

ТЕОРИЯ ПОЛНЫХ ОРТОГОНАЛЬНЫХ ПРЯМЫХ РАЗЛОЖЕНИЙ ВЕКТОРНЫХ ПРОСТРАНСТВ¹

М. И. Анохин

Институт проблем информационной безопасности

Московского государственного университета им. М. В. Ломоносова, г. Москва, Россия

E-mail: anokhin@mccme.ru

Построена теория полных ортогональных (относительно обобщенных ортогональностей, заданных некоторыми частичными симметричными билинейными функциями) прямых разложений векторных пространств V , таких, что фактор-пространство V по некоторому специальному подпространству конечномерно. Основным результатом этой теории является некоторое описание всех таких разложений. Вышеупомянутая теория имеет приложение к теории прямых разложений p -ичных функций, где p — простое число.

Ключевые слова: векторное пространство, ортогональность, частичная симметричная билинейная функция, полное разложение, абелева группа.

1. Введение

1.1. Прямые разложения функций φ и ∇_φ -ортогональные прямые разложения абелевых групп

В настоящей работе продолжены исследования, начатые в [1]. В более общем виде, чем в [1], предмет этих исследований можно описать следующим образом. Пусть A и B — абелевы группы, φ — функция из A в B , $A = \bigoplus_{m \in M} A_m$ — некоторое разложение группы A в прямую сумму семейства подгрупп $(A_m \mid m \in M)$, индексированного элементами конечного множества M (такие разложения будем для краткости называть *конечными прямыми разложениями*). Тогда естественно сказать, что функция φ *разлагается в прямую сумму* семейства функций $(\varphi_m \mid m \in M)$ для указанного прямого разложения группы A , если $\varphi_m: A_m \rightarrow B$ и

$$\varphi\left(\sum_{m \in M} x_m\right) = \sum_{m \in M} \varphi_m(x_m)$$

при любых $x_m \in A_m$, $m \in M$. Такие разложения, называемые в дальнейшем *прямыми разложениями* функции φ , будем записывать в виде $\varphi = \bigoplus_{m \in M} \varphi_m$ и отождествлять с соответствующими семействами функций $(\varphi_m \mid m \in M)$. Нас интересуют всевозможные прямые разложения функции φ и, в частности, конечные прямые разложения группы A , для которых прямые разложения φ существуют.

Определим теперь зависящее от функции φ бинарное отношение ∇_φ на группе A , которое играет важную роль в изучении прямых разложений этой функции. Для произвольного $a \in A$ обозначим через $\mathbf{D}_a \varphi$ функцию из A в B , определенную равенством

$$(\mathbf{D}_a \varphi)(x) = \varphi(x + a) - \varphi(x)$$

¹Работа поддержана грантами РФФИ №07-01-00154, 10-01-00475.

при всех $x \in A$. Функция $\mathbf{D}_a \varphi$ называется *производной* функции φ по направлению a ; это понятие хорошо известно (см., например, [2, определение 3], [3, определение 2.68]). Тогда $u \nabla_\varphi w$ (где $u, w \in A$) в том и только в том случае, когда функция $\mathbf{D}_u \mathbf{D}_w \varphi$ тождественно равна нулю на A . Отношение ∇_φ обладает свойствами, аналогичными некоторым свойствам ортогональностей на векторных пространствах. Например, $u \nabla_\varphi w$ тогда и только тогда, когда $\sigma_\varphi(u, w) = 0$, где $u, w \in A$, а σ_φ — частичная симметричная билинейная над кольцом целых чисел функция на A (в смысле естественного аналога определения из п. 4.1), принимающая значения в B и заданная следующим образом:

$$\sigma_\varphi(u, w) \begin{cases} = b, & \text{если } \exists b \in B \forall x \in A (\mathbf{D}_u \mathbf{D}_w \varphi)(x) = b; \\ \text{не определено в противном случае.} \end{cases} \quad (1)$$

Другими словами, (1) означает, что $\sigma_\varphi(u, w)$ определено, если и только если функция $\mathbf{D}_u \mathbf{D}_w \varphi$ тождественно равна на A некоторому элементу $b \in B$, который в этом случае и является значением $\sigma_\varphi(u, w)$. Кроме того, $0 \nabla_\varphi a$ (или, что эквивалентно, $\sigma_\varphi(0, a) = 0$) при всех $a \in A$. Следовательно, если назвать *ортогональностью* на A всякое бинарное симметричное отношение $\perp$ на этой группе, такое, что для любого $a \in A$ множество $C_A^\perp(a) = \{x \in A \mid x \perp a\}$ является подгруппой A , то ∇_φ — ортогональность на A . Ортогональностью на A является также область определения $\diamond_\varphi$ функции σ_φ , рассматриваемая как бинарное отношение. Кроме того, $\diamond_\varphi$ удовлетворяет следующему условию:

$$\forall x, y \in A \left(C_A^{\diamond_\varphi}(x) + C_A^{\diamond_\varphi}(y) = A \implies C_A^{\diamond_\varphi}(x + y) = C_A^{\diamond_\varphi}(x) \cap C_A^{\diamond_\varphi}(y) \right). \quad (2)$$

Это доказывается точно так же, как и соответствующее утверждение в лемме 10 из [1]. Очевидно также, что если A и B являются элементарными абелевыми 2-группами (другими словами, аддитивными группами векторных пространств над полем $\text{GF}(2)$), то $a \nabla_\varphi a$ для всех $a \in A$.

В этом пункте через $\perp$ будем обозначать произвольную ортогональность на A . Прямое разложение $A = \bigoplus_{m \in M} A_m$ группы A называется *$\perp$ -ортогональным*, если $a_1 \perp a_2$ для любых $a_1 \in A_{m_1}, a_2 \in A_{m_2}$, где $m_1, m_2 \in M$ и $m_1 \neq m_2$. Связь ∇_φ -ортогональных прямых разложений группы A с прямыми разложениями функции φ выражается следующей теоремой, которая доказывается точно так же, как и теорема 1 из [1].

Теорема 1.1. Пусть $A = \bigoplus_{m \in M} A_m$ — произвольное конечное прямое разложение группы A . Тогда для этого разложения существуют прямые разложения функции φ , если и только если оно ∇_φ -ортогонально и $(M \neq \emptyset \vee \varphi(0) = 0)$. Кроме того, если выполнены эквивалентные условия предыдущего предложения, то прямые разложения функции φ для рассматриваемого прямого разложения группы A — это в точности разложения вида

$$\varphi = \bigoplus_{m \in M} (\varphi|_{A_m} + b_m),$$

где $b_m \in B$ (рассматриваемый в указанном прямом разложении φ как функция-константа на A_m) и $\sum_{m \in M} b_m = (1 - |M|)\varphi(0)$.

Теорема 1.1 показывает, что изучение прямых разложений произвольной функции $\varphi: A \rightarrow B$ эквивалентно изучению ∇_φ -ортогональных конечных прямых разложений группы A . При этом, очевидно, достаточно ограничиться *нетривиальными* прямыми

разложениями группы A , т.е. прямыми разложениями этой группы, состоящими из ненулевых подгрупп. Кроме того, если группа A удовлетворяет условию минимальности для подгрупп, то всякое нетривиальное $\perp$ -ортогональное конечное прямое разложение группы A может быть продолжено до полного $\perp$ -ортогонального конечного прямого разложения этой группы. Поэтому в данном случае изучение прямых разложений функции φ сводится к изучению полных ∇_φ -ортогональных конечных прямых разложений этой группы. Здесь $\perp$ -ортогональное прямое разложение группы A называется *полным $\perp$ -ортогональным прямым разложением*, если оно нетривиально и не может быть продолжено до какого-либо другого нетривиального $\perp$ -ортогонального прямого разложения или, другими словами, если оно состоит из $\perp$ -неразложимых подгрупп (т.е. ненулевых подгрупп, не допускающих разложения в прямую сумму двух $\perp$ -ортогональных ненулевых подгрупп; $\perp$ -ортогональность подгрупп U и W означает, что $u \perp w$ для всех $u \in U$ и $w \in W$).

1.2. Краткое изложение результатов

В п. 1.1 мы видели, что если A и B — абелевы группы, причем A удовлетворяет условию минимальности для подгрупп, то изучение прямых разложений произвольной функции $\varphi: A \rightarrow B$ в некотором смысле эквивалентно изучению полных ∇_φ -ортогональных конечных прямых разложений группы A . Однако, по мнению автора, изучение последних в общем случае очень сложно и вряд ли может привести к каким-либо глубоким результатам. Материал п. 1.1 был приведен в основном с целью обоснования актуальности задачи. В настоящей работе рассматривается несколько другой случай, а именно: пусть V — векторное пространство над произвольным полем F . Все введенные выше понятия, относящиеся к абелевым группам (производная функции по направлению, ортогональность и т.д.), естественно переносятся на случай векторных пространств. Например, *ортогональностью* на V называется любое бинарное симметричное отношение $\perp$ на этом пространстве, такое, что для любого $a \in V$ множество $C_V^\perp(a) = \{x \in V \mid x \perp a\}$ является подпространством пространства V (см. также п. 3.1). Пусть σ — частичная симметричная билинейная над полем F функция на пространстве V , принимающая значения в F и такая, что $\sigma(0, a)$ определено (и, следовательно, равно 0) для всех $a \in V$ (подробнее см. п. 4.1). Тогда ортогональностями на V являются область определения $\diamond$ функции σ (рассматриваемая как бинарное отношение) и бинарное отношение ∇ , определенное следующим образом:

$$x \nabla y \iff (x, y) \in \diamond \ \& \ \sigma(x, y) = 0,$$

где $x, y \in V$. Возможно, что ортогональности (в указанном выше смысле) и частичные симметричные билинейные функции на векторных пространствах представляют самостоятельный интерес и заслуживают отдельного изучения.

В отличие от п. 1.1, здесь мы не предполагаем, что функция σ связана с какой-либо функцией φ . Предположим, что φ — произвольная функция из V в F . Тогда взять в качестве σ функцию σ_φ , определенную формулой (1), не всегда возможно, так как σ_φ будет частичной симметричной билинейной функцией над кольцом целых чисел и, если $\text{char } F \neq 0$, над простым подполем поля F , но, вообще говоря, не над F . В случае, когда σ_φ является частичной симметричной билинейной функцией над полем F , мы называем σ_φ , $\diamond_\varphi$ и ∇_φ *ассоциированными с функцией φ* .

Пусть T — множество всех $a \in V$, таких, что $C_V^\diamond(a) = V$ и $a \nabla b$ для любого $b \in V$, удовлетворяющего равенству $C_V^\diamond(b) = V$ (см. также (17)). Предположим, что простран-

ство V/T конечномерно и

$$\forall x, y \in V \quad (C_V^\diamond(x) + C_V^\diamond(y) = V \implies C_V^\diamond(x + y) = C_V^\diamond(x) \cap C_V^\diamond(y)). \quad (3)$$

В этом случае удалось построить некоторую теорию полных ∇ -ортогональных прямых разложений пространства V . Как уже отмечалось в п. 1.1 (см. условие (2)), если ортогональность $\diamond$ ассоциирована с некоторой функцией из V в F , то условие (3) выполнено.

Основным результатом настоящей работы является описание всех полных ∇ -ортогональных прямых разложений пространства V (теорема 5.2). Это описание или его промежуточный вариант (теорема 5.1) существенно используются в доказательстве критериев каждого из следующих условий:

- ∇ -неразложимость пространства V (теорема 6.1). В некотором частном случае критерий этого условия был дан в § 5 работы [1];
- σ -эквивалентность двух полных ∇ -ортогональных прямых разложений пространства V , если $\text{char } F \neq 2$ (п. 1 теоремы 6.2). Здесь два прямых разложения пространства V называются σ -эквивалентными, если одно из них (с точностью до перестановки индексов) переводится в другое некоторым автоморфизмом этого пространства, сохраняющим σ . Если же $\text{char } F = 2$, то при некотором дополнительном условии (которое заведомо выполнено в случае, когда σ ассоциирована с некоторой функцией из V в F) любые два полных ∇ -ортогональных прямых разложения пространства V σ -эквивалентны (п. 2 теоремы 6.2). Кроме того, показано, что если $\text{char } F \neq 2$, то для любых двух полных ∇ -ортогональных прямых разложений пространства V имеет место локальная $(\diamond, \nabla)$ -эквивалентность, являющаяся некоторым ослабленным вариантом σ -эквивалентности (теорема 6.3);
- единственность полного ∇ -ортогонального прямого разложения пространства V (теорема 6.4). Ранее в теореме 3 работы [1] было дано некоторое условие, достаточное для этого (в рассматриваемом там частном случае).

Рассмотрим случай, когда поле F конечно и пространство V конечномерно. Ценность указанных результатов состоит еще и в том, что в данном случае они имеют в некотором смысле эффективный характер. А именно, предположим, что носители F и V содержатся в множестве всех конечных строк, состоящих из нулей и единиц. Пусть также поле F задается для алгоритмов с помощью своего носителя и таблиц сложения и умножения, пространство V — посредством своего носителя вместе с таблицами сложения в V и умножения элементов V на элементы F , а функция σ — в виде таблицы своих значений. Тогда из описания всех полных ∇ -ортогональных прямых разложений пространства V следует существование полиномиального недетерминированного алгоритма, множество всех выходных значений которого при вычислении на произвольном входе вида (F, V, σ) совпадает с множеством всех таких разложений пространства V (теорема 6.5). Кроме того, полученные критерии перечисленных выше условий могут быть проверены детерминированными алгоритмами за полиномиальное время по (F, V, σ) (теоремы 6.6 и 6.7; разумеется, предполагается, что при проверке σ -эквивалентности двух полных ∇ -ортогональных прямых разложений пространства V на вход алгоритму подаются также эти разложения). Подробнее об этом см. в п. 6.4.

Предположим теперь, что $F = \text{GF}(p)$, где p — простое число, V конечномерно и φ — произвольная функция из V в F . Такие функции φ называют p -ичными; именно этот случай рассматривался в работе [1]. Тогда σ_φ является частичной симметричной билинейной над полем F функцией на V , причем, как уже отмечалось, $\sigma_\varphi(0, a) = 0$

для всех $a \in V$ и для $\diamond = \diamond_\varphi$ выполнено условие (3). Это показывает, что к $\sigma = \sigma_\varphi$ применима теория, построенная в настоящей работе. В то же время указанный случай по существу эквивалентен частному случаю ситуации п. 1.1, когда A — конечная элементарная абелева p -группа, а B — циклическая группа порядка p . Поэтому ввиду сказанного в п. 1.1 мы получаем некоторую теорию прямых разложений функций из A в B , где A и B указаны в предыдущем предложении. Возможно, что общая теория полных ∇ -ортогональных прямых разложений векторных пространств, построенная в настоящей работе, имеет и другие приложения.

2. Определения, обозначения и необходимые факты

На протяжении всей работы через F обозначается некоторое поле, а через $\text{char } F$ — характеристика этого поля. Пусть также F^* — мультипликативная группа всех ненулевых элементов поля F , а $(F^*)^2 = \{x^2 \mid x \in F^*\}$. Если не оговорено иное, все объекты и понятия линейной алгебры рассматриваются над основным полем F . Как обычно, через $\text{GF}(q)$ обозначаем конечное поле из q элементов.

Под термином «граф» в настоящей работе понимается неориентированный граф без петель и кратных ребер. Мы допускаем случай, когда граф не имеет вершин. В этом случае граф не имеет также ребер и связных компонент (последние предполагаются непустыми). Внутреннюю прямую сумму подгрупп абелевой группы или подпространств векторного пространства обозначаем символом $\oplus$, а объединение попарно непересекающихся множеств — символом $\sqcup$. Отметим, что символы $\subset$ и $\supset$ в настоящей работе обозначают строгие включения. Семейства каких-либо элементов записываются с помощью круглых скобок (например, $(x_m \mid m \in M)$); при этом мы не предполагаем, что элементы семейства, соответствующие разным индексам, различны. Для записи множеств, как обычно, используются фигурные скобки; в отличие от семейств, каждый элемент множества входит в него лишь один раз. Мы обозначаем одним и тем же символом (например, π) соответствующие друг другу бинарное отношение на произвольном множестве X , бинарный предикат на этом множестве и подмножество $X \times X$. При этом

$$a \pi b \iff \pi(a, b) = 1 \iff (a, b) \in \pi$$

для произвольных $a, b \in X$. Здесь в первом условии π рассматривается как бинарное отношение на X , во втором — как бинарный предикат на X , а в третьем — как подмножество $X \times X$. Произвольное бинарное отношение π на множестве X естественно переносится с элементов на подмножества этого множества, а именно: если $A, B \subseteq X$, то запись $A \pi B$ означает, что $a \pi b$ для всех $a \in A$ и $b \in B$. Кроме того, вместо $\{a\} \pi B$ и $A \pi \{b\}$, где $a, b \in X$ и $A, B \subseteq X$, пишем $a \pi B$ и $A \pi b$ соответственно.

Через V всегда обозначаем некоторое векторное пространство. Пространство V может иметь специальный вид, если это указано явно. Пусть A — подмножество, а W — подпространство V . Тогда $\langle A \rangle$ обозначает подпространство V , порожденное множеством A . Если $A = \{a_1, \dots, a_n\}$ то, как обычно, будем писать $\langle a_1, \dots, a_n \rangle$ вместо $\langle \{a_1, \dots, a_n\} \rangle$. Через $\nu_{A,W}$ будем обозначать ограничение на A естественного гомоморфизма V на V/W . Всякое подпространство R пространства V , удовлетворяющее равенству $V = R \oplus W$, называется *прямым дополнением* к W в V . Очевидно, что если R — произвольное прямое дополнение к W в V , то $\nu_{R,W}$ — изоморфизм R на V/W . Последним утверждением будем пользоваться, не оговаривая этого особо. Произвольный элемент вида $v + \{0\} \in V/\{0\}$, где $v \in V$, естественно отождествляется с v , а фактор-

пространство $V/\{0\}$ — с V . Под суммой $\sum_{m \in M} U_m$ некоторого семейства $(U_m \mid m \in M)$ подпространств V , как обычно, понимается $\left\langle \bigcup_{m \in M} U_m \right\rangle$.

Если $\mathfrak{S}$ — некоторое множество подпространств пространства V , то будем писать $\sum \mathfrak{S}$ и $\bigoplus \mathfrak{S}$ вместо $\sum_{S \in \mathfrak{S}} S$ и $\bigoplus_{S \in \mathfrak{S}} S$ соответственно, чтобы не загромождать обозначения. Таким образом, здесь множество $\mathfrak{S}$ рассматривается как семейство $(S \mid S \in \mathfrak{S})$. Пусть теперь $\mathfrak{X}$ — некоторое множество подмножеств какого-либо множества M . Тогда, по аналогии с вышеуказанными обозначениями, вместо $\bigcup_{X \in \mathfrak{X}} X$ и $\bigcup_{X \in \mathfrak{X}} X$ используем записи $\bigcup \mathfrak{X}$ и $\bigcup \mathfrak{X}$ соответственно. Кроме того, если μ — некоторое отображение, определенное на M , то через $\mu(\mathfrak{X})$ будем обозначать множество $\{\mu(X) \mid X \in \mathfrak{X}\}$.

Под словами «разложение (векторного) пространства» понимается разложение этого пространства в сумму некоторого семейства его подпространств. Такие разложения естественно отождествляются с соответствующими семействами подпространств. Будем пользоваться (не оговаривая этого особо) следующим очевидным замечанием: если $V = \sum_{m \in M} U_m$ и $V = \bigoplus_{m \in M} W_m$ — разложения пространства V , причем $U_m \subseteq W_m$ при любом $m \in M$, то $U_m = W_m$ для всех $m \in M$.

Предположим, что на пространстве V определены предикаты $\pi_1, \dots, \pi_k$, имеющие конечные арности $l_1, \dots, l_k$ соответственно. Тогда соответствующую алгебраическую систему сигнатуры, состоящую из символов стандартной сигнатуры векторных пространств над полем F и символа l_i -арного предиката для каждого $i \in \{1, \dots, k\}$, будем обозначать через $(V; \pi_1, \dots, \pi_k)$. Вообще говоря, предикаты $\pi_1, \dots, \pi_k$ могут быть частичными и/или многозначными; в этом случае мы рассматриваем алгебраические системы в несколько обобщенном смысле. Для обобщенных алгебраических систем указанного вида используем только понятия изоморфизма и автоморфизма, которые определяются естественным образом. А именно, пусть на некотором векторном пространстве V' определены предикаты $\pi'_1, \dots, \pi'_k$, причем π'_i имеет ту же арность l_i , что и π_i , для каждого $i \in \{1, \dots, k\}$. Тогда изоморфизм векторных пространств $\alpha: V \rightarrow V'$ называется *изоморфизмом* $(V; \pi_1, \dots, \pi_k)$ на $(V'; \pi'_1, \dots, \pi'_k)$, если для любых $i \in \{1, \dots, k\}$ и $v_1, \dots, v_{l_i} \in V$

$$\pi'_i(\alpha(v_1), \dots, \alpha(v_{l_i})) \text{ определено} \iff \pi_i(v_1, \dots, v_{l_i}) \text{ определено},$$

и в этом случае $\pi'_i(\alpha(v_1), \dots, \alpha(v_{l_i})) = \pi_i(v_1, \dots, v_{l_i})$. Отношение изоморфизма для алгебраических систем будет обозначаться символом $\cong$. Кроме того, как обычно, $\text{Aut } A$ обозначает группу всех автоморфизмов произвольной алгебраической системы A . Разложения $V = \sum_{m \in M} U_m$ и $V = \sum_{n \in N} W_n$ пространства V называем $(\pi_1, \dots, \pi_k)$ -эквивалентными, если существуют биекция $\mu: M \rightarrow N$ и автоморфизм $\alpha \in \text{Aut}(V; \pi_1, \dots, \pi_k)$, такие, что $\alpha(U_m) = W_{\mu(m)}$ для всех $m \in M$. Назовем также указанные разложения пространства V *локально* $(\pi_1, \dots, \pi_k)$ -эквивалентными, если существует биекция $\mu: M \rightarrow N$, такая, что $(U_m; \pi_1, \dots, \pi_k) \cong (W_{\mu(m)}; \pi_1, \dots, \pi_k)$ для всех $m \in M$. При $k = 1$ опускаем скобки вокруг π_1 , когда речь идет о (локальной) (π_1) -эквивалентности разложений. Очевидно, что из $(\pi_1, \dots, \pi_k)$ -эквивалентности двух разложений пространства V следует их локальная $(\pi_1, \dots, \pi_k)$ -эквивалентность. Легко также видеть, что разложения $V = \sum \mathfrak{S}$ и $V = \sum \mathfrak{T}$ пространства V $(\pi_1, \dots, \pi_k)$ -эквивалентны тогда и только тогда, когда $\alpha(\mathfrak{S}) = \mathfrak{T}$ для некоторого $\alpha \in \text{Aut}(V; \pi_1, \dots, \pi_k)$, и локаль-

но $(\pi_1, \dots, \pi_k)$ -эквивалентны, если и только если $(U; \pi_1, \dots, \pi_k) \cong (W_U; \pi_1, \dots, \pi_k)$ для некоторой биекции $U \mapsto W_U$ множества $\mathfrak{S}$ на множество $\mathfrak{T}$.

