □

Следствие 15.9
Невырожденная квадрика либо пуста, либо не содержится ни в какой гиперплоскости.

Доказательство. Если непустая невырожденная квадрика содержится в гиперплоскости H, то $H = T_pQ$ для всех $p \in Q$ и $Q = Q \cap T_VQ$ должна быть особа. □

Следствие 15.10
Проективные подпространства размерности m на гладкой m-планарной квадрике $Q \subset \mathbb{P}_n$, проходящие через данную точку $p \in Q$, взаимно однозначно соответствуют всем $(m-1)$-мерным проективным подпространствам, лежащим на гладкой $(m-1)$-планарной квадрике $Q' \subset \mathbb{P}_{n-2}$, высекаемой из Q любой не проходящей через p гиперплоскостью $\mathbb{P}_{n-2} \subset T_pQ = \mathbb{P}_{n-1}$.

Пример 15.11 (подпространства на квадриках над алгебраически замкнутым полем)
Над алгебраически замкнутым полем $\Bbbk$ на нульмерной и одномерной гладких квадриках $Q_0 \subset \mathbb{P}_1$ и $Q_1 \subset \mathbb{P}_2$ лежат только 0-мерные подпространства. Следующие две квадрики — двумерная $Q_2 \subset \mathbb{P}_3$ и трёхмерная $Q_3 \subset \mathbb{P}_4$ — не содержат плоскостей, но каждая точка $p \in Q_2$ лежит на паре прямых, проходящих через p и две точки неособой квадрики $Q_0 \subset \mathbb{P}_1 \subset T_pQ_2 \smallsetminus \{p\}$, а через каждую точку $p \in Q_3$ проходит одномерное семейство прямых, образующих конус с вершиной p над гладкой коникой $Q_1 \subset \mathbb{P}_2 \subset T_pQ_4 \smallsetminus \{p\}$.

Квадрика Плюккера $Q_4 \subset \mathbb{P}_5$ не содержит 3-мерных подпространств, но через любую точку $p \in Q_4$ проходят два пучка[1] плоскостей, взаимно однозначно соответствующих двум семействам прямых на квадрике Сегре , и т. д.

Пример 15.12 (подпространства на вещественных квадриках)
Над полем вещественных чисел $\mathbb{R}$ на n-мерной эллиптической квадрике $Q_{n,0}$ нет прямых. Через каждую точку n-мерной 1-планарной квадрики $Q_{n,1}$ проходит целый конус прямых с основанием в $(n-2)$-мерной эллиптической квадрике $Q_{n-2,0} \subset \mathbb{P}_{n-1} \subset T_pQ_{n,1} \smallsetminus \{p\}$. Так, через каждую точку поверхности Сегре $Q_{2,1} \subset \mathbb{P}_3$ проходит ровно две прямые, образующие конус над двухточечной гиперболической квадрикой на $\mathbb{P}_1$. Плоскости, проходящие через каждую точку n-мерной 2-планарной квадрики $Q_{n,2}$ являются линейными соединениями этой точки со всевозможными прямыми, лежащими на $(n-2)$-мерной 1-планарной квадрике $Q_{n-2,1} \subset \mathbb{P}_{n-1} \subset T_pQ_{n,2} \smallsetminus \{p\}$ и т. д.

15.5. Аффинные квадрики. Выберем в аффинном пространстве $\mathbb{A}^n = \mathbb{A}(V)$ какой-нибудь аффинный репер и отождествим $\mathbb{A}^n$ с координатным пространством $\Bbbk^n$. Фигура, задаваемая в $\mathbb{A}^n$ (неоднородным) многочленом второй степени

$$f(x) = f_0 + f_1(x) + f_2(x)\,, \quad \text{где} \quad f_0 \in \Bbbk\,,\ f_1 \in V^*\,,\ f_2 \in S^2V^*\,, \tag{15-26}$$

от координат $x = (x_1, x_2, \dots, x_n)$ пространства $\Bbbk^n$, называется *аффинной квадрикой.*

Упражнение 15.14. Покажите, что свойство фигуры $Q \subset \mathbb{A}^n$ быть аффинной квадрикой не зависит от выбора координатного репера.

