С.Н. Тронин

ВВЕДЕНИЕ В ТЕОРИЮ ГРУПП
ЗАДАЧИ И ТЕОРЕМЫ
ЧАСТЬ 2

Казань — 2006

Казанский государственный университет
им. В.И. Ульянова-Ленина

С.Н. Тронин

ВВЕДЕНИЕ В ТЕОРИЮ ГРУПП
ЗАДАЧИ И ТЕОРЕМЫ
ЧАСТЬ 2

УЧЕБНОЕ ПОСОБИЕ

Казань
2006

УДК 512

Печатается по решению
Учебно-методической комиссии
механико-математического факультета КГУ

Научный редактор
доктор физико-математических наук, профессор И.И. Сахаев

Тронин С.Н.

Введение в теорию групп. Задачи и теоремы. Часть 2.: Учебное пособие — Казань: Казанский государственный университет, 2006. 80 с.

Данное учебное пособие предназначено для студентов-математиков младших курсов. Оно может быть использовано для работы на практических занятиях по курсу алгебры как дополнение к уже имеющейся литературе, а также для самостоятельной работы. Материал пособия в целом охватывает все разделы теории групп, содержащиеся в действующей на данный момент программе курса алгебры.

СОДЕРЖАНИЕ

Введение

Данное учебное пособие предназначено для студентов-математиков, изучающих курс алгебры. В этот курс входят в качестве составной части некоторые начальные сведения из теории групп. Основам теории групп и посвящяется данное пособие.

Опишем вкратце содержание второй части. Отметим, что нумерация разделов является общей для обеих частей, так что вторая часть начинается с пятого раздела.

Задачи и теоремы пятого раздела связаны с действием групп на множествах. Это фундаментальная конструкция, работающая во многих областях математики, а не в одной только алгебре. Техника действий используется при доказательстве многих важных теорем. В данный параграф включены задачи, основанные на теоремах Силова, проясняющими сстроение конечных групп.

В шестом разделе рассматриваются линейные действия и самые простейшие понятия теории линейных представлений групп. То обстоятельство, что мы сознательно ограничились именно простейшими понятиями, существенно повлияло на тематику задач этого раздела.

Седьмой раздел содержит некоторые теоремы и задачи о группах вращений в двумерном и трехмерном евклидовом пространствах, и совсем немного — о конечных подгруппах групп вращений. В конечном счете речь идет об математических основах понятия симметрии.

Восьмой раздел посвящен кватернионам — четырехмерному обобщению поля комплексных чисел. На первый взгляд, эта тема не относится прямо к теории групп. Но, во-первых, она интерсна сама по себе, и студенту-математику будет полезен тот минимум сведений, который приведен в данном разделе. Во-вторых, кватернионы существеннейшим образом используются при доказательстве основных теорем следующего, девятого раздела, где выясняется строение специальной унитарной группы $SU(2)$ и специальной ортогональной группы $SO(3)$ — группы вращений в трехмерном евклидовом пространстве. В отличие от некоторых других учебников (например, [3]), где эти же результаты доказываются с использованием ссылок на общие теоремы линейной алгебры, мы приводим прямое доказательство, где ссылки на линейную алгебру сведены к минимуму, а известный факт о представлении каждого поворота в виде суперпозиции трех последовательных вращений вокруг осей OX, OZ и OX (“углы Эйлера") выводится как следствие.

Данное пособие охватывает весь материал теории групп, включенный в ныне действующую университетскую программу. Оно, разумеется, не может заменить подробных учебников, и не является альтернативой задачнику [4], не говоря уже о специализированном задачнике [5]. Автор надеется только, что его книга хотя бы в некоторых отношениях может служить им дополнением.

5. Действия

Напомним (см. раздел 3), что левым действием группы G на множестве X называется отображение

$$G \times X \longrightarrow X, \quad (g, x) \mapsto gx,$$

такое, что 1) $(g_1 g_2)x = g_1(g_2 x)$ для всех $g_1, g_2 \in G$, $x \in X$; 2) $1x = x$ для любого $x \in X$. Здесь $1 \in G$ — единица группы G. Правое действие определяется аналогично.

5.1. Пусть X — произвольное множество, и S_X — группа, состоящая из всех биекций $\sigma : X \to X$. Эта группа была определена в разделе 2. Определим отображение

$$S_X \times X \longrightarrow X,$$

полагая $(\sigma, x) \mapsto \sigma x = \sigma(x)$. Доказать, что это отображение является действием.

В следующих задачах обобщаются два примера действий, изучавшихся в разделе 3 — действия сдвигами и действия сопряжениями.

5.2. Пусть G — группа, X — множество всех непустых подмножеств G. Определим отображение

$$G \times X \longrightarrow X,$$

которое сопоставляет паре из элемента $g \in G$ и подмножества $A \subseteq G$ подмножество $gA \subseteq G$, состоящее из всех $ga \in G$, где $a \in A$. Доказать, что это — левое действие G на X.

В этой ситуации принято говорить, что G действует левыми сдвигами на множестве своих подмножеств.

5.3. Подобным же образом можно определить действие G на множествах X_n, состоящих из подмножеств X, в которых ровно n элементов ($n = 1, 2, \ldots, |G|$). Дайте точное определение, обоснуйте его корректность, и докажите, что это и в самом деле действие группы G.

5.4. Пусть, как и выше, G — группа, X — множество всех непустых подмножеств G. Определим отображение

$$G \times X \longrightarrow X,$$

которое сопоставляет паре из элемента $g \in G$ и подмножества $A \subseteq G$ подмножество ${}^{g}A \subseteq G$, состоящее из всех ${}^{g}a = gag^{-1} \in G$, где $a \in A$. Доказать, что это — левое действие G на X.

Для этого действия принято такое название: группа G действует слева сопряжениями на множестве своих подмножеств.

5.5. Аналогичным образом можно определить действие G на множествах X_n, состоящих из подмножеств X, в которых ровно n элементов ($n = 1, 2, \ldots, |G|$). Сформулируйте точное определение, обоснуйте его корректность, и докажите, что это и в самом деле действие группы G.

5.6. Пусть G — подгруппа группы X, $Sub(X)$ — множество всех подгрупп X. Определим отображение

$$G \times Sub(X) \longrightarrow Sub(X),$$

которое сопоставляет паре из элемента $g \in G$ и подгруппы $A \subseteq X$ подмножество ${}^{g}A = gAg^{-1} \subseteq G$, состоящее из всех ${}^{g}a = gag^{-1} \in G$, где $a \in A$. Доказать, что gAg^{-1} — подгруппа группы X, так что отображение $G \times Sub(X) \longrightarrow Sub(X)$ определено корректно. Доказать, что это отображение — левое действие G на $Sub(X)$.

Для этого действия принято такое название: группа G действует слева сопряжениями на множестве подгрупп группы X.

5.7. Подобным же образом можно определить действие G на множествах $Sub(X)_n$, состоящих из подгрупп X, чей порядок равен n ($n = 1, 2, \ldots, |X|$). Используя предыдущую задачу, дайте точное определение, обоснуйте его корректность, и докажите, что это действие группы G.

5.8. Пусть K и H — подгруппы группы G (допустим случай $K = H$). Определим отображение

$$(K \times H) \times G \longrightarrow G,$$

действующее по правилу: $((x, y), g) \mapsto (x, y)g = xgy^{-1}$. Здесь $x \in K$, $y \in H$, $g \in G$. Доказать, что это действие группы $K \times H$ на множестве G.

Орбиты этого действия называются *двойными смежными классами* группы G по K и H, и имеют вид $KgH = \{ xgy \mid x \in K, y \in H \}$ (определение орбиты см. ниже или в разделе 2). Двойные смежные классы широко используются в книге [7].

Для левых действий, построенных в предыдущих задачах, существуют и правые аналоги (определите их в явном виде!).

Пусть задано левое действие G на X, и $x \in X$. Напомним, что орбитой этого действия называется множество Gx всех элементов вида gx, где g пробегает всю группу G. Будем считать известным, что 1) $x \in Gx$; 2) если $y \in Gx$, то $Gy = Gx$; 3) если Gx и Gy — две орбиты, то либо $Gx = Gy$, либо Gx и Gy не пересекаются; 4) множество X можно представить в виде объединения попарно непересекающихся орбит.

Действие называется *транзитивным*, если у него всего одна орбита.

Множество X вместе с действием группы G будем называть *G-множеством* (левым или правым). *Гомоморфизм* из G-множества X в G-множество Y — это отображение $f : X \longrightarrow Y$, такое, что $f(gx) = gf(x)$ для всех $g \in G$ и $x \in X$.

Пример 5.1. Пусть Y — некоторое G-множество, X — некоторая его орбита. Очевидно, что ограничение на X действия G на Y является действием G на X, а включение $X \subseteq Y$, рассматриваемое как отображение, является гомоморфизмом G-множеств.

Изоморфизм G-множеств — это гомоморфизм, являющихся биекцией, причем обратная биекция также должна быть гомоморфизмом G-множеств.

Пусть X_i — семейство G-множеств, $i \in I$. Определим *копроизведение* этого семейства (обозначение: $\coprod\limits_{i \in I} X_i$) как дизъюнктное объединение множеств X_i (подмножества X_i внутри этого объединения попарно не пересекаются). Действие G на $X = \coprod_{i \in I} X_i$ определяется так: если $g \in G$, а $x \in X$, то существует однозначно определенный индекс $i \in I$ такой, что $x \in X_i$. В G-множестве X_i определено произведение $gx \in X_i$. Этот элемент по определению и будет результатом действия g на x во всем множестве X. Легко проверяется, что выполнены оба свойства из определения действия группы на множестве.

5.9. Доказать, что любое G-множество является копроизведением своих орбит.

Произведение семейства G-множеств $X_1, \ldots, X_n$ — это обычное прямое произведение множеств $X_1 \times \ldots \times X_n$, а действие G на $X = X_1 \times \ldots \times X_n$ определяется формулой: $g(x_1, \ldots, x_n) = (gx_1, \ldots, gx_n)$. В случае произвольного (бесконечного) семейства множеств определение, по сути, точно такое же. Легко проверяется, что свойства действия выполнены.

Пусть дано G-множество X и пусть $x \in X$. Определим *стабилизатор* $St(x)$ элемента x как множество тех $g \in G$, для которых $gx = x$.

5.10. Доказать, что $St(x)$ — подгруппа группы G.

5.11. Доказать, что $St(gx) = gSt(x)g^{-1}$. В частности, отсюда следует, что группа G действует слева сопряжениями на множестве своих подгрупп вида $St(x)$, где x пробегает фиксированное G-множество. (Однако взаимно-однозначного соответствия между x и $St(x)$ может не быть. Попробуйте найти пример!)

5.12. Пусть $X_1, \ldots, X_n$ — G-множества, $x_1 \in X_1, \ldots, x_n \in X_n$ и пусть $St(x_1), \ldots, St(x_n)$ — их стабилизаторы. Доказать, то стабилизатор элемента $(x_1, \ldots, x_n) \in X_1 \times \ldots \times X_n$ равен $St(x_1) \cap \ldots \cap St(x_n)$.

5.13. Пусть группа G действует сопряжениями на множестве $Sub(G)$ своих подгрупп. Показать, что для любой подгруппы $H \in Sub(G)$

1) $H \subseteq St(H)$;

2) H является нормальной подгруппой в $St(H)$;

3) H — нормальная подгруппа группы G тогда и только тогда, если $St(H) = G$.

Заметим, что подгруппа $St(H) = \{g \in G | gHg^{-1} = H\}$ из предыдущей задачи называется *нормализатором* подгруппы H, и обозначается через $N_G(H)$.

Следующий пример действия является очень важным для общей теории.

Пример 5.2. Пусть G — группа, и H — ее подгруппа. Обозначим через G/H множество различных левых смежных классов G по H, т.е. множеств вида xH (это не обязательно факторгруппа!). Определим отображение

$$G \times G/H \longrightarrow G/H,$$

полагая $(g, xH) \mapsto gxH$. Легко проверяется, что это отображение является действием. Очевидно также, что это действие транзитивно: любой элемент xH множества G/H есть произведение $x \in G$ и $H \in G/H$.

Теорема 5.1. *Пусть группа G действует на множестве X, $x \in X$, и $H = St(x)$. Тогда существует изоморфизм между G-множеством Gx (орбитой x) и G-множеством G/H, построеннном в примере 5.2. Это отображение $f : Gx \to G/H$ сопоставляет элементу gx смежный класс gH.*

Доказательство. Докажем сначала корректность определения f. Суть дела в том, что неясно, почему из $g_1x = g_2x$ следует, что $g_1H = g_2H$. Если бы это было не так, то получалось бы, что значение f зависит не от элемента орбиты Gx, а от способа его записи в виде gx. Положение спасает то, что $H = St(x)$. Ибо если $g_1x = g_2x$, то $g_1^{-1}g_2x = x$, а это значит, что $g_1^{-1}g_2 \in St(x) = H$, что равносильно равенству $g_1H = g_2H$. Чтобы показать биективность f, построим обратное отображение $r : G/H \to Gx$, которое будет сопоставлять классу gH элемент gx. Корректность этого определения обосновывается примерно так же, как и корректность определения f. А именно, если $g_1H = g_2H$, то $g_1^{-1}g_2 \in H = St(x)$, что означает равенство $g_1^{-1}g_2x = x$, или $g_1x = g_2x$. Взаимная обратность f и r очевидна из определений. Покажем, что f есть гомоморфизм G-множеств. В самом деле, пусть $x' \in Gx$. Если $x' = g'x$, то $f(x') = g'H$ и, как только что было установлено, это значение не зависит от выбора g'. Возьмем любой элемент $g \in G$. Тогда $gx' = gg'x$, и $f(gx') = gg'H = g(g'H) = gf(x')$, что и требовалось. Точно так же показывается, что если $H' \in G/H$, то $r(gH') = gr(H')$. $\square$

Биекцию между Gx и $G/St(x)$ можно также представлять себе в форме, которая описывется следующей задачей.

5.14. Пусть $y \in Gx$. Показать, что смежный класс по $St(x)$, который соответствует элементу y, есть множество $\{\ g \in G \mid gx = y\ \}$.

У теоремы 5.1 есть несколько простых, но важных следствий.

Следствие 5.1. *Пусть G — конечная группа, действующая на множестве X. Тогда мощностть любой орбиты Gx равна индексу $|G : St(x)|$ стабилизатора $St(x)$ элемента x. В частности, мощность каждой орбиты делит порядок группы $|G|$.*

Доказательство. В самом деле, если $H = St(x)$, то $|G| = |G : H|\cdot|H|$, но по теореме 5.1 $|G : H| = |G/H| = |Gx|$.$\square$

Следствие 5.2. *Пусть $|G| = p^k$, и p — простое число. Тогда центр группы G состоит более чем из одного элемента.*

Доказательство. Рассмотрим действие G на G сопряжениями, и пусть $X_1, \ldots, X_m$ — орбиты этого действия. Тогда $G = X_1 \cup \ldots \cup X_m$, и так как орбиты не пересекаются, то $|G| = p^k = |X_1| + \cdots + |X_m|$. Из предыдущего следствия вытекает, что все $|X_i|$ являются делителями $|G| = p^k$, то есть это какие-то степени простого числа p. Однако по крайней мере у одной орбиты мощность равна единице. Эта орбита — множество $\{1\}$. Если бы мощности всех остальных орбит были больше единицы, то получилось бы противоречие: левая часть равенства $|G| = |X_1| + \cdots + |X_m|$ делится на p, а правая нет. Следовательно, количество орбит, мощность которых равна единице, будет больше единицы. Но объединение всех таких орбит и является центром группы G. $\square$

5.15. Пусть G — конечная группа, $|G| = p^2$. Доказать, что либо G является циклической, либо $G \cong \mathbf{U}_p \times \mathbf{U}_p$. В частности, G коммутативна.

Указание. Пусть G не является циклической. Во-первых, надо помнить, что любая циклическая группа порядка n изоморфна $\mathbf{U}_n$, так что фактически надо искать в G две циклические подгруппы K и H, $|K| = p, |H| = p$, удовлетворяющие условиям разложения в прямое произведение. Во-вторых, можно воспользоваться следствием 5.2, в котором утверждается, что центр группы порядка p^2 отличен от единицы. Выберем в центре элемент x порядка p (почему это можно сделать?), и рассмотрим $K = \langle x \rangle = \{1, x, \ldots, x^{p-1}$. Так как $|G| = p^2$, то найдется $y \notin K$, порядок которого равен p (почему?). Положим $H = \langle y \rangle$. Тогда $G = KH$, $K \cap H = \{1\}$ (почему это так?), и для любых $a \in K$, $b \in H$ будем иметь $ab = ba$ (обоснуйте и этот факт).

Рассмотрим произвольное действие группы G на множестве X, $G \times X \to X$, $(g, x) \mapsto gx$. Пусть $g \in G$. Обозначим через $Fix(g)$ множество тех $x \in X$, для которых $gx = x$.

Теорема 5.2. (Бернсайд) *Пусть группа G и множество X конечны, и m — количество орбит действия G на X. Тогда*

$$m = \frac{1}{|G|} \sum_{g \in G} |Fix(g)|.$$

Доказательство. Пусть $X_1, \ldots, X_m$ — различные орбиты действия G на X. В частности, $|X| = |X_1| + \cdots + |X_m|$. Рассмотрим множество

$$Y = \{\ (g, x) \mid g \in G, x \in X, gx = x\ \},$$

и представим его в виде некоторых объединений непересекающихся подмножеств двумя разными способами. С одной стороны,

$$Y = \bigcup_{i=1}^{m} \bigcup_{x \in X_i} \{(g, x) | gx = x\} \qquad (1)$$

Очевидно, что если $x \neq y$, то $\{(g,x)|gx = x\} \cap \{(g,y)|gy = y\} = \emptyset$. Заметим еще, что если зафиксировать x, то существует очевидное взаимнооднозначное соответствие между множеством $\{(g,x)|gx = x\}$ и $St(x) = \{g|gx = x\}$. Кроме того, если x, y принадлежат одной и той же орбите X_i, то из стабилизаторы сопряжены, и потому их порядки (мощности) одинаковы. Напомним, что если $x \in X_i$, то (по теореме Лагранжа и по теореме 5.1) $|G| = |X_i| \cdot |St(x)|$. Поэтому порядки стабилизаторов всех элементов, принадлежащих к одной и той же орбите, равны $|G|/|X_i|$. Вычисляя мощности множеств, стоящих в левой и правой частях равенства (1), получим равенство:

$$|Y| = \sum_{i=1}^{m} \sum_{x \in X_i} \frac{|G|}{|X_i|} = \sum_{i=1}^{m} \frac{|G|}{|X_i|} (\sum_{x \in X_i} 1) = \sum_{i=1}^{m} \frac{|G|}{|X_i|} |X_i| = \sum_{i=1}^{m} |G| = m|G| \tag{2}$$

С другой стороны, представим Y таким образом:

$$Y = \bigcup_{g \in G} \{(g,x)|gx = x\} \tag{3}$$

Очевидно, что при фиксированном $g \in G$ существует взаимнооднозначное соответствие между множеством $\{(g,x)|gx = x\}$ и множеством $Fix(g) = \{x|gx = x\}$. Если $g_1 \neq g_2$ фиксированы, то множества $\{(g_1,x)|g_1x = x\}$ и $\{(g_2,x)|g_2x = x\}$ не пересекаются. Таким образом, вычисляя мощности множеств в левой и правой частях равенства (3), получим следующее:

$$|Y| = \sum_{g \in G} |\{(g,x)|gx = x\}| = \sum_{g \in G} |Fix(g)| \tag{4}$$

Сравнивая (2) и (4), приходим к равенству:

$$m|G| = \sum_{g \in G} |Fix(g)|,$$

из которого и следует утверждение теоремы. □

Следующая конструкция также является очень важной. Пусть дано действие G на X. Обозначим через φ отображение $G \times X \to X$. Таким образом, свойства действия записываются в виде:

1) $\varphi(g_1 g_2, x) = \varphi(g_1, \varphi(g_2, x))$;

2) $\varphi(1, x) = x$.

Зафиксируем $g \in G$, и рассмотрим отображение $T_\varphi(g) : x \mapsto \varphi(g, x)$. Это отображение биективно: обратным к нему является отображение $T_\varphi(g^{-1}) : x \mapsto \varphi(g^{-1}, x)$. Таким образом, $T_\varphi(g) \in S_X$ для всех $g \in G$, и соответствие $T_\varphi : g \mapsto T_\varphi(g)$ задает отображение $T_\varphi : G \longrightarrow S_X$. Напомним, что группа S_X определена в разделе 1.

Обратно, пусть дан гомоморфизм групп $T : G \longrightarrow S_X$. Сопоставим ему отображение $\varphi_T : G \times X \to X$, полагая $\varphi_T(g, x) = T(g)(x)$. Это надо понимать так. Элементу $g \in G$ сопоставляется элемент $T(g) \in S_X$, который сам является отображением из X в X. Его значение на аргументе $x \in X$ и обозначается через $T(g)(x)$.

Теорема 5.3. *Отображение T_φ, построенное выше по действию φ, является гомоморфизмом групп. Отображение φ_T, построенное по гомоморфизму T, является действием G на X. Имеет место взаимно-однозначное соответствие между действиями G на X, и гомоморфизмами из G в S_X, которое определяется так: $\varphi \mapsto T_\varphi$, $T \mapsto \varphi_T$.*

5.16. Проведите подробное доказательство этой теоремы.

5.17. Пусть $\varphi : G \times X \to X$ — некоторое действие, и $T_\varphi : G \to S_X$ — соответствующий ему гомоморфизм. Доказать, что

$$Ker(T_\varphi) = \bigcap_{x \in X} St(x).$$

5.18. Пусть G — группа, которая действует на себе самой сопряжениями, и $T : G \longrightarrow S_G$ — гомоморфизм, соответствующий этому действию. Доказать, что $Ker(T) = C(G)$ (напомним, что $C(G)$ — центр группы G).

5.19. Пусть X — группа, G — подгруппа группы X, и задано действие G на X левыми сдвигами. Рассмотрим соответствующий этому действию гомоморфизм $T : G \longrightarrow S_X$. Доказать, что отображение T инъективно.

Сделаем еще несколько замечаний о группах вида S_X. Суть дела в том, что если есть биекция между множествами X и Y, то есть и изоморфизм между группами S_X и S_Y. Его формальное построение таково. Пусть $\gamma : X \longrightarrow Y$ — биекция. Тогда отображение $\widetilde{\gamma} : S_X \longrightarrow S_Y$ задается правилом: $\widetilde{\gamma}(\sigma) = \widetilde{\sigma} = \gamma\sigma\gamma^{-1}$. Обратное отображение определяется так: $\tau \mapsto \gamma^{-1}\tau\gamma$.

5.20. Проверить, что построенные выше отображения взаимно обратны, и $\widetilde{\gamma}$ — гомоморфизм групп, а следовательно — изоморфизм.

На практике все выглядит очень просто. Рассмотрим, например, взаимно-однозначное соответствие между множествами $\{1, 2, \ldots, n\}$ и $X = \{x_1, x_2, \ldots, x_n\}$, где $i \mapsto x_i$. Элементы группы S_X можно, как и “обычные"подстановки, изображать в табличной форме. Запись биекции $\tau : X \to X$ в виде

$$\tau = \begin{pmatrix} x_1 & x_2 & \ldots & x_n \\ x_{i_1} & x_{i_2} & \ldots & x_{i_n} \end{pmatrix}$$

означает, что $\tau(x_1) = x_{i_1}$, $\tau(x_2) = x_{i_2}$, ..., $\tau(x_n) = x_{i_n}$. И тогда изоморфизм между S_n и S_X задается соответствием:

$$\begin{pmatrix} 1 & 2 & \ldots & n \\ i_1 & i_2 & \ldots & i_n \end{pmatrix} \mapsto \begin{pmatrix} x_1 & x_2 & \ldots & x_n \\ x_{i_1} & x_{i_2} & \ldots & x_{i_n} \end{pmatrix}.$$

Вследствие этого будем в дальнейшем называть группами подстановок любые группы вида S_X для конечных X. Все методы и результаты раздела 1 справедливы и для этих групп. В частности, можно определить циклы, а элементы из S_X можно раскладывать в произведения независимых циклов. Если, как и выше, перенумеровать элементы X, то суперпозиция изоморфизма $S_n \cong S_X$ и гомоморфизма $sgn : S_n \to \{\pm 1\}$ не зависит от выбора биекции между X и множеством $\{1, 2, \ldots, n\}$. В самом деле, из результата задачи **5.20** следует, что если есть два изоморфизма между S_X и S_n, построенные из двух разных биекций между X и $\{1, 2, \ldots, n\}$, то существует подстановка $\omega \in S_n$, такая, что образы σ_1 и σ_2 одного и того же τ связаны соотношением $\sigma_2 = \omega\sigma_1\omega^{-1}$. Но в этом случае $sgn(\sigma_2) = sgn(\sigma_1)$.

5.21. Докажите последние утверждения.