Следующая лемма обобщает лемму 5 из [1] и доказывается аналогично ей.

Лемма 2.1. Пусть ω — какое-либо отображение из V в некоторое частично упорядоченное множество, удовлетворяющее условию максимальности; I — множество всех $v \in V \setminus \{0\}$, для которых не существует представления в виде $v_1 + v_2$, где $v_i \in V$ и $\omega(v_i) > \omega(v)$ при $i = 1, 2$. Тогда $\langle I \rangle = V$.

Доказательство. Предположим, что множество $V \setminus \langle I \rangle$ непусто. Выберем некоторый элемент $v \in V \setminus \langle I \rangle$, для которого $\omega(v)$ максимален в множестве $\omega(V \setminus \langle I \rangle)$. Так как $v \in V \setminus \{0\}$ и $v \notin I$, v может быть представлен в виде $v_1 + v_2$, где $v_i \in V$ и $\omega(v_i) > \omega(v)$ при $i = 1, 2$. Но тогда $v_1, v_2 \in \langle I \rangle$ (ввиду максимальности $\omega(v)$ в $\omega(V \setminus \langle I \rangle)$) и, следовательно, $v \in \langle I \rangle$, что противоречит выбору v . ■

3. Ортогональности на векторных пространствах

3.1. Определения, обозначения и необходимые факты

Следуя [1], назовем *ортогональностью* на векторном пространстве V любое бинарное симметричное отношение $\perp$ на этом пространстве, такое, что для любого $a \in V$ множество $\{x \in V \mid x \perp a\}$ является подпространством пространства V . Здесь через $\perp$ будем обозначать некоторую ортогональность на V . Ортогональность $\perp$ может иметь специальный вид, если это указано явно. Алгебраическую систему $(V; \perp)$, где $\perp$ рассматривается как бинарный предикат, естественно назвать (*векторным*) *пространством с ортогональностью*. Если $a \perp b$, где $a, b \in V$, то говорят, что элементы a и b *$\perp$ -ортогональны*. Аналогично, подмножества A и B пространства V называются *$\perp$ -ортогональными*, если $A \perp B$.

Для множества $A \subseteq V$ его *$\perp$ -ортогональное дополнение* $C_B^\perp(A)$ в множестве $B \subseteq V$ определяется равенством

$$C_B^\perp(A) = \{b \in B \mid b \perp a \text{ для всех } a \in A\}.$$

Очевидно, что если U — подпространство V , то $C_U^\perp(A)$ является подпространством U . Вместо $C_B^\perp(\{a_1, \dots, a_n\})$, где $a_1, \dots, a_n \in V$ и $B \subseteq V$, пишем $C_B^\perp(a_1, \dots, a_n)$. Отметим, что в работе [1] множества $C_V^\perp(a)$ и $C_V^\perp(A)$ обозначались соответственно через $a^\perp$ и $A^\perp$.

Легко видеть, что класс всех векторных пространств с ортогональностями является квазимногообразием (напомним, что мы рассматриваем векторные пространства над фиксированным полем F). Поэтому, в частности, этот класс замкнут относительно взятия подсистем и декартовых произведений (а следовательно, и прямых произведений). Разумеется, под прямым произведением семейства $((V_m; \perp_m) \mid m \in M)$ векторных пространств с ортогональностями понимается подсистема декартова произведения этого семейства, состоящая из всех $(a_m \mid m \in M)$, таких, что $a_m \in V_m$ и множество $\{m \in M \mid a_m \neq 0\}$ конечно. Пусть теперь W — произвольное подпространство $C_V^\perp(V)$. Тогда фактор-система пространства с ортогональностью $(V; \perp)$ по W является пространством с ортогональностью. Полученная при взятии этой фактор-системы ортогональность на V/W совпадает с ограничением на множество всех смежных классов V по W определенного выше отношения $\perp$ -ортогональности подмножеств V . Поэтому указанную ортогональность на V/W будем обозначать так же, как и исходную ортогональность на V . Очевидно, что

$$a + W \perp b + W \iff a \perp b \quad (4)$$

для произвольных $a, b \in V$. Используя эту эквивалентность, легко получить равенство

$$\mathcal{C}_{V/W}^\perp(V/W) = \mathcal{C}_V^\perp(V)/W. \quad (5)$$

В частности,

$$\mathcal{C}_{V/\mathcal{C}_V^\perp(V)}^\perp(V/\mathcal{C}_V^\perp(V)) = \{0\} \quad (6)$$

(см. также лемму 4 из [1]).

Замечание 3.1. Пусть W — подпространство $\mathcal{C}_V^\perp(V)$, а R — произвольное прямое дополнение к W в V . Тогда ввиду эквивалентности (4) $\nu_{R,W}$ является изоморфизмом $(R; \perp)$ на $(V/W; \perp)$.

3.2. Ортогональные разложения векторных пространств

Приведем определения нескольких понятий, важных для настоящей работы. Разложение $V = \sum_{m \in M} V_m$ пространства V (где M — некоторое множество) назовём *нетривиальным*, если $V_m \neq \{0\}$ для всех $m \in M$. Вышеуказанное разложение пространства V называется *$\perp$ -ортогональным*, если $V_{m_1} \perp V_{m_2}$ для любых различных $m_1, m_2 \in M$. Пространство $V \neq \{0\}$ называется *$\perp$ -разложимым*, если существует нетривиальное $\perp$ -ортогональное разложение этого пространства в прямую сумму двух подпространств; в противном случае V называется *$\perp$ -неразложимым*. Отметим, что $\{0\}$ не считается ни $\perp$ -разложимым, ни $\perp$ -неразложимым пространством. Нетривиальное $\perp$ -ортогональное прямое разложение $V = \bigoplus_{m \in M} V_m$ пространства V называется *полным $\perp$ -ортогональным* разложением, если для каждого $m \in M$ подпространство V_m $\perp$ -неразложимо или, другими словами, если это разложение не может быть продолжено до какого-либо другого нетривиального $\perp$ -ортогонального прямого разложения. Очевидно, что если $V = \bigoplus_{m \in M} V_m$ — нетривиальное прямое разложение V (в частности, полное $\perp$ -ортогональное разложение), то $V_{m_1} \neq V_{m_2}$ при $m_1 \neq m_2$ ($m_1, m_2 \in M$), поэтому данное разложение можно записать в виде $V = \bigoplus \mathfrak{S}$, где $\mathfrak{S} = \{V_m \mid m \in M\}$.

Замечание 3.2 [1, лемма 3]. Предположим, что $\mathcal{C}_V^\perp(V) = \{0\}$. Пусть $V = U + W$ — $\perp$ -ортогональное разложение пространства V . Тогда $W = \mathcal{C}_V^\perp(U)$. Действительно, включение $W \subseteq \mathcal{C}_V^\perp(U)$ тривиально. Пусть теперь $v \in \mathcal{C}_V^\perp(U)$. Представим v в виде $u + w$, где $u \in U$ и $w \in W$. Тогда $u \perp U$ (так как $v \perp U$ и $w \perp U$) и $u \perp W$. Поэтому $u \perp V$. Следовательно, $u = 0$ и $v = w \in W$. Таким образом, $\mathcal{C}_V^\perp(U) \subseteq W$.

Замечание 3.3. Предположим, что $\mathcal{C}_V^\perp(V) = \{0\}$. Тогда всякое $\perp$ -ортогональное разложение $V = \sum_{m \in M} V_m$ пространства V является прямым. Действительно, пусть $v \in V_m \cap \sum_{k \in M \setminus \{m\}} V_k$, где $m \in M$. Тогда $v \perp V_k$ для любого $k \in M \setminus \{m\}$ (так как $v \in V_m$) и $v \perp V_m$ (так как $v \in \sum_{k \in M \setminus \{m\}} V_k$). Поэтому $v \perp V$ и, следовательно, $v = 0$. Таким образом, $V_m \cap \sum_{k \in M \setminus \{m\}} V_k = \{0\}$ для любого $m \in M$ (см. также лемму 3 работы [1]).

Следующая лемма усиливает лемму 6 из [1].

Лемма 3.1. Пусть $V = \sum_{m \in M} V_m$ — $\perp$ -ортогональное разложение пространства V . Тогда

$$\mathcal{C}_V^\perp(V) = \sum_{m \in M} \mathcal{C}_{V_m}^\perp(V), \quad (7)$$

причем $\mathcal{C}_{V_m}^\perp(V) = \mathcal{C}_V^\perp(V) \cap V_m = \mathcal{C}_{V_m}^\perp(V_m)$ для всех $m \in M$.

Доказательство. Включение $\sum_{m \in M} \mathbb{C}_{V_m}^\perp(V) \subseteq \mathbb{C}_V^\perp(V)$ тривиально. Пусть теперь $v \in \mathbb{C}_V^\perp(V)$. Представим v в виде $\sum_{m \in M} v_m$, где $v_m \in V_m$ при всех $m \in M$, причем $\{m \in M \mid v_m \neq 0\}$ конечно. Для произвольного $m \in M$ положим $v'_m = \sum_{k \in M \setminus \{m\}} v_k$. Тогда $v_m = v - v'_m \perp V_m$ (так как $v \perp V_m$ и $v'_m \perp V_m$) и $v_m \perp \sum_{k \in M \setminus \{m\}} V_k$, поэтому $v_m \perp V$ при любом $m \in M$. Следовательно, $v \in \sum_{m \in M} \mathbb{C}_{V_m}^\perp(V)$. Таким образом, равенство (7) доказано. Для произвольного $m \in M$ равенство $\mathbb{C}_{V_m}^\perp(V) = \mathbb{C}_V^\perp(V) \cap V_m$ очевидно, а равенство $\mathbb{C}_{V_m}^\perp(V) = \mathbb{C}_{V_m}^\perp(V_m)$ вытекает из $\perp$ -ортогональности разложения $V = \sum_{m \in M} V_m$. Лемма доказана. ■

Следующая лемма показывает, что задача описания всех полных $\perp$ -ортогональных разложений пространства V эквивалентна задаче описания всех таких разложений пространства $V/\mathbb{C}_V^\perp(V)$.

Лемма 3.2. Пусть $S = \mathbb{C}_V^\perp(V)$, а $\mathcal{D}$ — множество всех троек $(\mathfrak{B}, R, \mathfrak{C})$, таких, что $S = \bigoplus \mathfrak{B}$ — разложение пространства S в прямую сумму одномерных подпространств, R — прямое дополнение к S в V и $V/S = \bigoplus \mathfrak{C}$ — полное $\perp$ -ортогональное разложение пространства V/S . Тогда отображение

$$(\mathfrak{B}, R, \mathfrak{C}) \mapsto \mathfrak{B} \sqcup \nu_{R,S}^{-1}(\mathfrak{C}), \quad (\mathfrak{B}, R, \mathfrak{C}) \in \mathcal{D}, \quad (8)$$

является биекцией $\mathcal{D}$ на множество всех $\mathfrak{S}$, таких, что $V = \bigoplus \mathfrak{S}$ — полное $\perp$ -ортогональное разложение пространства V . Если $\mathfrak{S}$ — образ тройки $(\mathfrak{B}, R, \mathfrak{C}) \in \mathcal{D}$ при отображении (8), то эти $\mathfrak{B}$, R и $\mathfrak{C}$ могут быть найдены по $\mathfrak{S}$ следующим образом:

$$\mathfrak{B} = \{U \in \mathfrak{S} \mid U \cap S \neq \{0\}\} = \{U \in \mathfrak{S} \mid \mathbb{C}_U^\perp(U) \neq \{0\}\} = \{U \in \mathfrak{S} \mid U \subseteq S\}; \quad (9)$$

$$R = \bigoplus (\mathfrak{S} \setminus \mathfrak{B}); \quad (10)$$

$$\mathfrak{C} = \nu_{R,S}(\mathfrak{S} \setminus \mathfrak{B}). \quad (11)$$

Доказательство. Пусть $(\mathfrak{B}, R, \mathfrak{C}) \in \mathcal{D}$. Из замечания 3.1 следует, что

$$R = \bigoplus \nu_{R,S}^{-1}(\mathfrak{C}) \quad (12)$$

— полное $\perp$ -ортогональное разложение пространства R . Поэтому

$$V = S \oplus R = (\bigoplus \mathfrak{B}) \oplus (\bigoplus \nu_{R,S}^{-1}(\mathfrak{C}))$$

является полным $\perp$ -ортогональным разложением пространства V ($\perp$ -неразложимость всех пространств из $\mathfrak{B}$ и условие $S \perp R$ тривиальны).

Предположим теперь, что $V = \bigoplus \mathfrak{S}$ — полное $\perp$ -ортогональное разложение пространства V . Пусть $\mathfrak{B}$, R и $\mathfrak{C}$ определены формулами (9)–(11). Из леммы 3.1 вытекает, что

$$S = \bigoplus_{U \in \mathfrak{S}} (U \cap S) = \bigoplus_{U \in \mathfrak{B}} (U \cap S),$$

причем $U \cap S = \mathbb{C}_U^\perp(U)$ для всех $U \in \mathfrak{S}$ и, следовательно, $\mathfrak{B} = \{U \in \mathfrak{S} \mid \mathbb{C}_U^\perp(U) \neq \{0\}\}$. Пусть $W \in \mathfrak{B}$. Выберем некоторый элемент $w \in (W \cap S) \setminus \{0\}$ и какое-либо прямое дополнение W' к $\langle w \rangle$ в W . Так как $W = \langle w \rangle \oplus W'$ и $\langle w \rangle \perp W'$, из $\perp$ -неразложимости W вытекает, что $W' = \{0\}$. Следовательно, $W = \langle w \rangle = W \cap S \subseteq S$. Это показывает, что

$\mathfrak{B} = \{U \in \mathfrak{S} \mid U \subseteq S\}$ и что $S = \bigoplus \mathfrak{B}$ — разложение пространства S в прямую сумму одномерных подпространств.

Очевидно, что R — прямое дополнение к $S = \bigoplus \mathfrak{B}$ в V . Так как $R = \bigoplus (\mathfrak{S} \setminus \mathfrak{B})$ — полное $\perp$ -ортогональное разложение пространства R , из замечания 3.1 вытекает, что $V/S = \bigoplus \mathfrak{C}$ — полное $\perp$ -ортогональное разложение пространства V/S . Следовательно, $(\mathfrak{B}, R, \mathfrak{C}) \in \mathcal{D}$. Кроме того, $\nu_{R,S}^{-1}(\mathfrak{C}) = \mathfrak{S} \setminus \mathfrak{B}$. Это показывает, что $(\mathfrak{B}, R, \mathfrak{C})$ является прообразом $\mathfrak{S}$ при отображении (8). Легко видеть (используя равенство (12)), что других прообразов $\mathfrak{S}$ при отображении (8) нет. Таким образом, отображение (8) биективно. ■

3.3. Одно условие для пространств с ортогональностями

В дальнейшем нам понадобится следующее условие для пространства с ортогональностью $(V; \perp)$:

$$\forall x, y \in V \quad (\mathcal{C}_V^\perp(x) + \mathcal{C}_V^\perp(y) = V \implies \mathcal{C}_V^\perp(x+y) = \mathcal{C}_V^\perp(x) \cap \mathcal{C}_V^\perp(y)) \quad (13)$$

(см. также условие (2) из работы [1]). Очевидно, что если $\perp = V \times V$, то $(V; \perp)$ удовлетворяет условию (13).

Замечание 3.4. Пусть $(V; \perp)$ — декартово или прямое произведение семейства $((V_m; \perp_m) \mid m \in M)$ векторных пространств с ортогональностями. Тогда легко видеть, что для любого $v = (v_m \mid m \in M) \in V$ (где $v_m \in V_m$) пространство $\mathcal{C}_V^\perp(v)$ есть декартово или соответственно прямое произведение семейства $(\mathcal{C}_{V_m}^\perp(v_m) \mid m \in M)$. Из этого нетрудно получить, что класс всех векторных пространств с ортогональностями (над фиксированным полем F), удовлетворяющих условию (13), замкнут относительно взятия декартовых и прямых произведений.

Замечание 3.5. Пусть $V = U + W$ — $\perp$ -ортогональное разложение пространства V . Тогда если $\mathcal{C}_U^\perp(x) + \mathcal{C}_U^\perp(y) = U$, где $x, y \in U$, то $\mathcal{C}_V^\perp(x) + \mathcal{C}_V^\perp(y) = V$. Из этого следует, что если $(V; \perp)$ удовлетворяет условию (13), то и $(U; \perp)$ удовлетворяет этому условию.

Замечание 3.6. Пусть W — произвольное подпространство $\mathcal{C}_V^\perp(V)$. Тогда, используя замечания 3.1, 3.4 и 3.5 и эквивалентность (4), легко показать, что $(V/W; \perp)$ удовлетворяет условию (13), если и только если $(V; \perp)$ удовлетворяет этому условию.

Лемма 3.3. Предположим, что $(V; \perp)$ удовлетворяет условию (13). Пусть $V = \sum_{m \in M} V_m$ — $\perp$ -ортогональное разложение пространства V . Тогда если $x_m, y_m \in V_m$ для всех $m \in M$, причем $\{m \in M \mid x_m \neq 0\}$ и $\{m \in M \mid y_m \neq 0\}$ конечны, то

$$\sum_{m \in M} x_m \perp \sum_{m \in M} y_m \iff \forall m \in M \quad x_m \perp y_m.$$

Доказательство. Импликация « $\Leftarrow$ » очевидна. Пусть теперь $\sum_{m \in M} x_m \perp \sum_{m \in M} y_m$. Фиксируем $m \in M$ и положим $z = \sum_{k \in M \setminus \{m\}} x_k$. Легко видеть, что $\mathcal{C}_V^\perp(x_m) + \mathcal{C}_V^\perp(z) = V$, так как $\mathcal{C}_V^\perp(x_m) \supseteq V_k$ для любого $k \in M \setminus \{m\}$ и $\mathcal{C}_V^\perp(z) \supseteq V_m$. Поэтому из условия (13) вытекает, что $\mathcal{C}_V^\perp\left(\sum_{k \in M} x_k\right) \subseteq \mathcal{C}_V^\perp(x_m)$. В частности, $x_m \perp \sum_{k \in M} y_k$. В то же время $x_m \perp \sum_{k \in M \setminus \{m\}} y_k$. Следовательно, $x_m \perp y_m$. Импликация « $\Rightarrow$ » доказана. ■

Замечание 3.7. Предположим, что $(V; \perp)$ удовлетворяет условию (13). Пусть $V = \bigoplus_{m \in M} U_m$ и $V = \bigoplus_{n \in N} W_n$ — $\perp$ -ортогональные разложения пространства V . Пусть

также μ — биекция M на N и α_m — изоморфизм $(U_m; \perp)$ на $(W_{\mu(m)}; \perp)$ для каждого $m \in M$. Тогда, используя лемму 3.3, легко видеть, что отображение $\alpha: V \rightarrow V$, определенное равенством

$$\alpha \left(\sum_{m \in M} u_m \right) = \sum_{m \in M} \alpha_m(u_m),$$

где $u_m \in U_m$ и $\{m \in M \mid u_m \neq 0\}$ конечно, является автоморфизмом $(V; \perp)$. Очевидно также, что $\alpha(U_m) = W_{\mu(m)}$ при любом $m \in M$. Поэтому рассматриваемые разложения пространства V $\perp$ -эквивалентны, если и только если они локально $\perp$ -эквивалентны.

Приведем нужные нам результаты из работы [1]. Следуя указанной работе, назовем элемент $v \in V$ $\perp$ -неразложимым, если он не может быть представлен в виде $v_1 + v_2$, где $v_i \in V$ и $C_V^\perp(v_i) \supset C_V^\perp(v)$ при $i = 1, 2$. В следующих двух леммах через I обозначается множество всех ненулевых $\perp$ -неразложимых элементов пространства V .

Лемма 3.4. Предположим, что $(V; \perp)$ удовлетворяет условию (13), причем $C_V^\perp(V) = \{0\}$. Пусть $V = \bigoplus_{m \in M} V_m$ — $\perp$ -ортогональное разложение пространства V (всякое такое разложение является прямым ввиду замечания 3.3). Тогда $I \subseteq \bigcup_{m \in M} V_m$ или, что эквивалентно, $I = \bigsqcup_{m \in M} (I \cap V_m)$.

Лемма 3.5. Предположим, что $(V; \perp)$ удовлетворяет условию (13), причем V конечномерно и $C_V^\perp(V) = \{0\}$. Пусть Δ — некоторая ортогональность на V , содержащаяся в $\perp$. Пусть также $\mathfrak{X}$ — множество всех связных компонент графа с множеством вершин I , в котором две различные вершины a и b смежны тогда и только тогда, когда они не Δ -ортогональны. Тогда $V = \bigoplus_{X \in \mathfrak{X}} \langle X \rangle$, причем это равенство дает единственное полное Δ -ортогональное разложение пространства V .

Леммы 3.4 и 3.5 доказываются точно так же, как соответственно леммы 7 и 8 из работы [1].