Аффинные квадрики $Q' \subset \mathbb{A}^n$ и $Q'' \subset \mathbb{A}^n$ называются *аффинно эквивалентными* (или *изоморфными*), если имеется аффинный изоморфизм[2] $F : \mathbb{A}^n \xrightarrow{\sim} \mathbb{A}^n$, отображающий квадрику Q' в квадрику Q''.

15.5.1. Проективное замыкание аффинной квадрики. Аффинная квадрика Q, заданная неоднородным уравнением (15-26) в пространстве $\mathbb{A}^n = \mathbb{A}(\Bbbk^n)$ с координатами $(x_1, x_2, \dots, x_n)$, является аффинным изображением в стандартной аффинной карте U_0, где $x_0 = 1$, своего проективного замыкания $\overline{Q} \subset \mathbb{P}_n$ — проективной квадрики, заданной в проективном пространстве $\mathbb{P}_n = \mathbb{P}(\Bbbk^{n+1})$ с координатами $(x_0 : x_1 : \dots : x_n)$ однородным уравнением

$$\overline{f}(x) = f_0 \cdot x_0^2 + x_0 \cdot f_1(x_1, x_2, \dots, x_n) + f_2(x_1, x_2, \dots, x_n)\,. \tag{15-27}$$

Аффинная карта U_0 — это аффинное пространство над векторным пространством $\operatorname{Ann} x_0$, натянутым на базисные векторы $e_1, e_2, \dots, e_n$. Всякий аффинный автоморфизм

$$F : U_0 \xrightarrow{\sim} U_0\,,$$

отображающий аффинный координатный репер началом в точке $e_0 \in U_0$ и базисными векторами $e_1, e_2, \dots, e_n$ в аффинный координатный репер с началом в точке $e_0' \in U_0$ и базисными векторами $e_1', e_2', \dots, e_n' \in \operatorname{Ann} x_0$, является ограничением на карту U_0 проективного автоморфизма $\overline{F} : \mathbb{P}_n \xrightarrow{\sim} \mathbb{P}_n$, индуцированного линейным оператором

$$\widetilde{F} : \Bbbk^{n+1} \xrightarrow{\sim} \Bbbk^{n+1}\,,$$

[1]напомним, что *пучок* в этом контексте означает семейство фигур, образующих *прямую* в подходящем проективном пространстве фигур, в данном случае — в пространстве плоскостей в $\mathbb{P}_4$, представляющем собою грассманиан $\mathrm{Gr}(3,5)$

[2]см. ?? на стр. ??

переводящим e_i в e_i' при всех $0 \leqslant i \leqslant n$. Наоборот, любой линейный автоморфизм $\widetilde{F} : \Bbbk^{n+1} \xrightarrow{\sim} \Bbbk^{n+1}$, переводящий в себя подпространство $\operatorname{Ann} x_0$, т. е. имеющий в базисе $e_0, e_1, \dots , e_n$ матрицу вида

$$\left(\begin{array}{c|ccc} 1 & 0 & \dots & 0 \\ \hline a_1 & & & \\ \vdots & & D_F & \\ a_n & & & \end{array}\right) \cdot \text{const} ,$$

задаёт аффинный автоморфизм карты U_0, переводящий начало координат в точку $a = (a_1, a_2, \dots , a_n)$ и имеющий дифференциал $D_F : \operatorname{Ann} x_0 \xrightarrow{\sim} \operatorname{Ann} x_0$.

Поэтому с проективной точки зрения описание аффинных квадрик с точностью до аффинного изоморфизма есть описание пар

«проективная квадрика $\overline{Q}$ + проективная гиперплоскость L_∞»

с точностью до проективных автоморфизмов, изоморфно отображающих одну гиперплоскость на другую. Соответствующие аффинные квадрики при этом будут аффинными изображениями проективных квадрик в аффинных картах, покрывающих дополнения к проективным гиперплоскостям — бесконечно удалённым гиперплоскостям этих аффинных карт.

Возникающая на этом пути классификация аффинных квадрик разбивает их на 4 класса: гладкие центральные квадрики, параболоиды, простые конусы и цилиндры.