Итак, гомоморфизм sgn (знак подстановки) корректно определен для произвольного S_X, а это значит, что в этом общем случае существуют и знакопеременные группы, которые можно обозначить через A_X. При этом $A_X \cong A_n$ (докажите это!).

Следствием задачи **5.19** является известная *теорема Кэли*:

Теорема 5.4. *Любая конечная группа изоморфна подгруппе группы подстановок.*

Более конкретно, если $G = \{g_1, g_2, \dots, g_n\}$ и $g \in G$, то $\{g_1, g_2, \dots, g_n\} = \{gg_1, gg_2, \dots, gg_n\}$, и имеет место инъективный гомоморфизм из G в $S_n \cong S_G$, который сопоставляет элементу $g \in G$ подстановку

$$\begin{pmatrix} g_1 & g_2 & \cdots & g_n \\ gg_1 & gg_2 & \cdots & gg_n \end{pmatrix}.$$

Образ этого гомоморфизма — подгруппа группы подстановок, изоморфная G. Будем для удобства называть этот гомоморфизм *гомоморфизмом Кэли* для группы G. В литературе можно встретить более громоздкое название: левое регулярное (подстановочное) представление группы G.

5.22. Уточнить вид гомоморфизма Кэли следующим образом. Пусть $g \in G$, и k — порядок g. Пусть $x_1, \dots, x_m$ — полная система представителей правых смежных классов G по подгруппе $\langle x \rangle = \{1, g, g^2, \dots, g^{k-1}\}$. Здесь $|G| = n = km$. Доказать, что подстановка

$$\begin{pmatrix} g_1 & g_2 & \cdots & g_n \\ gg_1 & gg_2 & \cdots & gg_n \end{pmatrix}$$

разлагается в произведение независимых циклов следующим образом:

$$(x_1, gx_1, g^2x_1, \dots, g^{k-1}x_1) \dots (x_m, gx_m, g^2x_m, \dots, g^{k-1}x_m).$$

5.23. Рассмотреть суперпозицию гомоморфизмов Кэли $G \to S_G$ и $S_G \to S_{S_G}$. Показать, что образ G в S_{S_G} принадлежит к знакопеременной группе A_{S_G}.

Указание. Образ элемента $g \in G$ в группе S_G так же, как и g, имеет порядок k. Чему равен индекс в S_G подгруппы, порожденной этим элементом? В произведение скольки циклов раскладывается в S_{S_G} образ g и каковы длины этих циклов? Зная все это, можно вычислить знак этого образа как подстановки из S_{S_G}.

Таким образом, любая конечная группа G изоморфна подгруппе некоторой группы четных подстановок.

Рассмотрим теперь действие $G \times G/H \to G/H$, $(g, xH) \mapsto gxH$, и изучим соответствующий ему гомоморфизм $T : G \longrightarrow S_{G/H}$. При $H = \{1\}$ это в точности гомоморфизм Кэли. Ввиду этого будем называть T гомоморфизмом Кэли группы G по подгруппе H.

5.24. Показать, что если $\{x_1, \ldots, x_m\}$ — некоторая полная система представителей левых смежных классов G по H, то гомоморфизм Кэли T отображает элемент $g \in G$ в подстановку

$$T(g) = \begin{pmatrix} x_1H & x_2H & \ldots & x_mH \\ gx_1H & gx_2H & \ldots & gx_mH \end{pmatrix}.$$

5.25. Сохраним условия и обозначения предыдущей задачи. Доказать, что $Ker(T) \subseteq H$, и равенство $Ker(T) = H$ имеет место тогда и только тогда, когда H — нормальная подгруппа.

Доказательство можно начать с проверки того, что

$$Ker(T) = \bigcap_{g \in G} gHg^{-1}.$$

Вывести отсюда, что если H — нормальная подгруппа, то образ T (подгруппа $S_{G/H}$) изоморфен факторгруппе G/H.

5.26. Пусть K и H — подгруппы группы G. Рассмотрим действие $K \times H$ на G, определенное по правилу $(x, y)g = xgy^{-1}$. Пусть $T : K \times H \to S_G$ — соответствующий этому действию гомоморфизм. Доказать, что $Ker(T) \cong K \cap H$.

В следующей серии задач изучается группа G порядка $|G| = p^r l$, где p — простое число и l не делится на p. Зафиксируем целое число k, $1 \le k \le r$, и пусть X есть множество всех подмножеств G, состоящих ровно из p^k элементов.

5.27. Доказать, что мощность X есть целое число, которое делится на p^{r-k}, и не делится на p^{r-k+1}.

Указание. Установить сначала формулу

$$|X| = C_{p^r l}^{p^k} = p^{r-k} l \prod_{j=1}^{p^k - 1} \frac{p^r l - j}{j} .$$

5.28. Рассмотрим действие левыми сдвигами G на X, определяемое формулой $(g, A) \mapsto gA = \{\, ga \,|\, a \in A \,\}$ (проверьте корректность определения и свойства действия). Доказать, что у этого действия существует орбита, мощность которой не делится на p^{r-k+1}.

Указание: предположить противное, и использовать результат предыдущей задачи.

5.29. Пусть $Y = \{A_1, \ldots, A_s\}$ — орбита, существование которой устанавливается в предыдущей задаче (т.е. s не делится на p^{r-k+1}). Из общих свойств орбит следует, что $Y = GA_1$. Положим $H = St(A_1)$, $t = |H|$. Тогда $|G| = p^r l = st$ (почему?). По определению H как стабилизатора A_1 для каждого $a \in A_1$ имеет место включение $Ha \subseteq A_1$. Отсюда следует, что $t = |H| \leq p^k$ (почему?). Далее, сопоставьте два обстоятельства: s не делится на p^{r-k+1} и $p^r l = st$. Что можно сказать теперь о величине $t = |H|$?

Из этих трех задач выводится следующая теорема.

Теорема 5.5. *Пусть G — конечная группа, $|G| = p^r l$, где p — простое число и l не делится на p. Тогда для каждого k, $1 \leq k \leq r$ в группе G существует подгруппа порядка p^k.*

Эту теорему называют еще *первой теоремой Силова*. Впрочем, чаще под первой теоремой Силова понимают следующее утверждение.

Теорема 5.6. *Пусть G — конечная группа, $|G| = p^r l$, где p — простое число и l не делится на p. Тогда для каждого k, $1 \leq k \leq r$ в группе G существует подгруппа порядка p^k. Каждая подгруппа H порядка p^k при $k < r$ содержится по крайней мере в одной подгруппе K порядка p^{k+1}, причем K можно выбрать так, чтобы H была нормальной подгруппой группы K.*

Пусть p — простое число. Группа называется *p-группой*, если порядок каждого ее элемента равен некоторой степени числа p. Из первой теоремы Силова следует, что порядок любой конечной p-группы есть степень числа p. Пусть $|G| = p^r l$, и l не делится на p. Подгруппы группы G, имеющие порядок p^r, которые существуют по первой теореме Силова, называются *силовскими p-подгруппами* группы G.

Теорема 5.7. (Вторая теорема Силова). *В конечной группе G любые две силовские p-подгруппы сопряжены.*

Напомним, что это означает следующее. Если H_1 и H_2 — силовские p-группы, то существует $g \in G$ такой, что $H_2 = gHg^{-1}$.

Теорема 5.8. (Третья теорема Силова). *В конечной группе G количество силовских p-подгрупп равно $1 + pj$ для некоторого j, причем это число делит порядок группы G.*

5.30. Пусть p_1 и p_2 — простые числа, делящие порядок группы $|G|$, и $p_1 \neq p_2$. Допустим, что H_1 — p_1-подгруппа, и H_2 — p_2- подгруппа группы G. Доказать, что $H_1 \cap H_2 = \{1\}$.

5.31. Пусть p_1 и p_2 — простые числа, делящие порядок группы $|G|$, и $p_1 \neq p_2$. Допустим, что H_1 — силовская p_1-подгруппа, и H_2 — силовская p_2-подгруппа группы G. Предположим еще, что $|G| = p_1^r p_2^s$. Доказать, что $H_1 H_2 = G$.

5.32. Пусть p_1 и p_2 — простые числа, делящие порядок группы $|G|$, и $p_1 \neq p_2$. Пусть H_1 — силовская p_1-подгруппа, и H_2 — силовская p_2-подгруппа группы G. Предположим, как и выше, что $|G| = p_1^r p_2^s$, и допустим, что группа G коммутативна. Доказать, что $G \cong H_1 \times H_2$.

5.33. Пусть G — конечная коммутативная группа. Доказать, что группа G изоморфна прямому произведению своих силовских p-подгрупп по всем простым p, делящим порядок G.

5.34. Пусть дано действие $G \times X \to X$, где $|X| = m$, $|G| = p^n$, p — простое число и m не делится на p. Доказать, что у этого действия существует по крайней мере одна одноэлементная орбита.

5.35. Пусть дано действие $G \times X \to X$, где $|X| = m$, $|G| = p^n$, p — простое число. Доказать, что если у этого действия нет одноэлементных орбит, то m делится на p.

5.36. Пусть дано действие $G \times X \to X$, где $|G| = p^n l$, p — простое число и l не делится на p. Допустим, что стабилизаторы всех элементов X имеют порядки вида p^k. Доказать, что $|X|$ делится на l.

5.37. Пусть K, H — подгруппы конечной группы G, $|K| = p^r$, $|G : H| = m$, p — простое число и m не делится на p. Рассмотрим действие K левыми сдвигами на множестве $G/H = \{x_1 H, \ldots, x_m H\}$: $x(x_i H) = x x_i H$. Доказать, что существует орбита из одного элемента. Вывести отсюда, что группа K изоморфна некоторой подгруппе H.

Указание. Пусть $x_i H$ — одноэлементная орбита действия K на G/H. Покажите, что для каждого $x \in K$ имеет место включение $x_i^{-1} x x_i \in H$. Исходя из этого, можно определить отображение $\alpha : K \to H$ следующим образом: $\alpha(x) = x_i^{-1} x x_i$. Остается доказать, что α — инъективный гомоморфизм групп.

6. Представления

Часто встречаются случаи, когда группа G действует не на произвольном множестве, а на линейном пространстве V над полем F. Точное определение таково. Дано отображение

$$G \times V \longrightarrow V,$$

сопоставляющее паре (g, v), где $g \in G$, $v \in V$, элемент $gv \in V$. Это отображение называется *линейным действием* G на V, если выполняются следующие три свойства:

1) $(g_1 g_2)v = g_1(g_2 v)$;

2) $1v = v$;

3) $g(v_1\lambda_1 + v_2\lambda_2) = (gv_1)\lambda_1 + (gv_2)\lambda_2$, где $v_1, v_2 \in V$, $\lambda_1, \lambda_2 \in F$.

Здесь используется правосторонняя форма записи умножения на скаляры (элементы поля) в линейном пространстве. Эта форма является самой естественной, когда рассматриваются векторы-столбцы (векторы-строки, напротив, естественно умножать на скаляры слева). Впрочем, во многих случаях (например, когда не возникает необходимости рассматривать матрицы линейных преобразований), форма записи умножения векторов на элементы поля не играет особой роли, и можно использовать левостороннее умножение. Тем более, что запись вида $3v$ выглядит гораздо привычнее, чем $v3$.

Пространство V вместе с заданным линейным действием G называется еще (левым) *G-модулем.* Ясно, что любой G-модуль является и G-множеством, так что к G-модулям в принципе применимы все описанные выше конструкции и результаты. Однако, как правило, в теории G-модулей появляется много свойственных только ей особенностей. Например, если V_1 и V_2 — два G-модуля, то *гомоморфизмом G-модулей* называется линейное отображение $h : V_1 \longrightarrow V_2$, являющееся также гомоморфизмом G-множеств. Роль копроизведений играют прямые суммы линейных пространств, а понятие орбиты отходит на второй план. Вместо него используется понятие простого G-модуля, т.е. G-модуля, у которого отсутствуют нетривиальные подмодули. В ряде важных случаев удается доказать аналоги утверждения о том, что G-множество является объединением непересекающихся орбит. Например, если поле F является полем комплексных чисел $\mathbb{C}$, группа G конечна, и G-модуль V как линейное пространство имеет конечную размерность, то он является (точнее, изоморфен) прямой сумме простых G-модулей. Это доказывается в теории линейных представлений групп (см., например, [17], а также главы о представлениях в книгах [3], [7], [10], [11]).

Выясним, как для линейных действий выглядит аналог взаимно-однозначного соответствия между действиями и гомоморфизмами. Ту роль, которую в этом соответствии играли группы S_X, в данном случае будут играть другие группы, которые описываютя ниже.

Пусть V — линейное пространство над полем F. Обозначим через $GL(V)$ множество всех биективных линейных отображений из V в V. Определим на этом множестве структуру группы. Пусть $\varphi, \psi \in GL(V)$. Тогда их суперпозиция $\varphi\psi$ снова является биективным линейным отображением из V в V. Таким образом, определена бинарная операция (умножение):

$$GL(V) \times GL(V) \longrightarrow GL(V), \quad (\varphi, \psi) \mapsto \varphi\psi.$$

Суперпозиция функций является, как известно, ассоциативной операцией. Тождественное отображение $1_V : V \to V$ является линейным, и играет роль единицы для этой операции. Наконец, если φ — линейная биекция, то обратное отображение φ^{-1} также будет и биективным, и линейным. Следовательно, все свойства из определения группы для $GL(V)$ выполнены. Очевидно также, что $GL(V)$ является подгруппой группы S_V.

6.1. Рассмотрим отображение

$$GL(V) \times V \longrightarrow V,$$

которое сопоставляет паре (φ, v) элемент $\varphi(v)$. Доказать, что это — линейное действие $GL(V)$ на V.

Пусть задано некоторое линейное действие G на V. Обозначим его через $\alpha : G \times V \to V$. Таким образом, должны выполняться соотношения:

1) $\alpha(g_1 g_2, v) = \alpha(g_1, \alpha(g_2, v))$;

2) $\alpha(1, v) = v$;

3) $\alpha(g, v_1\lambda_1 + v_2\lambda_2) = \alpha(g, v_1)\lambda_1 + \alpha(g, v_2)\lambda_2$.

Рассуждая так же, как и для нелинейных действий, можно построить гомоморфизм групп $T_\alpha : G \longrightarrow S_V$, сопоставляющий элементу $g \in G$ биективное отображение $T_\alpha(g) : V \longrightarrow V$, которое действует по правилу $T_\alpha(g)(v) = \alpha(g, v)$. Но из условия 3) сразу следует, что $T_\alpha(g)(v_1\lambda_1 + v_2\lambda_2) = T_\alpha(g)(v_1)\lambda_1 + T_\alpha(g)(v_2)\lambda_2$. Таким образом, $T_\alpha(g) \in GL(V)$, а это означачает, что имеет место гомоморфизм $T_\alpha : G \longrightarrow GL(V)$.

Обратно, пусть дано гомоморфизм $T : G \longrightarrow GL(V)$. Рассматривая его сначала как гомоморфизм в S_V (ввиду того, что $GL(V)$ — подгруппа в S_V), строим действие $\alpha_T : G \times V \to V$ группы G на множестве V по правилу: $\alpha_T(g, v) = T(g)(v)$. Свойство линейности отображения $T(g)$ (т.е. свойство $T(g)(v_1\lambda_1 + v_2\lambda_2) = T(g)(v_1)\lambda_1 + T(g)(v_2)\lambda_2$) превращается в условие линейности действия: $\alpha_T(g, v_1\lambda_1 + v_2\lambda_2) = \alpha_T(g, v_1)\lambda_1 + \alpha_T(g, v_2)\lambda_2$.

В конечном счете имеет место следующая теорема.

Теорема 6.1. *Существует взаимно-однозначное соответствие между линейными действиями G на V, и гомоморфизмами групп $G \longrightarrow GL(V)$. Это соответствие задается описанными выше конструкциями: $\alpha \mapsto T_\alpha$, $T \mapsto \alpha_T$.*

Напомним, что если в пространстве V задан базис (например, $e_1, \ldots, e_n$), то существует взаимно-однозначное соответствие между линейными отображениями $\varphi : V \to V$ и квадратными $n \times n$-матрицами над полем F. Построение этого соответствия начинается с соотношения

$$\varphi(e_j) = \sum_{i=1}^{n} e_i a_{i,j},$$

где $a_{i,j} \in F$. Линейному отображению φ ставится в соответствие матрица M_φ с компонентами $a_{i,j}$. При этом суперпозиции линейных отображений $\varphi\psi$ соответствует умножение матриц: $M_{\varphi\psi} = M_\varphi M_\psi$. Заметим, что здесь правостороннее умножение векторов на элементы поля весьма облегчает доказательство. Тождественному линейному отображению соответствует единичная матрица. Из всего этого следует, что соответствие $\varphi \mapsto M_\varphi$ является изоморфизмом между группой $GL(V)$ и группой $GL_n(F)$ всех невырожденных $n \times n$-матриц над полем F.

Гомоморфизмы вида $T : G \to GL(V)$ или $T : G \to GL_n(F)$ называются *линейными представлениями* группы G над полем F (точнее, n-мерными представлениями, $n = dim(V)$).

6.2. Каково представление, соответствующее линейному действию

$$GL(V) \times V \longrightarrow V, \quad (\varphi, v) \mapsto \varphi(v) \ ?$$

По любому множеству X можно построить линейное пространство с базисом X. Его элементами являются (формальные) линейные комбинации $\sum\limits_{x \in X} x\lambda_x$, где $\lambda_x \in F$ и почти все $\lambda_x = 0$. Если на X задано действие группы G, то на V_X естественным образом определяется линейное действие G:

$$g(\sum_{x \in X} x\lambda_x) = \sum_{x \in X} (gx)\lambda_x \qquad (*)$$

6.3. Проверить, что формула (*) задает линейное действие.

6.4. Предположим, что группа G действует на конечном множестве $X, |X| = n$. Доказать, что линейное представление группы G, соответствующее действию (*), можно представить как суперпозицию двух гомоморфизмов:

$$T : G \longrightarrow S_n \ \text{ и } \ M : S_n \longrightarrow GL_n(F),$$

где T — гомоморфизм, соответствующий действию G на X, а M сопоставляет подстановке σ матрицу $M(\sigma)$, определенную в конце раздела 2 (там же показано, что $\sigma \mapsto M(\sigma)$ — инъективный гомоморфизм групп).

6.5. Пусть V_1 и V_2 — два G- модуля. Рассмотрим прямую сумму $V_1 \oplus V_2$ пространств V_1 и V_2. Элементы $V_1 \oplus V_2$ будем записывать в виде (v_1, v_2), где $v_1 \in V_1$, $v_2 \in V_2$. Напомним, что операции сложения, вычитания и умножения на элементы поля определяются в $V_1 \oplus V_2$ покомпонентно. Рассмотрим отображение

$$G \times (V_1 \oplus V_2) \longrightarrow V_1 \oplus V_2,$$

задаваемое по правилу $(g, (v_1, v_2)) \mapsto g(v_1, v_2) = (gv_1, gv_2)$. Докажите, что это — линейное действие G на $V_1 \oplus V_2$. Определенный таким способом G-модуль $V_1 \oplus V_2$ называется *прямой суммой* G-модулей V_1 и V_2. Выберем в V_1 базис $e_1, \dots, e_n$, а в V_2 — базис $e_{n+1}, \dots, e_{n+m}$. Тогда можно считать, что представления, соответствующие G-модулям V_1 и V_2 — это гомоморфизмы $T_1 : G \to GL_n(F)$ и $T_2 : G \to GL_m(F)$. Как известно из линейной алгебры, множество $e_1, \dots, e_n, e_{n+1}, \dots, e_{n+m}$ будет базисом прямой суммы $V_1 \oplus V_2$ (здесь мы уже считаем V_1 и V_2 подпространствами $V_1 \oplus V_2$ и отождествляем e_i с $(e_i, 0)$ при $1 \leq i \leq n$, и e_j с $(0, e_j)$ при $n+1 \leq j \leq n+m$). Докажите, что представление, соответствующее G-модулю $V_1 \oplus V_2$, т.е. в данном случае гомоморфизм $T : G \longrightarrow GL_{n+m}(F)$ имеет при данном выборе базиса следующий вид:

$$T(g) = \begin{pmatrix} T_1(g) & 0 \\ 0 & T_2(g) \end{pmatrix}.$$

6.6. Пусть V — некоторый G-модуль ($n = dim(V) < \infty$), и V_1 — G-*подмодуль* модуля V. Это означает, что для каждого $g \in G$ и любого $v \in V_1$ элемент gv снова принадлежит V_1, то есть ограничение действия G с V на V_1 будет линейным действием G на V_1. Выберем какой-нибудь базис $e_1, \dots, e_k$ в V_1, и дополним его элементами $e_{k+1}, \dots, e_n$ до базиса V. Рассмотрим представление T, соответствующее G-модулю V. Это гомоморфизм G $GL_n(F)$. Докажите, что матрицы $T(g)$ в выбранном базисе имеют следующий блочно-треугольный вид:

$$T(g) = \begin{pmatrix} T_1(g) & B(g) \\ 0 & T_2(g) \end{pmatrix},$$

где $T_1(g)$ — блоки размером $k\times k$, $T_2(g)$ — блоки размером $(n-k)\times(n-k)$. Докажите, что отображение $g \mapsto T_1(g)$ является линейным представлением, соответствующим G-модулю V_1, а отображение $g \mapsto T_2(g)$ является линейным представлением, соответствующим линейному действию G на $V_2 = V/V_1$, которое строится следующим образом: умножение $g \in G$ на смежный класс $v + V_1$ определяется по правилу $g(v + V_1) = gv + V_1$. Необходимо предварительно доказать корректность этого определения (то, что $gv + V_1$ не зависит от выбора представителя смежного класса v) и проверить все свойства линейного действия.

Построенный так G-модуль V/V_1 называется *фактормодулем* модуля V по подмодулю V_1.

С помощью матриц подстановок задаются инъективные гомоморфизмы из S_n в $GL_n(F)$. Оказывается, что можно определить инъективные гомоморфизмы S_n и в $GL_{n-1}(F)$. Прежде всего, заметим, что гомоморфизм $M : S_n \to GL_n(F)$ — это представление, соответствующее действию S_n на n-мерном линейном пространстве V с базисом $e_1, \dots, e_n$, которое опеределяется по правилу: $\sigma e_i = e_{\sigma(i)}$ (проверьте это!). Теперь можно использовать технику предыдущей задачи. Начнем со случая $n = 3$.

6.7. Пусть $n = 3$, и F – одно из полей $\mathbb{Q}, \mathbb{R}, \mathbb{C}$. Рассмотрим в $V = \langle e_1, e_2, e_3\rangle$ подпространство V_1 с базисом $v_1 = e_1 - e_2$, $v_2 = e_1 - e_3$. Доказать, что это подпространство состоит из всех тех линейных комбинаций $e_1\lambda_1 + e_2\lambda_2 + e_3\lambda_3$, в которых $\lambda_1 + \lambda_2 + \lambda_3 = 0$. Доказать далее, что V_1 является S_3-подмодулем в V. Построить в явном виде соответствующее ему представление (гомоморфизм из S_3 в $GL_2(F)$) и установить его инъективность.

6.8. Пусть F – одно из полей $\mathbb{Q}, \mathbb{R}, \mathbb{C}$. Рассмотрим n-мерное пространство V с базисом $e_1, e_2, \dots, e_n$ как S_n- модуль, линейное действие на котором задается по правилу $\sigma(e_1\lambda_1+e_2\lambda_2+\dots+e_n\lambda_n) = e_{\sigma(1)}\lambda_1+e_{\sigma(2)}\lambda_2+\dots+e_{\sigma(n)}\lambda_n$. Пусть V_1 — подпространство V, состоящее из всех тех линейных комбинаций $e_1\lambda_1 + e_2\lambda_2 + \dots + e_n\lambda_n$, для которых $\lambda_1 + \lambda_2 + \dots + \lambda_n = 0$. Доказать, что это S_n-подмодуль, и что базисом V_1 является множество $v_1 = e_1 - e_2$, $v_2 = e_1 - e_3$, $\dots$, $v_{n-1} = e_1 - e_n$. Не строя в явном виде соответствующее ему представление (гомоморфизм $T : S_n \to GL_{n-1}(F)$), доказать его инъективность.

Указание. Достаточно вычислить ядро T, которое состоит из всех тех $\sigma \in S_n$, для которых $T(\sigma)$ равен единичной матрице. То есть должны выполняться равенства $T(\sigma)(v_1) = v_1$, $T(\sigma)(v_2) = v_2$, $\ldots$, $T(\sigma)(v_{n-1}) = v_{n-1}$. Для каких подстановок σ выполнены все эти равенства?

6.9. Пусть V есть пространство всех многочленов от переменных x_1, x_2, x_3, x_4 вида $\sum\limits_{1 \le i < j \le 4} a_{i,j} x_i x_j$. Группа S_4 действует линейно на этом пространстве по правилу $\sigma(x_i x_j) = x_{\sigma(i)} x_{\sigma(j)}$ (обоснуйте это). Доказать, что подпространство $W = \langle x_1x_2 - x_3x_4, x_1x_3 - x_2x_4, x_1x_4 - x_2x_3 \rangle$ является S_4-подмодулем V. Построить соответствующее представление. Будет ли этот гомоморфизм инъективным?