4. Частичные симметричные билинейные функции на векторных пространствах, принимающие значения в основном поле

4.1. Определения, обозначения и необходимые факты

Пусть σ — функция из $\diamond$ в F , где $\diamond$ — некоторое подмножество $V \times V$. Тогда σ называется *частичной симметричной билинейной функцией* на V , если

$$a \diamond b \implies b \diamond a \text{ \& } \sigma(b, a) = \sigma(a, b), \quad (14)$$

$$a_1 \diamond b \text{ \& } a_2 \diamond b \implies a_1 + a_2 \diamond b \text{ \& } \sigma(a_1 + a_2, b) = \sigma(a_1, b) + \sigma(a_2, b), \quad (15)$$

$$a \diamond b \implies \lambda a \diamond b \text{ \& } \sigma(\lambda a, b) = \lambda \sigma(a, b) \quad (16)$$

для любых $a, a_1, a_2, b \in V$ и $\lambda \in F$. Очевидно, что из условий (14)–(16) следует линейность σ и по второму аргументу, т. е.

$$\begin{aligned} a \diamond b_1 \text{ \& } a \diamond b_2 &\implies a \diamond b_1 + b_2 \text{ \& } \sigma(a, b_1 + b_2) = \sigma(a, b_1) + \sigma(a, b_2), \\ a \diamond b &\implies a \diamond \lambda b \text{ \& } \sigma(a, \lambda b) = \lambda \sigma(a, b) \end{aligned}$$

при произвольных $a, b, b_1, b_2 \in V$ и $\lambda \in F$. Альтернативным образом можно считать, что σ определена на всем $V \times V$, но принимает значения в $F \sqcup \{\infty\}$. В этом случае σ называется *частичной симметричной билинейной функцией* на V , если условия (14)–(16) выполняются для множества $\diamond = \{(a, b) \mid a, b \in V, \sigma(a, b) \in F\}$. Очевидно,

что эти два подхода по сути эквивалентны. Все частичные симметричные билинейные функции, рассматриваемые в настоящей работе, предполагаются принимающими значения в основном поле F , если не оговорено противное.

Вообще говоря, область определения $\diamond$ частичной симметричной билинейной функции σ может быть пустой. Но этот случай не представляет интереса. Если же $\diamond \neq \emptyset$, то $V_0 = \{x \in V \mid 0 \diamond x\}$ — подпространство V и $\diamond \subseteq V_0 \times V_0$. Следовательно, в этом случае σ является по существу частичной симметричной билинейной функцией на V_0 , причем $0 \diamond V_0$.

В дальнейшем, если не оговорено противное, через σ будем обозначать некоторую частичную симметричную билинейную функцию на V с областью определения $\diamond \subseteq V \times V$. Кроме того, предполагаем, что $0 \diamond V$; это предположение почти не ограничивает общность (см. предыдущий абзац). Функция σ может иметь специальный вид, если это указано явно. Алгебраическую систему $(V; \sigma)$, где σ рассматривается как частичный многозначный бинарный предикат, будем называть *(векторным) пространством с частичной симметричной билинейной функцией*.

Очевидно, что $\diamond$ является ортогональностью на V . Определим бинарное отношение ∇ на V следующим образом:

$$a \nabla b \iff a \diamond b \ \& \ \sigma(a, b) = 0,$$

где $a, b \in V$. Тогда легко видеть, что ∇ — ортогональность на V . Положим для краткости

$$S_0 = C_V^\nabla(V), \quad S_1 = C_V^\diamond(V), \quad T = C_{S_1}^\nabla(S_1). \quad (17)$$

Очевидно, что $S_0 \subseteq T \subseteq S_1$.

Замечание 4.1. Легко видеть, что отображение, ставящее в соответствие произвольному смежному классу $a + S_0$, где $a \in S_1$, линейную функцию $v + T \mapsto \sigma(a, v)$ (где $v \in V$), определено корректно и является инъективным гомоморфизмом S_1/S_0 в векторное пространство всех линейных функций из V/T в F (т.е. в сопряженное пространство для V/T). Поэтому если V/T конечномерно, то и S_1/S_0 конечномерно, причем $\dim(S_1/S_0) \leq \dim(V/T)$. Следовательно, конечномерность V/T эквивалентна конечномерности V/S_0 .

Обозначим через ρ естественный гомоморфизм V/S_0 на V/T , т.е. гомоморфизм $a + S_0 \mapsto a + T$, где $a \in V$. Из эквивалентности (4) следует, что

$$x \diamond y \iff \rho(x) \diamond \rho(y) \quad (18)$$

для любых $x, y \in V/S_0$. Нам потребуется также легко проверяемое равенство

$$\rho^{-1}(\langle X \rangle) = \langle \rho^{-1}(X) \rangle + (T/S_0), \quad (19)$$

в котором X — произвольное подмножество V/T .

Замечание 4.2. Пусть L — подпространство V/T и Q — произвольное прямое дополнение к T/S_0 в $\rho^{-1}(L)$. Тогда очевидно, что $Q \cong \rho^{-1}(L)/(T/S_0) \cong L$ и, следовательно, $\dim Q = \dim L$.

Если U — подпространство V , то очевидно, что σ является частичной симметричной билинейной функцией на U с областью определения $\diamond_U = \diamond \cap (U \times U)$, причем $0 \diamond_U U$. Пусть теперь W — подпространство S_0 . Тогда легко видеть, что формула

$$(a + W, b + W) \mapsto \sigma(a, b), \quad a, b \in V, \ a \diamond b,$$

корректно определяет частичную симметричную билинейную функцию на V/W с областью определения

$$\{(a + W, b + W) \mid a, b \in V, a \diamond b\} = \{(x, y) \mid x, y \in V/W, x \diamond y\}$$

(см. эквивалентность (4)), причем $0 \diamond V/W$. Эту частичную симметричную билинейную функцию мы обозначаем так же, как и исходную, т. е. через σ .

Замечание 4.3. Пусть W — подпространство S_0 и R — произвольное прямое дополнение к W в V . Тогда $\nu_{R,W}$ является не только изоморфизмом $(R; \nabla)$ на $(V/W; \nabla)$ и $(R; \diamond)$ на $(V/W; \diamond)$ (см. замечание 3.1), но и изоморфизмом $(R; \sigma)$ на $(V/W; \sigma)$.

Предположим, что каждому $m \in M$, где M — некоторое множество, поставлены в соответствие векторное пространство V_m и частичная симметричная билинейная функция σ_m на V_m с областью определения $\diamond_m \subseteq V_m \times V_m$. Пусть $(V; \diamond)$ — прямое произведение семейства $((V_m; \diamond_m) \mid m \in M)$ векторных пространств с ортогональностями. Определим функцию $\sigma: \diamond \rightarrow F$ равенством

$$\sigma((a_m \mid m \in M), (b_m \mid m \in M)) = \sum_{m \in M} \sigma_m(a_m, b_m),$$

где $a_m, b_m \in V_m$ при любом $m \in M$, $(a_m \mid m \in M), (b_m \mid m \in M) \in V$ (т. е. $\{m \in M \mid a_m \neq 0\}$ и $\{m \in M \mid b_m \neq 0\}$ конечны) и $(a_m \mid m \in M) \diamond (b_m \mid m \in M)$ (указанная сумма определена, так как множество $\{m \in M \mid \sigma_m(a_m, b_m) \neq 0\}$ конечно). Тогда непосредственно проверяется, что σ — частичная симметричная билинейная функция на V с областью определения $\diamond$, причем если $0 \diamond V_m$ для всех $m \in M$, то $0 \diamond V$. Будем называть $(V; \sigma)$ *прямым ортогональным произведением* семейства $((V_m; \sigma_m) \mid m \in M)$ пространств с частичными симметричными билинейными функциями.

Пусть снова σ — произвольная частичная симметричная билинейная функция на некотором векторном пространстве V с областью определения $\diamond$, причем $0 \diamond V$. Следующая лемма является аналогом замечания 3.7 и доказывается аналогично ему.

Лемма 4.1. Предположим, что $(V; \diamond)$ удовлетворяет условию (13). Пусть $V = \bigoplus_{m \in M} U_m$ и $V = \bigoplus_{n \in N} W_n$ — ∇ -ортогональные разложения пространства V . Тогда

- 1) если μ — биекция M на N и α_m — изоморфизм $(U_m; \sigma)$ на $(W_{\mu(m)}; \sigma)$ для каждого $m \in M$, то отображение $\alpha: V \rightarrow V$, определенное равенством

$$\alpha \left(\sum_{m \in M} u_m \right) = \sum_{m \in M} \alpha_m(u_m),$$

где $u_m \in U_m$ и $\{m \in M \mid u_m \neq 0\}$ конечно, является автоморфизмом $(V; \sigma)$;

- 2) рассматриваемые разложения пространства V σ -эквивалентны, если и только если они локально σ -эквивалентны.

4.2. Пространства типов 1 и 2

Большая часть приводимого здесь материала известна в линейной алгебре, хотя и в других терминах.

Назовем $(V; \sigma)$ или, короче, V пространством *типа 1*, если $V = \langle a \rangle$ для некоторого $a \in V$, такого, что $a \diamond a$ (и, следовательно, $V \diamond V$, т. е. $\diamond = V \times V$) и $a \not\triangleright a$ (или, что эквивалентно, $\sigma(a, a) \neq 0$). Кроме того, $(V; \sigma)$ или просто V будет называться пространством *типа 2*, если $\text{char } F = 2$, $V \diamond V$ и $V = \langle a, b \rangle$ для некоторых $a, b \in V$, удовлетворяющих равенствам $\sigma(a, a) = \sigma(b, b) = 0$ и $\sigma(a, b) = 1$ (из которых следует,

что a и b линейно независимы). Другими словами, $(V; \sigma)$ имеет тип 2, если и только если $\text{char } F = 2$, $\Diamond = V \times V$ и матрица билинейной функции σ в некотором базисе пространства V имеет вид $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. Очевидно, что если $(V; \sigma)$ — пространство типа 1 или типа 2, то билинейная функция σ невырождена на V (т. е. $C_V^\nabla(V) = \{0\}$).

Пусть $(V; \sigma)$ — пространство типа 1. Поставим ему в соответствие смежный класс $\varkappa(V; \sigma) \in F^*/(F^*)^2$ следующим образом:

$$\varkappa(V; \sigma) = \sigma(v, v)(F^*)^2,$$

где v — произвольный элемент $V \setminus \{0\}$; очевидно, что это определение корректно.

Замечание 4.4. Пусть $(V; \sigma)$ и $(V'; \sigma')$ — пространства типа 1. Тогда легко видеть, что $(V; \sigma) \cong (V'; \sigma')$, если и только если $\varkappa(V; \sigma) = \varkappa(V'; \sigma')$.

Если пространство V имеет тип 1, то его ∇ -неразложимость тривиальна. Следующая лемма утверждает ∇ -неразложимость пространств типа 2.

Лемма 4.2. Если V — пространство типа 2, то оно ∇ -неразложимо.

Доказательство. Предположим, что V — ∇ -разложимое пространство типа 2. Тогда $V = \langle u \rangle \oplus \langle w \rangle$ для некоторых $u, w \in V \setminus \{0\}$, таких, что $u \nabla w$. Кроме того, $u \nabla u$ и $w \nabla w$, так как $v \nabla v$ для всех $v \in V$. Следовательно, $V \nabla V$, что неверно. ■

Лемма 4.3. Пусть $\Diamond = V \times V$ и $V \not\cong V$. Тогда V содержит подпространство типа 1 или типа 2.

Доказательство. Предположим сначала, что существует $a \in V$, для которого $a \not\cong a$. Тогда $\langle a \rangle$ — подпространство типа 1 пространства V . Считаем теперь, что

$$\forall x \in V \quad x \nabla x. \quad (20)$$

Это возможно только при $\text{char } F = 2$, так как в противном случае из условия (20) ввиду того, что

$$\forall x, y \in V \quad (\sigma(x, y) = (\sigma(x + y, x + y) - \sigma(x, x) - \sigma(y, y))/2),$$

следует, что $V \nabla V$, вопреки условию леммы. Выберем некоторые $a, b \in V$, такие, что $a \not\cong b$ (возможность такого выбора вытекает из условия $V \not\cong V$). Заменив a на $(1/\sigma(a, b))a$, можно добиться выполнения равенства $\sigma(a, b) = 1$. Кроме того, $\sigma(a, a) = \sigma(b, b) = 0$ ввиду условия (20). Таким образом, в данном случае $\langle a, b \rangle$ является подпространством типа 2 пространства V . ■

4.3. ∇ -ортогональные дополнения к конечномерным подпространствам S_1

Первое утверждение следующей леммы хорошо известно в случае, когда V конечномерно и $\Diamond = V \times V$.

Лемма 4.4. Пусть U — произвольное конечномерное подпространство S_1 , такое, что билинейная функция σ невырождена на U (другими словами, $C_U^\nabla(U) = \{0\}$). Тогда $V = U \oplus C_V^\nabla(U)$. Кроме того, если $V = U + W$ — ∇ -ортогональное разложение пространства V , то $W = C_V^\nabla(U)$.

Доказательство. Пусть $v \in V$. Тогда $x \mapsto \sigma(v, x)$, где $x \in U$, является линейной функцией из U в F . Ввиду конечномерности U и невырожденности σ на U всякая такая функция имеет вид $x \mapsto \sigma(u, x)$ (где $x \in U$) для некоторого $u \in U$. Следовательно,

можно выбрать $u \in U$, удовлетворяющий равенству $\sigma(v, x) = \sigma(u, x)$ для любого $x \in U$. Тогда $v = u + (v - u) \in U + C_V^\nabla(U)$, так как $v - u \nabla U$. Таким образом, $V = U + C_V^\nabla(U)$, причем эта сумма является прямой ввиду того, что $U \cap C_V^\nabla(U) = C_V^\nabla(U) = \{0\}$.

Предположим теперь, что $V = U + W$ — ∇ -ортогональное разложение пространства V . Тогда равенство $W = C_V^\nabla(U)$ легко вытекает из очевидного включения $W \subseteq C_V^\nabla(U)$ и уже доказанного равенства $V = U \oplus C_V^\nabla(U)$. ■

Лемма 4.5.

1. Пусть $\text{char } F \neq 2$, $u \in S_1$ и $t \in T$, причем $u \not\nabla u$. Тогда $(C_V^\nabla(u); \sigma) \cong (C_V^\nabla(u + t); \sigma)$.
2. Пусть $u_1, u_2 \in S_1$ и $t_1, t_2 \in T$, причем $\sigma(u_1, u_1) = \sigma(u_2, u_2) = 0$ и $\sigma(u_1, u_2) = 1$. Тогда $(C_V^\nabla(u_1, u_2); \sigma) \cong (C_V^\nabla(u_1 + t_1, u_2 + t_2); \sigma)$.

Доказательство. Докажем сначала утверждение 1. Легко видеть, что отображение

$$x \mapsto x - \frac{\sigma(x, t)}{\sigma(u, u)} \left(\frac{1}{2}t + u \right), \quad x \in C_V^\nabla(u),$$

является изоморфизмом $(C_V^\nabla(u); \sigma)$ на $(C_V^\nabla(u + t); \sigma)$ (обратным к этому отображению является $y \mapsto y + (\sigma(y, t)/\sigma(u, u))((1/2)t + u)$, где $y \in C_V^\nabla(u + t)$).

Утверждение 2 доказывается аналогично, а именно непосредственно проверяется, что отображение

$$x \mapsto x - \sigma(x, t_1)(u_2 + t_2) - \sigma(x, t_2)u_1, \quad x \in C_V^\nabla(u_1, u_2),$$

является изоморфизмом $(C_V^\nabla(u_1, u_2); \sigma)$ на $(C_V^\nabla(u_1 + t_1, u_2 + t_2); \sigma)$ (обратным к этому отображению является $y \mapsto y + \sigma(y, t_1)(u_2 + t_2) + \sigma(y, t_2)u_1$, где $y \in C_V^\nabla(u_1 + t_1, u_2 + t_2)$).

Лемма доказана. ■

Лемма 4.6. Предположим, что $(V; \diamond)$ удовлетворяет условию (13) и S_1/T конечномерно. Пусть также $x \nabla x$ для всех $x \in S_1$ в случае, когда $\text{char } F = 2$. Тогда если U и W — прямые дополнения к T в S_1 , то $(C_V^\nabla(U); \sigma) \cong (C_V^\nabla(W); \sigma)$.

Доказательство. Используем индукцию по $\dim(S_1/T) = \dim U = \dim W$. Если $\dim(S_1/T) = 0$, то $U = W = \{0\}$ и утверждение леммы тривиально. Пусть теперь $\dim(S_1/T) \geq 1$. Очевидно, что $U \not\nabla U$, поэтому ввиду леммы 4.3 существует подпространство $U_0 \subseteq U$, имеющее тип 1, если $\text{char } F \neq 2$, или тип 2, если $\text{char } F = 2$ (в последнем случае U не содержит подпространств типа 1, так как $x \nabla x$ для всех $x \in U$). Выберем базис $u_1, \dots, u_k$ пространства U_0 (здесь $k \in \{1, 2\}$), такой, что если $\text{char } F = 2$, то σ в этом базисе имеет матрицу $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. Пусть также $t_1, \dots, t_k$ — некоторые элементы T , для которых $u_1 + t_1, \dots, u_k + t_k \in W$. Тогда $u_1 + t_1, \dots, u_k + t_k$ линейно независимы. Положим $W_0 = \langle u_1 + t_1, \dots, u_k + t_k \rangle$. Очевидно, что σ в базисе $u_1 + t_1, \dots, u_k + t_k$ имеет ту же матрицу, что и в базисе $u_1, \dots, u_k$. Это показывает, что $(U_0; \sigma) \cong (W_0; \sigma)$. Кроме того, из леммы 4.5 вытекает, что $(C_V^\nabla(U_0); \sigma) \cong (C_V^\nabla(W_0); \sigma)$. Поэтому ввиду леммы 4.4 и утверждения 1 леммы 4.1 можно выбрать $\alpha \in \text{Aut}(V; \sigma)$, для которого $\alpha(U_0) = W_0$ и $\alpha(C_V^\nabla(U_0)) = C_V^\nabla(W_0)$.

Положим для краткости $V' = C_V^\nabla(W_0)$ и $S'_1 = C_{V'}^\diamond(V')$. Тогда $V = W_0 \oplus V'$ по лемме 4.4. Следовательно, $S_1 = W_0 \oplus S'_1$ и $T = C_{S'_1}^\nabla(S'_1)$ ввиду леммы 3.1, так как $C_{W_0}^\diamond(W_0) = W_0$ и $C_{W_0}^\nabla(W_0) = \{0\}$. С другой стороны, из леммы 4.4 вытекает, что

$$S_1 = W \oplus T = W_0 \oplus C_W^\nabla(W_0) \oplus T,$$

где $C_W^\nabla(W_0) \oplus T \subseteq S_1 \cap V' = S'_1$ (см. лемму 3.1). Поэтому $C_W^\nabla(W_0) \oplus T = S'_1$. Аналогично,

$$C_U^\nabla(U_0) \oplus T = C_{C_V^\nabla(U_0)}^\diamond(C_V^\nabla(U_0)).$$

Применив к обеим частям последнего равенства автоморфизм α и воспользовавшись очевидным равенством $\alpha(T) = T$, получим, что $C_{\alpha(U)}^\nabla(W_0) \oplus T = S'_1$. По предположению индукции, примененному к пространству V' и прямым дополнениям $C_{\alpha(U)}^\nabla(W_0)$ и $C_W^\nabla(W_0)$ к подпространству T в S'_1 , имеет место изоморфизм

$$(C_{V'}^\nabla(C_{\alpha(U)}^\nabla(W_0)); \sigma) \cong (C_{V'}^\nabla(C_W^\nabla(W_0)); \sigma). \quad (21)$$

Здесь применение предположения индукции возможно, так как $\dim(S'_1/T) = \dim(S_1/T) - k$. Кроме того, $\alpha(U) = W_0 \oplus C_{\alpha(U)}^\nabla(W_0)$ (так как $U = U_0 \oplus C_U^\nabla(U_0)$ по лемме 4.4) и, следовательно,

$$C_V^\nabla(\alpha(U)) = V' \cap C_V^\nabla(C_{\alpha(U)}^\nabla(W_0)) = C_{V'}^\nabla(C_{\alpha(U)}^\nabla(W_0)). \quad (22)$$

Аналогично, $W = W_0 \oplus C_W^\nabla(W_0)$ и

$$C_V^\nabla(W) = V' \cap C_V^\nabla(C_W^\nabla(W_0)) = C_{V'}^\nabla(C_W^\nabla(W_0)). \quad (23)$$

Утверждение леммы следует теперь из (21)–(23) и очевидного изоморфизма $(C_V^\nabla(U); \sigma) \cong (C_V^\nabla(\alpha(U)); \sigma)$. ■

4.4. Некоторые ∇ -ортогональные разложения пространства V в случае, когда σ всюду определена и V/S_0 конечномерно

Будем считать, что σ определена на всем $V \times V$ (т. е. $\diamond = V \times V$) и пространство V/S_0 конечномерно.

Пусть R — какое-либо прямое дополнение к S_0 в V . Тогда $(R; \sigma) \cong (V/S_0; \sigma)$ (см. замечание 4.3) и, следовательно, R конечномерно и σ невырождена на R . Применив к R известные результаты линейной алгебры (см. теоремы IV.6 и IV.7 из [4]), получим следующую лемму.

Лемма 4.7. Существует ∇ -ортогональное разложение

$$V = (\bigoplus \mathfrak{A}) \oplus S_0 \quad (24)$$

пространства V , в котором множество $\mathfrak{A}$ состоит из подпространств типов 1 и 2.

Очевидно, что множество $\mathfrak{A}$ в любом разложении вида (24) конечно.

Замечание 4.5. Разложение (24) из леммы 4.7 строится с помощью следующего хорошо известного процесса:

- 1) положить $\mathfrak{A} = \emptyset$ и $U = V$;
- 2) если $U \nabla U$, то закончить процесс;
- 3) если $U \not\nabla U$, то выбрать некоторое подпространство $W \subseteq U$ типа 1 или 2 (это возможно ввиду леммы 4.3), добавить W к множеству $\mathfrak{A}$, заменить U на $C_U^\nabla(W)$ и перейти к шагу 2.