15.5.2. Гладкие центральные квадрики. Пусть проективное замыкание $\overline{Q}$ аффинной квадрики Q гладко и бесконечно удалённая гиперплоскость L_∞ не является касательной гиперплоскостью к $\overline{Q}$. Тогда она пересекает $\overline{Q}$ по гладкой квадрике $Q_\infty = \overline{Q} \cap L_\infty$. В терминах уравнений это означает, что определитель Грама квадрики $\overline{Q}$ и определитель Грама квадратичной части $f_2(x_1, x_2, \dots , x_n)$ аффинного уравнения (15-26) оба отличны от нуля.

Полюс c бесконечно удалённой гиперплоскости L_∞ относительно квадрики $\overline{Q}$ называется *центром* аффинной квадрики Q. Он лежит в аффинной карте U_0 и является в ней центром симметрии аффинной квадрики Q, поскольку по **??** для любой прямой ℓ, проходящей через точку c и произвольную точку $d \in L_\infty \smallsetminus \overline{Q}$ и пересекающей квадрику в точках $a, b \in Q$, выполняется равенство $[d, c, b, a] = -1$, означающее, что в аффинной части $U_0 \cap \ell = \ell \smallsetminus d$ этой прямой точка c является серединой отрезка $[a, b]$.

По этой причине аффинные квадрики с гладким проективным замыканием, не касающимся бесконечно удалённой гиперплоскости, называются *гладкими центральными квадриками.*

В любой аффинной системе координат с центром в c аффинное уравнение квадрики имеет вид $f(x) = f_0 + f_2(x)$, где $f_0 \neq 0$, линейная форма f_1 отсутствует, а квадратичная форма f_2 невырождена. Выбирая в $\Bbbk^n$ координаты, в которых матрица Грама квадратичной формы f_2 диагональна, и деля обе части уравнения на f_0, приводим аффинное уравнение квадрики к виду

$$a_1 x_1^2 + a_2 x_2^2 + \dots + a_n x_n^2 = 1 \,. \tag{15-28}$$

Над алгебраически замкнутым полем перескалированием переменных это уравнение можно упростить до $x_1^2 + x_2^2 + \dots + x_n^2 = 1$. Тем самым, все центральные гладкие квадрики над алгебраически замкнутым полем аффинно эквивалентны.

Над полем $\mathbb{R}$ уравнение (15-28) упрощается до

$$x_1^2 + \dots + x_p^2 - x_{p+1}^2 - \dots - x_{p+m}^2 = \pm 1\,, \quad \text{где} \quad p \geqslant m\,,\ p+m=n \tag{15-29}$$

и в случае $p = m = n/2$ в правой части стоит знак «плюс[1]». Среди этих квадрик есть ровно одна пустая — с уравнением[2] $\sum x_i^2 = -1$, а также ровно одна непустая квадрика, не пересекающая бесконечно удалённую гиперплоскость. Эта квадрика задаётся имеет уравнением $\sum x_i^2 = 1$ с $m = 0$ и плюсом в правой части. Она называется *эллипсоидом*. Эллипсоид компактен и как следствие — 0-планарен. Все остальные квадрики имеют непустое пересечение с бесконечностью (в частности, неограничены) и называются *гиперболоидами*.

При $p > m$ проекивное замыкание квадрики (15-29) с плюсом в правой части имеет сигнатуру $(p, m+1)$, и стало быть, такая квадрика m-планарна. Если в правой части (15-29) стоит минус, сигнатура проективного замыкания равна (p, m), и такая квадрика $(m-1)$-планарна. При $p = m = n/2$ квадрика (15-29) имеет планарность $n/divs2$. В частности, 0-планарные квадрики (15-29) исчерпываются эллипсоидом и *двуполостным гиперболоидом* $x_1^2 + \dots + x_{n-1}^2 = x_n^2 - 1$.

Упражнение 15.15. Убедитесь, что двуполостный гиперболоид имеет две связных компоненты, а все остальные непустые квадрики (15-29) линейно связны.