6.10. Пусть V есть пространство всех многочленов от переменных x_1, x_2, x_3, x_4 вида $\sum\limits_{1 \le i < j \le 4} a_{i,j} x_i x_j$. Группа S_4 действует линейно на этом пространстве по правилу $\sigma(x_i x_j) = x_{\sigma(i)} x_{\sigma(j)}$ (обоснуйте это). Рассмотрим подпространство $W = \langle w_1, w_2 \rangle$, где $w_1 = x_1x_2 + x_3x_4 - x_2x_3 - x_1x_4$, $w_2 = x_1x_3 + x_2x_4 - x_1x_4 - x_2x_3$. Доказать, что W является S_4-подмодулем V. Построить соответствующее представление. Будет ли этот гомоморфизм инъективным?

6.11. Пусть V есть пространство всех многочленов от переменных x_1, x_2, x_3, x_4 вида $\sum\limits_{1 \le i < j < k \le 4} a_{i,j,k} x_i x_j x_k$. Группа S_4 действует линейно на этом пространстве по правилу $\sigma(x_i x_j x_k) = x_{\sigma(i)} x_{\sigma(j)} x_{\sigma(k)}$. Доказать, что подпространство $W = \langle x_1x_2x_3 - x_1x_3x_4, x_1x_2x_3 - x_1x_2x_4, x_1x_2x_4 - x_2x_3x_4 \rangle$ является S_4-подмодулем V. Построить соответствующее представление. Будет ли этот гомоморфизм инъективным?

Вернемся к ситуации, когда G действует на X, и линейно действует на пространстве V_X, базисом которого является множество X, по формуле (*). Особый интерес представляет случай, когда $X = G$. Для V_G имеется общеупотребительное обозначение FG (напомним, что F — поле), и на этом линейном пространстве можно вввести структуру ассоциативного кольца с единицей следующим образом:

$$(\sum_{x \in G} x\lambda_x)(\sum_{y \in G} x\mu_x) = (\sum_{g \in G} g \sum_{x,y;xy=g} \lambda_x \mu_y).$$

Кольцо FG называется *групповым кольцом* группы G над полем F, или же *групповой алгеброй* G над F. Фактически базисные элементы x, y перемножаются как элементы группы G, произведение элементов $x\lambda_x$ и $y\mu_y$ равно $(xy)\lambda_x\mu_y$ (коэффициенты λ_x и μ_x перемножаются как элементы поля F), а умножние произвольные линейных комбинаций производится по обычным правилам умножения сумм с учетом способа умножения слагаемых. Далее просто надо "привести подобные члены". Единицей кольца FG является единица группы G. Поле F отождествляется с подкольцом FG, состоящим из элементов вида $1_G\lambda$, $\lambda \in F$ (1_G — единица группы G, в дальнейшем обозначаемая просто как 1). Гомоморфизм F в FG, осуществляющий это отождествление, действует по правилу $\lambda \mapsto 1_G\lambda$. Ввиду этого выражения $x\lambda_x$ можно рассматривать как произведения элементов кольца, причем $x\lambda_x = \lambda_x x$, так что вместо записи коэффициентов справа от базисных элементов можно использовать и запись их слева от базисных элементов. Таким образом,

$$\sum_{x\in G} x\lambda_x = \sum_{x\in G} \lambda_x x.$$

Линейное действие G на FG, соответствующее действию G на G левыми сдвигами, называется *левым регулярным (линейным) представлением* группы G над полем F. Во многих важных случаях (например, когда G конечна и $F = \mathbb{C}$) оказывается, что все конечномерные G-модули являются (изоморфны) прямыми суммами G-подмодулей G-модуля FG.

Пусть G — конечная группа, и Z_1, ..., Z_m — классы сопряженных элементов G. В кольце FG можно определить элементы

$$C_i = \sum_{g\in Z_i} g, \quad i = 1, 2, \ldots, m.$$

Эти элементы обладают следующим свойством: для каждого $v \in FG$ имеет место равенство $aC_i = C_i a$.

6.12. Докажите последнее утверждение.

Указание. Сначала можно проверить, что достаточно рассмотреть лишь случай $a \in G$. Если эе $a \in G$, то $aC_i = C_i a$ равносильно $aC_i a^{-1} = C_i$. Далее можно представить C_i как $b_1 + \cdots + b_k$, где $\{b_1, \ldots, b_k\} = Z_i$, записать $aC_i a^{-1}$ как сумму, и вспомнить, что же такое класс сопряженных элементов.

Определим *центр* кольца FG как множество $C(FG)$, состоящее из всех таких $w \in FG$, что для любого $a \in FG$ имеет место равенство $aw = wa$.

6.13. Доказать, что $C(FG)$ является подкольцом кольца FG. При этом $F \subset C(FG)$ (напомним, что поле F считается подкольцом FG). Проверить, что $C(FG)$ — линейное подпространство пространства FG.

Теорема 6.2. *Элементы $C_1, \ldots, C_m$ являются базисом центра группового кольца FG как линейного пространства над полем F.*

Краткое доказательство. Пусть $w = \sum\limits_{x \in G} \lambda_x x \in C(FG)$. Легко проверяется, что условие $aw = wa$ для всех $a \in FG$ равносильно условию $gw = wg$ для всех $g \in G$, что, в свою очередь, эквивалентно соотношению $gwg^{-1} = w$ для всех $g \in G$. Сопоставляя в равенстве

$$g(\sum_{x \in G} \lambda_x x)g^{-1} = \sum_{x \in G} \lambda_x gxg^{-1} = \sum_{x \in G} \lambda_x x$$

коэффициенты при одних и тех же базисных элементах, получаем равенство

$$\lambda_x = \lambda_{gxg^{-1}},$$

выполняющееся для всех x и g. Из него следует, что если x и y принадлежат к одному и тому же классу сопряженных элементов, то $\lambda_x = \lambda_y$. Таким образом, коэффициенты λ_x зависят только от классов Z_i, таких, что $x \in Z_i$. Положим $\lambda_i = \lambda_x$ при $x \in Z_i$, тогда элемент w можно записать в виде

$$\sum_{x \in G} \lambda_x x = \sum_{i=1}^{m} \sum_{x \in Z_i} \lambda_i x = \sum_{i=1}^{m} \lambda_i (\sum_{x \in Z_i} x) = \sum_{i=1}^{m} \lambda_i C_i.$$

Таким образом, элементы C_i порождают $C(FG)$ как линейное пространство. Линейная независимость этих элементов следует из того, что они являются суммами базисных элементов FG, причем ни в одной паре C_i, C_j нет общих слагаемых. $\square$

То, что этом доказательстве скаляры (элементы поля) записаны слева от векторов, результат (в данном конкретном случае) не повлияло.

Элементы $C_1, \ldots, C_m$ играют особую роль в описании строения FG. Покажем это далее на трех простых примерах. В качестве поля F во всех случаях можно брать поле $\mathbb{Q}$.

6.14. Пусть $G = S_3 = \{1, a, b, b^2, ab, ab^2\}$, где $a^2 = b^3 = 1$, $ba = ab^2$. Для этой группы $C_1 = 1$, $C_2 = b + b^2$, $C_3 = a + ab + ab^2$. Поскольку эти элементы образуют базис подкольца, их произведения записываются в виде их линейных комбинаций. В данном случае таблица умножения элементов C_1, C_2, C_3 выглядит следующим образом (проверьте это):

	C_1	C_2	C_3
C_1	C_1	C_2	C_3
C_2	C_2	$2C_1 + C_2$	$2C_3$
C_3	C_3	$2C_3$	$3(C_1 + C_2)$

Положим

$$\begin{aligned} e_1 &= \tfrac{1}{6}(C_1 + C_2 + C_3) = \tfrac{1}{6}(1 + C_2 + C_3), \\ e_2 &= \tfrac{1}{3}(2C_1 - C_2) = \tfrac{1}{3}(2 - C_2), \\ e_3 &= \tfrac{1}{6}(C_1 + C_2 - C_3) = \tfrac{1}{6}(1 + C_2 - C_3). \end{aligned}$$

Ясно, что $e_1, e_2, e_3 \in C(FG)$.

1) Прямым вычислением покажите, что $e_i^2 = e_i$, $e_ie_j = 0$, $e_1+e_2+e_3 = 1$ для всех i и $j \neq i$.

2) Проверьте, что $dim(FG)e_1 = 1$, $dim(FG)e_2 = 1$, $dim(FG)e_3 = 4$.

3) Докажите, что $FG = (FG)e_1 \oplus (FG)e_2 \oplus (FG)e_3$.

4) Докажите, что $(FG)e_1$, $(FG)e_2$, $(FG)e_3$ — подмодули G-модуля FG.

6.15. Пусть $G = Q_8 = \{1, u, x, ux, y, uy, z, uz\}$, где $u^2 = 1$, $x^2 = y^2 = u$, $xu = ux$, $uy = uy$, $xy = z$, $xy = uyx$. Для этой группы $C_1 = 1$, $C_2 = u$, $C_3 = x + ux$, $C_4 = y + uy$, $C_5 = z + uz$. Составьте таблицу умножения элементов $C_1, C_2, C_{3,4}, C_5$. Положим

$$\begin{aligned} e_1 &= \tfrac{1}{8}(C_1 + C_2 + C_3 + C_4 + C_5), \\ e_2 &= \tfrac{1}{8}(C_1 + C_2 - C_3 - C_4 + C_5), \\ e_3 &= \tfrac{1}{8}(C_1 + C_2 - C_3 + C_4 - C_5), \\ e_4 &= \tfrac{1}{8}(C_1 + C_2 - C_3 + C_4 - C_5), \\ e_3 &= \tfrac{1}{2}(C_1 - C_2). \end{aligned}$$

1) Показать, что $e_i^2 = e_i$, $e_ie_j = 0$, $e_1 + e_2 + e_3 + e_4 + e_5 = 1$ для всех i и $j \neq i$.

2) Вычислить размерности $dim(FG)e_i$, $1 \le i \le 5$.

3) Доказать, что $FG = (FG)e_1 \oplus (FG)e_2 \oplus (FG)e_3 \oplus (FG)e_4 \oplus (FG)e_5$.

4) Доказать, что $(FG)e_i$— подмодули G-модуля FG для всех $1 \le i \le 5$.

6.16. Пусть $G = \{1, x, x^2, x^3, y, y^3, xy, xy^3\}$, где $x^4 = 1$, $x^2 = y^2$, $y = xyx$, $x = yxy$. Будем считать известным, что для этой группы $C_1 = 1$, $C_2 = x^2$, $C_3 = x + x^3$, $C_4 = y + y^3$, $C_5 = xy + xy^3$. Составьте таблицу умножения элементов $C_1, C_2, C_{3,4}, C_5$. Положим

$$
\begin{aligned}
e_1 &= \tfrac{1}{8}(C_1 + C_2 + C_3 + C_4 + C_5),\\
e_2 &= \tfrac{1}{8}(C_1 + C_2 + C_3 - C_4 - C_5),\\
e_3 &= \tfrac{1}{8}(C_1 + C_2 - C_3 - C_4 + C_5),\\
e_4 &= \tfrac{1}{8}(C_1 + C_2 - C_3 + C_4 - C_5),\\
e_3 &= \tfrac{1}{2}(C_1 - C_2).
\end{aligned}
$$

1) Показать, что $e_i^2 = e_i$, $e_i e_j = 0$, $e_1 + e_2 + e_3 + e_4 + e_5 = 1$ для всех i и $j \ne i$.

2) Вычислить размерности $dim(FG)e_i$, $1 \le i \le 5$.

3) Доказать, что $FG = (FG)e_1 \oplus (FG)e_2 \oplus (FG)e_3 \oplus (FG)e_4 \oplus (FG)e_5$.

4) Доказать, что $(FG)e_i$— подмодули G-модуля FG для всех $1 \le i \le 5$.

6.17. Пусть $G = \{1, x, x^2, x^3, y, xy, x^2y, x^3y\}$, где $x^4 = 1$, $y^2 = 1$, $yx = x^3y$. Так как группа G — это группа диэдра D_4, то известо, что для нее $C_1 = 1$, $C_2 = x^2$, $C_3 = x + x^3$, $C_4 = y + x^2y$, $C_5 = xy + x^3y$. Составьте таблицу умножения элементов $C_1, C_2, C_{3,4}, C_5$. Положим

$$
\begin{aligned}
e_1 &= \tfrac{1}{8}(C_1 + C_2 + C_3 + C_4 + C_5),\\
e_2 &= \tfrac{1}{8}(C_1 + C_2 + C_3 - C_4 - C_5),\\
e_3 &= \tfrac{1}{8}(C_1 + C_2 - C_3 + C_4 - C_5),\\
e_4 &= \tfrac{1}{8}(C_1 + C_2 - C_3 - C_4 + C_5),\\
e_3 &= \tfrac{1}{2}(C_1 - C_2).
\end{aligned}
$$

1) Показать, что $e_i^2 = e_i$, $e_i e_j = 0$, $e_1 + e_2 + e_3 + e_4 + e_5 = 1$ для всех i и $j \ne i$.

2) Вычислить размерности $dim(FG)e_i$, $1 \le i \le 5$.

3) Доказать, что $FG = (FG)e_1 \oplus (FG)e_2 \oplus (FG)e_3 \oplus (FG)e_4 \oplus (FG)e_5$.

4) Доказать, что $(FG)e_i$ — подмодули G-модуля FG для всех $1 \leq i \leq 5$.

Рассмотрим подробнее наиболее простой вид представлений — одномерные представления. Для определенности пусть полем F до конца этого раздела будет только поле комплексных чисел $\mathbb{C}$. Так как $GL_1(\mathbb{C}) = \mathbb{C}^*$, то одномерные представления группы G — это гомоморфизмы из G в $\mathbb{C}^*$. Традиционно такие гомоморфизмы обозначаются буквой χ (другое их название — одномерные *характеры* группы G). Отметим одно существенное свойство одномерных представлений: если $\chi : G \to \mathbb{C}^*$ — представление, то $\chi(gxg^{-1}) = \chi(x)$ для любых $g, x \in G$. Это значит, что χ принимает одни и те же значения для элементов из одного и того же класса сопряженных элементов. Другое наблюдение состоит в том, что если группа G конечна, порядки всех ее элементов конечны. Следовательно, если $g \in G$, то $g^n = 1$ для некоторого n. Отсюда $\chi(g^n) = \chi(g)^n = 1$. Таким образом, $\chi(g) \in \mathbf{U}_n \subset \mathbf{U}$. Отсюда следует, что $\chi(G) \subseteq \mathbf{U}_l$, где l есть наименьшее общее кратное порядков элементов G.

В следующем примере, и при решении дальнейших задач, используется одна конструкция, которая в данном пособии принимается без обоснования. А именно, пусть в группе G задано множество образующих X, и для каждого элемента $g \in G$ зафиксирована некоторая его запись в виде $g = x_{\alpha_1}^{\pm 1} \dots x_{\alpha_r}^{\pm 1}$, в которой $x_{\alpha_1}, \dots, x_{\alpha_r} \in X$. Назовем такую запись стандартной формой g. Допустим еще, что известно некоторое количество соотношений между элементами X, имеющих вид $w_1 = w_2$, где $w_1 = x_{i_1}^{\pm 1} \dots x_{i_k}^{\pm 1}$, $w_2 = x_{j_1}^{\pm 1} \dots x_{j_s}^{\pm 1}$, $x_{i_1}, \dots, x_{j_s} \in X$. Этих соотношений должно быть достаточно для того, чтобы можно было с их помощью привести произведение стандартных форм элементов g_1 и g_2 к стандартной форме элемента $g_1 g_2$, и по стандартной форме g вычислить стандартную форму g^{-1}. Пусть каждому элементу $x_i \in X$ сопоставлено комплексное число $u_i \in \mathbb{C}^*$. Теорема, о которой идет речь, утверждает, что если эти числа таковы, что для каждого соотношения $w_1 = w_2$, о котором говорилось выше, имеет место равенство вида

$$u_{i_1}^{\pm 1} \dots u_{i_k}^{\pm 1} = u_{j_1}^{\pm 1} \dots u_{j_s}^{\pm 1},$$

то существует, притом однозначно определенный, гомоморфизм (одномерное представление) $\chi : G \longrightarrow \mathbb{C}^*$, такой, что $\chi(x_i) = u_i$ для всех $x_i \in X$. При этом, если $g = x_{\alpha_1}^{\pm 1} \dots x_{\alpha_r}^{\pm 1}$, то $h(g) = u_{\alpha_1}^{\pm 1} \dots u_{\alpha_r}^{\pm 1}$. Доказательство (и более точную и общую формулировку) можно найти в тех разделах книг по теории групп, где говорится о свободных группах и о задании групп образующими и определяющими соотношениями. Фактически на последнем этапе этого доказательства применяется теорема о гомоморфизме.

То, что применяется не входящий в программу курса результат, не должно казаться чем-то необычным. Например, действительные числа начинают использоваться при изучении математики намного раньше того момента, когда студенты узнают (если это вообще происходит!), каково же их (действительных чисел) строгое построение, которое далеко не тривиально.

Пример 6.1. Найдем все одномерные представления группы диэдра D_{2m}. Напомним, что это группа, порожденная двумя элементами a и b, которые удовлетворяют соотношениям: $a^{2m} = b^2 = 1$, $ba = a^{2m-1}b$. Последнее соотношение равносильно равенству $(ab)^2 = 1$ (обоснуйте это!). Элементы D_{2m} — это $1, a, a^2, \dots, a^{2m-1}, b, ab, a^2b, \dots, a^{2m-1}b$. Классы сопряженных элементов — $\{1\}$, $\{a^m\}$, $\{a^k, a^{2m-k}\}$, $1 \leq k \leq m-1$, $\{b, a^2b, a^4b, \dots, a^{2m-2}b\}$, $\{ab, a^3b, a^5b, \dots, a^{2m-1}b\}$. Эта информация позволяет описать одномерные представления в компактном виде: для каждого χ достаточно знать его значения лишь для одного элемента из каждого класса сопряженных элементов.

Итак, пусть $\chi : D_{2m} \longrightarrow \mathbb{C}^*$ — некоторое одномерное представление. Положим $\chi(a) = x \in \mathbb{C}^*$, $\chi(b) = y \in \mathbb{C}^*$. Тогда из $a^{2m} = b^2 = 1$ следует, что $x^{2m} = y^2 = 1$, а из $(ab)^2 = 1$ следует $(xy)^2 = 1$. Так как a и b порождаю всю группу D_{2m}, а χ — гомоморфизм групп, то по значениям x и y однозначно вычисляется значение χ на любом элементе D_{2m}. Следовательно, нахождение χ сводится к нахождению x и y, то есть к решению системы уравнений:

$$\begin{cases} x^{2m} = 1 \\ y^2 = 1 \\ (xy)^2 = x^2y^2 = 1 \end{cases}$$

Очевидно, эта система равносильна следующей:

$$\begin{cases} x^2 = 1 \\ y^2 = 1 \end{cases}$$

Эта система легко решается. Имеется 4 решения, и это все возможные комбинации значений $x = \pm 1$, $y = \pm 1$. Окончательно получаем таблицу значений для четырех одномерных представлений D_{2m}:

	1	a	b	a^m	$\dots$	a^k	$\dots$	ab
χ_1	1	1	1	1	$\dots$	1	$\dots$	1
χ_2	1	1	-1	1	$\dots$	1	$\dots$	-1
χ_3	1	-1	1	$(-1)^m$	$\dots$	$(-1)^k$	$\dots$	-1
χ_4	1	-1	-1	$(-1)^m$	$\dots$	$(-1)^k$	$\dots$	1

В верхней строке указаны представители классов сопряженных элементов, $2 \le k \le m-1$.

6.18. Найти одномерные представления групп D_{2m+1}. В частности, что представляют из себя одномерные представления $D_3 = S_3$?

6.19. Найти одномерные представления группы S_4. Напомним, что эта группа порождается элементами S, T, для которых выполняются соотношения $S^4 = T^2 = 1$, $(ST)^3 = 1$ (подробности см. в разделе 2).

6.20. Найти одномерные представления группы A_4. Напомним, что эта группа порождается элементами S, R, для которых выполняются соотношения $S^3 = R^2 = (SR)^3 = 1$ (подробности см. в разделе 2).

6.21. Найти одномерные представления группы A_5. Эта группа порождается элементами R, S, для которых выполняются соотношения $R^2 = S^3 = (RS)^5 = 1$.

6.22. Найти одномерные представления группы Q_8. Напомним, что эта группа порождается элементами a, b, для которых выполняются соотношения $a^4 = 1$, $b^2 = a^2$, $bab^{-1} = a^2$. (подробности см. в разделе 3).

6.23. Найти одномерные представления группы $\mathbf{U}_n$. Напомним, что эта группа является циклической. Она порождается одним элементом u, таким, что $u^n = 1$.

6.24. Найти одномерные представления группы $\mathbb{Z}$. Напомним, что это бесконечная циклическая группа (по сложению), порожденная элементом 1 (нейтральный элемент здесь — нуль!).

6.25. Как выражаются одномерные представления представления группы $G_1 \times G_2$ через одномерные представления G_1 и G_2?

Указание. Пусть $\chi_1 : G_1 \to \mathbb{C}^*$, $\chi_2 : G_2 \to \mathbb{C}^*$ — представления. Определим функцию $\chi : G_1 \times G_2 \to \mathbb{C}^*$ по правилу $\chi(g_1, g_2) = \chi_1(g_1)\chi_2(g_2)$. Докажите, что это представление группы $G_1 \times G_2$. Каждое ли представление $G_1 \times G_2$ имеет такой вид?

Группы из следующей серии заданий должны быть подробно исследованы в задачах из раздела 3. В частности, при решении тех задач должны были быть вычислены классы сопряженных элементов этих групп, информация о которых необходима и для решения задач **6.26** – **6.47**.

6.26. Дана группа G с элементами

$$1, S, S^2, S^3, S^4, S^5, S^6, S^7, T, ST, S^2T, S^3T, S^4T, S^5T, S^6T, S^7T,$$

которые удовлетворяют следующим соотношениям:

$$S^8 = T^2 = 1,\ TS = S^3T.$$

Вычислить в явном виде все различные одномерные представления группы G.

6.27. Дана группа G с элементами

$$1, S, S^2, S^3, S^4, S^5, S^6, S^7, T, ST, S^2T, S^3T, S^4T, S^5T, S^6T, S^7T,$$

которые удовлетворяют следующим соотношениям:

$$S^8 = T^2 = 1,\ TS = S^5T.$$

Вычислить в явном виде все различные одномерные представления группы G.

6.28. Дана группа G с элементами

$$1, S, S^2, S^3, T, T^2, T^3, TS, TS^2, TS^3, T^2S, T^2S^2, T^2S^3, T^3S, T^3S^2, T^3S^3,$$

которые удовлетворяют следующим соотношениям:

$$S^4 = T^4 = 1, ST = TS^3.$$

Вычислить в явном виде все различные одномерные представления группы G.

6.29. Дана группа G с элементами

$$1, R, R^2, R^3, S, S^2, S^3, SR, SR^2, SR^3, S^2R, S^2R^2, S^2R^3, S^3R, S^3R^2, S^3R^3,$$

которые удовлетворяют следующим соотношениям:

$$R^4 = S^4 = 1, RS = S^3R^3, R^3S = S^3R.$$

Вычислить в явном виде все различные одномерные представления группы G.

6.30. Дана группа G с элементами

$$1, R, S, T, RS, RT, TR, SR, ST, TS, A, A^2, A^3, B, C, D,$$

которые удовлетворяют следующим соотношениям:

$$R^2 = S^2 = T^2 = 1, RST = TRS = STR, (RST)^4 = 1,$$
$$TRT = SRS, RTR = STS, TST = RSR,$$
$$A = RST, B = TRT, C = RTR, D = TST.$$

Вычислить в явном виде все различные одномерные представления группы G.

6.31. Дана группа G с элементами

$$1, S, S^2, S^3, S^4, S^5, S^6, S^7, T, ST, S^2T, S^3T, S^4T, S^5T, S^6T, S^7T,$$

которые удовлетворяют следующим соотношениям:

$$S^8 = T^4 = 1, S^4 = T^2, TS = S^7T, ST = TS^7.$$

Вычислить в явном виде все различные одномерные представления группы G.

6.32. Дана группа G с элементами

$$1, S, S^2, S^3, S^4, S^5, S^6, S^7, X, SX, S^2X, S^3X, S^4X, S^5X, S^6X, S^7X,$$

которые удовлетворяют следующим соотношениям:

$$S^8 = X^4 = 1, S^4 = X^2, XS = S^3X.$$

Вычислить в явном виде все различные одномерные представления группы G.

6.33. Дана группа G с элементами

$$1, S, S^2, S^3, S^4, S^5, S^6, S^7, X, SX, S^2X, S^3X, S^4X, S^5X, S^6X = X^3, S^7X,$$

которые удовлетворяют следующим соотношениям:

$$S^8 = X^8 = 1, X^2 = S^6, X^4 = S^4, X^6 = S^2, XS = S^5X.$$

Вычислить в явном виде все различные одномерные представления группы G.