Из леммы 4.4 вытекает, что перед каждым выполнением шага 2 имеет место равенство

$$V = (\bigoplus \mathfrak{A}) \oplus U, \quad (25)$$

дающее ∇ -ортогональное разложение пространства V . При этом $S_0 \subseteq U$ и $\dim(U/S_0)$ после каждого выполнения шага 3 уменьшается на 1 или 2. Следовательно, шаг 3 может выполняться не более $\dim(V/S_0)$ раз, после чего процесс закончится на шаге 2. После окончания процесса (на шаге 2) получим, что $U = S_0$ (ввиду равенства (25) и леммы 3.1), поэтому (25) дает требуемое разложение. Кроме того, легко видеть (используя лемму 4.4), что указанный процесс позволяет построить все разложения (24), удовлетворяющие условиям леммы 4.7.

Выясним теперь, когда разложение (24) из леммы 4.7 единственно.

Лемма 4.8. Разложение (24) пространства V , удовлетворяющее условиям леммы 4.7, является единственным разложением такого вида тогда и только тогда, когда выполнено хотя бы одно из следующих условий:

- 1) $\mathfrak{A} = \emptyset$ (т.е. $V = S_0$);
- 2) $S_0 = \{0\}$ и всякое подпространство пространства V , имеющее тип 1 или 2, принадлежит $\mathfrak{A}$.

Доказательство. Пусть указанное разложение единственно и $\mathfrak{A} \neq \emptyset$. Предположим, что $S_0 \neq \{0\}$, и выберем некоторый элемент $s \in S_0 \setminus \{0\}$, а также некоторое подпространство $W \in \mathfrak{A}$ и представим его в виде $\langle w \rangle \oplus W_0$, где $w \in W \setminus \{0\}$ и W_0 — подпространство W . Тогда $V = (\langle w + s \rangle \oplus W_0) \oplus (\bigoplus (\mathfrak{A} \setminus \{W\})) \oplus S_0$ — разложение пространства V , удовлетворяющее условиям леммы 4.7 и отличное от исходного. Полученное противоречие показывает, что $S_0 = \{0\}$.

Пусть подпространство $U \subseteq V$ имеет тип 1 или 2. По лемме 4.4 $V = U \oplus C_V^\nabla(U)$, так как σ невырождена на U . Из леммы 4.7 вытекает, что существует ∇ -ортогональное разложение $C_V^\nabla(U) = \bigoplus \mathfrak{A}'$ подпространства $C_V^\nabla(U)$, состоящее из подпространств типов 1 и 2 (очевидно, что σ невырождена на $C_V^\nabla(U)$). Тогда разложение $V = U \oplus (\bigoplus \mathfrak{A}')$ пространства V удовлетворяет условиям леммы 4.7. Следовательно, $U \in \mathfrak{A}$. Таким образом, выполнено условие 2. Обратно, если выполнено условие 1 или условие 2, то очевидно, что рассматриваемое разложение единственно. ■

5. Полные ∇ -ортогональные разложения пространства V

Предположим, что пространство с ортогональностью $(V; \diamond)$ удовлетворяет условию (13). Опишем полные ∇ -ортогональные разложения пространства V при условии конечномерности пространства V/T или, что эквивалентно, пространства V/S_0 (см. замечание 4.1). Это будет сделано в два этапа. Сначала (в п. 5.1), предполагая, что пространство S_1/T конечномерно, сведём задачу описания полных ∇ -ортогональных разложений пространства V к задаче описания таких разложений пространств некоторого специального вида (теорема 5.1). Затем (в п. 5.2) решим последнюю из указанных задач в предположении конечномерности пространства V/T (леммы 5.12 и 5.13). Основным результатом, описывающий полные ∇ -ортогональные разложения пространства V , приводится в п. 5.3 (теорема 5.2); при этом нужно предполагать конечномерность V/T .

5.1. Сведение задачи описания полных ∇ -ортогональных разложений пространства V к некоторому частному случаю

Пусть пространство S_1/T конечномерно. Обозначим через $\mathcal{A}$ множество всех множеств $\mathfrak{A}$, состоящих из подпространств S_1 типов 1 и 2 и таких, что

$$S_1 = (\bigoplus \mathfrak{A}) \oplus T$$

дает ∇ -ортогональное разложение пространства S_1 . Очевидно, что все множества из $\mathcal{A}$ конечны. По лемме 4.7, примененной к пространству S_1 , множество $\mathcal{A}$ непусто. Для произвольного $\mathfrak{A} \in \mathcal{A}$ положим

$$G(\mathfrak{A}) = C_V^\nabla(\bigoplus \mathfrak{A}).$$

Тогда ввиду леммы 4.4

$$V = (\bigoplus \mathfrak{A}) \oplus G(\mathfrak{A}), \quad (26)$$

так как $\bigoplus \mathfrak{A}$ конечномерно и билинейная функция σ невырождена на $\bigoplus \mathfrak{A}$. Кроме того, используя равенство (26) и лемму 3.1, легко видеть, что

$$S_0 = C_{G(\mathfrak{A})}^\nabla(G(\mathfrak{A})) \quad \text{и} \quad T = S_1 \cap G(\mathfrak{A}) = C_{G(\mathfrak{A})}^\diamond(V) = C_{G(\mathfrak{A})}^\diamond(G(\mathfrak{A})) \quad (27)$$

для любого $\mathfrak{A} \in \mathcal{A}$.

Через $\mathcal{B}$ обозначим множество всех множеств $\mathfrak{B}$, состоящих из одномерных подпространств S_0 и таких, что $S_0 = \bigoplus \mathfrak{B}$. Если U — подпространство V , содержащее S_0 , то через $\mathfrak{R}(U)$ будет обозначаться множество всех прямых дополнений к S_0 в U . Отметим, что $\mathcal{B} \neq \emptyset$ и $\mathfrak{R}(U) \neq \emptyset$ для любого подпространства $U \subseteq V$, содержащего S_0 . Обозначим через $\mathcal{P}$ множество всех четверок вида $(\mathfrak{A}, \mathfrak{B}, R, \mathfrak{C})$, в которых $\mathfrak{A} \in \mathcal{A}$, $\mathfrak{B} \in \mathcal{B}$, $R \in \mathfrak{R}(G(\mathfrak{A}))$, а $\mathfrak{C}$ — такое множество подпространств $G(\mathfrak{A})/S_0$, что $G(\mathfrak{A})/S_0 = \bigoplus \mathfrak{C}$ является полным ∇ -ортогональным разложением пространства $G(\mathfrak{A})/S_0$.

Лемма 5.1. Пусть $V = \bigoplus \mathfrak{S}$ — полное ∇ -ортогональное разложение пространства V . Тогда существует единственное подмножество $\mathfrak{A} \subseteq \mathfrak{S}$, принадлежащее $\mathcal{A}$. Это подмножество $\mathfrak{A}$ определяется формулами

$$\mathfrak{A} = \{U \in \mathfrak{S} \mid C_U^\diamond(U) \not\subseteq C_U^\diamond(U)\} = \{U \in \mathfrak{S} \mid U \subseteq S_1, C_U^\nabla(U) = \{0\}\}$$

и удовлетворяет равенству $G(\mathfrak{A}) = \bigoplus (\mathfrak{S} \setminus \mathfrak{A})$.

Доказательство. Положим $\mathfrak{A} = \{U \in \mathfrak{S} \mid C_U^\diamond(U) \not\subseteq C_U^\diamond(U)\}$. Рассмотрим произвольное подпространство $U \in \mathfrak{A}$. Выберем подпространство $W \subseteq C_U^\diamond(U)$, имеющее тип 1 или 2 (это возможно по лемме 4.3). Тогда $U = W \oplus C_U^\nabla(W)$ согласно лемме 4.4. Ввиду ∇ -неразложимости U получаем, что $U = W = C_U^\diamond(U)$ и, следовательно, $U = S_1 \cap U \subseteq S_1$ (см. лемму 3.1) и $C_U^\nabla(U) = C_W^\nabla(W) = \{0\}$. Это показывает, что $\mathfrak{A}$ состоит из подпространств типов 1 и 2 и содержится в $\{U \in \mathfrak{S} \mid U \subseteq S_1, C_U^\nabla(U) = \{0\}\}$. Пусть теперь U — произвольный элемент последнего множества. Тогда $U = C_U^\diamond(U)$ (так как $U \subseteq S_1$) и $U \not\subseteq U$ (в противном случае $U = C_U^\nabla(U) = \{0\}$, а это несовместимо с вхождением U в $\mathfrak{S}$). Поэтому $U \in \mathfrak{A}$. Таким образом,

$$\mathfrak{A} = \{U \in \mathfrak{S} \mid U \subseteq S_1, C_U^\nabla(U) = \{0\}\}. \quad (28)$$

Из леммы 3.1 и доказанного выше равенства $C_U^\diamond(U) = U$ для любого $U \in \mathfrak{A}$ вытекает, что

$$S_1 = (\bigoplus \mathfrak{A}) \oplus T', \quad (29)$$

где

$$T' = \bigoplus \{C_U^\diamond(U) \mid U \in \mathfrak{S}, C_U^\diamond(U) \nabla C_U^\diamond(U)\}.$$

Применив к разложению (29) пространства S_1 лемму 3.1 и воспользовавшись равенством (28), получим равенство $T = T'$. Поэтому из равенства (29) следует, что $\mathfrak{A} \in \mathcal{A}$ (как мы уже видели выше, $\mathfrak{A}$ состоит из подпространств типов 1 и 2).

Пусть теперь подмножество $\mathfrak{A}' \subseteq \mathfrak{S}$ принадлежит $\mathcal{A}$. Тогда $\mathfrak{A}' \subseteq \mathfrak{A}$ ввиду равенства (28). Поэтому $\mathfrak{A}' = \mathfrak{A}$, так как $S_1 = (\bigoplus \mathfrak{A}') \oplus T = (\bigoplus \mathfrak{A}) \oplus T$. Равенство $G(\mathfrak{A}) = \bigoplus (\mathfrak{S} \setminus \mathfrak{A})$ непосредственно вытекает из леммы 4.4. ■

Теорема 5.1. Отображение

$$(\mathfrak{A}, \mathfrak{B}, R, \mathfrak{C}) \mapsto \mathfrak{A} \sqcup \mathfrak{B} \sqcup \nu_{R, S_0}^{-1}(\mathfrak{C}), \quad (\mathfrak{A}, \mathfrak{B}, R, \mathfrak{C}) \in \mathcal{P}, \quad (30)$$

является биекцией $\mathcal{P}$ на множество всех $\mathfrak{S}$, таких, что $V = \bigoplus \mathfrak{S}$ — полное ∇ -ортогональное разложение пространства V . Если $\mathfrak{S}$ — образ четверки $(\mathfrak{A}, \mathfrak{B}, R, \mathfrak{C}) \in \mathcal{P}$ при отображении (30), то эти $\mathfrak{A}$, $\mathfrak{B}$, R и $\mathfrak{C}$ могут быть найдены по $\mathfrak{S}$ следующим образом:

$$\begin{aligned} \mathfrak{A} &= \{U \in \mathfrak{S} \mid C_U^\diamond(U) \not\subseteq C_U^\nabla(U)\} = \{U \in \mathfrak{S} \mid U \subseteq S_1, C_U^\nabla(U) = \{0\}\}; \\ \mathfrak{B} &= \{U \in \mathfrak{S} \mid U \cap S_0 \neq \{0\}\} = \{U \in \mathfrak{S} \mid C_U^\nabla(U) \neq \{0\}\} = \{U \in \mathfrak{S} \mid U \subseteq S_0\}; \\ R &= \bigoplus (\mathfrak{S} \setminus (\mathfrak{A} \sqcup \mathfrak{B})) = \bigoplus \{U \in \mathfrak{S} \mid C_U^\diamond(U) \supsetneq C_U^\nabla(U), C_U^\nabla(U) = \{0\}\}; \\ \mathfrak{C} &= \nu_{R, S_0}(\mathfrak{S} \setminus (\mathfrak{A} \sqcup \mathfrak{B})). \end{aligned}$$

Доказательство. Из равенства (26) и лемм 4.2 и 3.2 следует, что если $\mathfrak{S}$ — образ произвольной четверки $(\mathfrak{A}, \mathfrak{B}, R, \mathfrak{C}) \in \mathcal{P}$ при отображении (30), то $V = \bigoplus \mathfrak{S}$ является полным ∇ -ортогональным разложением пространства V . Пусть теперь $V = \bigoplus \mathfrak{S}$ — полное ∇ -ортогональное разложение пространства V . Обозначим через $\mathfrak{A}$ подмножество $\mathfrak{S}$, принадлежащее $\mathcal{A}$; согласно лемме 5.1, такое подмножество существует, единственно и определяется формулами, указанными в формулировке теоремы. Кроме того, $G(\mathfrak{A}) = \bigoplus (\mathfrak{S} \setminus \mathfrak{A})$ по той же лемме 5.1; очевидно, что это равенство дает полное ∇ -ортогональное разложение пространства $G(\mathfrak{A})$. Ввиду леммы 3.2 (примененной к пространству $G(\mathfrak{A})$) и равенства для S_0 в (27) множество $\mathfrak{B}$, пространство R и множество $\mathfrak{C}$, такие, что

$$(\mathfrak{A}, \mathfrak{B}, R, \mathfrak{C}) \in \mathcal{P} \quad \& \quad \mathfrak{S} = \mathfrak{A} \sqcup \mathfrak{B} \sqcup \nu_{R, S_0}^{-1}(\mathfrak{C}), \quad (31)$$

существуют, единственны и определяются формулами, указанными в формулировке теоремы. Здесь мы воспользовались тем, что условие (31) выполняется тогда и только тогда, когда $\mathfrak{B} \in \mathcal{B}$, $R \in \mathcal{R}(G(\mathfrak{A}))$, $G(\mathfrak{A})/S_0 = \bigoplus \mathfrak{C}$ — полное ∇ -ортогональное разложение пространства $G(\mathfrak{A})/S_0$ и $\mathfrak{S} \setminus \mathfrak{A} = \mathfrak{B} \sqcup \nu_{R, S_0}^{-1}(\mathfrak{C})$. Таким образом, $\mathfrak{S}$ имеет единственный прообраз при отображении (30), причем компоненты этого прообраза могут быть найдены по формулам, указанным в формулировке теоремы. ■

5.2. Полные ∇ -ортогональные разложения пространства $G(\mathfrak{A})/S_0$ для $\mathfrak{A} \in \mathcal{A}$

Предположим, что пространство V/T конечномерно. Согласно замечанию 4.1, это предположение эквивалентно предположению о конечномерности пространства V/S_0 . При указанном предположении пространство S_1/T также конечномерно, поэтому здесь применимы результаты п. 5.1.

Фиксируем произвольное множество $\mathfrak{A} \in \mathcal{A}$ и полагаем $G = G(\mathfrak{A}) = C_V^\nabla(\bigoplus \mathfrak{A})$ (см. п. 5.1). Многие объекты, определяемые и рассматриваемые в данном пункте, зависят от G . Однако здесь не будем явно указывать на их связь с подпространством G , так как последнее фиксировано. Некоторые из этих объектов понадобятся и далее, где будем указывать соответствующее подпространство G после объекта в круглых скобках (например, $\mathcal{K}(G)$).

Очевидно, что $S_0 \subseteq T \subseteq G$. Из (27) и (6) вытекает, что

$$C_{G/S_0}^\nabla(G/S_0) = \{0\} \quad \text{и} \quad C_{G/T}^\diamond(G/T) = \{0\}. \quad (32)$$

Поэтому все ∇ -ортогональные разложения пространства G/S_0 и $\diamond$ -ортогональные разложения пространства G/T являются прямыми ввиду замечания 3.3. Кроме того,

$$T/S_0 \nabla T/S_0, \quad (33)$$

так как $T \nabla T$.

Замечание 5.1. Из равенства $T = S_1 \cap G$ (см. (27)) следует, что отображение $g + T \mapsto g + S_1$, где $g \in G$, является изоморфизмом G/T на $(G + S_1)/S_1 = V/S_1$ (равенство $G + S_1 = V$ вытекает из (26)). Более того, ввиду эквивалентности (4) это отображение представляет собой изоморфизм $(G/T; \diamond)$ на $(V/S_1; \diamond)$. Таким образом, $(G/T; \diamond) \cong (V/S_1; \diamond)$. Это вместе с замечанием 3.6 показывает, что пространство с ортогональностью $(G/T; \diamond)$ удовлетворяет условию (13).

Опишем все полные ∇ -ортогональные разложения пространства G/S_0 .

Множества I и $\mathfrak{J}$

Пусть I — множество всех ненулевых $\diamond$ -неразложимых элементов пространства G/T . Это значит, что I — множество всех $a \in (G/T) \setminus \{0\}$, которые не могут быть представлены в виде $a_1 + a_2$, где $a_i \in G/T$ и $\mathbb{C}_{G/T}^\diamond(a_i) \supset \mathbb{C}_{G/T}^\diamond(a)$ при $i = 1, 2$ (см. п. 3.3, а также [1, § 3]). По лемме 2.1 (см. также лемму 5 из [1]) множество I порождает пространство G/T . Здесь в качестве ω из леммы 2.1 используется отображение $a \mapsto \mathbb{C}_{G/T}^\diamond(a)$ (где $a \in G/T$) пространства G/T в частично упорядоченное множество всех подпространств конечномерного пространства G/T относительно отношения включения.

Из леммы 3.4, которая применима здесь ввиду замечания 5.1 и второго из равенств (32), непосредственно вытекает

Следствие 5.1. Пусть $G/T = \bigoplus_{m \in M} W_m$ — $\diamond$ -ортогональное разложение пространства G/T . Тогда $I = \bigsqcup_{m \in M} (I \cap W_m)$.

Через $\mathfrak{J}$ будет обозначаться множество всех связных компонент графа с множеством вершин I , в котором две различные вершины a и b смежны тогда и только тогда, когда a и b не $\diamond$ -ортогональны. Лемма 3.5, которая применима здесь ввиду замечания 5.1 и второго из равенств (32), приводит к следующему выводу:

Следствие 5.2. Имеет место равенство $G/T = \bigoplus_{X \in \mathfrak{J}} \langle X \rangle$, которое дает единственное полное $\diamond$ -ортогональное разложение пространства G/T .

Из равенства следствия 5.2 вытекает неравенство

$$|\mathfrak{J}| \leq \dim(G/T). \quad (34)$$

В частности, множество $\mathfrak{J}$ конечно.

Множества $\Xi_X(a)$

Для $a \in T/S_0$ и $X \subseteq I$ положим

$$\Xi_X(a) = \{x \in X \mid a \not\in \rho^{-1}(x)\} = \{x \in X \mid \forall b \in \rho^{-1}(x) \ a \not\in b\}.$$

Совпадение двух последних множеств следует из (33).

Лемма 5.2. Пусть $G/S_0 = \bigoplus_{m \in M} U_m$ — ∇ -ортогональное разложение пространства G/S_0 . Пусть также $u = \sum_{m \in M} u_m$, где $u_m \in (T/S_0) \cap U_m$ при всех $m \in M$, причем $\{m \in M \mid u_m \neq 0\}$ конечно. Тогда

$$\langle \Xi_I(u) \rangle = \bigoplus_{m \in M} \langle \Xi_{I \cap \rho(U_m)}(u) \rangle, \quad (35)$$

причем $\Xi_{I \cap \rho(U_m)}(u) = \Xi_{I \cap \rho(U_m)}(u_m) = \Xi_I(u_m)$ для любого $m \in M$.

Доказательство. Согласно следствию 5.1, примененному к разложению $G/T = \bigoplus_{m \in M} \rho(U_m)$ (которое является $\diamond$ -ортогональным ввиду эквивалентности (18)),

$$I = \bigsqcup_{m \in M} (I \cap \rho(U_m)). \quad (36)$$

Поэтому $\Xi_I(u) = \bigsqcup_{m \in M} \Xi_{I \cap \rho(U_m)}(u)$, откуда непосредственно вытекает требуемое равенство (35), так как сумма подпространств $\rho(U_m)$ по всем $m \in M$ прямая. Последнее утверждение следует из того, что разложение $G/T = \sum_{m \in M} \rho(U_m)$ $\diamond$ -ортогонально (ввиду эквивалентности (18)).

Пусть теперь $m \in M$. Легко видеть, что если $a \in U_m$, то $u \nabla a$ тогда и только тогда, когда $u_m \nabla a$. Поэтому $\Xi_{I \cap \rho(U_m)}(u) = \Xi_{I \cap \rho(U_m)}(u_m)$. Равенство $\Xi_{I \cap \rho(U_m)}(u_m) = \Xi_I(u_m)$ вытекает из включения $\Xi_I(u_m) \subseteq I \cap \rho(U_m)$, которое, в свою очередь, следует из (36) и ∇ -ортогональности разложения $G/S_0 = \bigoplus_{m \in M} U_m$. ■

Лемма 5.3. Пусть $u \in T/S_0$. Тогда

$$\Xi_I(u) = \emptyset \iff u = 0.$$

Доказательство. Равенство $\Xi_I(0) = \emptyset$ очевидно. Предположим теперь, что $\Xi_I(u) = \emptyset$. Тогда $u \nabla \rho^{-1}(I)$. Кроме того, $u \nabla T/S_0$ ввиду (33). Из равенств (19) и $\langle I \rangle = G/T$ вытекает, что $\langle \rho^{-1}(I) \rangle + (T/S_0) = G/S_0$. Поэтому $u \nabla G/S_0$ и, следовательно, $u = 0$ ввиду первого из равенств (32). ■

Множество J

Обозначим через J множество всех $a \in (T/S_0) \setminus \{0\}$, которые не могут быть представлены в виде $a_1 + a_2$, где $a_i \in T/S_0$ и $\langle \Xi_I(a_i) \rangle \subset \langle \Xi_I(a) \rangle$ при $i = 1, 2$. Ввиду леммы 2.1 множество J порождает пространство T/S_0 . Здесь в качестве ω из леммы 2.1 используется отображение $a \mapsto \langle \Xi_I(a) \rangle$ (где $a \in T/S_0$) пространства T/S_0 в частично упорядоченное множество, двойственное частично упорядоченному множеству всех подпространств конечномерного пространства G/T относительно отношения включения.