Пересечение квадрики (15-29) с бесконечно удалённой гиперплоскостью задаётся в ней уравнением

$$x_1^2 + \dots + x_p^2 - x_{p+1}^2 - \dots - x_{p+m}^2 = 0$$

и имеет планарность m (вне зависимости от того, какой знак стоит в правой части формулы (15-29)). Таким образом, среди квадрик (15-29) нет аффинно эквивалентных.

15.5.3. Параболоиды. Аффинные квадрики с гладким проективным замыканием $\overline{Q}$, для которых бесконечно удалённая гиперплоскость L_∞ является касательной гиперплоскостью, называются *параболоидами*.

Согласно предл. 15.3 пересечение $Q_\infty = L_\infty \cap \overline{Q}$ является в этом случае особой квадрикой с единственной особой точкой — точкой касания квадрики $\overline{Q}$ с бесконечно удалённой гиперплоскостью. В терминах уравнений это означает, что определитель Грама квадрики $\overline{Q}$ отличен от нуля, а матрица Грама квадратичной части $f_2(x_1, x_2, \dots, x_n)$ аффинного уравнения (15-26) имеет одномерное ядро.

Обозначим через $\tilde{f}$ поляризацию однородной формы (15-27), задающей проективную квадрику $\overline{Q}$, и пусть $u \in \operatorname{Ann} x_0$ порождает ядро формы f_2. Поскольку форма $\tilde{f}$ невырождена и $\tilde{f}(e_i, u) = 0$ для всех $1 \leqslant i \leqslant n$, скалярное произведение $\tilde{f}(e_0, u) \neq 0$, и на векторы e_0 и u натягивается гиперболическая плоскость. Выберем в ней гиперболический базис[3]

$$\varepsilon_0 = e_0 - \frac{1}{2} \cdot \frac{\tilde{f}(e_0, e_0)}{\tilde{f}(e_0, u)} \cdot u = e_0 - \frac{f_0 \cdot u}{f_1(u)} \tag{15-30}$$

$$\varepsilon_n = \frac{1}{\tilde{f}(e_0, u)} \cdot u = \frac{2u}{f_1(u)}\,, \tag{15-31}$$

---

[1] уравнение со знаком «$-$» получается из уравнения со знаком «$+$» сменой знака в обоих частях и перенумерацией переменных, так что задаваемые ими квадрики аффинно эквивалентны

[2] иногда её называют «мнимым эллипсоидом»

[3] т. е. сдвинем начало аффинной системы координат в точку $-u \cdot f_0 / \big(2 f_1(u)\big)$ и возьмём вектор $p/f_1(u)$ в качестве n-того базисного вектора в $\Bbbk^n$

а в $\tilde{f}$-ортогональном дополнении к ней[1] — базис $\varepsilon_1, \varepsilon_2, \dots, \varepsilon_{n-1}$, в котором матрица Грама ограничения формы $\tilde{f}$ диагональна. В локальных аффинных координатах относительно базиса[2] $\varepsilon_0, \varepsilon_1, \dots, \varepsilon_n$ уравнение квадрики Q примет вид

$$a_1 x_1^2 + a_2 x_2^2 + \dots + a_{n-1} x_{n-1}^2 = x_n\,,$$

который над алгебраически замкнутым полем упрощается до

$$x_1^2 + x_2^2 + \dots + x_{n-1}^2 = x_n\,,$$

а над полем вещественных чисел $\mathbb{R}$ — до

$$x_1^2 + \dots + x_p^2 - x_{p+1}^2 - \dots - x_{p+m}^2 = x_n\,, \quad \text{где} \quad p \geqslant m \quad \text{и} \quad p + m = n - 1\,. \tag{15-32}$$

Параболоид (15-32) имеет планарность m. Таким образом, все параболоиды (15-32) непусты и неэквивалентны друг другу. Нуль-планарный параболоид $x_1^2 + \dots + x_{n-1}^2 = x_n$ называется *эллиптическим параболоидом*, а все остальные — *гиперболическими параболоидами*.

15.5.4. Простые конусы. Аффинная квадрика Q, проективное замыкание которой $\overline{Q}$ особо, но не имеет особенностей на L_∞, называется *простым конусом*.