6.34. Дана группа G с элементами

$$1, X, Y, Z, XY, XZ, YZ, (YZ)^2, (YZ)^3,$$
$$YZY, ZYZ, XYZ, XZY, XYZY, XZYZ, X(YZ)^2,$$

которые удовлетворяют следующим соотношениям:

$$X^2 = Y^2 = Z^2 = 1, XY = YX, XZ = ZX, ZY = (YZ)^3.$$

Вычислить в явном виде все различные одномерные представления группы G.

6.35. Дана группа G с элементами

$$1, S, S^2, S^3, S^4, S^5, S^6, S^7, R, SR, S^2R, S^3R, S^4R, S^5R, S^6R, S^7R,$$

которые удовлетворяют следующим соотношениям:

$$S^8 = R^4 = 1, S^4 = R^2, RS^2 = S^2R^3, RS^3 = S^5R.$$

Вычислить в явном виде все различные одномерные представления группы G.

6.36. Дана группа G с элементами

$$1, R, S, T, R^2, R^3, S^3, S^3, RS, SR, TR, TS, TR^2, TRS, TR^3, TS^3, TSR,$$

которые удовлетворяют следующим соотношениям:

$$R^4 = T^2 = 1, R^2 = S^2 = (RS)^2, RT = TR, TS = ST.$$

Вычислить в явном виде все различные одномерные представления группы G.

6.37. Дана группа G с элементами

$$1, A, B, A^2, A^3, A^4, A^5, A^6, A^7, B, AB, A^2B, A^3B, A^4B, A^5B, A^6B, A^7B,$$

которые удовлетворяют следующим соотношениям:

$$A^8 = B^2 = 1, BA^7 = A^5B.$$

Вычислить в явном виде все различные одномерные представления группы G.

6.38. Дана группа G с элементами

$$1, P, Q, P^2, P^3, P^4, P^5, P^6, P^7, Q, PQ, P^2Q, P^3Q, P^4Q, P^5Q, P^6Q, P^7Q,$$

которые удовлетворяют следующим соотношениям:

$$P^8 = Q^2 = 1, QP^7 = P^3Q.$$

Вычислить в явном виде все различные одномерные представления группы G.

6.39. Дана группа G с элементами

$$1, U, U^2, U^3, V, V^2, V^3, VU, VU^2, VU^3, V^2U, V^3U, V^3U^2, V^2U^2, V^2U^3, V^3U^3,$$

которые удовлетворяют следующим соотношениям:

$$U^4 = V^4 = 1, U^3V^3 = V^3U.$$

Вычислить в явном виде все различные одномерные представления группы G.

6.40. Дана группа G с элементами

$$1, X, X^2, X^3, Y, Y^2, Y^3, XY, XY^2, XY^3,$$
$$X^2Y, X^2Y^2, X^2Y^3, X^3Y, X^3Y^2, X^3Y^3,$$

которые удовлетворяют следующим соотношениям:

$$X^4 = Y^4 = 1, X^{-1} = YXY, Y = XY^{-1}X.$$

Вычислить в явном виде все различные одномерные представления группы G.

6.41. Дана группа G с элементами

$$1, X, Y, Z, XY, XZ, ZX, YX, YZ, ZY,$$
$$XYZ, (XYZ)^2, (XYZ)^3, XYX, XZX, YXY,$$

которые удовлетворяют следующим соотношениям:

$$X^2 = Y^2 = Z^2 = 1, XY = Z(XY)Z, ZX = Y(ZX)Y, ZY = X(ZY)X,$$
$$XYX = ZYZ, XZX = YZY, YXY = ZXZ.$$

Вычислить в явном виде все различные одномерные представления группы G.

6.42. Дана группа G с элементами

$$1, X, Y, X^2, X^3, X^4, X^5, X^6, X^7, Y, XY, X^2Y, X^3Y, X^4Y, X^5Y, X^6Y, X^7Y,$$

которые удовлетворяют следующим соотношениям:

$$X^8 = 1, X^4 = Y^2, YXY^{-1} = X^{-1}, XYX = Y.$$

Вычислить в явном виде все различные одномерные представления группы G.

6.43. Дана группа G с элементами

$$1, U, U^2, U^3, U^4, U^5, U^6, U^7, V, V^3, UV, U^2V, UV^3, U^2V^3U^3V, U^3V^3,$$

которые удовлетворяют следующим соотношениям:

$$U^8 = 1, V^2 = U^4, VU^3V^{-1} = U.$$

Вычислить в явном виде все различные одномерные представления группы G.

6.44. Дана группа G с элементами

$$1, C, C^2, C^3, C^4, C^5, C^6, C^7, Y, CY, C^2Y, C^3Y, C^4Y, C^5Y, C^6Y, C^7Y,$$

которые удовлетворяют следующим соотношениям:

$$C^8 = Y^8, Y^2 = C^6, Y^4 = C^4, Y^6 = C^2, YCY = C^3.$$

Вычислить в явном виде все различные одномерные представления группы G.

6.45. Дана группа G с элементами

$$1, A, B, C, AB, AC, BC, (BC)^2, (BC)^3,$$
$$BCB, CBC, ABC, ACB, ABCB, ACBC, A(BC)^2,$$

которые удовлетворяют следующим соотношениям:

$$A^2 = B^2 = C^2 = (BC)^4 = 1, AB = BA, AC = CA.$$

Вычислить в явном виде все различные одномерные представления группы G.

6.46. Дана группа G с элементами

$$1, X, X^2, X^3, X^4, X^5, X^6, X^7, Y, XY, X^2Y, X^3Y, X^4Y, X^5Y, X^6Y, X^7Y,$$

которые удовлетворяют следующим соотношениям:

$$Y^4 = 1, Y^2 = X^4, YX^2 = X^6Y, YX = X^7Y.$$

Вычислить в явном виде все различные одномерные представления группы G.

6.47. Дана группа G с элементами

$$1, X, X^2, X^3, Y, Y^3, Z, XY, YX, ZX, ZY, ZX^2, ZXY, ZX^3, ZY^3, ZYX,$$

которые удовлетворяют следующим соотношениям:

$$X^2 = Y^2 = (XY)^2, Z^2 = (XY)^4 = 1, ZXZ^{-1} = X, ZYZ^{-1} = Y.$$

Вычислить в явном виде все различные одномерные представления группы G.

7. Группы вращений

Напомним, что матрица A с действительными элементами, для которой $A^{-1} = {}^tA$, называется *ортогональной.*

Множество всех ортогональных $n \times n$-матриц обозначается через $O(n)$ и называется *ортогональной группой.* Подмножество $O(n)$, состоящее из матриц с единичными определителями, называется *специальной ортогональной* группой и обозначается через $SO(n)$.

7.1. Доказать, что $O(n)$ и $SO(n)$ являются подгруппами группы $GL_n(\mathbb{R})$. Доказать, что $SO(n)$ — нормальная подгруппа группы $O(n)$, и вычислить факторгруппу $O(n)/SO(n)$.

7.2. Пусть J — произвольная $n\times n$-матрица с компонентами из поля $\mathbb{R}$. Рассмотрим множество G_J, состоящее из всех тех $X \in GL_n(\mathbb{R})$, которые удовлетворяют равенству

$$ {}^tXJX = J. $$

Доказать, что G_J является подгруппой группы $GL_n(\mathbb{R})$.

Заметим, что при $J = E_n$ группа G_J совпадает с $O(n)$. Выбирая матрицы J иными способами, можно получить много других интересных примеров групп.

Наша цель — подробно изучить группы $SO(2)$ и $SO(3)$. Начнем с $SO(2)$. Пусть

$$ A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SO(2). $$

Тогда из $A({}^tA) = E_2$ и $det(A) = 1$ следует, что $a^2 + b^2 = c^2 + d^2 = 1$, $ac + bd = 0$, $ad - bc = 1$.

7.3. Вывести отсюда, что матрицу A можно представить в виде

$$ A = A(\varphi) = \begin{pmatrix} \cos\varphi & -\sin\varphi \\ \sin\varphi & \cos\varphi \end{pmatrix}, \quad \varphi \in [0, 2\pi). $$

Таким образом, группа $SO(2)$ состоит из всех матриц такого вида. Геометрическая интерпретация линейного преобразования, задаваемого матрицей A — поворот на угол φ против часовой стрелки. Проверьте это.

Далее нам потребуется определение кольца. Примеры колец и полей встречаются студенту-математику начиная с первого курса, так что их появление не должно оказаться чем-то неожиданным и совершенно незнакомым.

Ассоциативное кольцо R — это множество с двумя бинарными опреациями, сложением и умножением. Относительно операции сложения R является коммутативной (или абелевой) группой, нейтральным элементом которой является нуль, а относительно умножения — полугруппой (в наших примерах всегда с единицей). Операции сложения и умножения связаны друг с другом следующим свойством:

$$x(y \pm z) = xy \pm xz, \quad (x \pm y)z = xz \pm yz$$

для любых $x, y, z \in R$. Отсюда, в частности, следует, что $x0 = 0x = 0$ для каждого $x \in R$.

Ассоциативные кольца часто называются просто *кольцами.* Кольцо называется *коммутативным*, если $xy = yx$ для всех $x, y \in R$. Коммутативное кольцо называется *полем*, если каждый его ненулевой элемент имеет обратный по умножению, то есть для каждого $x \neq 0$ существует y, такой, что $xy = yx = 1$. Иными словами, множество $R \setminus \{0\}$ оказывается (коммутативной) группой по умножению.

Вот примеры колец и полей, которые должны быть известны каждому студенту-математику, окончившему первый курс. Прежде всего, кольцо целых чисел $\mathbb{Z}$. Далее, поля $\mathbb{Q}, \mathbb{R}, \mathbb{C}$. Затем кольцо квадратных $n \times n$-матриц над полем F, обозначаемое через $M_n(F)$. Оно некоммутативно. Наконец, кольца многочленов от n переменных над полем F, обозначаемые как $F[x_1, \ldots, x_n]$.

Подкольцом R' кольца R называется его подмножество, которое является подгруппой R по сложению, содержит единицу кольца R и замкнуто относительно умножения, то есть если $x, y \in R'$, то $xy \in R'$.

Гомоморфизм h из кольца R_1 в кольцо R_2 (*гомоморфизм колец*)— это отображение $h : R_1 \longrightarrow R_2$, являющееся гомоморфизмом абелевых групп (т.е. $h(x+y) = h(x)+h(y)$ и $h(0) = 0$), и обладающее, кроме того, свойствами $h(xy) = h(x)h(y)$, $h(1) = 1$. Изоморфизм колец определяется точно так же, как изоморфизм групп. В конечном счете это биективный гомоморфизм.

Будем считать, что читатель знаком с полем комплексных чисел $\mathbb{C}$ и его свойствами. Обычное определение состоит в том, что $\mathbb{C}$ — это линейное (или векторное) пространство размерности 2 над полем действительных чисел $\mathbb{R}$, причем само поле $\mathbb{R}$ содержится в $\mathbb{C}$ как подпространство, и существует базис $\mathbb{C}$ над $\mathbb{R}$ из двух элементов: $1 \in \mathbb{R}$ и i. Таким образом, каждый элемент $z \in \mathbb{C}$ однозначно записывается как линейная комбинация базисных векторов $z = a \cdot 1 + b \cdot i$ с коэффициентами $a, b \in \mathbb{R}$.

Теорема 7.1. *Поле комплексных чисел изоморфно и как кольцо, и как линейное пространство над* $\mathbb{R}$*, кольцу квадратных матриц вида*

$$\begin{pmatrix} a & -b \\ b & a \end{pmatrix}$$

с элементами $a, b \in \mathbb{R}$*.*

Доказательство. Введем обозначение: если $z = a + bi$, то

$$A(z) = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}.$$

Элементарные вычисления с матрицами второго порядка показывают, что $A(1) = E$, $A(0) = 0$, $A(\lambda z) = \lambda A(z)$ для $\lambda \in \mathbb{R}$, $A(z_1+z_2) = A(z_1)+A(z_2)$, и, наконец, $A(z_1 z_2) = A(z_1)A(z_2)$. Все это означает, что соответствие $z \mapsto A(z)$ есть гомоморфизм колец и линейных пространств над полем $\mathbb{R}$. Очевидно, что он инъективен и сюръективен. $\square$

Легко проверяется, что $|z|^2 = a^2 + b^2 = det(A(z))$. Очевидно также, что $SO(2)$ содержится в кольце матриц вида $A(z)$, $z \in \mathbb{C}$.

7.4. Доказать, что ограничение изоморфизма колец $z \mapsto A(z)$ на подгруппу $\mathbf{U}$ группы $\mathbb{C}^*$ является изоморфизмом между группами $\mathbf{U}$ и $SO(2)$.

Если $z \in \mathbf{U}$, то $z = \cos\varphi + i \sin\varphi$, так что $A(z) = A(\varphi)$.

Перейдем к изучению $SO(3)$. Для произвольной $n \times n$-матрицы A пусть $f_A(x)$ — ее характеристический многочлен, равный $det(xE_n - A)$. Напомним, что это многочлен n-й степени и его свободный член равен

$(-1)^n det(A)$. Так как определитель транспонированной матрицы совпадает с определителем исходной матрицы, то $det(xE_n - A) = det({}^t(xE_n - A)) = det(xE_n - {}^tA)$. Таким образом, $f_A(x) = f_{({}^tA)}(x)$. Если же $A^{-1} = {}^tA$, то представляя E_n как $A({}^tA)$, получим

$$xE_n - A = xA({}^tA) - A = xA({}^tA - \frac{1}{x}E).$$

Вычислим определитель от левой и правой части этого равенства:

$$\begin{aligned} f_A(x) &= det(xA({}^tA - \tfrac{1}{x}E)) = det(xA)det({}^tA - \tfrac{1}{x}E) = \\ &= x^n det(A)(-1)^n det(\tfrac{1}{x}E_n - {}^tA) = (-1)^n x^n det(A) f_{({}^tA)}(\tfrac{1}{x}) = \\ &= (-1)^n x^n det(A) f_A(\tfrac{1}{x}) \end{aligned}$$

Если к тому же $det(A) = 1$, то 0 не является корнем $f_A(x)$, и если $f_A(\lambda) = 0$, то $f_A(\frac{1}{\lambda}) = 0$. Иными словами, если λ — собственное значение матрицы из $SO(n)$, то и $\dfrac{1}{\lambda}$ — также собственное значение.

Лемма 7.1. *У любой неединичной матрицы из $SO(3)$ одно (и только одно) из собственных значений равно единице.*

Доказательство. Понятно, что у единичной 3×3-матрицы единица является единственным собственным значением, имеющим кратность три, и что это свойство характеризует только единичную матрицу. Допустим, что $A \neq E_3$, и пусть $\lambda_1, \lambda_2, \lambda_3$ — собственные значения A. Тогда $\lambda_1\lambda_2\lambda_3 = det(A) = 1$. Предположим, что все три корня вещественны. Если, например, $\lambda_3 \neq \dfrac{1}{\lambda_3}$ (это равносильно тому, что $\lambda_3 \neq \pm 1$), то $\lambda_3 = \dfrac{1}{\lambda_2}$. В частности, тогда и $\lambda_2 \neq \pm 1$, а так как в этом случае $\lambda_2\lambda_3 = 1$ и $\lambda_1\lambda_2\lambda_3 = 1$, то $\lambda_1 = 1$. Если же для всех $i = 1, 2, 3$ имеют место равенства $\lambda_i = \dfrac{1}{\lambda_i}$, то $\lambda_i^2 = 1$, $\lambda_i = \pm 1$. Единственная допустимая здесь (с учетом того, что $\lambda_1\lambda_2\lambda_3 = 1$) комбинация: одно собственное значение равно единице, два других равны минус единице. Если не все собственные значения вещественны, то надо использовать то, что у многочлена с действительными коэффициентами число, сопряженное к комплексному корню, также является корнем. Следовательно, все три корня $\lambda_1, \lambda_2, \lambda_3$ у многочлена с действительными коэффициентами $f_A(x)$ не могут быть комплексными. Например, λ_1 — действительное число, λ_2 и λ_3 — комплексные (то есть не действительные), $\lambda_3 = \overline{\lambda_2}$. Тогда $\lambda_1\lambda_2\lambda_3 = \lambda_1|\lambda_2^2| = 1$. Отсюда сдедует, что $\lambda_1 > 0$. Учитывая, что число $\dfrac{1}{\lambda_1}$ также должно быть корнем $f_A(x)$, приходим к выводу, что $\lambda_1 = \dfrac{1}{\lambda_1}$, откуда $\lambda_1 = 1$. Два других собственных значения по предположению не являются действительными, и поэтому не равны единице. $\square$

Рассмотрим $V = \mathbb{R}^n$ как евклидово пространство со скалярным произведением (v_1, v_2). Линейное преобразование $\alpha : V \to V$ называется *ортогональным*, если для любый $v_1, v_2 \in V$ выполняется равенство $(\alpha(v_1), \alpha(v_2)) = (v_1, v_2)$. Ортогональное линейное преобразование всегда обратимо. В самом деле, допустим, что α не инъективное отображение. Тогда существует вектор $v \in V$, $v \neq 0$, такой, что $\alpha(v) = 0$. Следовательно, $(\alpha(v), \alpha(v)) = (0, 0) = 0$. Но, с другой стороны, должно быть $(\alpha(v), \alpha(v)) = (v, v) > 0$. Значит, линейное отображение α инъективно, и отображает любое множество из $m \leq n$ линейно независимых элементов в m различных независимых элементов. Но пространство V конечномерно, и обладает базисом из n элементов. Отображение α переводит этот базис в множество из n линейно независимых элементов, которое в силу этого тоже обязано быть базисом. Отсюда следует, что α сюръективно.

7.5. Докажите, что если α — ортогональное линейное отображение, то линейное отображение α^{-1} также ортогонально, и что если $\beta : V \to V$ — другое ортогональное линейное отображение, то ортогональна и суперпозиция $\alpha\beta$.

Тождественное отображение $1_V : V \to V$, очевидно, тоже ортогонально. Из всего этого следует, что множество всех ортогональных линейных отображений из V в V образуют группу, которую мы будем обозначать через $O(V)$.

Из линейной алгебры известно, что если выбрать в V какой-нибудь ортонормированный базис, то матрица α в этом базисе является ортогональной. И наоборот, если зафиксировать в пространстве векторов-столбцов $\mathbb{R}^n$ стандартный базис и отождествлять каждую ортогональную матрицу A с линейным отображением $v \mapsto Av$, то это отображение будет ортогональным относительно скалярного произведения $(x, y) = \sum\limits_{i=1}^{n} x_i y_i$, где

$$x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}, \ y = \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}.$$

Отсюда следует, что тем же способом, которым в разделе 6 строился изоморфизм между $GL(V)$ и $GL_n(F)$, можно получить изоморфизм между $O(V)$ и $O(n)$. Отличие состоит только в том, что базис в пространстве V должен выбираться ортонормированным.

Определителем произвольного линейного отображения α является определитель матрицы A этого отображения в любом базисе. Определитель матрицы A не меняется при переходе к матрице XAX^{-1}, и это показывает, что от выбора базиса определитель α не зависит. Тем самым задается подгруппа $SO(V)$ группы $O(V)$, состоящая из ортогональных линейных отображений, определители которых равны единице. Ограничение описанного выше изоморфизма между $O(V)$ и $O(n)$ на подгруппу $SO(V)$ является изоморфизмом между $SO(V)$ и $SO(n)$. По мере необходимости удобно не делать различий между ортогональными матрицами и ортогональными линейными отображениями (при фиксированном ортонормированном базисе).

Напомним еще несколько необходимых для дальнейшего фактов. Пусть V_1 — инвариантное относительно α подпространство пространства V. Это значит, что $\alpha(v) \in V_1$ для любого $v \in V_1$. Ограничение α на инвариантное подпространство V_1 будет ортогональным линейным отображением $\alpha_1 : V_1 \to V_1$. Например, инвариантными подпространствами α будут подпространства собственных векторов, отвечающих собственным значениям α. Рассмотрим далее ортогональное дополнение V_2 подпространства V_1. Оно состоит из всех тех $v_2 \in V$, для которых $(v_1, v_2) = 0$ для каждого $v_1 \in V_1$. Имеют место два важных факта. Во-первых, $V = V_1 \oplus V_2$. Во-вторых, подпространство V_2, как и V_1, является инвариантным. Пусть $\alpha_2 : V_2 \to V_2$ — ортогональное линейное отображение, являющееся ограничением α на V_2. Выберем какие-нибудь ортонормирванные базисы в V_1 и V_2, и пусть A_i $(i = 1, 2)$ — матрицы α_i в этих базисах. Тогда матрица α в ортонормированном базисе V, являющемся объединением выбранных базисов V_1 и V_2, имеет следущий блочный вид:

$$\begin{pmatrix} A_1 & 0 \\ 0 & A_2 \end{pmatrix}.$$

Если первоначально был выбран какой-то другой ортонормированный базис V, и A есть линейного отображения α в этом базисе, то существует обратимая (также ортогональная) матрица X, такая что

$$XAX^{-1} = \begin{pmatrix} A_1 & 0 \\ 0 & A_2 \end{pmatrix}.$$

В случае матрицы $A \in SO(3)$ и соответствующего линейного отображения α ситуация выглядит следующим образом. Пусть V_1 — одномерное инвариантное подпространство, базисный вектор которого является собственным вектором α, отвечающим собственному значению единица. Тогда α_1 — тождественное отображение с матрицей (1), а подпространство V_2 двумерно, так что матрица A_2 отображения α_2 принадлежит группе $SO(2)$ (почему $det(A_2) = 1$?). Используя то, что уже известно о матрицах из $SO(2)$, приходим к следующему выводу.

Теорема 7.2. $A \in SO(3)$ *тогда и только тогда, если для некоторой ортогональной матрицы* X *имеет место равенство:*

$$XAX^{-1} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos\varphi & -\sin\varphi \\ 0 & \sin\varphi & \cos\varphi \end{pmatrix}$$

Введем один специальный тип линейных преобразований. Пусть $w \in V$ — ненулевой вектор. Определим отображение $\tau_w : V \longrightarrow V$ по формуле:

$$\tau_w(v) = v - 2\frac{(v,w)}{(w,w)}w.$$

7.6. Докажите, что τ_w — линейное отображение, и что $\tau_w^{-1} = \tau_w$.

Чтобы проверить, что $(\tau_w(v_1), \tau_w(v_2)) = (v_1, v_2)$, проделаем следующие выкладки.

$$\begin{aligned}(\tau_w(v_1), \tau_w(v_2)) &= (v_1 - 2\frac{(v_1,w)}{(w,w)}w, v_2 - 2\frac{(v_2,w)}{(w,w)}w) \\ &= (v_1, v_1) - 2\frac{(v_1,w)}{(w,w)}(w, v_2) - 2\frac{(v_2,w)}{(w,w)}(v_1,w) + 4\frac{(v_1,w)}{(w,w)} \cdot \frac{(v_1,w)}{(w,w)}(w,w) \\ &= (v_1, v_2).\end{aligned}$$

Таким образом, τ_w — ортогональное линейное преобразование. Пусть $V_1 = \langle w \rangle$ — подпространство с базисом w. Легко проверить, что $\tau_w(w) = -w$, так что это подпространство инвариантно относительно τ_w. Пусть V_2 — ортоональное дополнение к V_1.

7.7. Покажите, что $v \in V_2$ тогда и только тогда, если $\tau_w(v) = v$.

Ввиду всего этого отображения τ_w называются (зеркальными) *отражениями* относительно гиперплоскости V_2. Другое название для таких отображений — *перевертывания.*

Отметим еще одно свойство отражений: если $\lambda \in \mathbb{R}, \lambda \neq 0$, то $\tau_{\lambda w} = \tau_w$ (проверьте!). Ввиду этого свойства вектор w можно при необходимости считать нормированным, т.е. $(w, w) = 1$.

Вычислим определитель τ_w. Выберем ортонормированный базис V, взяв в качестве первого базисного вектора $e_1 = w$ (который можно считать нормированным), а в качестве $n-1$ других — какой-нибудь ортонормированный базис $e_2, \ldots, e_n$ пространства V_2. Тогда по определению τ_w получим $\tau_w(e_1) = -e_1$, $\tau_w(e_2) = e_2$, $\ldots$, $\tau_w(e_n) = e_n$. Следовательно, матрица τ_w в этом базисе такова:

$$\begin{pmatrix} -1 & 0 & \ldots & 0 \\ 0 & 1 & \ldots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \ldots & 1 \end{pmatrix}$$

Определитель этой матрицы равен -1, и, таким образом, $\tau_w \notin SO(n)$. Однако имеет место следующая теорема.