Лемма 5.4. Пусть $G/S_0 = \bigoplus_{m \in M} U_m$ — ∇ -ортогональное разложение пространства G/S_0 . Тогда $J \subseteq \bigcup_{m \in M} U_m$ или, что эквивалентно, $J = \bigsqcup_{m \in M} (J \cap U_m)$.

Доказательство. Пусть $a \in J$. Представим a в виде $\sum_{m \in M} a_m$, где $a_m \in (T/S_0) \cap U_m = \mathcal{C}_{U_m}^\diamond(G/S_0)$ при всех $m \in M$, причем $\{m \in M \mid a_m \neq 0\}$ конечно. Такое представление существует согласно лемме 3.1, так как $T/S_0 = \mathcal{C}_{G/S_0}^\diamond(G/S_0)$ ввиду равенств $T = \mathcal{C}_G^\diamond(G)$ (см. (27)) и (5). Выберем индекс $k \in M$, для которого $a_k \neq 0$

(это возможно, так как $a \neq 0$), и положим $b = a - a_k = \sum_{m \in M \setminus \{k\}} a_m$. Из леммы 5.2 (примененной к разложению $G/S_0 = U_k \oplus W$, где $W = \bigoplus_{m \in M \setminus \{k\}} U_m$) следует, что $\langle \Xi_I(a) \rangle = \langle \Xi_I(a_k) \rangle \oplus \langle \Xi_I(b) \rangle$. Кроме того, $\langle \Xi_I(a_k) \rangle \neq \{0\}$, так как $\Xi_I(a_k) \neq \emptyset$ (по лемме 5.3) и $\Xi_I(a_k) \subseteq I \subseteq (G/T) \setminus \{0\}$. Если $b \neq 0$, то аналогично показывается, что $\langle \Xi_I(b) \rangle \neq \{0\}$. Но тогда получаем противоречие с тем, что $a \in J$. Отсюда следует, что $b = 0$ и $a = a_k \in U_k \subseteq \bigcup_{m \in M} U_m$. ■

Граф Γ , множества $\mathcal{I}$ и $\mathfrak{K}$ и подпространства H_X

Обозначим через Γ граф с множеством вершин $\mathcal{J}$, в котором две различные вершины X и Y смежны тогда и только тогда, когда существует $a \in J$, такой, что $\Xi_X(a) \neq \emptyset$ и $\Xi_Y(a) \neq \emptyset$ (очевидно, что это отношение смежности симметрично). Пусть $\mathcal{I}$ — множество всех связных компонент графа Γ , а

$$\mathfrak{K} = \{\bigsqcup \mathcal{X} \mid \mathcal{X} \in \mathcal{I}\}.$$

Из неравенства (34) следует, что $|\mathfrak{K}| = |\mathcal{I}| \leq |\mathcal{J}| \leq \dim(G/T)$. Отметим, что все множества из $\mathfrak{K}$ непусты.

Замечание 5.2. Из следствия 5.2 вытекает, что $G/T = \bigoplus_{X \in \mathfrak{K}} \langle X \rangle$ — $\diamond$ -ортогональное разложение пространства G/T . Кроме того, это разложение нетривиально, так как $X \neq \emptyset$ и $X \subseteq I \subseteq (G/T) \setminus \{0\}$ при любом $X \in \mathfrak{K}$.

Для каждого $X \in \mathfrak{K}$ положим

$$H_X = C_{T/S_0}^\nabla(\rho^{-1}(\langle I \setminus X \rangle)) = C_{T/S_0}^\nabla(\rho^{-1}(I \setminus X)).$$

Совпадение двух последних множеств следует из (19), (33) и того, что $C_{T/S_0}^\nabla(\langle Y \rangle) = C_{T/S_0}^\nabla(Y)$ для произвольного подмножества $Y \subseteq V/S_0$. Легко также видеть, что

$$H_X = \{a \in T/S_0 \mid \Xi_I(a) \subseteq X\} \quad (37)$$

для любого $X \in \mathfrak{K}$.

Пусть a — произвольный элемент J . Тогда ввиду определения $\mathfrak{K}$ множество $\mathfrak{L} = \{X \in \mathfrak{K} \mid \Xi_X(a) \neq \emptyset\}$ не может содержать более одного элемента. С другой стороны, $\Xi_I(a) = \bigsqcup_{X \in \mathfrak{K}} \Xi_X(a)$ (так как $I = \bigsqcup \mathfrak{K}$), причем $\Xi_I(a) \neq \emptyset$ по лемме 5.3. Это показывает, что $\mathfrak{L} \neq \emptyset$ и, следовательно, $|\mathfrak{L}| = 1$. Поэтому

$$J = \bigsqcup_{X \in \mathfrak{K}} (J \cap H_X) \quad (38)$$

ввиду равенства (37) и леммы 5.3.

Лемма 5.5. Имеет место равенство

$$T/S_0 = \bigoplus_{X \in \mathfrak{K}} H_X,$$

причем $H_X = \langle J \cap H_X \rangle$ для всех $X \in \mathfrak{K}$.

Доказательство. Выше было отмечено, что $T/S_0 = \langle J \rangle$. Поэтому $T/S_0 = \sum_{X \in \mathfrak{K}} \langle J \cap H_X \rangle$ ввиду равенства (38). Предположим теперь, что $a \in H_Y \cap \sum_{X \in \mathfrak{K} \setminus \{Y\}} H_X$ для некоторого $Y \in \mathfrak{K}$. Тогда $\Xi_I(a) \subseteq Y$ согласно равенству (37). С другой стороны, $a \nabla \rho^{-1}(Y)$, так как $Y \subseteq I \setminus X$ для всех $X \in \mathfrak{K} \setminus \{Y\}$. Поэтому $\Xi_I(a) \subseteq I \setminus Y$. Следовательно, $\Xi_I(a) = \emptyset$ и $a = 0$ по лемме 5.3. Это показывает, что сумма подпространств H_X по всем $X \in \mathfrak{K}$ прямая. Таким образом,

$$T/S_0 = \bigoplus_{X \in \mathfrak{K}} \langle J \cap H_X \rangle = \bigoplus_{X \in \mathfrak{K}} H_X. \quad (39)$$

Равенство $H_X = \langle J \cap H_X \rangle$ для любого $X \in \mathfrak{K}$ легко вытекает из (39) и включения $\langle J \cap H_X \rangle \subseteq H_X$. ■

Согласно лемме 5.5, всякий элемент $u \in T/S_0$ единственным образом представляется в виде $\sum_{X \in \mathfrak{K}} u_X$, где $u_X \in H_X$; этот элемент u_X будем называть X -координатой элемента u ($X \in \mathfrak{K}$). Указанная сумма определена, так как множество $\mathfrak{K}$ конечно (см. начало п. 5.2).

Лемма 5.6. Пусть $a \in \rho^{-1}(\langle X \rangle)$ и $b \in \rho^{-1}(\langle Y \rangle)$, где $X, Y \in \mathfrak{K}$, $X \neq Y$. Пусть также $u, w \in T/S_0$. Тогда $a + u \nabla b + w$, если и только если $\sigma(a, w_X) + \sigma(b, u_Y) = -\sigma(a, b)$, где w_X — X -координата элемента w , а u_Y — Y -координата элемента u .

Доказательство. Из эквивалентности (18) вытекает, что $a \diamond b$, так как $\rho(a) \diamond \rho(b)$. Поэтому

$$a + u \nabla b + w \iff 0 = \sigma(a + u, b + w) = \sigma(a, b) + \sigma(a, w) + \sigma(b, u) + \sigma(u, w). \quad (40)$$

Для любого $Z \in \mathfrak{K} \setminus \{X\}$ из определения H_Z следует, что $\rho^{-1}(\langle X \rangle) \nabla H_Z$. Поэтому

$$\sigma(a, w) = \sigma(a, w_X) \quad (41)$$

ввиду леммы 5.5. Аналогично,

$$\sigma(b, u) = \sigma(b, u_Y). \quad (42)$$

Кроме того, из (33) вытекает равенство

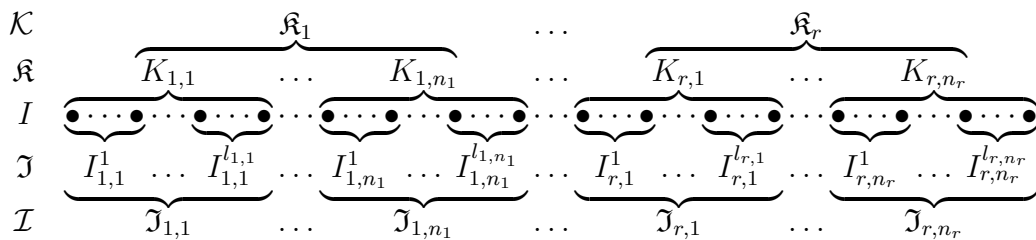
$$\sigma(u, w) = 0. \quad (43)$$

Утверждение леммы следует теперь из эквивалентности (40) и равенств (41)–(43). ■

Граф Δ , множество $\mathcal{K}$ и схема взаимных связей множеств I , $\mathfrak{I}$, $\mathcal{I}$, $\mathfrak{K}$ и $\mathcal{K}$

Обозначим через Δ граф с множеством вершин $\mathfrak{K}$, в котором две различные вершины X и Y смежны тогда и только тогда, когда не существует прямого дополнения Q_X к T/S_0 в $\rho^{-1}(\langle X \rangle)$ и прямого дополнения Q_Y к T/S_0 в $\rho^{-1}(\langle Y \rangle)$, таких, что $Q_X \nabla Q_Y$ (очевидно, что это отношение смежности симметрично). Пусть также $\mathcal{K}$ — множество всех связных компонент графа Δ . Из неравенства (34) следует, что $|\mathcal{K}| \leq |\mathfrak{K}| = |\mathcal{I}| \leq |\mathfrak{I}| \leq \dim(G/T)$.

Взаимные связи множеств I , $\mathfrak{I}$, $\mathcal{I}$, $\mathfrak{K}$ и $\mathcal{K}$ могут быть изображены с помощью следующей схемы:



На этой схеме черные кружки обозначают элементы множества I . Кроме того,

$$\begin{aligned}\mathcal{I} &= \{I_{m,n}^l \mid m \in \{1, \dots, r\}, n \in \{1, \dots, n_m\}, l \in \{1, \dots, l_{m,n}\}\}, \\ \mathcal{I}_{m,n} &= \{I_{m,n}^1, \dots, I_{m,n}^{l_{m,n}}\}, \quad \mathcal{I} = \{\mathcal{I}_{m,n} \mid m \in \{1, \dots, r\}, n \in \{1, \dots, n_m\}\}, \\ K_{m,n} &= \bigsqcup \mathcal{I}_{m,n}, \quad \mathcal{K} = \{K_{m,n} \mid m \in \{1, \dots, r\}, n \in \{1, \dots, n_m\}\}, \\ \mathcal{K}_m &= \{K_{m,1}, \dots, K_{m,n_m}\}, \quad \mathcal{K} = \{\mathcal{K}_1, \dots, \mathcal{K}_r\}.\end{aligned}$$

Критерий смежности вершин в графе Δ

Пусть X — произвольное множество из $\mathfrak{K}$. Выберем и зафиксируем некоторое линейно независимое множество D_X , такое, что $\langle D_X \rangle$ — прямое дополнение к T/S_0 в $\rho^{-1}(\langle X \rangle)$. Тогда из замечания 4.2 вытекает, что $|D_X| = \dim \langle X \rangle$ и, следовательно, множество D_X конечно. Легко также видеть, что $D_X \cap D_Y = \emptyset$ для любых различных $X, Y \in \mathfrak{K}$.

Лемма 5.7. Пусть $X, Y \in \mathfrak{K}$, $X \neq Y$. Тогда X и Y смежны в графе Δ , если и только если система уравнений

$$\sigma(a, u_{b,X}) + \sigma(b, u_{a,Y}) = -\sigma(a, b), \quad a \in D_X, b \in D_Y, \quad (44)$$

неразрешима относительно $u_{a,Y} \in H_Y$ ($a \in D_X$) и $u_{b,X} \in H_X$ ($b \in D_Y$).

Доказательство. Предположим сначала, что X и Y не смежны в графе Δ . Пусть Q_X и Q_Y — прямые дополнения к T/S_0 в $\rho^{-1}(\langle X \rangle)$ и $\rho^{-1}(\langle Y \rangle)$ соответственно, удовлетворяющие условию $Q_X \nabla Q_Y$. Для каждого $a \in D_X$ выберем $u_a \in T/S_0$, такой, что $a + u_a \in Q_X$. Аналогично, пусть для всякого $b \in D_Y$ элемент $u_b \in T/S_0$ удовлетворяет условию $b + u_b \in Q_Y$. Тогда $a + u_a \nabla b + u_b$. Из последнего условия и леммы 5.6 следует, что $\sigma(a, u_{b,X}) + \sigma(b, u_{a,Y}) = -\sigma(a, b)$ для любых $a \in D_X$ и $b \in D_Y$, где $u_{a,Y}$ — Y -координата элемента u_a , а $u_{b,X}$ — X -координата элемента u_b . Таким образом, система (44) разрешима.

Пусть теперь система (44) разрешима и $(u_{a,Y}, u_{b,X} \mid a \in D_X, b \in D_Y)$ — некоторое ее решение. Положим $Q_X = \langle a + u_{a,Y} \mid a \in D_X \rangle$ и $Q_Y = \langle b + u_{b,X} \mid b \in D_Y \rangle$. Тогда очевидно, что $\rho^{-1}(\langle X \rangle) = Q_X \oplus (T/S_0)$ и $\rho^{-1}(\langle Y \rangle) = Q_Y \oplus (T/S_0)$. Кроме того, ввиду леммы 5.6 $a + u_{a,Y} \nabla b + u_{b,X}$ для всех $a \in D_X$ и $b \in D_Y$. Поэтому $Q_X \nabla Q_Y$. Таким образом, X и Y не смежны в графе Δ . ■

Замечание 5.3. Пусть X и Y — различные множества из $\mathfrak{K}$, а Z_X и Z_Y — некоторые базисы пространств H_X и H_Y соответственно (ввиду замечания 4.1 Z_X и Z_Y конечны). Тогда очевидно, что $(u_{a,Y}, u_{b,X} \mid a \in D_X, b \in D_Y)$ — решение системы (44), если и только если координаты элементов $u_{a,Y}$ в базисе Z_Y и элементов $u_{b,X}$ в базисе Z_X образуют решение системы уравнений

$$\sum_{z_X \in Z_X} \sigma(a, z_X) u_{b,X,z_X} + \sum_{z_Y \in Z_Y} \sigma(b, z_Y) u_{a,Y,z_Y} = -\sigma(a, b), \quad a \in D_X, b \in D_Y, \quad (45)$$

относительно $u_{a,Y,z_Y}, u_{b,X,z_X} \in F$ ($a \in D_X, b \in D_Y, z_X \in Z_X, z_Y \in Z_Y$), где u_{a,Y,z_Y} — координата $u_{a,Y}$ при z_Y , а u_{b,X,z_X} — координата $u_{b,X}$ при z_X . Таким образом, нахождение решений системы (44) эквивалентно нахождению решений конечной системы (45) линейных уравнений над полем F , которая состоит из

$$|D_X| |D_Y| = \dim \langle X \rangle \dim \langle Y \rangle$$

уравнений и содержит

$$|D_X||Z_Y| + |D_Y||Z_X| = \dim\langle X \rangle \dim H_Y + \dim\langle Y \rangle \dim H_X$$

переменных, принимающих значения в F (здесь использовано то, что $|D_X| = \dim\langle X \rangle$ и $|D_Y| = \dim\langle Y \rangle$ ввиду замечания 4.2).

Множество $\mathcal{Q}$

Обозначим через $\mathcal{Q}$ множество всех семейств $(Q_X \mid X \in \mathfrak{K})$, удовлетворяющих следующим условиям:

- 1) для любого $X \in \mathfrak{K}$ семейство Q_X является прямым дополнением к T/S_0 в $\rho^{-1}(\langle X \rangle)$;
- 2) если $X, Y \in \mathfrak{K}$, причем X и Y принадлежат различным связным компонентам графа Δ , то $Q_X \nabla Q_Y$.

Из утверждения 2 следующей леммы, в частности, вытекает, что $\mathcal{Q} \neq \emptyset$.

Лемма 5.8. Для каждого двухэлементного подмножества $\{X, Y\} \subseteq \mathfrak{K}$, в котором X и Y принадлежат различным связным компонентам графа Δ , выберем некоторое решение $(u_{a,Y}, u_{b,X} \mid a \in D_X, b \in D_Y)$ системы уравнений (44) (такое решение существует ввиду леммы 5.7, так как X и Y не смежны в графе Δ). Выберем также произвольный элемент $u_{a,Y} \in H_Y$ для всех $a \in D_X$ ($X \in \mathfrak{K}$) и $Y \in \mathfrak{K}$, таких, что X и Y принадлежат одной связной компоненте графа Δ . Для каждого $X \in \mathfrak{K}$ положим

$$E_X = \left\{ a + \sum_{Y \in \mathfrak{K}} u_{a,Y} \mid a \in D_X \right\}.$$

Тогда

- 1) при любом $X \in \mathfrak{K}$ множество E_X линейно независимо;
- 2) семейство $(\langle E_X \rangle \mid X \in \mathfrak{K})$ принадлежит $\mathcal{Q}$.

Доказательство. Утверждение 1 очевидно. Ясно также, что $\rho^{-1}(\langle X \rangle) = \langle E_X \rangle \oplus (T/S_0)$ для любого $X \in \mathfrak{K}$. Пусть теперь $X, Y \in \mathfrak{K}$, причем X и Y принадлежат различным связным компонентам графа Δ . Тогда из леммы 5.6 непосредственно вытекает, что $E_X \nabla E_Y$ и, следовательно, $\langle E_X \rangle \nabla \langle E_Y \rangle$. Таким образом, утверждение 2 доказано. ■

Замечание 5.4. Пусть $(Q_X \mid X \in \mathfrak{K}) \in \mathcal{Q}$. Пусть также X — произвольное множество из $\mathfrak{K}$. Для каждого $a \in D_X$ выберем элемент $u_a \in T/S_0$, такой, что $a + u_a \in Q_X$. Положим $E_X = \{a + u_a \mid a \in D_X\}$. Очевидно, что множество E_X линейно независимо и, следовательно, $\dim\langle E_X \rangle = |D_X| = \dim\langle D_X \rangle = \dim\langle X \rangle = \dim Q_X$ (см. замечание 4.2), причем размерности в этих равенствах конечны. Поэтому из очевидного включения $\langle E_X \rangle \subseteq Q_X$ вытекает равенство $\langle E_X \rangle = Q_X$.

Для произвольных $a \in \bigsqcup_{X \in \mathfrak{K}} D_X$ и $Y \in \mathfrak{K}$ обозначим через $u_{a,Y}$ Y -координату элемента u_a . Предположим, что X и Y (где $X, Y \in \mathfrak{K}$) принадлежат различным связным компонентам графа Δ . Тогда $Q_X \nabla Q_Y$ и, следовательно, $E_X \nabla E_Y$. Поэтому из леммы 5.6 вытекает, что $(u_{a,Y}, u_{b,X} \mid a \in D_X, b \in D_Y)$ является решением системы уравнений (44). Таким образом, конструкция, описанная в лемме 5.8, позволяет построить все семейства из $\mathcal{Q}$.

Множества $\mathcal{K}_U$

Пусть U — произвольное подпространство G/S_0 , входящее в некоторое ∇ -ортогональное разложение $G/S_0 = U \oplus W$ пространства G/S_0 . Ввиду замечания 3.2 (которое применимо здесь согласно первому из равенств (32)) для произвольного такого

разложения W совпадает с $\mathbb{C}_V^\perp(U)$. Следовательно, это ∇ -ортогональное разложение при фиксированном U единственно. Обозначения U и W будут иметь вышеуказанный смысл в пределах всего п. 5.2.

Применив к разложению $G/S_0 = U \oplus W$ гомоморфизм ρ , получим разложение $G/T = \rho(U) \oplus \rho(W)$ пространства G/T , которое является $\diamond$ -ортогональным (и, следовательно, прямым) ввиду эквивалентности (18). Поставим в соответствие подпространству U подмножество $\mathcal{K}_U \subseteq \mathcal{K}$, такое, что

$$\rho(U) = \bigoplus_{X \in \mathcal{K}_U} \langle X \rangle. \quad (46)$$

Корректность этого определения непосредственно вытекает из следующей леммы.

Лемма 5.9. Подмножество $\mathcal{K}_U \subseteq \mathcal{K}$, удовлетворяющее равенству (46), существует и единственно (при фиксированном U).

Доказательство. Из следствия 5.2 вытекает, что $\rho(U) = \bigoplus_{X \in \mathcal{J}_U} \langle X \rangle$ и $\rho(W) = \bigoplus_{Y \in \mathcal{J} \setminus \mathcal{J}_U} \langle Y \rangle$, где $\mathcal{J}_U$ — некоторое однозначно определенное подмножество $\mathcal{J}$. Предположим, что некоторые $X \in \mathcal{J}_U$ и $Y \in \mathcal{J} \setminus \mathcal{J}_U$ смежны в графе Γ . Тогда существуют $u \in U$, $w \in W$ и $z \in J$, такие, что $u \not\perp z$ и $w \not\perp z$. С другой стороны, $z \in U$ или $z \in W$ ввиду леммы 5.4. Но тогда соответственно $w \nabla z$ или $u \nabla z$. Полученное противоречие показывает, что $\mathcal{J}_U = \bigsqcup \mathcal{I}_U$, где $\mathcal{I}_U$ — некоторое однозначно определенное подмножество $\mathcal{I}$.