Поскольку проективное подпространство $\operatorname{Sing}(\overline{Q})$ не пересекается с гиперплоскостью L_∞, оно нульмерно. На языке формул это означает, что матрица Грама формы $\overline{f}$ имеет одномерное ядро, порождённое некоторым вектором $u \in U_0$, а форма f_2 невырождена, поскольку всякий вектор из $\ker f_2$, будучи ортогональным к u, автоматически попадает в $\ker \tilde{f}$.

Поместим начало отсчёта аффинной координатной системы в u и выберем в $\operatorname{Ann} x_0$ базис, в котором матрица Грама формы f_2 диагональна. В полученной системе аффинных координат уравнение квадрики Q имеет вид

$$a_1 x_1^2 + a_2 x_2^2 + \dots + a_n x_n^2 = 0\,, \tag{15-33}$$

который над алгебраически замкнутым полем упрощается до

$$x_1^2 + x_2^2 + \dots + x_n^2 = 0\,, \tag{15-34}$$

а над полем $\mathbb{R}$ — до

$$x_1^2 + \dots + x_p^2 - x_{p+1}^2 - \dots - x_{p+m}^2 = 0\,, \quad \text{где} \quad p \geqslant m \quad \text{и} \quad p + m = n\,. \tag{15-35}$$

Эти уравнения задают n-мерном аффинном пространстве $\mathbb{A}(\operatorname{Ann} x_0)$ аффинный конус с вершиной в нуле над гладкой проективной квадрикой в $\mathbb{P}_{k-1} = \mathbb{P}(\operatorname{Ann} x_0) = L_\infty$ — пересечением $\overline{Q} \cap L_\infty$. Над алгебраически замкнутым полем такая квадрика единственна, над полем $\mathbb{R}$ все они перечисляются формулой (15-35) и отличаются друг от друга планарностью, которая равна m. Отметим, что при $m = 0$ вещественная аффинная квадрика (15-35) состоит из единственной точки 0.

---

[1] т. е. в $(n-1)$-мерном векторном пространстве $\varepsilon_0^\perp \cap \operatorname{Ann} x_0 \subset \Bbbk^n$

[2] т. е. в аффинной системе координат на U_0 с началом в $\varepsilon_0 \in U_0$ и базисными векторами $\varepsilon_1, \varepsilon_2, \dots, \varepsilon_n \in \operatorname{Ann} x_0$

15.5.5. Цилиндры. Квадрика Q, проективное замыкание которой $\overline{Q}$ вырождено и имеет особенности на бесконечности, называется *цилиндром*. На языке формул это означает, что обе матрицы Грама $\overline{f}$ и f_2 вырождены.

Выберем в векторном пространстве $\operatorname{Ann} x_0$ базис $e_1, e_2, \dots, e_n$ так, чтобы векторы e_i с $i > r$ составляли базис в $\ker \tilde{f} \cap \operatorname{Ann} x_0 \neq 0$. Уравнение квадрики Q в таком базисе не зависит от координат x_i с $i > r$. Поэтому квадрика является прямым произведением аффинного пространства $\mathbb{A}^{n-r}$, направленного вдоль этих координат, и аффинной квадрики в $\mathbb{A}^r$, проективное замыкание которой в $\mathbb{P}^r$ не имеет особенностей на бесконечности. Все такие квадрики уже были перечислены нами выше.

Пример 15.13 (вещественные аффинные кривые второй степени)
Полный список непустых неизоморфных друг другу аффинных квадрик в $\mathbb{R}^2$ таков:

- *эллипс* $x_1^2 + x_2^2 = 1$ — гладкая центральная коника, не пересекающая бесконечно удалённую прямую $x_0 = 0$
- *гипербола* $x_1^2 - x_2^2 = 1$ — гладкая центральная коника, пересекающая бесконечно удалённую прямую $x_0 = 0$ по паре точек $(0 : 1 : 0)$ и $(0 : 0 : 1)$
- *парабола* $x_1^2 = x_2$ — гладкая коника, касающаяся бесконечно удалённой прямой $x_0 = 0$ в точке $(0 : 0 : 1)$
- *двойная точка* $x_1^2 + x_2^2 = 0$ — аффинный конус над гладкой пустой квадрикой в $\mathbb{P}_1$
- *пересекающиеся прямые* $x_1^2 - x_2^2 = 0$ — аффинный конус над парой точек в $\mathbb{P}_1$
- *параллельные прямые* $x_1^2 = 1$ — цилиндр над парой точек в $\mathbb{A}^1$, являющийся аффинным изображением особой проективной коники, распавшейся в пару прямых, пересекающихся на бесконечности в точке $(0 : 0 : 1)$
- *двойная прямая* $x_1^2 = 0$ — цилиндр над двойной точкой в $\mathbb{A}^1$, являющийся аффинным изображением двойной проективной прямой

Как мы уже много раз отмечали, эллипс, гипербола и парабола являются различными аффинными изображениями одной и той же гладкой вещественной прективной коники Веронезе, имеющей сигнатуру $(2, 1)$.

Пример 15.14 (вещественные аффинные поверхности второй степени)
Непустые гладкие центральные аффинные поверхности второй степени в $\mathbb{R}^3$ суть

- *эллипсоид* $x_1^2 + x_2^2 + x_3^2 = 1$, который является аффинным изображением проективной квадрики сигнатуры $(3, 1)$ в карте, бесконечная гиперплоскость которой не пересекает эту проективную квадрику; эллипсоид компактен и 0-планарен
- *двуполостный гиперболоид*, который $x_1^2 + x_2^2 = x_3^2 - 1$ является аффинным изображением той же проективной квадрики сигнатуры $(3, 1)$, но в карте, бесконечная гиперплоскость которой пересекает квадрику по непустой гладкой конике; двуполостный гиперболоид 0-планарен и имеет две связных компоненты

- *однополостный гиперболоид* $x_1^2 + x_2^2 = x_3^2 + 1$, который является аффинным изображением вещественной проективной квадрики Сегре[1] в карте, бесконечная гиперплоскость которой пересекает квадрику Сегре по непустой гладкой конике; однополостный гиперболоид заметается двумя семействами прямых

Кроме того, в $\mathbb{R}^3$ имеются два параболоида:

- *эллиптический параболоид* $x_1^2 + x_2^2 = x_3$ является аффинным изображением проективной квадрики сигнатуры $(3, 1)$, которая касается бесконечно удалённой плоскости $x_0 = 0$ в точке $(0 : 0 : 1)$ и не имеет с ней никаких других точек пересечения; эллиптический параболоид 0-планарен

- *гиперболический параболоид* $x_1^2 - x_2^2 = x_3$ является аффинным изображением вещественной проективной квадрики Сегре в карте, которая касается бесконечно удалённой плоскости в точке $(0 : 0 : 1)$, пересекая её по паре прямых $x_1 = \pm x_2$; гиперболический параболоид выглядит как седло и заметается двумя семействами прямых

Остальные поверхности имеют вырожденное проективное замыкание. К ним относятся простые аффинные конусы над двумя различными гладкими вещественными прективными кониками:

- *двойная точка* $x_1^2 + x_2^2 + x_3^2 = 0$ (конус над пустой коникой)

- *эллиптический конус* $x_1^2 - x_2^2 = x_3^2$ (конус над непустой коникой)

а также цилиндры над семью кривыми второй степени в $\mathbb{R}^2$ из прим. 15.13, которые задаются ровно теми же уравнениями, но только в $\mathbb{R}^3$, а не в $\mathbb{R}^2$, и называются, соответственно, эллиптическим, гиперболическим и параболическим цилиндрами, парой параллельных плоскостей, двойной прямой, парой пересекающихся плоскостей и двойной плоскостью. Итого, в $\mathbb{R}^3$ имеется 14 аффинно неэквивалентных непустых аффинных квадрик.