Теорема 7.3. *Каждое нетождественное линейное преобразование из $SO(2)$ и $SO(3)$ можно представить в виде суперпозиции двух отражений.*

Доказательство. Пусть $\alpha \in SO(2)$. Так как $\alpha \neq 1$, то существуют два вектора $a \neq b$, такие, что $b = \alpha(a)$. Положим $c = a - b$ и рассмотрим отражение τ_c. Вычислим

$$\tau_c(b) = b - 2\frac{(b, c)}{(c, c)}c.$$

Известно, что в любом евклидовом пространстве

$$(v_1, v_2) = \frac{1}{2}(\| v_1 + v_2 \|^2 - \| v_1 \|^2 - \| v_2 \|^2).$$

(Правая часть — это выражение $\frac{1}{2}((v_1+v_2, v_1+v_2) - (v_1, v_1) - (v_2, v_2)) = \frac{1}{2}((v_1, v_1)+(v_1, v_2)+(v_2, v_1)+(v_2, v_2)-(v_1, v_1)-(v_2, v_2))$, и при этом $(v_1, v_2) = (v_2, v_1)$.)

Пусть $v_1 = b$, $v_2 = c$, тогда $v_1 + v_2 = a$, и мы приходим к равенству:

$$2(b, c) = \| a \|^2 - \| b \|^2 - \| c \|^2 .$$

Теперь вспомним, что отображение α ортогонально. Это значит, что $\| a \|^2 = (a, a) = (\alpha(a), \alpha(a)) = (b, b) = \| b \|^2$. В конечном счете получается, что $2(b, c) = - \| c \|^2 = (c, c)$. Подставляя это в выражение для $\tau_c(b)$, приходим к равенству: $\tau_c(b) = b + c = b + a - b = a$.

Теперь рассмотрим ортогональное линейное отображение $\xi = \tau_c\alpha$. По построению $\xi(a) = \tau_c(\alpha(a)) = \tau_c(b) = a$. Выберем вектор $w \neq 0$ так, чтобы $(a, w) = 0$. Поскольку все происходит пока в двумерном евклидовом пространстве, то векторы a, w будут его базисом. Ввиду того, что подпространство $V_1 = \langle a \rangle$ инвариантно относительно ξ, инвариантным будет и его ортогональное дополнение $V_2 = \langle w \rangle$. Следовательно, $\xi(w) = \lambda w$ для некоторого $\lambda \in \mathbb{R}$. Из ортогональности ξ следует, что $(\xi(w), \xi(w)) = (w, w) > 0$. Но, с другой стороны, $(\xi(w), \xi(w)) = (\lambda w, \lambda w) = \lambda^2(w, w)$. Отсюда $\lambda^2 = 1$. Если $\lambda = +1$, то $\xi = 1$, т.е. $\tau_c\alpha = 1$, а так как $\tau_c = \tau_c^{-1}$, то $\alpha = \tau_c$. Но это противоречит выбору $\alpha \in SO(2)$. Следовательно, $\xi(w) = -w$, а это значит, что $\xi = \tau_w$. Из $\tau_w = \tau_c\alpha$ теперь получаем $\alpha = \tau_c\tau_w$.

Пусть теперь V — техмерное евклидово пространство, и $\alpha \in SO(3)$ — нетождественное отображение. Как уже было показано, у α имеется собственное значение, равное единице. Выберем какой-нибудь собственный вектор e_1, отвечающий этому собственному значению, и пусть $V_1 = \langle e_1 \rangle$ — порожденное им подпространство. Очевидно, что $\alpha(v) = v$ для каждого $v \in V_1$. Пусть V_2 — ортогональное дополнение V_1. Это — двумерное евклидово пространство, и оно инвариантно относительно α. Ограничение α на V_2 является элементом группы $SO(2)$. Обозначим его через α'. Очевидно, что это — нетождественное отображение. К $\alpha' \in SO(2)$ применимо уже доказанное выше утверждение о том, что это — суперпозиция двух отражений. Но это отражения в V_2, а не в V! Обозначим их через τ'_c τ'_w. Здесь $w, c \in V_2$. Таким образом, пусть $\alpha' = \tau'_c\tau'_w$. Теперь рассмотрим отражения τ_c и t_v, действующие во всем пространстве V. Поскольку формулы, по которым они задаются, т.е.

$$\tau_c(v) = v - 2\frac{(v,c)}{(c,c)}c, \quad \text{и} \quad \tau_w(v) = v - 2\frac{(v,w)}{(w,w)}w$$

те же самые, что и у τ'_c и τ'_w, а отличие состоит только в том, что аргументы v принимают значения во всем пространстве V, то ограничения τ_c и τ_w на V_2 совпадают с τ'_c τ'_w. Следовательно, если $v \in V_2$, то $\alpha(v) = \alpha'(v) = \tau'_c(t'_w(v)) = \tau_c(t_w(v))$. Если же $v \in V_1$, то, так как $c, w \in V_2$, а V_2 — ортогональное дополнение к V_1, то $(v, c) = (v, w) = 0$, и $\tau_c(v) = \tau_w(v) = v = \alpha(v)$. Итак, если $v \in V_1$ или $v \in V_2$, то $\alpha(v) = \tau_c(\tau_w(v))$. Так как $V = V_1 \oplus V_2$, то это верно и для всех $v \in V$. Следовательно, $\alpha = \tau_c\tau_w$. $\square$

Опишем некоторые конечные подгруппы группы $SO(3)$.

Пример 7.1. Пусть Z_n — циклическая группа порядка n. Если x — какой-нибудь образующий Z_n, то $x^n = 1$ и $Z_n = \{1, x, \ldots, x^{n-1}\}$. Определим отображение $h : Z_n \longrightarrow SO(3)$, полагая

$$h(x^k) = \begin{pmatrix} \cos\dfrac{2\pi k}{n} & -\sin\dfrac{2\pi k}{n} & 0 \\ \sin\dfrac{2\pi k}{n} & \cos\dfrac{2\pi k}{n} & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Легко убедиться, что h является инъективным гомоморфизмом. Образ h, таким образом, циклическая подгруппа порядка n группы $SO(3)$, причем $n > 0$ — произвольное целое число.

7.8. Докажите, что h действительно является гомоморфизмом, и это отображение инъективно.

Пример 7.2. Напомним, что группа диэдра D_n описывается как подгруппа $GL_2(\mathbb{R})$, порожденная матрицами

$$a = \left(\begin{array}{cc} \cos\dfrac{2\pi k}{n} & -\sin\dfrac{2\pi k}{n} \\ \sin\dfrac{2\pi k}{n} & \cos\dfrac{2\pi k}{n} \end{array} \right) \quad \text{и} \quad b = \left(\begin{array}{cc} 0 & 1 \\ 1 & 0 \end{array} \right).$$

Будем считать известным, что группа D_n состоит из следующих $2n$ элементов:

$$1, a, a^2, \ldots, a^{n-1}, b, ab, a^2b, \ldots, a^{n-1}b.$$

При этом $a^n = 1$, $b^2 = 1$, $ba = a^{n-1}b$. С помощью этих трех соотношений можно произвести любые операции с элементами D_n, не обращаясь к их матричной форме.

Рассмотрим следующие элементы $SO(3)$:

$$A = \left(\begin{array}{ccc} \cos\dfrac{2\pi}{n} & -\sin\dfrac{2\pi}{n} & 0 \\ \sin\dfrac{2\pi}{n} & \cos\dfrac{2\pi}{n} & 0 \\ 0 & 0 & 1 \end{array} \right), \quad B = \left(\begin{array}{ccc} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & -1 \end{array} \right).$$

Прямым вычислением можно показать, что подгруппа группы $SO(3)$, порожденная матрицами A и B, состоит из $2n$ элементов:

$$E, A, A^2, \ldots, A^{n-1}, B, AB, A^2B, \ldots, A^{n-1}B.$$

При этом $A^n = B^2 = E$ и $BA = AB^{n-1}$.

Отсюда легко следует, что эта подгруппа $SO(3)$ изоморфна группе D_n, причем при изоморфизме соответствуют друг другу элементы A и a, B и b.

7.9. Проведите подробно вычисления и доказательства, опущенные в примере 7.2.

Пример 7.3. Пусть $\Gamma \subseteq \mathbb{R}^3$ — некоторое подмножество в трехмерном евклидовом пространстве (например, геометрическая фигура: сфера, шар, куб, тетраэдр и т.п.). Определим G_Γ как множество вращений $\alpha \in SO(3)$, обладающих свойством $\alpha(\Gamma) = \Gamma$. Иными словами, поворот

α (а мы уже знаем, что это поворот вокруг некоторой оси) совмещает множество Γ с самим собой. Элементы α с таким свойством естественно назвать *симметриями* множества (геометрической фигуры) Γ. Хотя вращения не являются единственным видом симметрии геометрических фигур, мы не будем рассматривать здесь другие виды симметрий, а сосредоточимся на множествах G_Γ.

Докажем, что G_Γ есть подгруппа $SO(3)$. В саом деле, ясно, что тождественное линейное преобразование (единица группы $SO(3)$) отображает Γ в Γ, и потому принадлежит G_Γ. Если $\alpha(\Gamma) = \Gamma$ и $\beta(\Gamma) = \Gamma$, то $\alpha\beta(\Gamma) = \alpha(\beta(\Gamma)) = \alpha(\Gamma) = \Gamma$, а значит $\alpha\beta \in G_\Gamma$. И, наконец, если $\alpha(\Gamma) = \Gamma$, то $\alpha^{-1}(\alpha(\Gamma)) = \alpha^{-1}(\Gamma)$, откуда $\Gamma = \alpha^{-1}(\Gamma)$ и $\alpha^{-1} \in G_\Gamma$.

Будем называть G_Γ *группой симметрий* или *группой вращений* фигуры Γ.

Отметим еще, что определено действие

$$G_\Gamma \times \Gamma \longrightarrow \Gamma.$$

Паре $\alpha \in G_\Gamma \subseteq SO(3)$ и $v \in \Gamma \subseteq \mathbb{R}^3$ сопоставляется точка (вектор) $\alpha v = \alpha(v)$. Проверку определения действия читатель должен рассматривать как (нетрудную) задачу.

Пример 7.4. Применим общую конструкцию предыдущего примера к простому, но интересному частному случаю. Пусть Γ — куб, геометрический центр которого помещен в начало координат. Можно представлятьс себе этот куб вписанным в сферу единичного радиуса, хотя это и не принципиально. Группа G_Γ в данном случае носит название группы вращений куба и обозначается в некоторых книгах (например, в [3]) через $\mathbf{O}$. Для того, чтобы оценить снизу порядок этой группы, можно воспользоваться геометрическими соображениями, и найти в кубе несколько осей симметрии, вращения вокруг которых переводят куб сам в себя.

Во-первых, это множество из трех осей, соединяющих центры противоположных граней куба. Граней всего 6, и это квадраты. Следовательно, осей будет три штуки. Обозначим множество таких осей через X. Вокруг каждой оси из X можно осуществить три нетривиальных поворота куба: на 90°, 180° и 270°. Поворот на 360° переместит куб в исходное положение, и поэтому его действие эквивалентно действию единицы группы $\mathbf{O}$ (а значит, он и есть эта самая единица). Таким образом, получаем 9 различных элементов $\mathbf{O}$ (три оси $\times$ три поворота вокруг каждой из них). Легко проверить, что все эти 9 вращений различны.

Во-вторых, рассмотрим оси симметрии, соединяющие середины противоположных ребер куба. Ребер у куба 12, поэтому таких осей будет 6. Обозначим множество, состоящее из них, через Y. Читателю рекомендуется нарисовать картинку, где изображена хотя бы одна такая ось, чтобы легче было понять, что вокруг каждой такой оси возможен лишь один нетривиальный поворот на $180°$. Следовательно, получаем еще 6 элементов группы $\mathbf{O}$.

В-третьих, рассмотрим диагонали куба. Это множество (обозначим его через Z) состоит из четырех элементов. Выбрав одну из диагоналей, и нарисовав куб таким образом, чтобы эта диагональ была перпендикулярна плоскости рисунка, легко увидеть, что нетривиальных поворотов вокруг этой оси всего два: на $120°$ и на $240°$. Таким образом, получаем еще 8 элементов группы $\mathbf{O}$. Добавляя к уже перечисленным единицу группы, делаем вывод, что в этой группе не менее 24 элементов.

7.10. Чтобы снять возникающий вопрос о том, а нет ли среди найденных элементов (вращений) на самом деле совпадающих, можно поступить следующим образом. Обозначим через $Vert$ множество всех вершин куба. Их всего 8, и можно перенумеровать их числами от 1 до 8. Каждое вращение из $\mathbf{O}$ каким-то образом переставляет местами эти вершины, и это определяет действие

$$\mathbf{O} \times Vert \longrightarrow Vert.$$

Этому действию соответствует гомоморфизм $\mathbf{O} \longrightarrow S_8$, сопоставляющий вращению соответствующую ему подстановку (перестановку множества вершин). Очевидно, что этот гомоморфизм инъективен. Теперь можно вычислить все подстановки из S_8, соответствующие описанным выше вращениям. Проделайте эти вычисления, и убедитесь, что всем двадцати четырем вращениям соответствуют разные подстановки из S_8.

7.11. Доказать, что описанное выше действие $\mathbf{O}$ на $Vert$ транзитивно, то есть имеет всего одну орбиту.

Указание. Транзитивность в данном случае означает, что для любых двух $v_1, v_2 \in Vert$ найдется $\alpha \in \mathbf{O}$ такой, что $v_2 = \alpha(v_1)$. Оказывается, что можно обойтись только суперпозициями вращений вокруг осей из множества X. В самом деле, если v_1 и v_2 расположены на одной грани куба, то достаточно одного такого вращения. Если v_1 и v_2 расположены на смежных гранях, то найдется вершина куба v, которая принадлежит одновременно грани, содержащей v_1, и грани, содержащей v_2. В этом случае надо сначала осуществить поворот, переводящий v_1 в v, а затем поворот, перводящий v в v_2. Остается рассмотреть случай, когда v_1 и v_2 принадлежат несмежным граням.

Продолжим изучение действия $\mathbf{O}$ на множестве $Vert$ вершин куба. Пусть $v \in Vert$. Что можно сказать о стабилизаторе $St(v)$ этой вершины? Если $\alpha \in St(v)$, то должна существовать ось вращения α, и она состоит в точности из всех тех точек $\mathbb{R}^3$, которые не меняются под действием α. Следовательно, сама вершина v должна лежать на этой оси. Но известна еще одна точка оси вращения α: начало координат, геометрический центр куба. Ось, проходящая через эти две точки, содержит диагональ куба, и, следовательно, все вращения вокруг этой оси (и только они), содержащиеся в $\mathbf{O}$, будут оставлять на месте вершину v. Таких вращений всего 3, и они образуют всю подгруппу $St(v)$. Применим к этой ситуации известный результат: мощность орбиты равна индексу $\mathbf{O}$ по стабилизатору любого элемента орбиты. В нашей ситуации мощность орбиты известна и равна 8, а индекс равен $|\mathbf{O}|/|St(v)| = \frac{1}{3}|\mathbf{O}|$. Отсюда получаем $|\mathbf{O}| = 3 \cdot 8 = 24$. Из этого следует, что $\mathbf{O}$ состоит только из описанных ранее вращений, и других элементов в группе $\mathbf{O}$ нет.

7.12. Убедитесь, что вращения, переводящие куб сам в себя, отображают оси симметрии из множеств X, Y, Z в оси симметрии из тех же самых множеств. Тем самым определены три действия группы $\mathbf{O}$:

$$\mathbf{O} \times X \longrightarrow X\ ,\ \mathbf{O} \times Y \longrightarrow Y\ ,\ \mathbf{O} \times Z \longrightarrow Z,$$

и три соответствующих им гомоморфизма

$$\mathbf{O} \longrightarrow S_3, \quad \mathbf{O} \longrightarrow S_6, \quad \mathbf{O} \longrightarrow S_4.$$

Вычислите в явном виде, в какие подстановки из S_3, S_6 и S_4 отображаются описанные выше явно вращения из группы $\mathbf{O}$. Докажите, что действия $\mathbf{O}$ на X, Y, Z транзитивны.

Рассмотрим более подробно действие группы вращений куба на множестве из четырех диагоналей куба, и соответствующий ему гомоморфизм $h : \mathbf{O} \longrightarrow S_4$. Вычислим ядро этого гомоморфизма. Оно должно состоять из вращений, оставляющих неподвижными все четыре диагонали куба. Но кроме тождественного линейного отображения, никакой из перечисленных выше 23 нетривиальных элементов группы $\mathbf{O}$ таким свойством не обладает (проверьте это). Таким образом, имеет место инъективный гомоморфизм группы $\mathbf{O}$, состоящей из 24 элементов, в группу S_4, также состоящуюиз 24 элементов. Следовательно, этот гомоморфизм является биекцией. Тем самым доказана следующая теорема.

Теорема 7.4. *Группа вращений куба* $\mathbf{O}$ *изоморфна группе* S_4.

Опишем вкратце, в какие подстановки отображает гомоморфизм из $\mathbf{O}$ в S_4 элементы $\mathbf{O}$. Вращения на 90° и 270° вокруг осей из множества Y отображаются в циклы длины 4. Вращения на 180° отображаются в произведения двух независимых транспозиций. Вращения на 180° вокруг осей из множества Y отображаются в транспозиции. Наконец, вращения вокруг диагоналей отображаются в тройные циклы. Все это проверяется прямыми вычислениями, причем удобнее всего в каждом случае рисовать картинку.

Пример 7.5. Рассмотрим группу вращений тетраэдра, геометрический центр которого находится в начале кооординат. Удобно представлять себе тетраэдр вписанным в куб. Тогда диагонали куба окажутся высотами тетраэдра, т.е. линиями, проведенными из вершин тетраэдра перпендикулярно противолежащим граням.

Обозначим через $\mathbf{T}$ группу вращений тетраэдра. Если представить себе куб вместе со вписанным в него тетраэдром как жесткую конструкцию, то становится ясно, что любое вращение тетраэдра, совмещающее его с самим собой, будет также и вращением куба, т.е. элементом группы $\mathbf{O}$. Таким образом, $\mathbf{T}$ как подгруппа $SO(3)$ будет также и подгруппой $\mathbf{O} \subseteq SO(3)$. Биективный гомоморфизм $\mathbf{O} \to S_4$ биективно отображает подгруппу $\mathbf{T}$ на некоторую подгруппу S_4. Выясним, что это за подгруппа. Легко проверяется, что вращения на 180° вокруг осей симметрии куба, соединяющих середины противоположных граней куба (множество Y) не являются симметриями тетраэдра. Не являются симметриями вписанного тетраэдра также вращения на 90° и 270° вокруг осей, соединяющих середины противоположных граней квадрата. Эти оси соединяют середины противоположных (взаимно перпендикулярных) ребер тетраэдра, и вращения вокруг них на 180° симметриями тетраэдра являются. Наконец, как уже было сказано, диагонали куба содержат в себе высоты вписанного тетраэдра, и каждое вращение куба вокруг этих осей (на 120° и 240°) соответствует вращению тетраэдра вокруг своей соответствующей высоты, совмещающщему тетраэдр с самим собой. Других вращательных симметрий у тетраэдра нет. Вспоминая, в какие подстановки из S_4 отображаются описанные только что вращения, видим, что это всевозможные циклы длины 3 и произведения циклов длины 2. Все эти подстановки (вместе с единичной) образуют знакопеременную группу A_4. Таким образом, доказана следующая теорема.

Теорема 7.5. *Группа* $\mathbf{T}$ *вращений тетраэдра изоморфна группе* A_4.

Кроме куба и тетраэдра, в трехмерном евклидовом пространстве имеются еще три правильных многогранника: октаэдр, икосаэдр и додекаэдр. Это так называемые “платоновы тела". Некоторые подробности о них можно узнать в [22]. Октаэдр тесно связан с кубом: если соединить отрезками середины граней куба, то получится контур октаэдра — правильного 8-гранника, все грани которого являются равносторонними треугольниками. Вращательные симметрии октаэдра и куба полностью совпадают, это одна и та же подгруппа группы $SO(3)$, обозначенная выше через $\mathbf{O}$. Само название, кстати, указывает на октаэдр. Икосаэдр — это правильный 20-гранник, все грани которого равносторонние треугольники, а додекаэдр — правильный 12-гранник, все грани которого правильные пятиугольники. Икосаэдр связан с додекаэдром примерно так же, как октаэдр с кубом: соединение центров граней икосаэдра отрезками прямых образует контур додекаэдра, а соединение центров граней додекаэдра образует икосаэдр. Поэтому у этих многогранников одна и та же группа вращательных симметрий, называемая группой икосаэдра и обозначаемая через $\mathbf{I}$. Рассуждения, аналогичные тем, которые были использованы при изучении группы $\mathbf{O}$ (только более длинные) показывают, что справедлива следующая теорема:

Теорема 7.6. *Имеет место изоморфизм:*

$$\mathbf{I} \cong A_5.$$

Оказывается, что других конечных подгрупп, кроме групп, изоморфных Z_n, D_n, $\mathbf{O}$, $\mathbf{T}$, $\mathbf{I}$, в группе $SO(3)$ нет. Подробное доказательство этого факта можно найти в § 3 главы 3 книги [3]. Книга [3], впрочем, не является первой, где приведено это доказательство: см., например, книгу [23]. Существенные подробности о группах симметрии геометрических фигур можно найти также в главе 11 книги [24]. О применениях теории групп в физике, которые также связаны с понятием симметрии, можно узнать из книг [26], [27], [28]. Идея симметрии и некоторые другие применения теории групп (например, в кристаллографии) на популярном уровне обсуждается в книге [25]. Отметим, наконец, перевод старой книги Ф.Клейна [18], где описываются связи между группой вращений икосаэдра и такими, на первый взгляд, слабо связанными с ней теориями, как дифференциальные уравнения, теория инвариантов и т.д.

8. Кватернионы

Обозначим через $\mathbf{H}$ множество всевозможных матриц вида

$$\begin{pmatrix} z_1 & z_2 \\ -\overline{z}_2 & \overline{z}_1 \end{pmatrix},$$

где $z_1, z_2 \in \mathbb{C}$ — комплексные числа.

Теорема 8.1. *Множество* $\mathbf{H}$ *является подкольцом кольца всех комплекснозначных* 2×2*-матриц* $M_2(\mathbb{C})$*, а также подпространством* $M_2(\mathbb{C})$ *как линейного пространства над полем* $\mathbb{R}$.

Доказательство. Очевидно, что нулевая и единичная матрицы содержатся в множестве $\mathbf{H}$. Из равенств

$$\begin{pmatrix} z_1 & z_2 \\ -\overline{z}_2 & \overline{z}_1 \end{pmatrix} \pm \begin{pmatrix} w_1 & w_2 \\ -\overline{w}_2 & \overline{w}_1 \end{pmatrix} = \begin{pmatrix} z_1 \pm w_1 & z_2 \pm w_2 \\ (-\overline{z}_2) \pm (-\overline{w}_2) & \overline{z}_1 \pm \overline{w}_1 \end{pmatrix} = \\ = \begin{pmatrix} z_1 \pm w_1 & z_2 \pm w_2 \\ -\overline{(z_2 \pm w_2)} & \overline{(z_1 \pm w_1)} \end{pmatrix}$$

и

$$\begin{pmatrix} z_1 & z_2 \\ -\overline{z}_2 & \overline{z}_1 \end{pmatrix} \begin{pmatrix} w_1 & w_2 \\ -\overline{w}_2 & \overline{w}_1 \end{pmatrix} = \begin{pmatrix} z_1 w_1 - z_2 \overline{w}_2 & z_1 w_2 + z_2 \overline{w}_1 \\ -\overline{z}_2 w_1 - \overline{z}_1 \overline{w}_2 & -\overline{z}_2 w_2 + \overline{z}_1 \overline{w}_1 \end{pmatrix} = \\ = \begin{pmatrix} z_1 w_1 - z_2 \overline{w}_2 & z_1 w_2 + z_2 \overline{w}_1 \\ -\overline{(z_2 \overline{w}_1 + z_1 w_2)} & \overline{(-z_2 \overline{w}_2 + z_1 w_1)} \end{pmatrix}$$

следует, что множество $\mathbf{H}$ замкнуто отностительно сложения, вычитания и умножения. Таким образом, оно является подкольцом кольца $M_2(\mathbb{C})$. Пусть $\lambda \in \mathbb{R}$, $z_1, z_2 \in \mathbb{C}$. Тогда

$$\lambda \begin{pmatrix} z_1 & z_2 \\ -\overline{z_2} & \overline{z_1} \end{pmatrix} = \begin{pmatrix} \lambda z_1 & \lambda z_2 \\ -\lambda \overline{z_2} & \lambda \overline{z_1} \end{pmatrix} = \begin{pmatrix} \lambda z_1 & \lambda z_2 \\ -\overline{\lambda z_2} & \overline{\lambda z_1} \end{pmatrix}.$$

Итак, аддитивная подгруппа группа $\mathbf{H}$ линейного пространства $M_2(\mathbb{C})$ замкнута отностительно умножения на элементы поля $\mathbb{R}$. Следовательно, она является линейным пространством над этим полем — подпространством $M_2(\mathbb{C})$. $\square$

Элементы кольца $\mathbf{H}$ называются *кватернионами*. Кольцо кватернионов в некоторых отношениях походит на поле комплексных чисел. В дальнейшем будем обозначать кватернионы подужирными буквами, например, $\mathbf{q}$. Пусть

$$\mathbf{q} = \begin{pmatrix} t + ix & y + iz \\ -y + iz & t - ix \end{pmatrix}.$$

Тогда

$$\mathbf{q} = t \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + x \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} + y \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} + z \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}.$$

Положим

$$\mathbf{1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \mathbf{i} = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \quad \mathbf{j} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad \mathbf{k} = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix},$$

так что $\mathbf{q} = t\mathbf{1}+x\mathbf{i}+y\mathbf{j}+z\mathbf{k}$. Очевидно, что $\mathbf{1}, \mathbf{i}, \mathbf{j}, \mathbf{k}$ — базис $\mathbb{R}$-линейного пространства $\mathbf{H}$.