Положим $\mathfrak{K}_U = \{\bigsqcup \mathfrak{X} \mid \mathfrak{X} \in \mathcal{I}_U\}$. Тогда легко видеть, что $\rho(U) = \bigoplus_{X \in \mathfrak{K}_U} \langle X \rangle$ и $\rho(W) = \bigoplus_{Y \in \mathfrak{K} \setminus \mathfrak{K}_U} \langle Y \rangle$, так как $\mathcal{J} \setminus \mathcal{J}_U = \bigsqcup (\mathcal{I} \setminus \mathcal{I}_U)$ и $\mathfrak{K} \setminus \mathfrak{K}_U = \{\bigsqcup \mathfrak{Y} \mid \mathfrak{Y} \in \mathcal{I} \setminus \mathcal{I}_U\}$. Предположим, что некоторые $X \in \mathfrak{K}_U$ и $Y \in \mathfrak{K} \setminus \mathfrak{K}_U$ смежны в графе Δ . Тогда легко видеть, что $\rho^{-1}(\langle X \rangle) \subseteq U + (T/S_0)$, поэтому $\rho^{-1}(\langle X \rangle) = Q_X \oplus (T/S_0)$ для некоторого подпространства $Q_X \subseteq U$. Аналогично, $\rho^{-1}(\langle Y \rangle) \subseteq W + (T/S_0)$ и $\rho^{-1}(\langle Y \rangle) = Q_Y \oplus (T/S_0)$ для некоторого подпространства $Q_Y \subseteq W$. Кроме того, такие подпространства Q_X и Q_Y ∇ -ортогональны ввиду ∇ -ортогональности U и W . Но это означает, что X и Y не смежны в графе Δ . Полученное противоречие показывает, что $\mathfrak{K}_U = \bigsqcup \mathcal{K}_U$, где $\mathcal{K}_U$ — некоторое однозначно определенное подмножество $\mathcal{K}$. Таким образом, существование требуемого множества $\mathcal{K}_U$ доказано, а единственность этого множества следует из замечания 5.2. ■

Замечание 5.5. Очевидно, что $\mathcal{K}_{G/S_0} = \mathcal{K}$. Непосредственно проверяется также, что если $U = \bigoplus_{m \in M} U_m$ — ∇ -ортогональное разложение пространства U , то $\mathcal{K}_U = \bigsqcup_{m \in M} \mathcal{K}_{U_m}$.

Из определения множества $\mathcal{K}_U$ вытекает, что $\rho(U) = \langle \bigsqcup \mathcal{K}_U \rangle$. Следовательно, $\bigsqcup \mathcal{K}_U \subseteq I \cap \rho(U)$. Аналогично, $\bigsqcup \mathcal{K}_W \subseteq I \cap \rho(W)$. Кроме того, $(\bigsqcup \mathcal{K}_U) \sqcup (\bigsqcup \mathcal{K}_W) = I$ (так как $\mathcal{K}_U \sqcup \mathcal{K}_W = \mathcal{K}$ ввиду замечания 5.5) и $(I \cap \rho(U)) \sqcup (I \cap \rho(W)) = I$ (согласно следствию 5.1). Поэтому

$$I \cap \rho(U) = \bigsqcup \mathcal{K}_U. \quad (47)$$

Кроме того, легко видеть, что произвольное подмножество $\mathcal{L} \subseteq \mathcal{K}$ определяется по $\bigsqcup \mathcal{L}$ однозначно (так как $\mathfrak{K}$ состоит из непустых попарно не пересекающихся множеств). Это показывает, что $\mathcal{K}_U$ эквивалентным образом можно определить как подмножество $\mathcal{K}$, удовлетворяющее равенству (47).

Лемма 5.10. Имеет место равенство

$$(T/S_0) \cap U = \bigoplus_{X \in \sqcup \mathcal{K}_U} H_X. \quad (48)$$

Доказательство. Пусть X — произвольное множество из $\sqcup \mathcal{K}_U$. Предположим, что существует $a \in J \cap H_X \cap W$. Тогда, с одной стороны, $\Xi_I(a) \subseteq X$ (см. равенство (37)). С другой стороны, очевидно, что $\rho^{-1}(X) \subseteq U + (T/S_0)$. Кроме того, $a \nabla U$ (так как $W \nabla U$) и $a \nabla T/S_0$ (ввиду (33)). Поэтому $a \nabla \rho^{-1}(X)$ и $\Xi_I(a) \subseteq I \setminus X$. Но тогда $\Xi_I(a) = \emptyset$ и, следовательно, $a = 0$ (см. лемму 5.3), что противоречит принадлежности a множеству J . Полученное противоречие вместе с равенством

$$J = (J \cap U) \sqcup (J \cap W), \quad (49)$$

имеющим место ввиду леммы 5.4, показывают, что

$$\bigsqcup_{X \in \sqcup \mathcal{K}_U} (J \cap H_X) \subseteq J \cap U. \quad (50)$$

Аналогично,

$$\bigsqcup_{Y \in \sqcup \mathcal{K}_W} (J \cap H_Y) \subseteq J \cap W. \quad (51)$$

Из (38) и (49)–(51) вытекает равенство

$$J \cap U = \bigsqcup_{X \in \sqcup \mathcal{K}_U} (J \cap H_X),$$

так как $\mathcal{K}_U \sqcup \mathcal{K}_W = \mathcal{K}$ (ввиду замечания 5.5) и $(\bigsqcup \mathcal{K}_U) \sqcup (\bigsqcup \mathcal{K}_W) = \bigsqcup \mathcal{K} = \mathfrak{K}$. Поэтому

$$\langle J \cap U \rangle = \bigoplus_{X \in \sqcup \mathcal{K}_U} \langle J \cap H_X \rangle = \bigoplus_{X \in \sqcup \mathcal{K}_U} H_X \quad (52)$$

(см. лемму 5.5). Кроме того,

$$T/S_0 = \langle J \rangle = \langle J \cap U \rangle \oplus \langle J \cap W \rangle$$

ввиду равенства (49), где $\langle J \cap U \rangle \subseteq (T/S_0) \cap U$ и $\langle J \cap W \rangle \subseteq (T/S_0) \cap W$. Следовательно, $\langle J \cap U \rangle = (T/S_0) \cap U$. Требуемое равенство (48) непосредственно вытекает из последнего равенства и (52). ■

Лемма 5.11. Следующие условия эквивалентны:

- 1) $U = \{0\}$;
- 2) $\rho(U) = \{0\}$;
- 3) $\mathcal{K}_U = \emptyset$.

Доказательство. Импликация $1 \implies 2$ и эквивалентность $2 \iff 3$ очевидны (см. замечание 5.2). Пусть теперь выполнены эквивалентные условия 2 и 3. Тогда $U \subseteq T/S_0$ (ввиду условия 2) и $(T/S_0) \cap U = \{0\}$ (ввиду условия 3 и леммы 5.10). Поэтому $U = (T/S_0) \cap U = \{0\}$, т. е. выполнено условие 1. ■

Из эквивалентности (18) и эквивалентности условий 1 и 2 леммы 5.11 вытекает

Следствие 5.3. Пусть пространство G/T $\Diamond$ -неразложимо или, что эквивалентно, $\mathfrak{J} = \{I\}$ (см. следствие 5.2). Тогда пространство G/S_0 ∇ -неразложимо.

Подпространства $C_{\mathfrak{X}}^{\Omega}$

Для произвольных $\Omega = (Q_X \mid X \in \mathfrak{K}) \in \mathcal{Q}$ и $\mathfrak{X} \in \mathcal{K}$ положим

$$C_{\mathfrak{X}}^{\Omega} = \bigoplus_{X \in \mathfrak{X}} (Q_X \oplus H_X).$$

Из замечания 5.2 и леммы 5.5 следует, что эта сумма прямая.

Замечание 5.6. Пусть $\Omega \in \mathcal{Q}$. Тогда легко видеть, что

$$\rho(C_{\mathfrak{X}}^{\Omega}) = \bigoplus_{X \in \mathfrak{X}} \langle X \rangle$$

при всех $\mathfrak{X} \in \mathcal{K}$. Из этого ввиду замечания 5.2 вытекает, что $\rho(C_{\mathfrak{X}}^{\Omega}) \neq \rho(C_{\mathfrak{Y}}^{\Omega})$ (и, следовательно, $C_{\mathfrak{X}}^{\Omega} \neq C_{\mathfrak{Y}}^{\Omega}$) для любых различных $\mathfrak{X}, \mathfrak{Y} \in \mathcal{K}$.

Лемма 5.12. Для любого $\Omega \in \mathcal{Q}$ имеет место равенство

$$G/S_0 = \bigoplus_{\mathfrak{X} \in \mathcal{K}} C_{\mathfrak{X}}^{\Omega}, \quad (53)$$

которое дает полное ∇ -ортогональное разложение пространства G/S_0 .

Доказательство. Пусть $\Omega = (Q_X \mid X \in \mathfrak{K})$. Непосредственно проверяется (с использованием замечания 5.2 и леммы 5.5), что

$$\begin{aligned} G/S_0 &= \rho^{-1}(G/T) = \left(\sum_{X \in \mathfrak{K}} \rho^{-1}(\langle X \rangle) \right) + (T/S_0) = \left(\bigoplus_{X \in \mathfrak{K}} Q_X \right) \oplus (T/S_0) = \\ &= \bigoplus_{X \in \mathfrak{K}} (Q_X \oplus H_X) = \bigoplus_{\mathfrak{X} \in \mathcal{K}} \bigoplus_{X \in \mathfrak{X}} (Q_X \oplus H_X) = \bigoplus_{\mathfrak{X} \in \mathcal{K}} C_{\mathfrak{X}}^{\Omega}. \end{aligned}$$

Таким образом, равенство (53) выполнено.

Выберем произвольное множество $\mathfrak{X} \in \mathcal{K}$. Пусть также $\mathfrak{Y} \in \mathcal{K} \setminus \{\mathfrak{X}\}$, $X \in \mathfrak{X}$ и $Y \in \mathfrak{Y}$. Тогда

- $Q_X \nabla Q_Y$, так как $\Omega \in \mathcal{Q}$;
- $Q_X \nabla H_Y$ и $Q_Y \nabla H_X$, так как $Q_X \subseteq \rho^{-1}(\langle X \rangle)$ и $Q_Y \subseteq \rho^{-1}(\langle Y \rangle)$;
- $H_X \nabla H_Y$ ввиду (33).

Поэтому $C_{\mathfrak{X}}^{\Omega} \nabla C_{\mathfrak{Y}}^{\Omega}$. Таким образом, разложение (53) ∇ -ортогонально.

Так как $\mathfrak{X} \neq \emptyset$, из замечаний 5.6 и 5.2 следует, что $C_{\mathfrak{X}}^{\Omega} \neq \{0\}$. Предположим теперь, что $C_{\mathfrak{X}}^{\Omega} = U \oplus W$ — нетривиальное ∇ -ортогональное разложение пространства $C_{\mathfrak{X}}^{\Omega}$. Тогда $\mathcal{K}_{C_{\mathfrak{X}}^{\Omega}} = \mathcal{K}_U \sqcup \mathcal{K}_W$ согласно замечанию 5.5. Но множество в левой части этого равенства одноэлементно (оно равно $\{\mathfrak{X}\}$ ввиду замечания 5.6), а множество в правой части содержит не менее двух элементов (так как $\mathcal{K}_U \neq \emptyset$ и $\mathcal{K}_W \neq \emptyset$ по лемме 5.11). Полученное противоречие показывает, что пространство $C_{\mathfrak{X}}^{\Omega}$ ∇ -неразложимо. ■

Лемма 5.13. Пусть $G/S_0 = \bigoplus \mathfrak{C}$ — полное ∇ -ортогональное разложение пространства G/S_0 . Тогда существует семейство $\Omega \in \mathcal{Q}$, такое, что

$$\mathfrak{C} = \{C_{\mathfrak{X}}^{\Omega} \mid \mathfrak{X} \in \mathcal{K}\}. \quad (54)$$

Доказательство. Согласно замечанию 5.5,

$$\bigsqcup_{U \in \mathfrak{C}} \mathcal{K}_U = \mathcal{K}. \quad (55)$$

Пусть X — произвольное множество из $\mathfrak{K}$. Тогда ввиду равенства (55) существует единственное подпространство $U \in \mathfrak{C}$, такое, что $X \in \bigsqcup \mathcal{K}_U$. Легко видеть, что $\rho^{-1}(\langle X \rangle) \subseteq U + (T/S_0)$. Поэтому можно выбрать линейно независимое множество $D_X \subseteq U$, удовлетворяющее равенству $\rho^{-1}(\langle X \rangle) = \langle D_X \rangle \oplus (T/S_0)$.

Построим теперь семейство $\mathfrak{Q} = (\langle E_X \rangle \mid X \in \mathfrak{K}) \in \mathcal{Q}$ в соответствии с леммой 5.8, используя выбранные в предыдущем абзаце множества D_X . При этом для любого двухэлементного множества $\{X, Y\}$, в котором $X \in \bigsqcup \mathcal{K}_U$ и $Y \in \bigsqcup \mathcal{K}_W$, где U и W — различные подпространства из $\mathfrak{C}$, выберем решение $(u_{a,Y}, u_{b,X} \mid a \in D_X, b \in D_Y)$ системы уравнений (44), состоящее из одних нулей. Это допустимо, так как $\sigma(a, b) = 0$ при всех $a \in D_X$ и $b \in D_Y$ ввиду того, что $D_X \subseteq U$, $D_Y \subseteq W$ и $U \nabla W$.

Пусть W — произвольное подпространство из $\mathfrak{C}$. Тогда из леммы 5.10 вытекает, что $\bigoplus_{\mathfrak{x} \in \mathcal{K}_W} C_{\mathfrak{x}}^{\mathfrak{Q}} \subseteq W$. В то же время $V/S_0 = \bigoplus_{U \in \mathfrak{C}} (\bigoplus_{\mathfrak{x} \in \mathcal{K}_U} C_{\mathfrak{x}}^{\mathfrak{Q}})$ ввиду равенств (53) (см. лемму 5.12) и (55). Кроме того, $V/S_0 = \bigoplus_{U \in \mathfrak{C}} U$. Следовательно, $\bigoplus_{\mathfrak{x} \in \mathcal{K}_W} C_{\mathfrak{x}}^{\mathfrak{Q}} = W$. Так как $W \nabla$ -неразложимо, из последнего равенства и леммы 5.12 вытекает, что $\mathcal{K}_W = \{\mathfrak{z}_W\}$ и

$$C_{\mathfrak{z}_W}^{\mathfrak{Q}} = W \quad (56)$$

для некоторого $\mathfrak{z}_W \in \mathcal{K}$. Требуемое равенство (54) следует теперь из равенства (56) (верного при любом $W \in \mathfrak{C}$) и того, что $W \mapsto \mathfrak{z}_W$ — биекция $\mathfrak{C}$ на $\mathcal{K}$ (это вытекает из равенства (55)). ■

Леммы 5.12 и 5.13 показывают, что полные ∇ -ортогональные разложения пространства G/S_0 — это в точности разложения вида $G/S_0 = \bigoplus_{\mathfrak{x} \in \mathcal{K}} C_{\mathfrak{x}}^{\mathfrak{Q}}$, где $\mathfrak{Q} \in \mathcal{Q}$.

Лемма 5.14. Пусть $\mathfrak{Q}, \mathfrak{Q}' \in \mathcal{Q}$ и $\mathfrak{x} \in \mathcal{K}$. Тогда

$$(C_{\mathfrak{x}}^{\mathfrak{Q}}; \sigma) \cong (C_{\mathfrak{x}}^{\mathfrak{Q}'}; \sigma). \quad (57)$$

Доказательство. Положим для краткости $U = \sum_{X \in \mathfrak{x}} \rho^{-1}(\langle X \rangle)$ и $W = \bigoplus_{X \in \mathfrak{K} \setminus \mathfrak{x}} H_X$. Тогда легко видеть, что $C_{\mathfrak{x}}^{\mathfrak{Q}} \oplus W = U$ (см. лемму 5.5). Из леммы 5.12 вытекает, что $C_{\mathfrak{y}}^{\mathfrak{Q}} \nabla C_{\mathfrak{x}}^{\mathfrak{Q}}$ при любом $\mathfrak{y} \in \mathcal{K} \setminus \{\mathfrak{x}\}$. Следовательно, $W \nabla C_{\mathfrak{x}}^{\mathfrak{Q}}$, так как $W \subseteq \bigoplus_{\mathfrak{y} \in \mathcal{K} \setminus \{\mathfrak{x}\}} C_{\mathfrak{y}}^{\mathfrak{Q}}$. Кроме того, $W \nabla W$ ввиду (33). Поэтому $W \subseteq C_U^{\nabla}(U)$ и

$$(C_{\mathfrak{x}}^{\mathfrak{Q}}; \sigma) \cong (U/W; \sigma) \quad (58)$$

согласно замечанию 4.3. Аналогично,

$$(C_{\mathfrak{x}}^{\mathfrak{Q}'}; \sigma) \cong (U/W; \sigma). \quad (59)$$

Требуемый изоморфизм (57) вытекает теперь из (58) и (59). ■

5.3. Основной результат

Из теоремы 5.1, лемм 5.12 и 5.13 и замечания 5.6 непосредственно вытекает следующий основной результат настоящей работы. В его формулировке напоминаются предположения, которые сделаны выше.

Теорема 5.2. Предположим, что пространство с ортогональностью $(V; \diamond)$ удовлетворяет условию (13) и что пространство V/T конечномерно. Тогда полные ∇ -ортогональные разложения пространства V — это в точности разложения вида

$$V = (\bigoplus \mathfrak{A}) \oplus (\bigoplus \mathfrak{B}) \oplus \bigoplus_{\mathfrak{x} \in \mathcal{K}(G(\mathfrak{A}))} \nu_{R, S_0}^{-1}(C_{\mathfrak{x}}^{\mathfrak{Q}}(G(\mathfrak{A}))), \quad (60)$$

где $\mathfrak{A} \in \mathcal{A}$, $\mathfrak{B} \in \mathcal{B}$, $R \in \mathfrak{R}(G(\mathfrak{A}))$ и $\mathfrak{Q} \in \mathcal{Q}(G(\mathfrak{A}))$. Множества $\mathfrak{A}$ и $\mathfrak{B}$ и подпространства R и $C_{\mathfrak{X}}^{\mathfrak{Q}}(G(\mathfrak{A}))$ для каждого $\mathfrak{X} \in \mathcal{K}(G(\mathfrak{A}))$ определяются произвольным разложением (60) однозначно. Кроме того, если $\mathfrak{S}$ — множество всех подпространств, входящих в это разложение, т. е.

$$\mathfrak{S} = \mathfrak{A} \sqcup \mathfrak{B} \sqcup \{ \nu_{R, S_0}^{-1}(C_{\mathfrak{X}}^{\mathfrak{Q}}(G(\mathfrak{A}))) \mid \mathfrak{X} \in \mathcal{K}(G(\mathfrak{A})) \},$$

то $\mathfrak{A}$, $\mathfrak{B}$ и R могут быть найдены по $\mathfrak{S}$ с помощью формул из теоремы 5.1, а $C_{\mathfrak{X}}^{\mathfrak{Q}}(G(\mathfrak{A}))$ для произвольного $\mathfrak{X} \in \mathcal{K}(G(\mathfrak{A}))$ — это единственное подпространство

$$U \in \nu_{R, S_0}(\mathfrak{S} \setminus (\mathfrak{A} \sqcup \mathfrak{B})),$$

такое, что $\rho(U) = \bigoplus_{X \in \mathfrak{X}} \langle X \rangle$.

6. Приложения

Напомним, что здесь, как и в п. 5.2 и 5.3, делаются следующие предположения:

- пространство с ортогональностью $(V; \diamond)$ удовлетворяет условию (13);
- пространство V/T конечномерно.

6.1. К р и т е р и й ∇ -н е р а з л о ж и м о с т и

Теорема 6.1. Пространство V ∇ -неразложимо тогда и только тогда, когда выполнено одно из следующих взаимоисключающих условий:

- 1) V — пространство типа 1 или 2;
- 2) V одномерно и σ тождественно равна 0 на $V \times V$;
- 3) $S_0 = \{0\}$, σ тождественно равна 0 на $S_1 \times S_1$, граф $\Delta(V)$ имеет непустое множество вершин и связан (это условие для графа $\Delta(V)$ может быть записано в виде равенства $\mathcal{K}(V) = \{\mathfrak{K}(V)\}$).

Доказательство. Из лемм 4.2 и 5.12 следует, что при выполнении любого из условий теоремы пространство V ∇ -неразложимо (очевидно, что если выполнено условие 3, то $T = S_1$, $\mathcal{A} = \{\emptyset\}$ и $V = G(\emptyset)$; здесь используется также то, что $\mathcal{Q}(V) \neq \emptyset$ ввиду п. 2 леммы 5.8). Пусть теперь пространство V ∇ -неразложимо. По теореме 5.1 существует единственная четверка $(\mathfrak{A}, \mathfrak{B}, R, \mathfrak{C}) \in \mathcal{P}$, такая, что

$$\{V\} = \mathfrak{A} \sqcup \mathfrak{B} \sqcup \nu_{R, S_0}^{-1}(\mathfrak{C}).$$

Возможны три случая:

- 1) $\mathfrak{A} = \{V\}$, $\mathfrak{B} = \emptyset$, $\mathfrak{C} = \emptyset$;
- 2) $\mathfrak{A} = \emptyset$, $\mathfrak{B} = \{V\}$, $\mathfrak{C} = \emptyset$;
- 3) $\mathfrak{A} = \emptyset$, $\mathfrak{B} = \emptyset$, $\nu_{R, S_0}^{-1}(\mathfrak{C}) = \{V\}$.

Легко заметить, что в каждом из этих случаев выполняется условие леммы с тем же номером (в случае 3 для этого нужно использовать лемму 5.13 и замечание 5.6). ■

Следующий пример приводится как для иллюстрации приведенного выше материала, так и для описания конструкции, которая понадобится нам в дальнейшем.

Пример 6.1. Предположим, что $\text{char } F = 2$ и V конечномерно, причем $\dim V \geq 3$. Пусть U — подпространство V , имеющее размерность не более $(\dim V) - 3$, а τ — билинейная функция из $U \times V$ в F , удовлетворяющая следующим условиям:

- τ тождественно равна 0 на $U \times U$;
- для любого $u \in U \setminus \{0\}$ существует $v \in V$, такой, что $\tau(u, v) \neq 0$.