[1]имеющей сигнатуру $(2, 2)$

Упр. 15.1. Переход к другому базису заключается в линейной однородной замене координат, в результате которой многочлены остаются многочленами. Если поле $\Bbbk$ конечно, то пространство функций $V \to \Bbbk$ тоже конечно, а кольцо многочленов бесконечно. Поэтому над конечным полем гомоморфизм, сопоставляющий многочлену функцию, не инъективен. Над бесконечным полем ненулевой многочлен от n переменных не может тождественно обращаться в нуль во всех точках $\Bbbk^n$. Это устанавливается индукцией по $n = \dim V$. Ненулевой многочлен $f(x)$ от одной переменной имеет не более $\deg f$ корней. Многочлен от n переменных $f(x_1, x_2, \dots, x_n) = \sum\limits_{\nu=0}^{d} \varphi_\nu(x_1, x_2, \dots, x_{n-1}) \cdot x_n^{d-\nu}$ является многочленом от одной переменной x_n с коэффициентами $\varphi_\nu \in \Bbbk[x_1, x_2, \dots, x_{n-1}]$. Вычисляя их в точке $p = (p_1, p_2, \dots, p_{n-1}) \in \Bbbk^{n-1}$, получаем многочлен от x_n с постоянными коэффициентами. Если он задаёт тождественно нулевую функцию на прямой $(x_1, x_2, \dots, x_{n-1}) = (p_1, p_2, \dots, p_{n-1})$, то все его коэффициенты нулевые. Если это происходит во всех точках $p \in \Bbbk^{n-1}$, то многочлены φ_ν оказываются тождественно нулевыми функциями на $\Bbbk^{n-1}$ и по индукции являются нулевыми многочленами.

Упр. 15.2. Надо показать, что образ отображения $\psi : V^* \to S^dV^*$, $\xi \mapsto \xi^d$, не содержится ни в какой гиперплоскости. Зафиксируем базис $x_1, x_2, \dots, x_n \in V^*$, выберем в качестве базиса в S^dV^* многочлены $\frac{d!}{m_1!\dots m_n!} x_1^{m_1} x_2^{m_2} \cdots x_n^{m_n}$ и обозначим через $a_{m_1 m_2 \dots m_n}$ координаты относительно этого базиса. Тогда ψ переводит линейную форму $\sum \alpha_i x_i$ в многочлен с координатами $a_{m_1 m_2 \dots m_n} = \alpha_1^{m_1} \alpha_2^{m_2} \cdots \alpha_n^{m_n}$. Если образ отображения ψ содержится в гиперплоскости, заданной линейным уравнением $\sum\limits_{m_1 m_2 \dots m_n} A_{m_1 m_2 \dots m_n} a_{m_1 m_2 \dots m_n} = 0$, где $A_{m_1 m_2 \dots m_n} \in \Bbbk$, то тождественно по $(\alpha_1, \alpha_2, \dots, \alpha_n) \in \Bbbk^n$ выполняется равенство $\sum\limits_{m_1 m_2 \dots m_n} A_{m_1 m_2 \dots m_n} \alpha_1^{m_1} \alpha_2^{m_2} \cdots \alpha_n^{m_n} = 0$. Поскольку поле $\Bbbk$ бесконечно, мы заключаем, что все коэффициенты $A_{m_1 m_2 \dots m_n}$ этого многочлена — нулевые. Что касается второго вопроса, то $6x_1^2 x_2 = (x_2 + x_1)^3 + (x_2 - x_1)^3 - 2x_2^3$ и аналогично для второго слагаемого.

Упр. 15.3. Зафиксируем в V какой-нибудь базис $e_1, e_2, \dots, e_n$, разложим v и w по этому базису как $v = \sum x_i e_i$ и $w = \sum y_i e_i$ и запишем q в виде (15-3). Тогда

$$q(v + w) - q(v) - q(w) = (x + y)B(x^t - y^t) - xBx^t - yBy^t = xBy^t + yBx^t = 2\, xBy^t\ .$$

(в последнем переходе мы воспользовались тем, что число yBx^t, будучи матрицей размера 1×1, совпадает со своей транспонированной версией, и в силу симметричности матрицы B равно $yBx^t = (yBx^t)^t = xB^t y^t = xBy^t$). Остальные утверждения проверяются аналогично.

Упр. 15.4. $\sigma_{f(e)}$ тождественно действует на $f(e)^\perp$ и переводит $f(e)$ в $-f(e) = f(-e)$. Композиция $f \circ \sigma_e \circ f^{-1}$ действует точно также, посколькуf^{-1} переводит $f(e)^\perp$ в $e^\perp$ в силу изометричности оператора f.