Элемент $\mathbf{1}$ является единицей кольца $\mathbf{H}$, а соответствие $\lambda \mapsto \lambda\mathbf{1}$ есть инъективный гомоморфизм поля $\mathbb{R}$ в кольцо $\mathbf{H}$. Легко проверяется, что $\mathbf{wq} = \mathbf{qw}$ для каждого $\mathbf{q}$ тогда и только тогда, если $\mathbf{w} = \lambda\mathbf{1}$ для некоторого $\lambda \in \mathbb{R}$ (если читатель все же испытал затруднения, то он может посмотреть доказательство теоремы 9.1 из следующего раздела). Ввиду этого, когда речь идет о кватернионах, принято отождествлять элементы $\lambda\mathbf{1}$ с элементами $\lambda \in \mathbb{R}$. Таким образом, будеи использоваться запись $\mathbf{q} = t + x\mathbf{i} + y\mathbf{j} + z\mathbf{k}$.

“Таблица умножения"для элементов базиса $\mathbf{H}$ выглядит теперь следующим образом:

$$\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = -1,$$

$$\mathbf{ij} = \mathbf{k} = -\mathbf{ji}, \quad \mathbf{jk} = \mathbf{i} = -\mathbf{kj}, \quad \mathbf{ki} = \mathbf{j} = -\mathbf{ik}.$$

Из этого следует, во-первых, что кольцо $\mathbf{H}$ некоммутативно. Во-вторых, что любое из подпространств $\mathbb{R} + \mathbb{R}\mathbf{i}$, $\mathbb{R} + \mathbb{R}\mathbf{j}$, $\mathbb{R} + \mathbb{R}\mathbf{k}$ есть подкольцо, изоморфное полю $\mathbb{C}$. Таким образом, кольцо $\mathbf{H}$ содержит в себе и поле $\mathbb{R}$, и поле $\mathbb{C}$.

Для произвольного кватерниона $\mathbf{q} = t + x\mathbf{i} + y\mathbf{j} + z\mathbf{k}$ определим сопряженный к нему кватернион $\overline{\mathbf{q}} = t - x\mathbf{i} - y\mathbf{j} - z\mathbf{k}$. В матричной форме, если

$$\mathbf{q} = \begin{pmatrix} z_1 & z_2 \\ -\overline{z_2} & \overline{z_1} \end{pmatrix},$$

то

$$\overline{\mathbf{q}} = \begin{pmatrix} \overline{z_1} & -z_2 \\ \overline{z_2} & z_1 \end{pmatrix}.$$

Очевидно, что, как и для сопряжения комплексных чисел, $\overline{\overline{\mathbf{q}}} = \mathbf{q}$, $\overline{\lambda_1\mathbf{q}_1 + \lambda_2\mathbf{q}_2} = \lambda_1\overline{\mathbf{q}_1} = \lambda_2\overline{\mathbf{q}_2}$ при $\lambda_1, \lambda_2 \in \mathbb{R}$.

8.1. Проверить, что

$$\mathbf{q}\overline{\mathbf{q}} = \overline{\mathbf{q}}\mathbf{q} = \begin{pmatrix} |z_1|^2 + |z_2|^2 & 0 \\ 0 & |z_1|^2 + |z_2|^2 \end{pmatrix} =$$
$$= (|z_1|^2 + |z_2|^2)\mathbf{1} = |z_1|^2 + |z_2|^2 = t^2 + x^2 + y^2 + z^2.$$

Ввиду этого логично назвать число $\mathbf{q}\overline{\mathbf{q}} = \overline{\mathbf{q}}\mathbf{q}$ квадратом *модуля* кватерниона $\mathbf{q}$ и обозначить через $|\mathbf{q}|^2$. Если мыслить кватернион $\mathbf{q}$ как вектор в четырехмерном евклидовом пространстве с координатами (t,x,y,z), то его модуль $|\mathbf{q}| = \sqrt{\mathbf{q}\overline{\mathbf{q}}} = \sqrt{t^2+x^2+y^2+z^2}$ является длиной этого вектора. Часто число $\mathbf{q}\overline{\mathbf{q}} = \overline{\mathbf{q}}\mathbf{q} \in \mathbb{R} \subset \mathbf{H}$ называется также *нормой* кватерниона $\mathbf{q}$ и обозначается через $N(\mathbf{q})$. И норма, и модуль кватерниона — неотрицательные действительные числа, $N(\mathbf{q}) = |\mathbf{q}|^2$.

8.2. Проверить, что $N(\mathbf{q}) = 0$ тогда и только тогда, если $\mathbf{q} = 0$.

Заметим еще, что

$$det \begin{pmatrix} z_1 & z_2 \\ -\overline{z_2} & \overline{z_1} \end{pmatrix} = |z_1|^2 + |z_2|^2.$$

Теорема 8.2. *Каждый ненулевой элемент кольца* $\mathbf{H}$ *обладает обратным (по умножению) элементом.*

Доказательство. Рассмотрим $\mathbf{q} \in \mathbf{H}$, $\mathbf{q} \neq 0$. Тогда $\overline{\mathbf{q}}\mathbf{q} = \mathbf{q}\overline{\mathbf{q}} = N(\mathbf{q}) > 0$. Ввиду того, что $N(\mathbf{q}) \in \mathbb{R}$, существует элемент $\dfrac{1}{N(\mathbf{q})} \in \mathbb{R}$. Умножим этот элемент на все части равенств $\overline{\mathbf{q}}\mathbf{q} = \mathbf{q}\overline{\mathbf{q}} = N(\mathbf{q})$. Получим

$$(\frac{1}{N(\mathbf{q})}\overline{\mathbf{q}})\mathbf{q} = \mathbf{q}(\frac{1}{N(\mathbf{q})}\overline{\mathbf{q}}) = 1.$$

Следовательно, $\mathbf{q}^{-1} = \dfrac{1}{N(\mathbf{q})}\overline{\mathbf{q}}$. Заметим, что эта формула обобщает формулу для обратного к комплексному числу. □

Кольцо $\mathbf{H}$ походит на поле, но поля по определению коммутативны. Ассоциативные кольца, которые не обязательно коммутативны, но обладают тем свойством,что каждый их ненулевой элемент имеет обратный по умножению, назвыаются *телами*. Таким образом, кольцо $\mathbf{H}$ называется *телом кватернионов* (или *гамильтоновых кватернионов*).

Через $\mathbf{H}^*$ обозначим множество ненулевых кватернионов. Это группа по умножению.

8.3. Элементы $\pm\mathbf{1}$, $\pm\mathbf{i}$, $\pm\mathbf{j}$, $\pm\mathbf{k}$ образуют подгруппу группы $\mathbf{H}^*$. Эта подгруппа изоморфна группе Q_8, введенной выше в разделе 2.

Опишем один способ вычислений с кватернионами. Отождествим поле $\mathbb{C}$ с подкольцом $\mathbb{R}+\mathbb{R}\mathbf{i}$ тела $\mathbf{H}$. Пусть $u = t + x\mathbf{i}, v = y + z\mathbf{i}$ — два комплексных числа. Тогда

$$t + x\mathbf{i} + y\mathbf{j} + z\mathbf{k} = t + x\mathbf{i} + y\mathbf{j} + x\mathbf{ij} = (t + x\mathbf{i}) + (y + z\mathbf{i})\mathbf{j} = u + v\mathbf{j} \qquad (1)$$

При этом $\mathbf{j}v = y\mathbf{j} + z\mathbf{ji} = y\mathbf{j} - z\mathbf{ij} = (y - z\mathbf{i})\mathbf{j} = \overline{v}\mathbf{j}$. Этого соотношения вместе с равенством $\mathbf{j}^2 = -1$ (плюс свойства комплексных чисел) вполне достаточно для того, чтобы проводить вычисления с кватернионами, записанными в форме (1). Заметим, что запись (1) можно истолковать еще и так: $\mathbf{H}$ есть линейное пространство над полем $\mathbb{C}$ с базисом из двух элементов: $\mathbf{1}$ (или 1) и $\mathbf{j}$. Отметим, что

$$\overline{\mathbf{q}} = \overline{u} - v\mathbf{j}.$$

Применим эту технику для решения нескольких задач.

Пример 8.1. Докажем, что что $\overline{\mathbf{q}_1\mathbf{q}_2} = \overline{\mathbf{q}}_2\overline{\mathbf{q}}_1$ для любых $\mathbf{q}_1, \mathbf{q}_2 \in \mathbf{H}$.

Представим кватернионы $\mathbf{q}_1$ и $\mathbf{q}_2$ в форме (1): $\mathbf{q}_1 = u_1 + v_1\mathbf{j}$, $\mathbf{q}_2 = u_2 + v_2\mathbf{j}$, $u_1, v_1, u_2, v_2 \in \mathbb{C}$. Тогда

$$\mathbf{q}_1\mathbf{q}_2 = (u_1u_2 - v_1\overline{v}_2) + (u_1v_2 + \overline{u}_2v_1)\mathbf{j} \qquad (2)$$

Вычисляем сопряженный кватернион:

$$\overline{\mathbf{q}_1\mathbf{q}_2} = (\overline{u}_1\overline{u}_2 - \overline{v}_1v_2) - (u_1v_2 + \overline{u}_2v_1)\mathbf{j}$$

С другой стороны,

$$\overline{\mathbf{q}}_s = \overline{u}_s - v_s\mathbf{j}, \quad s = 1, 2.$$

Следовательно, согласно (2), получим

$$\overline{q}_2\overline{q}_1 = (\overline{v}_2\overline{u}_1 - v_2\overline{v}_1) + (-v_2u_1 - \overline{u}_2v_1)\mathbf{j}.$$

Таким образом, имеет место требуемое равенство.

8.4. Доказать, что $N(\mathbf{q}_1\mathbf{q}_2) = N(\mathbf{q}_1)N(\mathbf{q}_2)$ и $|\mathbf{q}_1\mathbf{q}_2| = |\mathbf{q}_1| \cdot |\mathbf{q}_2|$.

Пример 8.2. Решим уравнение $\mathbf{q}^2 = -1$. Пусть $\mathbf{q} = u + v\mathbf{j}$, $u = t + x\mathbf{i}$, $v = y + z\mathbf{i}$. Используя (2), получаем равенство:

$$\mathbf{q}^2 = (u^2 - v\overline{v}) + v(u + \overline{u})\mathbf{j} \tag{3}$$

Приравнивая коэффициенты при одинаковых базисных векторах у $\mathbf{q}^2$ и $-1 = (-1)\mathbf{1} + 0\mathbf{j}$, получаем систему уравнений с двумя комплекснозначными неизвестными u и v:

$$\begin{cases} u^2 - |v|^2 = -1 \\ v(u + \overline{u}) = 0 \end{cases}$$

Начнем со второго уравнения. Из $v(u + \overline{u}) = 0$ следует, что либо $v = 0$, либо $u + \overline{u} = 0$. Итак, пусть $u + \overline{u} = 0$. Так как $u = t + x\mathbf{i}$, то это равносильно равенству $t = 0$. В этом случае $\mathbf{u}^2 = (x\mathbf{i})^2 = -x^2$, и первое уравнение превращается в

$$-x^2 - |v|^2 = -x^2 - y^2 - z^2 = -1,$$

или

$$x^2 + y^2 + z^2 = 1 \tag{4}$$

Итак, решениями уравнения $\mathbf{q}^2 = -1$ будут все $\mathbf{q} = u + v\mathbf{j}$, такие, что $u = x\mathbf{i}$, $v = y + z\mathbf{i}$, и x, y, z удовлетворяют соотношению (4).

Разберем случай $v = 0$. Тогда первое уравнение превращается в $u^2 = -1$. Если $u = t + x\mathbf{i}$, то получаем систему из двух уравнений с двумя неизвестными t, x, принимающими действительные значения:

$$\begin{cases} t^2 - x^2 = -1 \\ 2tx = 0 \end{cases} \tag{5}$$

Из второго уравнения (5) следует, что либо $t = 0$, либо $x = 0$ (возможно, что и то, и другое). Если $t = 0$, то $x^2 = 1$, а так как $v = 0$ означает $y = z = 0$, то получились решения из множества, описываемого равенствами $t = 0$ и (4). Если же $x = 0$, то приходим к противоречию: $t^2 = -1$ (напомним, что t может быть только действительным).

8.5. Решить уравнение $\mathbf{q}^2 = +1$.

8.6. Решить уравнение $\mathbf{q}^2 + \mathbf{q} + 1 = 0$.

8.7. Исследовать кватернионные решения уравнения $\mathbf{q}^2 + a\mathbf{q} + b = 0$, где $a, b \in \mathbb{R}$.

Пример 8.3. Пусть $\mathbf{q} = t + x\mathbf{i} + y\mathbf{j} + z\mathbf{k}$. Тогда $\overline{\mathbf{q}} = t - x\mathbf{i} - y\mathbf{j} - z\mathbf{k}$, $\mathbf{q} + \overline{\mathbf{q}} = 2t = a$, $\overline{\mathbf{q}}\mathbf{q} = t^2 + x^2 + y^2 + z^2 = b$, $a, b \in \mathbb{R}$. Рассмотрим тождество:

$$\mathbf{q}^2 - (\mathbf{q} + \overline{\mathbf{q}})\mathbf{q} + \overline{\mathbf{q}}\mathbf{q} = 0.$$

Замненяя $\mathbf{q} + \overline{\mathbf{q}}$ на a, и $\overline{\mathbf{q}}\mathbf{q}$ на b, получаем равенство:

$$\mathbf{q}^2 - a\mathbf{q} + b = 0.$$

Итак, каждый кватернион является корнем некоторого квадратного уравнения с действительными коэффициентами.

Теорема 8.3. *Пусть* $\mathbf{q} = t + x\mathbf{i} + y\mathbf{j} + z\mathbf{k}$. *Условие* $t = 0$ *равносильно тому, что* $\mathbf{q}^2 \le 0$.

Доказательство. Условие $\mathbf{q}^2 \le 0$ означает в частности, что кватернион $\mathbf{q}^2$ является скалярным, т.е. принадлежит множеству $\mathbb{R} = \{\lambda \mathbf{1} | \lambda \in \mathbb{R}\}$, т.е. $\mathbf{q}^2 = \lambda \mathbf{1}$, где $\lambda \in \mathbb{R}$, и при этом $\lambda < 0$. Вычисляя $\mathbf{q}^2$ и проделывая выкладки, аналогичные тем, что были проделаны в примере 8.2, получаем систему из неравенства и уравнения:

$$\begin{cases} u^2 - |v|^2 \le 0 \\ v(u + \overline{u}) = 0 \end{cases} \tag{6}$$

Итак, эта система равносильна условию $\mathbf{q}^2 \le 0$. Если $t = 0$, то $u = x\mathbf{i}$, $\overline{u} = -x\mathbf{i}$, $u + \overline{u} = 0$, и второе равенство из (6) выполнено. С другой стороны, $u^2 = -x^2$, и первое неравенство из (6) превращается в

$$-x^2 - y^2 - z^2 \le 0,$$

а это верно для любых действительных x, y, z.

Обратно, решая систему (5), начинаем со второго уравнения. Случай $u + \overline{u} = 0$ автоматически влечет $t = 0$. Случай $v = 0$ приводит к $u^2 \le 0$, откуда получаем систему, похожую на (5):

$$\begin{cases} t^2 - x^2 \le 0 \\ 2tx = 0 \end{cases}$$

Если $t = 0$, то все доказано. Случай $x = 0$ и $t \neq 0$ приводит к противоречию. $\square$

8.8. Какие кватернионы удовлетворяют неравенству $\mathbf{q}^2 \geq 0$?

Кватернионы вида $\mathbf{v} = x\mathbf{i}+y\mathbf{j}+z\mathbf{k}$ будем называть *векторами.* Другое название — *чисто векторные кватернионы.* Множество всех кватернионов –векторов будем обозначать через $\mathbf{V}$. Это — трехмерное линейное пространство над полем $\mathbb{R}$ с базисом $\mathbf{i}, \mathbf{j}, \mathbf{k}$. В произвольном кватернионе $\mathbf{q} = t + x\mathbf{i} + y\mathbf{j} + z\mathbf{k}$ слагаемое t называется скалярной частью кватерниона, а $x\mathbf{i} + y\mathbf{j} + z\mathbf{k}$ — векторной частью кватерниона $\mathbf{q}$. Итак, $\mathbf{v} \in \mathbf{V}$ тогда и только тогда, если $\mathbf{v}^2 \leq 0$.

Пусть $\mathbf{v}_1 = x_1\mathbf{i} + y_1\mathbf{j} + z_1\mathbf{k}$, $\mathbf{v}_2 = x_2\mathbf{i} + y_2\mathbf{j} + z_2\mathbf{k}$ — два вектора. Вычислим в явном виде их произведение.

$$\begin{aligned} \mathbf{v}_1\mathbf{v}_2 = \ & -(x_1x_2 + y_1y_2 + z_1z_2)+ \\ & +(y_1z_2 - z_1y_2)\mathbf{i}+ \\ & +(z_1x_2 - x_1z_2)\mathbf{j}+ \\ & +(x_1y_2 - y_1x_2)\mathbf{k} \end{aligned}$$

Скалярная часть этого кватерниона — не что иное, как скалярное произведение векторов $\mathbf{v}_1$ и $\mathbf{v}_2$, взятое со знаком минус. Векторную часть $\mathbf{v}_1\mathbf{v}_2$ можно (несколько условно) записать как определитель:

$$\begin{vmatrix} \mathbf{i} & \mathbf{j} & \mathbf{k} \\ x_1 & y_1 & z_1 \\ x_2 & y_2 & z_2 \end{vmatrix}$$

Очевидно, что это координатная запись известного из курса геометрии векторного произведения $[\mathbf{v}_1, \mathbf{v}_2]$ векторов $\mathbf{v}_1$ и $\mathbf{v}_2$. В конечном счете получается важное соотношение:

$$\mathbf{v}_1\mathbf{v}_2 = -(\mathbf{v}_1, \mathbf{v}_2) + [\mathbf{v}_1, \mathbf{v}_2] \tag{7}$$

Рассмотрим другое произведение:

$$\mathbf{v}_2\mathbf{v}_1 = -(\mathbf{v}_2, \mathbf{v}_1) + [\mathbf{v}_2, \mathbf{v}_1].$$

Так как $(\mathbf{v}_2, \mathbf{v}_1) = (\mathbf{v}_1, \mathbf{v}_2)$, а $[\mathbf{v}_2, \mathbf{v}_1] = -[\mathbf{v}_1, \mathbf{v}_2]$, то получим

$$\mathbf{v}_2\mathbf{v}_1 = -(\mathbf{v}_1, \mathbf{v}_2) - [\mathbf{v}_1, \mathbf{v}_2] \tag{8}$$

Из (7) и (8) получаем следующие равенства:

$$(\mathbf{v}_1, \mathbf{v}_2) = -\frac{1}{2}(\mathbf{v}_1\mathbf{v}_2 + \mathbf{v}_2\mathbf{v}_1) \tag{9}$$

$$[\mathbf{v}_1, \mathbf{v}_2] = \frac{1}{2}(\mathbf{v}_1\mathbf{v}_2 - \mathbf{v}_2\mathbf{v}_1) \tag{10}$$

Пример 8.4. Непосредственные вычисления показывают, что $(\mathbf{i}, \mathbf{i}) = (\mathbf{j}, \mathbf{j}) = (\mathbf{k}, \mathbf{k}) = 1$, $(\mathbf{i}, \mathbf{j}) = (\mathbf{j}, \mathbf{k}) = (\mathbf{k}, \mathbf{i}) = 0$,
$[\mathbf{i}, \mathbf{j}] = \mathbf{k}$, $[\mathbf{j}, \mathbf{k}] = \mathbf{i}$, $[\mathbf{k}, \mathbf{i}] = \mathbf{j}$.

На языке кватернионов легко получить доказательства основных тождеств векторной алгебры трехмерного пространства. При решении дальнейших задач используется тот факт, что $\mathbf{v}_1\mathbf{v}_2 + \mathbf{v}_2\mathbf{v}_1$ отличается от скаляра $(\mathbf{v}_1, \mathbf{v}_2)$ только скалярным множителем. Следовательно, $\mathbf{v}_1\mathbf{v}_2 + \mathbf{v}_2\mathbf{v}_1$ тоже скаляр. Это значит, что для произвольного кватерниона $\mathbf{q}$ имеет место равенство:

$$\mathbf{q}(\mathbf{v}_1\mathbf{v}_2 + \mathbf{v}_2\mathbf{v}_1) = (\mathbf{v}_1\mathbf{v}_2 + \mathbf{v}_2\mathbf{v}_1)\mathbf{q} \tag{11}$$

8.9. Пусть $\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3 \in \mathbf{V}$. Доказать, что имеет место равенство:

$$([\mathbf{v}_1, \mathbf{v}_2], \mathbf{v}_3) = (\mathbf{v}_1, [\mathbf{v}_2, \mathbf{v}_3])$$

8.10. Пусть $\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3 \in \mathbf{V}$. Доказать, что имеет место равенство:

$$[\mathbf{v}_1, [\mathbf{v}_2, \mathbf{v}_3]] = \mathbf{v}_2(\mathbf{v}_1, \mathbf{v}_3) - \mathbf{v}_3(\mathbf{v}_1, \mathbf{v}_2)$$

8.11. Пусть $\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3, \mathbf{v}_4 \in \mathbf{V}$. Доказать, что имеет место равенство:

$$([\mathbf{v}_1, \mathbf{v}_2], [\mathbf{v}_3, \mathbf{v}_4]) = (\mathbf{v}_1, \mathbf{v}_3)(\mathbf{v}_2, \mathbf{v}_4) - (\mathbf{v}_2, \mathbf{v}_3)(\mathbf{v}_1, \mathbf{v}_4)$$

Это равенство называется *тождеством Лагранжа.*

8.12. Пусть $\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3 \in \mathbf{V}$. Доказать, что имеет место равенство:

$$[[\mathbf{v}_1, \mathbf{v}_2], \mathbf{v}_3] + [[\mathbf{v}_3, \mathbf{v}_1], \mathbf{v}_2] + [[\mathbf{v}_2, \mathbf{v}_3], \mathbf{v}_1] = 0$$

Это равенство называется *тождеством Якоби.* Доказать, что его можно записать также в следующнй эквивалентной форме:

$$[\mathbf{v}_1, [\mathbf{v}_2, \mathbf{v}_3]] = [[\mathbf{v}_1, \mathbf{v}_2], \mathbf{v}_3] + [\mathbf{v}_2, [\mathbf{v}_1, \mathbf{v}_3]].$$

Продолжим изучение свойств кватернионов – векторов.

8.13. Проверить, что если $\mathbf{v}$ — вектор, то $\overline{\mathbf{v}} = -\mathbf{v}$ (это, разумеется, тоже вектор).

8.14. Доказать, что если $\mathbf{v}$ — вектор, и $\mathbf{v} \neq 0$, то $\mathbf{v}^{-1}$ — также вектор.

8.15. Доказать, что любой нескалярный кватернион можно представить в виде произведения двух векторов.

Решение. Пусть $\mathbf{q} = t + \mathbf{v}$, где t — скалярная часть $\mathbf{q}$, а $\mathbf{v} \neq 0$ — векторная. Выберем вектор $\mathbf{w} \neq 0$ так, чтобы $(\mathbf{v}, \mathbf{w}) = 0$, и умножим $\mathbf{q}$ справа на $\mathbf{w}$. Преобразуем равенство $\mathbf{qw} = t\mathbf{w} + \mathbf{vw}$, заменив $\mathbf{vw}$ на $-(\mathbf{v}, \mathbf{w}) + [\mathbf{v}, \mathbf{w}] = [\mathbf{v}, \mathbf{w}]$. Получим $\mathbf{qw} = t\mathbf{w} + [\mathbf{v}, \mathbf{w}]$. В правой части этого равенства стоит ненулевой вектор. Остается умножить обе части равенства справа на вектор $\mathbf{w}^{-1}$:

$$\mathbf{q} = (t\mathbf{w} + [\mathbf{v}, \mathbf{w}])\mathbf{w}^{-1}.$$

8.16. Доказать, что если $\mathbf{v}$ — вектор, и $\mathbf{q} \in \mathbf{H}^*$ (произвольный ненулевой кватернион), то $\mathbf{qvq}^{-1}$ — также вектор.

Указание. Используйте то, что если $\mathbf{a} \in \mathbb{R} = \{\lambda\mathbf{1} | \lambda \in \mathbb{R}\} \subset \mathbf{H}$, то $\mathbf{aw} = \mathbf{wa}$ для любого кватерниона $\mathbf{w}$.