Очевидно, что такая билинейная функция τ существует тогда и только тогда, когда $\dim U \leq (\dim V)/2$.

Определим подмножество $\diamond \subseteq V \times V$ и функцию $\sigma: \diamond \rightarrow F$ следующим образом. Пусть $x, y \in V$. Тогда считаем, что $x \diamond y$, если и только если $x + U$ и $y + U$ линейно зависимы (в V/U). Предположим теперь, что последнее условие выполнено. Если $x \in U$, то полагаем $\sigma(x, y) = \tau(x, y)$. Если же $x \notin U$, то y может быть единственным образом представлен в виде $\lambda x + u$, где $\lambda \in F$ и $u \in U$. Тогда полагаем $\sigma(x, y) = \tau(u, x)$. Непосредственно проверяется, что σ — частичная симметричная билинейная функция на V с областью определения $\diamond$, причем $0 \diamond V$ и

$$C_V^\diamond(x) = \begin{cases} V, & \text{если } x \in U, \\ \langle x \rangle \oplus U, & \text{если } x \in V \setminus U. \end{cases}$$

Используя эту формулу и неравенство $\dim V \geq (\dim U) + 3$, легко видеть, что

- пространство с ортогональностью $(V; \diamond)$ удовлетворяет условию (13);
- $S_0 = \{0\}$ и $S_1 = T = U$;
- $C_{V/U}^\diamond(a) = \langle a \rangle$ при всех $a \in (V/U) \setminus \{0\}$ (для доказательства этого утверждения используется также эквивалентность (4)).

Поэтому $\mathcal{A} = \{\emptyset\}$, $\mathcal{B} = \{\emptyset\}$, $\mathfrak{R}(V) = \{V\}$, $I(V) = (V/U) \setminus \{0\}$, $\mathfrak{I}(V) = \{I(V)\}$, $\mathcal{I}(V) = \{\mathfrak{I}(V)\}$, $\mathfrak{K}(V) = \{I(V)\}$ и $\mathcal{K}(V) = \{\mathfrak{K}(V)\}$, где $V = G(\emptyset)$. Согласно следствию 5.3, пространство V ∇ -неразложимо. Тот же самый вывод можно сделать, используя теорему 6.1 (для V выполняется условие 3 этой теоремы). Кроме того, $x \nabla x$ для любого $x \in V$.

6.2. Об эквивалентности полных ∇ -ортогональных разложений

Замечание 6.1. Пусть $\mathfrak{B}, \mathfrak{B}' \in \mathcal{B}$. Тогда $|\mathfrak{B}| = |\mathfrak{B}'| = \dim S_0$. Кроме того, если U и W — произвольные изоморфные (или, что эквивалентно, имеющие одинаковую размерность) подпространства S_0 , то всякий изоморфизм U на W является изоморфизмом $(U; \sigma)$ на $(W; \sigma)$. Поэтому биекции $U \mapsto W_U$ множества $\mathfrak{B}$ на множество $\mathfrak{B}'$ существуют и удовлетворяют условию $(U; \sigma) \cong (W_U; \sigma)$ для всех $U \in \mathfrak{B}$.

Лемма 6.1. Пусть $(\mathfrak{A}, \mathfrak{B}, R, \mathfrak{C}), (\mathfrak{A}', \mathfrak{B}', R', \mathfrak{C}') \in \mathcal{P}$. Предположим, что $(G(\mathfrak{A}); \sigma) \cong (G(\mathfrak{A}'); \sigma)$. Тогда существует биекция $U \mapsto W_U$ множества $\nu_{R, S_0}^{-1}(\mathfrak{C})$ на множество $\nu_{R', S_0}^{-1}(\mathfrak{C}')$, такая, что $(U; \sigma) \cong (W_U; \sigma)$ для любого $U \in \nu_{R, S_0}^{-1}(\mathfrak{C})$.

Доказательство. Согласно замечанию 4.3, $(\bigoplus \mathfrak{A}; \sigma) \cong (S_1/T; \sigma) \cong (\bigoplus \mathfrak{A}'; \sigma)$. Поэтому ввиду равенства (26) и п.1 леммы 4.1 можем выбрать $\alpha \in \text{Aut}(V; \sigma)$, для которого $\alpha(\bigoplus \mathfrak{A}') = \bigoplus \mathfrak{A}$. Применив α к элементам множества $\mathfrak{A}' \sqcup \mathfrak{B}' \sqcup \nu_{R', S_0}^{-1}(\mathfrak{C}')$, считаем, что $\bigoplus \mathfrak{A} = \bigoplus \mathfrak{A}'$ (очевидно, что утверждение леммы до этой замены равносильно таковому после нее). Тогда $G(\mathfrak{A}) = G(\mathfrak{A}')$; обе части последнего равенства для краткости обозначим через G .

По лемме 5.13 существуют $\mathfrak{Q}, \mathfrak{Q}' \in \mathcal{Q}(G)$, такие, что

$$\mathfrak{C} = \{C_{\mathfrak{X}}^{\mathfrak{Q}}(G) \mid \mathfrak{X} \in \mathcal{K}(G)\} \quad \text{и} \quad \mathfrak{C}' = \{C_{\mathfrak{X}}^{\mathfrak{Q}'}(G) \mid \mathfrak{X} \in \mathcal{K}(G)\}.$$

Ввиду замечания 5.6 для доказательства леммы достаточно показать, что

$$(\nu_{R, S_0}^{-1}(C_{\mathfrak{X}}^{\mathfrak{Q}}(G)); \sigma) \cong (\nu_{R', S_0}^{-1}(C_{\mathfrak{X}}^{\mathfrak{Q}'}(G)); \sigma)$$

при любом $\mathfrak{X} \in \mathcal{K}(G)$. Но это непосредственно следует из того, что для произвольного $\mathfrak{X} \in \mathcal{K}(G)$

$$(C_{\mathfrak{X}}^{\mathfrak{Q}}(G); \sigma) \cong (C_{\mathfrak{X}}^{\mathfrak{Q}'}(G); \sigma)$$

по лемме 5.14 и

$$(\nu_{R, S_0}^{-1}(C_{\mathfrak{X}}^{\mathfrak{Q}}(G)); \sigma) \cong (C_{\mathfrak{X}}^{\mathfrak{Q}}(G); \sigma), \quad (\nu_{R', S_0}^{-1}(C_{\mathfrak{X}}^{\mathfrak{Q}'}(G)); \sigma) \cong (C_{\mathfrak{X}}^{\mathfrak{Q}'}(G); \sigma)$$

согласно замечанию 4.3. ■

Напомним, что ввиду сделанных выше предположений и п. 2 леммы 4.1 произвольные ∇ -ортогональные разложения пространства V σ -эквивалентны тогда и только тогда, когда они локально σ -эквивалентны.

Теорема 6.2. Пусть $V = \bigoplus \mathfrak{S}$ и $V = \bigoplus \mathfrak{S}'$ — полные ∇ -ортогональные разложения пространства V . Тогда

- 1) если $\text{char } F \neq 2$, то указанные разложения пространства V σ -эквивалентны в том и только в том случае, когда

$$\forall x \in F^*/(F^*)^2 \quad |\{U \in \mathfrak{A} \mid \kappa(U; \sigma) = x\}| = |\{U \in \mathfrak{A}' \mid \kappa(U; \sigma) = x\}|, \quad (61)$$

где $\mathfrak{A}$ и $\mathfrak{A}'$ — первые компоненты прообразов множеств $\mathfrak{S}$ и $\mathfrak{S}'$ соответственно при биекции (30) из теоремы 5.1 (в данном случае $\mathfrak{A}$ и $\mathfrak{A}'$ состоят лишь из подпространств типа 1);

- 2) если $\text{char } F = 2$ и $x \nabla x$ для всех $x \in S_1$, то указанные разложения пространства V σ -эквивалентны.

Доказательство. Выберем $(\mathfrak{A}, \mathfrak{B}, R, \mathfrak{C}), (\mathfrak{A}', \mathfrak{B}', R', \mathfrak{C}') \in \mathcal{P}$, такие, что

$$\mathfrak{S} = \mathfrak{A} \sqcup \mathfrak{B} \sqcup \nu_{R, S_0}^{-1}(\mathfrak{C}) \quad \text{и} \quad \mathfrak{S}' = \mathfrak{A}' \sqcup \mathfrak{B}' \sqcup \nu_{R', S_0}^{-1}(\mathfrak{C}'). \quad (62)$$

Эти четверки существуют и единственны по теореме 5.1. Предположим, что имеет место один из следующих случаев:

- 1) $\text{char } F \neq 2$ и выполнено условие (61);
- 2) выполнено условие п. 2, т. е. $\text{char } F = 2$ и $x \nabla x$ для всех $x \in S_1$.

Тогда существует биекция $U \mapsto W_U$ множества $\mathfrak{A}$ на множество $\mathfrak{A}'$, такая, что

$$(U; \sigma) \cong (W_U; \sigma) \quad (63)$$

для всех $U \in \mathfrak{A}$. В случае 1 из замечания 4.4 вытекает, что в качестве такой биекции можно взять произвольную биекцию $U \mapsto W_U$ множества $\mathfrak{A}$ на множество $\mathfrak{A}'$, удовлетворяющую равенству $\kappa(U; \sigma) = \kappa(W_U; \sigma)$ для всех $U \in \mathfrak{A}$ (эти биекции существуют ввиду (61)). В случае 2 $\mathfrak{A}$ и $\mathfrak{A}'$ состоят лишь из подпространств типа 2. Кроме того, очевидно, что $(U; \sigma) \cong (W; \sigma)$ для любых подпространств $U, W \subseteq S_1$ типа 2. Поэтому в качестве такой биекции можно взять произвольную биекцию $\mathfrak{A}$ на $\mathfrak{A}'$ (эти биекции существуют, так как $|\mathfrak{A}| = |\mathfrak{A}'| = \dim(S_1/T)/2$).

Выберем некоторую биекцию $U \mapsto W_U$ множества $\mathfrak{A}$ на множество $\mathfrak{A}'$, удовлетворяющую условию (63) для всех $U \in \mathfrak{A}$. Замечание 6.1 и лемма 6.1 (которая применима ввиду леммы 4.6) позволяют продолжить эту биекцию до биекции $U \mapsto W_U$ множества $\mathfrak{S}$ на множество $\mathfrak{S}'$, удовлетворяющей условию (63) при любом $U \in \mathfrak{S}$ (см. равенства (62)). Таким образом, рассматриваемые разложения пространства V локально σ -эквивалентны и, следовательно, σ -эквивалентны (ввиду п. 2 леммы 4.1 — см. выше).

Пусть теперь $\text{char } F \neq 2$ и рассматриваемые разложения пространства V σ -эквивалентны. Выберем некоторый автоморфизм $\alpha \in \text{Aut}(V; \sigma)$, такой, что $\alpha(\mathfrak{S}) = \mathfrak{S}'$. Очевидно, что $\alpha(S_1) = S_1$ и $\alpha(T) = T$, поэтому $\alpha(\mathfrak{A}) \in \mathcal{A}$. Из равенств (62) вытекает, что $\alpha(\mathfrak{A})$ и $\mathfrak{A}'$ — подмножества $\mathfrak{S}'$, принадлежащие $\mathcal{A}$. Поэтому $\alpha(\mathfrak{A}) = \mathfrak{A}'$ ввиду утверждения о единственности из леммы 5.1. Условие (61) следует теперь из последнего равенства и замечания 4.4. ■

Замечание 6.2. Очевидно, что $(T; \sigma)$ не изоморфно никакому пространству типа 1. Поэтому из замечания 4.4 следует, что если $\mathfrak{A}$ и $\mathfrak{A}'$ принадлежат $\mathcal{A}$ и состоят лишь из подпространств типа 1 ($\text{char } F$ может быть произвольной), то условие (61) (см. п. 1 теоремы 6.2) выполняется тогда и только тогда, когда разложения $S_1 = (\bigoplus \mathfrak{A}) \oplus T$ и $S_1 = (\bigoplus \mathfrak{A}') \oplus T$ пространства S_1 локально σ -эквивалентны или, что в данном случае равносильно, σ -эквивалентны (см. п. 2 леммы 4.1).

Из п. 2 теоремы 6.2 непосредственно вытекает

Следствие 6.1. Если $\text{char } F = 2$ и ортогональность ∇ ассоциирована с некоторой функцией из V в F , то все полные ∇ -ортогональные разложения пространства V σ -эквивалентны.

Следующий пример показывает, что при $\text{char } F \neq 2$ аналог следствия 6.1 неверен.

Пример 6.2. Пусть F конечно, $\text{char } F \neq 2$, $\dim V = 3$, а σ определена на всем $V \times V$ и имеет в некотором базисе a_1, a_2, a_3 пространства V единичную матрицу. В этом случае σ ассоциирована с функцией φ , заданной формулой

$$\varphi(x_1 a_1 + x_2 a_2 + x_3 a_3) = \frac{1}{2} (x_1^2 + x_2^2 + x_3^2), \quad x_1, x_2, x_3 \in F.$$

Выберем произвольные элементы $\theta \in F^* \setminus (F^*)^2$ и $\xi, \eta \in F$, удовлетворяющие равенству $\xi^2 + \eta^2 = \theta$ (такие ξ и η существуют для любого $\theta \in F$ ввиду леммы IV.2 из [4]). Положим $b_1 = a_1$, $b_2 = \xi a_2 + \eta a_3$ и $b_3 = -\eta a_2 + \xi a_3$. Тогда σ в базисе b_1, b_2, b_3 имеет матрицу

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & \theta & 0 \\ 0 & 0 & \theta \end{pmatrix}$$

(см. лемму IV.3 из [4]). Поэтому $V = \langle a_1 \rangle \oplus \langle a_2 \rangle \oplus \langle a_3 \rangle$ и $V = \langle b_1 \rangle \oplus \langle b_2 \rangle \oplus \langle b_3 \rangle$ — полные ∇ -ортогональные разложения пространства V . Покажем, что эти разложения не только не σ -эквивалентны (это вытекает из замечания 4.4), но и не ∇ -эквивалентны. Пусть, напротив, некоторый автоморфизм $\alpha \in \text{Aut}(V; \nabla)$ удовлетворяет равенству

$$\alpha(\{\langle a_1 \rangle, \langle a_2 \rangle, \langle a_3 \rangle\}) = \{\langle b_1 \rangle, \langle b_2 \rangle, \langle b_3 \rangle\}.$$

Пусть также перестановка β множества $\{1, 2, 3\}$ такова, что $\alpha(\langle a_{\beta(i)} \rangle) = \langle b_i \rangle$ для всех $i \in \{1, 2, 3\}$. Тогда $\alpha(a_{\beta(i)}) = \lambda_i b_i$ при некоторых $\lambda_i \in F^*$ ($i = 1, 2, 3$). Очевидно, что $a_{\beta(1)} + a_{\beta(2)} \nabla -a_{\beta(1)} + a_{\beta(2)}$ и, следовательно, $\alpha(a_{\beta(1)} + a_{\beta(2)}) \nabla \alpha(-a_{\beta(1)} + a_{\beta(2)})$. В то же время

$$\alpha(a_{\beta(1)} + a_{\beta(2)}) \nabla \alpha(-a_{\beta(1)} + a_{\beta(2)}) \iff -\lambda_1^2 + \theta \lambda_2^2 = 0 \iff \theta = \left(\frac{\lambda_1}{\lambda_2} \right)^2,$$

а последнее равенство противоречит выбору θ . Таким образом, рассматриваемые разложения не ∇ -эквивалентны.

Пример 6.2 показывает, что при $\text{char } F \neq 2$ полные ∇ -ортогональные разложения пространства V могут не быть даже ∇ -эквивалентными. Следующая теорема утверждает, что в данном случае для любых двух таких разложений имеет место локальная $(\diamond, \nabla)$ -эквивалентность.

Теорема 6.3. Если $\text{char } F \neq 2$, то все полные ∇ -ортогональные разложения пространства V локально $(\diamond, \nabla)$ -эквивалентны.

Доказательство. Пусть $V = \bigoplus \mathfrak{S}$ и $V = \bigoplus \mathfrak{S}'$ — произвольные полные ∇ -ортогональные разложения пространства V . Как и в доказательстве теоремы 6.2, выберем $(\mathfrak{A}, \mathfrak{B}, R, \mathfrak{C}), (\mathfrak{A}', \mathfrak{B}', R', \mathfrak{C}') \in \mathcal{P}$, такие, что

$$\mathfrak{S} = \mathfrak{A} \sqcup \mathfrak{B} \sqcup \nu_{R, S_0}^{-1}(\mathfrak{C}) \quad \text{и} \quad \mathfrak{S}' = \mathfrak{A}' \sqcup \mathfrak{B}' \sqcup \nu_{R', S_0}^{-1}(\mathfrak{C}'). \quad (64)$$

Эти четверки существуют и единственны по теореме 5.1. Множества $\mathfrak{A}$ и $\mathfrak{A}'$ состоят лишь из подпространств типа 1. Кроме того, легко видеть, что $(U; \diamond, \nabla) \cong (W; \diamond, \nabla)$ для любых подпространств $U, W \subseteq S_1$ типа 1. Поэтому биекции $U \mapsto W_U$ множества $\mathfrak{A}$ на множество $\mathfrak{A}'$ существуют (так как $|\mathfrak{A}| = |\mathfrak{A}'| = \dim(S_1/T)$) и удовлетворяют условию

$$(U; \diamond, \nabla) \cong (W_U; \diamond, \nabla) \quad (65)$$

для всех $U \in \mathfrak{A}$. Замечание 6.1 и лемма 6.1 (которая применима ввиду леммы 4.6) позволяют продолжить произвольную такую биекцию до биекции $U \mapsto W_U$ множества $\mathfrak{S}$ на множество $\mathfrak{S}'$, удовлетворяющей условию (65) при любом $U \in \mathfrak{S}$ (см. равенства (64)). Таким образом, рассматриваемые разложения пространства V локально $(\diamond, \nabla)$ -эквивалентны. ■

Из теоремы 6.3 вытекает, что при $\text{char } F \neq 2$ мультимножество размерностей подпространств, входящих в полное ∇ -ортогональное разложение пространства V , одно и то же для всех таких разложений. Следующий пример показывает, что при $\text{char } F = 2$ это не всегда верно.

Пример 6.3. Пусть $\text{char } F = 2$, $\dim V = 3$, а σ определена на всем $V \times V$ и имеет в некотором базисе a_1, a_2, a_3 пространства V единичную матрицу. Положим $b_1 = a_1 + a_2 + a_3$, $b_2 = a_1 + a_3$ и $b_3 = a_2 + a_3$. Тогда σ в базисе b_1, b_2, b_3 имеет матрицу

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

(см. лемму IV.5 из [4]). Поэтому $V = \langle a_1 \rangle \oplus \langle a_2 \rangle \oplus \langle a_3 \rangle$ и $V = \langle b_1 \rangle \oplus \langle b_2, b_3 \rangle$ — полные ∇ -ортогональные разложения пространства V (см. лемму 4.2; здесь $\langle b_2, b_3 \rangle$ имеет тип 2).

Следующий пример показывает, что при $\text{char } F = 2$ утверждение, аналогичное п. 1 теоремы 6.2 (в предположении, что $\mathfrak{A}$ и $\mathfrak{A}'$ состоят лишь из подпространств типа 1), неверно.

Пример 6.4. Предположим, что $\text{char } F = 2$. Пусть V_1 — одномерное векторное пространство, a — некоторый порождающий элемент этого пространства, а симметричная билинейная функция $\sigma_1: V_1 \times V_1 \rightarrow F$ определена равенством $\sigma_1(a, a) = 1$. Обозначим через $(V_2; \sigma_2)$ некоторое пространство с частичной симметричной билинейной функцией, построенное в соответствии с конструкцией примера 6.1, где дополнительно предполагаем, что $U \neq \{0\}$. Пусть теперь $(V; \sigma)$ — прямое ортогональное произведение

семейства $((V_i; \sigma_i) \mid i \in \{1, 2\})$ пространств с частичными симметричными билинейными функциями. Ввиду замечания 3.4 пространство с ортогональностью $(V; \Diamond)$ удовлетворяет условию (13). Кроме того, $0 \Diamond V$. Будем считать V_1 и V_2 подпространствами V , отождествляя v_1 с $(v_1, 0)$ для любого $v_1 \in V_1$ и v_2 с $(0, v_2)$ для любого $v_2 \in V_2$. Тогда $V = V_1 \oplus V_2$ — ∇ -ортогональное разложение пространства V . Из леммы 3.1 вытекает, что

$$S_0 = \{0\}, \quad S_1 = V_1 \oplus U \quad \text{и} \quad T = U.$$

Выберем произвольный элемент $u \in U \setminus \{0\}$ и положим $V'_1 = \langle a + u \rangle$. Очевидно, что $\{V_1\}, \{V'_1\} \in \mathcal{A}$, причем V_1 и V'_1 имеют тип 1 и $\kappa(V_1; \sigma) = \kappa(V'_1; \sigma) = 1$ в $F^*/(F^*)^2$ (так как $\sigma(a, a) = \sigma(a + u, a + u) = 1$). Легко видеть, что $G(\{V_1\}) = V_2$ (см. лемму 4.4) и $G(\{V'_1\}) = \{w - \sigma(w, u)a \mid w \in V_2\}$; последнее подпространство обозначим для краткости через V'_2 . Непосредственно проверяется, что отображение $w \mapsto w - \sigma(w, u)a$, где $w \in V_2$, является изоморфизмом $(V_2; \Diamond)$ на $(V'_2; \Diamond)$. Кроме того, всякий изоморфизм $(V_2; \Diamond)$ на $(V'_2; \Diamond)$ отображает

$$T = C_{V_2}^\Diamond(V_2) = C_{V'_2}^\Diamond(V'_2)$$

(см. (27)) на себя. Поэтому $(V_2/T; \Diamond) \cong (V'_2/T; \Diamond)$ и пространство V'_2/T $\Diamond$ -неразложимо, так как $\Diamond$ -неразложимо пространство V_2/T (последнее условие ввиду следствия 5.2 эквивалентно равенству $\mathfrak{I}(V_2) = \{I(V_2)\}$). Следствие 5.3 показывает теперь, что V'_2 , как и V_2 , ∇ -неразложимо. Таким образом, $V = V_1 \oplus V_2$ и $V = V'_1 \oplus V'_2$ — полные ∇ -ортогональные разложения пространства V (см. равенство (26)), причем первые компоненты прообразов множеств $\{V_1, V_2\}$ и $\{V'_1, V'_2\}$ при биекции (30) из теоремы 5.1 равны соответственно $\{V_1\}$ и $\{V'_1\}$ (это вытекает из леммы 5.1). В то же время $(V_2; \nabla)$ и $(V'_2; \nabla)$ не изоморфны, так как $x \nabla x$ для любого $x \in V_2$, но существует $y \in V'_2$, такой, что $y \nabla y$ (в качестве такого y можно взять произвольный элемент $V'_2 \setminus V_2$). Следовательно, указанные разложения пространства V не локально ∇ -эквивалентны и тем более не σ -эквивалентны.