Упр. 15.7. Согласно прим. 15.1 на стр. 233, гиперболиность формы $x_1^2 + x_2^2$ равносильна тому, что -1 является квадратом в $\mathbb{F}_p$. Как мы видели в n° 3.5.2 на стр. 49, это происходит в точности при $p \equiv 1 \pmod 4$. Рассуждение про вторую форму аналогично.

Упр. 15.9. Поскольку $\tilde{q}(p, a) = 0$ для всех $a \in \mathbb{P}_n$, ограничение квадрики Q на любую прямую $(pa) \subset \mathbb{P}_n$ либо тождественно нулевое, либо вырожденное.

Упр. 15.10. Если прямая касается квадрики в точке b и пересекает её ещё в какой-нибудь точке $a \neq b$, то такая прямая целиком лежит на квадрике, поскольку матрица Грама векторов a, b тождественно нулевая. Поэтому, если точка p лежит в пересечении всех касательных пространств, то всякая проходящая через неё прямая либо больше уже нигде не пересекает квадрику, либо лежит на ней целиком. Это означает, что $p \in Q$ и все проходящие через p прямые касаются Q в точке p. Тем самым, $p \in \operatorname{Sing} Q$. Наоборот, любой элемент из $\ker \hat{q}$ лежит в пересечении $\bigcup\limits_{b \in \mathbb{P}_n} \operatorname{Ann} \hat{q}(b)$.

Упр. 15.11. Пусть σ переставляет между собою точки a_1 и a_2, а также точки b_1 и b_2. Прямые $(A_1 A_2)$ и (B_1, B_2), проходящие на $\mathbb{P}_2 = \mathbb{P}(S^2 U^*)$ через точки $A_i = \{a_i, a_i\}$ и $B_i = \{b_i, b_i\}$ коники Веронезе, пересекаются в некоторой точке $F = \{f_1, f_2\} \in \mathbb{P}_2$. Пучок проходящих через точку F прямых задаёт на конике Веронезе инволюцию, переставляющую между собою пары точек P_1, P_2, коллинеарных точке F. Эта инволюция совпадает с σ, поскольку действует на четыре точки A_1, A_2, B_1, B_2 точно так же, как и σ. Её неподвижными точками являются точки $F_1 = \{f_1, f_1\}$ и $F_2 = \{f_2, f_2\}$, в которых пересекаются с коникой Веронезе две касательные, опущенные на неё из точки F.

Упр. 15.12. Коники на $\mathbb{P}_2 = \mathbb{P}(V)$, проходящие через заданную точку $p \in \mathbb{P}_2$, образуют в пространстве коник $\mathbb{P}_5 = \mathbb{P}(S^2 V^*)$ гиперплоскость, задаваемую линейным по $q \in S^2 V^*$ уравнением $q(p) = 0$. Первое утверждение вытекает из того, что любые 5 гиперплоскостей в $\mathbb{P}_5$ имеют непустое пересечение, третье утверждение — из того, что на гладкой конике нет 3 коллинеарных точек, второе — из того, что через пять точек можно провести не более одной гладкой коники, а коника проходящая через три коллинеарные точки содержит прямую, на которой эти точки лежат.

Упр. 15.13. Первое следует из того, что проективное пространство $\mathbb{P}(S^2 V^*)$ квадрик на $\mathbb{P}_3 = \mathbb{P}(V)$ имеет размерность 9, и любые 9 гиперплоскостей в $\mathbb{P}_9$ имеют непустое пересечение. Второе — из того, что прямая, пересекающая квадрику в трёх различных точках, лежит на ней целиком. Третье — из того, что ни на одной из квадрик в $\mathbb{P}_3$, кроме гиперболической квадрики Сегре нет трёх попарно скрещивающихся прямых.

Упр. 15.14. Переход к другому реперу заключается в аффинной замене координат, которая представляет собой композицию параллельного переноса и линейного преобразования пространства V. От такой замены координат многочлен второй степени останется многочленом второй степени.