8.17. Доказать, что если $\mathbf{v}$ — вектор, то $\mathbf{v}^2 = -(\mathbf{v}, \mathbf{v})$.

Из этого равенства вытекает важное следствие: если $\mathbf{v}$ — вектор, а $\mathbf{q}$ — какой угодно кватернион, то $\mathbf{v}^2\mathbf{q} = \mathbf{qv}^2$. Обоснуйте это.

Пример 8.5. Докажем с помощью кватернионов неравенство Коши-Буняковсого:

$$(\mathbf{v}_1, \mathbf{v}_2)^2 \leq (\mathbf{v}_1, \mathbf{v}_1)(\mathbf{v}_2, \mathbf{v}_2).$$

Так как $(\mathbf{v}_1, \mathbf{v}_1) = -\mathbf{v}_1^2$, $(\mathbf{v}_2, \mathbf{v}_2) = -\mathbf{v}_2^2$, то доказываемое неравенство равносильно следующему:

$$(\mathbf{v}_1, \mathbf{v}_2)^2 \leq \mathbf{v}_1^2\mathbf{v}_2^2.$$

Из тождества (7) следует, что $[\mathbf{v}_1, \mathbf{v}_2] = \mathbf{v}_1\mathbf{v}_2 + (\mathbf{v}_1, \mathbf{v}_2)$. Так как $[\mathbf{v}_1, \mathbf{v}_2]$ вектор, то $[\mathbf{v}_1, \mathbf{v}_2]^2 \le 0$. Следовательно, $(\mathbf{v}_1\mathbf{v}_2 + (\mathbf{v}_1, \mathbf{v}_2))^2 \le 0$. Преобразуем левую часть этого неравенства.

$$(\mathbf{v}_1\mathbf{v}_2 + (\mathbf{v}_1, \mathbf{v}_2))^2 = \mathbf{v}_1\mathbf{v}_2\mathbf{v}_1\mathbf{v}_2 + 2(\mathbf{v}_1, \mathbf{v}_2)\mathbf{v}_1\mathbf{v}_2 + (\mathbf{v}_1, \mathbf{v}_2)^2 \le 0.$$

Заметим, что

$$\begin{aligned} \mathbf{v}_1\mathbf{v}_2\mathbf{v}_1\mathbf{v}_2 + 2(\mathbf{v}_1, \mathbf{v}_2)\mathbf{v}_1\mathbf{v}_2 &= \mathbf{v}_1\mathbf{v}_2\mathbf{v}_1\mathbf{v}_2 - (\mathbf{v}_1\mathbf{v}_2 + \mathbf{v}_2\mathbf{v}_1)\mathbf{v}_1\mathbf{v}_2 = \\ &= -\mathbf{v}_2\mathbf{v}_1\mathbf{v}_1\mathbf{v}_2 = -\mathbf{v}_2\mathbf{v}_1^2\mathbf{v}_2 = -\mathbf{v}_1^2\mathbf{v}_2^2. \end{aligned}$$

Последнее равенство следует из утверждения предыдущей задачи о том, что $\mathbf{v}_1^2$ можно переставлять с любым кватернионом. Отсюда

$$(\mathbf{v}_1, \mathbf{v}_2)^2 - \mathbf{v}_1^2\mathbf{v}_2^2 \le 0,$$

что и требовалось доказать.

8.18. Пусть $\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3 \in \mathbf{V}$. Доказать, что $\mathbf{v}_1\mathbf{v}_2\mathbf{v}_1$, $\mathbf{v}_1\mathbf{v}_3\mathbf{v}_3$ — также векторы, и если $\mathbf{v}_1^2 = -1$, то $(\mathbf{v}_1\mathbf{v}_2\mathbf{v}_1, \mathbf{v}_1\mathbf{v}_3\mathbf{v}_1) = (\mathbf{v}_2, \mathbf{v}_3)$.

8.19. Пусть $\mathbf{v}_1\mathbf{v}_2\mathbf{v}_3$ — вектор. Доказать, что тогда $\mathbf{v}_3\mathbf{v}_1\mathbf{v}_2$ и $\mathbf{v}_2\mathbf{v}_3\mathbf{v}_1$ — векторы, и $(\mathbf{v}_1\mathbf{v}_2\mathbf{v}_3, \mathbf{v}_1\mathbf{v}_2\mathbf{v}_3) = (\mathbf{v}_3\mathbf{v}_1\mathbf{v}_2, \mathbf{v}_3\mathbf{v}_1\mathbf{v}_2)$. Заметим, что здесь не предполагается, что векторами являются $\mathbf{v}_1, \mathbf{v}_2$ и $\mathbf{v}_3$.

8.20. Пусть $\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3$ и $\mathbf{v}_1\mathbf{v}_2\mathbf{v}_3$ — векторы. Доказать, что тогда вектором является и $\mathbf{v}_3\mathbf{v}_2\mathbf{v}_1$, причем $[\mathbf{v}_1\mathbf{v}_2\mathbf{v}_3, \mathbf{v}_3\mathbf{v}_2\mathbf{v}_1] = 0$.

Теорема 8.4. *Пусть* $\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3$ *— ортонормированный базис пространства* $\mathbf{V}$. *Тогда*

1) $\mathbf{v}_1^2 = \mathbf{v}_2^2 = \mathbf{v}_3^2 = -1$;

2) $\mathbf{v}_1\mathbf{v}_2 = -\mathbf{v}_2\mathbf{v}_1$, $\mathbf{v}_1\mathbf{v}_3 = -\mathbf{v}_3\mathbf{v}_1$, $\mathbf{v}_3\mathbf{v}_2 = -\mathbf{v}_2\mathbf{v}_3$;

3) $\mathbf{v}_1\mathbf{v}_2$ *— вектор, при этом* $\mathbf{v}_1\mathbf{v}_2 = \lambda\mathbf{v}_3$, *где* $\lambda = \pm 1$.

Доказательство. По условию, $(\mathbf{v}_l, \mathbf{v}_m) = -\frac{1}{2}(\mathbf{v}_l\mathbf{v}_m + \mathbf{v}_m\mathbf{v}_l) = \delta_{l,m}$ (символ Кронекера), $l, m = 1, 2, 3$. Отсюда следует, что $(\mathbf{v}_l, \mathbf{v}_l) = -\mathbf{v}_l^2 = -1$. Так как $(\mathbf{v}_l, \mathbf{v}_m) = 0$ при $l \neq m$, то $\mathbf{v}_l\mathbf{v}_m = -\mathbf{v}_m\mathbf{v}_l$. Используя это, вычислим $(\mathbf{v}_1\mathbf{v}_2)^2$:

$$(\mathbf{v}_1\mathbf{v}_2)^2 = \mathbf{v}_1\mathbf{v}_2\mathbf{v}_1\mathbf{v}_2 = -\mathbf{v}_1\mathbf{v}_1\mathbf{v}_2\mathbf{v}_2 = -\mathbf{v}_1^2\mathbf{v}_2^2 = -1.$$

Итак, $\mathbf{v}_3' = \mathbf{v}_1\mathbf{v}_2$ — снова вектор. Легко проверяется, что векторы $\mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3'$ образуют ортонормированный базис $\mathbf{V}$. Например,

$$(\mathbf{v}_1, \mathbf{v}_1\mathbf{v}_2) = -\frac{1}{2}(\mathbf{v}_1\mathbf{v}_1\mathbf{v}_2 + \mathbf{v}_1\mathbf{v}_2\mathbf{v}_1) = -\frac{1}{2}(\mathbf{v}_1\mathbf{v}_1\mathbf{v}_2 - \mathbf{v}_1\mathbf{v}_1\mathbf{v}_2) = 0,$$

так как $\mathbf{v}_1\mathbf{v}_2 = -\mathbf{v}_2\mathbf{v}_1$. Векторы $\mathbf{v}_3$ и $\mathbf{v}_3'$ перпендикулярны к плоскости, натянутой на $\mathbf{v}_1$ и $\mathbf{v}_2$, и оба имеют единичную длину. Поэтому они могут отличаться только знаком. $\square$

Исследование кватернионов будет продолжено в следующем разделе. Дополнительную информацию можно найти в книгах [20], [21], [19].

9. Кватернионы и вращения

Матрица $A \in GL_n(\mathbb{C})$ называется *унитарной*, если $A^{-1} = A^* = {}^t\overline{A}$. Множество унитарных $n \times n$-матриц обозначается через $U(n)$. Через $SU(n)$ обозначается подмножество $U(n)$, состоящее из унитарных матриц с определителями, равными единице.

9.1. Доказать, что $U(n)$ группа, а $SU(n)$ ее нормальная подгруппа.

Отметим, что $U(1) = \mathbf{U}$. В самом деле, $U(1) \subset GL_1(\mathbb{C}) = \mathbb{C}^*$ по определению, состоит из всех тех $z \in \mathbb{C}^*$, для которых $z^{-1} = \overline{z}$. Но это равносильно тому, что $|z| = 1$.

Группа $U(n)$ называется *унитарной группой* n-й степени, а $SU(n)$ — *специальной унитарной группой* n-й степени. Наша цель в этом параграфе — разобраться в строении $SU(2)$.

Лемма 9.1. *Матрица A принадлежит группе $SU(2)$ тогда и только тогда, если*

$$A = \begin{pmatrix} u & v \\ -\overline{v} & \overline{u} \end{pmatrix},$$

гда $u, v \in \mathbb{C}^*$ и $|u|^2 + |v|^2 = 1$.

Доказательство. Пусть

$$A = \begin{pmatrix} u & v \\ z & w \end{pmatrix} \in SU(2),$$

где $u, v, z, w \in \mathbb{C}$. Ввиду того, что $det(A) = 1$, т.е. $uw - vz = 1$, обратная к A матрица имеет вид:

$$A^{-1} = \begin{pmatrix} w & -v \\ -z & u \end{pmatrix}.$$

Запишем условие унитарности A:

$$A^{-1} = {}^t\overline{A} = \begin{pmatrix} \overline{u} & \overline{z} \\ \overline{v} & \overline{w} \end{pmatrix}.$$

Сопоставление элементов матриц на одних и тех же местах дает (после исключения повторений) следующие равенства:

$$w = \overline{u}, \quad v = -\overline{z}.$$

Это именно то, что требовалось доказать. Обратное утверждение очевидно. □

Непосредственным следствием это леммы является то, что группа $SU(2)$ оказывается подгруппой $\mathbf{H}^*$ — группы обратимых элементов тела кватернионов, причем это в точности все кватернионы $\mathbf{u}$, норма $N(\mathbf{u})$ которых равна единице.

9.2. Доказать, что $\mathbf{H}^* \cong SU(2) \times \mathbb{R}_+$.

9.3. Рассмотрим множество $M_2(\mathbb{C})$ квадратных 2×2-матриц с комплексными компонентами. Если

$$A = \begin{pmatrix} u & v \\ z & w \end{pmatrix} \in M_2(\mathbb{C}),$$

то нормой этой матрицы называется число $\| A \| = |u|^2 + |v|^2 + |z|^2 + |w|^2$. Допустим, что $det(A) = 1$. Докажите, что $A \in SU(2)$ тогда и только тогда, если $\| A \| = 2$.

Положим

$$\mathbf{b}_\varphi = \begin{pmatrix} \cos\frac{\varphi}{2} + i\sin\frac{\varphi}{2} & 0 \\ 0 & \cos\frac{\varphi}{2} - i\sin\frac{\varphi}{2} \end{pmatrix} = \cos\frac{\varphi}{2} + \sin\frac{\varphi}{2}\mathbf{i} \qquad (1)$$

$$\mathbf{c}_\theta = \begin{pmatrix} \cos\frac{\theta}{2} & i\sin\frac{\theta}{2} \\ i\sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{pmatrix} = \cos\frac{\theta}{2} + \sin\frac{\theta}{2}\mathbf{k} \qquad (2)$$

Легко убедиться, что $\mathbf{b}_\varphi, \mathbf{c}_\theta \in SU(2)$.

Лемма 9.2. *Каждая матрица из $SU(2)$ может быть представлена в виде*

$$\mathbf{b}_\varphi \mathbf{c}_\theta \mathbf{b}_\psi$$

для некоторых φ, θ, ψ. Углы φ, θ, ψ можно выбрать так, что $0 \leq \varphi < 2\pi$, $0 \leq \theta \leq \pi$, $-2\pi \leq \psi < 2\pi$.

Доказательство. Пусть $A \in SU(2)$. Представим A в виде:

$$A = \begin{pmatrix} u & v \\ -\overline{v} & \overline{u} \end{pmatrix} = \begin{pmatrix} |u|(\cos\alpha + i\sin\alpha) & |v|(\cos\beta + i\sin\beta) \\ |v|(-\cos\beta + i\sin\beta) & |u|(\cos\alpha - i\sin\alpha) \end{pmatrix}$$

Сначала рассмотрим случай, когда $uv \neq 0$. Прямым вычислением показывается, что $\mathbf{b}_\tau \mathbf{c}_\theta \mathbf{b}_\psi$ — это матрица

$$\begin{pmatrix} \cos\frac{\theta}{2}(\cos\frac{\varphi+\psi}{2} + i\sin\frac{\varphi+\psi}{2}) & \sin\frac{\theta}{2}(\cos\frac{\pi+\varphi-\psi}{2} + i\sin\frac{\pi+\varphi-\psi}{2}) \\ -\sin\frac{\theta}{2}(\cos\frac{\pi+\varphi-\psi}{2} - i\sin\frac{\pi+\varphi-\psi}{2}) & \cos\frac{\theta}{2}(\cos\frac{\varphi+\psi}{2} - i\sin\frac{\varphi+\psi}{2}) \end{pmatrix}$$

Попытаемся приравнять A и $\mathbf{b}_\tau \mathbf{c}_\theta \mathbf{b}_\psi$, и по известным $|u|, |v|$, α, β найти неизвестные φ, θ и ψ. Итак, рассмотрим равенства:

$$|u|(\cos\alpha + i\sin\alpha) = \cos\frac{\theta}{2}(\cos\frac{\varphi+\psi}{2} + i\sin\frac{\varphi+\psi}{2})$$
$$|v|(\cos\beta + i\sin\beta) = \sin\frac{\theta}{2}(\cos\frac{\pi+\varphi-\psi}{2} + i\sin\frac{\pi+\varphi-\psi}{2})$$

Так как $|u|^2 + |v|^2 = 1$, то можно представить модули $|u|, |v|$ в виде:

$$|u| = \cos\frac{\theta}{2}, \quad |v| = \sin\frac{\theta}{2}.$$

И синус, и косинус положительны, если $0 < \frac{\theta}{2} < \frac{\pi}{2}$, то есть при $0 < \theta < \pi$. С другой стороны, попытаемся решить систему уравнений:

$$\alpha = \frac{\varphi + \psi}{2}$$
$$\beta = \frac{\pi + \pi - \psi}{2}.$$

Формальное решение таково:

$$\varphi = \alpha + \beta - \frac{\pi}{2}, \quad \psi = \alpha - \beta + \frac{\pi}{2}.$$

Так как $0 \leq \alpha, \beta < 2\pi$, и допустимо отбрасывать величины, кратные 2π, то значения φ и ψ можно выбрать в промежутках $0 \leq \varphi < 2\pi$, $-2\pi \leq \psi < 2\pi$.

Расмотрим случай $uv = 0$, точнее, два случая: $u = 0, v \neq 0$ и $u \neq 0, v = 0$.

Если $u = 0$, то $|v| = 1$, и

$$A = \begin{pmatrix} 0 & \cos\beta + i\sin\beta \\ -\cos\beta + i\sin\beta & 0 \end{pmatrix}.$$

Рассмотрим

$$\mathbf{c}_\pi = \mathbf{k} = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix},$$

и попробуем представить матрицу A в виде $A = \mathbf{c}_\pi \mathbf{b}_\psi$. Иными словами, необходимо решить относительно ψ следующее уравнение:

$$\begin{pmatrix} 0 & \cos\beta + i\sin\beta \\ -\cos\beta + i\sin\beta & 0 \end{pmatrix} = \begin{pmatrix} 0 & \sin\frac{\psi}{2} + i\cos\frac{\psi}{2} \\ -\sin\frac{\psi}{2} + i\cos\frac{\psi}{2} & 0 \end{pmatrix}$$

Используя формулы приведения, получаем решение $\dfrac{\psi}{2} = \dfrac{\pi}{2} - \beta$, или $\psi = \pi - 2\beta$. Если $0 \leq \beta < 2\pi$, то $-\pi < \psi < \pi$. Если же учесть, что $\mathbf{b}_0 = \mathbf{1}$, то можно считать, что A снова имеет вид $A = \mathbf{b}_\varphi \mathbf{c}_\theta \mathbf{b}_\psi$.

Случай $v = 0$ является более легким. Так как $|u| = 1$, то $A = \mathbf{b}_\alpha$. Поскольку $\mathbf{c}_0 = \mathbf{1}$ и $\mathbf{b}_0 = \mathbf{1}$, то формально будем иметь и в этом случае $A = \mathbf{b}_\alpha \mathbf{c}_0 \mathbf{b}_0$. $\square$

9.4. Обосновать формулу для $\mathbf{b}_\tau \mathbf{c}_\theta \mathbf{b}_\psi$, приведенную в доказательстве леммы.

9.5. Доказать, что любую матрицу из $SU(2)$ можно представить в виде $\mathbf{u}\mathbf{b}_\varphi\mathbf{u}^{-1}$ для подходящего φ и $\mathbf{u}\in SU(2)$.

В дальнейшем будут необходимы следующие формулы.

$$\begin{aligned}
&\mathbf{b}_\varphi\mathbf{i}\mathbf{b}_\varphi^{-1}=\mathbf{i}\\
&\mathbf{b}_\varphi\mathbf{j}\mathbf{b}_\varphi^{-1}=\cos\varphi\mathbf{j}+\sin\varphi\mathbf{k}\\
&\mathbf{b}_\varphi\mathbf{k}\mathbf{b}_\varphi^{-1}=-\sin\varphi\mathbf{j}+\cos\varphi\mathbf{k}
\end{aligned}\tag{3}$$

$$\begin{aligned}
\mathbf{c}_\theta\mathbf{i}\mathbf{c}_\theta^{-1}&=\ \cos\theta\mathbf{i}+\sin\theta\mathbf{j}\\
\mathbf{c}_\theta\mathbf{j}\mathbf{c}_\theta^{-1}&=-\sin\theta\mathbf{i}+\cos\theta\mathbf{j}\\
\mathbf{c}_\theta\mathbf{k}\mathbf{c}_\theta^{-1}&=\ \mathbf{k}
\end{aligned}\tag{4}$$

Эти равенства устанавливаются непосредственными вычислениями. Например,

$$\begin{aligned}
\mathbf{b}_\varphi\mathbf{i}\mathbf{b}_\varphi^{-1}\ &=(\cos\tfrac{\varphi}{2}+\sin\tfrac{\varphi}{2}\mathbf{i})\mathbf{i}(\cos\tfrac{\varphi}{2}-\sin\tfrac{\varphi}{2}\mathbf{i})=\\
&=(\cos\tfrac{\varphi}{2}+\sin\tfrac{\varphi}{2}\mathbf{i})(\cos\tfrac{\varphi}{2}\mathbf{i}+\sin\tfrac{\varphi}{2})=\\
&=\cos\tfrac{\varphi}{2}\sin\tfrac{\varphi}{2}-\sin\tfrac{\varphi}{2}\cos\tfrac{\varphi}{2}+(\cos^2\tfrac{\varphi}{2}+\sin^2\tfrac{\varphi}{2})\mathbf{i}=\mathbf{i}.
\end{aligned}$$

Далее,

$$\begin{aligned}
\mathbf{b}_\varphi\mathbf{j}\mathbf{b}_\varphi^{-1}\ &=(\cos\tfrac{\varphi}{2}+\sin\tfrac{\varphi}{2}\mathbf{i})\mathbf{j}(\cos\tfrac{\varphi}{2}-\sin\tfrac{\varphi}{2}\mathbf{i})=\\
&=(\cos\tfrac{\varphi}{2}+\sin\tfrac{\varphi}{2}\mathbf{i})(\cos\tfrac{\varphi}{2}\mathbf{j}+\sin\tfrac{\varphi}{2}\mathbf{k})=\\
&=(\cos^2\tfrac{\varphi}{2}-\sin^2\tfrac{\varphi}{2})\mathbf{j}+2\sin\tfrac{\varphi}{2}\cos\tfrac{\varphi}{2}\mathbf{k}=\\
&=\cos\varphi\mathbf{j}+\sin\varphi\mathbf{k}.
\end{aligned}$$

Наконец,

$$\begin{aligned}
\mathbf{c}_\theta\mathbf{j}\mathbf{c}_\theta^{-1}\ &=(\cos\tfrac{\theta}{2}+\sin\tfrac{\theta}{2}\mathbf{k})\mathbf{j}(\cos\tfrac{\theta}{2}-\sin\tfrac{\theta}{2}\mathbf{k})=\\
&=(\cos\tfrac{\theta}{2}+\sin\tfrac{\theta}{2}\mathbf{k})(\cos\tfrac{\theta}{2}\mathbf{j}-\sin\tfrac{\theta}{2}\mathbf{i})=\\
&=(\cos^2\tfrac{\theta}{2}-\sin^2\tfrac{\theta}{2})\mathbf{j}-2\sin\tfrac{\theta}{2}\cos\tfrac{\theta}{2}\mathbf{k}=\\
&=\cos\theta\mathbf{j}-\sin\theta\mathbf{k}.
\end{aligned}$$

9.6. Проверить остальные равенства из семейств (3),(4).

Напомним, что через $\mathbf{V}$ обозначается линейное пространство над полем $\mathbb{R}$ с базисом $\mathbf{i},\mathbf{j},\mathbf{k}$, т.е. пространство кватернионов – векторов.

Лемма 9.3. *Пусть* $\mathbf{q}\in\mathbf{H}^*$. *Тогда существует ортогональное линейное отображение* $\Phi_\mathbf{q}:\mathbf{V}\longrightarrow\mathbf{V}$, *такое, что* $\Phi_\mathbf{q}(\mathbf{v})=\mathbf{q}\mathbf{v}\mathbf{q}^{-1}$ *для каждого* $\mathbf{v}\in\mathbf{V}$.

Доказательство. Начать необходимо с обоснования корректности определения, то есть с проверки того, что $\Phi_{\mathbf{q}}(\mathbf{v}) \in \mathbf{V}$ для каждого $\mathbf{v} \in \mathbf{V}$. Для этого достаточно убедиться, что $(\mathbf{q}\mathbf{v}\mathbf{q}^{-1})^2 \leq 0$. В самом деле,

$$(\mathbf{q}\mathbf{v}\mathbf{q}^{-1})^2 = \mathbf{q}\mathbf{v}\mathbf{q}^{-1}\mathbf{q}\mathbf{v}\mathbf{q}^{-1} = \mathbf{q}\mathbf{v}^2\mathbf{q}^{-1} = \mathbf{v}^2\mathbf{q}\mathbf{q}^{-1} = \mathbf{v}^2 \leq 0.$$

Здесь использовано то, что если $\mathbf{v}$ — вектор, то $\mathbf{v}^2 \leq 0$ — скаляр, и его можно переставлять с любыми кватернионами. Проверим линейность. Пусть $\mathbf{v}_1, \mathbf{v}_2 \in \mathbf{U}$, $\lambda_1, \lambda_2 \in \mathbb{R}$. Тогда

$$\begin{aligned}\Phi_{\mathbf{q}}(\lambda_1\mathbf{v}_1 + \lambda_2\mathbf{v}_2) &= \mathbf{q}(\lambda_1\mathbf{v}_1 + \lambda_2\mathbf{v}_2)\mathbf{q}^{-1} = \mathbf{q}(\lambda_1\mathbf{v}_1)\mathbf{q}^{-1} + \mathbf{q}(\lambda_2\mathbf{v}_2)\mathbf{q}^{-1} = \\ &= \lambda_1\mathbf{q}\mathbf{v}_1\mathbf{q}^{-1} + \lambda_2\mathbf{q}\mathbf{v}_2\mathbf{q}^{-1} = \lambda_1\Phi_{\mathbf{q}}(\mathbf{v}_1) + \lambda_2\Phi_{\mathbf{q}}(\mathbf{v}_2).\end{aligned}$$

Далее необходимо проверить ортогональность.

$$\begin{aligned}(\Phi_{\mathbf{q}}(\mathbf{v}_1), F_{\mathbf{q}}(\mathbf{v}_2)) &= -\frac{1}{2}((\mathbf{q}\mathbf{v}_1\mathbf{q}^{-1})(\mathbf{q}\mathbf{v}_2\mathbf{q}^{-1}) + (\mathbf{q}\mathbf{v}_2\mathbf{q}^{-1})(\mathbf{q}\mathbf{v}_1\mathbf{q}^{-1})) \\ &= -\frac{1}{2}(\mathbf{q}\mathbf{v}_1\mathbf{v}_2\mathbf{q}^{-1} + \mathbf{q}\mathbf{v}_2\mathbf{v}_1\mathbf{q}^{-1}) = -\frac{1}{2}\mathbf{q}(\mathbf{v}_1\mathbf{v}_2 + \mathbf{v}_2\mathbf{v}_1)\mathbf{q}^{-1} \\ &= -\frac{1}{2}(\mathbf{v}_1\mathbf{v}_2 + \mathbf{v}_2\mathbf{v}_1)\mathbf{q}\mathbf{q}^{-1} = -\frac{1}{2}(\mathbf{v}_1\mathbf{v}_2 + \mathbf{v}_2\mathbf{v}_1) \\ &= (\mathbf{v}_1, \mathbf{v}_2).\end{aligned}$$

Здесь использовано то, что кватернион вида $\mathbf{v}_1\mathbf{v}_2 + \mathbf{v}_2\mathbf{v}_1$ можно перставлять с любым другим кватернионам. $\square$

Лемма 9.4. *Имеют место равенства:*

1) $\Phi_{\mathbf{q}_1\mathbf{q}_2} = \Phi_{\mathbf{q}_1}\Phi_{\mathbf{q}_2}$*;*

2) $\Phi_{\mathbf{1}} = 1_{\mathbf{V}}$ *— тождественное отображение из* $\mathbf{V}$ *в* $\mathbf{V}$*;*

3) $\Phi_{\lambda\mathbf{q}} = \Phi_{\mathbf{q}}$*, если* $\lambda \in \mathbb{R}$*,* $\lambda \neq 0$*.*

Доказательство. Чтобы доказать 1), достаточно вычислить значения функций, стоящих в левой и правой частях равенства 1), на произвольном значении аргумента $\mathbf{v} \in \mathbf{V}$. Итак, с одной строны, $\Phi_{\mathbf{q}_1\mathbf{q}_2}(\mathbf{v}) = (\mathbf{q}_1\mathbf{q}_2)\mathbf{v}(\mathbf{q}_1\mathbf{q}_2)^{-1}$. С другой стороны, $\Phi_{\mathbf{q}_1}(\Phi_{\mathbf{q}_2}(\mathbf{v})) = \mathbf{q}_1(\mathbf{q}_2\mathbf{v}\mathbf{q}_2^{-1})\mathbf{q}_1^{-1}$. Ясно, что эти значения совпадают.