6.3. Критерий единственности полного ∇ -ортогонального разложения

Теорема 6.4. Полное ∇ -ортогональное разложение пространства V единственно тогда и только тогда, когда выполнено одно из следующих взаимоисключающих условий:

- 1) S_1 — пространство типа 1 или 2;
- 2) $F = \text{GF}(2)$ и σ в некотором базисе пространства S_1 имеет матрицу $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$;
- 3) $F = \text{GF}(3)$ и σ в некотором базисе пространства S_1 имеет матрицу $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$;
- 4) V одномерно и σ тождественно равна 0 на $V \times V$;
- 5) $S_0 = \{0\}$, σ тождественно равна 0 на $S_1 \times S_1$ и

$$\left| \left\{ \mathfrak{x} \in \mathcal{K}(V) \mid \bigoplus_{X \in \mathfrak{x}} H_X(V) \neq \{0\} \right\} \right| \leq 1. \quad (66)$$

Доказательство. Из теоремы 5.2 вытекает, что полное ∇ -ортогональное разложение пространства V единственно тогда и только тогда, когда

$$|\mathcal{A}| = 1; \quad (67)$$

$$|\mathcal{B}| = 1; \quad (68)$$

$$|\mathfrak{R}(G(\mathfrak{A}))| = 1; \quad (69)$$

$$\forall \Omega, \Omega' \in \mathcal{Q}(G(\mathfrak{A})) \forall \mathfrak{X} \in \mathcal{K}(G(\mathfrak{A})) C_{\mathfrak{X}}^{\Omega}(G(\mathfrak{A})) = C_{\mathfrak{X}}^{\Omega'}(G(\mathfrak{A})), \quad (70)$$

где $\mathfrak{A}$ — единственный элемент множества $\mathcal{A}$ (см. условие (67)). Поэтому для доказательства теоремы достаточно показать, что условия (67)–(70) выполнены, если и только если выполнено одно из условий, указанных в формулировке теоремы.

1. Предположим, что выполнены условия (67)–(70); при этом через $\mathfrak{A}$ будем обозначать единственный элемент множества $\mathcal{A}$. Пусть сначала $\mathfrak{A} \neq \emptyset$. Тогда ввиду равенства (67) и леммы 4.8, примененной к пространству S_1 , получаем, что $T = \{0\}$ и всякое подпространство пространства S_1 , имеющее тип 1 или 2, принадлежит $\mathfrak{A}$. Если $|\mathfrak{A}| = 1$, то выполнено условие 1. Считаем теперь, что $|\mathfrak{A}| \geq 2$. Предположим, что $\mathfrak{A}$ содержит подпространство U типа 2. Выберем базис u_1, u_2 подпространства U , в котором σ имеет матрицу $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. Так как $|\mathfrak{A}| \geq 2$, можно выбрать подпространство $W \in \mathfrak{A} \setminus \{U\}$. Рассмотрим два случая.

1. W имеет тип 1, т. е. $W = \langle w \rangle$, где $w \notin U$. Тогда $\langle w + u_1 \rangle$ — подпространство S_1 , имеющее тип 1 и не принадлежащее $\mathfrak{A}$.
2. W имеет тип 2, т. е. матрица симметричной билинейной функции σ в некотором базисе w_1, w_2 этого подпространства равна $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. Тогда $\langle u_1 + w_1, u_2 \rangle$ — подпространство S_1 , имеющее тип 2 и не принадлежащее $\mathfrak{A}$.

В обоих случаях получаем противоречие с доказанным выше свойством. Это показывает, что $\mathfrak{A}$ состоит только из подпространств типа 1.

Предположим, что существуют $u, w \in S_1$ и $\lambda \in F^*$, такие, что $\langle u \rangle$ и $\langle w \rangle$ — различные подпространства из $\mathfrak{A}$ и $\lambda^2 \neq -\sigma(u, u)/\sigma(w, w)$. Тогда $\langle u + \lambda w \rangle$ — подпространство S_1 , имеющее тип 1 и не принадлежащее $\mathfrak{A}$. Полученное противоречие показывает, что $\lambda^2 = -\sigma(u, u)/\sigma(w, w)$ для любых $u, w \in S_1$, порождающих различные подпространства из $\mathfrak{A}$, и любого $\lambda \in F^*$. Следовательно,

$$\forall \lambda \in F^* \lambda^2 = 1; \quad (71)$$

$$\forall u, w \in S_1 (\langle u \rangle, \langle w \rangle \in \mathfrak{A} \ \& \ \langle u \rangle \neq \langle w \rangle \implies \sigma(u, u) = -\sigma(w, w)). \quad (72)$$

Из (71) вытекает, что $F = \text{GF}(2)$ или $F = \text{GF}(3)$. Если $F = \text{GF}(2)$, то σ в некотором базисе пространства S_1 имеет единичную матрицу (размера $|\mathfrak{A}| \times |\mathfrak{A}|$). При этом $|\mathfrak{A}| \leq 2$ (иначе конструкция примера 6.3 дает противоречие с равенством (67)). Поэтому $|\mathfrak{A}| = 2$ и выполняется условие 2. Если же $F = \text{GF}(3)$, то из (72) следует, что для любого $\varepsilon \in \{-1, 1\}$ множество $\mathfrak{A}$ содержит не более одного подпространства $\langle u \rangle$, удовлетворяющего равенству $\sigma(u, u) = \varepsilon$ (здесь $\sigma(u, u)$ не зависит от выбора порождающего u ввиду (71)). Это вместе с условием $|\mathfrak{A}| \geq 2$ показывает, что в данном случае выполняется условие 3.

Считаем теперь, что $\mathfrak{A} = \emptyset$. Тогда σ тождественно равна 0 на $S_1 \times S_1$ и $G(\mathfrak{A}) = V$. Если $\dim S_0 \geq 2$, то получаем противоречие с равенством (68). Поэтому $\dim S_0 \leq 1$. Пусть сначала $\dim S_0 = 1$. Если $S_0 \neq G(\mathfrak{A})$, то имеет место противоречие с равенством (69). Таким образом, в данном случае $S_0 = G(\mathfrak{A}) = V$ и выполняется условие 4.

Рассмотрим теперь случай, когда $\dim S_0 = 0$, т.е. $S_0 = \{0\}$. Предположим, что неравенство (66) не выполняется. Тогда можем выбрать $\mathfrak{Z}_i \in \mathcal{K}(V)$, $Z_i \in \mathfrak{Z}_i$ и $w_i \in H_{Z_i}(V) \setminus \{0\}$ для $i = 1, 2$, где $\mathfrak{Z}_1 \neq \mathfrak{Z}_2$. Выберем также какое-либо семейство $\mathfrak{Q} = (Q_X | X \in \mathfrak{K}(V)) \in \mathcal{Q}(V)$ (из п. 2 леммы 5.8 вытекает, что $\mathcal{Q}(V) \neq \emptyset$). Пусть $i \in \{1, 2\}$. Очевидно, что $x \mapsto \sigma(x, w_i)$ (где $x \in Q_{Z_i}$) — линейная функция из Q_{Z_i} в F . Эта функция отлична от тождественного нуля на Q_{Z_i} , так как $w_i \notin \rho^{-1}(\langle Z_i \rangle) = Q_{Z_i} \oplus T$ (ввиду леммы 5.3 и равенства (37)) и $w_i \nabla T$ (согласно (33)). Поэтому можем выбрать базис D_{Z_i} пространства Q_{Z_i} , такой, что $\sigma(c_i, w_i) = 1$ для некоторого $c_i \in D_{Z_i}$ и $\sigma(a, w_i) = 0$ при всех $a \in D_{Z_i} \setminus \{c_i\}$. Для любого $X \in \mathfrak{K}(V) \setminus \{Z_1, Z_2\}$ выберем произвольное линейно независимое множество D_X , удовлетворяющее равенству $\rho^{-1}(\langle X \rangle) = \langle D_X \rangle \oplus T$. Очевидно, что если $\{X, Y\} = \{Z_1, Z_2\}$, то система уравнений (44) приобретает вид

$$\sigma(a, u_{b, Z_1}) + \sigma(b, u_{a, Z_2}) = 0, \quad a \in D_{Z_1}, b \in D_{Z_2}. \quad (73)$$

Построим теперь семейство $\mathfrak{Q}' = (\langle E_X \rangle | X \in \mathfrak{K}(V)) \in \mathcal{Q}(V)$ в соответствии с леммой 5.8, используя выбранные выше множества D_X . При этом в качестве решения системы (73) выбираем $(u_{a, Z_2}, u_{b, Z_1} | a \in D_{Z_1}, b \in D_{Z_2})$, где

$$u_{a, Z_2} = \begin{cases} w_2, & \text{если } a = c_1, \\ 0, & \text{если } a \in D_{Z_1} \setminus \{c_1\}; \end{cases} \quad u_{b, Z_1} = \begin{cases} -w_1, & \text{если } b = c_2, \\ 0, & \text{если } b \in D_{Z_2} \setminus \{c_2\}. \end{cases}$$

Непосредственно проверяется, что эти элементы действительно образуют решение системы (73). Выбор всех остальных элементов, требуемых в лемме 5.8, несуществен. Положим теперь $v = c_1 + \sum_{Y \in \mathfrak{K}(V)} u_{c_1, Y}$. Тогда $v \in E_{Z_1} \subseteq C_{\mathfrak{Z}_1}^{\mathfrak{Q}'}(V)$. В то же время если $v \in C_{\mathfrak{Z}_1}^{\mathfrak{Q}}(V)$, то $u_{c_1, Y} = 0$ для всех $Y \in \mathfrak{K}(V) \setminus \mathfrak{Z}_1$ ввиду того, что сумма Q_X и $H_X(V)$ по всем $X \in \mathfrak{K}(V)$ прямая (см. доказательство леммы 5.12). В частности, в этом случае $u_{c_1, Y} = 0$ при любом $Y \in \mathfrak{Z}_2$, что неверно, так как $u_{c_1, Z_2} = w_2 \neq 0$. Таким образом, $v \notin C_{\mathfrak{Z}_1}^{\mathfrak{Q}}(V)$ и $C_{\mathfrak{Z}_1}^{\mathfrak{Q}'}(V) \neq C_{\mathfrak{Z}_1}^{\mathfrak{Q}}(V)$.

II. Предположим теперь, что выполнено одно из условий 1–3. Тогда $T = \{0\}$, так как σ невырождена на S_1 . Если выполнено условие 1, то $\mathcal{A} = \{\mathfrak{A}\}$, где $\mathfrak{A} = \{S_1\}$ (см. лемму 4.2). Если же выполнено условие 2 или 3, то легко видеть, что $\mathcal{A} = \{\mathfrak{A}\}$, где $\mathfrak{A}$ — множество всех подпространств S_1 , имеющих тип 1. Отметим, что если a, b — произвольный базис S_1 , в котором σ имеет указанную в условии 2 или 3 матрицу, то $\mathfrak{A} = \{\langle a \rangle, \langle b \rangle\}$ (последнее множество не зависит от выбора указанного базиса a, b). Из включения $S_0 \subseteq T$ и равенства $T = \{0\}$ следует равенство $S_0 = \{0\}$. Поэтому $\mathcal{B} = \{\emptyset\}$ и $\mathfrak{K}(G(\mathfrak{A})) = \{G(\mathfrak{A})\}$. Кроме того, очевидно, что $\mathcal{Q}(G(\mathfrak{A})) = \{(\langle X \rangle | X \in \mathfrak{K}(G(\mathfrak{A})))\}$. Таким образом, в данном случае условия (67)–(70) выполнены.

Если выполнено условие 4, то $S_0 = T = S_1 = V$, $\mathcal{A} = \{\emptyset\}$, $\mathcal{B} = \{\{V\}\}$, $\mathfrak{K}(V) = \{\{0\}\}$, а множества $I(V)$, $\mathfrak{J}(V)$, $\mathcal{I}(V)$, $\mathfrak{K}(V)$ и $\mathcal{K}(V)$ пусты (здесь $V = G(\emptyset)$). Поэтому в данном случае условия (67)–(70) выполнены. Впрочем, в случае выполнения условия 4 единственность полного ∇ -ортогонального разложения пространства V тривиальна. Пусть теперь выполнено условие 5. Тогда $\mathcal{A} = \{\emptyset\}$, $\mathcal{B} = \{\emptyset\}$ и $\mathfrak{K}(V) = \{V\}$, где $V = G(\emptyset)$. Это показывает, что выполнены условия (67)–(69). Осталось доказать, что условие (70) также выполнено. Если $T = \{0\}$, то это вытекает из легко проверяемого равенства $\mathcal{Q}(V) = \{(\langle X \rangle | X \in \mathfrak{K}(V))\}$. Считаем теперь, что $T \neq \{0\}$. Обозначим через $\mathfrak{L}$ элемент множества $\mathcal{K}(V)$, удовлетворяющий равенству $T = \bigoplus_{X \in \mathfrak{L}} H_X(V)$

(существование и единственность такого элемента следуют из леммы 5.5). Выберем произвольные семейства $\mathfrak{Q} = (Q_X \mid X \in \mathfrak{K}(V))$ и $\mathfrak{Q}' = (Q'_X \mid X \in \mathfrak{K}(V))$, принадлежащие $\mathcal{Q}(V)$, и покажем, что

$$C_{\mathfrak{X}}^{\mathfrak{Q}}(V) = C_{\mathfrak{X}}^{\mathfrak{Q}'}(V) \quad (74)$$

для любого $\mathfrak{X} \in \mathcal{K}(V)$. Если $\mathfrak{X} = \mathfrak{L}$, то равенство (74) верно ввиду того, что обе его части равны $\sum_{X \in \mathfrak{L}} \rho^{-1}(\langle X \rangle)$. Пусть теперь $\mathfrak{X} \in \mathcal{K}(V) \setminus \{\mathfrak{L}\}$. Для каждого $X \in \mathfrak{K}(V)$ выберем некоторый базис D_X пространства Q_X . Воспользовавшись замечанием 5.4, выберем также в конструкции леммы 5.8 элементы $u_{a,Y} \in H_Y(V)$ ($a \in D_X$, $X, Y \in \mathfrak{K}(V)$) таким образом, что

$$Q'_X = \left\langle a + \sum_{Y \in \mathfrak{K}(V)} u_{a,Y} \mid a \in D_X \right\rangle = \left\langle a + \sum_{Y \in \mathfrak{L}} u_{a,Y} \mid a \in D_X \right\rangle \quad (75)$$

для любого $X \in \mathfrak{K}(V)$ (здесь последнее равенство вытекает из того, что $u_{a,Y} = 0$ при $Y \in \mathfrak{K}(V) \setminus \mathfrak{L}$). Пусть $a \in D_X$, где $X \in \mathfrak{X}$, и $Y \in \mathfrak{L}$. Тогда

$$\sigma(b, u_{a,Y}) = \sigma(a, u_{b,X}) + \sigma(b, u_{a,Y}) = -\sigma(a, b) = 0$$

для любого $b \in D_Y$, так как $u_{b,X} = 0$ и $\sigma(a, b) = 0$. Поэтому $u_{a,Y} \nabla D_Y$ и, следовательно, $u_{a,Y} \nabla \rho^{-1}(Y)$, так как $u_{a,Y} \nabla T$ (см. (33)) и $\rho^{-1}(Y) \subseteq \rho^{-1}(\langle Y \rangle) = \langle D_Y \rangle \oplus T$. С другой стороны, $u_{a,Y} \nabla \rho^{-1}(I(V) \setminus Y)$, так как $u_{a,Y} \in H_Y(V)$. Это показывает, что $\Xi_{I(V)}(u_{a,Y}) = \emptyset$. Поэтому $u_{a,Y} = 0$ ввиду леммы 5.3. Из (75) вытекает теперь, что $Q'_X = Q_X$ для любого $X \in \mathfrak{X}$, откуда непосредственно следует требуемое равенство (74). Таким образом, условие (70) выполнено и в случае выполнения условия 5. ■

Замечание 6.3. Из леммы 5.5 следует, что если в условии 5 теоремы 6.4 заменить неравенство (66) на дизъюнкцию

$$T = \{0\} \vee \exists \mathfrak{L} \in \mathcal{K}(V) \ T = \bigoplus_{X \in \mathfrak{L}} H_X(V) \neq \{0\},$$

то полученный вариант условия 5 будет эквивалентен исходному.

6.4. Вычислительные аспекты

Будем считать, что поле F конечно, а пространство V конечномерно (и, следовательно, конечно). Носители F и V предполагаются содержащимися в множестве всех конечных строк, состоящих из нулей и единиц. Поле F подается на вход алгоритмам в виде набора, состоящего из носителя этого поля и таблиц сложения и умножения в F . Аналогично, пространство V задается для алгоритмов с помощью носителя этого пространства вместе с таблицами сложения в V и умножения элементов V на элементы поля F . Частичная симметричная билинейная функция σ подается на вход алгоритмам в виде таблицы своих значений; эта же таблица задает область определения $\diamond$ функции σ и ортогональность ∇ . Кроме того, произвольная функция $\varphi: V \rightarrow F$ также подается на вход алгоритмам в виде таблицы своих значений.

Замечание 6.4. Очевидно, что существует полиномиальный детерминированный алгоритм, который по произвольным F , V и функции $\varphi: V \rightarrow F$ вычисляет таблицу значений частичной функции σ_φ , определенной по φ согласно (1).

Теорема 6.5. Существует полиномиальный недетерминированный алгоритм, множество всех выходных значений которого при вычислении на произвольном входе вида (F, V, σ) совпадает с множеством всех $\mathfrak{S}$, таких, что $V = \bigoplus \mathfrak{S}$ — полное ∇ -ортогональное разложение пространства V .

Доказательство. Работа искомого алгоритма заключается в выборе произвольных $\mathfrak{A} \in \mathcal{A}$, $\mathfrak{B} \in \mathcal{B}$, $R \in \mathfrak{R}(G(\mathfrak{A}))$, $\mathfrak{Q} \in \mathcal{Q}(G(\mathfrak{A}))$ и возвращении на выходе множества

$$\mathfrak{A} \sqcup \mathfrak{B} \sqcup \{ \nu_{R, S_0}^{-1} (C_{\mathfrak{X}}^{\mathfrak{Q}}(G(\mathfrak{A}))) \mid \mathfrak{X} \in \mathcal{K}(G(\mathfrak{A})) \}$$

(см. теорему 5.2). При этом для построения $\mathfrak{A}$ и $\mathfrak{Q}$ следует воспользоваться методами, описанными в замечании 4.5 и лемме 5.8 (вместе с замечанием 5.3) соответственно. (Согласно замечаниям 4.5 и 5.4, эти методы позволяют построить все множества $\mathfrak{A} \in \mathcal{A}$ и все семейства $\mathfrak{Q} \in \mathcal{Q}(G(\mathfrak{A}))$.) Легко видеть, что все действия, требуемые в приведенном выше описании алгоритма, могут быть выполнены за полиномиальное время. (Смежность вершин в графе $\Delta(G(\mathfrak{A}))$ проверяема за полиномиальное время ввиду леммы 5.7 и замечания 5.3.) ■

Приведем теперь две теоремы, первая из которых (теорема 6.6) непосредственно следует из теорем 6.1 и 6.4, а вторая (теорема 6.7) — из п. 1 теоремы 6.2.

Теорема 6.6. Следующие условия могут быть проверены с помощью полиномиального детерминированного алгоритма, на вход которому подается произвольная тройка вида (F, V, σ) :

- 1) ∇ -неразложимость V ;
- 2) единственность полного ∇ -ортогонального разложения пространства V .

Теорема 6.7. Существует полиномиальный детерминированный алгоритм, который для произвольного входа вида $(F, V, \sigma, \mathfrak{S}, \mathfrak{S}')$, такого, что $\text{char } F \neq 2$, а $V = \bigoplus \mathfrak{S}$ и $V = \bigoplus \mathfrak{S}'$ — полные ∇ -ортогональные разложения пространства V , проверяет, являются ли эти разложения σ -эквивалентными.

Отметим, что в замечании 6.4 и теоремах 6.5–6.7 полиномиальность (полиномиальное время работы) алгоритмов означает, что время их работы на указанных входах не превосходит $O((l(|F| + |V|))^c)$ для некоторой константы $c > 0$, где l — максимальная длина строк из $F \cup V$.

Автор благодарит О. А. Логачёва, А. А. Сальникова и В. В. Яценко за постановку первоначальной проблемы (см. задачу 2.17 из книги [3]) и признателен математикам Института проблем информационной безопасности МГУ им. М. В. Ломоносова (в котором он имеет честь работать), а также руководителям и участникам семинара «Кольца и модули» кафедры высшей алгебры механико-математического факультета указанного университета за полезные обсуждения настоящей работы.

ЛИТЕРАТУРА

1. Анохин М. И. О расщепляемости p -ичных функций // Матем. сб. 2007. Т. 198. № 7. С. 31–44.
2. Логачёв О. А., Сальников А. А., Яценко В. В. Некоторые характеристики «нелинейности» групповых отображений // Дискрет. анализ и исслед. опер. 2001. Т. 8. № 1. С. 40–54.
3. Логачёв О. А., Сальников А. А., Яценко В. В. Булевы функции в теории кодирования и криптологии. М.: МЦНМО, 2004.
4. Newman M. Integral matrices. New York and London: Academic Press, 1972.