Свойство 2) очевидно. Наконец, вычислим значения функций, стоящих в левой и правой частях равенства 3) на произвольном аргументе $\mathbf{v}$.

$$\Phi_{\lambda\mathbf{q}}(\mathbf{v}) = (\lambda\mathbf{q})\mathbf{v}(\lambda\mathbf{q})^{-1} = \lambda(\mathbf{q}\mathbf{v}\mathbf{q}^{-1})\lambda^{-1} = \mathbf{q}\mathbf{v}\mathbf{q}^{-1} = \Phi_{\mathbf{q}}(\mathbf{v}),$$

так как $\lambda \in \mathbb{R}$ можно переставлять с любыми кватернионами. Следовательно, функции $\Phi_{\lambda\mathbf{q}}$ и $\Phi_{\mathbf{q}}$ совпадают. $\square$

Теорема 9.1. *Соответствие* $\mathbf{u} \mapsto \Phi_{\mathbf{u}}$ *определяет гомоморфизм групп* $\Phi : SU(2) \longrightarrow SO(3)$*. Ядро этого гомоморфизма состоит из двух элементов:*

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

Доказательство. То, что при $\mathbf{u} \in SU(2)$ отображение $\Phi_{\mathbf{u}}$ принадлежит $O(3)$, и соответствие $\mathbf{u} \mapsto \Phi_{\mathbf{u}}$ является гомоморфизмом групп, следует из предыдущих лемм.

Покажем, что на самом деле $\Phi_{\mathbf{u}} \in SO(3)$. Рассмотрим сначала случаи $\mathbf{u} = \mathbf{b}_\varphi$ и $\mathbf{u} = \mathbf{c}_\theta$. Из равенств (3) следует, что матрица $\Phi_{\mathbf{b}_\varphi}$ в базисе $\mathbf{i}, \mathbf{j}, \mathbf{k}$ выглядит так:

$$\Phi_{\mathbf{b}_\varphi} = B_\varphi = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos\varphi & -\sin\varphi \\ 0 & \sin\varphi & \cos\varphi \end{pmatrix} \tag{5}$$

Точно так же из (4) получаем матрицу $\Phi_{\mathbf{c}_\theta}$:

$$\Phi_{\mathbf{c}_\theta} = C_\theta = \begin{pmatrix} \cos\theta & -\sin\theta & 0 \\ \sin\theta & \cos\theta & 0 \\ 0 & 0 & 1 \end{pmatrix} \tag{6}$$

Очевидно, что $B_\varphi, C_\theta \in SO(3)$. Как уже было показано, каждый элемент $\mathbf{u} \in SU(2)$ представим в виде $\mathbf{u} = \mathbf{b}_\varphi \mathbf{c}_\theta \mathbf{b}_\psi$. Применяя к $\mathbf{u}$ гомоморфизм Φ, получаем

$$\Phi_{\mathbf{u}} = \Phi_{\mathbf{b}_\varphi \mathbf{c}_\theta \mathbf{b}_\psi} = \Phi_{\mathbf{b}_\varphi} \Phi_{\mathbf{c}_\theta} \Phi_{\mathbf{b}_\psi},$$

или

$$\Phi_{\mathbf{u}} = B_\varphi C_\theta B_\psi \tag{7}$$

Таким образом, матрица $\Phi_{\mathbf{u}}$ представляется в виде произведения трех матриц из $SO(3)$ и, следовательно, сама является матрицей из $SO(3)$.

Остается разобраться с ядром. То, что $\mathbf{1}$ и $-\mathbf{1}$ содержатся в ядре Φ, очевидно. Допустим, что $\mathbf{w} \in Ker(\Phi)$. Это значит, что отображение

$\mathbf{v} \mapsto \mathbf{w}\mathbf{v}\mathbf{w}^{-1}$ является тождественным, то есть для каждого вектора $\mathbf{v} \in \mathbf{V}$ имеет место равенство $\mathbf{v} = \mathbf{w}\mathbf{v}\mathbf{w}^{-1} = \mathbf{v}$, или $\mathbf{w}\mathbf{v} = \mathbf{v}\mathbf{w}$. Положим $\mathbf{w} = t + x\mathbf{i} + y\mathbf{j} + z\mathbf{k}$ и посмотрим, что получится, если взять $\mathbf{v} = \mathbf{i}, \mathbf{j}, \mathbf{k}$. Из $\mathbf{w}\mathbf{i} = \mathbf{i}\mathbf{w}$ получим уравнение:

$$-x + t\mathbf{i} + z\mathbf{j} - y\mathbf{k} = -x + t\mathbf{i} - z\mathbf{j} + y\mathbf{k}.$$

Сравнивая коэффициенты при элементах базиса, получим $y = z = 0$. Итак, $\mathbf{w} = t + x\mathbf{i}$. Из $\mathbf{w}\mathbf{j} = \mathbf{j}\mathbf{w}$ будем иметь соотношение:

$$t\mathbf{j} + x\mathbf{k} = t\mathbf{j} - x\mathbf{k},$$

откуда получаем $x = 0$, и $\mathbf{w} = t = t\mathbf{1}$, т.е. это матрица

$$\begin{pmatrix} t & 0 \\ 0 & t \end{pmatrix}$$

с определителем t^2. Но у элементов группы $SU(2)$ определители равны единице. Отсюда $t^2 = 1$, $t = \pm 1$, и $\mathbf{w} = \pm\mathbf{1}$, что и утверждалось. $\square$

Напомним, что отражением в евклидовом пространстве $\mathbf{V}$ называется линейное отображение $\tau_{\mathbf{w}}$, действующее по правилу:

$$\tau_{\mathbf{w}}(\mathbf{v}) = \mathbf{v} - 2\frac{(\mathbf{v}, \mathbf{w})}{(\mathbf{w}, \mathbf{w})}\mathbf{w}.$$

Лемма 9.5. *Отражение $\tau_{\mathbf{w}}$ в пространстве $\mathbf{V}$ записывается следующим образом:*

$$\tau_{\mathbf{w}}(\mathbf{v}) = -\mathbf{w}\mathbf{v}\mathbf{w}^{-1}.$$

Доказательство. Как уже известно (см. раздел о кватернионах), $(\mathbf{w}, \mathbf{w}) = -\mathbf{w}^2$. Следовательно, $\dfrac{1}{(\mathbf{w}, \mathbf{w})} = -\mathbf{w}^{-2}$. Отсюда

$$\begin{aligned} \tau_{\mathbf{w}}(\mathbf{v}) &= \mathbf{v} - 2\frac{(\mathbf{v}, \mathbf{w})}{(\mathbf{w}, \mathbf{w})}\mathbf{w} = \mathbf{v} + 2(\mathbf{v}, \mathbf{w})\mathbf{w}^{-2}\mathbf{w} = \\ &= \mathbf{v} - (\mathbf{v}\mathbf{w} + \mathbf{w}\mathbf{v})\mathbf{w}^{-1} = \mathbf{v} - \mathbf{v} - \mathbf{w}\mathbf{v}\mathbf{w}^{-1} = -\mathbf{w}\mathbf{v}\mathbf{w}^{-1}. \ \square \end{aligned}$$

Теорема 9.2. *Гомоморфизм $\Phi : SU(2) \longrightarrow SO(3)$ сюръективен.*

Доказательство. Согласно теореме 7.3, каждый элемент группы $SO(3)$ есть суперпозиция двух отражений, например, $\tau_{\mathbf{c}}$ и $\tau_{\mathbf{w}}$. Значит, как только что показано, это отображение действует так:

$$\mathbf{v} \mapsto \tau_{\mathbf{c}}(\tau_{\mathbf{w}}(\mathbf{v})) = -\mathbf{c}(-\mathbf{w}\mathbf{v}\mathbf{w}^{-1})\mathbf{c}^{-1} = (\mathbf{c}\mathbf{w})\mathbf{v}(\mathbf{c}\mathbf{w})^{-1}.$$

Обозначая кватернион $\mathbf{cw}$ через $\mathbf{q}$, видим, что наше произвольно выбранное вращение совпадает с отображением $\Phi_{\mathbf{q}}$. Остается заменить $\mathbf{q}$ на элемент $\mathbf{u} = \dfrac{1}{N(\mathbf{q})}\mathbf{q}$ группы $SU(2)$. Согласно уже доказанному, в этом случае $\Phi_{\mathbf{q}} = \Phi_{\mathbf{u}}$. Это означает, что выбранное вращение является образом элемента $\mathbf{u} \in SU(2)$ при гомоморфизме Φ. $\square$

Другое доказательство можно найти в книге [29] на с. 80 – 82.

Важным следствием является следующая теорема.

Теорема 9.3. *Каждую матрицу A из $SO(3)$ можно представить в виде произведения трех матриц поворотов, определенных выше в* (5) *и* (6)*:*

$$A = B_\varphi C_\theta B_\psi,$$

где

$$B_\varphi = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos\varphi & -\sin\varphi \\ 0 & \sin\varphi & \cos\varphi \end{pmatrix}, \; C_\theta = \begin{pmatrix} \cos\theta & -\sin\theta & 0 \\ \sin\theta & \cos\theta & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

При этом $0 \le \varphi < 2\pi$, $0 \le \theta \le \pi$, $-2\pi \le \psi \le 2\pi$.

Доказательство. Как было показано выше, любая матрица вида $\Phi_{\mathbf{u}}$ представляется в виде $B_\varphi C_\theta B_\psi$. С другой стороны, так как гомоморфизм Φ сюръективен, то каждая матрица $A \in SO(3)$ равна $\Phi_{\mathbf{u}}$ для некоторого $\mathbf{u} \in SU(2)$. $\square$

9.7. Доказать, что если

$$\mathbf{q} = \begin{pmatrix} u & v \\ -\overline{v} & \overline{u} \end{pmatrix} \in SU(2),$$

то

$$\Phi_{\mathbf{q}} = \begin{pmatrix} \dfrac{u^2 - v^2 + \overline{u}^2 - \overline{v}^2}{2} & i\left(\dfrac{u^2 + v^2 - \overline{u}^2 - \overline{v}^2}{2}\right) & -uv - \overline{u}\,\overline{v} \\ i\left(\dfrac{-u^2 + v^2 + \overline{u}^2 - \overline{v}^2}{2}\right) & \dfrac{u^2 + v^2 + \overline{u}^2 + \overline{v}^2}{2} & i(uv - \overline{u}\,\overline{v}) \\ u\overline{v} + \overline{u}v & i(u\overline{v} - \overline{u}v) & u\overline{u} - v\overline{v} \end{pmatrix}$$

9.8. Пусть число l — целое или "полуцелое", т.е. имеющее вид $l = \dfrac{k}{2}$ для некоторого целого k. Обозначим через H_l множество всех однородным многочленов степени $2l$ от переменных x, y с комплексными коэффициентами, и зададим отображение

$$SU(2) \times H_l \longrightarrow H_l,$$

сопоставляющее паре $g \in SU(2)$ и $f(x,y) \in H_l$ многочлен ${}^g f$, определяемый по следующей формуле: если

$$g = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix},$$

то

$${}^g f(x,y) = f(\alpha x + \gamma y, \beta x + \delta y).$$

Доказать, что эта формула определяет линейное действие $SU(2)$ на H_l. Доказать, что $dim(H_l) = 2l + 1$.

Попытаться доказать, что H_l не имеет нетривиальных $SU(2)$-подмодулей (это более трудная задача; решение можно найти, например, в книге [29], с. 83 – 84).

9.9. Пусть число l — целое или "полуцелое", т.е. имеющее вид $l = \dfrac{k}{2}$ для некоторого целого k. Обозначим через P_l множество всех многочленов степени не выше $2l$ от переменной z с комплексными коэффициентами, и зададим отображение

$$SU(2) \times P_l \longrightarrow P_l,$$

сопоставляющее паре $g \in SU(2)$ и $f(x) \in P_l$ многочлен ${}^g f$, определяемый по следующей формуле: если

$$g = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix},$$

то

$$^{g}f(z) = (\beta z + \delta)^{2l} f\left(\frac{\alpha z + \gamma}{\beta z + \delta}\right).$$

Доказать, что эта формула определяет линейное действие $SU(2)$ на P_l. Доказать, что $dim(P_l) = 2l + 1$.

Более сложная задача: доказать, что P_l не имеет нетривиальных $SU(2)$-подмодулей, и что фактически $SU(2)$-модули H_l и P_l изоморфны.

Термин “полуцелые числа"часто употребляется физиками, и имеет отношение к такой характеристике элементарных частиц, как спин (см., например, книгу [30], с. 433 – 438).

Рассмотрим кватернион $\mathbf{q} = a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}$, $a, b, c, d \in \mathbb{R}$. Допустим, что норма $\mathbf{q}$ равна единице, т.е. $a^2 + b^2 + c^2 + d^2 = 1$. Предположим, что $\mathbf{q}$ не скаляр, и пусть $\mathbf{q}' = b\mathbf{i} + c\mathbf{j} + d\mathbf{k}$. Тогда $a^2 + |\mathbf{q}'|^2 = 1$. Отсюда следует, что существует угол φ такой, что $a = \cos\frac{\varphi}{2}$, а $|\mathbf{q}'| = \sin\frac{\varphi}{2}$. Положим $\mathbf{p} = \frac{1}{|\mathbf{q}'|}\mathbf{q}'$. Очевидно, $|\mathbf{p}| = 1$. Кроме того, $\mathbf{p}^2 = -1$. В этих обозначениях оказывается, что

$$\mathbf{q} = \cos\frac{\varphi}{2} + \sin\frac{\varphi}{2}\mathbf{p},$$

$$\mathbf{q}^{-1} = \cos\frac{\varphi}{2} - \sin\frac{\varphi}{2}\mathbf{p}.$$

Теорема 9.4. *Линейное преобразование $\Phi_{\mathbf{q}}$ есть поворот вокруг оси $\mathbf{p}$ на угол φ.*

Доказательство. Пусть $V_1 = \langle \mathbf{p} \rangle$, и V_2 — ортогональное дополнение V_1. Таким образом, $\mathbf{V} = V_1 \oplus V_2$. Представим аргумент $\mathbf{v}$ отображения $\Phi_{\mathbf{q}} : \mathbf{v} \mapsto \mathbf{q}\mathbf{v}\mathbf{q}^{-1}$ в виде суммы $\mathbf{v} = \mathbf{v}_1 + \mathbf{v}_2$, где $v_1 \in V_1$, $v_2 =\in V_2$. Это значит, что $\mathbf{v}_1 = \lambda\mathbf{p}$, где $\lambda \in \mathbb{R}$, а $(\mathbf{v}_2, \mathbf{p}) = 0$. Так как $(\mathbf{v}_2, \mathbf{p}) = -\frac{1}{2}(\mathbf{v}_2\mathbf{p} + \mathbf{p}\mathbf{v}_2)$, отсюда следует $\mathbf{v}_2\mathbf{p} = -\mathbf{p}\mathbf{v}_2$. Кроме того, из равенства $\mathbf{p}\mathbf{v}_2 = -(\mathbf{p}, \mathbf{v}_2) + [\mathbf{p}, \mathbf{v}_2]$ следует, что $\mathbf{p}\mathbf{v}_2 = [\mathbf{p}, \mathbf{v}_2]$. Используя это, проделаем следующие вычисления:

$$\mathbf{q}\mathbf{v}\mathbf{q}^{-1} = \mathbf{q}(\mathbf{v}_1 + \mathbf{v}_2)\mathbf{q}^{-1} = \mathbf{q}\mathbf{v}_1\mathbf{q}^{-1} + \mathbf{q}\mathbf{v}_2\mathbf{q}^{-1};$$

$$\mathbf{q}\mathbf{v}_1\mathbf{q}^{-1} = (\cos\frac{\varphi}{2} + \sin\frac{\varphi}{2}\mathbf{p})(\lambda\mathbf{p})(\cos\frac{\varphi}{2} - \sin\frac{\varphi}{2}\mathbf{p}) = (\lambda\mathbf{p})\mathbf{q}\mathbf{q}^{-1} = \mathbf{v}_1;$$

$$\begin{aligned}\mathbf{q}\mathbf{v}_2\mathbf{q}^{-1} &= (\cos\frac{\varphi}{2} + \sin\frac{\varphi}{2}\mathbf{p})\mathbf{v}_2(\cos\frac{\varphi}{2} - \sin\frac{\varphi}{2}\mathbf{p}) = \\ &= (\cos^2\frac{\varphi}{2} - \sin^2\frac{\varphi}{2})\mathbf{v}_2 + 2\sin\frac{\varphi}{2}\cos\frac{\varphi}{2}[\mathbf{p},\mathbf{v}_2] = \\ &= \cos\varphi\,\mathbf{v}_2 + \sin\varphi\,[\mathbf{p},\mathbf{v}_2].\end{aligned}$$

Из курса геометрии читателю должно быть известно, что если векторы $\mathbf{v}_2$ и $\mathbf{p}$ перпендикулярны (т.е. $(\mathbf{p},\mathbf{v}_2) = 0$), то вектор $[\mathbf{p},\mathbf{v}_2]$ перпендикулярен к ним обоим, причем направлен так, что три вектора $\mathbf{p},\mathbf{v}_2,[\mathbf{p},\mathbf{v}_2]$ образуют “правую тройку": наблюдателю, расположенному на конце вектора $[\mathbf{p},\mathbf{v}_2]$ кратчайший поворот от $\mathbf{p}$ к $\mathbf{v}_2$ кажется идущим против часовой стрелки. Отсюда следует, что с точки зрения наблюдателя, находящегося на конце вектора $\mathbf{p}$, преобразование вектора $\mathbf{v}_2$ в вектор $\mathbf{q}\mathbf{v}_2\mathbf{q}^{-1} = \cos\varphi\,\mathbf{v}_2 + \sin\varphi\,[\mathbf{p},\mathbf{v}_2]$ есть поворот против часовой стрелки на угол φ.

Итак, действие $\Phi_{\mathbf{q}}$ на вектор $\mathbf{v}$ описывается следующим образом: проекция $\mathbf{v}$ на ось, направленную по вектору $\mathbf{p}$, не меняется, а проекция на плоскость, перпендикулярную вектору $\mathbf{p}$, если смотреть на нее с конца вектора $\mathbf{p}$, поворачивается против часовой стрелки на угол φ. Это и означает поворот всего вектора $\mathbf{v}$ вокруг $\mathbf{p}$ на угол φ против часовой стрелки. $\square$

Литература

[1] Кострикин А.И. Введение в алгебру. Часть I. Основы алгебры. — 2-е изд., исправл. — М.: Физ.-мат. лит., 2001. — 272 с.

[2] Кострикин А.И. Введение в алгебру. Часть II. Линейная алгебра. — 2-е изд., исправл. — М.: Физ.-мат. лит., 2001. — 368 с.

[3] Кострикин А.И. Введение в алгебру. Часть III. Основные структуры. — 2-е изд., исправл. — М.: Физ.-мат. лит., 2001. — 272 с.

[4] Сборник задач по алгебре / Под ред. А.И. Кострикина. — М.: Наука. Гл.ред. физ.-мат. лит. , 1987. — 352 с.

[5] Белоногов В.А. Задачник по теории групп. — М.: Наука, 2000. — 239 с.

[6] Курош А.Г. Теория групп. — 3-е изд. — М.: Наука. Гл. ред. физ.-мат. лит., 1967. — 648 с.

[7] Холл М. Теория групп. — М: ИЛ, 1962. — 468 с.

[8] Каргаполов М.И., Мерзляков Ю.И. Основы теории групп. — 3-е изд., перераб. и доп. — М.: Наука, 1982. — 288 с.

[9] Богопольский О.В. Введение в теорию групп. — Москва-Ижевск: Институт компьютерных исследований, 2002. — 148 с.

[10] Ван-дер-Варден Б.Л. Алгебра. — М.:Наука, 1976. — 648 с.

[11] Ленг С. Алгебра. — М.: Мир, 1968 — 564 с.

[12] Скорняков Л.А. Элементы алгебры. — М.: Наука. Гл.ред. физ.-мат. лит. , 1980. — 240 с.

[13] Бахтурин Ю.А. Основные структуры современной алгебры. — М.: Наука, 1990. — 320 с.

[14] Фаддеев Д.К. Лекции по алгебре. — Изд. 3-е, стер. — СПб.: Лань, 2004. — 415 с.

[15] Винберг Э.Б. Курс алгебры. — 3-е изд., перераб. и доп. — М.: Факториал Пресс, 2002. — 544 с.

[16] Коксетер Г.С.М., Мозер У.О. Порождающие элементы и определяющие соотношения дискретных групп. — М.: Наука. Гл. ред. физ.-мат. лит., 1980. — 240 с.

[17] Кэртис Ч., Райнер И. Теория представлений конечных групп и ассоциативных алгебр. — М.: Наука. Гл. ред. физ.-мат. лит., 1980. — 668 с.

[18] Клейн Ф. Лекции об икосаэдре и решении уравнений пятой степени. — М.: Наука. Гл. ред. физ.-мат. лит., 1989. — 336 с.

[19] Дьедонне Ж. Линейная алгебра и элементарная геометрия. — М.: Наука. Гл.ред. физ.-мат. лит. , 1972. — 336 с.

[20] Бранец В.Н., Шмыглевский И.П. Применение кватернионов в задачах оринтации твердого тела. — М.: Наука. Гл.ред. физ.-мат. лит., 1973. — 320 с.

[21] Кантор И.Л., Солодовников А.С. Гиперкомплексные числа. — М.: Наука. Гл.ред. физ.-мат. лит., 1973. — 144 с.

[22] Гильберт Д., Кон-Фоссен С. Наглядная геометрия. — 3-е изд. — М.: Наука, 1981. — 344 с.

[23] Вейль Г. Симметрия. — М.: Наука. Гл. ред. физ.-мат. лит., 1968. — 192 с.

[24] Головина Л.И. Линейная алгебра и некоторые ее приложения. — Изд. 2-е, дополн. — М.: Наука. Гл. ред. физ.-мат. лит., 1975. — 408 с.

[25] Шубников А.В., Копцик В.А. Симметрия в науке и искусстве. — Изд. 3-е, дополн. — Москва-Ижевск: Ин-т компьютерн. исслед., 2004. — 560 с.

[26] Эллиот Дж., Добер П. Симметрия в физике. Том 1. Основные принципы и простые приложения. — М.: Мир, 1983. — 368 с.

[27] Эллиот Дж., Добер П. Симметрия в физике. Том 2. Дальнейшие приложения. — М.: Мир, 1983. — 416 с.

[28] Любарский Г.Я. Теория групп и физика. — М.: Наука. Гл. ред. физ.-мат. лит., 1986. — 224 с.

[29] Винберг Э.Б. Линейные представления групп. — М.: Наука. Гл. ред. физ.-мат. лит., 1985. — 144 с.

[30] Медведев Б.В. Начала теоретической физики. — М.: Наука. Гл. ред. физ.-мат. лит., 1977. — 496 с.